Владимирский государственный университет

Н.Ю. Куранова

ТЕОРИЯ СРАВНЕНИЙ И ЕЁ АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ

Учебно-практическое пособие

Электронное издание

Владимир
2023

Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

Н. Ю. КУРАНОВА

ТЕОРИЯ СРАВНЕНИЙ И ЕЁ АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ

Учебно-практическое пособие

Электронное издание

ISBN 978-5-9984-1848-8

Владимир 2023

УДК 511.11

ББК 22.141

Рецензенты:

Кандидат физико-математических наук, доцент
доцент кафедры вычислительной техники и систем управления
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
А. В. Шутов

Кандидат физико-математических наук, доцент
доцент кафедры специальной техники и информационных технологий
Владимирского юридического института ФСИН России
А. В. Хорошева

Куранова, Н. Ю. ТЕОРИЯ СРАВНЕНИЙ И ЕЁ АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ [Электронный ресурс] : учеб.-практ. пособие / Н. Ю. Куранова; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2023. – 456 с. – ISBN 978-5-9984-1848-8. – Электрон. дан. (258 Мб). – 1 электрон. опт. диск (DVD-ROM). – Систем. требования: Intel от 1,3 ГГц ; Windows XP/7/8/10 ; Adobe Reader ; дисковод DVD-ROM. – Загл. с титул. экрана.

Доступно и всесторонне рассмотрены основные понятия теории сравнений, ее арифметические приложения. Предложены разнообразные примеры и задачи, а также решения типовых заданий. Упражнения и задачи могут быть использованы как задания контрольных работ. В конце пособия предложены задания для самостоятельной работы студентов, а также практикум по рассмотренным темам теории сравнений. Составлено в соответствии с учебной программой по дисциплине «Алгебра и теория чисел».

Предназначено для студентов 1 – 2-го курсов высших учебных заведений, обучающихся по направлению 44.03.05 – Педагогическое образование. Пособие адресовано широкому кругу учащихся, абитуриентов, студентов педагогических вузов, учителей.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Библиогр.: 15 назв.

ISBN 978-5-9984-1848-8

Оглавление

Кафедра ФМО и ИТ

Кафедра ФМО и ИТ

Начало

Содержание

◄ ►

◄◄ ►►

Страница 6 из 456

Назад

На весь экран

Закрыть

Кафедра ФМО и ИТ

Кафедра ФМО и ИТ

Кафедра ФМО и ИТ

Глава 7. АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

ПРАКТИКУМ

1. Делимость целых чисел. Теорема о делении с остатком. НОД и НОК.Взаимно простые числа
2. Системы счисления
3. Линейные диофантовы уравнения
4. Сравнения в кольце целых чисел. Кольцо классов вычетов по данному модулю
5. Числовые функции. Функция Эйлера
6. Решение сравнений
7. Системы сравнений
8. Порядок числа по данному модулю. Первообразные корни. Индексы по простому модулю
9. Двучленные сравнения. Квадратичные вычеты. Показательные двучленные сравнения. Символ Лежандра

Кафедра ФМО и ИТ

Кафедра ФМО и ИТ

"Математики до сих пор безуспешно пытались обнаружить какой-то порядок в последовательности простых чисел, и у нас есть основания полагать, что это загадка, в которую человеческий разум никогда не проникнет." (Леонард Эйлер)

Кафедра ФМО и ИТ

Введение

Основная задача теории чисел - изучение свойств целого числа. Ряд важных проблем этой теории непосредственно связан с понятием сравнения двух чисел по данному модулю.

Учебно-практическое пособие посвящено изучению свойств срав нимых между собой чисел по данному модулю и арифметических приложений теории делимости.

Пособие должно оказать помощь в овладении основными понятиями, утверждениями и методами теории сравнений, а также в умении применять их при решении различных математи ческих задач.

Весь материал пособия разбит на разделы и подразделы, в которых приведены основные теоретические сведения (определения, утверждения и правила), примеры и задачи с подробными решениями, а также варианты для самостоятельного решения типовых задач. Такое изложение материала позволит студентам, изучающим вопросы теории чисел, овладеть стандартными приёмами и навыками и впоследствии творчески применять их в решении сложных задач.

Кафедра ФМО и ИТ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

$a \equiv b (\mathrm{mod}\ p)$ — число a сравнимо с числом b по модулю p;
$n \vdots m$ — n делится на m;
$n \mid m$ — число n делит число m;
$n \nmid m$ — число n не делит число m;
$p^a \top n$ — p^a делит n, но p^{a+1} не делит n.

Множества

$\mathbb{P}$ — множество всех простых чисел;
$\mathbb{N}$ — множество всех натуральных чисел;
$\mathbb{Z}$ — множество всех целых чисел;
$\mathbb{Q}$ — множество всех рациональных чисел;
$\mathbb{R}$ — множество всех действительных чисел;
$m\mathbb{Z}$ — множество кратных m целых чисел;
$\mathbb{Z}_m$ — множество вычетов по модулю m;
$\mathbb{U}_m$ — мультипликативная группа кольца $\mathbb{Z}_m$;
$\mathbb{Z}[i]$ — кольцо гауссовых чисел.

Функции

$\mid a \mid$ — порядок элемента a;
$n!$ — факториал числа n;
НОД(a, b) — наибольший общий делитель чисел a и b;
НОК(a, b) — наименьшее общее кратное чисел a и b;

$[x]$ — целая часть числа x;

$\{x\}$ — дробная часть числа x;

$N(z)$ — норма гауссова числа;

$\overline{z}$ — сопряженное к комплексному числу z;

$\overline{a}$ — класс вычетов, содержащий число a;

$\theta(a \mod m)$ — порядок (показатель) числа a по модулю m;

$\mathrm{ind}_a b$ — индекс числа b по модулю p и первообразному корню (основанию) a;

$\left(\frac{a}{p}\right)$ — символ Лежандра;

$\varphi(n)$ — Функция Эйлера числа n.

$\tau(n)$ — число натуральных делителей числа n;

$\sigma(n)$ — сумма натуральных делителей числа n.

Глава 1. ТЕОРИЯ СРАВНЕНИЙ

1.1. Сравнения в кольце $\mathbb{Z}$

Понятие сравнения было введено впервые Гауссом его знаменитой книге «Исследования по арифметике». Гаусс начал писать ее в 19 лет (1796 г.) и значительная часть сочинения была написана им в студенческие годы. В первом разделе книги Гаусс дал понятие сравнения. Сравнения по модулю — очень важное открытие в математике, они помогают выполнять вычисления любого типа.

Исследования Гаусса в этой области арифметики были революционными для математики начала XIX века и позволили ученым обнаруживать структуры, до этого скрытые. Сегодня арифметика сравнений по модулю, также называемая модульной арифметикой, является фундаментальной для безопасности в интернете, где сравнения используются для величин, превышающих количество атомов во Вселенной.

Определение. *Модулем m называется натуральное число больше единицы.*

Определение. *Целые числа a и b называются сравнимыми по натуральному модулю m, если разность a-b делится на m.*

Записывается это так: $a \equiv b \ (mod\ m)$.

Пример. Сравнимы ли числа a и b по модулю m.

$$a = 48, b = 18, m = 10.$$

Заметим, что $48 - 18 = 30, 30 \vdots 10$. Следовательно, $28 \equiv 18(10)$.

Теорема. *Целые числа a и b сравнимы по натуральному модулю m тогда и только тогда, когда числа a и b имеют одинаковые остатки при делении на m.*

Доказательство.

По теореме о делении с остатком целые числа a и b можно единственным образом представить в виду

$$a = mq_1 + r_1, q_1 \in \mathrm{Z}, 0 \leq r_1 \leq m,$$

$$b = mq_2 + r_2, q_2 \in \mathrm{Z}, 0 \leq r_2 \leq m.$$

Докажем сначала, что если $a \equiv b \ (mod\ m)$, то $r_1 = r_2$.

Так как $a \equiv b\ (mod\ m)$, то $(a-b) \vdots m$. Но $a-b=(mq_1+r_1)-(mq_2+r_2)=m(q_1-q_2)+(r_1-r_2)$.Тогда, так как $(a-b) \vdots m$ и $m(q_1-q_2) \vdots m$, то и, следовательно, $(r_1-r_2) \vdots m$.

Так как $0 \le r_{1,2} \le m$, то $0 \le r_1-r_2 \le m$. Очевидно, что такое возможно только, если $r_1-r_2=0$. Отсюда $r_1=r_2$. Теперь докажем, что если $r_1=r_2=r$ (r – натуральное число или 0), то $a=mq_1+r$ и $b=mq_2+r$, тогда $a-b=m(q_1-q_2)+(r-r)=m(q_1-q_2)$, следовательно, $(a-b) \vdots m$, а потому $a \equiv b\ (m)$. ■

Критерий сравнения. *Целые числа a и b называются сравнимыми по натуральному модулю m, если*

1) a и b имеют одинаковые остатки от деления на m;

2) $a-b$ делится на m, т.е. $a-b=mq$ для подходящего целого q;

3) $a=b+mq$ для некоторого целого q.

Пример. Проверить истинность сравнений

$$a)\ 75 \equiv 18\ (13);\ b)\ 174 \equiv 18\ (13).$$

Решение.

Способ 1. $a)\ 75-18=57,57$ не делится на 13, поэтому сравнение $75 \equiv 18\ (13)$ ложно.

$b)\ 174-18=156, 156 \vdots 13$, сравнение $174 \equiv 18\ (13)$ истинно.

Способ 2. $a)\ 75 = 13 \cdot 5 + 10, r_1 = 10, 18 = 13 \cdot 1 + 5, r_2 = 5.$

$r_1 \neq r_2$, следовательно, $75 \equiv 18\ (13)$ ложно.

$b) 174 = 13 \cdot 13 + 5, r_1 = 5, 18 = 13 \cdot 1 + 5, r_2 = 5, r_1 = r_2$,следовательно, сравнение $174 \equiv 18\ (13)$ истинно.

1.2. Основные свойства сравнений

Теорема. *Отношение сравнения по модулю является отношением эквивалентности на множестве целых чисел.*

Отношение сравнения по модулю m рефлексивно, так как $m|\ (a - a)$ для любого целого числа a, т.е. $a \equiv a(m)$. Отношение сравнения по модулю m симметрично в силу условия критерия. Отношение сравнения по модулю m транзитивно.

Действительно, если $a \equiv b(mod\ m), b \equiv c(mod\ m)$, то $m|(a - b)$, $(b - c)$. Следовательно, $(a - b) + (b - c) = a - c$ и $a \equiv c(mod\ m)$. ■

Свойство 1. Сравнения по одинаковому модулю можно почленно складывать.

$a_1 \equiv b_1(mod\ m), a_2 \equiv b_2(mod\ m), \ldots, a_k \equiv b_k(mod\ m), \rightarrow$

$$a_1 + a_2 + \cdots + a_k \equiv b_1 + b_2 + \cdots + b_k(\ mod\ m).$$

Свойство 2. Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, изменив его знак на обратный.

$$a+b \equiv c \pmod{m} \rightarrow a \equiv c-b \pmod{m}.$$

Свойство 3. К любой части сравнения можно прибавить любое число, кратное модулю.

$$a \equiv b \pmod{m} \rightarrow a+mt \equiv b+mk \pmod{m} \ (t, k \in Z).$$

Свойство 4. Сравнения по одинаковому модулю можно почленно перемножать

$$a \equiv b \ (mod\ m),\ c \equiv d \ (mod\ m) \rightarrow ac \equiv bd \ (mod\ m)$$

и, следовательно,

Свойство 5. Обе части сравнения можно возвести в одну и ту же степень.

$$a \equiv b \ (mod\ m) \rightarrow a^k \equiv b^k (mod\ m).$$

Свойство 6. Если $a_0 \equiv b_0\ (m)$, $a_1 \equiv b_1\ (mod\ m)$, …, $a_n \equiv b_n\ (m)$, $x \equiv y(\ m)$, то $a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv b_0 y^n + b_1 y^{n-1} + \ldots + b_n\ (m)$.

Свойство 7. Обе части сравнения можно разделить на их общий делитель, взаимно простой с модулем.

$$a \equiv b \pmod{m},\ (a, b) = c,\ (c, m) = 1 \rightarrow \frac{a}{(a,b)} \equiv \frac{b}{(a,b)} (mod\ m)$$

Свойство 8. Обе части сравнения и его модуль можно умножить на одно и то же целое число или разделить на их общий делитель.

$$a \equiv b \pmod{m} \rightarrow ak \equiv bk \pmod{mk},$$

$$a = a_1 d,\ b = b_1 d,\ m = m_1 d \rightarrow a_1 \equiv b_1 \pmod{m_1}.$$

Свойство 9. Если сравнение $a \equiv b$ имеет место по нескольким разным модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.

$$a \equiv b \pmod{m_1},\ a \equiv \mathrm{b} \pmod{m_2},\ \ldots,\ a \equiv b \pmod{m_\mathrm{k}} \rightarrow$$

$$a \equiv b \pmod{НОК(m_1, \ldots, m_\mathrm{k})}.$$

Свойство 10. Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.

$$a \equiv b \pmod{m},\ d \mid m \rightarrow a \equiv b \pmod{d}.$$

Свойство 11. Если одна часть сравнения и модуль делятся на некоторое число, то и другая часть сравнения должна делиться на то же число.

1.3. Кольцо классов вычетов. Полная и приведенная системы вычетов

Отношение $\equiv_m$ сравнимости по произвольному модулю m есть отношение эквивалентности на множестве целых чисел. Это отношение эквивалентности индуцирует разбиение множества целых чисел на классы эквивалентных между собой элементов, т.е. в один класс объединяются числа, дающие при делении на m одинаковые остатки. Число классов эквивалентности $\equiv_m$ ("индекс эквивалентности $\equiv_m$ ") в точности равно m.

Определение. *Классом вычетов $\bar{a}$ по натуральному модулю m называется множество целых чисел, сравнимых с некоторым данным целым числом a по модулю m.*

$$\bar{a} = \{x \in Z | x \equiv a \ (mod\ m)\}.$$

Пример. Определить классы вычетов по модулю $m=9$.

При делении целого числа на 9 получим следующие всевозможные остатки: 0, 1, 2, 3, 4, 5, 6, 7, 8.

1) Все целые числа, дающие остаток 0 при делении на 9, т.е. кратные 9, будут сравнимы между собой по модулю 9, следовательно, такие числа принадлежат одному классу вычетов по

mod 9. Этот класс вычетов можно записать как $\bar{0}$ или $x \equiv 0(9)$, где $x \in Z$.

$$\bar{0} = \{0, 9, 18, 27, \dots, -9, -18, -27, \dots\}.$$

Этот класс так же можно записать иначе: $\bar{9}, \overline{18}, \dots$

$x \equiv 9(9), x \equiv 18(9), x \equiv -18(9)$ и т.д.

2) Все целые числа, дающие остаток 1 при делении на 9, будут сравнимы между собой по модулю 9, следовательно, такие числа принадлежат одному классу вычетов по *mod 9*. Этот класс вычетов можно записать как $\bar{1}$ или $x \equiv 1(9)$, где $x \in Z$.

$1 = \{1,10, 19, 28, \dots, -8, -17, -26, \dots\}.$

Этот класс так же можно записать иначе: $\overline{10}, \overline{19}, \dots$

$x \equiv 10(9), x \equiv -8(9), x \equiv -26(9)$ и т.д.

3) Рассуждая аналогично, получим остальные классы вычетов по *mod 9:*

$\bar{2} = \{2, 11, 20, 29, \dots, -7, -16, -25, \dots\}$ или $x \equiv 2(9)$,

$\bar{3} = \{3, 12, 21, 30, \dots, -6, -15, -24, \dots\}$ или $x \equiv 3(9)$,

$\bar{4} = \{4, 13, 22, 31, \dots, -5, -14, -23, \dots\}$ или $x \equiv 4(9)$,

$5 = \{5, 14, 23, 32, \dots, -4, -13, -22, \dots\}$ или $x \equiv 5(9)$,

$\bar{6} = \{6, 15, 24, 33, \ldots, -3, -12, -21, \ldots\}$ или $x \equiv 6(9)$,

$\bar{7} = \{7, 16, 25, 34, \ldots, -2, -11, -20, \ldots\}$ или $x \equiv 7(9)$,

$8 = \{8, 17, 26, 35, \ldots, -1, -10, -19, \ldots\}$ или $x \equiv 8(9)$.

Следовательно, классов вычетов по *mod 9* будет 9: $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, 5, \bar{6}, \bar{7}, \bar{8}$.

Как известно, всякий класс эквивалентности определяется любым своим представителем. В нашем случае всякий вычет из класса вычетов по модулю *m* определяет этот класс.

Класс вычетов, содержащий число *a*, будем обозначать через $\bar{a}$. Так как при делении чисел возможны *m* различных остатков 0, 1, 2, ..., *m*−1, то существуют *m* различных классов вычетов по модулю *m*, а именно: $0 = \{k \cdot m \mid k \in Z\}$ — класс чисел, кратных m, $1 = \{k \cdot m + 1 \mid k \in Z\}$ — класс чисел, дающих в остатке 1 при делении на *m*, ..., $m-1 = \{k \cdot m + (m-1) \mid k \in Z\}$ — класс чисел, дающих в остатке $m-1$ при делении на *m*. В общем случае $a = \{m \cdot k + a \mid k \in Z\}$. Множество всех классов вычетов по данному модулю *m* будем обозначать через Z_m.

Введем на множестве Z_m операции сложения и умножения.

Определение. *Суммой классов вычетов* $\bar{a}$ *и* $\bar{b}$ *из* Z_m *называется класс вычетов, содержащий число* $a + b$, *т.е.* $\bar{a} + \bar{b} = \overline{a + b}$.

Пример. Если $m = 8$, то $\bar{5} + \bar{4} = \bar{9} = \bar{1}$.

Определение. Произведением классов вычетов $\bar{a}$ *и* $\bar{b}$ из Z_m называется класс вычетов, содержащий число $a\,b$, т.е. $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Пример. Если $m = 8$, то $\bar{5} \cdot \bar{4} = \overline{20} = \bar{4}$.

Теорема. *Множество Z_m классов вычетов по модулю m образует коммутативное кольцо с единицей относительно операций сложения и умножения классов вычетов.*

Доказательство.

Операция сложения и умножения классов вычетов на множестве Z_m коммутативны и ассоциативны, операция умножения дистрибутивна относительно операции сложения. Это следует из того, что указанные операции, согласно их определениям, сводятся к операциям над числами, для которых аналогичные свойства справедливы. Во множестве Z_m существует нулевой элемент, а именно $\bar{0}$. Противоположным для класса вычетов $\bar{a}$, очевидно, является класс вычетов $\overline{-a}$, т.е. $-\bar{a} = \overline{-a}$. Роль единичного элемента во множестве Z_m выполняет класс $\bar{1}$. Из всего изложенного следует, что Z_m образует коммутативное кольцо с 1. ■

Определение. *Так как Z_m — кольцо, то относительно операции сложения это множество образует абелеву группу. Ее называют аддитивной группой классов вычетов по модулю m.*

Теорема. *Если m — составное число, то кольцо Z_m содержит делители нуля. 2. Класс $\bar{a}$ из кольца Z_m обратим тогда и только тогда, когда НОД(a, m) = 1. 3. Если m — простое число, то Z_m является полем, в частности, не содержит делителей нуля.*

Доказательство.

1. Пусть m — составное число, тогда его можно представить в виде произведения двух натуральных чисел $m = p\,q$, каждое из которых меньше m. Очевидно, что $\bar{p} \neq \bar{0}$ и $\bar{q} \neq \bar{0}$. В тоже время $\bar{p} \cdot \bar{q} = \overline{p \cdot q} = \bar{0}$. Таким образом, в Z_m существуют элементы $\bar{p}$ и $\bar{q}$, которые отличны от нулевого, но их произведение равно $\bar{0}$, т.е. Z_m содержит делители нуля.

2. Если a обратим в Z_m, то существует $x \in Z_m$ такой, что $a \cdot x = 1$. Это значит, $\bar{a} \cdot \bar{x} = \bar{1}$ или $ax \equiv 1 \pmod m$. Из свойства следует, что НОД $(a, m) = 1$. Обратно.

Если a и m взаимно просты, то согласно теореме о взаимно простых числах существуют целые числа x и y такие, что $ax+my=1$. Тогда $ax+ my \equiv 1 \pmod m$. В таком случае ввиду свойства верно, что $ax \equiv 1 \pmod m$. Это значит, что $\overline{ax} = \bar{1}$ или $\bar{a} \cdot \bar{x} = \bar{1}$. Из последнего равенства следует, что $\bar{a}$ обратим в Z_m.

3. Так как m — простое число, то по п. 2 в Z_m каждый ненулевой элемент обратим, а, значит, Z_m — поле. ■

Определение. *Отметим, что множество обратимых элементов кольца Z_m образует абелеву группу относительно операции умножения. Ее называют мультипликативной группой обратимых элементов кольца Z_m.*

Выделим следующие свойства класса вычетов.

Свойство 1. *Любые два класса вычетов по mod m или совпадают, или не пересекаются. Объединение всех классов вычетов по модулю m есть множество Z_m.*

Доказательство.

Пусть классы вычетов $\bar{a}$ и $\bar{b}$ по *mod m* имеют общий элемент c. Покажем, что тогда $\bar{a} = \bar{b}$.

1. Покажем, что $\forall x \left((x \in \bar{a}) \to \left(x \in \bar{b}\right)\right)$.

   Имеем: $x \in \bar{a}$, следовательно, $x \equiv a(m)$,

$c \in \bar{a}$, следовательно, $x \equiv c(m)$, поэтому $a \equiv c(m)$. Тогда по транзитивности получим, что $x \equiv c(m)$.

Кроме того, $c \in \bar{b}$, следовательно, $c \equiv b(m)$, поэтому по транзитивности $x \equiv b(m)$. Значит, $x \in \bar{b}$.

2. Аналогично докажем, что $\forall y \left(\left(y \in \bar{b}\right) \to (y \in \bar{a})\right)$.

Имеем: $y \in \bar{b}$, следовательно, $y \equiv b(m)$,

$c \in \bar{b}$, следовательно, $c \equiv b(m)$, поэтому $b \equiv c(m)$. Тогда по транзитивности получим, что $y \equiv c(m)$.

Кроме того, $c \in \bar{a}$, следовательно, $c \equiv a(m)$, поэтому по транзитивности $y \equiv a(m)$. Значит, $y \in \bar{a}$.

Таким образом, из 1) и 2) получим, что $\bar{a} = \bar{b}$ (по определению равных множеств). ■

Свойство 2. *Если $\bar{a}$ и $\bar{b}$ - классы вычетов по mod m, $x \in \bar{a}, y \in \bar{b}$, то $\bar{a} = \bar{b}$ тогда и только тогда, когда $x \equiv y(m)$.*

Доказательство.

1. Если $\bar{a} = \bar{b}$, то $(\forall x \in \bar{a})(x \in \bar{b})$, но так как и $y \in \bar{b}$, то тогда $x \equiv y(m)$.
2. Если $x \equiv y(m)$, где $x \in \bar{a}, y \in \bar{b}$, то тогда $y \equiv x(m)$ и $x \equiv a(m)$, следовательно, по транзитивности получим, что $y \equiv a(m)$, поэтому $y \in \bar{a}$. Таким образом, по свойству 1, классы вычетов $\bar{a}$ *и* $\bar{b}$, как содержащие общий элемент *y* будут совпадать: $\bar{a} = \bar{b}$.

■

Свойство 3. *Если $\bar{a}$ – класс вычетов по mod m, то*

$$\bar{a} = \{a + mk | k \in Z\}.$$

Доказательство.

Имеем $\forall x \in \bar{a}$, $x \equiv a(m)$, отсюда получим, что $(x - a) \vdots m$, следовательно,

$$(\exists k \in \mathrm{Z})(x - a = mk).$$

Поэтому $x = a + mk$, где k – целое число. Но тогда $= \{x | x \equiv a(m)\} = \{a + mk | k \in \mathrm{Z}\}$. ■

Любое число из класса вычетов $\bar{a}$ mod m будем называть *представителем* этого класса вычетов.

Определение. *Любое число из класса эквивалентности $\equiv_m$ будем называть вычетом по модулю m. Совокупность вычетов, взятых по одному из каждого класса эквивалентности $\equiv_m$, называется полной системой вычетов по модулю m (в полной системе вычетов, таким образом, всего m штук чисел). Непосредственно сами остатки при делении на m называются наименьшими неотрицательными вычетами и, конечно, образуют полную систему вычетов по модулю m. Вычет называется абсолютно наименьшим, если он наименьший среди модулей вычетов данного класса.*

Пример. Пусть $m = 5$. Тогда:

0, 1, 2, 3, 4 - наименьшие неотрицательные вычеты;

-2, -1, 0, 1, 2 - абсолютно наименьшие вычеты.

Обе приведенные совокупности чисел образуют полные системы вычетов по модулю **5**.

Лемма. *1) Любые m штук попарно несравнимых по модулю m чисел образуют полную систему вычетов по модулю m.*

2) Если a и m взаимно просты, а x пробегает полную систему вычетов по модулю m, то значения линейной формы ax+b, где b - любое целое число, тоже пробегают полную систему вычетов по модулю m.

Доказательство.

Утверждение 1) – очевидно.

Докажем утверждение 2). Чисел $ax + b$ ровно m штук. Покажем, что они между собой не сравнимы по модулю m. Ну пусть для некоторых различных x_1 и x_2 из полной системы вычетов оказалось, что $ax_1 + b \equiv ax_2 + b \ (mod\ m)$. Тогда, по свойствам сравнений из предыдущего пункта, получаем: $ax_1 \equiv ax_2 \ (mod\ m)$, $x_1 \equiv x_2 \ (mod\ m)$ – противоречие с тем, что x_1 и x_2 различны и взяты из полной системы вычетов. ■

Поскольку все числа из данного класса эквивалентности получаются из одного числа данного класса прибавлением числа, кратного m, то все числа из данного класса имеют с модулем m один и тот же наибольший общий делитель. По некоторым соображениям, повышенный интерес представляют те вычеты, которые имеют с модулем m наибольший общий делитель, равный единице, т.е. вычеты, которые взаимно просты с модулем.

Определение. *Приведенной системой вычетов по модулю m называется совокупность всех вычетов из полной системы, взаимно простых с модулем m.*

Приведенную систему обычно выбирают из наименьших неотрицательных вычетов. Ясно, что приведенная система вычетов по модулю m содержит $\varphi(m)$ штук вычетов, где $\varphi(m)$ – функция Эйлера – число чисел, меньших m и взаимно простых с m.

Пример. Пусть $m = 42$. Тогда приведенная система вычетов суть: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

Лемма. *Любые $\varphi(m)$ чисел, попарно не сравнимые по модулю m и взаимно простые с модулем, образуют приведенную систему вычетов по модулю m.*

Доказательство.

Пусть M есть совокупность $\varphi(m)$ чисел, взаимно простых с m и попарно несравнимых по модулю m. Тогда эти числа принадлежат к различным классам вычетов, взаимно простым с модулем m. Поэтому множество M содержит по одному представителю из каждого такого класса. Следовательно, M есть приведённая система вычетов по модулю m. ■

Лемма. *Если $(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m , то ax так же пробегает приведенную систему вычетов по модулю m.*

Доказательство.

Действительно, чисел ax будет столько же, сколько и чисел x, т.е. $\varphi(m)$. Так как произведение двух чисел, взаимно простых с третьим числом m, есть число взаимно простое с m, то числа ax взаимно просты с m. Кроме того, числа ax попарно несравнимы по модулю m. В самом деле, если $ax_1 \equiv ax_2(m)$, то в силу условия НОД$(a, m) = 1$, следует, что $x_1 \equiv x_2(m)$, что невозможно. Таким образом, ax пробегает приведённую систему вычетов по модулю m. ■

1.4. Представление рациональных чисел цепными дробями

Определение. *Целое число, являющееся делителем каждого из целых чисел $a_1, a_2, \ldots, a_n$ называется общим делителем этих чисел. Общий делитель этих чисел называется их наибольшим общим делителем, если он делится на всякий общий делитель данных чисел.*

Пусть $\frac{a}{b}$ - рациональное число, причем $b>0$. Применяя к a и b алгоритм Евклида для определения их наибольшего общего делителя, получаем конечную систему равенств:

$$\left.\begin{aligned} a &= bq_1 + r_2, \\ b &= r_2 q_2 + r_3, \\ r_2 &= r_3 q_3 + r_4, \\ &\cdots\cdots\cdots\cdots, \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \\ r_{n-1} &= r_n q_n, \end{aligned}\right\}$$

где неполным частным последовательных делений $q_1, q_2, \ldots, q_{n-1}$ соответствуют остатки $r_2, r_3, \ldots, r_n$ с условием $b > r_2 > r_3 > \ldots > r_n > 0$, а соответствует остаток 0.

Системе равенств соответствует равносильная система

$$\left.\begin{aligned}
&\frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{\frac{b}{r_2}},\\
&\frac{b}{r_2} = q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},\\
&\frac{r_{n-1}}{r_n} = q_n,
\end{aligned}\right\}$$

из которой последовательной заменой каждой из дробей $\frac{b}{r_2}, \frac{r_2}{r_3}$ и т.д. ее соответствующим выражением из следующей строки получается представление дроби $\frac{a}{b}$ в виде:

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

Такое выражение называется правильной (конечной) цепной или правильной непрерывной дробью, при этом предполагается, что q_1 – целое число, а $q_2, \ldots, q_n$ - натуральные числа.

Имеются различные формы записи цепных дробей:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

$$\frac{a}{b} = q_1 + \frac{1}{q_2} + \frac{1}{q_3} + \ldots + \frac{1}{q_n}, \quad \frac{a}{b} = (q_1, q_2, \ldots, q_n). \ (q_1, q_2, \ldots, q_n) = q_1 + \frac{1}{(q_2, \ldots, q_n)}.$$

Числа $q_1, \ldots, q_n$ называются элементами цепной дроби.

Алгоритм Евклида дает возможность найти представление (или разложение) любого рационального числа в виде цепной дроби. В качестве элементов цепной дроби получаются неполные частные последовательных делений в системе равенств, поэтому элементы цепной дроби называются также неполными частными. Кроме того, равенства системы показывают, что процесс разложения в цепную дробь состоит в последовательном выделении целой части и перевертывании дробной части.

Разложение рационального числа $\frac{a}{b}$ имеет конечное число элементов, так как алгоритм Евклида последовательного деления a на b является конечным.

Каждая цепная дробь представляет определенное рациональное число, то есть равна определенному рациональному числу. Но возникает вопрос, не имеются ли различные представления одного и того же рационального числа цепной дробью? Оказывается, что не имеются, если потребовать, чтобы было $q_n > 1$.

Теорема. *Существует одна и только одна конечная цепная дробь, равная данному рациональному числу, но при условии, что* $q_n > 1$.

Доказательство.

1) Заметим, что при отказе от указанного условия единственность представления отпадает. В самом деле, при $q_n > 1$:

$$q_n = (q_n - 1) + \frac{1}{1},$$

так что представление можно удлинить:

$$(q_1, q_2, \dots, q_n) = (q_1, q_2, \dots, q_n - 1, 1).$$

Например, (2, 3, 1, 4, 2) = (2, 3, 1, 4, 1, 1).

2) Принимая условие $q_n > 1$, можно утверждать, что целая часть цепной дроби $(q_1, q_2, \ldots, q_n)$ равна ее первому неполному частному q_1. В самом деле:

1. если n=1, то
2. если n=2, то $(q_1, q_2) = q_1 + \frac{1}{q_2}, q_2 > 1$; поэтому $[(q_1, q_2)] = q_1$.
3. если n>2, то $(q_1, q_2, \ldots, q_n) = q_1 + \frac{1}{q_2 +}$

$$\ddots$$

$$+ \frac{1}{q_n},$$

где $q_2 + \frac{1}{q_3 +} > 1$, т.к. $q_2 \geq 1$.

$$\ddots$$

$$+ \frac{1}{q_n}$$

Поэтому и здесь $[(q_1, q_2, \dots, q_n)] = q_1$. Докажем то, что рациональное число $\frac{a}{b}$ однозначно представляется цепной дробью $(q_1, q_2, \dots, q_n)$, если $q_n > 1$.

Пусть $\frac{a}{b} = (q_1, q_2, \dots, q_n) = (q_1', q_2', \dots, q_n')$ с условием $q_n > 1$, $q_{n'}' > 1$. Тогда $\left[\frac{a}{b}\right] = q_1 = q_1'$, так что $(q_2, \dots, q_n) = (q_2', \dots, q_n')$. Повторным сравнением целых частей получаем $q_2 = q_2'$, а следовательно $(q_3, \dots, q_n) = (q_3', \dots, q_n')$ и так далее. Если $n = n'$, то в продолжении указанного процесса получим также $q_n = q_n'$. Если же $n \neq n'$, например $n' > n$, то получим $0 = \frac{1}{(q_{n+1}', \dots, q_{n'}')}$, что невозможно.

Замечания:

1. В случае разложения правильной положительной дроби первый элемент $q_1 = 0$, например, $\frac{77}{187} = 0 + \frac{1}{\frac{187}{77}} = (0,2,2,3)$.

2. При разложении отрицательной дроби (отрицательный знак дроби всегда относится к числителю) первый элемент будет отрицательным, остальные положительными, так как целая часть отрицательной дроби является целым отрицательным числом, а ее дробная часть, как всегда, положительна.

Пример. $-\frac{95}{42} = -3 + \frac{1}{\frac{42}{31}} = (-3,1,2,1,4,2)$

3. Всякое целое число можно рассматривать как непрерывную дробь, состоящую из одного элемента.

Пример. 5=(5); $\frac{1}{m} = (0, m)$.

Подходящие дроби. Их свойства

Задаче разложения обыкновенной дроби в непрерывную дробь противостоит обратная задача – обращения или свертывания цепной дроби $(q_1, q_2, \ldots, q_n)$ в простую дробь $\frac{a}{b}$.

Основную роль играют дроби вида: $\delta_1 = q_1, \delta_2 = (q_1, q_2), \delta_3 = (q_1, q_2, q_3), \ldots,$, которые называются подходящими дробями данной непрерывной дроби или соответствующего ей числа $\frac{a}{b}$.

Заметим, что $\frac{a}{b} = (q_1, q_2, \ldots, q_n) = \delta_n$. Считается, что подходящая дробь δ_k имеет порядок k.

Прежде чем приступить к вычислению подходящих дробей заметим, что δ_k переходит в δ_{k+1}, если в первой заменить δ_k выражением $q_k + \frac{1}{q_k + 1}$.

Имеем, $\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}$,

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_2 q_1 + 1}{q_2} = \frac{q_2 q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_3(q_2 P_1 + P_0) + P_1}{q_3(q_2 Q_1 + Q_0) + Q_1} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}, \ldots,$$

при этом принимается, что $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1$, $Q_1 = 1$, $P_2 = q_2 P_1 + P_0$, $Q_2 = q_2 Q_1 + Q_0$ и так далее.

Закономерность в построении формулы для δ_2 (ее числителя P_2 и знаменателя Q_2), сохраняется при переходе к δ_3 и сохранится также при переходе от k к (k+1).

Поэтому, на основании принципа математической индукции, для любого k, где $2 \le k \le n$, имеем

$\delta_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}$, причем $P_k = q_k P_{k-1} + P_{k-2}$; $Q_k = q_k Q_{k-1} + Q_{k-2}$.

Соотношения являются рекуррентными формулами для вычисления подходящих дробей, а также их числителей и знаменателей. Из

формул для числителя и знаменателя сразу видно, что при увеличении k они возрастают. Последовательное вычисление числителей P_k и знаменателей Q_k подходящих дробей по формулам удобно располагать по схеме:

		q_1	q_2	…	q_{k-2}	q_{k-1}	q_k	…	q_n
P_k	$P_0 = 1$	$P_1 = q_1$	P_2	…	P_{k-2}	P_{k-1}	P_k	…	P_n
Q_k	$Q_0 = 0$	$Q_1 = 1$	Q_2	…	Q_{k-2}	Q_{k-1}	Q_k	…	Q_n

Пример. Найти подходящие дроби к цепной дроби (2,2,1,3,1,1,4,3).

	2	2	1	3	1	1	4	3
P_k	2	5	7	26	33	59	269	866
	1	2	3	11	14	25	114	367

Подходящие дроби $\frac{P_n}{Q_n}$ равны соответственно

$$\frac{2}{1}; \frac{5}{2}; \frac{7}{3}; \frac{26}{11}; \frac{33}{14}; \frac{59}{25}; \frac{269}{114}; \frac{866}{367}.$$

1.5. Определение обратного числа к заданному числу по модулю *m*

Определение. *Целое число a называется обратным к целому числу b по mod m, если* $ab \equiv 1(m)$.

Пример. m=9, классы вычетов по mod 7: $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}$. Пусть b=7. Найдем число a, обратное к числу b=7 по mod 9, то есть такое число a, что $ab \equiv 1(9)$ или $a \cdot 7 \equiv 1(9)$. При a=4 получим верное сравнение $4 \cdot 7 \equiv 1(9)$, так как $(28-1) \vdots 9$, следовательно, число 4 является обратным к числу 7 по mod 9. При a= 13 получим так же верное сравнение $13 \cdot 7 \equiv 1(9)$, так как $(91-1) \vdots 9$, следовательно, число 13 так же является обратным к числу 7 по mod 9. И таких чисел бесконечно много, но для удобства будем выбирать наименьшее положительное.

Заметим, что для класса вычетов $\bar{b}$ существует единственный класс $\bar{a}$, обратный к $\bar{b}$ по модулю m.

Теорема. *Пусть* $a \in \mathrm{Z}, m \in \mathrm{N}, \mathrm{НОД}\,(a, m) = 1, \frac{m}{a} = \frac{P_n}{Q_n}$, P_{n-1} *числитель предпоследней подходящей дроби. Тогда имеет место сравнение:*

$$a \cdot ((-1)^n P_{n-1}) \equiv 1(mod\ m),$$

Кафедра ФМО и ИТ

то есть число $(-1)^n P_{n-1}$ *является обратным к числу* a *по модулю* m.

Доказательство.

Так как $\frac{m}{a} = \frac{P_n}{Q_n}$ и НОД $(a, m) = 1$, то дробь $\frac{m}{a}$ является несократимой , следовательно,

$$m = P_n, a = Q_n.$$

Тогда получим равенство

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1}Q_n},$$

отсюда:

$$\frac{m}{a} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1}Q_n},$$

следовательно, $mQ_{n-1} - aP_{n-1} = (-1)^{n-1}$. Умножим данное равенство на $(-1)^{n-1}$, тогда получим: $m(-1)^{n-1}Q_{n-1} - a(-1)^{n-1}P_{n-1} = 1$.

Обозначим через c произведение $(-1)^{n-1}Q_{n-1}$, тогда это равенство примет вид

$$mc - a(-1)^{n-1}P_{n-1} = 1,$$

отсюда

$$mc = a(-1)^{n-1}P_{n-1} + 1.$$

Так как $mc \vdots m$, то $mc \equiv 0\ (mod\ m)$, следовательно, получим, что и

$$a(-1)^{n-1}P_{n-1} + 1 \equiv 0(mod\ m)$$

или

$$a(-1)^{n-1}P_{n-1} \equiv -1(mod\ m),$$

а тогда

$$a(-1)^{n}P_{n-1} \equiv 1(mod\ m).$$

Из этого следует, что число $(-1)^n P_{n-1}$ является обратным к числу a по mod m. ■

Пример. m=7, a=3, $\frac{m}{} = \frac{7}{3}$.

$$\frac{7}{3} = [2;3], a_0 = 2, a_1 = 3.$$

q_i		2	3
P_i	1	2	7
Q_i	0	1	3

$$\frac{P_0}{Q_0} = \frac{2}{1}, \frac{P_1}{Q_1} = \frac{7}{3}.$$

n=1 $(-1)^n P_0 = -1 \cdot 2 = -2; -2 \equiv 5(mod\ 7)$,

следовательно, $(-1)^n P_0 \equiv 5(mod\ 7)$, поэтому каждое число из класса вычетов $\bar{5}$ по mod 7 будет обратным числом к числу a=3 по mod 7:

например,

1) $b = 5, 5 \in \bar{5}, 3 \cdot 5 \equiv 1(mod\ 7)$ верно, следовательно, число 5 является обратным к числу 3 по mod 7.
2) $b = 12, 12 \in \bar{5}, 3 \cdot 12 \equiv 1(mod\ 7)$ верно, следовательно, число 12 является обратным к числу 3 по mod 7.
3) $b = -2, -2 \in \bar{5}, 3 \cdot (-2) \equiv 1(mod\ 7)$ верно, следовательно, число (-2) является обратным к числу 3 по mod 7.
   Т.е. $\forall x \in \bar{5}$ будет обратным к числу 3 по mod 7.

1.6. Функция Эйлера

В теории чисел рассматриваются разнообразные функции, значения которых при натуральных значениях n связаны с арифметической природой n. Множество рассматриваемых функций удобнее не ограничивать заранее какими-либо требованиями, кроме единственного требования: каждая функция должна быть определена для всех натуральных значений аргумента.

Обычно в теории чисел рассматривают числовые функции, которые либо вообще определены только при натуральных значениях аргумента, либо функции, для которых натуральные значения аргумента

являются характерными точками, определяющими величину функции и в других точках.

Определение. *Функцией Эйлера $\varphi(n)$ называется функция, определяющая для каждого натурального числа n количество неотрицательных чисел, меньших n и взаимно простых с n.*

Заметим, что функцию Эйлера $\varphi(n)$ можно определить и как функцию, значение которой равно числу классов вычетов по модулю n, взаимно простых с модулем n.

Составим таблицу значений $\varphi(n)$ для n от 1 до 9 :

n	1	2	3	4	5	6	7	8	9
$\varphi(n)$	1	1	2	2	4	2	6	3	6

При n=1, $\varphi(1)$: количество натуральных чисел, ≤ 1 и взаимно простых с 1, равно 1 – это само число n=1. Следовательно, $\varphi(1)$=1.

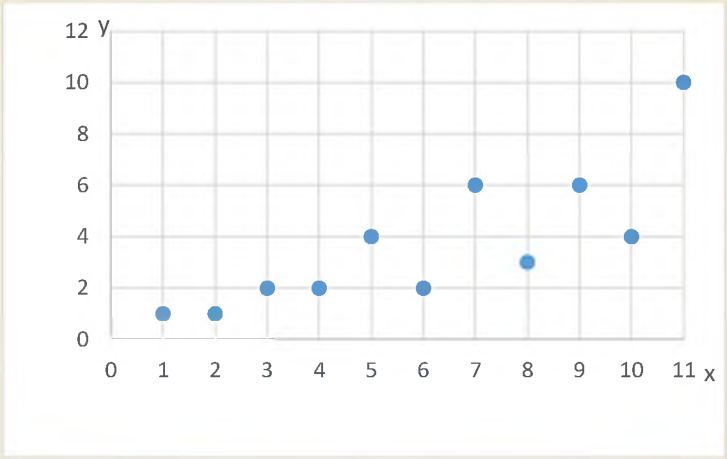
При n=2, $\varphi(2)$: количество натуральных чисел, ≤ 2 и взаимно простых с 2, равно 1 – это число 1. Следовательно, $\varphi(2)$=1.

При n=3, $\varphi(3)$: количество натуральных чисел, ≤ 3 и взаимно простых с 3, равно 2 – это числа 1 и 2. Следовательно, $\varphi(3)$=2.

При n=4, $\varphi(4)$: количество натуральных чисел, ≤ 4 и взаимно простых с 4, равно 2 – это числа 1, 3. Следовательно, $\varphi(4)$=2.

При n=5, $\varphi(5)$: количество натуральных чисел, не превосходящих 5 и взаимно простых с 5, равно 4 – это числа 1, 2, 3, 4. Следовательно, $\varphi(5)$=4.

Изобразим графически функцию Эйлера $\varphi(n)$, полагая $y = \varphi(n)$, где $x \in N$.



Графически $\varphi(n)$ есть множество M точек плоскости.

Теорема. *Пусть a и b – натуральные числа и НОД (a, b) = 1. Тогда имеет место равенство:*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

то есть функция $\varphi(n)$ является мультипликативной.

Доказательство.

1. Рассмотрим натуральные числа $x \leq ab$: $x \in \{1, 2, \dots, b, \dots, ab\}$. Разделим каждое такое число x на натуральное число b с остатком:

$$\exists!\, q, r \in \mathrm{N}, x = bq + r, 0 \leq r < b.$$

Так как НОД (x, b) = НОД (b,r), то НОД (x, b)=1 тогда и только тогда, когда НОД (b,r)=1. Но чисел x, взаимно простых с b, будет $\varphi(b)$, поэтому, чисел r тоже таких будет всего $\varphi(b)$.

2. Если одно из таких чисел r обозначить через k, то числа

$$k, k + b, k + 2b, k + 3b, \dots, k + (a - 1)b$$

образуют полную систему вычетов по модулю a.

3. Получили, что каждому числу k, взаимно простому с числом b, соответствует $\varphi(a)$ чисел, взаимно простых с a, а, значит, взаимно простых и с числом ab. Поэтому всего чисел x, взаимно простых с ab будет $\varphi(a) \cdot \varphi(b)$, то есть

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b). \quad \blacksquare$$

Теорема. *Пусть n – натуральное число, большее 1 и имеет каноническое разложение*

$$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_s}^{\alpha_s},$$

где $p_1, p_2, \dots, p_s$ *– попарно различные положительные простые числа,* $\alpha_1, \alpha_2, \dots, \alpha_s$ *– натуральные числа. Тогда имеет место равенство:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right).$$

Доказательство.

Так как функция $\varphi(n)$ является мультипликативной, то получим

$$\varphi(n) = \varphi({p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_s}^{\alpha_s}) = \varphi({p_1}^{\alpha_1})\varphi({p_2}^{\alpha_2}) \dots \varphi({p_s}^{\alpha_s}).$$

Если рассмотреть числа 1,2, 3, …, p^α,то чисел $\leq p^\alpha$ и взаимно простых с p^α, будет столько, сколько чисел $\leq p^\alpha$, не делится на p, то есть равно

$$p^\alpha - \left[\frac{p^\alpha}{p}\right].$$

Преобразуем эту разность:

$$p^\alpha - \left[\frac{p^\alpha}{p}\right] = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right),$$

следовательно, $\varphi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right)$.

Учитывая это, получим

$$\varphi(n) = {p_1}^{\alpha_1}\left(1-\frac{1}{p_1}\right){p_2}^{\alpha_2}\left(1-\frac{1}{p_2}\right)\dots{p_s}^{\alpha_s}\left(1-\frac{1}{p_s}\right)=$$

$$= {p_1}^{\alpha_1}{p_2}^{\alpha_2}\dots{p_s}^{\alpha_s}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_s}\right)=$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_s}\right).$$

■

Примеры.

1. $\varphi(270)=\varphi(2\cdot3^3\cdot5)=3^2\,(2-1)\,(3-1)\,(5-1)=72$;
2. $\varphi(700000)=\varphi(2^5\,5^5\,7)=2^4\,\,5^4(2-1)\,(5-1)\,(7-1)=240000$;
3. $\varphi(45375)=\varphi(3\,\,5^3 11^2)=5^2\,11\,2\,10=22000$

Заметим, что если $n = p$, где p – простое число, то среди чисел 1, 2, 3, …, p будут взаимно простые с модулем p, кроме самого числа p, так как НОД$(p, p) = p, p \neq 1$. Поэтому чисел $\leq p$ и взаимно простых с p будет всего $p - 1$, так что получим равенство

$$\varphi(p) = p - 1.$$

1.7. Теоремы Эйлера и Ферма. Теорема Вильсона

Теорема (Эйлера). *Пусть* $m \in N$, $(a,m)=1$, $\varphi(m)$ – *функция Эйлера. Тогда* $a^{\varphi(m)} \equiv (mod\ m)$.

Доказательство.

Пусть x пробегает приведенную систему вычетов по $mod\ m$:

$$x=r_1, r_2, \dots, r_c,$$

где $c=\varphi(m)$ их число, $r_1, r_2, \dots, r_c$ - наименьшие неотрицательные вычеты по $mod\ m$. Следовательно, наименьшие неотрицательные вычеты, соответствующие числам ax суть соответственно:

$$\rho_1, \rho_2, \dots, \rho_c$$

тоже пробегают приведенную систему вычетов, но в другом порядке. Значит:

$$ar_1 \equiv \rho_1 (mod\ m),$$

$$ar_2 \equiv \rho_2 (mod\ m),$$

$$\dots$$

$$ar_c \equiv \rho_c (mod\ m).$$

Перемножим эти c штук сравнений. Получится

$$a^c r_1 r_2 \dots r_c \equiv \rho_{j_1}\rho_{j_2}\dots\rho_{j_c} (mod\ m).$$

Так как $r_1 r_2 \dots r_c = \rho_1\rho_2 \dots \rho_c \neq 0$ и взаимно просто с модулем m, то, поделив последнее сравнение на $r_1 r_2 \dots r_c$, получим $a^{\varphi(m)} \equiv (mod\ m)$. ■

Вторая теорема этого пункта – теорема Ферма – является непосредственным следствием теоремы Эйлера.

Теорема (Ферма). *Пусть p – простое число, $p \nmid a$. Тогда*

$$a^{p-1} \equiv a(mod\ p).$$

Доказательство.

Положим в условии теоремы Эйлера $m=p$, тогда $\varphi(m)=p-1$. Получаем $a^{p-1} \equiv (mod\ p)$. ■

Необходимо отметить важность условия взаимной простоты модуля и числа a в формулировках теорем Эйлера и Ферма. Простой пример: сравнение $6^2 \equiv 1 (\mathrm{mod}\ 3)$ очевидно не выполняется.

Следствие. *Без всяких ограничений на $a \in Z$:* $a^p \equiv a(mod\ p)$.

Доказательство.

Умножим обе части сравнения $a^{p-1} \equiv 1(mod\ p)$ на a. Ясно, что получится сравнение, справедливое и при a, кратном p.

Пример 1. Девятая степень однозначного числа оканчивается на 7. Найти это число.

Решение.

Дано $a^9 \equiv 7 (mod\ 10)$. Кроме того, очевидно, что (7, 10) =1 и (*a*, 10) = 1. По теореме Эйлера, $a^{\varphi(10)} \equiv 1 (mod\ 10)$. Следовательно, $a^4 \equiv 1 (mod\ 10)$ и, после возведения в квадрат, $a^8 \equiv 1 (mod\ 10)$.

Поделим $a^9 \equiv 7 (mod\ 10)$ на $a^8 \equiv 1 (mod\ 10)$ и получим $a \equiv 7 (mod\ 10)$. Это означает, что a=7.

Пример 2. Найти остаток от деления 7^{402} на 101.

Решение.

Число 101 – простое, (7, 101) =1, следовательно, по теореме Ферма: $7^{100} \equiv 1 (mod\ 101)$. Возведем это сравнение в четвертую степень: $7^{400} \equiv 1 (mod\ 101)$, домножим его на очевидное сравнение

$7^2 \equiv 49 (mod\ 101)$, получим: $7^{402} \equiv 49 (mod\ 101)$. Значит, остаток от деления 7^{402} на 101 равен 49.

Пример 3. Найти две последние цифры числа 243^{402}.

Решение.

Две последние цифры этого числа суть остаток от деления его на 100. Имеем: 243=200+43; 200+43 ≡ 43(*mod* 100) и, возведя последнее очевидное сравнение в 402-ю степень, раскроем его левую часть по биному Ньютона.

В этом выражении все слагаемые, кроме последнего, содержат степень числа 200, т.е. делятся на 100, поэтому их можно выкинуть из сравнения, после чего понятно, почему $243^{402} \equiv 43^{402}$ (*mod* 100).

Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера $43^{\varphi(100)} \equiv 1(mod\ 100)$. Считаем:

$$\varphi(100)= \varphi(2^2 5^2)=(10–5)(10–2)=40.$$

Имеем сравнение: $43^{40} \equiv 1(mod\ 100)$, которое немедленно возведем в десятую степень и умножим почленно на очевидное сравнение, проверенное на калькуляторе: $43^2 \equiv 49(mod\ 100)$.

Следовательно, две последние цифры числа 243^{402} суть 4 и 9.

Пример 4. Доказать, что $(73^{12}-1)$ делится на 105.

Решение.

Имеем: 105=3 5 7, (73,3) = (73,5) = (73,7) = 1. По теореме Ферма:

$$73^2 \equiv 1 (\mathrm{mod}\ 3)$$

$$73^4 \equiv 1 (\mathrm{mod}\ 5)$$

$$73^6 \equiv 1 (\mathrm{mod} 7)$$

Перемножая, получаем:

$$73^{12} \equiv 1 (\mathrm{mod}\ 3), (\mathrm{mod}\ 5), (\mathrm{mod}\ 7),$$

откуда, по свойствам сравнений следует:

$$73^{12} - 1 \equiv 0 (\mathrm{mod}\ 105),$$

ибо 105 - наименьшее общее кратное чисел 3, 5 и 7.

Пример 5. Найти остаток от деления 171^{2147} на 52.

Решение.

Обозначим остаток от деления через x

$$x \equiv 171^{2147} (mod\ 52).$$

Так как $171 > 52$, то можно число 171 заменить остатком от деления на 52. $171 = 52 \cdot 3 + 15$. Отсюда $171 \equiv 15 (mod\ 52)$, но тогда

$$171^{2147} \equiv 15^{2147}(mod\ 52),$$

а поэтому сравнение примет вид:

$$x \equiv 15^{2147}(mod\ 52).$$

НОД $(a_1, m) =$ НОД$(15, 52) = 1$. Следовательно, применяя теорему Эйлера, согласно которой

$$a_1^{\varphi(m)} \equiv 1(mod\ m), \text{если НОД } (a_1, m) = 1,$$

поэтому $15^{\varphi(52)} \equiv 1(mod\ 52)$.

Вычислим $\varphi(52) = \varphi(2^2 \cdot 13) = (2^2 - 2^1) \cdot (13^1 - 13^0) = 24$.

Итак, $15^{24} \equiv 1(mod\ 52)$.

Выделим из степени 15^{2147} степень 15^{24}.

Так как $2147 = 24 \cdot 89 + 11$, то $15^{2147} = (15^{24})^{89} \cdot 15^{11}$,

Поэтому получим следующую цепочку преобразований сравнений и равенств с учетом полученного разложения:

$x \equiv 15^{2147} = (15^{24})^{89} \cdot 15^{11} \equiv 1^{89} \cdot 15^{11} = 15^{11} = 15 \cdot (15^2)^5 =$

$= 15 \cdot 225^5 \equiv 15 \cdot 17^5 = (15 \cdot 17) \cdot (17^2)^2 = 255 \cdot 289^2 \equiv 47 \cdot 29^2 = -5 \cdot (-23)^2 = -5 \cdot 529 \equiv -5 \cdot 9 = -45 \equiv 7(mod\ 52),$

Следовательно, $x \equiv 7(mod\ 52)$.

Заметим, что в сравнении *остаток* x не может быть отрицательным или $\geq m$, поэтому:

а) если получено последнее число в сравнении отрицательное, то надо заменить его положительным представителем из того же класса вычетов;

б) если последнее число в сравнении получено положительное, но $\geq m$, то надо его уменьшить, то есть заменить другим представителем r из того же класса вычетов так, чтобы было $0 \leq r < m$.

Теорема Вильсона. *Для любого простого числа p выполняется сравнение* $(p-1)! + 1 \equiv 0\ (mod\ p)$.

Доказательство.

Для $p = 2$ утверждение очевидно выполняется, поэтому далее будем считать, что p нечетно. Пусть a — некоторое целое число из промежутка $1 < a < p$. Так как НОД(a, p) = 1, то по теореме существует целое число b, удовлетворяющее сравнению $ab \equiv 1\ (mod\ p)$. При этом можно считать, что b есть наименьший неотрицательный вычет в своем классе. Ясно, что $b \neq 0$, т.е. $1 < b < p$. Кроме того, число b определяется единственным образом. Ведь если $ab_1 \equiv 1\ (mod\ p)$ и $ab_2 \equiv 1\ (mod\ p)$, то p делит $a(b_1 - b_2)$ и p делит $(b_1 - b_2)$, что при различных b_1, b_2 из промежутка $1 < b < p$ невозможно.

Если $a \equiv b\ (mod\ p)$, то $a^2 \equiv 1\ (mod\ p)$ и p делит $(a^2 - 1) = (a - 1)(a + 1)$.

Так как p — простое число, это возможно лишь в случае $a = 1$ или $a = p - 1$. Из доказанного следует, что множество целых чисел a из промежутка $1 < a < p - 1$ может быть разбито на пары различных целых чисел a, b, удовлетворяющих сравнению $ab \equiv 1\ (mod\ p)$. Следовательно,

$$\prod_{k=2}^{p-2} k \equiv 1(mod\ p).$$

Умножив это сравнение на p–1, получим

$$(p - 1)! \equiv p - 1 \equiv -1\ (mod\ p).$$

Для составных чисел теорема Вильсона, конечно, нарушается. Ведь если целое число N имеет делитель d, $1 < d < N$, то $(N - 1)!$ Делится на d. Значит, $(N - 1)! + 1$ на d не делится, а потому не делится и на N.

Эта теорема была сформулирована Д. Вильсоном. Приведенное доказательство принадлежит Лагранжу (1771 г.) и до опубликования рукописей Л. Эйлера считалось первым.

Справедлива

Обратная теорема Вильсона. *Если для натурального* $p > 1$ *имеет место сравнение* $(p-1)! + 1 \equiv 0 \ (mod\ p)$, *то* p *— простое число.*

Доказательство.

Если p — составное, то его простой делитель меньше p и поэтому должен делить $(p-1)!$, но тогда он должен делить и 1.

Теорема Вильсона дает **критерий простоты натурального числа Лейбница.** *Для того, чтобы натуральное* $p > 2$ *было простым, необходимо и достаточно, чтобы* $(p-2)! \equiv 1 \ (mod\ p)$,

Упражнения

1. По какому модулю все целые числа сравнимы между собой?
2. Привести примеры целых чисел, сравнимых по модулю 8.
3. Привести примеры целых чисел, имеющих с модулем 6 один и тот же наибольший общий делитель, но не сравнимых по этому модулю.
4. Применить понятие сравнения к доказательству того, что числа 210 и 858 имеют с модулем 12 один и тот же наибольший общий делитель. Применим ли этот прием относительно чисел 385 и 77 по модулю 6?
5. Какие из следующих сравнений являются верными:
   $1) 1 \equiv -5(6);\ 2)\ 546 \equiv 0(13); 3)\ 8 \equiv 1(4);\ 4) 3 \equiv -1(6)$?

6. Доказать, что следующие сравнения являются верными:
   1)$121 \equiv 13145\ (2)$; 2) $121247 \equiv 92817\ (10)$;
   3) $31 \equiv -9(10)$; 4) $(m-1)^2 \equiv 1(m)$?
7. Доказать, что следующие сравнения являются неверными:
   $$1)\ 5^{1812} \equiv 1994(25);\ 2)\ 7^{103} \equiv 3(27);$$
   $$3) 4^{1994} \equiv 25(10); \quad 4)\ 30 \cdot 17 \equiv 81 \cdot 19(6).$$
8. Доказать, что каждое целое число сравнимо со своим остатком по данному модулю.
9. Целое число x удовлетворяет условию: $x \equiv 2(10)$. Записать это условие в виде уравнения с параметром и найти несколько значений x.
10. Найти все значения x, удовлетворяющие сравнениям:
    $$1)\ x \equiv 0(3), 2)\ x \equiv 1(2).$$
11. Найти значения m, удовлетворяющие условию:
    $$1)\ 20 \equiv 8(m),\ 2) 3p+1 \equiv p+1(m).$$
12. Указать возможные значения модуля в сравнении $x \equiv 5(m)$, если известно, что этому сравнению удовлетворяет $x_0 = 13$.
13. Записать в виде сравнений все классы вычетов по модулю 10.
14. Записать все классы вычетов по модулю 10 при помощи формулы $x = 10q + r, r \in \mathrm{Z}, 0 \le r < 10$.
15. Найти полную и приведенную системы вычетов по модулю 10.
16. По какому модулю числа 20, -4, 22, 18, -1 составляют полную систему вычетов?

17. Доказать, что система чисел 20, 31, -8, -5, 25, 14, 8, -1, 13, 6 не является полной системой вычетов.
18. Почему система чисел -5, 13, 11, -21, 5 не является приведенной системой вычетов по модулю 12?
19. Доказать, что система чисел $5, 5^2, 5^3, 5^4, 5^5, 5^6$ является приведенной системой вычетов по модулю 7.
20. Найти хотя бы одну полную систему вычетов вида $5x$ по mod 4.
21. Вычислить $\varphi(n)$, если:
    $1) n = 10000$, $2) n = 125$, $3) n = 10000$,
    $4) n = 180$, $5) n = 360$, $6) n = 1001$.
22. Найти число классов вычетов, взаимно простых с mod 1225.
23. Сколько существует правильных несократимых дробей со знаменателем m?
24. Сколько натуральных чисел в промежутке от 1 до 120, не взаимно простых с 30?
25. Доказать, что $\varphi(4n + 2) = \varphi(2n + 1)$.
26. Решить в натуральных числах уравнения:
    1) $\varphi(5^x) = 100, 3)\ \varphi(p^x) = p^{x-1}$,
    2) $\varphi(7^x) = 292, 4)\ \varphi(3^x \cdot 5^y) = 600$.
27. Доказать, что:
    1) $a^{12} - 1$ делится на 7, если НОД (a, 7) =1.
    2) $a^{12} - b^{12}$ делится на 65, если НОД (a, 65) = НОД (b, 65) =1,
    3) $3^{100} - 3^{60} - 3^{40} + 1$ делится на 77.

28. Доказать, что число вида $a^{p-1}+p-1$, где $a \not\equiv 0\ (mod\ p)$ и $a \neq 1$, является составным.
29. Доказать, что:
    1) $a^{561} \equiv a\ (mod\ 11)$, если $11 \nmid a$,
    2) $a^{560} \equiv 1\ (mod\ 561)$, если НОД $(a, 561) = 1$;
    3) $1^{19}+2^{19}+4^{19}+5^{19}+7^{19}+8^{19} \equiv 0 (\mathrm{mod}\ 9)$;
    4) $1^{14}+3^{14}+7^{14}+9^{14} \equiv 0 (\mathrm{mod}\ 10)$.
30. Доказать, что $2^{1093 \cdot 1092} \equiv 1\ (mod\ 1093^2)$.
31. Найти остаток от деления 100-й степени натурального числа a на 125, если НОД $(a, 125) = 1$.
32. Доказать, что цифра единиц 12-й степени натурального числа, каноническое разложение которого не содержит множителей 2 и 5, есть 1.
33. Докажите, что существует такая степень числа 2, все последние 1000 цифр которой в десятичной записи будут единицами и двойками.
34. Пользуясь теоремой Эйлера, найти последнюю цифру в десятичном представлении чисел: 3^{100},
    1) 13^{219},
    2) 17^{500},
    3) 243^{402},
    4) 473^{1971},
    5) 43^{93}.

35. Найти остаток от деления:
    1) 3^{78} на 11,
    2) 4^{93} на 13,
    3) 46^{921} на 21,
    4) $3^{200}+7^{200}$ на 101,
    5) 327^{8493} на 29,
    6) 473^{569} на 45,
    7) 39^{93} на 17.
36. Известно, что $12 \equiv a\ (mod\ 10), a \in \mathrm{Z}$. Укажите верные и неверные утверждения:
    1) $12 = 10a + r, 0 \leq r < 10, r \in \mathrm{N}$;
    2) $2 \equiv a\ 9mod\ 10)$;
    3) $(a-2) \vdots 5$;
    4) $a \vdots 2$;
    5) $(\exists t \in \mathrm{Z})(12 = 10t + a)$.
37. Найти наименьший положительный вычет числа 3^{1000} по модулю 13.
38. Известно, что $\varphi(ab) = 6$, где $a, b \in \mathrm{N}, a \neq b$. Укажите верный и неверные утверждения:
    1) $(a = 1)$или $(b = 1)$;
    2) Таких a и b не существует;
    3) $ab > 6$;
    4) НОД $(a, b) = 1$ или НОД $(a, b) = 3$.

Глава 2. СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

2.1. Основные понятия

Определение. *Сравнением первой степени с одой переменной называется сравнение вида*

$$ax \equiv b \ (mod\ m),$$

где $m \in N, a, b \in Z, m \nmid a.$

Теорема. *Если целое число c удовлетворяет сравнению* $ax \equiv b \ (mod\ m)$, *то и все числа класса* $\bar{c}$ *по mod m будут удовлетворять этому сравнению.*

Доказательство.

Имеем $ax \equiv b \ (mod\ m)$. Значит $ax - b \equiv 0 \ (mod\ m)$. Обозначим через $f(x) = ax - b$. Следовательно, $f(x) \equiv 0 \ (mod\ m)$. Так как число c удовлетворяет сравнению $ax \equiv b \ (mod\ m)$, то сравнение

$$f(c) \equiv 0 \ (mod\ m)$$

Является верным. Кроме того,

$$(\forall s \in \bar{c})\big(s \equiv c \ (mod\ m)\big).$$

Поэтому, по свойствам сравнения,

$$f(s) \equiv f(c)(mod\ m).$$

Тогда по свойству транзитивности получим, что

$$f(s) \equiv 0(mod\ m),$$

то есть s удовлетворяют сравнению $ax \equiv b\ (mod\ m)$, поэтому весь класс $\bar{c}$ состоит из чисел, удовлетворяющих этому сравнению. ■

Определение. *Решением сравнения* $ax \equiv b\ (mod\ m)$ *называется класс вычетов по mod m, которые при подстановке в сравнение обращают его в верное сравнение.*

Число решений сравнения по mod m – это число решений этого сравнения в какой-либо полной системе вычетов по mod m.

Пример. Решить сравнение $3x \equiv 2\ (mod\ 7)$.

Полная система наименьших неотрицательных вычетов по модулю 7: $\{0, 1, 2, 3, 4, 5, 6\}$.

Если x=0, то $3 \cdot 0 - 2 = -2, -2$ не делится на 7, следовательно, x=0 не удовлетворяет сравнению.

Если x=1, то $3 \cdot 1 - 2 = 1$, 1 не делится на 7, следовательно, x=1 не удовлетворяет сравнению.

Если x=2, то $3 \cdot 2 - 2 = 4$, 4 не делится на 7, следовательно, x=2 не удовлетворяет сравнению.

Если x=3, то $3 \cdot 3 - 2 = 7$, 7 делится на 7, следовательно, x=3 удовлетворяет сравнению.

Если x=4, то $3 \cdot 4 - 2 = 10$, 10 не делится на 7, следовательно, x=4 не удовлетворяет сравнению.

Если x=5, то $3 \cdot 5 - 2 = 13$, 13 не делится на 7, следовательно, x=5 не удовлетворяет сравнению.

Если x=6, то $3 \cdot 6 - 2 = 16$, 16 не делится на 7, следовательно, x=6 не удовлетворяет сравнению.

Таким образом, сравнение имеет одно решение $\overline{3}$ по mod 7 или, в другом виде, $x \equiv 3\ (mod\ 7)$.

Пример. Решить сравнение $5x \equiv 3\ (mod\ 10)$.

Полная система наименьших неотрицательных вычетов по модулю 10: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Проверим для каждого из этих чисел, будет ли выполнено условие $(5x - 3) \vdots 10$. $x = 0, -3$ не $\vdots 10$,

$x = 1, 2$ не $\vdots 10$, $x = 2, 7$ не $\vdots 10$, $x = 3, 12$ не $\vdots 10$,

$x = 4, 17$ не $\vdots 10$, $x = 5, 22$ не $\vdots 10$, $x = 6, 27$ не $\vdots 10$,

$x = 7, 32$ не $\vdots 10$, $x = 8, 37$ не $\vdots 10$, $x = 9, 42$ не $\vdots 10$.

Ни одно из чисел полной системы вычетов не удовлетворяет сравнению, следовательно, данное сравнение не имеет решения.

Определение. *Сравнения называются равносильными, если они имеют одинаковые решения.*

2.2. Теорема о неразрешимости сравнения

Теорема. *Пусть дано сравнение* $ax \equiv b\ (mod\ m)$, где $m \in N, a, b\ \in Z$, НОД $(a, m) = d, d > 1, b$ не $\vdots\ d$. *Тогда сравнение не имеет решения.*

Доказательство.

От противного. Предположим, что существует решение: класс вычетов $\overline{x_0}$ по модулю m. Тогда x_0 $(x_0\ \in \overline{x_0})$ удовлетворяет сравнению, то есть $ax_0\ \equiv b\ (mod\ m)$ – верное сравнение. Отсюда получим, что

$$(ax_0 - b) \vdots m.$$

Из условия теоремы: НОД $(a, m)=d$ следует, что

$$a \vdots d, m \vdots d.$$

Поэтому получим, что $(ax_0 - b) \vdots d$ и $a \vdots d$, отсюда следует , что $b \vdots d$. Получим противоречие: b не $\vdots\ d$ и $b \vdots d$,

так как сделали неверное предположение. Отбросив его. Получаем, что сравнение $ax \equiv b\ (mod\ m)$ не имеет решение. ■

2.3. Теорема о разрешимости сравнения

Рассмотрим сравнение $ax \equiv b\ (mod\ m)$, где $m \in$ N, $a, b \in$ Z, a не $\vdots\ m$. Если НОД $(a, m) = d, d > 1, b$ не $\vdots\ d$, то сравнение не имеет решение.

Пусть теперь $b \vdots d$, тогда будем иметь:

$a = da_1, a_1 \in$ Z,

$m = dm_1, m_1 \in Z$, НОД $(a_1, m_1) = 1$,

$b = db_1, b_1 \in Z$.

Поэтому $(da_1)x \equiv db_1(mod\ dm_1)$, НОД $(a_1, m_1) = 1$. Так как по определению. НОД число $d \in$ N, то из последнего сравнения получим $a_1x \equiv b_1(mod\ m_1)$, где НОД $(a_1, m_1) = 1$.

Таким образом, полагая в сравнении $ax \equiv b\ (mod\ m)$, что НОД $(a, m) = d, d > 1, b \vdots d$, приходим к сравнению такого же вида, но с условием НОД $(a_1, m_1) = 1$.

Исследуем этот случай.

Теорема. *Пусть дано сравнение* $ax \equiv b\ (mod\ m)$ *и* НОД $(a, m) = 1$. *Тогда сравнение имеет единственное решение.*

Доказательство.

Так как НОД $(a, m) = 1$, то класс вычетов $\bar{a}$ по mod m принадлежит мультипликативной группе классов вычетов, взаимно простых с mod m. Поэтому уравнение $\bar{a} \cdot \bar{x} = \bar{1}$ имеет единственное решение $\bar{c}$, где $\bar{c}$ – класс вычетов по mod m, взаимно простых с m. Значит, для $\bar{a}\ \exists \bar{c}$ такое, что $\bar{a} \cdot \bar{c} = \bar{1}$. Но тогда $(\bar{a}\bar{c})\bar{b} = \bar{1}\bar{b}$, отсюда $\bar{a}(\bar{c}\bar{b}) = \bar{b}$. Обозначим $\overline{x_0}$ класс вычетов $\overline{cb}$ по mod m, взаимно простых с m, тогда получим, что для $\bar{a}\ \exists\overline{x_0}$ такое, что $\bar{a}\,\overline{x_0}=\bar{b}$. Следовательно, $\bar{a}\,\overline{x_0}=\bar{b}$, а $ax_0 \equiv b\ (mod\ m)$ -верное сравнение, то есть класс $\overline{x_0}$ является решением сравнения $ax \equiv b\ (mod\ m)$. Это решение единственно, так как существует единственный класс $\bar{c}$ такой, что $\overline{x_0}=\overline{cb} = \bar{c}\bar{b}$. ■

Пример. Решить сравнение $5x \equiv 2\ (mod\ 9)$.

НОД (5, 9) = 1, следовательно, сравнение имеет единственное решение. Найдем его способом «подбора», то есть перебирая все числа из полной системы вычетов по mod 9: {0, 1, 2, 3, 4, 5, 6, 7, 8}.

$x = 0, 5x - 2 = -2, -2$ не $\vdots\ 9$; $x = 1, 5x - 2 = 3, 3$ не $\vdots\ 9$;

$x = 2, 5x - 2 = 8, 8$ не $\vdots\ 9$;

$x = 3, 5x - 2 = 13, 13$ не $\vdots$ 9;

$x = 4, 5x - 2 = 18, 18 \vdots 9$, следовательно, x=4 удовлетворяет сравнению, поэтому решением будет класс вычетов $\overline{4}$ по mod 9 или, по-другому $x \equiv 4\ (mod\ 9)$.

А так как данное сравнение имеет единственное решение, то остальные числа x: 5, 6, 7, 8 проверять не нужно.

Для нахождения решения сравнения первой степени с одной переменной существует несколько способов:

1) подбора,
2) преобразования коэффициентов,
3) Эйлера,
4) цепных дробей
5) диофантовы уравнения.

2.4. Метод преобразования коэффициентов

Теорема. *Пусть дано сравнение* $ax \equiv b\ (mod\ m)$, *НОД(a,m)=1,* $k \in Z$ *и* $(b + mk) \vdots a$. *Тогда класс вычетов* $\overline{x_0} = \overline{\left(\frac{b+mk}{a}\right)}$ *по модулю m является решением сравнения.*

Доказательство.

Так как НОД*(a,m)*=1, то сравнение $ax \equiv b\ (mod\ m)$ имеет одно решение. Кроме того, $(b + mk) \vdots a$. Возьмем целое число $x_0 = \frac{b+mk}{a}$, $x_0 \in \overline{x_0}$, тогда $ax_0 = b + mk$, следовательно, получим сравнение: $b + mk \equiv b\ (mod\ m)$, которое является верным сравнением. Поэтому целое число $x_0 = \frac{b+mk}{a}$ удовлетворяет сравнению, а, значит, класс вычетов $\overline{x_0} = \overline{\left(\frac{b+mk}{a}\right)}$ по модулю m является решением сравнения. ■

Пример. Решить сравнение $5x \equiv 2\ (mod\ 9)$.

НОД (5, 9) = 1, следовательно, сравнение имеет единственное решение.

$5x \equiv 2 + 9k(mod\ 9), k \in \mathrm{Z}.$

Найдем такое целое k, чтобы 2+9k делилось на 5. Например, k=2: $2 + 9 \cdot 2 = 20, 20 \vdots 5$. Тогда получим

$5x \equiv 2 + 9 \cdot 2(mod\ 9),$

$5x \equiv 20(mod\ 9),$

$x \equiv 4(mod\ 9).$

Проверка: $4 \cdot 5 - 2 = 18, 18 \vdots 9$, поэтому при подстановке в сравнение переменной значения 4, получим верное сравнение, следовательно, число 4 удовлетворяет сравнению, а потому класс вычетов, содержащий число 4, является решением сравнения.

Пример. Решить сравнение $3x \equiv 2\ (mod\ 7)$.

НОД (3, 7) = 1, следовательно, сравнение имеет единственное решение.

$3x \equiv 2 + 7k(mod\ 7), k \in \mathrm{Z}$.

Найдем такое целое k, чтобы 2+7k делилось на 3.

Например, k=1: $2 + 7 \cdot 1 = 9, 9 \vdots 3$. Тогда получим

$3x \equiv 2 + 7 \cdot 1(mod\ 7)$,

$3x \equiv 9(mod\ 7)$,

$x \equiv 3(mod\ 7)$.

2.5. Метод Эйлера

Получим метод решения сравнения $ax \equiv b\ (mod\ m)$ с помощью функции Эйлера.

Теорема. *Пусть дано сравнение* $ax \equiv b\ (mod\ m)$, *НОД(a,m)=1. Тогда класс вычетов* $\overline{x_0} = \overline{b \cdot a^{\varphi(m)-1}}$ *по модулю m является решением сравнения, где* $\varphi(m)$ *– функция Эйлера.*

Доказательство.

Так как *НОД(a,m)=1,* то по теореме Эйлера имеет место сравнение

$$a^{\varphi(m)} \equiv 1(mod\ m),$$

где $\varphi(m)$ – функция Эйлера.

Выберем $x_0 = b \cdot a^{\varphi(m)-1}$, $x_0 \in \overline{x_0}$, тогда при подстановке его вместо x в сравнение $ax \equiv b\ (mod\ m)$ и, учитывая, что

$$ax_0 = a\left(b \cdot a^{\varphi(m)-1}\right) = b \cdot a^{\varphi(m)},$$

Получим сравнение $b \cdot a^{\varphi(m)} \equiv b\ (mod\ m)$,

Которое является верным в силу теоремы Эйлера. Следовательно, x_0 удовлетворяет сравнению, а класс вычетов

$$\overline{x_0} = \overline{b \cdot a^{\varphi(m)-1}}$$

По модулю m является решением сравнения, или, по-другому

$x_0 \equiv b \cdot a^{\varphi(m)-1} (mod\ m)$ – решение сравнения. ■

Пример. Решить сравнение $3x \equiv 2\ (mod\ 5)$.

НОД(3,5)=1, следовательно, сравнение имеет единственное решение, $x \equiv 2 \cdot 3^{\varphi(5)-1} (mod\ 5)$. Преобразуем произведение $2 \cdot 3^{\varphi(5)-1}$. Так как 5 – простое число, то $\varphi(5) = 5 - 1 = 4$. Поэтому $2 \cdot 3^{\varphi(5)-1} = 2 \cdot 3^{4-1} = 2 \cdot 3^3 = 54$.

$x \equiv 54\ (mod\ 5)$, $x \equiv 4\ (mod\ 5)$.

Рассмотрим еще один пример и решим сравнение тремя способами.

Пример. Решить сравнение $9x \equiv 8\ (mod\ 34)$.

НОД(9,34)=1, следовательно, сравнение имеет единственное решение.

1 способ –подбором.

Полная система наименьших неотрицательных вычетов по модулю 34: {0, 1, 2, …, 33}.

Проверим, какое из этих чисел x удовлетворяет сравнению, то есть $(9x-8) \vdots 34$. Это будет x=16, так как $9 \cdot 16 - 8 = 144 - 8 = 136, 136 \vdots 34$. Следовательно, $x \equiv 16\ (mod\ 34)$ – решение сравнения.

2 способ – преобразование коэффициентов.

$9x \equiv 8 + 34k (mod\ \ 34), k \in \mathrm{Z}$.

Найдем такое целое число k, при котором $(8 + 34k) \vdots 9$. Например, $k = 4$, тогда $8 + 34k = 8 + 34 \cdot 4 = 144, 144 \vdots 9$.

$9x \equiv 8 + 34 \cdot 4 (mod\ \ 34)$,

$9x \equiv 144 (mod\ \ 34)$,

$x \equiv 16 (mod\ \ 34)$ – решение сравнения.

3 способ – метод Эйлера (с помощью функции Эйлера).

$x \equiv 8 \cdot 9^{\varphi(34)-1} (mod\ 34)$.

Упростим произведение $8 \cdot 9^{\varphi(34)-1}$.

$\varphi(34) = \varphi(2 \cdot 17) = 2 \cdot 17 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{17}\right) = 16$.

$x \equiv 8 \cdot 9^{16-1} \equiv 8 \cdot 9^{15} \equiv 8 \cdot (9^2)^7 \cdot 9 \equiv (8 \cdot 9) \cdot 81^7 \equiv 4 \cdot 13^7 \equiv 52 \cdot 169^3 \equiv 18 \cdot 33^3 \equiv 18 \cdot (-1)^3 \equiv -18 \equiv 16 (mod\ 34)$.

$x \equiv 16 (mod\ \ 34)$ – решение сравнения.

2.6. Метод цепных дробей

Рассмотрим сравнение $ax \equiv b \pmod m$, *НОД(a,m)=1*. Если модуль большой, то лучше для решения сравнения применять следующую теорему.

Теорема. *Пусть дано сравнение* $ax \equiv b \pmod m$, *НОД(a,m)=1 и пусть* $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \dots, \frac{P_n}{Q_n} = \frac{m}{a}$ *– подходящие дроби разложения дроби* $\frac{m}{a}$ *в цепную дробь. Тогда класс вычетов*

$$x \equiv (-1)^n \cdot b \cdot P_{n-1} \pmod m$$

является решением сравнения.

Доказательство.

Так как НОД*(a,m)*=1, то дробь $\frac{m}{a}$ является несократимой, поэтому дробь $\frac{P_n}{Q_n}$ – несократимая, следовательно,

НОД $(P_n, Q_n) = 1$. Тогда $P_n = m, Q_n = a$. Имеем:

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1}Q_n}.$$

Отсюда

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1},$$

$$mQ_{n-1} - P_{n-1}a = (-1)^{n-1}.$$

Но $mQ_{n-1} \equiv 0\ (mod\ m)$, следовательно, получим сравнение:

$P_{n-1}a + (-1)^{n-1} \equiv 0\ (mod\ m)$,

$P_{n-1}a \equiv -(-1)^{n-1}\ (mod\ m)$,

$(-1)^n aP_{n-1} \equiv 1(mod\ m)$,

$a((-1)^n bP_{n-1}) \equiv b(mod\ m)$.

Полученное сравнение является верным сравнением, следовательно, целое число $x = (-1)^n \cdot b \cdot P_{n-1}$ удовлетворяет сравнению $ax \equiv b\ (mod\ m)$, то есть класс вычетов

$$\bar{x} = \overline{(-1)^n \cdot b \cdot P_{n-1}}$$

Является решением сравнения, или, по-другому,

$$x \equiv (-1)^n \cdot b \cdot P_{n-1}(mod\ m)$$

Является решением сравнения $ax \equiv b\ (mod\ m)$. ■

Пример. $55x \equiv 7(\ mod\ 87)$.

Решение.

НОД (55, 87)=1, следовательно, сравнение имеет одно решение.

1) Разложим дробь $\frac{m}{a} = \frac{87}{55}$ цепную дробь.

$$\frac{87}{55} = 1 + \frac{32}{55} = 1 + \frac{1}{\frac{55}{32}} = 1 + \frac{1}{1+\frac{23}{32}} = 1 + \frac{1}{1+\frac{1}{\frac{32}{23}}} = 1 + \frac{1}{1+\frac{1}{1+\frac{9}{23}}}$$

$$= 1 + \frac{1}{1+\frac{1}{1+\frac{1}{\frac{23}{9}}}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{2+\frac{5}{9}}}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{2+\frac{1}{\frac{9}{5}}}}} =$$

$$= 1 + \frac{1}{1+\frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{4}{5}}}}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{1}{\frac{5}{4}}}}}} =$$

$$1 + \frac{1}{1+\frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{4}}}}}} = [1; 1,1,2,1,1,4].$$

Найдем числители подходящих дробей.

	a_0	a_1	a_2	a_3	a_4	a_5	a_6
	1	1	1	2	1	1	4
1	**1**	2	3	8	11	19	87

$n = 6, P_{n-1} = P_5 = 19.$

Применяя теорему, согласно которой класс чисел

$$x \equiv (-1)^n \cdot b \cdot P_{n-1}(mod\ m)$$

является решением сравнения, получим $x \equiv (-1)^6 \cdot 7 \cdot 19(mod\ 87)$,

$$x \equiv 133 \equiv 46(mod\ 87).$$

Пример. Решить сравнение $256x \equiv 179(mod\ 337)$.

Решение.

(256,337)=1→одно решение.

Разложим дробь $\frac{337}{256}$ в цепную дробь. $\frac{337}{256} = [1; 3,6,4,3]$.

a		1	3	6	4	3
P_s	**1**	1	4	25	104	337

$n = 5, n-1 = 4, P_4 = 104, b = 179,$

$x \equiv (-1)^4 \cdot 104 \cdot 179 \equiv 18616 \equiv 81(mod\ 337).$

Кафедра ФМО и ИТ

2.7. Сравнения первой степени и диофантовы уравнения

Рассмотрим сравнение $ax \equiv b\ (mod\ m)$, *НОД(a,m)=1*. Данное сравнение можно записать в виде линейного диофантова уравнения от двух неизвестных

$$ax + my = b, m \in \mathrm{N}; a, x, y, b \in \mathrm{Z}.$$

Так как *НОД(a,m)=1*, то оно разрешимо в целых числах.

Пример. Решить сравнение $3x \equiv 1\ (mod\ 4)$.

Данное сравнение можно свести к линейному диофнатову уравнению $3x + 4y = 1$.

Не будем подробно останавливаться на решении таких уравнение (один из способов основан на алгоритме Евклида и линейном разложении НОДа (a,b)).

$$x = 4t + 3; y = 3t + 2, t \in \mathrm{Z}.$$

Очевидно, что $x \equiv 3(mod\ 4)$.

Это и есть решения сравнения, в чем можно убедиться при проверке.

2.8. Случай *d* решений

Рассмотрим сравнение $ax \equiv b \pmod m$, *НОД(a,m)=d, d>1.*

Если b не $\vdots d$, то сравнение не имеет решения. Исследуем теперь случай, когда $b \vdots d$.

Теорема. *Числа класса $\bar{\alpha}$ по mod k образуют s классов вычетов по mod ks:* $\bar{\alpha}$, $\overline{\alpha + k}$, $\overline{\alpha + 2k}$, …, $\overline{\alpha + (s-1)k}$.

Доказательство.

Все числа класса вычетов $\bar{\alpha}$ по mod k можно записать так: $\bar{\alpha} = \{\alpha + ks | s \in \mathrm{Z}\}$.

Возьмем s чисел из класса вычетов по mod k:

$$\alpha, \alpha + k, \alpha + 2k, \dots, \alpha + (s-1)k \in \bar{\alpha},$$

Они попарно сравнимы по mod k, но эти числа попарно несравнимы по модулю ks, так как разность каждой пары не делится на модуль ks.

Следовательно, классы вычетов по mod ks, содержащие эти числа, будут попарно различны: $\bar{\alpha}$, $\overline{\alpha + k}$, $\overline{\alpha + 2k}$, …, $\overline{\alpha + (s-1)k}$ по mod ks

$$\bar{\alpha} = \{\alpha, \alpha + ks, \alpha + 2ks, \dots\} = \{\alpha + (ks)n | n \in \mathrm{Z}\},$$

$\overline{\alpha + k} = \{\alpha + k, (\alpha + k) + ks, (\alpha + k) + 2ks, \dots\} =$

$= \{(\alpha + k) + (ks)n | n \in \mathrm{Z}\},$

$\overline{\alpha + 2k} = \{\alpha + 2k, (\alpha + 2k) + ks, (\alpha + 2k) + 2ks, \dots\} =$

$= \{(\alpha + 2k) + (ks)n | n \in \mathrm{Z}\},$

…

$\overline{\alpha + (s-1)k} = \{\alpha + (s-1)k, (\alpha + (s-1)k) + ks, (\alpha + (s-1)k) + 2ks, \dots\} = \{(\alpha + (s-1)k) + (ks)n | n \in \mathrm{Z}\}.$

Таким образом, класс вычетов $\bar{\alpha}$ по mod k можно разбить на s классов вычетов о модулю ks (они не все пустые, попарно не пересекаются и объединение всех их совпадает с классом вычетов $\bar{\alpha}$ по mod k) ■

Теперь, применяя эту теорему, получим, что все решения сравнения $ax \equiv b\ (mod\ m)$ в случае, когда *НОД(a,m)=d, d>1* число $b \vdots d$.

Теорема. *Пусть дано сравнение* $ax \equiv b\ (mod\ m)$, *НОД(a,m)=d, d>1 и пусть* $b \vdots d$. *Тогда сравнение имеет d решений. Все эти решения образуют один класс по модулю* $\frac{m}{d}$.

Доказательство.

Так как *НОД(a,m)=d, d>1,* $d \in \mathrm{N}$, то $a = da_1, m = dm_1$, где $a_1 \in \mathrm{Z}, m_1 \in \mathrm{N}$ и $\text{НОД}\,(a_1, m_1) = 1$. Кроме того, $b \vdots d$, поэтому $\exists b_1 \in \mathrm{Z},\ b = db_1$.

Преобразуем сравнение

$$ax \equiv b\ (mod\ m),$$

$$da_1x \equiv db_1\ (mod\ dm_1), \text{НОД}\,(a_1, m_1) = 1,$$

$$a_1x \equiv b_1\ (mod\ m_1), \text{НОД}\,(a_1, m_1) = 1.$$

Но последнее сравнение имеет одно решение. Пусть это будет класс вычетов $\overline{x_0} = \bar{\alpha}$ по mod m_1, то есть $x \equiv \alpha\ (mod\ m_1)$ или, заменяя m_1, $x \equiv \alpha\ (mod\ \frac{m}{d})$.

Согласно предыдущей теореме, $\bar{\alpha}$ по mod k образует s классов вычетов по mod ks: $\bar{\alpha}$, $\overline{\alpha + k}$, $\overline{\alpha + 2k}$, ..., $\overline{\alpha + (s-1)k}$. Тогда получим, что $\bar{\alpha}$ по mod $\frac{m}{d}$ образует d классов вычетов по mod m $\left(\frac{m}{d} \cdot d = m\right)$:

$$\bar{\alpha},\ \overline{\alpha + \frac{m}{d}},\ \overline{\alpha + 2\frac{m}{d}},\ \ldots,\ \overline{\alpha + (s-1)\frac{m}{d}}.$$

Следовательно, исходное сравнение имеет d решений:

$$x \equiv \alpha(mod\ m),$$

$$x \equiv \alpha + \frac{m}{d}(mod\ m),$$

$$x \equiv \alpha + 2\frac{m}{d}(mod\ m),$$

…

$$x \equiv \alpha + (d-1)\frac{m}{d}(mod\ m),$$

причем, все эти решения образуют один класс $\bar{\alpha}$ по модулю $\frac{m}{d}$, так как

$\alpha + \frac{m}{d} \equiv \alpha\left(mod\ \frac{m}{d}\right)$, $\alpha + 2\frac{m}{d} \equiv \alpha\left(mod\ \frac{m}{d}\right)$, …, $\alpha + (d-1)\frac{m}{d} \equiv \alpha\left(mod\ \frac{m}{d}\right)$. ■

Пример. Решить сравнение $20x \equiv 44(\ mod\ 108)$.

НОД(20, 108)=4, 44⋮4. Следовательно, сравнение имеет 4 решения.

1) По свойству сравнений имеем :$5x \equiv 11(\ mod\ 27)$.

НОД $(5, 27) = 1$, следовательно, полученное сравнение имеет одно решение. Найдем его любым рассмотренным способом, например, преобразованием коэффициентов:

$5x \equiv 11 + 27k(\ mod\ 27), k \in \mathrm{Z}$.

При этом k=2, будет $11 + 27 \cdot 2 = 11 + 54 = 65, 65 \vdots 5$.

$5x \equiv 11 + 27 \cdot 2(\ mod\ 27)$,

$5x \equiv 65(\,mod\ 27)$,

$x \equiv 13(\,mod\ 27)$ – решение сравнения $5x \equiv 11(\,mod\ 27)$.

2) Теперь получим все 4 решения исходного сравнения.

$x_1 \equiv 13(\,mod\ 108)$,

$x_2 \equiv 13 + 27 \equiv 40(\,mod\ 108)$,

$x_3 \equiv 13 + 2 \cdot 27 \equiv 67(\,mod\ 108)$,

$x_4 \equiv 13 + 3 \cdot 27 \equiv 94(\,mod\ 108)$ или, по-другому, $\overline{13}, \overline{40}, \overline{67}, \overline{94}$.

Пример. Решить сравнение $1215x \equiv 560(mod\ 2755)$.

Решение.

(1215,2755)=5→пять решений.

$243x \equiv 112(mod\ 551)$.

Разложим дробь $\frac{551}{243256}$ в цепную дробь. $\frac{551}{243256} = [2;3,1,2,1,4,1,2]$.

a		2	3	1	2	1	4	1	2
P_s	1	2	7	9	25	34	161	195	551

$n = 8, n-1 = 7, P_7 = 195, b = 112$,

$x \equiv (-1)^7 \cdot 195 \cdot 112 \equiv -21840 \equiv -351 \equiv 200(mod\ 551)$.

Найдем теперь пять решений исходного сравнения

$x_1 \equiv 200(\,mod\,2755),$

$x_2 \equiv 200 + 551 \equiv 751(\,mod\,2755),$

$x_3 \equiv 200 + 2 \cdot 551 \equiv 1302(\,mod\,2755),$

$x_4 \equiv 200 + 3 \cdot 551 \equiv 1853(\,mod\,2755),$

$x_4 \equiv 200 + 4 \cdot 551 \equiv 2404(\,mod\,2755).$

Ответ: $x \equiv 200, 751, 1302, 1853, 2404(mod\,2755).$

Упражнения

1. Решить сравнения:
   a) $2x + 5 \equiv 0(mod\,3)$, f) $7x \equiv 9(mod\,10)$,
   b) $2x - 3 \equiv 0(mod\,6)$, g) $7x \equiv 13(mod\,29)$,
   c) $29x \equiv 1(mod\,17)$, h) $8x \equiv 15(mod\,29)$,
   d) $21x + 5 \equiv 0(mod\,29)$, k) $9x \equiv 17(mod\,31)$,
   e) $7x \equiv 15(mod\,9)$, l) $2x \equiv -1(mod\,13)$.
2. Решить сравнения методом цепных дробей:
   a) $243x \equiv 271(mod\,317)$, c) $327x \equiv 78(mod\,379)$,
   b) $139x \equiv 118(mod\,239)$, d) $256x \equiv 179(mod\,337)$.
3. Решить сравнения:
   a) $12x \equiv 11(mod\,35)$, f) $8x \equiv 20(mod\,12)$,

b) $3x \equiv 5(mod\ 7)$, g) $6x \equiv 27(mod\ 12)$,
c) $72x \equiv 2(mod\ 10)$, h) $10x \equiv 15(mod\ 35)$.

4. Решить уравнения в целых числах:
   a) $5x + 4y = 3$, f) $91x - 28y = 35$,
   b) $50x - 42y \equiv 34$, g) $2x + 3y = 4$,
   c) $17x + 13y = 1$, h) $4x - 3y = 2$.
5. Сколько билетов по 30 руб. и по 50 руб. можно купить на 1490 руб.?
6. На станцию прибыло 500т. угля в 18 вагонах. В вагонах было по 15т., 20т., 30т. угля. Сколько вагонов было по 15т., сколько – по 20т, сколько – по 30т.?
7. Дано сравнение с переменной x: $2ax \equiv 12\ (mod\ a)$. Укажите верные и неверные утверждения:
   1) Если $a \neq 3$, то решений нет.
   2) Если $a = 6$, то сравнению удовлетворяет любое целое число.
   3) Если $a = 3$, то сравнению удовлетворяет любое целое число.
   4) Если $a = p$ – простое число и $a > 3$, то сравнение решений не имеет.
   5) Если $a > 6$, то решений нет.

Глава 3. СРАВНЕНИЯ ВЫСШИХ СТЕПЕНЕЙ

3.1 Основные понятия

Определение. *Сравнением n-й степени с одной переменной называется сравнение вида*

$$f(x) \equiv 0(\ mod\ m)\ (*),$$

где $m \in N$, $f(x)$ *- многочлен с целыми коэффициентами:*

$f(x) = a_n x^n + \cdots + a_1 x + a_0$, *причем* a_n не $\vdots\ m$.

Целое число c удовлетворяет сравнению $f(x) \equiv 0(\ mod\ m)$, если сравнение $f(c) \equiv 0(\ mod\ m)$, является верным сравнением.

Теорема. *Пусть дано сравнение* $f(x) \equiv 0(\ mod\ m)$, *и целое число* c *удовлетворяет сравнению. Тогда весь класс* $\bar{c}$ *по* $mod\ m$ *состоит из чисел, удовлетворяющих сравнению.*

Доказательство.

Число c удовлетворяет сравнению $f(x) \equiv 0(\ mod\ m)$, следовательно, $f(c) \equiv 0(\ mod\ m)$верное сравнение. Для любого $b \in \bar{c}$ всегда $b \equiv c(mod\ m)$. Но тогда по свойству сравнений $f(b) \equiv f(c)(mod\ m)$, поэтому по транзитивности получим, что $f(b) \equiv 0(\ mod\ m)$, отсюда

следует, что число b удовлетворяет сравнению. А так как b - произвольное из $\bar{c}$, то, следовательно, весь класс вычетов $\bar{c}$ по mod m состоит из чисел, удовлетворяющих сравнению $f(x) \equiv 0(\ mod\ m)$. ■

Определение. *Решением сравнения* $f(x) \equiv 0(\ mod\ m)$ *называется класс вычетов по модулю m, состоящий из чисел, удовлетворяющих сравнению.*

Если класс $\bar{c}$ mod m является решением сравнения $f(x) \equiv 0(\ mod\ m)$, то будем говорить, что класс $\bar{c}$ удовлетворяет сравнению (*). Числом решений сравнения (*) называется число классов вычетов по mod m, удовлетворяющих сравнению (*).

Задача нахождения чисел, удовлетворяющих сравнению (*), сводится к нахождению классов, удовлетворяющих уравнению $f(\bar{x}) = \bar{0}$.

Действительно:

- так как $f(c) \equiv 0(\ mod\ m)$ верно, то $\overline{f(c)} = \bar{0}$, но $\overline{f(c)} = f(\bar{c})$;
- обратно, если $f(\bar{c}) = \bar{0}$, то $\overline{f(c)} = \bar{0}$, следовательно, $f(\mathrm{c}) \equiv 0(\ \mathrm{mod\ m})$

Чтобы решить сравнение $f(x) \equiv 0(\ mod\ m)$, можно

1) взять любую полную систему вычетов по mod m:

$x_0, x_1, \dots, x_{m-1}$, где $x_0 \in \bar{0}, x_1 \in \bar{1}, \dots, x_{m-1} \in \overline{m-1}$;

2) вычислить $f(x_0), f(x_1), \dots, f(x_{m-1})$;

3) взять те числа x_i , при которых сравнение $f(x_i) \equiv 0(\,mod\, m)$ является верным, то есть $f(x_i) \vdots m$. Соответствующие классы $\overline{x_i}$, дадут все решения сравнения.

Удобнее брать полную систему наименьших по абсолютной величине вычетов по mod m. Если сравнение имеет несколько решений $\overline{c_1}, \overline{c_2}, \dots, \overline{c_s}$, то эти решения можно записывать в виде $x \equiv c_1, \dots, c_s (mod\ m)$(то есть x принимает любые значения, сравнимые с одним из чисел $c_1, \dots, c_s$) вместо записи $x \equiv c_1 (mod\ m), \dots, x \equiv c_s (mod\ m)$.

Примеры.

1) $x^3 - 2x + 6 \equiv 0 (mod\ 11)$.

$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}$ - классы вычетов по mod 11.

$x \equiv 5 (mod\ 11)$ – решение сравнения.

2) $x^4 + 2x^3 + 6 \equiv 0 (mod\ 8)$.

$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}$ - классы вычетов по mod 8.

Сравнение не имеет решений.

3) $x^4 - x^3 - x^2 + 5x - 2 \equiv 0 (mod\ 6)$.

$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$ - классы вычетов по mod 6.

$x \equiv 2; 5(mod\ 6)$ – решение сравнения.

Задача нахождения решения сравнения $f(x) \equiv 0(\ mod\ m)$ проще, чем рассматриваемая в курсе алгебры задача нахождения решения уравнения $f(x) = 0$.

Так как решая уравнение в некотором бесконечном множестве (R, C) нельзя перебрать все числа x. А решая сравнение $f(x) \equiv 0(\ mod\ m)$, ищем решение в конечном кольце Z_m классов вычетов по mod m. Следовательно, с помощью конечного числа операций можно найти все решения.

Но надо заметить, что при больших m будут громоздкие вычисления, поэтому надо изучить способы, позволяющие определить число решений, а иногда и способы нахождения решения с помощью возможно меньшего числа операций.

3.2. Сравнения вида $f(x) \equiv g(x)(\,mod\, m)$

Рассмотрим сравнение с одной переменной вида

$$f(x) \equiv g(x)(\,mod\, m),$$

где $f(x), g(x) \in Z[x], m \in N$, коэффициенты при старшем члене $f(x)$ и $g(x)$ не делятся на m.

Определение. *Решением сравнения $f(x) \equiv g(x)(\,mod\, m)$ называется класс вычетов по mod m, состоящий из чисел, удовлетворяющих этому сравнению.*

Теорема. *Пусть $f(x)$ и $g(x)$многочлены с целыми коэффициентами и целое число α удовлетворяет сравнению $f(x) \equiv g(x)(\,mod\, m)$. Тогда весь класс вычетов $\bar{\alpha}$ (mod m) состоит из чисел, удовлетворяющих этому сравнению.*

Доказательство.

1) Так как число α удовлетворяет сравнению $f(x) \equiv g(x)(\,mod\, m)$, то оно удовлетворяет сравнению $h(x) \equiv 0(\,mod\, m)$, где $h(x) = f(x) - g(x)$.

2) $\forall b \in \bar{a}$ mod m будет $b \equiv a\ (mod\, m)$, следовательно, $h(a) \equiv h(b)(\,mod\, m)$, поэтому число b удовлетворяет сравнению

$h(x) \equiv 0(\ mod\ m)$то есть сравнению $f(x) - g(x) \equiv 0(\ mod\ m)$. Следовательно, число b удовлетворяет сравнению $f(x) \equiv g(x)(\ mod\ m)$. Таким образом, класс вычетов $\bar{a}$ состоит из чисел, удовлетворяющих сравнению $f(x) \equiv g(x)(\ mod\ m)$. ■

Определение. *Два сравнения*

$$f_1(x) \equiv g_1(x)(mod\ m_1)\ и\ f_2(x) \equiv g_2(x)(mod\ m_2)$$

называются эквивалентными, если множество чисел, удовлетворяющих одному из них, совпадает с множеством чисел, удовлетворяющих другому сравнению.

Если $m_1 = m_2 = m$ и сравнения имеют одни и те же решения, то получим два эквивалентных сравнения по mod m.

Эквивалентные сравнения могут иметь разную степень.

Пример. $2x + 1 \equiv 0\ (mod\ 3), x^3 - 1 \equiv (mod\ 3)$.

Решение первого сравнения: $x \equiv 1\ (mod\ 3)$, решением второго сравнения тоже будет класс вычетов $x \equiv 1\ (mod\ 3)$. Следовательно, они эквивалентны. Но степени их различны (степень первого сравнения равна 1, степень второго – 3).

3.3. Теоремы об эквивалентных сравнениях

Теорема. *Пусть дано сравнение*

$$f(x) \equiv g(x)(\bmod m),$$

где $f(x), g(x) \in Z[x], m \in N$. *Тогда имеют место следующие утверждения:*

1) Если к обеим частям сравнения прибавить любой многочлен $t(x) \in Z[x]$ *то получится сравнение, эквивалентное сравнению* $f(x) \equiv g(x)(\bmod m)$.

2) Если обе части сравнения умножить на одно и то же целое число, взаимно простое с модулем, то получится сравнение, эквивалентное сравнению $f(x) \equiv g(x)(\bmod m)$.

3) Если обе части сравнения и модуль умножить на одно и то же натуральное число k, то получится сравнение, эквивалентное исходному сравнению $f(x) \equiv g(x)(\bmod m)$.

Доказательство.

1) Пусть класс вычетов $\overline{x_0}$ по модулю m - решение сравнения $f(x) \equiv g(x)(\bmod m)$, то есть для $x_0 \in \overline{x_0}$ сравнение

$$f(x_0) \equiv g(x_0)(\bmod m)$$

является верным сравнением, следовательно, сравнение

$$f(x_0) + t(x_0) \equiv g(x_0) + t(x_0)(\,mod\, m),$$

где $t(x_0) \in Z$, тоже верно. Поэтому класс вычетов $\overline{x_0}$ по модулю m является решением сравнения

$$f(x) + t(x) \equiv g(x) + t(x)(\,mod\, m),$$

Обратное также верно: если $\overline{x_0}$ по модулю m - решение сравнения $f(x) + t(x) \equiv g(x) + t(x)(\,mod\, m)$, то для $x_0 \in \overline{x_0}$, будет верно сравнение $f(x_0) + t(x_0) \equiv g(x_0) + t(x_0)(\,mod\, m)$, а, следовательно, верно и сравнение $f(x_0) \equiv g(x_0)(\,mod\, m)$, поэтому $\overline{x_0}$ является решением сравнения $f(x) \equiv g(x)(\,mod\, m)$.

Таким образом, эти сравнения эквивалентны.

2) Пусть класс вычетов $\overline{x_0}$ по модулю m – решение исходного сравнения, тогда для $x_0 \in \overline{x_0}$, получим верное сравнение $f(x_0) \equiv g(x_0)(\,mod\, m)$. Возьмем целое число k, взаимно простое с модулем. Умножим последнее сравнение почленно на k, получим верное сравнение:

$$kf(x_0) \equiv kg(x_0)(\,mod\, m),$$

отсюда получим, что класс вычетов $\overline{x_0}$ по модулю m - решение сравнения

$$kf(x) \equiv kg(x)(\,mod\ m).$$

Обратно, если класс вычетов $\overline{x_0}$ по модулю m - решение сравнения $kf(x) \equiv kg(x)(\,mod\ m)$, то для $x_0 \in \overline{x_0}$ верно сравнение $kf(x_0) \equiv kg(x_0)(\,mod\ m)$, следовательно, будет верно и сравнение:

$$f(x_0) \equiv g(x_0)(\,mod\ m)$$

(заметим, что $k \neq 0$, так как НОД (k,m)=1, в противном случае было бы: НОД (k,m)=m). Поэтому класс вычетов $\overline{x_0}$ по модулю m - решение сравнения $f(x) \equiv g(x)(\,mod\ m)$.

Таким образом, сравнения $f(x) \equiv g(x)(\,mod\ m)$ и $kf(x) \equiv kg(x)(\,mod\ m)$, где НОД ($k$,$m$)=1, будут эквивалентными.

3) Пусть класс вычетов $\overline{x_0}$ по модулю m - решение сравнения $f(x) \equiv g(x)(\,mod\ m)$, тогда для $x_0 \in \overline{x_0}$ верно сравнение $f(x_0) \equiv g(x_0)(\,mod\ m)$, а, значит, верно и сравнение

$$kf(x_0) \equiv kg(x_0)(\,mod\ m)$$

для любого натурального числа k, поэтому класс вычетов $\overline{x_0}$ по модулю m - решение сравнения

$$kf(x) \equiv kg(x)(\,mod\ m).$$

Обратно, если класс вычетов $\overline{x_0}$ по модулю m - решение сравнения $kf(x) \equiv kg(x)(\,mod\ m)$, то для $x_0 \in \overline{x_0}$ верно сравнение

$kf(x_0) \equiv kg(x_0)(\ mod\ m)$, но тогда по свойству сравнений верно сравнение:

$$f(x_0) \equiv g(x_0)(\ mod\ m),$$

поэтому класс вычетов $\overline{x_0}$ по модулю m - решение сравнения $f(x) \equiv g(x)(\ mod\ m)$. Следовательно, сравнения $f(x) \equiv g(x)(\ mod\ m)$ и $kf(x) \equiv kg(x)(\ mod\ m)$ эквивалентны. ■

В дальнейшем сравнение $f(x) \equiv g(x)(\ mod\ m))$ можно заменить эквивалентным сравнением:

$$h(x) \equiv 0(\ mod\ m),$$

где $h(x) \equiv f(x) - g(x)(\ mod\ m)$.

Теорема. *Пусть даны сравнения*

$$f(x) \equiv 0(\ mod\ m) \text{ и } g(x) \equiv 0(\ mod\ m),$$

где $f(x) = a_n x^n + \cdots + a_0$, $g(x) = b_n x^n + \cdots + b_0$ *и пусть* $a_i \equiv b_i (\mathrm{mod}\, m), i = \{0, \ldots n\}$. *Тогда сравнения эквивалентны.*

Доказательство.

Умножим почленно верные сравнения на $x_0^n, \ldots, x_0$ соответственно, где x_0 - некоторое целое число:

$$a_n x_0^n \equiv b_n x_0^n \ (mod\ m),$$

$$\dots$$

$$a_1 x_0 \equiv b_1 x_0 (mod\ m),$$

$$a_0 \equiv b_0 (mod\ m),$$

Сложим почленно полученные сравнения, тогда получим сравнение

$$a_n x_0^n + \dots + a_0 \equiv b_n x_0^n + \dots + b_0 \ (mod\ m),$$

отсюда получим, что $f(x_0) \equiv g(x_0)(\ mod\ m)$. Но тогда

$$f(x_0) \equiv 0(\ mod\ m) \text{ и } g(x_0) \equiv 0(\ mod\ m).$$

Следовательно, сравнения $f(x) \equiv 0(\ mod\ m)$ и $g(x) \equiv 0(\ mod\ m)$ эквивалентны. ■

Заметим, из доказанной теоремы, в частности, следует, что сравнение заменится эквивалентным, если отбросить (или добавить) слагаемое с коэффициентами, делящимися на модуль.

3.4. Сравнения по простому модулю с одним неизвестным

Переходя от сравнений 1-й степени к сравнениям более высоких степеней, целесообразно сначала рассмотреть тот случай, когда модуль – простое число. В этом случае имеется ряд весьма важных теорем, которые, вообще говоря, неверны для составных модулей. Вместе с тем теория сравнений по простому модулю является основой, на которой строится изучение сравнений по составному модулю.

Во всей этой главе буквой p будем обозначать модуль, представляющий собой простое число.

Теорема. *Если* $p \nmid c_0$, *то сравнение*

$$c_0 x^n + c_1 x^{n-1} + \cdots + c_n \equiv 0 \ (mod\ p)$$

может быть заменено эквивалентным сравнением с коэффициентом при старшем члене, равном единице.

Доказательство.

Рассмотрим сравнение 1-й степени $c_0 y \equiv 1 \ (mod\ p)$. Поскольку $p \nmid c_0$, то и сравнение имеет решение. Найдем число y_0, удовлетворяющее этому сравнению, т.е. y_0 такое, что $c_0 y_0 \equiv 1 \ (mod\ p)$.

Тогда сравнение $c_0 x^n + c_1 x^{n-1} + \cdots + c_n \equiv 0 \ (mod\ p)$ эквивалентно сравнению

$$(c_0y_0)x^n + (c_1y_0)x^{n-1} + \cdots + (c_ny_0) \equiv 0\ (mod\ p),$$

а, следовательно, сравнению

$$x^n + b_1x^{n-1} + \cdots + b_n \equiv 0\ (mod\ p),$$

где $b_i \equiv c_iy_0\ (mod\ p)$ для i $\in \{1, \ldots n\}$. ■

Пример. Заменить сравнение

$$27x^3 + 14x^2 - 10x + 13 \equiv 0 (\mathrm{mod}\ 59)$$

эквивалентным сравнением с коэффициентом при старшем члене, равным 1.

Решаем сравнение $27y_0 \equiv 1 (\mathrm{mod}\ 59)$ и находим $y_0 = 35$. Данное нам сравнение эквивалентно сравнению

$x^3 + 14 \cdot 35x^2 - 10 \cdot 35x + 13 \cdot 35 \equiv O (\mathrm{mod}\ 59)$, т.е. сравнению

$$x^3 + 18x^2 + 4x - 17 \equiv O (\mathrm{mod}\ 59).$$

Теорема. *Если $f(x)$ и $g(x)$ многочлены с целыми коэффициентами, то сравнения по простому модулю*

$$f(x) \equiv 0 (mod\ p)\ и\ f(x) - (x^p - x)g(x) \equiv 0\ (mod\ p)$$

эквивалентны.

Доказательство.

Пусть x_0 удовлетворяет сравнению $f(x) \equiv 0(mod\ p)$, т.е. $f(x_0) \equiv 0(mod\ p)$. Поскольку при любом x_0 согласно теореме Ферма $x^p - x \equiv 0\ (mod\ p)$, то $f(x_0) - (x_0^p - x_0)g(x_0) \equiv 0\ (mod\ p)$.

Пользуясь той же теоремой Ферма, получаем, что если x_0 удовлетворяет сравнению $f(x) \equiv 0(mod\ p)$, то

$$f(x_0) \equiv (x_0^p - x_0)g(x_0) \equiv 0\ (mod\ p)$$

и, таким образом, сравнения

$$f(x) \equiv 0(mod\ p)\ и\ f(x) - (x^p - x)g(x) \equiv 0\ (mod\ p)$$

эквивалентны. ■

Теорема. *Сравнение*

$$f(x) \equiv 0(mod\ p)$$

по простому модулю p, степеньn $\geq p$, может быть заменено эквивалентным сравнением степени, меньшей p.

Доказательство.

Пусть $f(x)$ - многочлен с целыми коэффициентами степени $n \geq p$. При делении $f(x)$ - на $(x^p - x)$, частное $g(x)$ - и остаток $r(x)$ -будут также многочленами с целыми коэффициентами:

Кафедра ФМО и ИТ

$$f(x) = (x^p - x)g(x) + r(x),$$

Согласно предыдущей теореме, сравнения $f(x) \equiv 0(mod\ p)$ и $r(x) \equiv 0(mod\ p)$ эквивалентны.

А так как $\deg r(x) < \deg(x^p - x) = p$, то сравнение можно заменить на эквивалентное степени, меньшей p. ■

Если все коэффициенты $r(x)$ делятся на p, где

$$f(x) = g(x)q(x) + r(x),$$

то любое решение сравнения $f(x) \equiv 0(mod\ p)$ является решением по крайней мере одного из сравнений $g(x) \equiv 0(mod\ p)$ или $q(x) \equiv 0(mod\ p)$.

Каждое слагаемое x^s многочлена $f(x)$ при $s \geq p$ надо заменить на слагаемое

$$x^s - (x^p - x)x^{s-p} = x^s - x^{p+s-p} + x^{1+s-p} = x^{s-p+1} = x^{s-(p-1)},$$

то есть на $x^{s-(p-1)}$.

Следовательно, если $s = (p-1)q + r, 0 \leq r < p-1$, то x^s можно заменить на x^r.

Пример. Сравнение $x^{16} + 3x^8 - 5x^7 - x^4 + 6x - 2 \equiv 0(\mathrm{mod}\,7)$ заменить эквивалентным сравнением степени, меньшей чем 7.

Решение.

Заменим x^{16} на $x^{16-2\cdot 6} = x^4$, x^8 на x^2, x^7 на x. Таким образом, заданное сравнение эквивалентно сравнению

$$(x^4 + 3x^2 - 5x) - x^4 + 6x - 2 \equiv 0(\mathrm{mod}\,7),$$

т.е. сравнению $3x^2 + x - 2 \equiv 0(\mathrm{mod}\,7)$.

Теорема. *Если $f(x), g(x), h(x), r(x)$ многочлены с целыми коэффициентами: $f(x) = g(x)h(x) + r(x)$, и все коэффициенты $r(x)$ делятся на простое число p, то любое решение сравнения*

$$f(x) \equiv 0(mod\ p)$$

является решением, по крайней мере, одного из сравнений:

$$g(x) \equiv 0(mod\ p) \text{ или } h(x) \equiv 0(mod\ p).$$

Доказательство.

Пусть x_0 - решение сравнения $f(x) \equiv 0(mod\ p)$, т.е. $f(x_0) \equiv 0(mod\ p)$. Поскольку все коэффициенты r(x) делятся на p, будем также иметь $r(x) \equiv 0(mod\ p)$, поэтому

$$g(x_0)h(x_0) = f(x_0) - r(x_0) \equiv 0\ (mod\ p).$$

Из сравнимости произведения $g(x_0)h(x_0)$ с нулем по модулю p следует, что по крайней мере один из этих множителей сравним с нулем по этому модулю, т.е. x_0 решение по крайней мере одного из сравнений $g(x) \equiv 0(mod\ p)$ или $h(x) \equiv 0(mod\ p)$.

Пример. В сравнении $x^4 + 18x^2 + 5 \equiv 0(\mathrm{mod}\,31)$ левую часть можно представить в виде $(x^2 - 4)(x^2 - 9) + (31x^2 - 31)$, и мы находим все решения этого сравнения, решая сравнения:

$$x^2 - 4 \equiv 0(\mathrm{mod}\,31),\ x^2 - 9 \equiv 0(\mathrm{mod}\,31),$$

т.е. $x \equiv \pm 2(\mathrm{mod}\,31)$ и x $\equiv \pm 3(\mathrm{mod}\,31)$. Все эти четыре класса удовлетворяют нашему сравнению.

Для составных модулей эта теорема неверна. Например, сравнению

$$x^2 + 4x = x(x + 4) \equiv 0(\mathrm{mod}\,12)$$

удовлетворяет класс $\bar{6}$, не являющийся решением ни одного из сравнений: $x \equiv 0(\mathrm{mod}\,12)$, $x + 4 \equiv 0(\mathrm{mod}\,12)$.

Теорема. *Сравнение* $f(x) \equiv 0(mod\ p)$,*где* $f(x) = a_n x^n + \cdots + a_0$ *с коэффициентом при старшем члене, не делящимся на p, может иметь не больше чем n решений.*

Доказательство.

Утверждение теоремы верно при $n=1$. Действительно, в этом случае мы имеем сравнение 1-й степени: $c_0x + c_1 \equiv (mod\ p)$, где $p \nmid c_0$, т.е. $(c_0, p) = 1$, а такое сравнение имеет в точности одно решение. Применим теперь для доказательства теоремы метод полной математической индукции. Предположим, что утверждение теоремы верно для всех многочленов (n-1) – й степени со старшими коэффициентами, не делящимися на простой модуль p. Возьмем теперь произвольный многочлен n–ой степени:

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n,$$

где $p \nmid c_0$, и рассмотрим сравнение $f(x) \equiv 0(mod\ p)$,

Если это сравнение не имеет ни одного решения, то число решений меньше чем n.

Если же это сравнение имеет решения, то возьмем любое число x_0, удовлетворяющее ему, и разделим f(x) на x-x_0. Согласно теореме Безу будем иметь:

$$f(x) = (x - x_0)g(x) + f(x_0).$$

Коэффициенты многочлена (n-1)-ой степени

$$g(x) = b_0x^{n-1} + \cdots + b_{n-1}$$

могут быть найдены по схеме Горнера и представляют собой целые числа, причем $b_0 = c_0$.

Поскольку x_0 удовлетворяет сравнению $f(x) \equiv 0(mod\ p)$, $p|f(x_0)$, то все решения сравнения находятся среди решений сравнений $x - x_0 \equiv 0\ (mod\ p)$ и $g(x) \equiv 0(mod\ p)$, удовлетворяя либо одному из них, либо обоим.

Сравнение $x - x_0 \equiv 0\ (mod\ p)$ имеет одно решение, а сравнение $g(x) \equiv 0(mod\ p)$ представляет собой сравнение (n-1) – ой степени по простому модулю с коэффициентом при старшем члене $b_0 = c_0$, не делящемся на p, и, по предположению, может иметь не больше чем n-1 решений. Таким образом, сравнение $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n$ имеет не больше, чем $1 + (n - 1)$, т.е. не больше чем n решений.

Согласно принципу математической индукции справедливость теоремы доказана. ■

Пример. x_0=31 удовлетворяет сравнению $11x^2 \equiv 65\ (mod\ 103)$ Найти все решения этого сравнения.

Очевидно, что вместе с классом $\overline{31}$ этому сравнению удовлетворяет и класс $\overline{-31}$. Коэффициент при старшем члене 11 не делится на простой модуль 103, поэтому сравнение не может иметь больше двух решений.

Для составных модулей эта теорема неверна. Сравнение степени n по составному модулю с коэффициентом при старшем члене, не делящемся на модуль или даже взаимно простом с модулем, может иметь больше чем n решений. Например, сравнение $x^2 - 3x + 2 \equiv 0\ (mod\ 6)$ имеет 4 решения: $\overline{1}, \overline{2}, \overline{4}, \overline{5}$.

Теорема. *Если сравнение степени n по простому модулю p имеет больше чем n решений, то все коэффициенты сравнения делятся на p.*

Доказательство.

Возьмем любое простое число p. Если сравнение $c_0x + c_1 \equiv 0\ (mod\ p)$ имеет больше чем одно решение, то $(c_0, p) = 1$, т.е. $p|c_0$, . Таким образом, при $n = 1$ теорема верна. Предположим, что утверждение теоремы верно для многочленов степени, меньшей чем n, т.е. предположим, что число решений сравнения степени, меньшей чем n, может превосходить степень сравнения только тогда, когда все коэффициенты делятся на модуль p.

Возьмем любое сравнение степени n

$$c_0x^n + c_1x^{n-1} + \cdots + c_n \equiv 0\ (mod\ p),$$

имеющее больше чем n решений. В таком сравнении c_0 делится на p, а тогда сравнение

$$c_1 x^{n-1} + \cdots + c_n \equiv 0 \ (mod\ p),$$

эквивалентное первому сравнению, также имеет больше чем n решений.

В данном сравнении, степень которого меньше чем n, а число решений превосходит степень согласно предположению, все коэффициенты должны делиться на p, т.е. $p|c_1$, …, $p|c_n$. Поскольку уже раньше было установлено, что $p|c_0$, утверждение теоремы верно для n. Согласно принципа математической индукции справедливость теоремы доказана. ■

Теорема. *Пусть* $f(x) = x^n + c_1 x^{n-1} + \cdots + c_n$ *- многочлен с целыми коэффициентами и свободным членом* $c_n \not\equiv 0 \ (mod\ p)$, *где* p *- простое число, причем* $p \geq n$. *Сравнение* $f(x) \equiv 0 \ (mod\ p)$ *имеет n решений тогда и только тогда, когда все коэффициенты остатка от деления* $x^{p-1} - 1$ *на* f(x) *кратны p.*

Доказательство.

Пусть $x^{p-1} - 1 = f(x)g(x) + r(x)$, где $g(x)$ и $r(x)$многочлены с целыми коэффициентами, причем степень $r(x)$ меньше чем n.

1) Докажем достаточность условия. Пусть коэффициенты $r(x)$ делятся на p. Обозначим через S и T соответственно число решений сравнений

$$f(x) \equiv 0\ (mod\ p),\ g(x) \equiv 0\ (mod\ p).$$

Сравнение $x^{p-1} - 1 \equiv 0\ (mod\ p)$ по теореме Ферма имеет $p-1$ решений. Каждое из этих $p-1$ решений является решением хотя бы одного из сравнений $f(x)$ или $g(x) \equiv 0\ (mod\ p)$, т.е. $S + T \geq p - 1$.

Сравнение $x^{p-1} - 1 \equiv 0\ (mod\ p)$ степени $p - 1 - n$ имеет коэффициент при старшем члене, равный единице, так что $T \leq p - 1 - n$ и, следовательно,

$$S \geq (p-1) - T \geq p - 1 - (p - 1 - n) = n.$$

Поскольку при этом $S \leq n$, получаем $S = n$, т.е. из делимости коэффициентов $r(x)$ на p следует, что число решений сравнения $f(x) \equiv 0\ (mod\ p)$ равно n.

2) Докажем необходимость условия.

Пусть сравнение $f(x) \equiv 0\ (mod\ p)$, имеет n решений. Если x_0 решение этого сравнения, то $f(x_0) \equiv 0\ (mod\ p)$, и вместе с тем, поскольку $p \nmid c_n$, то $p \nmid x_0$, а, следовательно, согласно теореме Ферма, $x_0^{p-1} - 1 \equiv 0\ (mod\ p)$, так что

$$r(x_0) = \left(x_0^{p-1} - 1\right) - f(x_0)g(x_0) \equiv 0(mod\ p).$$

Таким образом, каждое из n решений сравнения $f(x) \equiv 0\ (mod\ p)$ является решением сравнения $r(x) \equiv 0\ (mod\ p)$,

степень которого меньше чем n. Следовательно, все коэффициенты $r(x)$ делятся на p.

Пример. Сравнению $x^3 \equiv 1\ (mod\ 13)$ удовлетворяют классы $\overline{1}$ и $\overline{3}$. Имеет ли это сравнение еще одно решение?

Делим $x^{12} - 1$ на $x^3 - 1$, находим

$$x^{12} - 1 = (x^3 - 1)(x^9 + x^6 + x + 1).$$

так что $r(x) = 0$ и, следовательно, это сравнение имеет три решения.

3.5. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю

Рассмотрим способ приведения сравнения по составному модулю к сравнению по простому модулю.

1. *Приведение сравнения по составному модулю к сравнению по степени простого числа.*

Теорема. *Пусть натуральное число m, большее 1, имеет каноническое разложение $m = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_s}^{\alpha_s}$, где $p_1, p_2, \ldots, p_s$ – попарно различные положительные простые числа, $\alpha_1, \alpha_2, \ldots, \alpha_s$ – натуральные числа. Тогда сравнение*

$$f(x) \equiv 0 (mod\ m)$$

Эквивалентно следующей системе сравнений:

$$\begin{cases} f(x) \equiv 0 (\ mod\ {p_1}^{\alpha_1}), \\ f(x) \equiv 0 (\ mod\ {p_2}^{\alpha_2}), \\ \ldots \\ f(x) \equiv 0 (\ mod\ {p_s}^{\alpha_s}). \end{cases}$$

Теорема. *Число решений сравнения* $f(x) \equiv 0(mod\ m)$

равно $k_1, k_2, \dots, k_s$, *где* $k_1, k_2, \dots, k_s$ *соответственно равно числу решений каждого из сравнений системы*

$$\begin{cases} f(x) \equiv 0(\ mod\ {p_1}^{\alpha_1}), \\ f(x) \equiv 0(\ mod\ {p_2}^{\alpha_2}), \\ \dots \\ f(x) \equiv 0(\ mod\ {p_s}^{\alpha_s}). \end{cases}$$

Пример. Решить сравнение $x^2 - 3x + 23 \equiv 0\ (mod\ 63)$.

Так как $63 = 7 \cdot 9$, поэтому получим систему из двух сравнений

$$\begin{cases} x^2 - 3x + 23 \equiv 0\ (mod\ 7), \\ x^2 - 3x + 23 \equiv 0\ (mod\ 9). \end{cases}$$

Решим первое сравнение системы, получим два решения $x \equiv 1; 2\ (mod\ 7)$. Решим второе сравнение системы, получим так же два решения $x \equiv 4; 8\ (mod\ 9)$.

В результате получим четыре системы сравнений, каждая из которых состоит из двух сравнений:

1. $\begin{cases} x \equiv 1\ (mod\ 7), \\ x \equiv 4\ (mod\ 9), \end{cases}$

2. $\begin{cases} x \equiv 1 \ (mod\ 7), \\ x \equiv 8 \ (mod\ 9), \end{cases}$

3. $\begin{cases} x \equiv 2 \ (mod\ 7), \\ x \equiv 4 \ (mod\ 9), \end{cases}$

4. $\begin{cases} x \equiv 2 \ (mod\ 7), \\ x \equiv 8 \ (mod\ 9). \end{cases}$

Получим соответственно решения:

$x \equiv 22 \ (mod\ 63), x \equiv 8 \ (mod\ 63), x \equiv 58 \ (mod\ 63), x \equiv 44 \ (mod\ 63).$

2. *Приведение сравнения по модулю p^α к сравнению по простому модулю p.*

Рассмотрим сравнение по модулю p^α, где p – простое число. Нахождение решений такого сравнения сводится к решению сравнению по простому модулю на основании следующей теоремы.

Теорема. *Пусть класс вычетов $\bar{a}$ по простому модулю p удовлетворяет сравнению $f(x) \equiv 0(mod\ p)$ и $f'(a)$ не делится на p. Тогда числа из класса $\bar{a}$, удовлетворяющее сравнению $f(x) \equiv 0(mod\ p^k)$, где k – натуральное число, образует класс по модулю p^k.*

Доказательство.

Доказательство проводится методом математической индукции по переменной k.

Для того, чтобы, зная решение $x \equiv b(mod\, p^k)$ сравнения $f(x) \equiv 0(mod\, p^k)$, такое, что $f'(b)$ не делится на p, найти решение $x \equiv c(mod\, p^{k+1})$ сравнения $f(x) \equiv 0(mod\, p^{k+1})$, надо взять

$$c = b + p^k \cdot t_0,$$

где t_0 удовлетворяет сравнению $f'(b) \cdot p^k \cdot t + f(b) \equiv 0(\, mod\, p^{k+1})$.

Для каждого решения $\bar{a}$ сравнения $f(x) \equiv 0(mod\, p)$, такого, что $f'(a)$ не делится на p, можно найти последовательно решение сравнений $f(x) \equiv 0(mod\, p^2), \ldots, f(x) \equiv 0(mod\, p^\alpha)$ при любом сколь угодно большом α.

Итак, решение сравнения $f(x) \equiv 0(\, mod\, {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_s}^{\alpha_s})$ сводится к решению сравнений вида $f(x) \equiv 0(mod\, p^\alpha)$. Оказывается, что решение этого последнего сравнения, в свою очередь, сводится к решению некоторого сравнения $g(x) \equiv 0(mod\, p)$ с другим многочленом в левой части, но уже с простым модулем, а это приводит в рамки предыдущего пункта. Сейчас я расскажу процесс сведения решения сравнения $f(x) \equiv 0(mod\, p^\alpha)$ к решению сравнения $g(x) \equiv 0(mod\, p)$.

Процесс сведения

Решение сравнение вида $f(x) \equiv 0(mod\, p^\alpha)$ может быть найдено, если известно решение сравнения $f(x) \equiv 0(mod\, p)$. Покажем это.

Пусть $x \equiv x_1(mod\, p)$– решение сравнения $f(x) \equiv 0(mod\, p)$. Тогда x можно представить в виде $x=x_1+pt_1$, где $t_1 \in Z$.

Подставляя такое x в сравнение $f(x) \equiv 0(mod\ p^2)$ и применяя формулу Тейлора (учитывая, что $f(x)$ – многочлен, x_1 – целое число, поэтому $\frac{f^{(k)}(x_1)}{k!} \in Z$), получаем

$$f(x_1)+pt_1f'(x_1)\equiv 0(\mathrm{mod}\ p^2).$$

Поскольку $f(x_1)\equiv 0(\mathrm{mod}\ p)$, то p делит $f(x_1)$, а значит можно сократить в получившемся выражении на p правую, левую части и модуль. Получим:

$$\frac{f(x_1)}{p}+t_1f'(x_1)\equiv 0(\mathrm{mod}\ p)$$

Если $f'(x_1)$ не делится на p, то данное сравнение имеет одно решение:

$$t_1=\bar{t_1}(\mathrm{mod}\ p)\ (\text{т.е. } t=\bar{t_1}+pt_2)\ \Rightarrow\ x=x_1+p\bar{t_1}+p\bar{t_1}t_2=x_2+p^2t_2$$

Подставляя полученное x в сравнение $f(x)\equiv 0(\mathrm{mod}\ p^3)$, имеем

$$f(x_2)+p^2t_2f'(x_2)\equiv 0(\mathrm{mod}\ p^3),$$

откуда, сократив правую, левую части и модуль на p^2, получим

$$\frac{f(x_2)}{p}+t_2f'(x_2)\equiv 0(\mathrm{mod}\ p)$$

[Здесь $f'(x_2)$ не может быть кратно p, если $f'(x_1)$ не кратно p, т.к. $x_2\equiv x_1(\mathrm{mod}\ p)$, а значит, $f'(x_2)\equiv f'(x_1)\ (\mathrm{mod}\ p)$]

Тогда сравнение имеет одно решение $t_2=\bar{t_2}(\mathrm{mod}\ p)$, или, что то же самое, $t_2=\bar{t}_2+pt_3$, откуда получаем решение по модулю p^3: $x=x_3+p^3t_3$.

Продолжим этот процесс до тех пор, пока не будет решено сравнение по модулю p^{α}. Итак, по данному решению сравнения $f(x)\equiv 0 \pmod p$ можно найти решение сравнения $f(x)\equiv 0 \pmod{p^{\alpha}}$.

Итак:

Всякое решение $x \equiv x_1 \pmod p$ сравнения $f(x) \equiv 0 \pmod p$, при условии p делит $f'(x_1)$, дает одно решение сравнения $f(x) \equiv 0 \pmod{p^a}$ вида $x \equiv x_a + p^a t_a$, т.е. $x \equiv x_a \pmod{p^a}$.

Пример 1. Требуется решить сравнение $x^3+9x-1\equiv 0 \pmod{125}$.

Решение.

Известно, что сравнение $x^3+9x-1\equiv 0 \pmod 5$ имеет одно решение:

$$x\equiv 2 \pmod 5, \text{ или } x=2+5t_1.$$

Подставим получившееся x в сравнение по модулю 25:

$$(2+5t_1)^3+9(2+5t_1)-1\equiv 0 \pmod{25}.$$

Решим это сравнение.

$$8+4\cdot 5t_1+2\cdot(5t_1)^2+(5t_1)^3+18+9\cdot 5t_1-1\equiv 0 \pmod{25}$$

$$25+13\cdot 5t_1+25(5t_1{}^3+2\,t_1{}^2) \equiv 0 \pmod{25}$$

$$13\cdot 5t_1\equiv 0 \pmod{25}$$

$$13t_1\equiv 0 \pmod 5$$

$$t_1\equiv 0 \pmod 5$$

или, что тоже самое, $t_1=0+5t_2$, откуда решение по модулю 25 есть $x=2+25t_2$. Подставим полученное x в сравнение по модулю 125:

$$(2+25t_2)^3+9(2+25t_2) - 1\equiv 0 \pmod{125}$$

$$8+4\cdot 25t_2+2\cdot(25t_2)^2+(25t_1)^3+18+9\cdot 25t_1-1\equiv 0 \pmod{125}$$

$$25+13\cdot 25t_2+625\cdot(25t_2^3+2t_2^2)\equiv 0 \pmod{125}$$
$$25+13\cdot 25t_2\equiv 0 \pmod{125}$$
$$1+13t_2\equiv 0 \pmod 5$$
$$13t_2\equiv -1 \pmod 5$$
$$3t_2\equiv 4 \pmod 5$$

Получили сравнение первой степени. Найдем $3^{-1}(\mathrm{mod}\ 5)$, для чего, как всегда, воспользуемся расширенным алгоритмом Евклида:

$$5=3+2$$
$$3=2+1$$
$$2=1+0$$
$$1=3-2=3-(5-3)=2\cdot 3-1\cdot 5.$$
$$2\equiv 3^{-1}(\mathrm{mod}\ 5).$$

Тогда решением сравнения относительно t_2 будет

$$t_2\equiv 2\cdot 4 \pmod 5$$
$$t_2\equiv 3 \pmod 5$$

или, что то же самое, $t_2=3+5t_3$, откуда решение по модулю 125 есть $x=2+25(3+5t_3)=2+75+125t_3=77+125t_3$, или, что то же самое,

$$x\equiv 77 \pmod{125}.$$

Пример 2. Решить сравнение $x^4+7x+4\equiv 0(\mathrm{mod}27)$.

Решение.

$$27=3^3.$$

Процесс решения должен быть таким:

$$f'(x)=(4x^3+7)\,|_{x\equiv 1}\equiv 2(\mathrm{mod}\ 3),$$

т.е. не делится на $p = 3$. Далее: $x_1 = 1+3\,t_1$

$$f(1)+f'(1)\,3\,t_1 \equiv 0 (\mathrm{mod}\ 3^2)$$

Ищем t_1 : $3+3\,t_1 \cdot 2 \equiv 0(\mathrm{mod}\ 9)$, после деления на $p = 3$:

$$1+2\,t_1 \equiv 0(\mathrm{mod}\ 3),$$

$t_1 \equiv 1(\mathrm{mod}\ 3)$ - единственное решение.

Далее: $t_1 = 1+3\,t_2$,

$$x = 1+3\,t_1 = 4+9\,t_2, f(4)+9\,t_2 f'(4) \equiv 0(\mathrm{mod}\ p^3 = 27),$$

$$18+9\ 20\,t_2 \equiv 0(\mathrm{mod}27),$$

и, после деления на $p^2 = 9$, ищем t_2: $2+20t_2 \equiv 0(\mathrm{mod}3)$, $t_2 \equiv 2(\mathrm{mod}3)$, $t_2 = 2+3t_3$, откуда $x = 4+9\,(2+3\,t_3) = 22+27\,t_3$.

Значит, решением сравнения является $x \equiv 22(\mathrm{mod}27)$.

Пример 3. Решить сравнение

$$x^3 - 2x^2 - 30x + 41 \equiv 0\ (mod\ 125)$$

1) Решим сравнение $f(x) \equiv 0(\ mod\ 5)$. Оно эквивалентно сравнению $x^3 - 2x^2 + 4 \equiv 0\ (mod\ 5)$. Решим его методом подбора, получим что оно имеет два решения $x \equiv 1; 3\ (mod\ 5)$.
2) Возьмем решение $x \equiv 1(mod\ 5)$. Составим сравнение

$$f'(1)t + \frac{f(1)}{5} \equiv 0\ (mod\ 5),$$

$$-31t + 2 \equiv 0\ (mod\ 5),$$

$$4t + 2 \equiv 0\ (mod\ 5),$$

$t \equiv 2\ (mod\ 5)$ – решение сравнения, составленного в пункте 2).

Выберем теперь $t_0 = 2$ из класса $t \equiv 2\ (mod\ 5)$. Найдем решение сравнения $f(x) \equiv 0(mod\ 25)$ в виде $x \equiv 1 + 2 \cdot 5\ (mod\ 25)$, то есть $x \equiv 11\ (mod\ 25)$.

Составим сравнение

$$f'(11)t + \frac{f(11)}{25} \equiv 0\ (mod\ 5),$$
$$289t + 32 \equiv 0\ (mod\ 5),$$
$$4t + 2 \equiv 0\ (mod\ 5),$$
$$t \equiv 2\ (mod\ 5).$$

Пусть $t_0 = 2$, тогда решение сравнения $f(x) \equiv 0(mod\ 125)$ будет иметь вид $x \equiv 11 + 2 \cdot 25\ (mod\ 125)$, то есть $x \equiv 61\ (mod\ 125)$.

3) Возьмем решение $x \equiv 1(mod\ 5)$. Рассуждая аналогично пункту 2), составим сравнение, которое будет иметь решения.

В случай, когда $f'(a)$ делится на p, среди значений x, удовлетворяющих сравнению $f(x) \equiv 0(mod\ p)$, может не быть чисел, удовлетворяющих сравнению $f(x) \equiv 0(p^{\alpha})$, но может быть и несколько классов по модулю p^{α}, являющихся решениями последнего сравнения.

Теорема. *Пусть класс вычетов $\bar{a}$ по простому модулю p удовлетворяет сравнению $f(x) \equiv 0(mod\ p)$ и $f'(a)$ делится на p. Тогда*

1) *если $f(a)$ не делится на p^{k+1}, то среди чисел класса $\bar{a}$ нет ни одного числа, удовлетворяющего сравнению $f(x) \equiv 0(mod\ p^{k+1})$;*
2) *если $f(a)$ делится на p^{k+1}, то все числа класса $\bar{a}$ удовлетворяют сравнению $f(x) \equiv 0(mod\ p^{k+1})$.*

Упражнения

1. Сколько решений имеет сравнение $x^5 + x + 1 \equiv 0 (\mathrm{mod}\, 105)$?

2. Решите сравнения:

а) $7x^4 + 19x + 25 \equiv 0 (\mathrm{mod}\, 27)$;

б) $9x^2 + 29x + 62 \equiv 0 (\mathrm{mod}\, 64)$;

в) $6x^3 + 27x^2 + 17x + 20 \equiv 0 (\mathrm{mod}\, 30)$;

г) $31x^4 + 57x^3 + 96x + 191 \equiv 0 (\mathrm{mod}\, 225)$;

д) $x^3 + 2x + 2 \equiv 0 (\mathrm{mod}\, 125)$;

е) $x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0 (\mathrm{mod}\, 625)$.

Глава 4. СИСТЕМЫ СРАВНЕНИЙ

4.1. Системы сравнений с одной переменной

Теорема. *Пусть дана система сравнений*

$$\begin{cases} f_1(x) \equiv 0 (mod\ m_1), \\ f_2(x) \equiv 0 (mod\ m_2), \\ \dots \\ f_s(x) \equiv 0 (mod\ m_n) \end{cases}$$

$M = \text{НОК}\,(m_1, m_2, \dots, m_s)$ *и целое число* a *удовлетворяет всем сравнениям системы. Тогда весь класс* $\bar{a}$ *по mod* m *состоит из чисел, удовлетворяющих всем сравнениям системы.*

Доказательство.

Если число a удовлетворяет системе сравнений, то $f_1(a) \vdots m_1, \dots, f_s(a) \vdots m_s$. но так как $M = \text{НОК}\,(m_1, m_2, \dots, m_s)$, то $\forall b \in \bar{a}$, такого, что $b \equiv a\ (mod\ M)$, получим, что $f_1(b) \equiv f_1(a) (mod\ M), \dots, f_s(b) \equiv f_s(a) (mod\ M)$, следовательно, так как $M \vdots m_1, \dots, M \vdots m_s$, получим сравнения: $f_1(b) \equiv f_1(a) (mod\ m_1)$, …, $f_s(b) \equiv f_s(a) (mod\ m_s)$. Таким образом, число b удовлетворяет системе

сравнений, а потому весь класс вычетов $\bar{a}$ по *mod m* состоит из чисел, удовлетворяющих системе. ■

Определение. *Решением системы сравнений*

$$\begin{cases} f_1(x) \equiv 0 (mod\ m_1), \\ f_2(x) \equiv 0 (mod\ m_2), \\ \dots \\ f_s(x) \equiv 0 (mod\ m_n) \end{cases}$$

называется класс вычетов по mod M, $M = \text{НОК}\ (m_1, m_2, \dots, m_s)$, *состоящий из чисел, удовлетворяющих всем сравнениям системы.*

Число решений системы означает число классов по mod *M*, удовлетворяющих всем этим сравнениям. Решение будем находить в любой полной системе вычетов по mod M.

Если $m_1 = m_2 = \dots = m_s = m$, то решениями являются классы вычетов по mod *m*.

Пример 1. Решить систему сравнений

$$\begin{cases} x^2 + x + 7 \equiv 0\ (mod\ 9), \\ x^2 - x + 3 \equiv 0\ (mod\ 9). \end{cases}$$

Классы вычетов по $mod\ 9$: $\bar{0},\ \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{7}, \bar{8}$ при $x = -2$ имеем:

1) $(-2)^2 - 2 + 7 = 9 \equiv 0\ (mod\ 9)$, следовательно, $x = -2$ удовлетворяет первому сравнению системы,

2) $(-2)^2 - (-2) + 3 = 9 \equiv 0\ (mod\ 9)$, следовательно, $x = -2$ удовлетворяет второму сравнению системы,, следовательно, $x \equiv -2(mod\ 9)$ удовлетворяет второму сравнению системы.

Поэтому класс вычетов $x = \overline{-2}$ является решением системы. Можно записать этот класс иначе: прибавив к -2 модуль 9, получим, что $x \equiv 7\ (mod\ 9)$.

Итак, данная система сравнений имеет решение $x \equiv 7\ (mod\ 9)$.

Пример 2. Решить систему сравнений

$$\begin{cases} x^2 - 3x + 2 \equiv 0\ (mod\ 6), \\ 2x^2 + x + 2 \equiv 0\ (mod\ 4). \end{cases}$$

$M = \text{НОК}\ (6,4) = 12, M = 12$. Классы $mod\ 12$: $\overline{0},\ \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, 1\overline{0}, 1\overline{1}$.

Непосредственной подстановкой определяем

$$x \equiv \pm 2\ (mod\ 12).$$

4.2. Системы сравнений первой степени

Систему сравнений первой степени с одним и тем же неизвестным, но с разными модулями, запишем в общем виде так:

$$\begin{cases} a_1 x \equiv b_1 (mod\ m_1), \\ a_2 x \equiv b_2 (mod\ m_2), \\ \dots \\ a_n x \equiv b_n (mod\ m_n). \end{cases}$$

Общий способ (способ последовательного решения) состоит в том, что сначала находится $x \equiv \alpha (mod\ m)$ из первого сравнения, где α – наименьший неотрицательный или абсолютно наименьший вычет по модулю m_1 и берется класс чисел

$$x = m_1 t + \alpha,$$

удовлетворяющих первому сравнению.

Затем это значение x подставляется во второе сравнение, что дает

$$a_2 (m_1 t + \alpha) \equiv b_2 (mod\ m_2)$$

откуда находится t опять в виде класса чисел и подставляется в равенство.В результате получается значение x в виде класса чисел, удовлетворяющих первым двум сравнениям системы. Дальше это значение x

подставляется в третье сравнение системы, так же находится t_1, затем находится x и подставляется в четвертое сравнение системы и т.д.

Заметим, что можно идти и несколько иным путем: сначала решается каждое из сравнений системы и представляется в виде:

$$\begin{cases} x \equiv \alpha_1 (mod\ m_1), \\ x \equiv \alpha_2 (mod\ m_2), \\ \dots \\ x \equiv \alpha_n (mod\ m_n), \end{cases}$$

а затем поступают описанным способом.

Если окажется, что хотя бы одно из сравнений системы не имеет решения или сравнение относительно t_1 в описанном способе неразрешимо, то система не имеет решения.

Если для сравнений $a_1 x \equiv b_1 (mod\ m_1)$ системы $(a_i, m_i) = d_i$ и $d_i | b_i$, то, сокращая члены и модуль каждого сравнения на d_i, получаем систему:

$$\begin{cases} \frac{a_1}{d_1} x \equiv \frac{b_1}{d_1} (mod\ \frac{m_1}{d_1}), \\ \frac{a_2}{d_2} x \equiv \frac{b_2}{d_2} (mod\ \frac{m_2}{d_2}), \\ \dots \\ \frac{a_n}{d_n} x \equiv \frac{b_n}{d_n} (mod\ \frac{m_n)}{d_n}, \end{cases}$$

эквивалентную системе $\begin{cases} a_1 x \equiv b_1 (mod\ m_1), \\ a_2 x \equiv b_2 (mod\ m_2), \\ \dots \\ a_n x \equiv b_n (mod\ m_n). \end{cases}$

Сравнения этой системы можно решить относительно x и свести ее решение к решению системы:

$$\begin{cases} x \equiv \alpha_1\ (mod\ \frac{m_1}{d_1}), \\ x \equiv \alpha_2\ (mod\ \frac{m_2}{d_2}), \\ \dots \\ x \equiv \alpha_n\ (mod\ \frac{m_n}{d_n}). \end{cases}$$

Если в системе модули $m_1, m_2, \dots, m_n$ попарно просты, то решение ее можно находить не указанным выше общим способом, а по формуле $x_0 = \frac{M}{m_1} y_1 \alpha_1 + \dots + \frac{M}{m_n} y_n \alpha_n$,

где $M = [m_1, \dots, m_n]$ и $y_1, \dots, y_n$ есть решения сравнений

$$\frac{M}{m_i} y_i \equiv 1\ (mod\ m_i).$$

Решением системы будет $x \equiv x_0 (mod\ M)$.

Этим способом можно решать и последнюю систему, если модули $\frac{m_1}{d_1}, \dots, \frac{m_n}{d_n}$ попарно просты.

4.3. Число решений системы из двух сравнений

Теорема. *Пусть дана система сравнений вида*

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ x \equiv c_2 (mod\ m_2) \end{cases}$$

$M = НОК\ (m_1, m_2), d = НОД(m_1, m_2), (c_2 - c_1) \vdots d.$

Тогда система имеет одно решение, представляющее собой класс чисел по mod M.

Доказательство.

Из первого сравнения системы $x \equiv c_1 (mod\ m_1)$ получим равенство $x = c_1 + m_1 t$, где $t \in Z$. Поэтому надо выбрать такие числа $t \in Z$, при которых число x удовлетворяет второму сравнению системы $x \equiv c_2 (mod\ m_2)$, то есть $c_1 + m_1 t \equiv c_2 (mod\ m_2)$. Отсюда

$$m_1 t \equiv c_2 c_1 (mod\ m_2).$$

Получили сравнение первой степени.

1) Если $НОД(m_1, m_2) = d, d > 1$ и $(c_2 - c_1)$ не делится на d, то это сравнение не имеет решений.
2) Если $НОД(m_1, m_2) = 1$, то сравнение имеет одно решение $t \equiv \alpha (mod\ m_2)$.

Так как d=1, то $M = m_1 \cdot m_2$ и $(c_2 - c_1) \vdots 1$, тогда из сравнения $x = c_1 + m_1 t$ найдем x, подставив вместо t: $t = \alpha + m_2 \cdot k, k \in \mathrm{Z}$.

Получим, что $x = c_1 + m_1(\alpha + m_2 \cdot k) = (c_1 + m_1\alpha) + m_1 m_2 k$, следовательно, $x = \delta + Mk$, где $\delta = c_1 + m_1\alpha$. Поэтому $x \equiv \delta \ (mod\ M)$ – решение системы.

3) Если НОД$(m_1, m_2) = d$, $d > 1$ и $(c_2 - c_1) \ \vdots \ d$, то это сравнение имеет d решений.

$t \equiv \beta \ (mod\ m_2)$,

$t \equiv \beta + \frac{m_2}{d} (mod\ m_2)$,

…

$t \equiv \beta + (d-1)\frac{m_2}{d} (mod\ m_2)$,

Которые образуют один класс вычетов по $mod \frac{m_2}{d}$, содержащий числом β. Отсюда получим $t = \beta + \frac{m_2}{d} s$, где $s \in \mathrm{Z}$.

Подставив данное равенство в равенство $x = c_1 + m_1 t$, получим, что

$$x = c_1 + m_1 \left(\beta + \frac{m_2}{d} s\right) = (c_1 + m_1\beta) + \frac{m_1 m_2}{d} s.$$

Так как по свойству для НОК двух чисел имеет место равенство $Md = m_1 m_2$, то $M = \frac{m_1 m_2}{d} s$, поэтому

$x = \gamma + Ms$, где $\gamma = c_1 + \beta m_1$.

Отсюда получаем, что $x \equiv \gamma \ (mod\ M)$ – решение системы. ■

Пример 1. Решить систему сравнений $\begin{cases} x \equiv 9 \ (mod\ 34), \\ x \equiv 4 \ (mod\ 19). \end{cases}$

НОД(34, 19)=1, 9-4=5, $5 \vdots 1$, следовательно, система имеет одно решение по модулю М=НОК (34, 19)=646.

$x \equiv 9 \ (mod\ 34)$, значит $x = 9 + 34t, t \in \mathrm{Z}$,

$9 + 34t \equiv 4 \ (mod\ 19)$, $34t \equiv -5 \ (mod\ 19)$,

$15t \equiv -5 \ (mod\ 19)$, $3t \equiv -1 \ (mod\ 19)$,

методом преобразования коэффициентов

$3t \equiv -1 + 19 (mod\ 19)$, $3t \equiv 18 (mod\ 19)$,

$t \equiv 6 \ (mod\ 19)$, потому $t = 6 + 19s, s \in \mathrm{Z}$,

$x = 9 + 34\ (6 + 19s) = 213 + 646s$,

$x \equiv 213 \ (mod\ 646)$ – решение системы сравнений.

Пример 2. Решить систему сравнений $\begin{cases} x \equiv 29 \ (mod\ 63), \\ x \equiv 9 \ (mod\ 35). \end{cases}$

НОД (63, 35) =7, 7>1, 29-9=20, 20 не делится на 7, следовательно, система не имеет решений.

4.4. Число решений системы из нескольких сравнений

Теорема. *Пусть дана система сравнений вида*

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_n (mod\ m_n), \end{cases}$$

где $m_1, m_2, \dots, m_n \in \mathrm{N}$, $c_1, c_2, \dots, c_n \in \mathrm{Z}$, $n \in \mathrm{N}$. *Тогда система или не имеет решений, или имеет одно решение.*

Доказательство.

Метод математической индукции. По определению решения системы сравнений найдем класс вычетов по mod M, где $M = HOK\ (m_1, \dots, m_n)$.

1) При n=1 система состоит из одного сравнения и утверждение верно.
2) При n=2 утверждение теоремы доказано в предыдущем пункте.
3) Предположим, что утверждение верно при n=k ($k \in \mathrm{N}, \mathrm{k} > 2$), то есть система сравнений

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_k (mod\ m_k) \end{cases}$$

или не имеет решений, или имеет одно решение по модулю M, где $M = HOK\,(m_1, \dots, m_k)$, и докажем, что тогда утверждение теоремы верно и при n=k+1, то есть система сравнений

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_k (mod\ m_k), \\ x \equiv c_{k+1} (mod\ m_{k+1}) \end{cases}$$

или не имеет решений, или имеет одно решение по модулю

$$M_1 = HOK\,(m_1, \dots, m_k, m_{k+1}).$$

По свойству *НОК*а имеем

$$HOK\,(m_1, \dots, m_k, m_{k+1}) = \text{НОК}(HOK\,(m_1, \dots, m_k), m_{k+1}),$$

поэтому

$$M_1 = \text{НОК}\,(M, m_{k+1}).$$

а) Если система $\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_k (mod\ m_k) \end{cases}$ не имеет решений, то система

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_k (mod\ m_k), \\ x \equiv c_{k+1} (mod\ m_{k+1}) \end{cases}$$

не имеет решений, следовательно, утверждение доказано.

б) Если система $\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_k (mod\ m_k) \end{cases}$ имеет решение $\bar{\alpha}$ по mod M, то $x \equiv \alpha\ (mod\ M)$ $(\alpha \in \bar{\alpha})$.

В этом случае система эквивалентна системе

$$\begin{cases} x \equiv \alpha (mod\ M), \\ x \equiv c_{k+1} (mod\ m_{k+1}) \end{cases}.$$

НОД $(M, m_{k+1}) = d$. Если $(c_{k+1} - \alpha)$ не делится на d, то данная система не имеет решения. Если $(c_{k+1} - \alpha) \vdots d$, то система имеет одно решение по модулю НОЛ (M, m_{k+1}), то есть, в силу того, что $M_1 = HOK\ (m_1, \dots, m_k, m_{k+1})$, по модулю M_1, поэтому утверждение доказано.

4) На основании принципа математической индукции получим, что утверждение верно для любого натурального числа n. ■

Если система сравнений совместна, то можно решить сначала систему из двух сравнений системы, а затем добавить третье сравнение и так далее.

Пример. Решить систему сравнений

$$\begin{cases} x \equiv 6\ (mod\ 17), \\ x \equiv 4\ (mod\ 11), \\ x \equiv -3\ (mod\ 8). \end{cases}$$

Решение.

$x \equiv 6\ (mod\ 17)$, значит $x = 6 + 17t, t \in Z$,

$6 + 17t \equiv 4\ (mod\ 11)$,

$17t \equiv -2\ (mod\ 11)$, НОД $(17,11) = 1$, значит одно решение,

$6t \equiv -2\ (mod\ 11)$,

$3t \equiv -1\ (mod\ 11)$,

$3t \equiv -1 + 11\ (mod\ 11)$,

$t \equiv -4\ (mod\ 11)$, следовательно, $t = -4 + 11k, k \in Z$,

$x = 6 + 17t = 6 + 17\ (-4 + 11k) = -62 + 187k, k \in Z$,

$$x \equiv -62\ (mod\ 187),$$

следовательно, получим систему:

$$\begin{cases} x \equiv -62\ (mod\ 187), \\ x \equiv -3\ (mod\ 8). \end{cases}$$

$-62 + 187k \equiv -3\ (mod\ 8)$,

$187k \equiv 59\ (mod\ 8)$,

заменим остатками от деления на 8.

$3k \equiv 3\ (mod\ 8)$,

$k \equiv 1\ (mod\ 8)$,

следовательно, $k = 1 + 8s, s \in Z$,

$x \equiv 125\ (mod\ 1496)$,

$\overline{125}\ mod\ 1496$ – решение системы.

4.5. Единственность решения системы сравнений. Китайская теорема об остатках

Теорема. *Пусть дана система сравнений вида*

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_n (mod\ m_n), \end{cases}$$

где $c_1, c_2, \dots, c_n \in \mathrm{Z}$, $m_1, m_2, \dots, m_n \in \mathrm{N}$, *причем* $m_1, m_2, \dots, m_n$ *- попарно взаимно простые числа. Тогда система совместна и имеет одно решение, представляющий класс вычетов по модулю* $M = m_1, m_2 \dots m_n$.

Доказательство.

1) При n=1 система состоит из одного сравнения и утверждение верно.
2) При n=2 утверждение теоремы доказано в предыдущем пункте.
3) Предположим, что утверждение верно при $n=k$ ($k \in \mathrm{N}, \mathrm{k} > 2$), то есть система сравнений

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_k (mod\ m_k) \end{cases}$$

из k сравнений, где $m_1, m_2, \dots, m_k$ - попарно взаимно простые числа, совместна и имеет одно решение по модулю или не имеет решений, или имеет одно решение по модулю $M = m_1 m_2 \dots m_k$.

Докажем, что тогда утверждение теоремы верно и при $n=k+1$, то есть система

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_n (mod\ m_n), \end{cases}$$

из $(k+1)$ сравнений, где $m_1, m_2, \dots, m_k, m_{k+1}$ - попарно взаимно простые числа, совместна и имеет одно решение по модулю $M_1 = m_1, m_2 \dots m_k m_{k+1}$.

Доказательство проводится аналогично пункту 2) доказательства предыдущей теоремы. В результате приходим к системе сравнений вида.

$$\begin{cases} x \equiv \beta (mod\ M), \ \ M = m_1 m_2 \dots m_k, \\ x \equiv c_{k+1} (mod\ m_{k+1}). \end{cases}$$

Но m_{k+1} – взаимно простое с каждым из чисел $m_1, m_2, \dots, m_k$, следовательно, m_{k+1} будет взаимно простым с их произведением, то есть НОД $(M, m_{k+1}) = 1$. А поэтому исходная система совместна и имеет одно решение – класс вычетов по модулю $M_1 = M \cdot m_{k+1}$.

Таким образом, утверждение пункта 2) доказано.

4) На основании принципа математической индукции получим, что утверждение верно для любого натурального числа n. ■

Пример. Решить систему сравнений

$$\begin{cases} x \equiv 2 \ (mod\ 7), \\ x \equiv 5 \ (mod\ 9), \\ x \equiv 11 \ (mod\ 15). \end{cases}$$

НОД(7,9)=1б НОД (5,9)=3, $3 \neq 1$, следовательно, доказанную теорему нельзя применить.

В этом случае по теореме предыдущего пункта получим, что данная система или не имеет решения, или имеет одно решение.

Китайская теорема об остатках в её арифметической формулировке была описана в трактате китайского математика Сунь Цзы «Сунь Цзы Суань Цзин», предположительно датируемом третьим веком н.э. и затем была обобщена Цинь Цзюшао в его книге «Математические рассуждения в 9 главах», датируемой 1247 годом, где было приведено точное решение.

На практике китайская теорема об остатках позволяет работать не с длинными числами, а с наборами их коротких по длине остатков, поскольку устанавливает взаимно однозначное соответствие между числом и множеством его остатков, определяемым набором взаимно простых чисел. Если в качестве базиса взять, к примеру, первые 500 простых чисел, длина каждого из которых не превосходит 12 бит, то этого хватит для представления десятичных чисел длиной до 1500 знаков.

Китайская теорема об остатках. *Пусть дана система*

$$\begin{cases} x \equiv c_1 (mod\ m_1), \\ \dots \\ x \equiv c_n (mod\ m_n), \end{cases}$$

где $m_1 m_2 \dots m_n$ *– попарно простые числа,* $M = m_1 m_2 \dots m_n$ *и числа* $y_1, y_2, \dots, y_n$ *подобраны так, что*

$$\begin{cases} \frac{M}{m_1} y_1 \equiv 1\ (mod\ m_1), \\ \frac{M}{m_2} y_2 \equiv 1\ (mod\ m_2), \\ \dots \\ \frac{M}{m_n} y_n \equiv 1\ (mod\ m_n), \end{cases}$$

и пусть число C *определено равенством*

$$C = \frac{M}{m_1} y_1 c_1 + \dots + \frac{M}{m_n} y_n c_n.$$

тогда класс вычетов $\bar{C}$ *по mod* M *является решением системы.*

Доказательство.

Так как $M = m_1 m_2 \dots m_n$, то $\frac{M}{m_2} \vdots m_1, \dots, \frac{M}{m_n} \vdots m_1$, следовательно,

$$\frac{M}{m_1} y_1 c_1 + \dots + \frac{M}{m_n} y_n c_n \equiv \frac{M}{m_1} y_1 c_1\ (mod\ m_1)\ .$$

Отсюда получим, что $C \equiv c_1 (mod\ m_1)$.Аналогично получим, что $\equiv c_2 (mod\ m_2), \dots, C \equiv c_n (mod\ m_n)$.Таким образом, число C удовлетворяет всем сравнениям исходной системы. ■

Пример. Решить систему сравнений:

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 3) \\ x \equiv 2 (\mathrm{mod}\, 4) \\ x \equiv 3 (\mathrm{mod}\, 5) \end{cases}$$

Решение.

Заметим, что модули попарно взаимно простые, следовательно, можно применить китайскую теорему об остатках.

Вычислим параметры, необходимые для нахождения решения и составим таблицу, в которой $M_i = \frac{M}{m_i}$, $M_i' = y_i$.

$$\begin{cases} 4 \cdot 5 \cdot y_1 \equiv 1\ (mod\ 3), \\ 3 \cdot 5 \cdot y_2 \equiv 1\ (mod\ 4), \\ 3 \cdot 4 \cdot y_3 \equiv 1\ (mod\ 5), \end{cases} \begin{cases} 20 \cdot y_1 \equiv 1\ (mod\ 3), \\ 15 \cdot y_2 \equiv 1\ (mod\ 4), \\ 12 \cdot y_3 \equiv 1\ (mod\ 5). \end{cases}$$

Решим каждое сравнение системы.

1) $20 \cdot y_1 \equiv 1\ (mod\ 3)$,
   $2 \cdot y_1 \equiv 1\ (mod\ 3)$,
   $2 \cdot y_1 \equiv 1 + 3\ (mod\ 3)$,
   $y_1 \equiv 2\ (mod\ 3)$.

Выберем $y_1 = 2$.

2) $15 \cdot y_2 \equiv 1\ (mod\ 4)$,
   $3 \cdot y_2 \equiv 1\ (mod\ 4)$,
   $3 \cdot y_2 \equiv 1 + 4 \cdot 2\ (mod\ 4)$,
   $y_2 \equiv 3\ (mod\ 3)$.

Выберем $y_2 = 3$.

3) $12 \cdot y_3 \equiv 1\ (mod\ 5)$,

$2 \cdot y_3 \equiv 1\ (mod\ 5)$,

$2 \cdot y_3 \equiv 1 + 5\ (mod\ 5)$,

$y_3 \equiv 3\ (mod\ 3)$.

Выберем $y_3 = 3$.

$M_1' = y_1 = 2, M_2' = y_2 = 3, M_3' = y_3 = 3$.

m_i	3	4	5
M_i	20	15	12
M_i'	2	3	3
c_i	1	2	3

Согласно китайской теореме об остатках, решением будет являться

$x_0 \equiv 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 (\text{mod } 60) \equiv 40 + 90 + 108 (\text{mod } 60) \equiv 58 (\text{mod } 60)$.

Ответ: $x \equiv 58 (\text{mod } 60)$.

Пример. Решить систему сравнений:

$$\begin{cases} x \equiv 1 (\text{mod } 4) \\ x \equiv 3 (\text{mod } 5) \\ x \equiv 2 (\text{mod } 7) \end{cases}$$

Заметим, что модули попарно взаимно простые, следовательно, можно применить китайскую теорему об остатках.

Вычислим параметры, необходимые для нахождения решения и составим таблицу, в которой $M_i = \frac{M}{m_i}$, $M_i' = y_i$.

$$\begin{cases} 5 \cdot 7 \cdot y_1 \equiv 1 \ (mod\ 4), \\ 4 \cdot 7 \cdot y_2 \equiv 1 \ (mod\ 5), \\ 4 \cdot 5 \cdot y_3 \equiv 1 \ (mod\ 7), \end{cases} \begin{cases} 35 \cdot y_1 \equiv 1 \ (mod\ 4), \\ 28 \cdot y_2 \equiv 1 \ (mod\ 5), \\ 20 \cdot y_3 \equiv 1 \ (mod\ 7). \end{cases}$$

Решим каждое сравнение системы.

4) $35 \cdot y_1 \equiv 1 \ (mod\ 4)$,
$3 \cdot y_1 \equiv 1 \ (mod\ 4)$,
$3 \cdot y_1 \equiv 1 + 4 \cdot 2 \ (mod\ 4)$,
$y_1 \equiv 3 \ (mod\ 3)$.

Выберем $y_1 = 2$.

5) $28 \cdot y_2 \equiv 1 \ (mod\ 5)$,
$3 \cdot y_2 \equiv 1 \ (mod\ 5)$,
$3 \cdot y_2 \equiv 1 + 5 \ (mod\ 5)$,
$y_2 \equiv 2 \ (mod\ 3)$.

Выберем $y_2 = 2$.

6) $20 \cdot y_3 \equiv 1 \ (mod\ 7)$,
$6 \cdot y_3 \equiv 1 \ (mod\ 7)$,
$6 \cdot y_3 \equiv 1 + 7 \cdot 5 \ (mod\ 7)$,
$y_3 \equiv 6 \ (mod\ 3)$.

Выберем $y_3 = 3$.

$M_1' = y_1 = 3, M_2' = y_2 = 2, M_3' = y_3 = 6.$

$M_1' = y_1 = 3, M_2' = y_2 = 2, M_3' = y_3 = 6.$

m_i	4	5	7
M_i	35	28	20
M_i'	3	2	6
c_i	1	3	2

Согласно китайской теореме об остатках, решением будет являться

$x_0 = 35 \cdot 3 \cdot 1 + 28 \cdot 2 \cdot 3 + 20 \cdot 6 \cdot 2 = 513.$

$x \equiv 513 (\text{mod } 140) \equiv 93 (\text{mod } 140.$

Ответ: $x \equiv 93 (\text{mod } 140)$.

Заметим, что если дана система сравнений вида

$$\begin{cases} a_1 x \equiv b_1 \ (mod\ m_1), \\ \quad \ldots \\ a_n x \equiv b_n \ (mod\ m_n), \end{cases}$$

то

1) если НОД $(a_i, m_i) = d_i$, $d_i > 1, d_i \nmid b_i$ в i - сравнении, то i – сравнение не имеет решение, следовательно, система несовместна.

2) если НОД $(a_i, m_i) = d_i$, $d_i > 1$, $b_i \vdots d_i$, то г
обеих частей сравнения и модуля получим

$$\begin{cases} x \equiv c_1 \left(mod\ \frac{m_1}{d_1}\right), \\ \dots \\ x \equiv c_n \left(mod\ \frac{m_n}{d_n}\right). \end{cases}$$

Полученная система или не имеет решение,
шение, которым является класс вычетов по модулю

$$M = HOK\left(\frac{m_1}{d_1}, \dots, \frac{m_n}{d_n}\right).$$

Пример. Решить систему сравнений.

$$\begin{cases} 7x \equiv 3\ (mod\ 11), \\ 15x \equiv 5\ (mod\ 35), \\ 3x \equiv 2\ (mod\ 5). \end{cases}$$

Посвящение в тайну

Бенджамен Франклин (Franklin) однажды сказал: «Трое могут хранить тайну, если двое из них мертвы.» В этом параграфе мы изучаем безопасную систему допуска живых к секретным сведениям, основанную на китайской теореме об остатках. Представьте себе следующую ситуацию. Подвал банка должен открываться каждый день. В банке служат пять старших кассиров, имеющих доступ к подвалу. По причинам безопасности руководство банка предпочитает систему, требующую присутствия хотя бы двух из этой пятерки для возможности открыть подвал. Проблема в том, чтобы подвал могли открыть *любые* два старших кассира.

Рассмотрим эту проблему в более общем виде. Для того, чтобы открыть подвал банка, необходимо знать код, который можно считать натуральным числом s. Мы хотим распределить этот код между n старшими кассирами так, чтобы каждый из них знал что-то об s. Назовем такую частичную информацию *фрагментом* кода. Более того, открыть подвал должно быть невозможно, если в банке присутствуют менее k старших кассиров, где $k \geqslant 2$ — натуральное число, меньшее n.

Мы добьемся этого условия, распределив информацию о коде таким образом, что

- число s *легко* определяется, если известно k или более фрагментов;
- число s *трудно* определимо, если известно менее k фрагментов.

Фрагменты кода, сообщаемые каждому из старших кассиров, — это, в действительности, элементы множества $\mathbb{S}$, состоящего из n упорядоченных пар натуральных чисел. Чтобы построить $\mathbb{S}$, выберем сначала множество $\mathcal{L}$ из n попарно взаимно простых чисел. Пусть N — произведение наименьших k из них, а M — произведение $k-1$ наибольших. Будем говорить, что k является *порогом для* $\mathcal{L}$, если $M < N$. Из этого условия следует, что произведение любых k (или более) элементов из $\mathcal{L}$ всегда больше, чем N, а произведение $k-1$ (или менее) его элементов — всегда меньше M.

Предположим, код s выбран так, что $M < s < N$, а множество $\mathbb{S}$ состоит из пар (m, s_m), где $m \in \mathcal{L}$, а s_m — вычет числа s по модулю m. Эти пары и являются теми *фрагментами кода*,

которые сообщаются старшим кассирам. Тот факт, что множество $\mathfrak{L}$ имеет порог $k \geqslant 2$, обеспечивает неравенство $s > m$ для каждого $m \in \mathfrak{L}$. В частности, $s_m < s$ для любого $m \in \mathfrak{L}$.

Что произойдет, если k или более старших кассиров находятся в банке? В этом случае известны t $(\geqslant k)$ пар из множества $\mathbb{S}$. Обозначив эти пары через $(m_1, s_1), \ldots, (m_t, s_t)$, рассмотрим систему сравнений:

$$\begin{cases} x \equiv s_1 \pmod{m_1}, \\ x \equiv s_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv s_t \pmod{m_t}. \end{cases}$$

Элементы множества $\mathfrak{L}$ попарно взаимно просты. Значит, по китайской теореме об остатках, эта система имеет решение $0 \leqslant x_0 < m_1 \cdots m_t$. Но совпадает ли x_0 с s? Это как раз та причина, по которой мы накладывали требование: $\mathfrak{L}$ имеет порог k. Поскольку $t \geqslant k$, то наше требование влечет:

$$m_1 \cdots m_t \geqslant N > s.$$

Но s тоже удовлетворяет системе, и по китайской теореме об остатках

$$x_0 \equiv s \pmod{m_1 \cdots m_t}.$$

А так как s и x_0 — натуральные числа, меньшие $m_1 \cdots m_t$, то $s = x_0$.

Предположим теперь, что в банке находится менее k старших кассиров. Несмотря на то, что t теперь меньше k, мы все равно сможем решить систему. Пусть x_0 — наименьшее неотрицательное решение, тогда $0 \leqslant x_0 < m_1 \cdots m_t$. Но произведение меньшего, чем k количества элементов из $\mathfrak{L}$ всегда меньше M; так что $x_0 < M < s$. Следовательно, решения системы не достаточно для восстановления кода s. Однако как x_0, так и s — решения системы, поэтому

$$s = x_0 + y \cdot (m_1 \cdots m_t),$$

где y — некоторое натуральное число. Неравенство

$$N > s > M > x_0$$

влечет

$$\frac{M - x_0}{m_1 \cdots m_t} \leqslant y \leqslant \frac{s - x_0}{m_1 \cdots m_t} \leqslant \frac{N - x_0}{m_1 \cdots m_t}.$$

Приходим к выводу: если $t < k$, то для восстановления кода s нам предстоит отыскивать недостающий множитель y среди более чем

$$d = \left[\frac{N - M}{M}\right]$$

целых чисел. Выбрав модули так, чтобы d оказалось очень большим, мы сделаем задачу поиска y практически нерешаемой.

Для завершения разбора задачи осталось осветить один вопрос: можно ли найти множество $\mathcal{L}$, удовлетворяющее всем необходимым требованиям? Ответ на него положителен, но нуждается в результатах о распределении простых чисел, которые выходят за рамки данной книги.

Сделаем обзор рассмотренной конструкции. Для нее требуются начальные данные: число n старших кассиров, имеющих доступ в подвал банка, и наименьшее число k из них, присутствие которых в банке достаточно для открытия подвала. Первое число определяет размер множества $\mathcal{L}$, а второе — его порог k. Далее нам нужно подобрать множество $\mathcal{L}$ из n элементов с порогом k (эту часть конструкции мы подробно не обсуждали), и вычислить M и N, определенные выше. Напомним,

что $\mathfrak{L}$ нужно выбирать с таким расчетом, чтобы число d, о котором мы говорили, было как можно больше; в противном случае код может быть разгадан простым перебором. Код s — натуральное число, которое выбирается лежащим между M и N. Теперь можно вычислить элементы множества $\mathbb{S}$ и сообщить их сотрудникам. Конечно, безопасность этой схемы зависит от того, насколько велико k, уменьшающее вероятность, что одновременно k кассиров из одного банка окажутся нечестными. Если это все-таки произойдет, то нам придется утешать себя мыслью, что не существует систем безопасности 100-процентной надежности.

Рассмотрим пример. Допустим, что в банке работают 5 старших кассиров и из соображений безопасности по крайней мере двое из них должны присутствовать при открытии подвала. Значит, $\mathfrak{L}$ должно состоять из пяти элементов, а его порог равен 2. Выбрав элементы $\mathfrak{L}$ среди малых простых чисел, получим:

$$\mathfrak{L} = \{11,\ 13,\ 17,\ 19,\ 23\}.$$

Произведение двух наименьших чисел этого множества равно $N = 11 \cdot 13 = 143$. С другой стороны, поскольку $k = 2$, произведение $k - 1$ наибольших простых из $\mathfrak{L}$ в действительности равно его максимальному элементу. Таким образом, $M = 23$ и $\mathfrak{L}$ имеет порог 2. Код s может быть любым целым числом, лежащим между 23 и 143. Пусть $s = 30$. Тогда

$$\mathbb{S} = \big\{(11,19),(13,17),(17,13),(19,11),(23,7)\big\}.$$

Наконец, что будет, если в банке присутствуют старшие кассиры с фрагментами (17,13) и (23,7)? Код из их фрагментов получается как наименьшее число, удовлетворяющее системе:

$$\begin{cases} x \equiv 13 \pmod{17}, \\ x \equiv 7 \pmod{23}. \end{cases}$$

Легко увидеть, что таким числом будет 30. Этот код корректен, он позволяет открыть подвал.

Упражнения

1. Решить системы сравнений:

a) $\begin{cases} x \equiv 3 \pmod 7, \\ x \equiv 5 \pmod 9; \end{cases}$

b) $\begin{cases} x \equiv 6 \pmod 9, \\ x \equiv 9 \pmod{12}; \end{cases}$

c) $\begin{cases} 7x \equiv 10 \pmod{11}, \\ 5x \equiv 3 \pmod 6; \end{cases}$

d) $\begin{cases} x \equiv 2 \pmod 8, \\ 3x \equiv 6 \pmod 9; \end{cases}$

e) $\begin{cases} 28x \equiv 40 \pmod{44}, \\ 2x \equiv 3 \pmod 5; \end{cases}$

f) $\begin{cases} x \equiv 7 \pmod{13}, \\ x \equiv 5 \pmod{10}, \\ x \equiv 2 \pmod 3; \end{cases}$

g) $\begin{cases} x \equiv 4 \pmod{15}, \\ x \equiv 1 \pmod{12}, \\ x \equiv 7 \pmod{14}; \end{cases}$

h) $\begin{cases} 9x \equiv 12 \pmod{21}, \\ 9x \equiv 2 \pmod{14}, \\ 2x \equiv 1 \pmod{11}; \end{cases}$

k) $\begin{cases} 2x \equiv 6 \pmod{12}, \\ 3x \equiv 5 \pmod{14}, \\ 12x \equiv 7 \pmod{13}; \end{cases}$

l) $\begin{cases} 5x \equiv 200 \pmod{251}, \\ 11x \equiv 192 \pmod{401}, \\ 3x \equiv -1512 \pmod{9073}; \end{cases}$

$$\text{m)}\begin{cases} x \equiv 1 (\mathrm{mod}\, 25), \\ x \equiv 2 (\mathrm{mod}\, 4), \\ x \equiv 3 (\mathrm{mod}\, 7), \\ x \equiv 4 (\mathrm{mod}\, 9). \end{cases}$$

3. При каких значениях параметра a следующие системы сравнений совместны:

$$\text{a)}\begin{cases} x \equiv 5 (\mathrm{mod}\, 18), \\ x \equiv 8 (\mathrm{mod}\, 21), \\ x \equiv a (\mathrm{mod}\, 35); \end{cases}$$

$$\text{b)}\begin{cases} x \equiv 3 (\mathrm{mod}\, 11), \\ x \equiv 11 (\mathrm{mod}\, 20), \\ x \equiv 1 (\mathrm{mod}\, 15), \\ x \equiv a (\mathrm{mod}\, 18). \end{cases}$$

ГЛАВА 5. ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

5.1. Порядок числа и класса вычетов по модулю

Пусть $a \in \mathrm{Z}, m \in \mathrm{N}$ и НОД(a, m)=1. Тогда по теореме Эйлера имеет место сравнение $a^{\varphi(m)} \equiv 1\ (mod\ m)$.

Например, $m = 20,\ \varphi(m) = \varphi(20) = \varphi(2^2 \cdot 5) = 8$. Так как $a = 3, \mathrm{НОД}\ (3, 20) = 1$, следовательно, $3^{\varphi(20)} \equiv 1\ (mod\ 20)$, то есть $3^8 \equiv 1\ (mod\ 20)$.

Вообще, $3^1 \equiv 3\ (mod\ 20)$, $3^2 \equiv 9\ (mod\ 20)$, $3^3 \equiv 7\ (mod\ 20)$, $3^4 \equiv 1\ (mod\ 20)$следовательно, число 4 - наименьший натуральный показатель d, для которого $3^d \equiv 1\ (mod\ 20)$.

Определение. *Порядком числа a по натуральному модулю m, где НОД(a,m) = 1, называется наименьшее натуральное число d, такое, что*

$$a^d \equiv 1\ (mod\ m).$$

Все числа из класса вычетов $\bar{a}$ по mod m также имеют порядок d, поэтому число d называется еще и порядком класса вычетов по mod m.

Определение. *Порядком класса вычетов a по mod m, где НОД(a, m) = 1, называется наименьшее натуральное число d, такое, что* $a^d \equiv 1\ (mod\ m)$.

Обозначение: $d = O\ (a\ mod\ m)$. Например, $O\ (3\ mod\ 20) = 4$.

Заметим, что порядок *d* также еще называют показателем и обозначают $P_m(a)$. Например, $P_{20}(3) = 4$.

Свойства порядка классов вычетов

Пусть *m*- натуральное число и *a*- целое число и НОД (*a*, *m*)=1.

Свойство 1. *Если d - порядок класса вычетов a по mod m, где НОД (a,m) = 1, то числа* $a, a^2, a^3, \dots, a^d$ *попарно несравнимы по mod m.*

Доказательство. (От противного).

Предположим, что для чисел k и s, $k \neq s$, $k, s \in \{1, 2, \dots, d\}$ верно сравнение $a^k \equiv a^s\ (mod\ m)$. Пусть, для определенности, $k > s$, тогда $a^{k-s} \equiv 1\ (mod\ m)$, следовательно, существует натуральное число $k - s$, меньшее *d*, такое, что

$$a^{k-s} \equiv 1\ (mod\ m).$$

Получили противоречие, так как d - наименьшее натуральное число, для которого $a^d \equiv 1\ (mod\ m)$. Поэтому числа $a, a^2, a^3, \dots, a^d$ попарно несравнимы по mod m.

Свойство 2. *Если d - порядок класса вычетов a по mod m, где НОД(a,m) = 1, и n - целое неотрицательное число, то сравнение $a^n \equiv 1\ (mod\ m)$ верно тогда и только тогда, когда $n \vdots d$.*

Доказательство.

1) Пусть $a^n \equiv 1\ (mod\ m)$, докажем, что $n \vdots d$. По теореме о делении с остатком

$$\exists!\, q, r \in \mathbb{Z}, n = dq + r, 0 \le r < d.$$

Отсюда получим, что $a^n = a^{dq+r} = (a^d)^r \cdot a^r$, $a^n \equiv 1\ (mod\ m)$ следовательно,

$$(a^d)^q \cdot a^r \equiv 1\ (mod\ m).$$

Кроме того, так как d - порядок, то $a^d \equiv 1\ (mod\ m)$. Следовательно, из сравнения получим, что

$$a^r \equiv 1\ (mod\ m)$$

Но $0 \le r < d$, поэтому данное сравнение верно только при $r = 0$ (при

$r = 1, 2, \dots, d-1$ числа $a, a^2, a^3, \dots, a^{d-1}$несравнимы с 1 по mod m). Тогда получим при $r = 0$ равенство $n = dq$, а, значит, $n \vdots d$.

2) Пусть $n \vdots d$, докажем, что $a^n \equiv 1\ (mod\ m)$.Так как $n \vdots d$, то

$$\exists k \in \mathrm{Z}, n = dk.$$

Имеем, что $a^n = a^{dk} = (a^d)^k$. Но так же $a^d \equiv 1\ (mod\ m)$, следовательно, $(a^d)^k \equiv 1\ (mod\ m)$, поэтому и $a^n \equiv 1\ (mod\ m)$.

Свойство 3. *Если d - порядок класса вычетов a по mod m, где НОД(a,m) = 1, то* $\varphi(m) \vdots d$.

Доказательство.

Так как НОД(*a,m*)=1, то по теореме Эйлера $a^{\varphi(m)} \equiv 1\ (mod\ m)$. А так как число d - порядок и $\varphi(m)$ - натуральное число, то по свойству 2 получим, что $\varphi(m) \vdots d$.

Свойство 4. *Если d - порядок класса вычетов a по mod m, где НОД(a,m) = 1, то* $a^k \equiv a^s\ (mod\ m)$ *тогда и только тогда, когда* $k \equiv s\ (mod\ d)$.

Доказательство.

1) Пусть $a^k \equiv a^s\ (mod\ m)$, докажем, что $k \equiv s\ (mod\ d)$. Пусть для определенности $k > s$, тогда $a^{k-s} \equiv 1\ (mod\ m)$, (если $k < s$, то мож-

но по свойству симметричности отношения сравнимости записать, что $a^s \equiv a^k \ (mod\ m)$ и рассуждения будут аналогичными).

Следовательно, $(k-s) \vdots d$ (по свойству 2), поэтому $k \equiv s \ (mod\ d)$.

2) Пусть $k \equiv s \ (mod\ d)$, докажем, что $a^k \equiv a^s \ (mod\ m)$.Так как $k \equiv s \ (mod\ d)$, то $(k-s) \vdots d$, следовательно, $a^{k-s} \equiv 1 \ (mod\ m)$. Умножим почленно сравнение на a^s, тогда получим, что сравнение $a^k \equiv a^s \ (mod\ m)$.

Свойство 5. *Если* $a \equiv b \ (mod\ m)$, *и НОД(a,m) = НОД(b,m)* = 1, *то порядки классов вычетов a и b по mod m равны.*

Доказательство.

Обозначим через d_1 и d_2 соответственно порядки классов вычетов a и b по mod m. Имеем:

$$a^{d_1} \equiv 1 \ (mod\ m),\ b^{d_2} \equiv 1 \ (mod\ m),$$

и d_1, d_2 - наименьшие натуральные из возможных. Кроме того, по условию $a \equiv b \ (mod\ m)$, следовательно,

$$a^n \equiv b^n \ (mod\ m),$$

где n - натуральное число.

Отсюда, так как

$a^{d_1} \equiv 1\ (mod\ m)$, то $b^{d_1} \equiv 1\ (mod\ m)$,

то

$b^{d_2} \equiv 1\ (mod\ m)$, то $a^{d_2} \equiv 1\ (mod\ m)$.

Получим теперь, что $d_1 \vdots d_2$ и $d_2 \vdots d_1$. Но числа d_1 и d_2 - натуральные, поэтому $d_1 = d_2$.

5.2. Первообразные корни по модулю *m*

Определение. *Класс вычетов* $\bar{a}$ *по* $mod\ m$, *где* $a \in Z, m \in N$, НОД$(a, m) = 1$ *называется первообразным корнем по* $mod\ m$, *если порядок класса вычетов a по* $mod\ m$ *равен* $\varphi(m)$, *то есть* $d = O(a\ mod\ m) = \varphi(m)$.

Все числа из $\bar{a}$ также будут называться первообразными корнями.

Примеры. 1) $m = 12$, $\varphi(12) = \varphi(2^3 \cdot 3) = 4$.

$$\bar{1}, \bar{5}, \bar{7}, \overline{11}\ mod\ 12.$$

a) $\bar{a} = \bar{1}\ mod\ 12$, НОД $(1, 12) = 1$,

$1^1 \equiv 1\ (mod\ 12), d = 1, d \neq \varphi(12)$,

класс вычетов $\bar{1}$ не является первообразным корнем по $mod\ 12$.

b) $\bar{b} = \bar{5}\ mod\ 12$, НОД $(5, 12) = 1$,

$5^1 \equiv 5\ (mod\ 12)$,

$5^2 \equiv 1\ (mod\ 12)$, следовательно, $d = O(5\ mod\ 12) = 2$.

Поэтому $d \neq \varphi(12)$, значит, класс вычетов $\bar{5}$ не является первообразным корнем по $mod\ 12$.

c) $\bar{c} = \bar{7}\ mod\ 12$, НОД $(7, 12) = 1$,

$7^1 \equiv 7\ (mod\ 12)$,

$7^2 \equiv 1\ (mod\ 12)$, следовательно, $d = 2,\ d \neq \varphi(12)$,

тогда класс вычетов $\bar{7}$ не является первообразным корнем по $mod\ 12$.

d) $\bar{d} = \overline{11}\ mod\ 12$, НОД $(11, 12) = 1$,

$11^1 \equiv 11\ (mod\ 12)$,

$11^2 \equiv 1\ (mod\ 12)$, следовательно, $d = 2,\ d \neq \varphi(12)$,

следовательно, $\overline{11}$ не является первообразным корнем по $mod\ 12$.

Таким образом, по mod 12 не существует первообразных корней.

2) $m = 10$, $\varphi(10) = \varphi(2 \cdot 5) = 4$.

$\bar{1}, \bar{3}, \bar{7}, \bar{9}\ mod\ 10$.

a) $\bar{a} = \bar{1}\ mod\ 10$, НОД $(1, 10) = 1$,

$1^1 \equiv 1\ (mod\ 10), d = 1, d \neq \varphi(10)$,

класс вычетов $\bar{1}$ не является первообразным корнем по $mod\ 10$.

b) $\bar{b} = \bar{3}\ mod\ 10, \text{НОД}\ (3, 10) = 1,$

$3^1 \equiv 3\ (mod\ 10),$

$3^2 \equiv 9\ (mod\ 10),$

$3^3 \equiv 7\ (mod\ 10),$

$3^4 \equiv 1\ (mod\ 10)$, следовательно, $d = O(3\ mod\ 10) = 4.$

Поэтому $d = \varphi(10)$, значит, класс вычетов $\bar{3}$ является первообразным корнем по $mod\ 10$.

Так как $3^{\varphi(10)} \equiv 1\ (mod\ 10)$, то есть $3^4 \equiv 1\ (mod\ 10)$, то проверять надо было не все степени 1, 2, 3, 4, а только делители числа 4: 1, 2, 4, то есть $3^1, 3^2, 3^4$, а 3^3 не надо было рассматривать.

c) $\bar{c} = \bar{7}\ mod\ 10, \text{НОД}\ (7, 10) = 1,$

$7^1 \equiv 7\ (mod\ 10),$

$7^2 \equiv 9\ (mod\ 10)\ ,$

$7^4 \equiv 1\ (mod\ 10),$

следовательно, $d = 4,\ d = \varphi(10)$, тогда класс вычетов $\bar{7}$ является первообразным корнем по $mod\ 10$.

d) $\bar{d} = \bar{9}\ mod\ 10, НОД\ (9, 10) = 1,$

$9^1 \equiv 9\ (mod\ 10),$

$9^2 \equiv 1\ (mod\ 10), следовательно, d = 2,\ d \neq \varphi(10),$

следовательно, $\bar{9}$ не является первообразным корнем по $mod\ 10$.

Таким образом, по mod 12 не существует первообразных корней.

Заметим, что класс вычетов $\bar{1}$ не является первообразным корнем по любому натуральному модулю, большему 2.

Так как при НОД $(a,m) = 1$ будет верно сравнение $a^{\varphi(m)} \equiv 1\ (mod\ m)$ и $\varphi(m) \vdots d$, то чтобы убедиться, является ли $\bar{a}$ первообразным корнем, достаточно проверить, что $a^k \not\equiv 1\ (mod\ m)$ для $k|\varphi(m)$.

Пусть $m = p$, тогда $\varphi(m) = \varphi(p) = p - 1$. Следовательно, первообразных корнем по простому модулю p является класс вычетов $\bar{a}$, порядок которого равен $p - 1$.

Пример. $m = p = 11, \varphi(11) = 10, 10 \vdots 1, 2, 5, 10.$

Если $d = O(a\ mod\ 11) = 10$, то класс вычетов $\bar{a}$ будет первообразным корнем по $mod\ 11$.

$$\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, 6, \bar{7}, \bar{8}, \bar{9}, \overline{10}\ mod\ 11.$$

Класс вычетов $\bar{1}$ не является первообразным корнем по $mod\ 11$.

a) $\bar{b} = \bar{2}\ mod\ 11, \text{НОД}\ (2, 11) = 1,$

$2^1 \equiv 2\ (mod\ 11),$

$2^2 \equiv 4\ (mod\ 11),$

$2^5 \equiv 10\ (mod\ 11),$

$2^{10} \equiv 1\ (mod\ 11),$

следовательно, $d = O(2\ mod\ 11) = 10.$

Поэтому $d = \varphi(11)$, значит, класс вычетов $\bar{2}$ является первообразным корнем по $mod\ 11$.

b) $\bar{c} = \bar{3}\ mod\ 13, \text{НОД}\ (3, 11) = 1,$

$3^1 \equiv 1\ (mod\ 11),$

$3^2 \equiv 9\ (mod\ 11),$

$3^5 \equiv 1\ (mod\ 11),\ d = 5,\ d \neq \varphi(11),$

тогда класс вычетов $\bar{3}$ не является первообразным корнем по $mod\ 13$.

И так далее.

5.3. Первообразные корни по простому модулю

Исследуем вопрос: сколько существует первообразных, корней по простому модулю p.

Теорема. По *любому простому модулю p существует* $\varphi(p-1)$ *классов первообразных корней.*

Доказательство.

По определению первообразного корня надо вычислить количество s классов по модулю p, y которых порядок k равен $\varphi(p)$, то есть равен $p-1, k=p-1$. А так как порядок является делителем числа $p-1$, то тогда $s=\varphi(k)$. Следовательно, $s=\varphi(p-1)$. ■

Пример. $p=11$, $\varphi(11)=10, 10 \vdots 1, 2, 5, 10$.

Класс вычетов $\bar{2}$ является первообразным корнем по $mod\ 11$, так как $2^{10} \equiv 1\ (mod\ 11)$. Количество таких первообразных корней будет $\varphi(p-1)=\varphi(10)=4$. Следовательно, точно 4 класса будут первообразными корнями по $mod\ 11$.

Отметим, что:

1) Первообразные корни существуют для всякого простого модуля p, их будет в точности $\varphi(p-1)$ для данного p.

2) Первообразные корни существуют не для всякого модуля m, а только для модулей:

$$m = 2, m = 4, m = 2 \cdot p^{\alpha}, m = p^{\alpha},$$

где p – нечетное, α – натуральное число.

5.4. Первообразные корни по модулям p^{α} и $2p^{\alpha}$

Пусть $p > 2, \alpha \geq 1$. Докажем существование первообразного корня по $mod\ p^{\alpha}$ и $2p^{\alpha}$.

Теорема. *Пусть a, b, m, x - натуральные числа и порядок класса вычетов $\bar{x}$ по mod m равен ab. Тогда порядок класса вычетов $\overline{x^a}$ по mod m равен числу b.*

Доказательство.

Обозначим порядок класса вычетов $\overline{x^a}$ через k, k - наименьшее натуральное число, для которого $(x^a)^k \equiv 1\ (mod\ m)$. Тогда получим:

1) $(x^a)^k \equiv 1\ (mod\ m)$, отсюда $x^{ak} \equiv 1\ (mod\ m)$, следовательно, число ak делится на порядок класса вычетов $\bar{x}$, то есть на число ab. Но тогда $k \vdots b$.

2) По условию $x^{ab} \equiv 1\ (mod\ m)$, отсюда $(x^a)^b \equiv 1\ (mod\ m)$, следо-

вательно, число b делится на порядок класса вычетов $\overline{x^a}$, $b \vdots k$.

Таким образом, из 1) и 2) получим, что $k = b$. ■

Теорема. *Пусть a, b, m, x - натуральные числа, НОД(a, b) = 1 и порядок класса вычетов $\bar{x}$ по mod m равен a, а порядок класса вычетов $\bar{y}$ по mod m равен b. Тогда порядок класса вычетов $\overline{xy}$ по mod m равен ab.*

Доказательство.

Обозначим порядок класса вычетов $\overline{xy}$ по mod m через k, то есть k - наименьшее натуральное число, для которого $(xy)^k \equiv 1\ (mod\ m)$. Тогда, применяя свойства сравнений, получим, что

1) $((xy)^k)^b \equiv 1\ (mod\ m)$, отсюда $x^{kb}y^{kb} \equiv 1\ (mod\ m)$, следовательно, $x^{kb}(y^b)^k \equiv 1\ (mod\ m)$. А из этого сравнения, учитывая известные сведения для числа b из условия теоремы, получим теперь сравнение $x^{kb} \equiv 1\ (mod\ m)$. Но тогда $kb \vdots a$. И так как *НОД(a, b)* = 1, то получим, что $k \vdots a$.

Аналогично докажем, что $k \vdots b$. Учитывая теперь, что числа a и b являются взаимно простыми, приходим к выводу, что $k \vdots ab$.

2) Из условия получим $x^a \equiv 1\ (mod\ m)$, $y^a \equiv 1\ (mod\ m)$, отсюда

$x^{ab} \equiv 1\ (mod\ m)$, $y^{ab} \equiv 1\ (mod\ m)$, а потому, $(xy)^{ab} \equiv 1\ (mod\ m)$. Но тогда $(ab) \vdots k$. Таким образом, из 1) и 2) получим, что $k = ab$. ■

Теорема. *Существуют первообразные корни по mod p.*

Доказательство.

Пусть числа

$$\delta_1, \delta_2, \dots, \delta_{p-1}$$

являются порядками чисел 1, 2, ..., $(p - 1)$ или классов, содержащих эти числа соответственно по mod p, то есть это наименьшие натуральные числа, для которых

$$1^{\delta_1} \equiv 1\ (mod\ p),\ 2^{\delta_2} \equiv 1\ (mod\ p), \dots,\ (p-1)^{\delta_{p-1}} \equiv 1\ (mod\ p),$$

Пусть r - НОК этих порядков и $r = {q_1}^{\alpha_1} \dots {q_k}^{\alpha_k}$ - его каноническое разложение. Каждый множитель ${q_s}^{\alpha_s}$ этого разложения делит хотя бы одно число δ_i ряда, поэтому существует натуральное число a, такое, что $\delta_i = a{q_s}^{\alpha_s}$. Пусть ξ_j - одно из чисел ряда 1, 2, ... , $p - 1$, имеющих порядок δ_i.

Число $n_j = {\xi_j}^a$ имеет порядок ${q_s}^{\alpha_s}$, а произведение $g = \eta_1\eta_2 \dots \eta_k$ имеет порядок ${q_1}^{\alpha_1} \dots {q_k}^{\alpha_k} = \tau$, тогда, τ - делитель числа $p - 1$.

Но так как числа $\delta_1, \delta_2, \ldots, \delta_{p-1}$ делят τ, все 1, 2, ... , $p-1$ являются решениями сравнения $x^\tau \equiv 1\ (mod\ p)$ => $p-1 \leq \tau$ => $\tau = p-1$ и число g – первообразный корень и класс вычетов, содержащий это число, является первообразным корнем. ■

Теорема. *Пусть класс вычетов $\bar{g}$ по модулю p является первообразным корнем, $g \in \bar{g}$. Тогда можно указать целое число t с условием, что целое число u, определяемое равенством $(g+pt)^{p-1} = 1 + pu$, не делится на число p. Соответствующее число (а, значит, и класс вычетов $\overline{g+p}$) будет первообразным корнем по mod p^α при $\forall \alpha > 1$.*

Доказательство.

Так как класс вычетов $\bar{g}$ - первообразный корень по модулю p, то порядок класса вычетов $\bar{g}$ равен $\varphi(p)$, то есть для $g \in \bar{g}$ справедливо $g^{p-1} \equiv 1\ (mod\ p)$.

$$g^{p-1} = 1 + pk, k \in \mathrm{Z}\ (g+pt)^{p-1} = 1 + p(k + ug^{p-2} \cdot t + pT) =$$
$$= 1 + pu,$$

где $k, T, t \in \mathrm{Z}$, и одновременно с t, число u пробегает полную систему вычетов по модулю p. Следовательно, можно указать t с условием,

что u не делится на p. При таком t выводим

$$(g+pt)^{p(p-1)} = (g+pu)^p = 1 + p^2 u_2,$$

$$(g+pt)^{p^2(p-1)} = 1 + p^3 u_3,$$

$$(g+pt)^{p^{\alpha-1}(p-1)} = 1 + p^\alpha u_\alpha,$$

где все $u_2, u_3, \dots, u_\alpha$ также не делятся на p. Пусть $g+pt$ имеет порядок δ по mod p^α. Тогда $(g+pt)^\delta \equiv 1\ (mod\ p^\alpha)$, отсюда следует, в частности, $g^\delta \equiv 1\ (mod\ p),)$. Поэтому $\delta \vdots (p-1)$ и, будучи делителем числа $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, должно иметь вид $\delta = p^{r-1}(p-1)$, где r - одно из чисел 1, ..., α. А так как равенств выше показывают, что сравнение

$$(g+pt)^{p^{r-1}(p-1)} \equiv 1\ (mod\ p^\alpha)$$

верно при $r = \alpha$ и неверно при $r < \alpha$, то $\delta = p^{\alpha-1}(p-1) = \varphi(p^\alpha)$ и класс вычетов $\overline{g+p}$ - первообразный корень по модулю p^α. ■

Теорема. *Пусть $\alpha \geq 1$ и класс вычетов $\bar{g}$, а значит, и $g \in \bar{g}$ - первообразный корень по модулю p^α. Тогда нечетное g_0 из чисел g и $g + p^\alpha$ будет первообразным корнем по модулю $2p^\alpha$.*

Доказательство.

1) Если число $g \in \bar{g}$ - первообразный корень по модулю m, то оно имеет порядок $c = \varphi(m)$, следовательно, не удовлетворяет ни одному из сравнений теоремы.

2) Обратно, пусть число $g \in \bar{g}$ не удовлетворяет ни одному из сравнений теоремы. Если бы показатель δ, которому принадлежит число g, оказался $< c$, то, обозначая q один из простых делителей $\frac{c}{\delta}$, мы имели бы $\frac{c}{\delta} = qu, \frac{c}{q} = \delta u, g^{\frac{c}{q}} \equiv 1 \ (mod\ p)$, что противоречит нашему предположению. Таким образом, $\delta = c$ и число g (а, следовательно, $\bar{g}$) является первообразным корнем по модулю m. ■

Пример. 1) $m = 41, \varphi(41) = 40 = 2^3 \cdot 5, \frac{40}{5} = 8, \frac{40}{2} = 20$.

Поэтому для того, чтобы число g, не делящееся на 41, было первообразным корнем по mod 41, необходимо и достаточно, чтобы это число g не удовлетворяло ни одному из сравнений

$$g^8 \equiv 1 \ (mod\ 41), g^{20} \equiv 1 \ (mod\ 41).$$

Но проверяя числа 2, 3, 4, ... , находим (по mod 41)

$$2^8 \equiv 10, 3^8 \equiv 1, 4^8 \equiv 18\ , 5^8 \equiv 18, 6^8 \equiv 10,$$

$$2^{20} \equiv 1, 3^{20} \equiv 40, 4^{20} \equiv 1, 5^{20} \equiv 1, 6^{20} \equiv 40.$$

Таким образом, числа 2, 3, 4, 5 не являются первообразными корнями по модулю 11, так как каждое удовлетворяет, по крайней мере, одному из сравнений $g^8 \equiv 1\ (mod\ 41), g^{20} \equiv 1\ (mod\ 41)$. Число 6 – первообразный корень, так как оно не удовлетворяет ни одному из этих сравнений.

2) m=1681 = 41^2. Зная из 1), что 6 – первообразный корень по mod 41, находим $6^{40} = 1 + 41(3 + 41l)$,

$$(6 + 41t)^{40} = 1 + 41(3 + 41l - 6^{39}t + 41T) = 1 + 41u.$$

Чтобы u не делилось на 41, достаточно взять t = 0. Получаем $6 + 41 \cdot 0 = 6$, 6 – первообразный корень по mod 1681.

3) $m = 3362 = 2 \cdot 1681$.

Число 6 – первообразный корень по модулю 1681, тогда в качестве первообразный корень по mod $2 \cdot 1681$ можно взять нечетное из чисел 6, 6 + 1681, то есть число 1687. Таким образом, число 1687 - первообразный корень по mod 3362.

Замечание. В работе математика Мешковского К.А. «Добавления в теории сравнений» математически обоснован новый алгоритм нахождения первообразных корней. Определена вся совокупность

первообразных корней всех простых чисел Ферма

$$(2^{2^k}+1, k=0,1,2,3,4, p=3,5,17,257,65537).$$

5.5. Индексы по модулю *m*

Заметим, что если $log_a b = c$, то число c - показатель степени, в которую надо возвести число a, чтобы получить число b:

$$a^c = b, a^{log_a b} = b\ .$$

В записи $ind_a b = s$ число s есть порядок (показатель) числа a, сравнимого с b по модулю m. Читать: «индекс b по mod m и основанию a».

Определение. *Число s называется индексом b по mod m и основанию a, если $a^s \equiv b\ (mod\ m)$, где $a, b \in \mathrm{Z}, m \in \mathrm{N}$ и НОД(a,m) = НОД(b,m) = 1.*

Запись $s = ind_a b$ при фиксированном mod m или $s = ind\ b$, если основание a не меняется все время.

Если число $b_0 \in \bar{b}$, то $a^s \equiv b_0\ (mod\ m)$,, то есть $ind_a b$ является индексом и всех чисел из класса вычетов $\bar{b}$ по модулю m. Число можно называть и индексом класса вычетов b по модулю m.

Определение. *Число s называется индексом класса вычетов b по mod m и основание a, если по этому модулю $(\bar{a})^s = \bar{b}$.*

Пример. $m = 13$, $a = 2$, $b = 12$.

$$2^s \equiv 12\ (mod\ 13), s - ?$$

$s = 6, 2^6 \equiv 12\ (mod\ 13)$, следовательно, $6 = ind_2 12$. Поэтому для $\forall b_0 \in \bar{b}, b_0 \in \overline{12}$, то есть $b_0 \equiv 12\ (mod\ 13)$, будет $ind_2 b_0 = 6$.

$$2^1 \equiv 2\ (mod\ 13) \to 1 = ind_2 2,$$

$$2^{12} \equiv 1\ (mod\ 13) \to 12 = ind_2 1,$$

$$2^{13} \equiv 2\ (mod\ 13) \to 13 = ind_2 2,$$

Если класс вычетов $\bar{a}$, не является первообразным корнем, то индексы могут существовать не для всех классов вычетов $\bar{b}$, взаимно простых с модулем m.

Например, $m = 21$, $a = 5$, $b = 2$.

$5^s \equiv 2\ (mod\ 21)$, не существует s, то есть не существует $ind_5 2$.

Обозначим первообразный корень по mod m через $g \in \bar{g}$, тогда

$$g^{\varphi(m)} \equiv 1\ (mod\ m), d = O\ (g\ mod\ m) = \varphi(m).$$

5.6. Индексы по простому модулю

Пусть натуральный модуль $m = p$, где p - простое число. По простому модулю p всегда существуют первообразные корни g. $ind_g b$ есть число неотрицательное.

Для данного g можно получить таблицы индексов, при этом имеют место следующие *свойства*:

1) Если $a \equiv b \ (mod\ p)$, то $ind\ a \equiv ind\ b \ (mod\ p-1)$ и наоборот.
2) $ind\ (a \cdot b) \equiv inda + ind\ b \ (mod\ p-1)$.
3) $ind\ a^n \equiv n \cdot ind\ a \ (mod\ p-1)$.
4) $ind\ \frac{b}{a} \equiv ind\ b - ind\ a \ (mod\ p-1)$.

Но НОД(a, p) = НОД(b, p) = 1, то есть a, b, g не делятся на p. По модулю p существует бесконечное множество индексов для данного числа p, все они сравнимы по $mod\ (p-1)$, и в качестве индекса можно брать любой из них (обычно берут наименьший из них). Следовательно, индексы меньше $mod\ (p-1)$.

Таблицы индексов составляются аналогично таблицам логарифмов.

Пример. $p = 7, \varphi(7) = 6, g = 2, \text{НОД}\,(2,7) = 1$, делители 6: 1, 2, 3, 6.

$2^1 \equiv 2\ (mod\ 7), 2^2 \equiv 4\ (mod\ 7), 2^3 \equiv 1\ (mod\ 7), d = 3,$

$d \neq \varphi(7),\ g = 2$ не является первообразным корнем.

$g = 3, 3^1 \equiv 3\ (mod\ 7), 3^2 \equiv 2\ (mod\ 7), 3^3 \equiv -1\ (mod\ 7),$

$3^6 \equiv 1\ (mod\ 7),\ d = 6, d = \varphi(7),\ g = 3$ является первообразным корнем по модулю 7.

Итак, выберем $g = 3$.

$s = ind_3 1, 3^s \equiv 1\ (mod\ 7), s = 6, ind_3 1 = 6,$

$s = ind_3 2, 3^s \equiv 2\ (mod\ 7), s = 2, ind_3 2 = 2,$

$s = ind_3 3, 3^s \equiv 3\ (mod\ 7), s = 1, ind_3 3 = 1,$

$s = ind_3 4 = ind_3 2^2 = 2 \cdot ind_3 2 = 2 \cdot 2 = 4, ind_3 4 = 4,$

$s = ind_3 5, 3^s \equiv 5\ (mod\ 7), s = 5, ind_3 5 = 5,$

$s = ind_3 6 = ind_3 (2 \cdot 3) = ind_3 2 + ind_3 3 = 2 + 1 = 3, ind_3 6 = 3.$

Иногда вместо $p - 1$ берут 0, то есть полагают $ind_3 1 = 0$, а не $ind_3 1 = 6$, так как $3^s \equiv 1\ (mod\ 7)$ верно и при $s = 0$.

Следовательно, получим такую таблицу индексов по mod 7 при основании $g = 3$.

a	1	2	3	4	5	6
ind	6 или 0	2	1	4	5	3

5.7. Индексы по модулям $p^\alpha, 2p^\alpha$

Пусть $p > 2, \alpha \geq 1, m$ - одно из чисел p^α и $2p^\alpha$, $c = \varphi(m)$, число $g \in \bar{g}$ – первообразный корень по mod m.

Теорема. *Пусть число $g \in \bar{g}$ – первообразный корень по mod m и число γ пробегает наименьшие неотрицательные вычеты: $\gamma = 0, 1, \ldots, c-1$ по mod c. Тогда число g^γ пробегает приведенную систему вычетов по mod m.*

Доказательство.

Число g^γ пробегает с чисел, взаимно простых с m, не сравнимых по модулю m, поэтому значения его образуют приведенную систему вычетов по модулю m. ■

Если $(a, m) = 1$, то у первообразного корня - роль, аналогичная основанию логарифма.

Определение. *Если $a \equiv g^v \pmod m$ (считаем $v \geq 0$) то v называется индексом числа a по mod m при основании g и обо-*

значается символом $v = ind_g a$.

Всякое a, с условием *НОД*$(a, m) = 1$, имеет некоторый единственный ind, γ, среди чисел ряда $\gamma = 0, 1, \ldots, c-1$. Зная γ', можно указать все ind числа a - это будут все неотрицательные числа класса $\gamma \equiv \gamma' \ (mod\ c)$. Из определения следует, что числа c данным индексом γ образуют класс чисел по mod m.

Теорема. *Имеет место сравнение:*

$$ind\ ab \ldots l \equiv ind\ a + ind\ b + \cdots + ind\ l\ (mod\ c).$$

В частности, $ind\ a^n \equiv n \cdot ind\ a\ (mod\ c)$.

Доказательство.

По определению индекса

$$a \equiv g^{ind\ a}\ (mod\ m), b \equiv g^{ind\ b}\ (mod\ m), \ldots, l \equiv g^{ind\ l}\ (mod\ m).$$

Следовательно, по свойству сравнений,

$$ab \ldots l \equiv g^{ind\ a + ind\ b + \cdots + ind\ l}\ (mod\ m).$$

Таким образом, $ind\ a + ind\ b + \cdots + ind\ l$ - один из индексов произведения $(ab \ldots l)$. ■

На практике удобно пользоваться для каждого p (не слишком большого) таблицами индексов:

1) для нахождения индекса по числу,

2) числа по индексу.

Таблицы содержат наименьшие неотрицательные вычеты чисел (приведенная система) и их наименьших индексов (полная система) соответственно по модулям p и $c = \varphi(p) = p - 1$.

Пример. Построим указанные таблицы для модуля $p = 41$,

$p - 1 = 2^3 \cdot 5, g = 6$ – первообразный корень по модулю 41.

$6^0 \equiv 1$	$6^{10} \equiv 32$	$6^{20} \equiv 40$	$6^{30} \equiv 9$
$6^1 \equiv 6$	$6^{11} \equiv 28$	$6^{21} \equiv 35$	$6^{31} \equiv 13$
$6^2 \equiv 36$	$6^{12} \equiv 4$	$6^{22} \equiv 5$	$6^{32} \equiv 37$
$6^3 \equiv 11$	$6^{13} \equiv 24$	$6^{23} \equiv 30$	$6^{33} \equiv 17$
$6^4 \equiv 25$	$6^{14} \equiv 21$	$6^{24} \equiv 16$	$6^{34} \equiv 20$
$6^5 \equiv 27$	$6^{15} \equiv 3$	$6^{25} \equiv 14$	$6^{35} \equiv 38$
$6^6 \equiv 39$	$6^{16} \equiv 18$	$6^{26} \equiv 2$	$6^{36} \equiv 23$
$6^7 \equiv 29$	$6^{17} \equiv 26$	$6^{27} \equiv 12$	$6^{37} \equiv 15$
$6^8 \equiv 10$	$6^{18} \equiv 33$	$6^{28} \equiv 31$	$6^{38} \equiv 8$
$6^9 \equiv 19$	$6^{19} \equiv 34$	$6^{29} \equiv 22$	$6^{39} \equiv 7$

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

J	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	2
3	9	13	27	17	20	38	23	15	8	7

Номер строки - число десятков индекса, номер столбца - число единиц индекса, в поле - число.

Например, 1) $ind\ 25$, I таблица, строка 2, столбец 5 → 4. $ind\ 25 = 4$.

2) $ind\ x = 33$, I I таблица, строка 3, столбец 3 → 17. $ind\ 17 = 33$.

Отметим еще некоторые утверждения, которые следуют из изложенного выше.

Пусть $p > 2, \alpha \geq 1, m$ - одно из чисел p^α и $2p^\alpha$, $c = \varphi(m)$, НОД $(n, c) = d$, тогда:

1. Сравнение

$$x^n \equiv a \ (mod\ m), (a, m) = 1$$

разрешимо (и тем. самым число a есть вычет степени n по mod m) тогда и только тогда, когда $ind \vdots d$. В случае разрешимости сравнение имеет d решений.

2. В приведенной системе вычетов по mod m число вычетов степени n равно $\frac{c}{d}$.

Доказательство.

1. Сравнение $x^n \equiv a \ (mod\ m)$ равносильно сравнению

$$n\ ind\ x \equiv ind\ a \ (mod\ c),$$

которое разрешимо тогда и только тогда, когда $ind\ a \vdots d$. В случае разрешимости сравнения найдем d несравнимых по mod c значений для $ind\ x$, им отвечают d несравнимых (mod m) значений для x. Утверждение 1) доказано.

2. Среди чисел $0, 1, \ldots, c-1$, являющихся наименьшими ин-

дексами вычетов приведенной системы по mod m, имеется $\frac{c}{d}$ чисел, кратных d. ■

Примеры. 1) Для сравнения $x^8 \equiv 23\ (mod\ 41)$ имеем НОД(8, 40) = 8, ind 23=36, которое не делится на 8 => сравнение не разрешимо.

2) $x^{12} \equiv 37\ (mod\ 41)$. НОД(12, 40)=4, $ind\ 37 = 32 \vdots 4$ => сравнение разрешимо, имеет 4 решения.

$$12\ ind\ x \equiv 32\ (mod\ 40),$$

$$3\ ind\ x \equiv 8\ (mod\ 10),$$

$$3\ ind\ x \equiv 8 + 10\ (mod\ 10),$$

$$ind\ x \equiv 6\ (mod\ 10),$$

$$ind\ x = 6, 16, 26, 36.$$

Итак, $x \equiv 39, 18, 2, 23\ (mod\ 41)$ - решения сравнения.

3) Числа

$$1, 4, 10, 16, 18, 23, 25, 31, 37, 40,$$

индексы которых делятся на 4, есть биквадратичные вычеты (или также все вычеты любой степени $n = 4, 12, 28, ...$, где НОД(4,40) = 4, имеющиеся среди наименьших положительных вычетов по mod 41.

Число чисел ряда равно $10 = \frac{40}{4}$.

3. Число a есть вычет степени n по mod m тогда и только тогда, когда

$$a^{\frac{c}{d}} \equiv 1 \ (mod\ m).$$

Доказательство.

Сравнение $ind\ a \equiv 0 \ (mod\ d)$, эквивалентно другому сравнению $\frac{c}{d} ind\ a \equiv 0 \ (mod\ c)$, из которого получаем, что $a^{\frac{c}{d}} \equiv 1 \ (mod\ m)$. ■

Пример. Невозможность сравнения $g^{\frac{c}{q}} \equiv 1 \ (mod\ m)$ эквивалентна тому, что число g - невычет степени q по mod m. В частности, невозможность сравнения $g^{\frac{c}{2}} \equiv 1 \ (mod\ m)$ означает, что g - квадратичный невычет по mod m.

4. 1) Показатель δ, которому число a принадлежит по mod m, определяется равенством $(ind\ a, c) = \frac{c}{\delta}$; в частности, принадлежность числа a к числу первообразных корней по mod m определяется равенством $(ind\ a, c) = 1$.

2) В приведенной системе вычетов по mod m число чисел,

принадлежащих показателю δ, есть $\varphi(\delta)$; в частности, число первообразных корней есть $\varphi(c)$.

Доказательство.

1) δ — наименьший делитель c с условием $a^{\delta} \equiv 1\ (mod\ m)$. Это условие эквивалентно еще условию $\delta\ ind\ a \equiv 0\ (mod\ c)$ или $ind\ a \equiv 0\ \left(mod\ \frac{c}{\delta}\right)$. Следовательно, δ - минимальный делитель c, при котором $\frac{c}{\delta} \mid ind\ a$, тогда $\frac{c}{\delta}$ - максимальный делитель c, делящий $ind\ a$, то есть $\frac{c}{\delta} = (ind\ a, c)$. Таким образом, утверждение 1) доказано.

2) Среди чисел $0, 1, \dots, c-1$, являющихся минимальными индексами вычетов приведенной системы по mod m, кратными $\frac{c}{\delta}$ являются числа вида $\frac{c}{\delta}y$, где $y = 0, 1, \dots, \delta - 1$. Условие $\left(\frac{c}{\delta}y, c\right) = \frac{c}{\delta}$ равносильно условию $(y, \delta) = 1$. Но последнему удовлетворяют $\varphi(\delta)$ значений y. ■.

Пример. 1) В приведенной системе вычетов по *mod* 41 числами, принадлежащими показателю 10, являются числа a с условием $(ind\ a, 40) = \frac{40}{10} = 4$, то есть числа 4, 23, 25, 31. Всего их $4 = \varphi(10)$.

2) В приведенной системе вычетов по *mod* 41 первообразными корнями являются числа a с условием $(ind\ a, 40) = 1$, то есть числа

6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

Число этих первообразных корней есть $16 = \varphi(40)$.

5.8. Индексы по mod 2^α

Для mod 2 предыдущая теория заменяется несколько более сложной. Пусть $\alpha = 1, 2^\alpha = 2$, $\varphi(2) = 1$. Первообразным корнем по mod 2 будет, например, число $1 \in \bar{1}, 1 \equiv -1\ (mod\ 2)$. Тогда числа $1^0 = (-1)^0 = 1$ образует приведенную систему вычетов по mod 2.

Пусть $\alpha = 2, 2^\alpha = 4$, $\varphi(4) = 2$. Так, например, первообразным корнем по mod 4 будет число $3 \in \bar{3}, 3 \equiv -1\ (mod\ 4)$. Тогда числа $(-1)^0 \equiv 1, (-1)^1 \equiv 3\ (mod\ 4)$ образуют приведенную систему вычетов по mod 4.

Пусть $\alpha \geq 3, 2^\alpha \geq 8$, $\varphi(2^\alpha) = 2^{\alpha-1}$. Первообразных корней в этом случае нет. Более точно, показатель, которому принадлежит по mod 2^α нечетное число x, не превосходит $2^{\alpha-2} = \frac{1}{2}\varphi(2^\alpha)$.

Доказательство.

$x^2 = 1 + 8t_1,\ \ x^4 = 1 + 16t_2,\ \ \ldots,\ \ x^{2^{\alpha-2}} = 1 + 2^{\alpha}t_{\alpha-2} \equiv 1\ (mod\ 2^{\alpha})$.

При этом числа, принадлежащие показателю $2^{\alpha-2}$, существуют. Таким числом будет, например, число 5.

$$5 = 1 + 4, 5^2 = 1 + 8 + 16, 5^4 = 1 + 16 + 31u_2, \ldots, 5^{2^{\alpha-3}}$$
$$= 1 + 2^{\alpha-1} + 2^{\alpha}u_{\alpha-3} \not\equiv 1\ (mod\ 2^{\alpha})$$

откуда видим, что ни одна из степеней $5^1, 5^2, \ldots, 5^{2^{\alpha-1}} \not\equiv 1\ (mod\ 2^{\alpha})$. Числа вида:

$$5^0,\quad 5^1, \ldots,\quad 5^{2^{\alpha-2}-1},$$
$$-5^0, -5^1, \ldots, -5^{2^{\alpha-2}-1},$$

образуют приведенную систему вычетов по mod 2^{α}, Число этих чисел будет $2 \cdot 2^{\alpha-2} = \varphi(2^{\alpha})$; числа каждой отдельно взятой строки несравнимы между собой по mod 2^{α}; наконец, числа верхней строки несравнимы с числами нижней, так как первые по mod 4 сравнимы с 1, а вторые с -1. ■

Для удобства выразим результаты в следующей форме, которая будет пригодна и в случае $\alpha = 0$.

Теорема. *Пусть* $c = 1$, $c_0 = 1$, *если* $a = 1$ *или* $a - 1$; $c = 2$, $c_0 = 2^{\alpha-2}$, *если* $\alpha \geq 2$ *(таким образом всегда* $cc_0 = \varphi(2^\alpha)$*), и пусть* γ и γ_0 *независимо друг от друга пробегают наименьшие неотрицательные вычеты по модулям* c *и* c_0. *Тогда* $(-1)^\gamma 5^{\gamma_0}$ *пробегает приведенную систему вычетов по mod* 2^α.

Теорема. *Сравнение*

$$(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0'} \ (mod\ 2^\alpha)$$

имеет место тогда и только тогда, когда

$$\gamma \equiv \gamma' (mod\ c), \gamma_0 \equiv \gamma_0' \ (mod\ c_0).$$

Доказательство.

1) При $\alpha = 0$ утверждение верно.

2) Пусть $\alpha > 0$. Пусть наименьшие неотрицательные вычеты по mod c и c_0 для чисел γ и γ_0 будут r и r_0, а для чисел γ' и γ_0' будут r' и r_0'. (-1 принадлежит показателю c, 5 - показателю c_0), сравнение $(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0'} \ (mod\ 2^\alpha)$ имеет место тогда и только тогда, когда $(-1)^r 5^{r_0} \equiv (-1)^{r'} 5^{r_0'} \ (mod\ 2^\alpha)$, то есть когда $r = r'$, $r_0 = r_0'$. ■

Определение. *Если* $a \equiv (-1)^{\gamma} 5^{\gamma_0} (mod\ 2^{\alpha})$, *то система* γ, γ_0 *называется системой индексов числа* a *по mod* $(mod\ 2^{\alpha})$.

Всякое a, взаимно простое с 2^{α} (то есть нечетное), имеет единственную систему индексов γ' и γ_0' среди $cc_0 = \varphi(2^{\alpha})$ пар значений γ и γ_0.

Зная систему γ' и γ_0', можно указать все системы ind числа a; это будут все пары γ и γ_0, составленные из неотрицательных чисел классов $\gamma \equiv \gamma' (mod\ c), \gamma_0 \equiv \gamma_0'\ (mod\ c_0)$.

Из определения следует, что числа с данной системой $ind\ \gamma$ и γ_0 образуют класс чисел по mod 2^{α}.

Теорема. *Индексы произведения сравнимы по модулям* c *и* c_0 *с суммами индексов сомножителей.*

Доказательство.

Пусть $\gamma(a), \gamma_0(a), \dots, \gamma\ (l), \gamma_0(l)$ - системы ind чисел $a, b, \dots, l$ Имеем

$$ab \dots l \equiv (-1)^{\gamma(a)+\dots+\gamma(l)} 5^{\gamma_0(a)+\dots+\gamma_0(l)} \rightarrow$$

$$\rightarrow \gamma(a) + \dots + \gamma\ (l), \gamma_0(a) + \dots + \gamma_0(l)$$

- индексы произведения $ab \dots l$. ■

5.9. Индексы по любому составному модулю

Пусть $m = 2^{\alpha} p_1^{\alpha_1} \dots p_k^{\alpha_k}$ - каноническое разложение натурального числа m, числа c и c_0 имеют значения, указанные в теореме выше, $c_s = \varphi(p_s^{\alpha_s})$, g_s наименьший первообразный корень по mod $p_s^{\alpha_s}$.

Определение. *Система чисел* $\gamma, \gamma_0, \gamma_1, \dots, \gamma_k$ *называется системой индексов числа a по mod m, если имеют место сравнения:*

$$a \equiv (-1)^{\gamma} 5^{\gamma_0} (mod\ 2^{\alpha}),$$

$$a \equiv g_1^{\gamma_1} (mod\ p_1^{\alpha_1}),\ \dots,\ a \equiv g_k^{\gamma_k} (mod\ p_k^{\alpha_k}).$$

Следовательно, числа γ и γ_0 - система индексов числа a по mod 2^{α}, числа $\gamma_1, \dots, \gamma_k$- индексы числа a по модулям $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$.. Тогда всякое число a, взаимно простое с m (тем самым оно взаимно просто и со всеми $2^{\alpha}, p_1^{\alpha_1}, \dots p_k^{\alpha_k}$), имеет единственную систему индексов $\gamma', \gamma_0', \gamma_1', \dots, \gamma_k'$ среди $cc_0c_1 \dots c_k = \varphi(m)$, систем $\gamma, \gamma_0, \gamma_1, \dots, \gamma_k$, которые получим, если $\gamma, \gamma_0, \gamma_1, \dots, \gamma_k$ независимо друг от друга пробегают минимальные неотрицательные вычеты по модулям $c, c_0, c_1, \dots, c_k$ а все системы индексов числа a есть все системы

$\gamma, \gamma_0,\ \gamma_1, \ldots, \gamma_k$, составленные из неотрицательных чисел классов

$$\gamma \equiv \gamma'(mod\ c), \gamma_0 \equiv \gamma_0'\ (mod\ c_0),$$

$$\gamma_1 \equiv \gamma_1'\ (mod\ c_1), \ldots, \gamma_k \equiv \gamma_k'\ (mod\ c_k).$$

Числа a с данной системой индексов $\gamma, \gamma_0,\ \gamma_1, \ldots, \gamma_k$ могут быть найдены путем решения системы

$$\begin{cases} a \equiv g_1^{\gamma_1}\left(mod\ p_1^{\alpha_1}\right) \\ \ldots \\ a \equiv g_k^{\gamma_k}\left(mod\ p_k^{\alpha_k}\right) \end{cases},$$

а, следовательно, они образуют класс чисел по модулю m.

Так как индексы $\gamma, \gamma_0,\ \gamma_1, \ldots, \gamma_k$ числа a по mod m являются индексами его соответственно по модулям $2^\alpha, p_1^{\alpha_1}, \ldots\ p_k^{\alpha_k}$, то верна

Теорема. *Индексы произведения сравнимы по модулям $c, c_0, c_1, \ldots, c_k$ с суммами индексов сомножителей.*

Пусть $r = \varphi(2^\alpha)$ при $\alpha \leq 2, r = \frac{1}{2}\varphi(2^\alpha)$ при $\alpha > 2$ и пусть h - НОК чисел $r, c_1, \ldots, c_k$. При всяком a, взаимно простом с m, сравнение $a^h \equiv 1\ (mod\ k)$ верно по всем модулям $k, k \in \left\{2^\alpha, p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}\right\}$, следовательно, оно верно и по mod m.

Тогда a не может быть первообразным корнем по mod m в тех

случаях, когда $h < \varphi(m)$. Но $h < \varphi(m)$ при $\alpha > 2$, при $k > 1$, в случае $\alpha = 2, k = 1$, тогда получаем, что для $m > 1$ первообразные корни могут существовать лишь в случаях $m = 2, 4,\ p_1^{\alpha_1}, 2p_1^{\alpha_1}$. Но как раз для этих случаев существование первообразных корней было уже доказано.

Таким образом, все случаи, когда существуют первообразные корни по mod m, большие 1, есть $m = 2, 4,\ p^{\alpha}, 2p^{\alpha}$.

Таблицу индексов можно составить и для любого целого положительного m, выписывая соответственно каждому числу приведенной систему вычетов по mod m отвечающие этому числу значения индексов $\gamma, \gamma_0,\ \gamma_1, \dots, \gamma_k$ (полные системы вычетов по модулям $c, c_0, c_1, \dots, c_k$).

Пример. 1) Построить таблицу ind по mod 8.

$$c = 2, c_0 = 2^{3-2} = 2.$$

Для любого числа N, принадлежащего приведенной системе вычетов по mod 8 $\mathrm{N} \equiv (-1)^{\gamma} 5^{\gamma_0} (mod\ 2^3)$, где $\gamma = 0 \vee 1$(полная система вычетов по mod c) и $\gamma_0 = 0 \vee 1$ (полная система вычетов по mod c_0). Находим

$$(-1)^0 = 1, 5^0 = 1, -5^0 \equiv 7\ (mod\ 8),$$

$$(-1)^1 = -1, 5^1 = 5, -5^1 \equiv 3\ (mod\ 8).$$

N	1	3	5	7
γ	0	1	0	1
γ_0	0	1	1	0

2) по mod $40.40 = 2^3 \cdot 5$, причем для любого N из приведенной системы вычетов по модулю 40 значения $ind\ \gamma$ и γ_0 найдем в таблице по mod 8, а значения $ind\ \gamma_1$ в таблице по mod 5.

N	**1**	**2**	**3**	**4**
$\boldsymbol{\gamma_1}$	0	1	3	2

Кафедра ФМО и ИТ

В результате получим следующую таблицу 14 по mod 40.

N	1	3	7	9	11	13	17	19
γ	0	1	1	0	1	0	0	1
γ_0	0	1	0	0	1	1	0	1
γ_1	1	0	3	1	2	0	3	1
N	21	23	27	29	31	33	37	39
γ	0	1	1	0	1	0	0	1
γ_0	1	0	1	1	0	0	1	0
γ_1	2	0	3	1	2	0	3	1

3) $m = 9.\varphi(9) = 6 = 2 \cdot 3.$

5 – первообразный корень по mod 9, так как оно не удовлетворяет ни одному из сравнений

$5^{\left(\frac{6}{2}\right)} \equiv 1\ (mod\ 9), 5^{\left(\frac{6}{3}\right)} \equiv 1\ (mod\ 9), 5^0 \equiv 1\ (mod\ 9), 5^1 \equiv 5\ (mod\ 9)$,

$5^2 \equiv 7\ (mod\ 9), 5^3 \equiv 8\ (mod\ 9), 5^4 \equiv 4\ (mod\ 9), 5^5 \equiv 2\ (mod\ 9).$

N	1	2	4	5	7	8
γ_1	0	5	4	1	2	3

N	1	2	4	5	7	8
γ	0	0	0	0	0	0
γ_1	0	1	2	5	4	3

4) $m = 21, 21 = 3 \cdot 7$, для любого N из приведенной системы вычетов по модулю 21 значения $ind\ \gamma_1$ найдем в таблице ind по mod 3, а значения $ind\ \gamma_2$ в таблице по mod 7.

N	1	2
γ_1	0	1

N	1	2	3	4	5	6
γ_2	0	2	1	4	5	3

В результате получим следующую таблицу.

N	1	2	4	5	8	10	11	13	16	17	19	20
γ_1	0	1	0	1	1	0	1	0	0	1	0	1
γ_2	0	2	4	5	0	1	4	3	2	1	5	3

Упражнения

1. Найти порядок класса вычетов $x \equiv 2\ (mod\ 11)$.
2. Найти все возможные порядки по модулю 9.
3. Найти натуральные значения *x*, удовлетворяющие сравнению:

$$1)\ 5^x \equiv 1(mod\ 8),\ 2)\ 4^x \equiv 1(mod\ 3).$$

4. Найти:

1) $O(25 \bmod 31)$,
2) $O(5 \bmod 61)$,
3) $O(18 \bmod 29)$,
4) $O(5 \bmod 31)$.

5. Решить сравнения:

1) $5^x \equiv 1(mod\ 9)$,
2) $2^x \equiv 1(mod\ 25)$,
3) $6^x \equiv 1(mod\ 49)$,
4) $2^x \equiv 1(mod\ 49)$.

6. Найти классы первообразных корней модуля 7.
7. Найти классы первообразных корней модуля 6.
8. Доказать, что модуль 8 не имеет первообразных корней.
9. Решить сравнения:

1) $x^2 \equiv 3(mod\ 11)$,
2) $x^{10} \equiv 3(mod\ 17)$,
3) $x^5 \equiv 14(mod\ 41)$,
4) $x^2 \equiv 89(mod\ 97)$.

10. При каких целых значениях a разность делится на задан-

ное число:

1) $3a^2$-5 на 7,
2) $13a^2$ – 11 на 29,
3) $7a^2$ + 13 на 23,
4) a^2 - 5 на 11.

11. Решить сравнения при помощи индексов:

1) $2^x \equiv 1(mod\ 67)$,
2) $7^{3x} \equiv 7^5(mod\ 5)$,
3) $13^x \equiv 7(mod\ 4)$,
4) $7^x \equiv 3(mod\ 19)$

12. При помощи индексов доказать, что 2 есть первообразный корень модуля 37.

13. При помощи индексов найти порядок класса 6 по модулю 23.

14. Найти все возможные основания индексов по модулю 11 и составить таблицу индексов при наименьшем из найденных оснований.

15. Укажите верные и неверные утверждения.

a. Порядок числа 2 по модулю 5 равен 2;
b. Порядок числа 2 по модулю 3 равен 2;
c. Порядок числа 2 по модулю 5 равен 4;
d. Порядок числа 2 по модулю 15 равен 9;
e. Порядок числа 2 по модулю 15 равен 4.

16.Какому показателю принадлежат:

a) число 5 по модулю 12, c) число 3 по модулю 17,

b) число 6 по модулю 17, d) число 11 по модулю 31.

17. Найти все показатели, которым принадлежат числа:

a) по модулю 11, c) по модулю 12, b) по модулю 17,

d) по модулю 15.

18. Найти наименьший первообразный корень: a) модулю 13, c) по модулю 29,

b) по модулю 19, d) по модулю 43.

19. Найти все первообразные корни:

a) по модулю 23, c) по модулю 41, b) по модулю 37, d) по модулю 53.

20. Зная, что число 2 есть первообразный корень по модулю 37, пока-зать справедливость сравнения

$$2^{18} \equiv 6^2 (\mathrm{mod}\ 37).$$

21. Найти $P_m(m\text{-}1)$.

22. Доказать, что модуль 8 не имеет первообразных корней.

Указание: испытать приведенную систему вычетов.

23. Показать, что если $(a, p)=1$, где p - простое число, $a^{2k} \equiv 1(\mathrm{mod}\ p)$ и число a принадлежит показателю $2k$ по модулю p, то $a^k \equiv -1(\mathrm{mod}\ p)$. *Указание.* Исследовать сравнение $(a^k\text{-}1)(a^k+1) \equiv 0(\mathrm{mod}\ p)$.

24. Доказать, что если число a – первообразный корень простого модуля p, то a^k, где $(k,p-1)=1$, также является первообразным корнем по модулю p.

25.Доказать, что если числа a и b являются первообразными корнями по простому модулю $p>2$, то произведение ab не может быть первообразным корнем по модулю p.

26. Доказать, что первообразный корень g по простому модулю p есть квадратичный невычет по тому же модулю.

27. Число 43 – первообразный корень по модулю 89; показать, что сравнение $x^2 \equiv 43 \pmod{89}$ не имеет решение

28. Составить таблицу индексов:

a) по модулю 11,
b) по модулю 19,
c) по модулю 23,
d) по модулю 31.

29. Решить сравнения при помощи таблицы индексов:

a) $8x \equiv 26 \pmod{37}$,
b) $x^2 \equiv 3 \pmod{11}$,
c) $13x^{12} \equiv 26 \pmod{31}$,
d) $40x^{10} \equiv 3 \pmod{17}$,
e) $13a^2 - 11 \equiv 0 \pmod{29}$,
f) $3x^6 \equiv 7 \pmod{61}$,
g) $3\,x^3 \equiv 2 \pmod{37}$,
h) $2^x \equiv 7 \pmod{19}$,
i) $16^x \equiv 11 \pmod{43}$,
j) $27^{x^2} \equiv 17 \pmod{31}$,
k) $3^{x^2} \equiv 23 \pmod{29}$,
l) $123^{x^2} \equiv 17 \pmod{47}$.

30. С помощью таблиц индексов найти остатки от деления:

a) $89 \cdot 78$ на число 61,
b) числа 15^{27} на число 59,
c) $53 \cdot 41 \cdot 19$ на число 89,
d) числа 31^{124} на число 37.

31. Доказать, что индекс числа -1 по нечетному модулю p всегда равен $\frac{p-1}{2}$.

ГЛАВА 6. ДВУЧЛЕННЫЕ СРАВНЕНИЯ

6.1. Двучленные сравнения по простому модулю

Определение. *Двучленным сравнением по простому модулю называется сравнение вида*

$$cx^n \equiv b \pmod p,$$

где $b,c \in Z$, p *- простое,* c *не делится на* p, $n \in N$.

Рассмотрим сравнение

$$x^n \equiv a \pmod p,\ p \neq 2.$$

Имеем:

1) Если $a \vdots p$, то $a \equiv 0 \pmod p$, тогда $x^n \equiv 0 \pmod p$. Получим единственное решение $\bar{0}$ *mod* p.

Если *а не делится на p,* то данное сравнение или совсем не имеет решений, или имеет ровно d решений, где d = НОД(n, p - 1), а именно, получим еще два случая.

2) Если *ind* $a \vdots d$, то сравнение (1) имеет d решений'.

3) Если *ind a не делится на d,* то сравнение не имеет решений.

Например:

1. $x^3 \equiv 14 \pmod 7$, $a = 14$, $14 \vdots 7$, следовательно, сравнение имеет единственное решение $\bar{0} \ mod\ 7$.

2. $x^4 \equiv 2 \pmod 5$, d = НОД(4, 5 - 1) = НОД (4,4) = 4, $a = 2$, 2 не делится на 5, $ind\ 2 = 3$ (из таблицы индексов), $ind\ 2$ не делится на 4, следовательно, сравнение не имеет решения.

3. $x^3 \equiv 8 \pmod{13}$, 8 не делится на 13, d = НОД(3, 12) = 3, $ind\ 8 = 9$ (из таблицы индексов), $ind\ 8 \vdots 3$, следовательно, сравнение имеет 3 решения.

Определение. *Если сравнение $x^n \equiv a \pmod p$ имеет решение, то число a называется вычетом n-й степени по mod p. Если сравнение не имеет решения, то a называется невычетом n-й степени по mod p.*

Например, 14 - вычет 3-й степени по *mod* 7,

2 - невычет 4-й степени по *mod* 5,

8 - вычет 3-й степени по *mod* 13.

В частности, вычеты 2-й степени называются *квадратичными*, вычеты 3-й степени - *кубическими*, вычеты 4-й степени - *биквадратичными*.

Если в сравнении $x^n \equiv a \ (mod\ p)$ заменить a любым числом из класса вычетов $\bar{a}$, то есть числом, сравнимым с ним по $mod\ p$, то получим сравнение, равносильное данному.

Если a - вычет, то $\forall a_0 \in \bar{a}$, a_0 - вычет, следовательно, $\bar{a}$ - вычет. Если a — невычет, то $\forall a_0 \in \bar{a}$, a_0 ¯ невычет, следовательно, $\bar{a}$ - невычет.

Сравнения можно решать и в-виде $cx^n \equiv b \ (mod\ p)$, и в виде $x^n \equiv a \ (mod\ p)$. Решим сравнение

$$cx^n \equiv b \ (mod\ p) \text{ ,} c \text{ не делится на } p.$$

Индексируем сравнение, получим

$$ind(cx)^n \equiv ind\ b \ (mod\ p-1),$$

$$ind\ c + n \cdot ind\ x \equiv ind\ b \ (mod\ p-1),$$

$$n \cdot ind\ x \equiv ind\ b - ind\ c \ (mod\ p-1).$$

По таблице находим *ind b, ind* c, получим:

$$n \cdot ind\ x \equiv m \ (mod\ p-1)).$$

Решая далее, получим после исследования $\emptyset$ или

$$ind\ x \equiv k \ (mod\ p-1)).$$

По другой таблице находим *x*.

Пример. $13x^{21} \equiv 5\ (mod\ 31)$.

$$ind\ 13 + 21 \cdot ind\ x \equiv ind\ 5\ (mod\ 30),$$

$$11 + 21 \cdot ind\ x \equiv 20\ (mod\ 30),$$

$$21 \cdot ind\ x \equiv 9\ (mod\ 30),$$

т.к. НОД $(21, 30) = 3, 3 > 1, 9 \vdots 3$, то полученное сравнение имеет 3 решения.

$$7 \cdot ind\ x \equiv 3\ (mod\ 10),$$

$$7 \cdot ind\ x \equiv 3 - 10\ (mod\ 10),$$

$$7 \cdot ind\ x \equiv -7\ (mod\ 10),$$

$$ind\ x \equiv -1\ (mod\ 10),$$

$$ind\ x \equiv 9\ (mod\ 10).$$

Следовательно, получим 3 решения:

$$ind\ x \equiv 9\ (mod\ 30),$$

$$ind\ x \equiv 9 + 10\ (mod\ 30),$$

$$ind\ x \equiv 9 + 2 \cdot 10\ (mod\ 30),$$

то есть

$$ind\ x \equiv 9\ (mod\ 30),$$

$$ind\ x \equiv 19\ (mod\ 30),$$

$$ind\ x \equiv 29\ (mod\ 30).$$

По другой таблице для последних трех сравнений находим:

$$x \equiv 29\ (mod\ 31),$$

$$x \equiv 12\ (mod\ 31),$$

$$x \equiv 21\ (mod\ 31).$$

Итак, сравнение $13x^{21} \equiv 5\ (mod\ 31)$ имеет три решения

$$x = \overline{12, 21, 29} \text{ по модулю } 31.$$

Общие теоремы

Рассмотрим двучленное сравнение

$$x^n \equiv a\ (mod\ m), (a, m) = 1.$$

Если это сравнение имеет решения, то число a называется вычетом степени n по mod m. В противном случае a называется невычетом степени n по mod m. $n = 2$ - квадратичные, $n = 3$ - кубические, $n = 4$ - биквадратичные.

Рассмотрим сравнение $x^2 \equiv a\ (mod\ p), (a, p) = 1, p > 2$.

Теорема. *Если число a - квадратичный вычет по* mod p, *то сравнение $x^2 \equiv a\ (mod\ p)$ имеет 2 решения.*

Доказательство.

Число a - квадратичный вычет, следовательно, сравнение имеет, по крайней мере, одно решение

$$x \equiv x_1 \ (mod\ p).$$

Тогда ввиду $(-x_1)^2 = {x_1}^2$, то же сравнение имеет и второе решение $x \equiv -x_1 \ (mod\ p)$. Это второе решение отлично от первого, так как из $x_1 \equiv -x_1 \ (mod\ p)$ мы имели бы $2x_1 \equiv 0 \ (mod\ p)$, что невозможно ввиду $(2, p) = (x_1, p) = 1$.

Этими двумя решениями исчерпываются все решения сравнения $x^2 \equiv a \ (mod\ p)$, так как сравнение 2-й степени более двух решений иметь не может (если сравнение n-й степени имеет более чем n решений, то все коэффициенты кратны p). ■

Теорема. *Приведенная система вычетов по mod p состоит из* $\frac{p-1}{2}$ *квадратичных вычетов, сравнимых с числами*

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2,$$

и $\frac{p-1}{2}$ *квадратичных невычетов.*

Доказательство.

Среди вычетов приведенной системи по $mod\ p$ квадратичными невычетами являются те и только те, которые сравнимы с квадратами чисел (приведенной системы вычетов)

$$-\frac{p-1}{2}, \dots, -2, -1, 1, 2, \dots, \frac{p-1}{2},$$

то есть с числами $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$. При этом эти числа по $mod\ p$ несравнимы, так как из $k^2 \equiv e^2\ (mod\ p), 0 < k < e \leq \frac{p-1}{2}$, следовало бы, что сравнению $x^2 \equiv e^2\ (mod\ p)$, вопреки предыдущей теореме, удовлетворяло бы 4 решения $x = -e, -k, k, e$. ■

6.2. Символ Лежандра

$\left(\frac{a}{p}\right)$ – символ a по p; a - числитель, p - знаменатель, a не делится на p.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{если } a - \text{квадратичный вычет по } mod\ p, \\ -1, \text{если } a - \text{квадратичный вычет по } mod\ p. \end{cases}$$

Вычислить символ $\left(\frac{a}{p}\right)$ (и таким путем определить, является ли a квадратичным вычетом или невычетом по mod p) позволяет теорема:

Теорема (критерий Эйлера). *При a не делящемся на p имеет место сравнение*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \ (mod\ p).$$

Доказательство.

По теореме Ферма $a^{p-1} \equiv 1\ (mod\ p)$, при условии, что a не делится на p,

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0\ (mod\ p) \rightarrow \begin{bmatrix} a^{\frac{p-1}{2}} - 1 \equiv 0\ (mod\ p), \\ a^{\frac{p-1}{2}} + 1 \equiv 0\ (mod\ p). \end{bmatrix}$$

(оба не могут выполняться, так как в противном случае их разность, равная 2, должна делиться на p). Всякий квадратичный вычет a удовлетворяет при некотором x сравнению $a \equiv x^2\ (mod\ p)$, и, следовательно, так же получающемуся из него при возведении в степень $\frac{p-1}{2}$ сравнению $a^{\frac{p-1}{2}} - 1 \equiv 0\ (mod\ p)$. При этом квадратичными вычетами и исчерпываются все решения данного сравнения, так как сравнение $\frac{p-1}{2}$степени не может иметь больше $\frac{p-1}{2}$ решений, следовательно, квадратичные вычеты удовлетворяют $a^{\frac{p-1}{2}} + 1 \equiv 0\ (mod\ p)$. ■

Примеры.

1) $5^{14} \equiv 1\ (mod\ 29)$. $\left(\frac{5}{29}\right) = 1$, 5 - квадратичный вычет по *mod* 29, так как сравнение $x^2 \equiv 5\ (mod\ 29)$. имеет 2 решения.

2) $3^{14} \equiv -1\ (mod\ 29)$. $\left(\frac{3}{29}\right) = -1$, 3 - квадратичный невычет по *mod* 29, так как сравнение $x^2 \equiv 3\ (mod\ 29)$ не имеет решения.

Свойство 1. *Если* $a \equiv a_1\ (mod\ p)$, то $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.

Доказательство.

Числа одного и того же класса будут одновременно квадратичными вычетами или невычетами.

Свойство 2. $\left(\frac{1}{p}\right) = 1$.

Доказательство.

$1 = 1^2$.

Свойство 3. $\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Доказательство.

Так как $\frac{p-1}{2}$ четное, если p вида $4m + 1$ и нечетное, если p вида $4m + 3$,

то отсюда следует, что -1 является квадратичным вычетом по mod p, если p вида $4m + 1$, и – 1 является квадратичным невычетом, если p вида $4m + 3$.

Свойство 4. $\left(\frac{a\cdot b\cdot \ldots \cdot l}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\cdot \ldots \cdot\left(\frac{l}{p}\right)$

Доказательство.

$$\left(\frac{a\cdot b\cdot \ldots \cdot l}{p}\right) \equiv (a\cdot b\cdot \ldots \cdot l)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}\cdot \ldots \cdot l^{\frac{p-1}{2}} \equiv$$

$$\equiv \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\cdot \ldots \cdot\left(\frac{l}{p}\right)\ (mod\ p).$$

Следствие. $\left(\frac{a\cdot b^2}{p}\right) = \left(\frac{a}{p}\right)$.

То есть в числителе можно отбросить любой квадратный множитель.

Получим еще оно ***свойство***. Для этого получим сначала вспомогательную формулу. Пусть $p_1 = \frac{p-1}{2}$, рассмотрим сравнения

$$a\cdot 1 \equiv \varepsilon_1 r_1\ (mod\ p),$$

$$a\cdot 2 \equiv \varepsilon_2 r_2\ (mod\ p),$$

$$a\cdot p_1 \equiv \varepsilon_{p_1} r_{p_1}\ (mod\ p),$$

где $\varepsilon_x r_x$ - абсолютно наименьший вычет ax, r_x - его модуль, $\varepsilon_x = \pm 1$.

Числа $a \cdot 1, -a \cdot 1\ a \cdot 2, -a \cdot 2, \ldots, a \cdot p_1, -a \cdot p_1$ образуют приведенную систему вычетов по mod p (если $(a,\ m) = 1$ и x пробегает приведенную систему вычетов по mod m, то ax тоже пробегает приведенную систему вычетов по mod m). Их абсолютно наименьшие вычеты есть

$$\varepsilon_1 r_1, -\varepsilon_1 r_1, \ldots, \varepsilon_{p_1} r_{p_1}, -\varepsilon_{p_1} r_{p_1}.$$

Положительные $r_1, r_2, \ldots, r_{p_1}$ должны совпадать с числами $1, 2, \ldots, p_1$ (в качестве полной системы обычно берут наименьшие неотрицательные вычеты 0, 1, ... ,m - 1).

Тогда следует, что

$$a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot \ldots \cdot p_1 \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p_1} r_1 r_2 \ldots r_{p_1} \ (mod\ p),$$

так как $1 \cdot 2 \cdot \ldots \cdot p_1 = r_1 r_2 \ldots r_{p_1}$, то

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p_1} \ (mod\ p) \rightarrow \left(\frac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p_1}.$$

Далее, $\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right]$, что будет четным или нечетным в зависимости от того, будет ли наименьший неотрицательный вычет числа ax больше или меньше чем $\frac{1}{2}p$, то есть

будет ли $\varepsilon_x = 1$ или $\varepsilon_x = -1$. Отсюда очевидно

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]}, \text{ поэтому } \left(\frac{a}{p} = (-1)^{\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}\right).$$

Предполагая a нечетным, преобразуем последнее равенство. Имеем ($a + p$ - четное число).

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]} =$$

$$(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\sum_{x=1}^{p_1}x}.$$

Отсюда следует, что $\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}$.

Свойство 5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Доказательство.

Следует из равенства $\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}$ при $a = 1$.

Но число p можно представить в виде $p = 8m + s$, где s одно из чисел 1, 3, 5, 7. При этом

$$\frac{(8m+s)^2-1}{8} = 8m^2 + 2ms + \frac{s^2-1}{8}$$

будет четным при $s = 1$ и при $s = 7$ и нечетным при $s = 3$ и $s = 5$.

Следовательно, 2 будет квадратичным вычетом по mod p, если p вида $p = 8m + 1$ или $p = 8m + 7$, и 2 будет квадратичным невычетом, если $p = 8m + 3$ или $p = 8m + 5$.

Свойство 6. (*закон взаимности квадратичных вычетов*). *Если p и q - простые нечетные числа, то*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Получим другую формулировку этого **свойства.**

Число $\frac{p-1}{2}\cdot\frac{q-1}{2}$ будет нечетным лишь в случае, когда оба числа p и q будут вида $4m + 3$, и четным, если хоть одно из них вида $4m + 1$.

Следовательно, это свойство можно формулировать иначе:

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), \text{если оба числа } p \text{ и } q \text{ вида } 4m + 3, \\ \left(\frac{p}{q}\right), \text{если хоть одно из чисел } p \text{ и } q \text{ вида } 4m + 1 \end{cases}.$$

Доказательство.

Кафедра ФМО и ИТ

Число $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, тогда из $x^2 \equiv a \ (mod\ p)$ следует

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]}.$$

Пусть $\frac{q-1}{2} = q_1$, рассмотрим $p_1 q_1$ пар чисел, получаемых, когда в выражениях qx, py, числа x и y независимо друг от друга пробегают системы значений $x = 1, 2, \dots, p_1$, $y = 1, 2, \dots, q_1$. Равенство $qx = py$ невозможно, так как из этого равенства следовало бы, что $py \vdots q$, что ввиду $(p, q) = (y, q) = 1$ (так как $0 < y < q$) невозможно. Поэтому можно положить $p_1 q_1 = S_1 + S_2$, где S_1 - число пар с $qx < py$ и S_2 - число пар с $qx > py$. Очевидно, S_1 есть также число пар с $x < \frac{p}{q} y$ (этому не противоречит неравенство $x \leq p_1$), так как из $\frac{p}{q} y < \frac{p}{2}$ следует $\left[\frac{p}{q} y\right] \leq \left[\frac{p}{2}\right] = p_1$. Поэтому получим:

$$S_1 = \sum_{y=1}^{q_1} \left[\frac{p}{q} y\right], \ S_2 = \sum_{x=1}^{p_1} \left[\frac{q}{p} x\right].$$

Но тогда $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]}$ дает нам $\left(\frac{p}{q}\right) = (-1)^{S_1}$, $\left(\frac{q}{p}\right) = (-1)^{S_2}$, следовательно, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S_1+S_2} = (-1)^{p_1 q_1}$.

6.3. Символ Якоби

Пусть P - нечетное, $P > 1$, $P = p_1 p_2 \dots p_n$ – его каноническое разложение на простые. Пусть $(a, P) = 1$.

Определим *символ Якоби:*

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_n}\right).$$

Свойство 1. *Если* $a \equiv a_1 \pmod P$, *то* $\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right)$.

Доказательство.

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_n}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\dots\left(\frac{a_1}{p_n}\right) = \left(\frac{a_1}{P}\right).$$

Так как a, будучи сравнимым с a_1 по mod P, будет сравнимым с a_1 и по модулям $p_1, p_2, \dots, p_n$, которые являются делителями P.

Свойство 2. $\left(\frac{1}{P}\right) = 1$.

Доказательство.

$$\left(\frac{1}{P}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\dots\left(\frac{1}{p_n}\right) = 1 \cdot 1 \cdot \dots \cdot 1.$$

Свойство 3. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

Доказательство.

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\dots\left(\frac{-1}{p_n}\right)=(-1)^{\frac{p_1-1}{2}+\dots+\frac{p_n-1}{2}},$$

$$\frac{P-1}{2}=\frac{\left(1+2\frac{p_1-1}{2}\right)\dots\left(1+2\frac{p_n-1}{2}\right)-1}{2}=\frac{p_1-1}{2}+\dots+\frac{p_n-1}{2}+2N,$$

отсюда $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$.

Свойство 4. $\left(\frac{ab\dots l}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\dots\left(\frac{l}{P}\right)$.

Доказательство.

$$\left(\frac{ab\dots l}{P}\right)=\left(\frac{ab\dots l}{p_1}\right)\left(\frac{ab\dots l}{p_2}\right)\dots\left(\frac{ab\dots l}{p_n}\right)=$$

$$\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\dots\left(\frac{l}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\dots\left(\frac{l}{p_2}\right)\dots\left(\frac{a}{p_n}\right)\left(\frac{b}{p_n}\right)\dots\left(\frac{l}{p_n}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\dots\left(\frac{l}{P}\right)$$

Отсюда следует, что $\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right)$.

Свойство 5. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$.

Доказательство.

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\dots\left(\frac{2}{p_n}\right)=(-1)^{\frac{{p_1}^2-1}{8}+\dots+\frac{{p_n}^2-1}{8}},$$

$$\frac{P^2-1}{8}=\frac{\left(1+8\frac{{p_1}^2-1}{8}\right)\dots\left(1+8\frac{{p_n}^2-1}{8}\right)-1}{8}=\frac{{p_1}^2-1}{8}+\dots+\frac{{p_n}^2-1}{8}+2N.$$

Следовательно, $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$.

Свойство 6. *Если P и Q - положительные нечетные взаимно простые числа, то*

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Доказательство.

Пусть $Q = q_1 q_2 \dots q_s$,

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\dots\left(\frac{Q}{p_n}\right) =$$

$$\prod_{\alpha=1}^{n}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right) = (-1)^{\sum_{\alpha=1}^{n}\sum_{\beta=1}^{s}\frac{p_\alpha-1}{2}\cdot\frac{p_\beta-1}{2}} = (-1)^{\left(\sum_{\alpha=1}^{n}\frac{p_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{p_\beta-1}{2}\right)}\left(\frac{P}{Q}\right).$$

Но $\frac{P-1}{2} = \sum_{\alpha=1}^{n}\frac{P_\alpha-1}{2} + 2N$, $\frac{Q-1}{2} = \sum_{\beta=1}^{s}\frac{Q_\beta-1}{2} + 2N$.

Отсюда $\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$

Свойство 7. *Рассматривая символ Лежандра как частный случай символа Якоби и пользуясь свойствами символа Якоби, можно вычислить символ Лежандра быстрее, чем с помощью теоремы - критерия Эйлера.*

Пример. Сколько решений имеет сравнение $x^2 \equiv 219\ (mod\ 383)$?

Решение.

$Q = 219, P = 383.$

$$\left(\frac{219}{383}\right) = (-1)^{\frac{383-1}{2}\cdot\frac{219-1}{2}}\left(\frac{383}{219}\right) = (-1)^{191\cdot 109}\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) =$$

$$-\left(\frac{4\cdot 41}{219}\right) = -\left(\frac{41}{219}\right) = -1\cdot(-1)^{\frac{40}{2}\cdot\frac{218}{2}}\left(\frac{219}{41}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) =$$

$$-\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1(-1)^{\frac{41^2-1}{8}}\left(\frac{7}{41}\right) = -\left(\frac{7}{41}\right) = -1\cdot(-1)^{\frac{6}{2}\cdot\frac{40}{2}}\left(\frac{41}{7}\right) = -\left(\frac{41}{7}\right) =$$

$$-\left(\frac{-1}{7}\right) = -1\cdot(-1)^{\frac{7-1}{2}} = -1\cdot(-1) = 1.$$

Следовательно, данное сравнение имеет 2 решения.

6.4. Случай составного модуля

Рассмотрим сравнение

$$x^2 \equiv a\ (mod\ p^\alpha), \alpha > 0, (a,p) = 1, p > 2.$$

Пусть $f(x) = x^2 - a, f'(x) = 2x$. Если $x \equiv x_1\ (mod\ p)$ есть решение сравнения

$$x^2 \equiv a\ (mod\ p).$$

То, так как $(a,p) = 1$, также $(x_1,p) = 1$, а так как p – нечетное,

то $(x_1, p) = 1$, то есть $f'(x)$ не делится на $f(x)$, следовательно, можно решить как и раньше.

Сравнение $x^2 \equiv a \pmod{p^\alpha}$ имеет два решения или же ни одного в зависимости от того, будет ли a квадратичным вычетом или же невычетом по mod p.

Теперь рассмотрим сравнение

$$x^2 \equiv a \pmod{2^\alpha}, \alpha > 0, (a, 2) = 1.$$

$f'(x) = 2x \vdots 2$, следовательно, получим изменение.

Если $x^2 \equiv a \pmod{2^\alpha}$ разрешимо, то так как $(a, 2) = 1$, имеем $(x, 2) = 1$, следовательно, $(x^2 - 1) \vdots 8$, $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$.

Приведем $x^2 \equiv a \pmod{2^\alpha}$ к виду $(x^2 - 1) + 1 \equiv a \pmod{2^\alpha}$, необходимо для разрешимости

$$a \equiv 1 \pmod{4} \text{ при } \alpha = 2,$$

$$a \equiv 1 \pmod{8} \text{ при } \alpha \geq 3.$$

В случаях когда эти условия выполнены, рассмотрим вопрос об отыскании решений и их числа.

Для $\alpha \leq 3$ сравнению удовлетворяют все нечетные числа, то

есть сравнение $x^2 \equiv a \ (mod\ 2)$ имеет одно решение

$$x \equiv 1 \ (mod\ 2).$$

Сравнение $x^2 \equiv a \ (mod\ 4)$ имеет 2 решения

$$x \equiv 1, 3 \ (mod\ 4).$$

Сравнение $x^2 \equiv a \ (mod\ 8)$ имеет 4 решения

$$x \equiv 1, 3, 5, 7 \ (mod\ 8).$$

Для $\alpha = 4, 5, \ldots$ все нечетные числа объединим в арифметические прогрессии

$$x = \pm(1 + 4t_3),$$

$$(1 + 4t_3 \equiv 1 \ (mod\ 4), -1 - 4t_3 \equiv -1 \equiv 3 \ (mod\ 4)).$$

Выясним, какие из чисел удовлетворяют сравнению $x^2 \equiv a \ (mod\ 16)$.

$$(1 + 4t_3)^2 \equiv a \ (mod\ 16), t_3 \equiv \frac{a-1}{8} \ (mod\ 2),$$

$$t_3 = t'_3 + 2t_4, x = \pm(1 + 4t'_3 + 8t_4) = \pm(x_4 + 8t_4).$$

Посмотрим, какие из последних чисел удовлетворяют сравнению $x^2 \equiv a \ (mod\ 32)$.

$(x_4 + 8t_4)^2 \equiv a \ (mod\ 32), t_4 = t'_4 + 2t_5, x = \pm(x_5 + 16t_5)$, и так далее.

Тогда при любом $a > 3$ значения x, удовлетворяющие сравнению

$$x^2 \equiv a \ (mod\ 2^\alpha),$$

представятся в виде

$$x = \pm(x_\alpha + 2^{\alpha-1} t_\alpha).$$

Эти значения x образуют 4 различных решения сравнения:

$$x \equiv x_\alpha;\ x_\alpha + 2^{\alpha-1}; -x_\alpha;\ -x_\alpha - 2^{\alpha-1}\ (mod\ 2^\alpha)$$

(по mod 4 два первых сравнимы с 1, два последних с - 1).

Пример. Сравнение $x^2 \equiv 57\ (mod\ 64)$ имеет 4 решения, так как $57 \equiv 1\ (mod\ 8)$.

Представим x в виде $x = \pm(1 + 4t_3)$, находим

$(1 + 4t_3)^2 \equiv 57\ (mod\ 16)$, $8t_3 \equiv 56\ (mod\ 16)$, $t_3 \equiv 1\ (mod\ 2)$,

$t_3 = 1 + t_4$,

$x = \pm(5 + 8t_4)$, $(5 + 8t_4)^2 \equiv 57\ (mod\ 32)$, $t_4 \equiv 0\ (mod\ 2)$,

$t_4 \equiv 2t_5\ (mod\ 32)$,

$x = \pm(5 + 16t_5)$, $(5 + 16t_5)^2 \equiv 57\ (mod\ 64)$, $5 \cdot 32t_5 \equiv 32\ (mod\ 64)$,

$t_5 \equiv 1\ (mod\ 2)$, $t_5 = 1 + 2t_6$, $x = \pm(21 + 32t_6)$.

Следовательно, решениями сравнения $x^2 \equiv 57\ (mod\ 64)$ будут $x \equiv \pm 21; \pm 53;\ (mod\ 64)$.

Вывод: *Для сравнения* $x^2 \equiv a \pmod{2^\alpha}, (a,2) = 1$ *необходимыми условиями разрешимости будут:*

$$a \equiv 1 \pmod 4 \text{ при } \alpha = 2,$$

$$a \equiv 1 \pmod 8 \text{ при } \alpha \geq 3.$$

Если эти условия не нарушены, число решений будет:

1 *при* $\alpha = 1$,

2 *при* $\alpha = 2$,

4 *при* $\alpha \geq 3$.

Для сравнения вида $x^2 \equiv a \pmod m$, $m = 2^\alpha {p_1}^{\alpha_1} \dots {p_k}^{\alpha_k}$, $(a,m) = 1$ *необходимыми условиями разрешимости будут:*

$$a \equiv 1 \pmod 4 \text{ при } \alpha = 2,$$

$$a \equiv 1 \pmod 8 \text{ при } \alpha \geq 3.$$

Если ни одно из этих условий не нарушено, число решений будет

$$2^k \text{ при } \alpha = 0 \text{ и при } \alpha = 1,$$

$$2^{k+1} \text{ при } \alpha = 2, 2^{k+2} \text{ при } \alpha \geq 3.$$

6.5. Сравнения с несколькими переменными

Если уравнение $f(x_1, \dots, x_n) = 0$, где $f(x_1, \dots, x_n)$ – многочлен с целыми коэффициентами имеет решение в целых числах, то

$$f(x_1, \dots, x_n) \equiv 0 \ (mod\ m)$$

разрешимо при любом модуле m ($m \in \mathrm{N}$). Так как вопрос о разрешимости сравнения всегда можно решить хотя бы методом перебора (число классов вычетов по mod m конечно и равно m), то отсюда можно получить некоторые необходимые условия для разрешимости уравнения $f(x_1, \dots, x_n) = 0$ в целых числах. Труднее вопрос о достаточности этих условий. Утверждение: «Неопределенное, уравнение разрешимо тогда и только тогда, когда оно разрешимо как сравнение по любому модулю» неверно в общем случае, но справедливо для некоторых частных классов уравнений.

Например, когда $f(x_1, \dots, x_n)$ - форма второй степени и, кроме того, добавлено еще одно необходимое требование - разрешимость уравнения в R. Заметим, что если f - форма, то под разрешимостью уравнения $f = 0$ понимают существование ненулевого решения.

Для модуля $m = {p_1}^{\alpha_1} \dots {p_s}^{\alpha_s}$, где $p_1, \dots, p_s$ - попарно различные

простые числа, $\alpha_1, \ldots, \alpha_s \in \mathrm{N}$, разрешимость сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \ (mod\ m)$$

равносильна разрешимости сравнений

$$f(x_1, \ldots, x_n) \equiv 0 \ (mod\ {p_i}^{\alpha_i})$$

для всех $i = 1, 2, \ldots, s$. Таким образом, разрешимость сравнений для всех модулей m эквивалентна разрешимости этих сравнений только для модулей, являющихся степенями простых чисел. Следовательно, можно зафиксировать простое число p и исследовать вопрос о разрешимости сравнений

$$f(x_1, \ldots, x_n) \equiv 0 \ (mod\ p^k)$$

для всех натуральных показателей k.

6.6 Суммы степеней вычетов

Пусть p - простое число. Классы вычетов по модулю p образуют конечное поле из p элементов. (Обозначим его через Z_p). Всякое сравнение по модулю p можно рассматривать как равенство в этом поле. Следовательно, решение сравнений по mod p равносильно решению уравнений в поле Z_p.

Теорема. *Пусть* $m \in N, S = \sum_{x \bmod p} x^m$, *где* x *пробегает полную систему вычетов по модулю* p. *Тогда*

$$S \equiv \begin{cases} -1\ (mod\ p), \text{если } m \vdots (p-1), \\ 0\ (mod\ p), \text{если } m \text{ не} \vdots (p-1). \end{cases}$$

Доказательство.

1) Пусть $m \vdots (p-1)$. По теореме Ферма для всякого x, не делящегося на p, верно сравнение $x^{p-1} \equiv 1\ (mod\ p)$. Но тогда будет верным и сравнение $x^m \equiv 1\ (mod\ p)$, поэтому

$$S = \sum_{x \bmod p} x^m \equiv \sum_{x \bmod p} 1 + \sum_{x \bmod p} 0 \equiv$$

$$\equiv (p-1) \cdot 1 + 1 \cdot 0 \equiv p - 1 \equiv -1\ (mod\ p)$$

(для $\bar{0} \bmod p$ имеем: $0 \vdots p$, для остальных $\bar{x} \bmod p$ будет выполнено условие: x не $\vdots\ p$).

Следовательно, если $m \vdots (p-1)$, то $S \equiv -1\ (mod\ p)$.

2) Пусть m не делится на $(p-1)$. Тогда

$$(\exists a \in \mathrm{Z})\big((a \text{ не} \vdots p) \wedge \rceil(a^m \equiv 1\ (mod\ p))\big).$$

Так как x пробегает полную систему вычетов по $\bmod p$, то ax также пробегает полную систему вычетов по $\bmod p$, поэтому

$$a^m \cdot S = \sum_{x \bmod p} (ax)^m \equiv S\ (mod\ p).$$

Отсюда получим сравнение:

$$a^m \cdot S - S \equiv S \ (mod\ p),$$

$$(a^m - 1)S \equiv 0 \ (mod\ p).$$

Но $a^m - 1$ не $\vdots\ p$ в силу отрицания: $\rceil(a^m \equiv 1 \ (mod\ p))$. Следовательно, $S \equiv 0 \ (mod\ p)$.

Итак, если m не $\vdots\ (p-1)$, то $S \equiv 0 \ (mod\ p)$.

Следствие. *Пусть* $g(x_1, \dots, x_n)$ *- целочисленный многочлен степени* $< n(p - 1)$. *Тогда имеет место сравнение:*

$$\sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) \equiv 0 \ (mod\ p),$$

где в сумме $x_1, \dots, x_n$ *независимо друг от друга пробегают полную систему вычетов по mod p.*

Доказательство.

Достаточно рассмотреть случай, когда g есть одночлен ${x_1}^{k_1} \dots {x_n}^{k_n}$ для $k_1, \dots, k_n \in \mathrm{N} \cup \{0\}$. Имеем:

$$\sum_{x_1, \dots, x_n} {x_1}^{k_1} \dots {x_n}^{k_n} = \left(\sum_{x_1} {x_1}^{k_1}\right) \dots \left(\sum_{x_n} {x_n}^{k_n}\right).$$

По условию $k_1 + \dots + k_n < n(p-1)$, поэтому хоть при одном l выполнено неравенство $0 \le k_i < p - 1$. Следовательно, хоть одна из

сумм справа будет $\equiv 0\ (mod\ p)$. (в случае $k = 0$ все слагаемые x^k равны 1, включая $x = 0$, поэтому $\sum_x x^k \equiv 0\ (mod\ p)$

Замечание. Мультипликативная группа поля Z_p есть циклическая группа порядка $p - 1$ (ее образующим элементом является класс вычетов, содержащий первообразный корень по mod *p)*. Сумму в теореме поэтому можно интерпретировать как сумму $m - x$ степеней всех корней степени $(p - 1)$ из 1. Если НОД $(p - 1, m) = d$, то такая сумма распадается на d сумм, каждая из которых равна сумме всех корней степени из 1. Утверждение теоремы является по существу следствием того факта, что сумма всех корней степени r из 1 равна 1 при $r = 1$ и равна 0 при $r \geq 2$.

6.7. Теоремы о числе решений сравнений

Теорема Варнинга. *Если степень r целочисленного многочлена $f(x_1, \dots, x_n)$ меньше числа переменных n, то число решений сравнения $f(x_1, \dots, x_n) \equiv 0\ (mod\ p)$ делится на p.*

Доказательство.

Обозначим число решений сравнения $f(x_1, \dots, x_n) \equiv 0\ (mod\ p)$

через k. Рассмотрим многочлен

$$g(x_1, \dots, x_n) = 1 - f^{p-1}(x_1, \dots, x_n)$$

степень которого $< n\,(p - 1)$.

Если $f(a_1, \dots, a_n) \equiv 0\ (mod\ p)$, то $g(a_1, \dots, a_n) \equiv 0\ (mod\ p)$. сли $\neg\big(f(a_1, \dots, a_n) \not\equiv 0\ (mod\ p)\big)$, то $g(a_1, \dots, a_n) \not\equiv 0\ (mod\ p)$. Суммируя все значения $g(x_1, \dots, x_n)$, когда $x_1, \dots, x_n$ независимо друг от друга пробегают полную систему вычетов по mod p, получим, следовательно, сравнение

$$\sum_{x_1,\dots,x_n} g(x_1, \dots, x_n) \equiv k\ (mod\ p).$$

Но тогда, учитывая сравнения $\sum_{x_1,\dots,x_n} g(x_1, \dots, x_n) \equiv 0\ (mod\ p)$, получим, что $k \equiv 0\ (mod\ p)$, а, следовательно, $k \vdots p$. ■

Теорема Шевалле. *Если $f(x_1, \dots, x_n)$ - форма степени $r < n$, то сравнение $f(x_1, \dots, x_n) \equiv 0\ (mod\ p)$ имеет нетривиальное решение.*

Доказательство.

Так как в случае однородного многочлена f степени $r \geq n$ всегда имеется тривиальное решение $x_i \equiv 0\ (mod\ p)$, то для числа решений k

сравнения $f(x_1, \dots, x_n) \equiv 0 \ (mod\ p)$ имеем $k \geq 1$. С другой стороны, по теореме Варнинга $k \equiv 0 \ (mod\ p)$. Следовательно, $k \geq p \geq 2$. ■

Теорема. *Пусть* $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ *целочисленные многочлены степени* $r_1, \dots, r_m$ *соответственно. Если сумма* $r_1 + \cdots + r_m < n$, *то число решений k системы сравнений*

$$\begin{cases} f_1(x_1, \dots, x_n) \equiv 0 \ (mod\ p), \\ \dots \\ f_m(x_1, \dots, x_n) \equiv 0 \ (mod\ p) \end{cases}$$

делится на p.

Доказательство.

Рассмотрим многочлен

$$g(x_1, \dots, x_n) = \prod_{i=1}^{m} \left(1 - f_i^{p-1}(x_1, \dots, x_n)\right)$$

степени $(r_1 + \cdots + r_m)(p-1) < n(p-1)$. Так же, как и при доказательстве теоремы Варнинга, убедимся в том, что

$$\sum_{x_1,\dots,x_n} g(x_1, \dots, x_n) \equiv k \ (mod\ p,$$

следовательно, ввиду сравнения $\sum_{x_1,\dots,x_n} g(x_1, \dots, x_n) \equiv 0 \ (mod\ p)$ будет $k \equiv 0 \ (mod\ p)$, то есть $k \vdots p$. ■

6.8. Квадратичные формы по простому модулю

Рассмотрим случай квадратичных форм.

Теорема. *Пусть* $f(x_1, \dots, x_n)$ - *целочисленная квадратичная форма. Если* $n \geq 3$, *то сравнение* $f(x_1, \dots, x_n) \equiv 0 \pmod p$ *имеет ненулевое решение.*

Доказательство.

Доказательство вытекает из теоремы Шевалле. ■

Рассмотрим оставшийся случай бинарных квадратичных форм. Будем считать, что $p \neq 2$ (при $n = 2, p = 2$ можно непосредственно перебрать все имеющиеся квадратичные формы).

В этом случае форма может быть записана в виде $f(x, y) = ax^2 + 2bxy + cy^2$. Ее определитель $(ac - b^2$ обозначим через *d.*

Теорема. *Сравнение*

$$f(x, y) \equiv 0 \pmod p,$$

где $p \neq 2$, *тогда и только тогда имеет ненулевое решение, когда (-d)) или делится на p, или является квадратичным вычетом по mod p.*

Доказательство.

Для двух форм f и f_1, эквивалентных в поле Z_p сравнения или одновременно имеют, или одновременно не имеют ненулевое решение.

Так как, кроме того, при переходе к эквивалентной форме ее определитель умножается на квадрат ненулевого элемента поля Z_p, то можно заменить форму f любой, ей эквивалентной. Всякая форма эквивалентна диагональной форме, поэтому можно считать, что $f(x,y) = ax^2 + cy^2, d = ac$.

Если $a \vdots p$ или $c \vdots p$, то теорема верна. Если ac не $\vdots p$ и сравнение имеет ненулевое решение (x_0, y_0), то из верного сравнения $ax_0{}^2 + cy_0{}^2 \equiv (mod\ p)$ получим

$$-ac \equiv \left(\frac{cy_0}{x_0}\right)^2 \ (mod\ p)$$

(дробь $w \equiv \frac{u}{v}\ (mod\ p)$ означает результат деления в поле Z_p, то есть решение сравнения $vw \equiv u\ (mod\ p)$).

Таким образом, $\left(\frac{-d}{p}\right) = 1$ и $-ac \equiv (u)^2\ (mod\ p)$, то можно положить $(x_0, y_0) = (u, a)$. ■

Замечание. (*О квадратичных формах) Квадратичной формой над полем F называется однородный многочлен второй степени с коэффициентами из F. Всякую квадратичную форму можно записать в виде*

$$f = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

где $a_{ij} = a_{ji}$. *Симметрическая матрица* $A = (a_{ij})$ *называется матрицей квадратичной формы* f. *Заданием своей матрицы квадратичная форма вполне определена с точностью до наименования переменных. Определитель d,* $d = |A|$, *называемая определителем квадратичной формы* f. *Если* $d = 0$, *то форма* f *называется особенной, если* $d \neq 0$, *то* f *- неособенная.*

Две квадратичные формы f и g называются *эквивалентными*, если существует неособенное линейное преобразование переменных, при котором одна из этих форм переходит и другую (с точностью до наименования переменных). Запись $f \sim g$. Всякая квадратичная форма эквивалентна диагональной форме. Определители эквивалентных квадратичных форм отличаются друг от друга на ненулевой множитель, являющийся квадратом в поле *F*.

Упражнения

1. Среди вычетов приведенной системы по mod 23 указать квадратичные вычеты.
2. Среди вычетов приведенной системы по mod 37 указать квадратичные невычеты.
3. Указать число решений сравнений:

   1) $x^2 \equiv 3\ (mod\ 31)$, 2) $x^2 \equiv 2\ (mod\ 31)$.
4. Указать число решений сравнений:

   1) $x^2 \equiv 5\ (mod\ 73)$, 2) $x^2 \equiv 3\ (mod\ 73)$.
5. Вычисляя символ Якоби, указать число решений сравнений:

   1) $x^2 \equiv 226\ (mod\ 563)$, 2) $x^2 \equiv 429\ (mod\ 563)$.
6. Указать число решений сравнений:

   1) $x^2 \equiv 3766\ (mod\ 5987)$, 2) $x^2 \equiv 3149\ (mod\ 5987)$.
7. Применяя различные способы, решить сравнения:

   1) $x^2 \equiv 5\ (mod\ 19)$, 2) $x^2 \equiv 5\ (mod\ 29)$, 3) $x^2 \equiv 2\ (mod\ 97)$.
8. Решить сравнения:

   1) $x^2 \equiv 2\ (mod\ 311)$, 2) $x^2 \equiv 3\ (mod\ 277)$.
9. Решить сравнение $x^2 \equiv 59\ (mod\ 125)$ разными способами.

10. Решить сравнение $x^2 \equiv 91\ (mod\ 243)$.
11. Решить сравнение $x^2 \equiv 41\ (mod\ 64)$, разными способами.
12. Решить сравнение $x^2 \equiv 145\ (mod\ 256)$.
13. Пользуясь таблицей индексов, найти классы вычетов 6-й степени по модулю $p = 11$.
14. Пользуясь таблицей индексов, решить $13x^{21} \equiv 5\ (mod\ 31$.
15. Пользуясь таблицей индексов, найти все числа *a,* такие, что $a^6 \equiv 1\ (mod\ 49)$.
16. Пользуясь таблицей индексов, решить $7x^6 \equiv 23\ (mod\ 64)$.
17. Определить число квадратных корней из 1 по модулю *m,* если:

    a) $m = 600$; b) $m = 18$; c) $\frac{p-1}{2} = \frac{10}{2} = 5$.
18. Найти классы квадратичных вычетов по mod $p = 17$.
19. Существуют ли значения ж, такие, чтобы $x^2 + 1 \vdots 127$?
20. $5^2 \equiv 2\ (mod\ 23)$. Пользуясь тем, что 2 - квадратичный вычет по $mod\ p = 23$, найти все классы квадратичных вычетов по этому модулю.
21. Имеет ли решение сравнение $x^2 \equiv 6\ (mod\ 19)$?

22. Существует ли целое число x, такое, что $x^2 - 2$ делится на 79?

23. Имеет ли решение сравнение:

a) $x^2 \equiv 68 \ (mod\ 113)$;

b) $x^2 \equiv 310 \ (mod\ 521)$;

c) $x^2 \equiv -174 \ (mod\ 619)$?

24. Для каких простых чисел $p > 2$ сравнение $x^2 \equiv 3 \ (mod\ p)$ имеет решение?

25. Определить, какие простые множители могут быть у чисел вида $x^2 + 6$.

26. Разложить на простые множители число

$$10541 = 3 \cdot 59^2 + 2 \cdot 7^2.$$

27. Имеет ли решение сравнение $x^2 \equiv 506 \ (mod\ 1103)$?

28. Решить сравнение $x^2 \equiv 3 \ (mod\ 11^3)$?

29. Решить сравнение $x^2 + 71 \equiv 0 \ (mod\ 128)$?

30. Имеет ли решение сравнение $x^2 \equiv 903 \ (mod\ 2111)$?

31. С помощью критерия Эйлера установить, какие из чисел 3, 5, 7, 8, 11 являются квадратичными вычетами по модулю 13.

32. С помощью критерия Эйлера установить, какие из чисел 5, 6. 7, 8, 10 являются квадратичными невычетами по модулю 17.

33. Доказать, что для символа Лежандра справедливо свойство $\left(\frac{q^n}{p}\right)=\left(\frac{q}{p}\right)^n$.

34. С помощью символа Лежандра установить, имеют ли решения сравнения:

a) $x^2 \equiv 104 (\mathrm{mod}\, 321)$;

b) $x^2 \equiv 219 (\mathrm{mod}\, 383)$;

c) $x^2 \equiv 231 (\mathrm{mod}\, 101)$;

d) $x^2 \equiv 65 (\mathrm{mod}\, 193)$.

35. Символ Якоби $\left(\frac{a}{m}\right)$ для нечетного $m=p_1 p_2 \ldots p_k$, где p_i – числа простые, среди которых могут быть и равные, и $(a, m)=1$, определяется равенством

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a_n}{p_k}\right),$$

где $\left(\frac{a}{p_i}\right)$ - символы Лежандра. Доказать, что символ Якоби обладает всеми свойствами символа Лежандра.

свойствами символа Лежандра.

36. Применить символ Якоби к исследованию уравнений:

a) $x^2 \equiv 903 (\mathrm{mod}\, 2111)$;

b) $x^2 \equiv 219 (\mathrm{mod}\, 383)$;

c) $x^2 \equiv 7 (\mathrm{mod}\, 2003)$.

37. Решить уравнени $\left(\frac{a}{21}\right) = 1$, где $\left(\frac{a}{21}\right)$ - символ Якоби.

ГЛАВА 7. АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

7.1. Основные понятия

Определение. *Критерий, устанавливающий необходимое и достаточное условия делимости произвольного натурального числа n на данное натуральное число m, называется признаком делимости на m.*

Широкое практическое значение имеют следующие свойства:

- *Если остаток от деления a_1 на b равен r_1, а остаток от деления a_2 на b равен r_2, то остаток от деления $a_1 + a_2$ на b равен остатку от деления $r_1 + r_2$ на b.*
- *Если остаток от деления a_1 на b равен r_1, а остаток от деления a_2 на b равен r_2, то остаток от деления $a_1 \cdot a_2$ на равен остатку от деления $r_1 \cdot r_2$ на b.*

На основе данных свойств выводятся признаки делимости на *d*. Пусть число *a* представлено в десятичной системе счисления

$$a = \sum_{i=0}^{n} 10^n a_i.$$

Используя свойства 1,2 и сравнения получим признаки делимости.

Признак делимости на 2.

$$a \equiv a_0 \,(\, mod\ 2).$$

На 2 делятся все те натуральные числа, запись которых оканчивается четной цифрой. Если запись числа оканчивается нечетной цифрой, то число не делится на 2.

Признак делимости на 3.

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \,(\, mod\ 3).$$

На 3 делятся все те натуральные числа, сумма цифр которого делится на 3. Более того, остаток числа при делении на 3 равен остатку суммы его цифр при делении на 3.

Признак делимости на 4.

$$a \equiv 2a_1 + a_0 \,(\, mod\ 4).$$

На 4 делятся все те натуральные числа, сумма удвоенной предпоследней цифры и последней цифры которого делится на 4. Более того, остаток числа при делении на 4 равен остатку суммы удвоенной предпоследней цифры и последней цифры при делении на 4.

Признак делимости на 5.

$$a \equiv a_0 \,(\, mod\ 5).$$

На 5 делятся все те натуральные числа, последней цифра которого делится на 5 Более того, остаток числа при делении на 5 равен остатку последней цифры при делении на 5.

На 5 делятся все те натуральные числа, запись которых оканчивается цифрой 0 или цифрой 5.

Признак делимости на 6.

$$a \equiv 4a_n + \cdots + 4a_2 + 4a_1 + a_0 \ (mod\ 6).$$

На 6 делятся все те натуральные числа, сумма всех цифр без последней, умноженных на 4, и последней цифры которого делится на 6. Более того, остаток числа при делении на 6 равен остатку суммы всех цифр без последней, умноженных на 4, и последней цифры при делении на 4.

Признак делимости на 8.

$$a \equiv 4a_2 + 2a_1 + a_0 \ (mod\ 8).$$

На 8 делятся все те натуральные числа, сумма учетверенной цифры из разряда сотен, удвоенной цифры из разряда десятков и последней цифры которого делится на 8. Более того, остаток числа при делении на 8 равен остатку суммы учетверенной цифры из разряда

сотен, удвоенной цифры из разряда десятков и последней цифры при делении на 8.

Признак делимости на 9.

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \ (mod\ 9).$$

На 3 делятся все те натуральные числа, сумма цифр которого делится на 9. Более того, остаток числа при делении на 9 равен остатку суммы его цифр при делении на 9.

Признак делимости на 10.

$$a \equiv a_0 \ (mod\ 10).$$

На 10 делятся все те натуральные числа, последней цифра которого делится на 10 Более того, остаток числа при делении на 10 равен остатку последней цифры при делении на 10.

На 10 делятся все те натуральные числа, запись которых оканчивается цифрой 0.

Признак делимости на 11.

$$a \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \cdots + a_2 - a_1 + a_0 \ (mod\ 11).$$

На 11 делятся все те натуральные числа, разность суммы цифр, стоящих на позициях четных разрядов, и суммы цифр, стоящих на по-

зициях нечетных разрядов, делится на 11. Более того, остаток числа при делении на 11 равен остатку разности суммы цифр, стоящих на позициях четных разрядов, и суммы цифр, стоящих на позициях нечетных разрядов, при делении на 11.

7.2. Признак делимости на число, взаимно простое с 10

Теорема. *Пусть m и n- натуральные числа, НОД* $(m, 10) = 1$ *и k - наименьшее натуральное число, для которого справедливо*

$$10^k \equiv 1 \ (mod\ m).$$

Тогда n делится на m тогда и только тогда, когда на m делится сумма чисел, которые получаются при разбиении справа налево цифровой записи числа n на грани по k цифр в каждой грани.

Доказательство.

1) Запишем число n в системе счисления с основанием $g = 10^k$, где k определено в условии теоремы, то есть k есть наименьшее натуральное число, для которого сравнение $10^k \equiv 1 \ (mod\ m)$ верно.

$$n = a_s(10^k)^s + a_{s-1}(10^k)^{s-1} + \cdots + a_1(10^k)^1 + a_0,$$

где $s \in \mathrm{N} \cup \{0\}, a_i \in \{0, 1, \ldots, (10^k - 1)\}, i = 0,1, \ldots, s$, причем, $a_s \neq 0$.

По свойству сравнений, если $a = b \pmod m$, и $n \in \mathrm{N}$, то имеем $a^n \equiv b^n \ (mod\ m)$, получим следующие верные сравнения:

$$10^k \equiv 1 \ (mod\ m),$$

$$(10^k)^2 \equiv 1^2 (mod\ m),$$

$$\ldots$$

$$(10^k)^s \equiv 1^s (mod\ m).$$

Умножим почленно соответственно на $a_1, a_2, \ldots, a_s$ сравнения, поменяем их местами и добавим еще одно верное сравнение:

$$a_s(10^k)^s \equiv a_s (mod\ m),$$

$$\ldots$$

$$a_1(10^k)^1 \equiv a_1 (mod\ m),$$

$$a_0 \equiv a_0 (mod\ m).$$

Сложим почленно полученные сравнения:

$$a_s(10^k)^s + a_{s-1}(10^k)^{s-1} + \cdots + a_1(10^k)^1 + a_0 \equiv$$

$$\equiv a_s + a_{s-1} + \cdots + a_1 + a_0 (mod\ m).$$

Учитывая теперь равенство

$n = a_s(10^k)^s + a_{s-1}(10^k)^{s-1} + \cdots + a_1(10^k)^1 + a_0$, тогда

$$n \equiv a_s + a_{s-1} + \cdots + a_1 + a_0 (mod\ m).$$

Из данного сравнения следует, что натуральное число n и число $(a_s + a_{s-1} + \cdots + a_1 + a_0)$ имеют одинаковые остатки от деления на m. Следовательно, $n \vdots m$ тогда и только тогда, когда на m делится сумма

$$a_s + a_{s-1} + \cdots + a_1 + a_0.$$

2) Из равенства $n = a_s(10^k)^s + a_{s-1}(10^k)^{s-1} + \cdots + a_1(10^k)^1 + a_0$ имеем: число a_0 равно остатку от деления числа n на 10^k, то есть имеет цифры, одинаковые с последними k цифрами записи числа n.

a_1 - число, равное остатку от деления числа $\frac{n-a_0}{10^k}$ на 10^k,то есть имеет цифры, одинаковые с цифрами из предпоследней грани из k цифр. И так далее.

Таким образом, $a_0, a_1, a_2, \ldots, a_s$ - числа, которые получаются при разбиении справа налево цифровой записи числа n на грани по k цифр в каждой грани.

Примеры. Запишем натуральные числа до 11, для которых

НОД $(m, 10) = 1$: 1,3,7,9,11.

1) m=3. Найдем наименьшее натуральное число k, такое, что

$$10^k \equiv 1 \ (mod\ 3).$$

Таким числом k будет k=1, так как $10^1 - 1 = 9,9 : 3$, следовательно, $10^1 = 1$ (mod 3) верно. Тогда, применяя доказанную теорему, получим следующий признак делимости на 3:

Натуральное число n делится на 3 тогда и только тогда, когда на 3 делится сумма чисел, которые получаются при разбиении справа налево цифровой записи числа n на грани по одной цифре в каждой грани, то есть n⋮3 тогда и только тогда, когда на 3 делится сумма цифр числа n.

Например, n = 1272, 1+2+7+2=12, 12⋮3, следовательно, 1272⋮3.

2) m=9. Наименьшее натуральное число k, для которого сравнение

$$10^k \equiv 1 \ (mod\ 9),$$

k=1, так как 10^1-1=9, 9⋮9, следовательно, сравнение $10^1 \equiv 1 \ (mod\ 9)$ верно. Тогда, применяя доказанную теорему, получим следующий признак делимости на 9:

Натуральное число n делится на 9 тогда и только тогда, когда на 9 делится сумма цифр числа n.

Например, n = 936, 9+3+6=18, 18⋮9, следовательно, 936⋮9.

Кафедра ФМО и ИТ

3) $m = 11 \cdot 10^k \equiv 1 \ (mod\ 11)$, k - наименьшее натуральное число, для которого сравнение верно.

$10^1 - 1 = 9$, 9 не делится на 11, $10^2 - 1 = 99$, $99 \vdots 11$, следовательно, $10^2 = 1 \pmod{11}$ верно, поэтому наименьшее искомое число $k = 2$.

Натуральное число n делится на 11 тогда и только тогда, когда на 11 делится сумма чисел, которые получаются при разбиении справа налево цифровой записи числа n на грани по 2 цифры в каждой грани.

Например, $n = 2354$, $23 + 54 = 77$, $77 \vdots 11 \Rightarrow 2354 \vdots 11$. $n = 4328$, $43 + 28 = 71$, 71 не делится на11 => 4328 не делится на 11.

4) $m = 7$.

$$10^k \equiv 1 \ (mod\ 7),$$

k - наименьшее натуральное число, для которого сравнение верно.

k	$10^k - 1$	остаток r
1	9	2
2	99	1
3	999	5
4	9999	3
5	99999	4
6	999999	0

Следовательно, k=6, $10^6 \equiv 1(mod\ 7)$.

Натуральное число n делится на 7 тогда и только тогда, когда на 7 делится сумма чисел, которые получаются при разбиении справа налево цифровой записи числа n на грани по 6 цифр в каждой грани.

Например, 342217344, 342+217344=217686, 217686:7, следовательно, n: 7.

На практике полученным признаком для m = 7 пользоваться неудобно.

7.3. Признак делимости, сводящийся к знакопеременной сумме

Теорема. *Пусть* $m, n \in \mathrm{N}$, *НОД(m,* 10) = 1, l *- наименьшее натуральное число, для которого* $10^l \equiv -1(mod\ m)$. *Тогда n делится на m тогда и только тогда, когда на m делится сумма, взятых попеременно со знаками (+) и (-) чисел, которые получаются при разбиении справа налево цифровой записи числа n на грани по l цифр в каждой грани.*

Доказательство.

1) Запишем число n в системе счисления с основанием $g = 10^l$, где l определено в условии теоремы.

$$n = a_s(10^l)^s + a_{s-1}(10^l)^{s-1} + \cdots + a_1(10^l)^1 + a_0,$$

где $s \in \mathrm{N} \cup \{0\}, a_i \in \{0, 1, \ldots, (10^l - 1)\}, i = 0,1, \ldots, s,$ причем, $a_s \neq 0$.

Применяя свойства сравнений, получим следующие сравнения:

$$10^l \equiv -1\ (mod\ m),$$

$$(10^l)^2 \equiv (-1)^2 (mod\ m),$$

$$\ldots$$

$$(10^l)^s \equiv (-1)^s (mod\ m).$$

Умножим почленно каждое сравнение на $a_1, a_2, \dots, a_s$ соответственно и добавим еще одно сравнение, тогда получим:

$$a_s(10^l)^s \equiv a_s(-1)^s (mod\ m),$$

$$\dots$$

$$a_1(10^l)^1 \equiv a_1(-1)^1 (mod\ m),$$

$$a_0 \equiv a_0 (mod\ m).$$

Сложим почленно полученные сравнения, тогда получим сравнение:

$$a_s(10^l)^s + a_{s-1}(10^l)^{s-1} + \dots + a_1(10^l)^1 + a_0 \equiv$$

$$\equiv (-1)^s a_s + (-1)^{s-1} a_{s-1} + \dots - a_1 + a_0 (mod\ m).$$

Учитывая теперь равенство

$$n = a_s(10^l)^s + a_{s-1}(10^l)^{s-1} + \dots + a_1(10^l)^1 + a_0,$$

получим, что

$$n \equiv (-1)^s a_s + (-1)^{s-1} a_{s-1} + \dots - a_1 + a_0 (mod\ m).$$

Из данного сравнения следует, что натуральное число n и число $((-1)^s a_s + (-1)^{s-1} a_{s-1} + \dots - a_1 + a_0)$ имеют одинаковые остатки от деления на m.

Следовательно, $n \vdots m$ тогда и только тогда, когда на m делится знакопеременная сумма $(-1)^s a_s + (-1)^{s-1} a_{s-1} + \dots - a_1 + a_0$.

2) Из равенства $n = a_s(10^l)^s + a_{s-1}(10^l)^{s-1} + \cdots + a_1(10^l)^1 + a_0$ имеем: число a_0 равно остатку от деления числа *n* на 10^l, то есть имеет цифры, одинаковые с последними *l* цифрами записи числа *n*.

a_1 - число, равное остатку от деления числа $\frac{n-a_0}{10^l}$ на 10^l, то есть имеет цифры, одинаковые с цифрами из предпоследней грани из *l* цифр. И так далее.

Таким образом, $a_0, a_1, a_2, \ldots, a_s$ - числа, которые получаются при разбиении справа налево цифровой записи числа *n* на грани по *l* цифр в каждой грани.

Примеры. 1) $m = 11$.

Найдем наименьшее натуральное для которого $10^l \equiv -1\ (mod\ 11)$. Если $l = 1$, то $10^l - (-1) = 10^1 + 1 = 11$, $11 \vdots 11$, следовательно, $10^1 \equiv -1\ (mod\ 11)$ - верное сравнение. Тогда применяя доказанную теорему, получим признак делимости на 11.

Натуральное число n делится на 11 тогда и только тогда, когда на 11 делится сумма цифр числа n, взятых попеременно со знаками (+) и (-).

Например, n = 2354, 4-5+3-2=0, 0:11 => 2354:11.

n = 4328, 8-24-3-4=5, 5 /11 => 4328 не делится на11.

2) m=7. Найдем наименьшее натуральное число l, для которого $10^l \equiv -1\ (mod\ 7)$.

l	$10^l + 1$	остаток
1	11	4
2	101	3
3	1001	0

Следовательно, при l= 3 сравнение $10^3 \equiv -1\ (mod\ 7)$ является верным. Тогда получим следующий признак делимости на 7.

Натуральное число n делится на 7 тогда и только тогда, когда на 7 делится сумма взятых попеременно со знаками (+) и (-) чисел, которые получаются при разбиении справа налево цифровой записи числа n на грани, по 3 цифры в каждой грани.

Например, n= 342217344, 344-217+342=469, 469:7 => n:7.

n = 1345, 345-1 = 344, 344 не делится на 7 => n не делится на 7.

7.4. Признак делимости на 2^m(или на 5^m)

Теорема. *Пусть m, n* ∈ N. *Тогда число n делится на* 2^m *(или на* 5^m*) тогда и только тогда, когда на* 2^m *(соответственно на* 5^m*) делится число, имеющее те же цифры, что и последние m цифр записи числа n.*

Доказательство.

Разделим число n на 10^m с остатком. По теореме о делении с остатком имеем:

$$(\exists!\, q, r \in \mathrm{Z})\ \big((n = 10^m \cdot q + r) \wedge (0 \le r \le 10^m)\big)$$

Отсюда получим, учитывая, что 10 = 2·5:

1) Если $n \vdots 2^m$, то $r \vdots 2^m$. И обратно, если $r \vdots 2^m$, то и $n \vdots 2^m$.
2) Если $n \vdots 5^m$, *то* $r \vdots 5^m$. Обратно, если $r \vdots 2^m$, то и $n \vdots 2^m$.

Следовательно, $n \vdots 2^m$тогда и только тогда, когда $r \vdots 2^m$.

Аналогично, $n \vdots 5^m$тогда и только тогда, когда $r \vdots 5^m$.

Но остаток r есть число, цифры которого такие же, как и последние m цифр записи числа n.

Примеры. 1) $m = 1$, $2^1 = 2$, получим признак делимости на 2:

$n \vdots 2$ тогда и только тогда, когда последняя цифра делится на 2 (то есть когда последняя цифра четная).

$m = 2$, $2^2 = 4$, получим признак делимости на 4:

$n \vdots 4$ тогда и только тогда, когда на 4 делится число, имеющие те же цифры, что и последние две цифры числа n.

Например, $n = 232$, 32:4 => 232⋮4. $n = 446$, 46 не делится на 4 => 446 не делится на 4.

2) $m = 1$, $5^1 = 5$, получим признак делимости на 5:

$n \vdots 5$ тогда и только тогда, когда последняя цифра делится на 5 (то есть когда число оканчивается 0 или 5).

$m = 2$, $5^2 = 25$, получим признак делимости на 25:

$n \vdots 25$ тогда и только тогда, когда на 25 делится число, имеющее те же цифры, что и последние две цифры числа n.

Например, $n = 625$, 25⋮25 => 625⋮25.

$n = 345$, 45 не делится на 25 => 345 не делится на 25.

Аналогично из доказанной теоремы можно получить признак делимости на 2^3, на 5^3 (то есть на 8, на 125). И так далее.

7.5. Признак делимости Паскаля

Общий признак делимости выражает правило, с помощью которого по цифрам числа *n*, записанного в системе счисления с основанием д, можно сделать вывод о делимости его на другое натуральное число *m*.

Теорема. *Пусть n записано в системе счисления с основанием g:*

$$n = a_s g^s + a_{s-1} g^{s-1} + \cdots + a_1 g + a_0,$$

где $m \in \mathrm{N}, g \in \mathrm{N}\backslash\{1\}, s \in \mathrm{N} \cup \{0\}, a_1 \in \{0, 1, \ldots, (g-1)\}$,

$i = 0, 1, \ldots, s$, *причем,* $a_s \neq 0$, *и пусть целые числа* $b_0, b_1, \ldots, b_s$,

$$b_0 = 1, b_1 \equiv g^1 (mod\ m), \ldots, b_s \equiv g^s (mod\ m).$$

Тогда n делится на m тогда и только тогда, когда на m делится число $(a_s b_s + a_{s-1} b_{s-1} + \cdots + a_1 b_1 + a_0 b_0)$.

Доказательство.

Из условия теоремы получим следующие верные сравнения:

$$g^s \equiv b_s (mod\ m),$$

$$g^{s-1} \equiv b_{s-1} (mod\ m),$$

$$\ldots$$

$$g^1 \equiv b_1 (mod\ m).$$

Умножим почленно каждое из сравнений соответственно на $a_s, a_{s-1}, \dots, a_1$ и добавим одно верное сравнение $a_0 \equiv a_0 b_0 (\,mod\, m)$, тогда получим:

$$a_s g^s \equiv a_s b_s (mod\ m),$$
$$a_{s-1} g^{s-1} \equiv a_{s-1} b_{s-1} (mod\ m),$$
$$\dots$$
$$a_1 g \equiv a_1 b_1 (mod\ m),$$
$$a_0 \equiv a_0 b_0 (mod\ m).$$

Сложим почленно теперь полученные сравнения:

$$a_s g^s + a_{s-1} g^{s-1} + \dots + a_1 g + a_0 \equiv a_s b_s + a_{s-1} b_{s-1} + \dots + a_1 b_1 + a_0 b_0 (mod\ m)$$

Учитывая равенство $n = a_s g^s + a_{s-1} g^{s-1} + \dots + a_1 g + a_0$, из последнего сравнения получим сравнение:

$$n \equiv a_s b_s + a_{s-1} b_{s-1} + \dots + a_1 b_1 + a_0 b_0 (mod\ m).$$

Отсюда получим, что числа n и $(a_s b_s + a_{s-1} b_{s-1} + \dots + a_1 b_1 + a_0 b_0)$ имеют одинаковые остатки от деления на m. Следовательно, число n делится на натуральное число m тогда и только тогда, когда на m делится число $a_s b_s + a_{s-1} b_{s-1} + \dots + a_1 b_1 + a_0 b_0$.

Заметим, что признак делимости на число, взаимно простое с 10 и признак делимости, сводящийся к знакоопределенной сумме, являются частными случаями признака делимости Паскаля и получаются из него соответственно при

1) $g = 10^k, b_0 = b_1 = \cdots = b_s = 1$, где k - наименьшее натуральное число, для которого $10^k \equiv 1\ (mod\ m)$,

2) $g = 10^l$, где l - наименьшее натуральное число, для которого $10^l \equiv -1\ (mod\ m)$, $b_0 = 1, b_1 = -1, b_2 = 1, \ldots, b_s = (-1)^s$.

Из доказанной теоремы получим следующую схему для получения признака делимости в десятичной системе счисления (то есть при $g = 10$):

1) Найти остатки от деления степеней числа 10 на m - это будут числа b_i, i = 0, ...,s. Или взять не сами остатки в качестве чисел b_i, а числа, сравнимые с ними по модулю 10, т.е. $b_i \equiv r_i\ (mod\ 10)$.

2) Составить алгебраическую сумму $\sum_{i=0}^{s} a_i b_i$ и проверить делимость суммы на m.

Пример. g= 10, 1) m = 7. Получим признак делимости на 7.

$b_0 = 1,$

$b_1 \equiv 10^1 \ (mod\ 7),$

$b_2 \equiv 10^2 \ (mod\ 7),$

$b_3 \equiv 10^3 \ (mod\ 7),$

$b_4 \equiv 10^4 \ (mod\ 7)$, и так далее.

Заменим числа 10^1, 10^2, 10^3, 10^4 остатками от деления на 7, получим следующие сравнения:

$b_1 \equiv 3 \ (mod\ 7,$

$b_2 \equiv 2 \ (mod\ 7),$

$b_3 \equiv 6 \ (mod\ 7) \equiv -1 \ (mod\ 7),$

$b_4 \equiv 4 \ (mod\ 7) \equiv -3 \ (mod\ 7).$

Следовательно, получим признак делимости на 7:

n ⋮ 7 тогда и только тогда, когда на 7 делится число

$$a_s b_s + a_{s-1} b_{s-1} + \cdots + a_4(-3) + a_3(-1) + a_2 \cdot 2 + a_1 \cdot 3 + a_0 \cdot 1.$$

Например, если n=4251, то $a_0 = 6, a_1 = 5, a_2 = 2, a_3 = 4, s = 3,$ алгебраическая сумма будет

$$a_3(-1) + a_2 \cdot 2 + a_1 \cdot 3 + a_0 \cdot 1 = 4(-1) + 2 \cdot 2 + 5 \cdot 3 + 6 \cdot 1 = 21.$$

Так как 21⋮ 7, то, следовательно, 4256⋮ 7.

2) $m = 11$. Получим признак делимости на 11.

$b_0 = 1$,

$b_1 \equiv 10^1 \ (mod\ 11)$,

$b_2 \equiv 10^2 \ (mod\ 11)$,

$b_3 \equiv 10^3 \ (mod\ 11)$,

$b_4 \equiv 10^4 \ (mod\ 11)$, и так далее.

Заменим числа 10^1, 10^2, 10^3, 10^4 остатками от деления на 11, получим следующие сравнения:

$b_1 \equiv 10 \ (mod\ 11) \equiv -1 (\ mod\ 11)$,

$b_2 \equiv 1 \ (mod\ 11)$,

$b_3 \equiv 10 \ (mod\ 11) \equiv -1 \ (mod\ 11)$,

$b_4 \equiv 1 \ (mod\ 7)$.

Следовательно, получим признак делимости на 11:

n ⋮ 11 тогда и только тогда, когда на 11 делится число

$$a_s b_s + a_{s-1} b_{s-1} + \cdots + a_4 \cdot 1 + a_3 (-1) + a_2 \cdot 1 + a_1 \cdot (-1) + a_0 \cdot 1.$$

Например, если n=451, то $a_0 = 1, a_1 = 5, a_2 = 4$, $s = 2$, алгебраическая сумма будет

$a_2 \cdot 1 + a_1 \cdot (-1) + a_0 \cdot 1 = 4 \cdot 1 + 5 \cdot (-1) + 1 \cdot 1 = 0.$

Так как 0⋮11, то, следовательно, 451⋮11.

Если n=37891, то $a_0 = 1, a_1 = 9, a_2 = 8, a_3 = 7,\ a_4 = 3, s = 4$, алгебраическая сумма будет

$$a_4 \cdot 1 + a_3 (-1) + a_2 \cdot 1 + a_1 \cdot (-1) + a_0 \cdot 1 = 3 \cdot 1 + 7(-1) + 8 \cdot 1 + +9 \cdot (-1) + 1 \cdot 1 = -4.$$

Так как (-4) не делится на 11, то, следовательно, 37891 не делится на 11.

Заметим, что здесь в признаке делимости на 11 остатки от деления степеней 10^1, 10^2, 10^3, 10^4, ..., 10^s на 11 будут соответственно равны 10, 1, 10, 1, ... , то есть при замене числа 10 на (-1) получим, что числа $b_0, b_1, b_2, \ldots, b_s$ будут состоять из единиц с чередующимися знаками: 1, -1, 1, -1, 1, ..., следовательно, признак делимости на 11 в этом случае можно сформулировать так:

n⋮11 тогда и только тогда, когда на 11 делится числа, равное знакопеременной сумме

$$a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^s a_s.$$

Для n=451 составим алгебраическую сумму 1-5+4=0, 0⋮11 => 451⋮11.

Если n=37891, то составим алгебраическую сумму 1-9+8-7+3=-4, -4 не делится на 11 => 37891 не делится 11.

7.6. Проверка арифметических действий

Выберем некоторый модуль m и заменим большие числа $a, b, c, ...$, над которыми надо производить арифметические действия, небольшими числами $a', b', c', ...,$ ', сравнимыми с ними по модулю m.

Выполним действия над $, b, c, ...$, а затем такие же действия над $a', b', c', ...$ Если действия выполнены правильно, то результаты этих действий (S и S') должны быть сравнимы: $S \equiv S'(mod\ m)$.

Для проверки частного $\frac{a}{b} = c\ (b \neq 0)$ представим равенство в виде $a = bc$.

Применение такого способа проверки имеет смысл только тогда, когда такие числа $a', b', ...,$ можно найти легко и быстро. Для этого в качестве m берут 9 или 11. Каждое число (в десятичной системе счисления) сравнимо с суммой его цифр по mod 9. Поэтому получим *способ проверки* с помощью девятки:

Вычислить остаток от деления на 9 суммы цифр каждого числа. Это и будут $a', b', \ldots$. Результаты (S и S') будут отличаться на число, кратное девяти.

Заметим, что если ошибка такая, что разность $S - S'$ кратна 9, то ошибка при таком способе проверки не будет замечена.

По модулю $m = 11$ каждое число (в десятичной системе счисления) будет сравнимо с суммой цифр, взятых справа налево попеременно со знаками (+) и (-). Поэтому *получим способ проверки* с помощью одиннадцати:

Вычислить остаток от деления на *11 суммы цифр, взятых попеременно справа налево со знаками (+) и (-). Результаты (S и S') будут отличаться на число, кратное 11.*

Если ошибка кратна 11, она не будет замечена при таком способе проверки действий.

При сложных вычислениях лучше проводить две проверки: одну с помощью модуля 9, другую - с помощью модуля 11. Тогда ошибка не будет замечена, если она кратна 99 (что бывает редко).

Примеры. 1) 73416·8539 = 626899224.

m= 9, 7 + 3 + 4+1 + 6 = 21, 21 ≡ 3 (*mod* 9)

8+ 5 + 3 + 9 = 25, 25 ≡ 7 (*mod* 9), 3·7 = 21

6+ 2+6+8+9 + 9 + 2 + 2+4 = 48, 48 ≡ 21 (*mod* 9) - верно.

Следовательно, 48 отличается от 21 на число, кратное 9, поэтому результат умножения верен.

2)$(3197)^3$ = 32675926373,

7- 9 + 1 - 3 = -4, -4 ≡ 7 (*mod* 11), 7·7·7 = 343.

3- 7 + 3 - 6 + 2 - 9 + 5 - 7 + 6 - 2 + 3 = -9, 343 ≡ -9 (*mod* 11) - верно, так как 352⋮11.

Следовательно, 343 отличается от (-9) на число, кратное 11, поэтому результат возведения в степень верен.

7.7. Признаки делимости квадратов и кубов целых чисел

Пример 1. Докажите, что квадрат целого числа не может иметь вид $4k + 2, k \epsilon Z$

Заметим, что числа вида $4k + 2$ при делении на 4 имеют остаток 2. Рассмотрим всевозможные остатки квадратов целых чисел при делении на 4.

a	0	1	2	3
a^2	0	1	0	1

Квадраты целых чисел при делении на 4 могут иметь лишь остатки 0 или 1. А потому они не могут иметь вид 4k + 2. На языке теории сравнения решение можно оформить так:

$$4k + 2 \equiv 2 \ (mod\ 4),$$

$$a^2 \equiv \{0; 1\} \ (mod\ 4).$$

Следовательно, квадрат целого числа не может иметь вид $4k + 2$.

Пример 2. Докажите, что сумма кубов трех последовательных целых чисел делится на 3.

Доказать этот факт можно разными способами. Применим подход,

использованный выше. Составим таблицу остатков для трех последовательных чисел $f(a) = a^3+(a+1)^3 + (a+2)^3$

a	a^3	a+1	$(a+1)^3$	a+2	$(a+2)^3$	$f(a)$
0	0	1	1	2	2	0
1	1	2	2	0	0	0
2	2	0	0	1	1	0

В последнем столбце получен остаток ноль, что означает делимость без остатка на 3 суммы кубов трех последовательных целых чисел.

Нетрудно доказать следующие утверждения:

- *Остаток от деления на 3 числа 5^k равен 1, если k четно, и 2, если k нечетно.*
- *Квадрат любого натурального числа или делится на 2 (на 4), когда само число чётное, или при делении на 2 (на 4) даёт в остатке 1.*
- *Квадрат любого натурального числа или делится на 3, когда на 3 делится само число, или при делении на 3 даёт в остатке 1.*
- *Квадрат любого натурального числа или делится на 5, когда на 5*

делится само число, или при делении на 5 даёт в остатке 1 или 4.

- *Квадрат любого натурального числа или делится на 7, когда на 7 делится само число, или при делении на 7 даёт в остатке 1, 2 или 4.*
- *Разность квадратов двух целых чисел одинаковой чётности делится на 4.*
- *Число 4^n при делении на 3 дает в остатке 1.*
- *Число 5^{2n} при делении на 3 дает в остатке 1, а 5^{2n+1} дает в остатке 2.*
- *При делении на 3 куб целого числа и само число дают одинаковые остатки (0, 1, 2).*
- *При делении на 9 куб целого числа дает в остатке 0, 1, 8.*
- *При делении на 4 куб целого числа дает в остатке 0, 1, 3.*

Используя арифметику остатков, можно получить ценные свойства для теоретико-числовых задач.

Составим таблицы квадратов и кубов при делении на числа d.

	d=3		
a	0	1	2
a^2	0	1	1
a^3	0	1	2

Выделим арифметические свойства при делении чисел на 3.

$$a \equiv a^3 (mod\ 3),\ a^2 \equiv \{0;1\} (mod\ 3).$$

	d=4			
a	0	1	2	3
a^2	0	1	0	1
a^3	0	1	0	3

Выделим арифметические свойства при делении чисел на 4.

$$a^2 \equiv \{0;1\} (mod\ 4),\ a^3 \equiv \{0;1;3\} (mod\ 4).$$

	d=5				
a	0	1	2	3	4
a^2	0	1	4	4	1
a^3	0	1	3	2	4

Выделим арифметические свойства при делении чисел на 5.

$$a^2 \equiv \{0; 1; 4\}(mod\ 5).$$

	d=6					
a	0	1	2	3	4	5
a^2	0	1	4	3	4	1
a^3	0	1	2	3	4	5

Выделим арифметические свойства при делении чисел на 6.

$$a \equiv a^3(mod\ 6),\ a^2 \equiv \{0; 1; 3; 4\}(mod\ 6).$$

	d=7						
a	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1
a^3	0	1	1	6	1	6	6

Выделим арифметические свойства при делении чисел на 7.

$$a^2 \equiv \{0;1;2;4\}(mod\ 7), a^3 \equiv \{0;1;6\}(mod\ 7).$$

	d=8							
a	0	1	2	3	4	5	6	7
a^2	0	1	4	1	0	1	4	1
a^3	0	1	0	3	0	5	0	7

Выделим арифметические свойства при делении чисел на 8.

$$a^2 \equiv \{0;1;4\}(mod\ 8), a^3 \equiv \{0;1;5;7\}(mod\ 8).$$

	d=9								
a	0	1	2	3	4	5	6	7	8
a^2	0	1	4	0	7	7	0	4	1
a^3	0	1	8	0	1	8	0	1	8

$$a^2 \equiv \{0;1;4;7\}(mod\ 9), a^3 \equiv \{0;1;8\}(mod\ 9).$$

Примеры.

1. Может ли число 200...009 быть квадратом целого числа при каком-либо количестве нулей?

$$20\ldots009 \equiv 2\ (mod\ 3),$$

$a^2 \equiv \{0;1\}(mod\ 3)$. Не может.

2. Может ли число 100...004 быть квадратом целого числа?

$$100\ldots004 \equiv 2\ (mod\ 3),$$

$a^2 \equiv \{0;1\}(mod\ 3)$. Не может.

3. Может ли число 100…050…01 быть кубом целого числа?

$$100\ldots050\ldots01 \equiv 7\ (mod\ 9),$$

$a^3 \equiv \{0;1;8\}(mod\ 9)$. Не может.

Упражнения

1. На какие цифры может оканчиваться квадрат целого числа?
2. Может ли квадрат целого числа иметь вид:
   a) 5q + 2,
   b) 3q − 1,
   c) 6q − 1?
3. Существует ли натуральное число N такое, что $N^2 + 1$ делится на 3? $\boldsymbol{N^3} + 3$ делится на 99.
4. Докажите, что если $\boldsymbol{x^2 + y^2}$ делится на 3 (x, y — целые), то x и y делятся на 3.
5. Может ли сумма квадратов двух нечетных чисел быть квадратом целого числа? А трех нечетных чисел?
6. a, b, c — натуральные числа, причем a + b + c делится на 6. Докажите, что $a^3 + b^3 + c^3$ тоже делится на 6
7. Докажите, что $a^3 + b^3 + 4$ не является кубом натурального числа при натуральных a и b
8. Докажите, что ваше 28-летие будет отмечаться в тот же день недели, в который вы родились.

9. Докажите, что если в трехзначном числе две последние цифры одинаковы, а сумма цифр делится на 7, то и само число делится на 7.

10. К числу 15 припишите слева и справа по одной цифре так, чтобы полученное число делилось на 15.

11. У числа 22011 зачеркнули первую цифру и прибавили ее к оставшемуся числу. С результатом проделали ту же операцию и т. д., пока не получили 10-значное число. Докажите, что в этом числе есть две одинаковые цифры.

12. Докажите, что для любого целого a:

a) $a^{10} - 9a + 8$ делится на 2; $a^5 + 3a^3 - 12$ делится на 4;

b) $a^3 - 7a + 18$ делится на 6; $a^7 - a - 56$ делится на 7;

c) $a^5 - 17a^3 + 24$ делится на 8; $a^9 + 17a^3 - 18$ делится на 9.

13. Докажите, что при любом натуральном n:

a) $25^{n-2} + 5^n - 13^{n+1}$ делится на 17;

b) $12^{2n+1} + 11^{n+2}$ делится на 133;

c) $2^{n+2} + 2^{n+1} + 2^n$ делится на 14;

d) $7^{2n} - 4^{2n}$ делится на 33;

e) $5^{2n+1} + 3^{n+2} \cdot 2^{n-1}$ делится на 19.

14. Докажите, что уравнения не имеют решений в целых числах:

a) $12x + 5 = y^2$;

b) $x^2 - 5y + 3 = 0$;

c) $x^2 + y^2 = 2007$;

d) $a^2 - 3b^2 = 8$;

e) $-x^2 + 7y^3 + 6 = 0$;

f) $15x^2 - 7y^2 = 9$.

7.8. Длина периода систематической дроби

Систематическая запись целого числа n:

$$n = a_s g^s + a_{s-1} g^{s-1} + \cdots + a_1 g + a_0 = (a_s a_{s-1} \ldots a_1 a_0)_g.$$

Периодическую g-ичную дробь будем записывать так: $(0, c_1 c_2 \ldots c_{k_1} \overline{a_1 a_2 \ldots a_{k_2}})_g$, где $\overline{a_1 a_2 \ldots a_{k_2}}$ – период дроби, k_2 - длина периода, $c_1 c_2 \ldots c_{k_1}$ - предпериод дроби, k_2 - длина предпериода. Если нет предпериода, то дробь чисто периодическая:

$$b(0, \overline{a_1 a_2 \ldots a_{k_2}})_g.$$

Рассмотрим десятичную систему счисления.

Изучим вопрос об определении длины периода, который получается при обращении обыкновенной дроби в десятичную. Пусть знаменатель дроби не делится ни на 2, ни на 5.

Рассмотрим дробь $\frac{a}{m}$, где $a, m \in \mathrm{N}, m > 1, \mathrm{НОД}(a, m) = 1$ и $\mathrm{НОД}(a, 10) = 1$. Пусть k -наименьшее натуральное число, такое, что $10^k \equiv 1 \ (mod\ m)$. Тогда можно доказать, что разложение дроби $\frac{a}{m}$ в бесконечную десятичную дробь будет содержать k цифр в периоде.

Пример. Найти число k цифр в периоде разложения дроби $\frac{22}{91}$ в бесконечную десятичную дробь.

Имеем: $22,\ 91 \in \mathrm{N}, 91 > 1, 22 = 2 \cdot 11, 91 = 7 \cdot 13,$ НОД $(22,91) = 1$ и НОД $(91,10) = 1$. Найдем наименьшее натуральное число k, такое, что $10^k \equiv 1\ (mod\ 91)$. Так как НОД $(91,10) = 1$, то по теореме Эйлера $10^{\varphi(91)} \equiv 1(\ mod\ 91)$. Вычислим $\varphi(91)$ одним из следующих двух способов:

1). $\varphi(91) = 91\left(1 - \frac{1}{17}\right)\left(1 - \frac{1}{13}\right) = 72.$

2). $\varphi(91) = \varphi(7 \cdot 13) = \varphi(7) \cdot \varphi(13) = 6 \cdot 12 = 72.$

Следовательно, $10^{72} \equiv 1(\ mod\ 91)$. Поэтому будем проверять не все подряд натуральные показатели, а только делители числа 72: 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72 (всего их будет $\tau(72) = \tau(2^3 \cdot 3^2) = = (3 + 1) \cdot (2 + 1) = 12$. Поэтому всего натуральных делителей числа 72 будет 12).

$k = 1, 10^1 - 1 = 9, 9$ не кратно 91, остаток $r = 9$,

$k = 2, 10^2 - 1 = 99, 99$ не кратно 91, остаток $r = 8$,

$k = 3, 10^3 - 1 = 999, 999$ не кратно 91, остаток $r = 89$,

$k = 4, 10^4 - 1 = 9999, 9999$ не кратно 91, остаток $r = 80$,

$k = 5, 10^5 - 1 = 99999, 99999$ не кратно 91, остаток $r = 81$,

$k = 6, 10^6 - 1 = 999999, 999999 \ \vdots \ 91$, остаток $r = 0$.

Следовательно, наименьшее натуральное число k, такое, что $10^k \equiv 1(\,mod\ 91)$, будет число k = 6. Поэтому длина периода в разложении дроби будет равна 6.

Отметим, что искомое число k можно найти еще иначе:

$10^1 \equiv 10\ (mod\ 91)$,

$10^2 \equiv 9\ (mod\ 91)$,

$10^3 \equiv -1\ (mod\ 91) => 10^6 \equiv 1\ (mod\ 91) => к = 6$.

Проверку найденного числа k=6 можно выполнить непосредственным делением числа a на m: $\frac{22}{91} = 0, (241758)$.

Заметим, что

1) Обращение обыкновенной дроби в периодическую получается непосредственным делением числителя на знаменатель.

Например, $\frac{22}{91} = 0, \overline{241758}$:

2) При обращении в обыкновенную дробь чистой периодиче-

ской дроби получим дробь, числитель которой равен периоду, а знаменатель состоит из стольких девяток, сколько цифр в периоде:

$$0,\overline{a_1a_2\dots a_{k_2}}=\frac{a_1a_2\dots a_k}{\underbrace{99\dots9}_{k}}.$$

Например, $0,\overline{35}=\frac{35}{39}$, $0,\overline{489}=\frac{489}{999}$.

3) При обращении смешанной периодической дроби в обыкновенную получится дробь, числитель которой равен разности между числом до второго периода и числом до первого периода, знаменатель состоит из стольких девяток, сколько цифр в периоде и стольких нулей, сколько цифр в предпериоде:

$$0,c_1c_2\dots c_{k_1}\overline{a_1a_2\dots a_{k_2}}=\frac{c_1c_2\dots c_{k_1}a_1a_2\dots a_{k_2}-c_1c_2\dots c_{k_1}}{\underbrace{99\dots9}_{k_2}\underbrace{00\dots0}_{k_1}}.$$

Например, $0,7\overline{61}=\frac{761-7}{990}=\frac{754}{990}=\frac{377}{495}$.

4) $\frac{m}{n}$ можно представить в виде:

a) в виде конечной дроби, если $n=2^{\alpha_1}\cdot5^{\alpha_2}$, где $\alpha_1,\alpha_2\in\mathrm{N}\cup\{0\}$;

b) в виде чистой периодической дроби, если n не кратно 2 и 5;

c) в виде смешанной периодической дроби, если $n\vdots2$ или $n\vdots5$, но

$n \neq 2^{\alpha_1} \cdot 5^{\alpha_2}$.

Например,

a) $\frac{3}{20}$ — можно представить в виде конечной дроби ($20 = 2^2\ 5$);

b) $\frac{7}{13}$, 13 не делится на 2, 13 не делится на 5, следовательно, $\frac{7}{13}$ можно представить в виде чистой периодической дроби;

c) $\frac{17}{60}$,60:2 (или иначе 60:5), но $60 = 2^2\ 3\ 5 \neq 2^{\alpha_1} \cdot 5^{\alpha_2}$, есть еще число 3 в разложении, следовательно, $\frac{17}{60}$ можно представить в виде смешанной периодической дроби.

Так как число k находится среди натуральных делителей числа $\varphi(m)$, то длина периода (число цифр в периоде) $k \leq \varphi(m)$.

В частности, если $m = p$, то $\varphi(m) = \varphi(p) = p - 1$, поэтому при разложении дроби $\frac{a}{p}$, где $a \in \mathrm{N}, p -$ - положительное простое число, *НОД(a,p)* = 1, *НОД(p,* 10) = 1, в бесконечную десятичную дробь число цифр в периоде $k \leq p - 1$, причем k будет натуральным делителем числа $(p - 1)$. Если $k = p - 1$, то разложения в бесконечные десятичные дроби всех дробей

$$\frac{1}{p}, \frac{2}{p}, \frac{3}{p}, \ldots, \frac{p-1}{p}$$

получаются друг из друга циклической перестановкой, поэтому, зная одну из них, можно найти все остальные.

Пример. Найти разложение для дроби $\frac{14}{19}$, зная, что

$$\frac{1}{19} = 0,(052631578947368421).$$

Имеем: число цифр в периоде $k = 18$, число 19 (знаменатель дроби) является простым числом, следовательно, условие $k =$ выполнено.Найдем две цифры разложения непосредственным делением:

$$\frac{14}{19} = 0,73 \ldots$$

Найдем в записанном периоде для $\frac{1}{19}$ число 73, а затем допишем остальные цифры с помощью циклической перестановки:

$$\frac{1}{19} = 0,(736842105263157894).$$

Если в дроби $\frac{a}{m}$ знаменатель $m \vdots 2$, $m \vdots 5$, то тогда

$$m = 2^{\alpha_1} \cdot 5^{\alpha_2} \cdot m_1,$$

где НОД (m_1,10) = 1. В этом случае обозначим наибольшее из чисел α_1 и α_2 через α, то есть $\alpha = \max(\alpha_1, \alpha_2)$, и преобразуем дробь $\frac{a}{m}$:

$$\frac{a}{m} = \frac{a}{2^{\alpha_1} \cdot 5^{\alpha_2} \cdot m_1} = \frac{a \cdot 2^{\alpha - \alpha_1} \cdot 5^{\alpha - \alpha_2}}{10^{\alpha} \cdot m_1} = \frac{1}{10^{\alpha}} \cdot \frac{a_1}{m_1}, \text{ где } a_1 = a \cdot 2^{\alpha - \alpha_1} \cdot 5^{\alpha - \alpha_2}.$$

Так как НОД *(a,m)* = 1, НОД(m_1,10) = 1, то будет НОД(a_1, m)=1, и дробь $\frac{a_1}{m_1}$ можно разложить в бесконечную десятичную дробь, найдя период k_1 цифр, где k_1 - наименьшее натуральное число, для которого

$$10^{k_1} \equiv 1 \ (mod\ m).$$

После этого выполним умножение на $\frac{1}{10^{\alpha}}$переносом запятой влево на a разрядов. Таким образом, в этом случае получим разложение смешанно периодическое с периодом из k_1 цифр.

Определение. *Под периодом простого числа p, отличного от 2 и 5, будем понимать период числа* $\frac{1}{p}$. *Простое число называется числом с единичным периодом, если оно имеет период, не одинаковый с любым другим простым числом.*

Например, для простых чисел $p_1 = 3$, $p_2 = 7$, $p_3 = 11$ будем иметь:

$$\frac{1}{3} = 0{,}33\ldots = 0{,}(3),$$

следовательно, период числа $p_1 = 3$ равен 1.

$$\frac{1}{7} = 0{,}142857142857\ldots = 0,\ (142857),$$

следовательно, период числа $p_2 = 7$ равен 6.

$$\frac{1}{11} = 0{,}0909\ldots = 0{,}(09),$$

следовательно, период числа $p_3 = 11$ равен 2.

Поэтому числа $p_1 = 3,\ p_2 = 7,\ p_3 = 11$ являются простыми числами с единичным периодом.

$$\frac{1}{13} = 0{,}076923076923\ldots = 0{,}(076923),$$

следовательно, период числа $p_4 = 13$ равен 6.

Тогда числа $p_2 = 7,\ p_4 = 13$ не являются простыми числами с единичным периодом. Такие простые числа очень редки, находятся новые числа и указан метод поиска таких чисел. До него в 1991 году Самуэль Иейте (S. Yates) нашел 29-е такое простое число с 217-ю цифрами и с длиной периода 654.

7.9. Определение целочисленных корней многочлена

Если $a \equiv b \ (mod\ m)$, и $f(x) \in \mathrm{Z}[x]$ то по свойству сравнений имеем:

$$f(a) \equiv f(b) \ (mod\ m).$$

Возьмем модуль $m = 2$. Тогда или $a \equiv 0 \ (mod\ 2)$, или $a \equiv 1 \ (mod\ 2)$, и, значит, или

$f(a) \equiv f(0) \ (mod\ 2)$, или $f(a) \equiv f(1) \ (mod\ 2)$.

Если $f(x) = a_n x^n + \cdots + a_1 x + a_0$, то $f(1) = a_n + \cdots + a_1 + a_0$.

Таким образом, если $f(x) \in \mathrm{Z}[x]$ и $f(0)$ и $f(1)$ оба нечетные, то они сравнимы с 1 по модулю 2, поэтому многочлен $f(x)$ не имеет целочисленных корней.

Например, многочлен $f_1(x) = x^2 - 117x + 31$ имеет свободный член $f_1(0) = 31$, а сумма его коэффициентов $f_1(1) = -85$, оба эти числа нечетные, следовательно, $f_1(x)$ не имеет корней в Z. Аналогично для

$$f_2(x) = 2x^2 + 2x + 1, f_3(x) = 3x^3 + 2x^2 + x + 3.$$

Заметим, что можно по-другому доказать, что, например, мно-

Действительно, пусть $n \in \mathrm{Z}$. Оно или четное, или нечетное:

a) если n - четное, то n^2 и $117n$ тоже четные, следовательно, $f_1(x)$ будет нечетным;

b) если n - нечетное, то n^2 и $117n$ тоже нечетные, следовательно, $f_1(x)$ будет нечетным.

Поэтому при всех $n \in \mathrm{Z}$ получим, что $f_1(x)$ - нечетное, а, значит

$$(\forall n \in \mathrm{Z})(f_1(x) \neq 0).$$

Таким образом, многочлен $f_1(x)$ не имеет корней в Z.

7.10. Приложение теоремы Эйлера и Ферма

Заметим, что теорема Ферма и теорема Эйлера позволяют находить остатки от деления больших степеней на модуль.

Пример. Найти остаток от деления 171^{2147} на 52.

Решение.

Обозначим остаток от деления через x:

$$171^{2147} \equiv x \pmod{52},$$

отсюда

$$x \equiv 171^{2147} \pmod{52}.$$

Введем обозначения: $m = 52$, $a = 171$. Так как $171 > 52$, то можно число 171 заменить остатком от деления на 52: $171 = 52\text{-}3\text{+}15$, отсюда $171 \equiv 15 \pmod{52}$, но тогда

$$171^{2147} \equiv 15^{2147} \pmod{52},$$

а поэтому сравнение примет вид:

$$x \equiv 15^{2147} \pmod{52}.$$

НОД (a_1, m) = НОД (15,52) = 1, где $a_1 = 15$. Следовательно, применима теорема Эйлера, согласно которой

$$a_1^{\varphi(m)} \equiv 1(mod\ m), \text{ если НОД}(a_1, m) = 1,$$

поэтому

$$15^{\varphi(52)} \equiv 1(mod\ 52).$$

$$\varphi(52) = \varphi(2^2 \cdot 13) = 2^2 \cdot \left(1 - \frac{1}{2}\right) \cdot 13 \cdot \left(1 - \frac{1}{13}\right) = 24.$$

Итак, $15^{24} \equiv 1 \pmod{52}$.

Выделим теперь из степени 15^{2147} степень 15^{24}. Так как $2147 = 24 \cdot 89 + 11$, то $15^{2147} \equiv (15^{24})^{89} \cdot 15^{11}$, поэтому получим следующую цепочку преобразований сравнений:

$$x \equiv 15^{2147} \equiv (15^{24})^{89}\ 15^{11} \equiv I^{89} \cdot 15^{11} \equiv 15^{11} \equiv 15 \cdot (15^2)^5 \equiv 15 \cdot 225^5 \equiv$$

$\equiv 15\cdot 17^5 \equiv (15\cdot 17)\cdot(17^2)^2 \equiv 255\cdot 289^2 \equiv 47\cdot 29^2 \equiv -5(-23)^2 \equiv -5\cdot 529 \equiv$

$\equiv -5\cdot 9 \equiv -45 \equiv 7 \pmod{52}$, следовательно, $x \equiv 7 \pmod{52}$.

Таким образом, остаток от деления 171^{2147} на число 52 равен 7.

Заметим, что в сравнении остаток x не может быть отрицательным или $\geq m$, поэтому:

a) если получено последнее число в сравнении отрицательное, то надо заменить его неотрицательным из того же класса вычетов;

b) если последнее число в сравнении получено положительное, $\geq m$, то надо его уменьшить, то есть заменить другим представителем r из того же класса вычетов так, чтобы было $0 \geq r < m$.

7.11. Общий признак делимости Паскаля

Основные арифметические приложения теории сравнений следующие:

1) вычисление остатка;

2) признаки делимости;

3) обращение обыкновенной дроби в десятичную.

Признаки делимости.

Рассмотрим применение теории сравнений к выводу некоторых признаков делимости на данное натуральное число a. Отметим, что под признаком делимости на a понимают необходимое и достаточное условие делимости произвольного натурального числа n на a. Различают общие признаки, имеющие силу для любого a, и частные — для отдельных значений a.

Французский математик Блез Паскаль (1623–1662) нашел общий признак делимости.

Всякое натуральное число n в десятичной системе счисления можно записать в виде:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Составим число

$$m = a_k \cdot r_k + a_{k-1} \cdot r_{k-1} + ... + a_1 \cdot r_1 + a_0,$$

где $a_i, i = 0, k$ — цифры числа n, а $r_i, i = 1, k$ — абсолютно наименьшие вычеты соответствующих степеней 10^i по модулю a.

Теорема. (общий признак делимости Паскаля). Натуральное число n делится на натуральное число a тогда и только тогда, когда m делится на a.

□

Из общего признака Паскаля вытекают различные частные признаки делимости. Рассмотрим некоторые из них, наиболее часто используемые в практике.

1) $a = 2$.

$10 \equiv 0 \pmod 2$, $10^i \equiv 0 \pmod 2$, $i = \overline{1,k}$. Тогда $r_i = 0$ и $m = a_0$. Следовательно, по теореме, n делится на 2 тогда и только тогда, когда a_0 делится на 2, т.е. натуральное число n делится на 2 тогда и только тогда, когда его последняя цифра a_0 делится на 2 (последняя цифра чётная).

2) $a = 3$.

$10 \equiv 1 \pmod 3$, $10^i \equiv 1 \pmod 3$, $i = \overline{1,k}$. Поэтому $r_i = 1$ и $m = a_k + a_{k-1} + \ldots + a_1 + a_0$. Тогда по теореме, n делится на 3 тогда и только тогда, когда $a_k + a_{k-1} + \ldots + a_1 + a_0$ делится на 3, т.е. натуральное число n делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

3) $a = 4$.

$10 \equiv 2 \pmod 4$, $10^2 \equiv 0 \pmod 4$, $10^i = 10^2 10^{i-2} \equiv 0 \pmod 4$, $i = \overline{2,k}$. Значит, $r_1 = 2$, $r_i = 0$, $i = \overline{2,k}$ и $m = 2a_1 + a_0$. Таким образом, n делится на 4 тогда и только тогда, когда $2a_1 + a_0$ делится на 4, т.е. сумма удвоенной цифры десятков и цифры единиц числа n делится на 4.

4) $a = 5$.

$10 \equiv 0 \pmod 5$, $10^i \equiv 0 \pmod 5$, $i = \overline{1,k}$. Значит, $r_i = 0$ и $m = a_0$. Таким образом, n делится на 5 тогда и только тогда, когда a_0 делится

на 5, т.е. последняя цифра числа n есть 0 или 5.

5) $a = 8$.

$10 \equiv 2 \pmod 8$, $10^2 \equiv 4 \pmod 8$, $10^3 \equiv 0 \pmod 8$, $10^i = 10^3 10^{i-3} \equiv 0 \pmod 8$, $i = \overline{3,k}$. Поэтому $r_1 = 2$, $r_2 = 4$, $r_i = 0$, $i = \overline{3,k}$ и $m = 4a_2 + 2a_1 + a_0$.

Таким образом, n делится на 8 тогда и только тогда, когда $4a_2 + 2a_1 + a_0$ делится на 8, т.е. сумма учетверенной цифры сотен, удвоенной цифры десятков и цифры единиц делятся на 8.

Покажите, что $4a_2 + 2a_1 + a_0$ делится на 8 тогда и только тогда, когда $100a_2 + 10a_1 + a_0 = \overline{a_2 a_1 a_0}$ делится на 8.

Поэтому n делится на 8 тогда и только тогда, когда число, записанное последними тремя цифрами числа n, делится на 8.

6) $a = 9$.

$10 \equiv 1 \pmod 9$, $10^i \equiv 1 \pmod 9$, $i = \overline{1,k}$. Значит, $r_i = 1$ и $m = a_k + a_{k-1} + \ldots + a_1 + a_0$. Таким образом, n делится на 9 тогда и только тогда, когда $a_k + a_{k-1} + \ldots + a_1 + a_0$ делится на 9, т.е. сумма цифр числа n делится на 9.

7) $a = 11$.

$10 \equiv -1 \pmod{11}$, $10^2 \equiv 1 \pmod{11}$, ..., т.е.

$$10^k \equiv \begin{cases} -1, & k \text{ — нечетное} \\ 1, & k \text{ — четное} \end{cases} \pmod{11}.$$

Поэтому $r_k = -1$, если k — нечетное; $r_k = 1$, если k — четное, и $m =$

$(a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)...$

Итак, по теореме, число n делится на 11 тогда и только тогда, когда разность между суммой цифр, стоящих на чётных местах и суммой цифр, стоящих на нечетных местах числа n, делится на 11.

Признаки делимости на 7 и 13 также следуют из признака Паскаля, но они получаются неудобными для практического использования.

Теорема. (общий признак делимости на 7, 11, 13). Натуральное число n делится на 7, 11, 13 тогда и только тогда, когда разность между числом, записанным последними тремя цифрами числа n и числом, записанным остальными его цифрами, делится на 7, 11, 13, т.е. $n = \overline{a_k a_{k-1} ... a_0}$ делится на 7, 11, 13 тогда и только тогда, когда $(\overline{a_2 a_1 a_0} - \overline{a_k a_{k-1} ... a_3})$ делится на 7, 11, 13.

□

Теорема. (признак делимости на составное число).

Если НОД$(a, b) = 1$, то $n \vdots (ab)$ тогда и только тогда, когда $n \vdots a$ и $n \vdots b$.

Обращение обыкновенной дроби в десятичную.

Применим некоторые из рассмотренных свойств сравнений к вопросу об обращении обыкновенной дроби в десятичную.

Замечание. Несократимая обыкновенная дробь $\frac{a}{b}$ обращается в конечную десятичную дробь тогда и только тогда, когда каноническое разложение её знаменателя содержит лишь простые числа 2 или 5.

Доказательство. Доказательство проведем для положительной несократимой обыкновенной дроби.

Необходимость. Пусть дробь $\frac{a}{b}$ представляется в виде конечной десятичной дроби, т.е. $\frac{a}{b} = a_k a_{k-1}...a_0, b_1 b_2...b_s = a_k 10^k + ... + a_0 + b_1 10^{-1} + ... + b_s 10^{-s} = \frac{n}{10^s} = \frac{n}{2^s \cdot 5^s}$. Сократим дробь $\frac{n}{2^s \cdot 5^s}$, получим:

$$\frac{a}{b} = \frac{n_1}{2^{s_1} \cdot 5^{s_2}}, s_1, s_2 \in \mathbb{Z}, s_1, s_2 \geq 0.$$

Две положительные несократимые дроби равны тогда и только тогда, когда равны их числители и знаменатели (докажите). Поэтому из следует, что $b = 2^{s_1} \cdot 5^{s_2}$, т.е. каноническое разложение знаменателя b содержит лишь простые множители 2 или 5.

Достаточность. Пусть каноническое разложение знаменателя дроби $\frac{a}{b}$ имеет вид: $b = 2^{s_1} \cdot 5^{s_2}$, $s_1, s_2 \in \mathbb{Z}, s_1, s_2 \geq 0$. Если $s_1 = s_2 = s$, то $\frac{a}{b} = \frac{a}{10^s} = a_k a_{k-1}...a_0, b_1 b_2...b_s$. Если же $s_1 > s_2$, то

$$\frac{a}{b} = \frac{a \cdot 5^{s_1 - s_2}}{2^{s_1} \cdot 5^{s_2} \cdot 5^{s_1 - s_2}} = \frac{a \cdot 5^{s_1 - s_2}}{2^{s_1} \cdot 5^{s_1}} = \frac{n}{10^{s_1}} = a_k a_{k-1}...a_0, b_1 b_2...b_{s_1}.$$

□

Следствие 2.12.1. Несократимая обыкновенная дробь $\frac{a}{b}$ обращается в бесконечную десятичную дробь тогда и только тогда, когда каноническое разложение её знаменателя содержит хотя бы одно простое число, отличное от 2 и 5.

Определение. Бесконечная десятичная дробь, у которой, начиная с некоторого десятичного знака, повторяется некоторая совокупность цифр, называется *бесконечной периодической дробью*. Повторяющаяся совокупность цифр называется *периодом*, а число цифр в периоде называется *длиной периода*. Записывается бесконечная периодическая дробь в виде $m, a_1 ... a_s (b_1 ... b_k)$, где m — её целая часть.

Определение. Бесконечная периодическая дробь называется *чистой периодической*, если период начинается с первого десятичного знака и *смешанной периодической* — если не с первого десятичного знака.

Обращение обыкновенной дроби в чистую периодическую дробь.

Теорема. Несократимая обыкновенная дробь $\frac{a}{b}$, знаменатель которой взаимно прост с 10, обращается в чистую периодическую дробь, длина периода которой равна порядку 10 по модулю b, т.е $\theta(10 \mod m)$.

Доказательство. 1. Пусть $\frac{a}{b}$ — правильная несократимая дробь, знаменатель которой взаимно прост с 10. Тогда b не делится на 2 и b не делится на 5, т.е. каноническое разложение знаменателя не содержит простых множителей 2 и 5. Поэтому дробь $\frac{a}{b}$ обращается в бесконечную десятичную дробь. Покажем, что эта дробь будет чистой периодической, длина периода которой равна k, где $k = \theta\ (10 \mod b)$. Применим следующий алгоритм обращения обыкновенной дроби $\frac{a}{b}$ в десятичную: делим с остатком $10a$ на b : $10a = bq_1 + r_1$.

Так как НОД(b, r_1) = НОД$(10a, b) = 1$, то $r_1 \neq 0$. Значит, $0 < r_1 < b$;
делим с остатком $10r_1$ на b : $10r_1 = bq_2 + r_2$. Аналогично, $0 < r_2 < b$;
делим с остатком $10r_2$ на b : $10r_2 = bq_3 + r_3$, где $0 < r_3 < b$;
. . . . . .
делим с остатком $10r_{k-1}$ на b : $10r_{k-1} = bq_k + r_k$, $0 < r_k < b$;
делим с остатком $10r_k$ на b : $10r_k = bq_{k+1} + r_{k+1}$, $0 < r_{k+1} < b$.
. . . . . .

Так как остатки в этом алгоритме не обращаются в 0, то он бесконечный. Разделим получающиеся равенства на $10b$:

$$\frac{a}{b} = \frac{q_1}{10} + \frac{r_1}{10b},$$
$$\frac{r_1}{b} = \frac{q_2}{10} + \frac{r_2}{10b},$$
$$\frac{r_2}{b} = \frac{q_3}{10} + \frac{r_3}{10b},$$

$$\frac{r_{k-1}}{b} = \frac{q_k}{10} + \frac{r_k}{10b},$$

$$\frac{a}{b} = \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{q_3}{10^3} + \frac{r_3}{10^3 b} = \ldots =$$

$$= \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{q_3}{10^3} + \ldots + \frac{q_k}{10^k} + \frac{r_k}{10^k b} = \ldots . \qquad (2.12.4)$$

Покажем, что все q_i — целые неотрицательные числа, меньше 10. Действительно, из первого равенства в описанном алгоритме $q_1 = \dfrac{10a - r_1}{b}$, где $0 < a < b$, $0 < r_1 < b$. Поэтому $-1 < q_1 < 10$. Из других равенств в алгоритме получаем $q_i = \dfrac{10r_{i-1} - r_i}{b}$, где $0 < r_{i-1} < b$, $0 < r_i < b$, $i = 2, 3, \ldots$. Отсюда $-1 < q_i < 10$.

Таким образом, $q_1, q_2, \ldots, q_k$ — k первых десятичных знаков бесконечной десятичной дроби, в которую обращается дробь $\dfrac{a}{b}$.

Покажем, что они будут повторяться, т.е. образуют период десятичной дроби, в которую обращается обыкновенная дробь $\dfrac{a}{b}$.

Равенство (2.12.4) умножим на $10^k b$:

$$a \cdot 10^k = b \cdot (q_1 \cdot 10^{k-1} + q_2 \cdot 10^{k-2} + \ldots + q_k) + r_k, 0 < r_k < b.$$

Значит, r_k — остаток от деления $10^k \cdot a$ на b. Поэтому $10^k \cdot a \equiv r_k \pmod b$. Так как $k = \theta(10 \mod b)$, то $10^k \equiv 1 \pmod b$.

Следовательно, $a \cdot 10^k \equiv a \pmod b$ и $r_k \equiv a \pmod b$. Тогда $r_k - a$ делится на b. Отсюда $\mid r_k - a \mid \geq b$ или $r_k - a = 0$. С другой стороны, учитывая, что $0 < r_k < b$, $0 < a < b$, имеем $-b < r_k - a < b$, т.е. $\mid r_k - a \mid < b$.

Таким образом, $r_k - a = 0$, т.е. $r_k = a$. Поэтому $10r_k = 10a$; следовательно, $q_{k+1} = q_1$ и $r_{k+1} = r_1$. Тогда $10r_{k+1} = 10r_1$, значит, $q_{k+2} = q_2$ и т.д. Итак, десятичные знаки $q_1, q_2, ..., q_k$ будут повторяться. Они образуют период десятичной дроби, в которую обращается обыкновенная дробь $\frac{a}{b}$; длина периода равна k, где $k = \theta(10 \mod b)$.

2. Если дробь $\frac{a}{b}$ неправильная ($a > b$), то при обращении её в десятичную из неё предварительно выделяется целая часть: $\frac{a}{b} = m + \frac{a_1}{b} = m, (q_1, ..., q_k)$ – чистая периодическая дробь, где m — целая часть $\frac{a}{b}$, $\frac{a_1}{b}$ – правильная несократимая дробь. □

Теорема 2.12.5. Несократимая обыкновенная дробь $\frac{a}{b}$, знаменатель которой $b = 2^\alpha \cdot 5^\beta \cdot b_1$, где α, β — целые неотрицательные числа, не равные 0 одновременно,НОД$(b_1, 10) = 1$, $b_1 \neq 1$, т.е. в каноническое разложение b входит хотя бы одно из простых чисел 2 и 5, а также хотя бы одно простое число, отличное от 2 и 5, обращается в смешанную перио-

дическую дробь, у которой число знаков до периода равно наибольшему из чисел α и β, а длина периода равна $\theta(10 \mod b_1)$.

Доказательство. Обозначим через n наибольшее из чисел α и β, и рассмотрим дробь:

$$\frac{10^n a}{b} = \frac{2^n \cdot 5^n \cdot a}{2^\alpha 5^\beta b_1} = \frac{2^{n-\alpha} \cdot 5^{n-\beta} \cdot a}{b_1} = \frac{a_1}{b_1}.$$

Так как НОД$(a, b) = 1$, то НОД$(a, b_1) = 1$. По условию НОД$(10, b_1) = 1$. Значит, НОД$(2, b_1) = 1$, НОД$(5, b_1) = 1$. Следовательно, НОД$(2^{n-\alpha}, b_1) = 1$, НОД$(5^{n-\beta}, b_1) = 1$, НОД$(a_1, b_1) = 1$, т.е. дробь $\frac{a_1}{b_1}$ несократима, причем НОД$(b_1, 10) = 1$.

По теореме 2.12.4 дробь $\frac{a_1}{b_1}$ обращается в чистую периодическую дробь, длина периода которой равна $\theta(10 \mod b_1)$, т.е. $\frac{10^n a}{b} = \frac{a_1}{b_1} = l, (q_1 ... q_k)$, где l — целая часть $\frac{a_1}{b_1}$.

Отсюда $\frac{a}{b} = \frac{l, (q_1 ... q_k)}{10^n} = m,\ m_1 ... m_n (q_1 ... q_k)$, где m – целая часть $\frac{a}{b}$. Таким образом, получили смешанную периодическую дробь с n десятичными знаками до периода и длиной периода $k = \theta(10 \mod b_1)$. □

Следствие 2.12.2. Всякая несократимая обыкновенная дробь обращается или в конечную десятичную дробь или в бесконечную периоди-

ческую дробь, причём длина периода не зависит от числителя дроби, а зависит только от её знаменателя.

Пример. Найти длину периода при обращении следующих обыкновенных дробей в десятичные:

1) несократимой дроби со знаменателем $b = 41$.

2) несократимой дроби со знаменателем $b = 1260$.

Доказательство. 1. Так как НОД$(41, 10) = 1$, то по теореме 2.12.4 данная дробь обращается в чистую периодическую дробь, длина периода которой равна $\theta(10 \mod 41)$. Известно, что $\theta(10 \mod 41)$ является делителем $\varphi(41) = 40$, т.е. одним из чисел $1, 2, 4, 5, 8, 10, 20, 40$. Испытывая эти числа, получаем: $\theta(10 \mod 41) = 5$.

2. $b = 2^2 \cdot 5 \cdot 3^2 \cdot 7$, т.е. каноническое разложение b входят простые числа 2 и 5, а также простые числа 3 и 7. Поэтому по теореме 2.12.5 данная дробь обращается в смешанную периодическую, у которой число десятичных знаков до периода равно 2, а длина периода равна $\theta(10 \mod 63) = 6$.

Ответ: 1) 5; 2) 6. □

7.12. Обращение периодических дробей в обыкновенные

Теорема 2.13.1. Чистая периодическая дробь $0,(b_1 \dots b_k)$ равна обыкновенной дроби, числитель которой есть период, а знаменатель за-

писан столькими девятками, какова длина периода, т.е.

$$0,(b_1\dots b_k)=\frac{\overline{b_1\dots b_k}}{\underbrace{9\dots9}_{k}}.$$

Доказательство. Очевидно, что $0,(b_1\dots b_k)=0,b_1\dots b_kb_1\dots b_k\dots=0,b_1\dots b_k+0,\underbrace{0\dots0}_{k}b_1\dots b_k+0,\underbrace{0\dots0}_{2k}b_1\dots b_k+\dots=\frac{\overline{b_1\dots b_k}}{10^k}+\frac{\overline{b_1\dots b_k}}{10^{2k}}+\frac{\overline{b_1\dots b_k}}{10^{3k}}+\dots=$ [сумма бесконечно убывающей геометрической прогрессии $S=\frac{a_1}{1-q}$, где $a_1=\frac{\overline{b_1\dots b_k}}{10^k}$, $q=\frac{1}{10^k}$] $=\frac{\overline{b_1\dots b_k}}{10^k}\cdot\frac{1}{1-\frac{1}{10^k}}=\frac{\overline{b_1\dots b_k}}{10^k-1}=\frac{\overline{b_1\dots b_k}}{\underbrace{9\dots9}_{k}}.$ □

Пример 2.13.1. $0,(321)=\frac{321}{999}=\frac{107}{333}.$

Теорема 2.13.2. Смешанная периодическая дробь $0,a_1\dots a_m(b_1\dots b_k)$ равна обыкновенной дроби, числитель которой есть разность между числом, записанным десятичными знаками до второго периода и числом, записанным десятичными знаками до первого периода, а знаменатель

записан столькими девятками, какова длина периода и столькими нулями, сколько десятичных знаков до первого периода, т.е.

$$0,a_1\dots a_m(b_1\dots b_k)=\frac{\overline{a_1\dots a_mb_1\dots b_k}-\overline{a_1\dots a_m}}{\underbrace{9\dots9}_{k}\underbrace{0\dots0}_{m}}$$

Доказательство. $0,a_1\dots a_m(b_1\dots b_k)=0,a_1\dots a_m+0,\underbrace{0\dots0}_{m}b_1\dots b_k+$

$0,\underbrace{0\dots0}_{k+m}b_1\dots b_k+\dots=\frac{\overline{a_1\dots a_m}}{10^m}+\frac{\overline{b_1\dots b_k}}{10^{m+k}}+\frac{\overline{b_1\dots b_k}}{10^{m+2k}}+\frac{\overline{b_1\dots b_k}}{10^{m+3k}}+\dots=$

[члены, начиная со второго, образуют бесконечно убывающую геометрическую прогрессию со знаменателем $\frac{1}{10^k}$ и $a_1=\frac{\overline{b_1\dots b_k}}{10^{m+k}}$]

$$=\frac{\overline{a_1\dots a_m}}{10^m}+\frac{\overline{b_1\dots b_k}}{10^{m+k}}\cdot\frac{1}{1-\frac{1}{10^k}}=\frac{\overline{a_1\dots a_m}}{10^m}+\frac{\overline{b_1\dots b_k}}{10^m(10^k-1)}=$$

$$=\frac{\overline{a_1\dots a_m}\cdot10^k-\overline{a_1\dots a_m}+\overline{b_1\dots b_k}}{10^m(10^k-1)}=\frac{\overline{a_1\dots a_mb_1\dots b_k}-\overline{a_1\dots a_m}}{\underbrace{9\dots9}_{k}\underbrace{0\dots0}_{m}}.$$

□

Пример 2.13.2. $0,12(3)=\frac{\cancel{123}-\cancel{12}}{900}=\frac{111}{900}=\frac{37}{300}.$

7.13. Приложения в криптографии

Рассмотрим современные методы шифрования (криптография - тайнопись): «без передач ключа», «открытый ключ» и «электронная подпись», описанные в книге В. И. Нечаева.

В 1976г. У. Диффи (Diffi W.) и М. Хеллман (Heilman M.) предложили новый принцип построения криптосистем, не требующий не только передачи ключа принимающему сообщение, но даже сохранения в тайне метода шифрования. Эти шифры позволяют легко зашифровывать и дешифровать текст и их можно использовать многократно.

Криптосистема «Без передачи ключа»

Пусть абоненты A, B, C, … условились установить между собой секретную переписку. Для этой цели они выбирают достаточно большое простое число p такое, что p-1 хорошо раскладывается на не очень большие простые множители. Если среди множителей такое числа кратных нет, то число p-1называется *евклидовым*. Каждый их абонентов независимо друг от друга выбирает случайное натуральное число, взаимно простое с числом p-1: a, b, c, … - выбранные ими чис-

ла соответственно.

Далее абонент А находит число α, которое является решением сравнения

$$a \cdot \alpha \equiv 1 \ (mod\ p-1).$$

Абонент В находит число β, которое является решением сравнения

$$b \cdot \beta \equiv 1 \ (mod\ p-1).$$

Абонент	Секретные ключи	
А	a	α
В	b	β

Пусть абонент А собирается отправить сообщение m абоненту В, будем считать, что $0 < m < p-1$. Тогда он сначала шифрует сообщение своим первым секретным ключом, находит

$$m_1 \equiv m^a \ (mod\ p), 0 < m_1 < p$$

и отправляет его абоненту В. Абонент В, в свою очередь, зашифровывает полученное сообщение так же свои первым секретным ключом

$$m_2 \equiv {m_1}^b \ (mod\ p), 0 < m_2 < p$$

и отправляет его обратно абоненту А. Абонент А зашифровывает по-

лученное сообщение своим вторым секретным ключом

$$m_3 \equiv {m_2}^{\alpha} \ (mod\ p), 0 < m_3 < p$$

и вновь отправляет абоненту B. Последний расшифровывает полученное сообщение своим вторым секретным ключом

$$m_4 \equiv {m_3}^{\beta} \ (mod\ p), 0 < m_4 < p.$$

Очевидно, что $m_4 \equiv m^k \ (mod\ m)$, где $k \equiv a \cdot b \cdot \alpha \cdot \beta \ (mod\ p-1)$. Заметим, что $k \equiv 1 \ (mod\ \varphi(p))$. Нетрудно заметить, что

$$m_4 \equiv m \ (mod\ p),$$

а так как $0 < m_4 < p$, то $m_4 = m$.

Пример. Предположим, что два абонента A и B решили установить между собой секретную переписку без передачи ключей. Для это они выбрали простое число p=23, далее абонент A выбирает случайное число a=5, а абонент B выбирает случайное число b=7.

Далее абонент A находит число $\alpha = 9$, которое является решением сравнения

$$5 \cdot \alpha \equiv 1 \ (mod\ 22).$$

Абонент B находит число $\beta = 19$, которое является решением сравнения

$$7 \cdot \beta \equiv 1 \ (mod\ 22).$$

Абонент	Секретные ключи	
A	5	9
B	7	19

Пусть абонент A собирается отправить сообщение m=17 абоненту B, $0 < 17 < 22$. Тогда он сначала шифрует сообщение своим первым секретным ключом, находит

$$m_1 \equiv 17^5 \equiv 21\ (mod\ 23), 0 < m_1 < 23$$

и отправляет его абоненту B. Абонент B, в свою очередь, зашифровывает полученное сообщение так же свои первым секретным ключом

$$m_2 \equiv 21^7 \equiv 10\ (mod\ 23), 0 < m_2 < 23$$

и отправляет его обратно абоненту A. Абонент A зашифровывает полученное сообщение своим вторым секретным ключом

$$m_3 \equiv 10^9 \equiv 20\ (mod\ m), 0 < m_3 < 23$$

и вновь отправляет абоненту B. Последний расшифровывает полученное сообщение своим вторым секретным ключом

$$m_4 \equiv 20^{19} \equiv 17\ (mod\ m), 0 < m_4 < 23.$$

а так как $0 < m_4 < 23$, то $m_4 = 17 = m$.

Криптосистема «Открытый ключ»

Пусть абоненты A и B договорились установить между собой секретную переписку с открытым ключом. Тогда каждый их них, независимо друг от друга, выбирает по два больших простых числа, находит их произведение, функцию Эйлера от произведения и выбирает случайное число, меньшее вычисленного значения функции Эйлера и взаимно простого с ним.

$$A\colon p_1, p_2, r_A = p_1 \cdot p_2, \varphi(r_A), \left(a, \varphi(r_A)\right) = 1, 0 < a < \varphi(r_A),$$

$$B\colon q_1, q_2, r_B = q_1 \cdot q_2, \varphi(r_B), \left(b, \varphi(r_B)\right) = 1, 0 < b < \varphi(r_B).$$

Затем публикуется «телефонная книга», доступная всем желающим.

Абонент	Открытые ключи	
A	r_A	a
B	r_B	b

Каждый из абонентов находит свой секретный ключ из сравнений

$$a \cdot \alpha \equiv 1 \ (mod\ r_A), 0 < \alpha < r_A,$$

$$b \cdot \beta \equiv 1 \ (mod\ r_B), 0 < \beta < r_B,$$

В результате получен открытые и секретный ключ, которые удобно внести в книгу (секретный ключ виден только его владельцу).

Абонент	Открытые ключи		Секретный ключ
A	r_A	a	α
B	r_B	b	β

Пусть абонент A отправляет сообщение m абоненту B:

1) A шифрует сообщение m открытым ключом абонента B, который находится в телефонной книге, и находит

$$m_1 \equiv m^b \ (mod\ r_B), 0 < m_1 < r_B,$$

которое отправляет абоненту B.

2) B расшифровывает полученное сообщение своим секретным ключом

$$m_2 \equiv {m_1}^\beta \ (mod\ r_B), 0 < m_2 < r_B.$$

Очевидно, что $m_2 \equiv m^k \ (mod\ r_B)$, где $k \equiv b \cdot \beta \ (mod\ \varphi(r_B))$. Очевидно, что $k \equiv 1 \ (mod\ \varphi(r_B))$. Нетрудно заметить, что

$$m_2 \equiv m \ (mod\ r_B),$$

а так как $0 < m_2 < r_B$, то $m_2 = m$.

Пример. Пусть $p_1 = 7$ и $p_2 = 23$ – простые числа абонента A; $q_1 = 11$ и $q_2 = 17$ – простые числа абонента B; $r_A = 161$ и $r_B = 187$ – произведения простых чисел соответственно,

$(a, 161) = 1, a = 7, \varphi(r_B) = \varphi(187) = 160, (b, 187) = 1, b = 9.$

Затем публикуется «телефонная книга», доступная всем желающим.

Абонент	Открытые ключи	
A	$r_A = 161$	$a = 7$
B	r_B =187	

Каждый из абонентов находит свой секретный ключ из сравнений

$$7 \cdot \alpha \equiv 1 \ (mod\ 161), 0 < \alpha < 161,$$

$$9 \cdot \beta \equiv 1 \ (mod\ 187), 0 < \beta < 187,$$

В результате получены открытые и секретный ключ, которые удобно внести в книгу (секретный ключ виден только его владельцу).

Абонент	Открытые ключи		Секретный ключ
A	$r_A = 161$	$a = 7$	$\alpha = 19$
B	r_B=187	$b = 9$	$\beta = 89$

Пусть абонент A отправляет сообщение m=3 абоненту B:

1) A шифрует сообщение m=3 открытым ключом абонента B, который находится в телефонной книге, и находит

$$m_1 \equiv 3^9 \equiv 48 \ (mod\ 187), 0 < m_1 < 187,$$

которое отправляет абоненту B.

2) В расшифровывает полученное сообщение $m_1 = 48$ своим секретным ключом

$$m_2 \equiv 48^{89}\ (mod\ 187), 0 < m_2 < 187,\ m_2 \equiv 3\ (mod\ r_B).$$

Криптосистема «Электронная подпись»

Изложенная криптосистема с открытым ключом неудобна для получателя, так как он не знает, кто является отправителем сообщения. Этого недостатка нет у криптосистемы «Электронная подпись».

Пусть банкир В и несколько вкладчиков $W_1, W_2,\ W_3, \ldots$ решили установить переписку. Банкир и вкладчики независимо друг от друга выбирают по два больших простых числа и держат их в секрете. Пусть P и Q – простые числа банкира, p_n, q_n – простые числа вкладчика $W_n, n = 1, 2, 3, \ldots$. Далее $R = P \cdot Q, r_n = p_n \cdot q_n$. И пусть банкир В выбирает совершенно случайно целое число S с условиями $0 < S < \varphi(R), \big(S, \varphi(R)\big) = 1$, а каждый из вкладчиков также совершенно случайно и независимо друг от друга выбирает число s_n с условиями $0 < s_n < \varphi(r_n), \big(s_n, \varphi(r_n)\big) = 1,\ n = 1, 2, 3, \ldots$.

После этого публикуется «телефонная книжка»:

Абоненты	Открытые ключи	
B	R	S
W_1	r_1	s_1
W_2	r_2	s_2
…	…	…

Далее каждый, и банкир, и вкладчики находят свои секретные ключи T, t_n из условий

$$S \cdot T \equiv 1 \left(mod\ \varphi(R)\right), 0 < T < \varphi(R),$$

$$s_n \cdot t_n \equiv 1 \left(mod\ \varphi(r_n)\right), 0 < t_n < \varphi(t_n), n = 1, 2, 3, \ldots .$$

В результате получены открытые и секретный ключ, которые удобно внести в книгу (секретный ключ виден только его владельцу).

Абонент	Открытые ключи		Секретный ключ
B	R	S	T
W_1	r_1	s_1	t_1
W_2	r_2	s_2	t_2
…	…	…	…

Предположим, что вкладчик $W = W_1$ собирается дать распоряжение m своему банкиру, и пусть также $r = r_1, t = t_1, s = s_1$ и

$$\mathbf{0 < r < R}.$$

Данное неравенство существенно для дальнейшего шифрования распоряжения m. Будем считать, что $m < r$ и $(m, r) = 1$.

1) Вкладчик шифрует распоряжение m сначала своим секретным ключом t:

$$m_1 \equiv m^t \ (mod\ r), 0 < m_1 < r.$$

2) Далее вкладчик шифрует m_1 открытым ключом S банкира:

$$m_2 \equiv {m_1}^S \ (mod\ R), 0 < m_2 < R.$$

3) Банкир В, получив зашифрованное распоряжение m_2, расшифровывает его пользуясь сначала своим секретным ключом T:

$$m_3 \equiv {m_2}^T \ (mod\ R), 0 < m_3 < R.$$

4) Далее банкир расшифровывает открытым ключом вкладчика:

$$m_4 \equiv {m_3}^s \ (mod\ r), 0 < m_4 < r \text{ и получает } m_4 \equiv m.$$

Предположим, что вкладчик $W = W_1$ собирается дать распоряжение m своему банкиру, и пусть также $r = r_1, t = t_1, s = s_1$ и

$$\mathbf{0 < R < } r.$$

Данное неравенство существенно для дальнейшего шифрования распоряжения m. Будем считать, что $m < R$ и $(m, R) = 1$.

1) Вкладчик шифрует распоряжение m сначала открытым ключом банкира S:

$$m_1 \equiv m^S \ (mod\ R), 0 < m_1 < R.$$

2) Далее вкладчик шифрует m_1 своим секретным ключом t:

$$m_2 \equiv {m_1}^t \ (mod\ r), 0 < m_2 < r.$$

3) Банкир В, получив зашифрованное распоряжение m_2, расшифровывает его пользуясь сначала открытым ключом вкладчика s:

$$m_3 \equiv {m_2}^s \ (mod\ r), 0 < m_3 < r.$$

4) Далее банкир расшифровывает своим секретным ключом T:

$$m_4 \equiv {m_3}^T \ (mod\ R), 0 < m_4 < R \text{ и получает } m_4 \equiv m.$$

Для удобства последовательность передачи распоряжения представим

в виде последовательности

SW OB, SB OW, если $0 < r < R$ и

OB SW, OW SB, если $0 < R < r$

где $R = P \cdot Q, r = p \cdot q,$ произведения простых чисел, выбранных банкиром и вкладчиком, символы S – секретный, O – открытый, B – банкир, W – вкладчик.

Доказательство.

Так как $m_3 \equiv {m_2}^T \, (mod\ R)$, $m_2 \equiv {m_1}^S \, (mod\ R)$, то $m_3 \equiv {m_1}^{ST} \, (mod\ R)$, где $ST \equiv 1 \, (mod\ \varphi(R))$, т.е. $m_3 \equiv m_1 \, (mod\ R)$. Но $0 < m_3 < R$, $0 < m_1 < r < R$, следовательно, $m_3 = m_1$. Имеем

$m_4 \equiv {m_3}^s \equiv {m_1}^s \equiv m^{st} (mod\ r)$, $st \equiv 1 \, (mod\ \varphi\,(r))$ и $(m, r) = 1$.

Значит, $m_4 \equiv m (mod\ r)$, но каждое из них меньше r и больше нуля. Следовательно, эти числа равны: $m_4 = m$. Таким образом, банкир B получит распоряжение m от вкладчика W.

Пример. Пусть банкир B выбирает простые числа 7 и 13, вкладчик W выбирает простые числа 11 и 23, таким образом, $R = 7 \cdot 13 = 91$ и $r = 11 \cdot 23 = 253$. Пусть 5 и 31 – открытые ключи банкира и вкладчика соответственно.

$$5 \cdot 29 \equiv 1\ (mod\ 72),\ 31 \cdot 71 \equiv 1\ (mod\ 220).$$

Тогда «телефонная книжка» имеет вид

Абонент	Открытые ключи		Секретный ключ
B	$R = 91$	$S = 5$	$T = 29$
W	$r = 253$	$s = 31$	$t = 71$

Вкладчик W дает поручение $m = 41$ своему банкиру B и, замечая, что $R < r$, выбирает следующую комбинацию - *OB SW, OW SB.*

1) Вкладчик W шифрует поручение $m = 41$ открытым ключом банкира, а потом своим секретным ключом:

$$m_1 \equiv m^5 \equiv 41^5 \equiv 6\ (mod\ 91);$$

$$m_2 \equiv {m_1}^{71} \equiv 6^{71} \equiv 94\ (mod\ 253).$$

2) Банкир, получив зашифрованное поручение $m_2 = 94$ и, замечая, что $R < r$, расшифровывает его сначала открытым ключом вкладчика, а потом

$$m_3 \equiv {m_2}^{31} \equiv 94^{31} \equiv 6\ (mod\ 253),$$

$$m_4 \equiv {m_3}^{29} \equiv 6^{29} \equiv 41\ (mod\ 91).$$

А так как 41<91, то банкир делает вывод, что 41 и есть распоряжение этого вкладчика.

7.14. Коды, исправляющие несимметрические ошибки

Многие годы перед математиками-кодировщиками стоит проблема помехоустойчивого кодирования. - процесса преобразования информации, способного обнаружить и исправить ошибки, возникающие при передаче информации по каналам передачи данных.

Процесс помехоустойчивого кодирования заключается во введении избыточных символов, позволяющих на основе информационных, корректировать полученную информацию.

Но нередко можно встретить каналы, обладающие асимметричным типом ошибок, таких, в которых доминируют замещения определенного типа, а замещения остальных видов практически невозможны. В этом случае так же применяют избыточные коды, но хотелось бы избежать их недостатков.

Замещение символа

Попробуем создать неизбыточный код, способный исправлять замещение вида $0 \to 1$, тогда как замещение $1 \to 0$ практически невозможно. Заметим, что в принятом слове не нужно анализировать нулевые символы, а потому будем проверять только единичные.

Пусть отправлено двоичное слово $v = x_1 x_2 \dots x_n$. Составим сумму

$$S(\vartheta) = \sum_{i=1}^{n} x_i \cdot i,$$

чтобы ненулевые слагаемые соответствовали только единичным символам и совпадали с номерами этих символов.

Алгоритм исправления одной ошибки:

1. Построим код $V_{n,l}$. Выделим параметр l, для которого в данном коде будут присутствовать только слова v такие, что

$$S(\vartheta) \equiv 0 \ (mod\ l).$$

2. Пусть получено слово $u = x_1 x_2 \dots x_n$. Если ошибка в j-м символе, то

$$S(u) \equiv S(\vartheta) + j \equiv j \ (mod\ l),$$

т.е. значение данной суммы в сравнении по модулю l даст номер позиции ошибки.

Пример. Рассмотрим двоичный код $V_{4,5} = \{0000, 1001, 0110, 1111\}$. По несимметрическому каналу связи получены следующие кодовые слова: $u = 1110$. Получим сумму $S(u) = 1 + 2 + 3 = 6 \equiv 1(5)$, значит ошибка в позиции $j = 1$. Делаем вывод, что отправлено слово

$v = 0110$.

$u = 0100$. Получим сумму $S(u) = 2 \equiv 2(5)$, значит ошибка в позиции $j = 2$ отправлено слово $v = 0000$.

Заметим, что достоинства этого кода - отсутствие избыточных символов, простота и скорость проверки; недостатки – невозможность исправления более одной ошибки. Коды $V_{n,l}$ так же способны исправлять так называемые выпадения и вставки, характерные для несимметричных каналов.

Коды с проверкой на выпадение символа

Допустим, что в двоичном коде $V_{n,l}$ при передаче по несимметричному каналу связи в некотором слове $v = x_1 x_2 \dots x_n$ произошло выпадение одного символа и принято слово $u = y_1 y_2 \dots y_{n-1}$.

Алгоритм исправления ошибки:

1. Определим n_1 – число единиц, n_0 – число нулей, правее выпавшего символ с помощью суммы

$$S(u) = \sum_{i=1}^{n-1} i \cdot y_i.$$

2. Рассмотрим $S(v) - S(u)$, т.к. $S(v) \equiv 0(mod\ l)$, то

$$S(v) - S(u) \equiv -S(u)(\ mod\ l).$$

А потому если $-S(u) = n_1$, то выпал 0, если $-S(u) = n - n_0$, то выпала 1.

3. Если $w(u)$ – вес двоичного кодового слова u, равный количеству единичных символов кодового слова, то

$$n_1 \le w(u) < n - n_0 \le n.$$

4. При выпадении нулевого символа, надо вставить его так, чтобы справа от него были единицы, число которых равно вычету числа $-S(u)$ по модулю l. При выпадении единичного символа, в слово надо вставить единицу так, чтобы справа от него были нули, число которых равно разности n и вычета числа $-S(u)$ по модулю l.

Пример. Дан двоичный код $V_{4,5} = \{0000, 1001, 0110, 1111\}$. Принято двоичное кодовое слово $u = 1\ 0\ 1$. Сумма вес кодового слова $w(u) = 2$. Вычислим $-S(u) = -4 \equiv 1(5)$. Значит $n_1 \le 2 < n - n_0 \rightarrow n_1 = 1$. Делаем вывод, что выпал ноль. Вставим его так, чтобы правее него была одна единица. Значит переданное кодовое слово v= 1001.

Пример. Дан двоичный код $V_{4,5} = \{0000, 1001, 0110, 1111\}$. Принято двоичное кодовое слово $u = 010$. Определим $S(u) = 2$,

вес кодового слова $w(u) = 1$. Вычислим $-S(u) = -2 \equiv 3(5)$. В результате получим $n_1 \leq 1 < n - n_0 \rightarrow n - n_0 = 3$. Делаем вывод, что выпала единица. Вставим ее так, чтобы правее нее был один ноль. Значит переданное кодовое слово $v = 0110$.

Коды с проверкой на вставку символа

Предположим, что при передаче в кодовом слове $v = x_1x_2 \dots x_n$ произошла вставка символа и принято слово $u = y_1y_2 \dots y_{n+1}$, для которого определим коэффициент k следующим образом:

$$S(u) \equiv k(mod\ l).$$

Алгоритм исправления ошибки:

1) Если $k=0$, то отбрасываем последний символ;

2) $0 < k < w(u)$, то отбрасываем 0, правее которого k единиц;

3) $k = w(u)$, то отбрасывали первый символ;

4) $k > w(u)$, то отбрасываем 1, правее которой $n+1-k$ нулей.

Пример. Дан код $V_{4,5} = \{0000, 1001, 0110, 1111\}$.

Принято слово $u = 10011$. Сумма $S(u) \equiv 1 + 4 + 5 = 10 \equiv 0(5)$, $k = 0$. Отбрасываем последний символ – отправленное слово v=1001.

Для полученного слова $u = 00110$, сумма $S(u) = 3 + 4 = 7 \equiv 2(5)$, тогда $k = 2$, $w(u) = 2$, значит отбрасываем первый символ. Переданное слово $v = 0110$.

Отметим, что такие коды могут быть любой длины. Обязательным условием является получение параметра l, для которого

$$S(v) \equiv 0(mod\ l).$$

Благодаря своим эффектным достоинствам и простоте коды, исправляющие несимметричные ошибки, успешно применяются в системах передачи и хранения информации, в вычислительной технике, различных автоматизированных цифровых устройствах.

Упражнения

1. Передать сообщение m от одного абонента другому, используя криптосистему «Открытый ключ».
   a) $m = 11, p_1 = 13, p_2 = 17$;
   b) $m = 7, p_1 = 11, p_2 = 19$;
   c) $m = 5, p_1 = 7, p_2 = 23$;
   d) $m = 13, p_1 = 17, p_2 = 23$.

2. Передать сообщение m от одного абонента другому, используя криптосистему «Без передачи ключа».
   e) $m = 11, p = 13$;
   f) $m = 7, p = 19$;
   g) $m = 5, p = 23$;
   h) $m = 13,\ p = 29$.
3. Передать сообщение m от одного вкладчика банкиру, используя криптосистему «Электронная подпись».
   i) $m = 11, p_1 = 13, p_2 = 17, q_1 = 7, q_2 = 19$;
   j) $m = 7, p_1 = 11, p_2 = 19, q_1 = 17, q_2 = 23$;
   k) $m = 5, p_1 = 7, p_2 = 23, q_1 = 3, q_2 = 31$;
   l) $m = 13, p_1 = 17, p_2 = 23, q_1 = 5, q_2 = 11$.
4. Дан код $V_{4,5} = \{0000, 1001, 0110, 1111\}$. В полученных сообщениях исправить ошибку:
   a) 11001;
   b) 10001;
   c) 001;
   d) 100;
   e) 1101;
   f) 1011.

Посвящение в тайну

Бенджамен Франклин (Franklin) однажды сказал: «Трое могут хранить тайну, если двое из них мертвы.» В этом параграфе мы изучаем безопасную систему допуска живых к секретным сведениям, основанную на китайской теореме об остатках. Представьте себе следующую ситуацию. Подвал банка должен открываться каждый день. В банке служат пять старших кассиров, имеющих доступ к подвалу. По причинам безопасности руководство банка предпочитает систему, требующую присутствия хотя бы двух из этой пятерки для возможности открыть подвал. Проблема в том, чтобы подвал могли открыть *любые* два старших кассира.

Рассмотрим эту проблему в более общем виде. Для того, чтобы открыть подвал банка, необходимо знать код, который можно считать натуральным числом s. Мы хотим распределить этот код между n старшими кассирами так, чтобы каждый из них знал что-то об s. Назовем такую частичную информацию *фрагментом* кода. Более того, открыть подвал должно быть невозможно, если в банке присутствуют менее k старших кассиров, где $k \geqslant 2$ — натуральное число, меньшее n.

Мы добьемся этого условия, распределив информацию о коде таким образом, что

- число s *легко* определяется, если известно k или более фрагментов;
- число s *трудно* определимо, если известно менее k фрагментов.

Фрагменты кода, сообщаемые каждому из старших кассиров, — это, в действительности, элементы множества $\mathbb{S}$, состоящего из n упорядоченных пар натуральных чисел. Чтобы построить $\mathbb{S}$, выберем сначала множество $\mathcal{L}$ из n попарно взаимно простых чисел. Пусть N — произведение наименьших k из них, а M — произведение $k-1$ наибольших. Будем говорить, что k является *порогом для* $\mathcal{L}$, если $M < N$. Из этого условия следует, что произведение любых k (или более) элементов из $\mathcal{L}$ всегда больше, чем N, а произведение $k-1$ (или менее) его элементов — всегда меньше M.

Предположим, код s выбран так, что $M < s < N$, а множество $\mathbb{S}$ состоит из пар (m, s_m), где $m \in \mathcal{L}$, а s_m — вычет числа s по модулю m. Эти пары и являются теми *фрагментами кода*,

которые сообщаются старшим кассирам. Тот факт, что множество $\mathfrak{L}$ имеет порог $k \geqslant 2$, обеспечивает неравенство $s > m$ для каждого $m \in \mathfrak{L}$. В частности, $s_m < s$ для любого $m \in \mathfrak{L}$.

Что произойдет, если k или более старших кассиров находятся в банке? В этом случае известны t $(\geqslant k)$ пар из множества $\mathbb{S}$. Обозначив эти пары через $(m_1, s_1), \ldots, (m_t, s_t)$, рассмотрим систему сравнений:

$$\begin{cases} x \equiv s_1 \pmod{m_1}, \\ x \equiv s_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv s_t \pmod{m_t}. \end{cases}$$

Элементы множества $\mathfrak{L}$ попарно взаимно просты. Значит, по китайской теореме об остатках, эта система имеет решение $0 \leqslant x_0 < m_1 \cdots m_t$. Но совпадает ли x_0 с s? Это как раз та причина, по которой мы накладывали требование: $\mathfrak{L}$ имеет порог k. Поскольку $t \geqslant k$, то наше требование влечет:

$$m_1 \cdots m_t \geqslant N > s.$$

Но s тоже удовлетворяет системе, и по китайской теореме об остатках

$$x_0 \equiv s \pmod{m_1 \cdots m_t}.$$

А так как s и x_0 — натуральные числа, меньшие $m_1 \cdots m_t$, то $s = x_0$.

Предположим теперь, что в банке находится менее k старших кассиров. Несмотря на то, что t теперь меньше k, мы все равно сможем решить систему. Пусть x_0 — наименьшее неотрицательное решение, тогда $0 \leqslant x_0 < m_1 \cdots m_t$. Но произведение меньшего, чем k количества элементов из $\mathfrak{L}$ всегда меньше M; так что $x_0 < M < s$. Следовательно, решения системы не достаточно для восстановления кода s. Однако как x_0, так и s — решения системы (6.1), поэтому

$$s = x_0 + y \cdot (m_1 \cdots m_t),$$

где y — некоторое натуральное число. Неравенство

$$N > s > M > x_0$$

влечет

$$\frac{M - x_0}{m_1 \cdots m_t} \leqslant y \leqslant \frac{s - x_0}{m_1 \cdots m_t} \leqslant \frac{N - x_0}{m_1 \cdots m_t}.$$

Приходим к выводу: если $t < k$, то для восстановления кода s нам предстоит отыскивать недостающий множитель y среди более чем

$$d = \left[\frac{N - M}{M}\right]$$

целых чисел. Выбрав модули так, чтобы d оказалось очень большим, мы сделаем задачу поиска y практически нерешаемой.

Для завершения разбора задачи осталось осветить один вопрос: можно ли найти множество $\mathcal{L}$, удовлетворяющее всем необходимым требованиям? Ответ на него положителен, но нуждается в результатах о распределении простых чисел, которые выходят за рамки данной книги.

Сделаем обзор рассмотренной конструкции. Для нее требуются начальные данные: число n старших кассиров, имеющих доступ в подвал банка, и наименьшее число k из них, присутствие которых в банке достаточно для открытия подвала. Первое число определяет размер множества $\mathcal{L}$, а второе — его порог k. Далее нам нужно подобрать множество $\mathcal{L}$ из n элементов с порогом k (эту часть конструкции мы подробно не обсуждали), и вычислить M и N, определенные выше. Напомним,

что $\mathfrak{L}$ нужно выбирать с таким расчетом, чтобы число d, о котором мы говорили, было как можно больше; в противном случае код может быть разгадан простым перебором. Код s — натуральное число, которое выбирается лежащим между M и N. Теперь можно вычислить элементы множества $\mathbb{S}$ и сообщить их сотрудникам. Конечно, безопасность этой схемы зависит от того, насколько велико k, уменьшающее вероятность, что одновременно k кассиров из одного банка окажутся нечестными. Если это все-таки произойдет, то нам придется утешать себя мыслью, что не существует систем безопасности 100-процентной надежности.

Рассмотрим пример. Допустим, что в банке работают 5 старших кассиров и из соображений безопасности по крайней мере двое из них должны присутствовать при открытии подвала. Значит, $\mathfrak{L}$ должно состоять из пяти элементов, а его порог равен 2. Выбрав элементы $\mathfrak{L}$ среди малых простых чисел, получим:

$$\mathfrak{L} = \{11,\ 13,\ 17,\ 19,\ 23\}.$$

Произведение двух наименьших чисел этого множества равно $N = 11 \cdot 13 = 143$. С другой стороны, поскольку $k = 2$, произведение $k - 1$ наибольших простых из $\mathfrak{L}$ в действительности равно его максимальному элементу. Таким образом, $M = 23$ и $\mathfrak{L}$ имеет порог 2. Код s может быть любым целым числом, лежащим между 23 и 143. Пусть $s = 30$. Тогда

$$\mathbb{S} = \big\{(11, 19), (13, 17), (17, 13), (19, 11), (23, 7)\big\}.$$

Наконец, что будет, если в банке присутствуют старшие кассиры с фрагментами (17,13) и (23,7)? Код из их фрагментов получается как наименьшее число, удовлетворяющее системе:

$$\begin{cases} x \equiv 13 \pmod{17}, \\ x \equiv 7 \pmod{23}. \end{cases}$$

Легко увидеть, что таким числом будет 30. Этот код корректен, он позволяет открыть подвал.

1. Практическое занятие по теме «Делимость целых чисел. Теорема о делении с остатком. НОД и НОК. Взаимно простые числа»

Пример 1. Разделить ± 367 на ± 33.

Доказательство. Так как $363 = 33 \cdot 11 < 367 < 33 \cdot 12 = 396$, то $367 = 23 \cdot 11 + 4$. Здесь 11 — неполное частное, 4 — остаток.

Разделим -367 на 33. Для этого найдем целое q, такое, что $33q \leq -367 < 33(q+1)$. Так как $33(-12) = -396 < -367 < 33(-11)$, то $-367 = 33(-12) + 19$.

Делим на -23. Берем $367 = 33 \cdot 11 + 4$ и записываем в виде $367 = (-33)(-11) + 4$. Для деления -367 на -33 берем $-367 = 33(-12) + 19$ и записываем в виде $-367 = (-33)12 + 19$.

Ответ. $367 = 33 \cdot 11 + 4$, $367 = (-33)(-11) + 4$,
$-367 = 33(-12) + 19$, $-367 = (-33)12 + 19$. □

Пример 2. Докажите, что при любом натуральном n выражение $n^3 + 5n$ делится на 6.

Доказательство. Воспользуемся методом математической индукции. Если $n = 0$, то выражение делится на 6. Предположим, что утверждение

справедливо при $n = k$, где k — целое неотрицательное число, т.е. что число $k^3 + 5k$ делится на 6. Тогда установим, что утверждение справедливо при $n = k + 1$, т.е что число $(k+1)^3 + 5(k+1)$ делятся на 6.

Рассмотрим выражение $(k+1)^3 + 5(k+1)$. После преобразования получим сумму двух слагаемых $\left(k^3 + 5k\right) + \left(3k^2 + 3k + 6\right)$, из которых первое делится на 6 по предположению индукции, а второе, представленное в виде $3(k(k+1)+2)$, делится на 6, так как содержит множитель 3 и сумму, у которой каждое слагаемое делится на 2 (первое — как произведение двух последовательных целых чисел).

Итак, на основании принципа математической индукции делаем вывод, что при любом натуральном n выражение $n^3 + 5n$ делится на 6.

□

Пример 3. Вычислите НОД$(1152, 840)$. Выразите НОД через исходные числа.

Доказательство. Применим алгоритм Евклида, то есть запишем систему равенств:

$$1152 = 840 \cdot 1 + 312,$$

$$840 = 312 \cdot 2 + 216,$$

$$312 = 216 \cdot 1 + 96,$$

$$216 = 96 \cdot 1 + 24,$$

$$96 = 24 \cdot 4.$$

Последний отличный от нуля остаток $24 = \text{НОД}(1152, 840)$. Выражая остатки из полученной системы равенств, имеем

$$24 = 216 - 2 \cdot 96 = 216 - 2 \cdot (312 - 216) = (-2) \cdot 312 + 3 \cdot 216 =$$

$$= (-2) \cdot 312 + 3 \cdot (840 - 2 \cdot 312) = 3 \cdot 840 - 8 \cdot 312 =$$

$$= 3 \cdot 840 - 8 \cdot (1152 - 840) = (-8) \cdot 1152 + 11 \cdot 840.$$

Ответ. $\text{НОД}(1152, 840) = 24 = (-8) \cdot 1152 + 11 \cdot 840.$

□

Пример 4. Найдите натуральные числа a и b, если $\text{НОД}(a, b) = 12$, а $\text{НОК}(a, b) = 420$.

Доказательство. Пусть $a = 12m$, $b = 12n$. Так как $\text{НОД}(a, b) = 12$, то m и n — взаимно простые натуральные числа. Пусть для определенности $m < n$. Используя связь НОК и НОД натуральных чисел, имеем $12 \cdot 420 = 24m \cdot 24n$, откуда $m \cdot n = 35 = 5 \cdot 7$. Поскольку m и n взаимно просты, то возможны два случая:

1) $m = 1$, $n = 35$. Тогда $a = 12$, $b = 420$;

2) $m = 5$, $n = 7$. Тогда $a = 60$, $b = 84$.

Ответ. $a = 12$, $b = 420$ или $a = 60$, $b = 84$. □

Пример 5. Найдите НОД(29 568, 8580).

Доказательство. Шаг 1. Выделяем наибольшую степень двойки, на которую делятся эти числа: $29\,568 = 2^2 \cdot 7392$, $8580 = 2^2 \cdot 2145$. Запоминаем 2^2.

Шаг 2. Число 7392 четное. Делим его на максимально возможную степень 2, оставляя второе число 2145 без изменения. $7392 = 2^5 \cdot 231$. Теперь надо искать $d = \text{НОД}(231, 2145)$.

Шаг 3. Вычитаем из большего числа 2145 меньшее 231. Имеем: $2145 - 231 = 1914$, $d = \text{НОД}(231, 1914)$.

Шаг 4. Применяем к 1914 действие шага 2. Получаем $1914 = 2 \cdot 957$. Теперь $d = \text{НОД}(231, 957)$, и надо возвращаться к действиям шага 2 и шага 3 и т. д.

Все эти вычисления записываются следующим образом.

шаг 1	$29\,568 = 2^2 \cdot 7392$	$8580 = 2^2 \cdot 2145$
шаг 2	$7392 = 2^5 \cdot 231$	
шаг 3		$2145 - 231 = 1914$
шаг 2		$1914 = 2 \cdot 957$
шаг 3		$957 - 231 = 726$
шаг 2		$726 = 2 \cdot 363$
шаг 3		$363 - 231 = 132$
шаг 2		$132 = 2^2 \cdot 33$
шаг 3	$231 - 33 = 198$	
шаг 2	$198 = 2 \cdot 99$	
шаг 3	$99 - 33 = 66$	
шаг 2	$66 = 2 \cdot 33$	
шаг 3	$33 - 33 = 0$	

Итак, НОД$(29\,568, 8580) = 2^2 \cdot 33 = 132$.

Вычислим НОД с помощью алгоритма Евклида. $29\,568 = 8580 \cdot 3 + 3828$, $8580 = 3828 \cdot 2 + 924$, $3828 = 924 \cdot 4 + 132$, $924 = 132 \cdot 7$.

Ответ. НОД$(29\,568, 8580) = 132$. □

Пример 6. Докажите, что для любого натурального a дробь $\frac{a+1}{2a+3}$ несократима.

Доказательство. Предположим, что $(a+1, 2\,a+3) = d$. Тогда разность $(2a+3) - 2\,(a+1) = 1$ делится на d.

Следовательно, $d = 1$. Значит, дробь $\frac{a+1}{2a+3}$ несократима. □

Пример 7. Разложите 3059 на простые множители.

Доказательство. Так как $\sqrt{3059} < 56$, то надо испытать все простые числа не более 56. Числа 2, 3, 5 не делят 3059, а 7 делит $3059 = 7 \cdot 437$. Числа 11, 13, 17 не делят 437, а 19 делит $437 = 19 \cdot 23$. Число 23 также простое число.

Ответ. $3059 = 7 \cdot 19 \cdot 23$. □

Пример 8. Найдите все простые числа между 2640 и 2660.

Доказательство. Так как $\sqrt{2659} = 51,565...$, то наименьший простой делитель указанных чисел ≤ 47. Выпишем указанные числа 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659 и будем отсеивать числа, кратные простым числам,

не превышающим 47. Сначала удалим каждое четное число: 2641, 2643, 2645, 2647, 2649, 2651, 2653, 2655, 2657, 2659. Затем найдем первое число, кратное 3, используя признак делимости на 3 (этим числом является 2643), и удалим его, а также каждое третье число. Останутся 2641, 2645, 2647, 2651, 2653, 2657, 2659. Из этих чисел удалим число 2645, т.к. оно делится на 5. Так как $2641 = 7 \cdot 377 + 2$, то наименьшее кратное 7 число — пятое от 2641, т.е. 2646; но оно уже удалено, а следующее число кратное 7 — 2653. После его удаления останутся числа 2641, 2647, 2651, 2657, 2659. Заметим, что число 2641 при делении на простое число 11 дает в остатке 1. Значит, следующее число, которое делится на 11, будет 2651. Далее выясняется, что ни одно из оставшихся чисел не делится ни на 13, ни на 17.Следующее простое число 19 делит нацело число 2641. Таким образом, остаются числа 2647, 2657 и 2659, которые не делятся ни на 23, ни на 29, 31, 37, 41, 43, 47, а значит, оставшиеся числа являются простыми.

Ответ. 2647, 2657, 2659. □

Пример 9. Найти простое число p, чтобы число $2p^2 + 1$ было также простым.

Доказательство. Разобьем множество простых чисел на три класса: класс простых чисел $3q$ $(q = 1)$, класс простых чисел вида $3q+1$ $(q = 2, 4, \ldots)$ и класс простых чисел вида $3q + 2$ $(q = 1, 3, \ldots)$. Единственное простое число первого класса $p = 3$ удовлетворяет требованиям задачи. При

$p = 3q + 1$ или $p = 3q + 2$ число $2p^2 + 1$ является составным – кратным трем. □

Пример 10. Методом Евклида докажите, что простых чисел вида $3n + 1$ бесконечно.

Доказательство. Все множество натуральных чисел разобьем на три подмножества с общими членами: $3u$, $3u+1$, $3u+2$; среди чисел первого подмножества имеется лишь одно простое число 3, остальные простые числа входят в два других подмножества. Допустим, что P – наибольшее простое число вида $3n + 1$; запишем число $N = 3 \cdot 7 \cdot 13 \cdot 19 \cdot \ldots \cdot P + 1$, где в произведение включено число 3 и все простые числа вида $3n + 1$; очевидно, число N будет вида $3n + 1$ и, следовательно, $N = 3s + 1$.

Число N не может быть простым, так как $N > P$, но оно не может иметь простыми делителями число 3 и числа вида $3n+1$; следовательно, все его простые делители вида $3u + 2$, откуда $N = 3t + 2$, но равенство $3t + 2 = 3s + 1$ невозможно ни при каких целых положительных значениях t и s, так как последнее равенство может быть переписано в виде $3(t - s) = -1$. Полученное противоречие доказывает существование бесконечного множества простых чисел вида $3n + 1$. □

Задачи для самостоятельного решения

1. Найдите неполное частное и остаток от деления числа a на число b.

1.1. $a = \pm 761$, $b = \pm 13$. 1.2. $a = \pm 652$, $b = \pm 21$.
1.3. $a = \pm 529$, $b = \pm 15$. 1.4. $a = \pm 632$, $b = \pm 18$.
1.5. $a = \pm 437$, $b = \pm 24$. 1.6. $a = \pm 512$, $b = \pm 27$.
1.7. $a = \pm 521$, $b = \pm 29$. 1.8. $a = \pm 530$, $b = \pm 28$.
1.9. $a = \pm 621$, $b = \pm 41$. 1.10. $a = \pm 606$, $b = \pm 19$.
1.11. $a = \pm 723$, $b = \pm 35$. 1.12. $a = \pm 785$, $b = \pm 39$.
1.13. $a = \pm 282$, $b = \pm 32$. 1.14. $a = \pm 241$, $b = \pm 24$.
1.15. $a = \pm 338$, $b = \pm 15$. 1.16. $a = \pm 396$, $b = \pm 26$.
1.17. $a = \pm 873$, $b = \pm 42$. 1.18. $a = \pm 812$, $b = \pm 34$.
1.19. $a = \pm 927$, $b = \pm 48$. 1.20. $a = \pm 986$, $b = \pm 47$.

2. Методом математической индукции докажите, что для любого натурального числа n число a делится на b.

2.1. $a = n(n+1)(2n+1)$, $b = 6$.
2.2. $a = n^3 + 65n$, $b = 6$.
2.3. $a = n(n^2+5)$, $b = 6$.
2.4. $a = n(2n+1)(7n+1)$, $b = 6$.
2.5. $a = n(n^3 + 2n^2 - n + 22)$, $b = 24$.
2.6. $a = n^8 + 4n^7 + 6n^6 + 4n^5 + n^4$, $b = 16$.
2.7. $a = n^4 - 2n^3 + 11n^2 + 62n$, $b = 24$.
2.8. $a = n^4 + 3n^3 - n^2 - 3n$, $b = 6$.
2.9. $a = n^5 - n$, $b = 10$.
2.10. $a = n^7 - n$, $b = 42$.
2.11. $a = 2n^3 - 3n^2 + n$, $b = 6$.

2.12. $a = 9n^5 - 5n^3 - 4n$, $b = 120$.
2.13. $a = n^4 + 6n^3 + 11n^2 + 6n$, $b = 24$.
2.14. $a = n^5 - 5n^3 + 4n$, $b = 120$.
2.15. $a = n^4 + 2n^3 + 3n^2 + 2n$, $b = 8$.
2.16. $a = n^3 + 5n + 12$, $b = 6$.
2.17. $a = (n+2)(n^2 + 4n + 9)$, $b = 6$.
2.18. $a = n^3 + (n+1)^3 + (n+2)^3$, $b = 9$.
2.19. $a = (n-1)(n^2 + n + 12)$, $b = 6$.
2.20. $a = n^4 + 6n^3 + 11n^2 + 6n$, $b = 24$.

3. С помощью алгоритма Евклида найдите НОД(a, b) и выразите его через исходные числа. Используя связь НОД и НОК двух натуральных чисел, вычислите НОК(a, b).

3.1. $a = 5544$, $b = 7644$. 3.2. $a = 2585$, $b = 7975$.
3.3. $a = 1188$, $b = 3080$. 3.4. $a = 4704$, $b = 9100$.
3.5. $a = 1296$, $b = 6600$. 3.6. $a = 1463$, $b = 6391$.
3.7. $a = 1711$, $b = 4189$. 3.8. $a = 1891$, $b = 4087$.
3.9. $a = 1739$, $b = 2867$. 3.10. $a = 2911$, $b = 4189$.
3.11. $a = 3713$, $b = 4187$. 3.12. $a = 4399$, $b = 3403$.
3.13. $a = 5251$, $b = 4183$. 3.14. $a = 5551$, $b = 3367$.
3.15. $a = 6499$, $b = 5335$. 3.16. $a = 7171$, $b = 3131$.
3.17. $a = 9559$, $b = 3509$. 3.18. $a = 4067$, $b = 1127$.
3.19. $a = 8099$, $b = 2275$. 3.20. $a = 7553$, $b = 1411$.

4. Вычислите НОД(a, b) с помощью бинарного алгоритма.

4.1. $a = 46\,368$, $b = 41\,496$. 4.2. $a = 27\,456$, $b = 24\,640$.
4.3. $a = 43\,776$, $b = 56\,448$. 4.4. $a = 47\,600$, $b = 39\,984$.
4.5. $a = 50\,016$, $b = 49\,728$. 4.6. $a = 49\,920$, $b = 74\,400$.
4.7. $a = 39\,744$, $b = 26\,712$. 4.8. $a = 49\,000$, $b = 38\,080$.
4.9. $a = 49\,104$, $b = 60\,192$. 4.10. $a = 49\,504$, $b = 75\,344$.
4.11. $a = 82\,944$, $b = 52\,800$. 4.12. $a = 75\,264$, $b = 36\,400$.
4.13. $a = 76\,032$, $b = 49\,280$. 4.14. $a = 82\,720$, $b = 63\,800$.
4.15. $a = 44\,352$, $b = 30\,576$.

5. Известны НОД(a, b) и НОК(a, b). Найдите натуральные числа a и b.

5.1. НОД$(a, b) = 16$, НОК$(a, b) = 1584$.
5.2. НОД$(a, b) = 15$, НОК$(a, b) = 630$.
5.3. НОД$(a, b) = 22$, НОК$(a, b) = 3630$.
5.4. НОД$(a, b) = 19$, НОК$(a, b) = 5187$.
5.5. НОД$(a, b) = 14$, НОК$(a, b) = 2856$.
5.6. НОД$(a, b) = 15$, НОК$(a, b) = 6900$.
5.7. НОД$(a, b) = 30$, НОК$(a, b) = 15\,660$.
5.8. НОД$(a, b) = 27$, НОК$(a, b) = 5589$.
5.9. НОД$(a, b) = 36$, НОК$(a, b) = 6480$.
5.10. НОД$(a, b) = 12$, НОК$(a, b) = 1872$.
5.11. НОД$(a, b) = 21$, НОК$(a, b) = 756$.
5.12. НОД$(a, b) = 26$, НОК$(a, b) = 4914$.

5.13. НОД$(a,b)=35$, НОК$(a,b)=8925$.
5.14. НОД$(a,b)=18$, НОК$(a,b)=4896$.
5.15. НОД$(a,b)=14$, НОК$(a,b)=4410$.

6. Сократима ли дробь? Если сократима, то на какое число (в заданиях 6.11 – 6.20 элементы a и b взаимно простые).

6.1. $\frac{12n+5}{6n+3}$. 6.2. $\frac{6n+5}{8n+7}$. 6.3. $\frac{5n+2}{3n+2}$. 6.4. $\frac{21n+4}{14n+3}$.
6.5. $\frac{9n+8}{7n+4}$. 6.6. $\frac{n}{2n+1}$. 6.7. $\frac{n^3+2n}{n^4+3n^2+1}$. 6.8. $\frac{3n+2}{4n+3}$.
6.9. $\frac{7n+5}{3n+2}$. 5.10. $\frac{2n^2-1}{2n+1}$. 6.11. $\frac{a^2+b^2}{ab}$. 6.12. $\frac{a^3+b^3}{ab}$.
6.13. $\frac{a^3-b^3}{ab}$. 6.14. $\frac{a^2+ab+b^2}{a+b}$. 6.15. $\frac{a+b}{a^2-ab+b^2}$. 6.16. $\frac{a+b}{a^2+ab+b^2}$.
6.17. $\frac{a^2-ab+b^2}{a+b}$. 6.18. $\frac{a^2-b^2}{ab}$. 6.19. $\frac{a+b}{ab}$. 6.20. $\frac{a-b}{ab}$.

7. Разложите число a на простые множители.

7.1. $a=420$. 7.2. $a=2401$. 7.3. $a=38808$. 7.4. $a=3591$.
7.5. $a=11856$. 7.6. $a=44044$. 7.7. $a=30420$. 7.8. $a=38115$.
7.9. $a=55242$. 7.10. $a=22015$. 7.11. $a=6118$. 7.12. $a=5124$.
7.13. $a=1512$. 7.14. $a=2142$. 7.15. $a=2145$. 7.16. $a=2130$.
7.17. $a=2430$. 7.18. $a=2448$. 7.19. $a=3220$ 7.20. $a=4225$.

8. Найдите все простые числа между числом a и числом b.

8.1. $a=1300$, $b=1350$. 8.2. $a=1350$, $b=1400$.
8.3. $a=1400$, $b=1450$. 8.4. $a=1450$, $b=1500$.
8.5. $a=1500$, $b=1550$. 8.6. $a=1550$, $b=1600$.
8.7. $a=1600$, $b=1650$. 8.8. $a=1650$, $b=1700$.
8.9. $a=1700$, $b=1750$. 8.10. $a=1750$, $b=1800$.

8.11. $a = 2320$, $b = 2350$. 8.12. $a = 2640$, $b = 2680$.
8.13. $a = 2680$, $b = 2720$. 8.14. $a = 2720$, $b = 2760$.
8.15. $a = 2760$, $b = 2800$.

9.1. Найти натуральные значения n, такие, чтобы числа n, $n + 10$, $n + 14$ были простыми.

9.2. Найти все простые p, для которых число $p^2 - 1$ является простым.

9.3. Найти все простые p, для которых число $p^2 - 36$ является простым.

9.4. Найти все простые p, для которых число $p^2 - 324$ является простым.

9.5. Найти все простые p, для которых число $p^2 - 900$ является простым.

9.6. Найти все простые p, для которых число $p^2 - 1296$ является простым.

9.7. Найти все простые p, для которых число $8p^2 + 1$ является простым.

9.8. Найти все простые p, для которых число $p^4 - 6$ является простым.

9.9. Найти все простые p, для которых число $2^p + 1$ является простым.

9.10. Найти такое простое число p, чтобы числа $4p^2 + 1$ и $6p^2 + 1$ оба были простыми.

9.11. Найти такое простое число p, чтобы числа $p^2 - 6$ и $p^2 + 16$ оба были простыми.

9.12. Найти такое простое число p, чтобы числа $p^2 + 4$ и $p^2 + 16$ оба

были простыми.

9. 13. Найдите такое простое число p, чтобы числа $p+2$, $p+6$, $p+8$, $p+12$, $p+14$ были простыми.

9. 14. Найдите такое простое число p, чтобы числа $p+10$ и $p+20$ были простыми.

9. 15. Найдите такое простое число p, чтобы числа $p+10$ и $p+14$ были простыми.

Докажите методом Евклида, что простых чисел вида a, бесконечно много, где $m \in \mathbb{N}$.

9. 16. $a = 4m - 1$.

9. 17. $a = 4m + 3$.

9. 18. $a = 6m + 5$.

9. 19. $a = 3m + 2$.

2. Практическое занятие по теме «Системы счисления»

Пример 1. Переведите числа $3A_{16}$ и $11,01_2$ в десятичную систему счисления.

Доказательство. Воспользуемся алгоритмом предложенным в п.1.

$3A_{16} = 3 \cdot 16^1 + 10 \cdot 16^0 = 58_{10}$;

$11,01_2 = 1 \cdot 2^1 + 1 \cdot 2^0 + 0 \cdot 2^{-1} + 1 \cdot 2^{-2} = 3,25_{10}$.

Ответ. $3A_{16} = 58_{10}$; $11,01_2 = 3,25_{10}$. □

Пример 2. Переведите целое число 925 из десятичной системы счисления в восьмеричную.

Доказательство.

$$\begin{array}{r|l} 925 & 8 \\ \cline{2-2} 920 & 15 \quad \vert \quad 8 \\ \cline{2-3} 5 & 8 \quad \vert \quad 1 \\ \cline{3-3} & 7 \end{array}$$

Ответ. $925_8 = 175_8$. □

Пример 3. Переведите дробь $0,129$ из десятичной системы счисления в шестнадцатеричную с тремя знаками.

Доказательство.

0	129
×	16
2	064
×	16
1	024
×	16
0	384

Ответ. $0,129 = 0,21_{16}$.

□

Пример 4. Переведите число $111000101,101001$ из двоичной системы счисления в восьмеричную и шестнадцатеричную.

Доказательство.

$$\begin{array}{rccccccc} 111000101,101001= & 111 & 000 & 101, & 101 & 001_2 & = & 705,51_8 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \\ & 7 & 0 & 5, & 5 & 1 & & \end{array}$$

$$\begin{array}{rccccccc} 111000101,101001= & 0001 & 1100 & 0101, & 1010 & 0100_2 & = & 1C5,A4_{16} \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \\ & 1 & C & 5, & A & 4 & & \end{array}$$

Ответ. $111000101,101001_2 = 705,51_8$; $111000101,101001 = 1C5,A4_{16}$.

□

Пример 5. Число ABC записано в шестнадцатеричной системе

счисления. Наиболее рациональным способом переведите его в систему счисления по основанию 8.

Доказательство.

$$\mathrm{ABC}_{16} = 1010\ 1011\ 1100_2 = 101010111100_2 = 101\ 010\ 111\ 100 = 5274_8.$$

Ответ. $\mathrm{ABC}_{16} = 5274_8$.

□

Пример 6. Число 252 записано в восьмеричной системе счисления. Прямым делением в этой системе перевести его в систему по основанию 16.

Доказательство. Число 31_8 поделим на основание системы, в которую переводим, записанное в восьмеричной системе счисления: $16_{10} = 20_8$.

$$\begin{array}{r|l} 252_8 & 20_8 \\ \hline 240 & 12 < 20 \\ \hline 12 & \end{array}$$

Таким образом, $252_8 = \mathrm{CC}_{16}$.
Ответ. $252_8 = \mathrm{CC}_{16}$.

□

Задачи для самостоятельного решения

1. Переведите числа a и b в десятичную систему счисления.

1.1. $a = 100110_2$, $b = 111001,101_2$.
1.2. $a = 101010_2$, $b = 101001,011_2$.
1.3. $a = 100111_2$, $b = 101101,11_2$.
1.4. $a = 10211_3$, $b = 11201,111_3$.
1.5. $a = 11202_3$, $b = 120012,21_3$.
1.6. $a = 10121_3$, $b = 110202,102_3$.
1.7. $a = 13201_4$, $b = 3012,23_4$.
1.8. $a = 13102_4$, $b = 3311,003_4$.
1.9. $a = 31102_4$, $b = 1133,012_4$.
1.10. $a = 1506_7$, $b = 4016,501_7$.
1.11. $a = 5006_7$, $b = 1016,005_7$.
1.12. $a = 1104_7$, $b = 3305,04_7$.
1.13. $a = 1506_8$, $b = 1157,103_8$.
1.14. $a = 1701_8$, $b = 1325,017_8$.
1.15. $a = 10064_8$, $b = 712,006_8$.
1.16. $a = 2601_8$, $b = 5007,031_8$.
1.17. $a = \mathrm{A09}_{16}$, $b = \mathrm{E01,307}_{16}$.
1.18. $a = \mathrm{30B}_{16}$, $b = \mathrm{1D2,06}_{16}$.
1.19. $a = \mathrm{3C0}_{16}$, $b = \mathrm{20B,201}_{16}$.
1.20. $a = \mathrm{10D}_{16}$, $b = \mathrm{195,0A}_{16}$.

2. Переведите целое число a из десятичной системы счисления в g-ичную.

2. 1. $a = 257$, $g = 2$. 2. 2. $a = 361$, $g = 2$.
2. 3. $a = 452$, $g = 2$. 2. 4. $a = 498$, $g = 3$.
2. 5. $a = 583$, $g = 3$. 2. 6. $a = 637$, $g = 3$.
2. 7. $a = 694$, $g = 4$. 2. 8. $a = 639$, $g = 4$.
2. 9. $a = 785$, $g = 4$. 2. 10. $a = 791$, $g = 7$.
2. 11. $a = 765$, $g = 7$. 2. 12. $a = 867$, $g = 7$.
2. 13. $a = 803$, $g = 8$. 2. 14. $a = 869$, $g = 8$.
2. 15. $a = 974$, $g = 8$. 2. 16. $a = 913$, $g = 8$.
2. 17. $a = 961$, $g = 16$. 2. 18. $a = 1027$, $g = 16$.
2. 19. $a = 1045$, $g = 16$. 2. 20. $a = 1865$, $g = 16$.

3. Переведите дробь a из десятичной системы счисления в g-ичную с тремя знаками.

3. 1. $a = 0,2571$, $g = 2$. 3. 2. $a = 0,3612$, $g = 2$.
3. 3. $a = 0,4523$, $g = 3$. 3. 4. $a = 0,4984$, $g = 3$.
3. 5. $a = 0,5835$, $g = 4$. 3. 6. $a = 0,6376$, $g = 4$.
3. 7. $a = 0,6947$, $g = 5$. 3. 8. $a = 0,6398$, $g = 5$.
3. 9. $a = 0,7859$, $g = 6$. 3. 10. $a = 0,7911$, $g = 6$.
3. 11. $a = 0,7652$, $g = 7$. 3. 12. $a = 0,8673$, $g = 7$.
3. 13. $a = 0,8034$, $g = 8$. 3. 14. $a = 0,8695$, $g = 8$.
3. 15. $a = 0,9746$, $g = 9$. 3. 16. $a = 0,9137$, $g = 9$.
3. 17. $a = 0,9618$, $g = 12$. 3. 18. $a = 0,1527$, $g = 12$.
3. 19. $a = 0,2945$, $g = 16$. 3. 20. $a = 0,1865$, $g = 16$.

4. Переведите число a из двоичной системы счисления в восьмерич-

ную и шестнадцатеричную.

4. 1. $a = 1100111011, 10000000111$.
4. 2. $a = 1001110011, 1001$.
4. 3. $a = 1100000000, 1101011111$.
4. 4. $a = 1100001001, 1100100101$.
4. 5. $a = 1101010001, 1000111$.
4. 6. $a = 1110001, 1011001101$.
4. 7. $a = 1111000111, 11010101$.
4. 8. $a = 110010001, 1001$.
4. 9. $a = 1000110110, 111100001$.
4. 10. $a = 101111111, 111110011$.
4. 11. $a = 11101000, 1010001111$.
4. 12. $a = 10000011001, 101011$.
4. 13. $a = 110111101, 1110011101$.
4. 14. $a = 1101100000, 10000101$.
4. 15. $a = 101111100, 100001001$.
4. 16. $a = 10010010, 1100101$.
4. 17. $a = 11100011, 1111001101$.
4. 18. $a = 110010010, 11100101$.
4. 19. $a = 1001100111, 111001001$.
4. 20. $a = 1001100111, 110001001$.

5. Число a записано в p-ичной системе счисления. Наиболее рациональным способом переведите его в систему счисления по основанию g.

6.1. $a = 123113$, $p = 4$, $g = 8$.
6.2. $a = 3450$, $p = 8$, $g = 4$.
6.3. $a = 206$, $p = 9$, $g = 3$.
6.4. $a = 33033$, $p = 4$, $g = 16$.
6.5. $a = 373$, $p = 16$, $g = 4$.
6.6. $a = 10166$, $p = 8$, $g = 16$.
6.7. $a = \mathrm{ACD}$, $p = 16$, $g = 8$.
6.8. $a = 101000111$, $p = 2$, $g = 4$.
6.9. $a = 12230$, $p = 4$, $g = 2$.
6.10. $a = 110101111$, $p = 2$, $g = 16$.
6.11. $a = 213$, $p = 16$, $g = 2$.
6.12. $a = 22002$, $p = 4$, $g = 8$.
6.13. $a = 1403$, $p = 8$, $g = 4$.
6.14. $a = 10165$, $p = 8$, $g = 16$.
6.15. $a = \mathrm{AC9}$, $p = 16$, $g = 8$.
6.16. $a = 21300$, $p = 4$, $g = 8$.
6.17. $a = 1530$, $p = 16$, $g = 8$.
6.18. $a = 112113$, $p = 4$, $g = 8$.
6.19. $a = 3273$, $p = 8$, $g = 4$.
6.20. $a = 1120022$, $p = 3$, $g = 9$.

6. Число a записано в p-ичной системе счисления. Прямым делением в этой системе перевести его в систему по основанию g.

6.1. $a = 1030033, \quad p = 5, \quad g = 11.$
6.2. $a = 1041303, \quad p = 5, \quad g = 12.$
6.3. $a = 1420224, \quad p = 5, \quad g = 13.$
6.4. $a = 1143224, \quad p = 5, \quad g = 14.$
6.5. $a = 2004012, \quad p = 5, \quad g = 15.$
6.6. $a = 2022321, \quad p = 5, \quad g = 16.$
6.7. $a = 523044, \quad p = 6, \quad g = 11.$
6.8. $a = 531505, \quad p = 6, \quad g = 12.$
6.9. $a = 141244, \quad p = 6, \quad g = 13.$
6.10. $a = 150051, \quad p = 6, \quad g = 14.$
6.11. $a = 304323, \quad p = 6, \quad g = 15.$
6.12. $a = 242401, \quad p = 6, \quad g = 16.$
6.13. $a = 160421, \quad p = 7, \quad g = 11.$
6.14. $a = 163352, \quad p = 7, \quad g = 12.$
6.15. $a = 233564, \quad p = 7, \quad g = 13.$
6.16. $a = 236524, \quad p = 7, \quad g = 14.$
6.17. $a = 311136, \quad p = 7, \quad g = 15.$
6.18. $a = 314065, \quad p = 7, \quad g = 16.$
6.19. $a = 175470, \quad p = 8, \quad g = 11.$
6.20. $a = 177440, \quad p = 8, \quad g = 12.$

7. Выполните действия над числами, а затем проверьте результаты, выполнив соответствующие действия в десятичной системе счисления.

7.1. $10011,1_2 + 11,00111_2$.
7.2. $1111,0111_2 - 1,0001_2$.
7.3. $111,01_2 \cdot 1,01_2$.
7.4. $\frac{1001,11_2}{11,01_2}$.
7.5. $34,1_8 + 11,17_8$.
7.6. $12,121_8 - 1,1755_8$.
7.7. $62,1_8 \cdot 67,17_8$.
7.8. $\frac{174,23_8}{34,5_8}$.
7.9. $\mathrm{A23,F1_{16}} + 1,7_{16}$.
7.10. $1343,31_{16} - \mathrm{D1,7F_{16}}$.
7.11. $23,\mathrm{F1_{16}} \cdot \mathrm{A},7_{16}$.
7.12. $\frac{231,\mathrm{CD_{16}}}{1,67_{16}}$.
7.13. $101,1_2 + 11,101_2$.
7.14. $111,01_2 - 1,11_2$.
7.15. $100,001_2 \cdot 10,101_2$.
7.16. $25,6_8 + 12,37_8$.
7.17. $11,51_8 - 4,17_8$.
7.18. $21,1_8 \cdot 67,7_8$.
7.19. $\mathrm{C93,F1_{16}} + 9,7\mathrm{E}_{16}$.
7.20. $1343,31_{16} - \mathrm{A1,6E_{16}}$.

3. Практическое занятие по теме «Линейные диофантовы уравнения»

Пример 1. Решите уравнение $54x - 42y = -18$ в целых числах.

Доказательство. Так как НОД$(54, -42, -18) = 6$, то уравнение $54x - 42y = -18$ не является диофантовым. Сократив его на 6, получим диофантово уравнение $9x - 7y = -3$, так как НОД$(9, -7, -3) = 1$.

Поскольку НОД$(9, -7) = 1$, то уравнение $9x - 7y = -3$ разрешимо в целых числах. С помощью алгоритма Евклида выразим 1 линейно через числа 9 и -7. Получим, что $1 = 9 \cdot 4 + (-7) \cdot 5$. Умножив последнее равенство на -3, получим $9 \cdot (-12) - 7 \cdot (-15) = -3$. Отсюда $(x_0, y_0) = (-12, -15)$ — частное решение уравнения $9x - 7y = -3$.

Таким образом, $(-12 - 7t, -15 - 9t), t \in \mathbb{Z}$ — общее решение уравнения $9x - 7y = -3$.

Ответ. $\{(-12 - 7t, -15 - 9t) \mid t \in \mathbb{Z}\}$.

□

Пример 2. Решите в целых числах $7x + 4y + 9z = 89$.

Доказательство. Выразим неизвестное, коэффициент при котором наименьший, через остальные неизвестные.

$$y = \frac{(89 - 9z - 7x)}{4} = (22 - 3z - 2x) + \frac{(1 + 3z + x)}{4}. \qquad (3.3.1)$$

Обозначим

$$\frac{(1+3z+x)}{4} = t_1. \tag{3.3.2}$$

Из (3.3.1) следует, что t_1 может принимать только целые значения.

Из (3.3.2) имеем

$$4t_1 = 3z + x + 1. \tag{3.3.3}$$

Откуда $x = 4t_1 - 3z - 1$.

Из (3.3.1) имеем

$$y = 22 - 3z - 2 \cdot (4t_1 - 3z - 1) + t_1 = 24 + 3z - 7t_1. \tag{3.3.4}$$

Итак,

$$x = 4t_1 - 3z - 1,$$

$$y = 24 + 3z - 4t_1.$$

Ответ: $\{(4t_1 - 3z - 1,\ 24 + 3z - 4t_1,\ z) \mid t_1, z \in \mathbb{Z}\}$.

□

Пример 3. Решите диофантово уравнение $9x + 13y = 150$ с использованием цепной дроби.

Доказательство. Представим дробь $\frac{9}{13}$ в виде конечной цепной дроби.

$$\frac{9}{13} = 0 + \frac{1}{1+\frac{4}{9}} = 0 + \frac{1}{1+\frac{1}{2+\frac{1}{4}}}$$

Таким образом, $\frac{9}{13} = [0; 1, 2, 4]$.

Составим таблицу

s		0	1	2	3
q_s		0	1	2	4
P_s	1	0	1	2	9
Q_s	0	1	1	3	13

Тогда общее решение уравнения имеет вид:

$$\begin{cases} x = (-1)^2 \cdot 150 \cdot 3 + 13t, \\ y = (-1)^3 \cdot 150 \cdot 2 - 9t, \\ t \in \mathbb{Z}. \end{cases} \Leftrightarrow \begin{cases} x = 450 + 13t, \\ y = -300 - 9t. \end{cases}$$

Ответ. $\{(450 + 13t, -300 - 9t) \mid t \in \mathbb{Z}\}$.

□

Целыми точками называют точки, координаты которых являются целыми числами.

Пример 4. Через какие целые точки проходит отрезок с концами $X_1 = (2; 7)$ и $X_2 = (11; 13)$?

Доказательство. Уравнение прямой, проходящей через две точки $X_1 = (x_1; y_1)$ и $X_2 = (x_2; y_2)$, задается формулой:

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1}.$$

Подставим координаты точек X_1 и X_2 в эту формулу:

$$\frac{x - 2}{11 - 2} = \frac{y - 7}{13 - 7},\ 2x - 3y = -17.$$

Решим полученное уравнение в целых числах.

Поскольку НОД$(2, -3) = 1$, то уравнение $2x - 3y = -17$ разрешимо в целых числах. С помощью алгоритма Евклида выразим 1 линейно через числа 2 и -3. Получим, что $1 = 2 \cdot 2 + (-3) \cdot 1$. Умножив последнее равенство на -17, получим $2 \cdot (-34) - 3 \cdot (-17) = -17$. Отсюда $(x_0, y_0) = (-34, -17)$ — частное решение уравнения $2x - 3y = -17$.

Таким образом, $(-34 - 3t, -17 - 2t), t \in \mathbb{Z}$ — общее решение уравнения $2x - 3y = -17$.

Поскольку искомые точки лежат на отрезке с концами $X_1 = (2; 7)$ и $X_2 = (11; 13)$, то $7 \leq -17 - 2t \leq 13$, поэтому $-15 \leq t \leq -12$. Подставляя эти значения t в формулы $x = -34 - 3t$, $y = -17 - 2t$, получим внутренние целые точки: $(5; 9)$ и $(8; 11)$.

Ответ. $(2; 7)$, $(5; 9)$, $(8; 11)$, $(11; 13)$.

□

Пример 5. Плоскость проходит через три точки $X_1 = (5; -4; 3)$, $X_2 = (2; 4; -3)$ и $X_3 = (-3; -2; 1)$. Найдите все внутренние целые точки плоскости, ограниченной треугольником $X_1X_2X_3$.

Доказательство. Уравнение плоскости, проходящей через три точки $X_1 = (x_1; y_1; z_1)$, $X_2 = (x_2; y_2; z_2)$ и $X_2 = (x_3; y_3; z_3)$, задается формулой:

$$\begin{vmatrix} x - x_1 & y - y_1 & z - z_1 \\ x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \\ x_3 - x_1 & y_3 - y_1 & z_3 - y_1 \end{vmatrix}.$$

Подставляя координаты точек в эту формулу и вычисляя определитель, получим: $-2x + 21y + 29z = -7$. Решим полученное уравнение в целых числах. Так как $29 = 21+8$, то получим уравнение $-2x+21(y+z)+8z = -7$ и, полагая $y + z = m$, получим уравнение $-2x + 21m + 8z = -7$ или $-2(x - 4z) + 21m = -7$. Положим $x - 4z = s$. Тогда $21m - 2s = -7$.

Поскольку НОД$(21, -2) = 1$, то уравнение $21m-2s = -7$ разрешимо в целых числах. С помощью алгоритма Евклида выразим 1 линейно через числа 21 и -2. Получим, что $1 = 21 \cdot 1 + (-2) \cdot 10$. Умножив последнее равенство на -7, получим $21 \cdot (-7) - 2 \cdot (-70) = -7$. Отсюда $(m_0, s_0) = (-7, -70)$ — частное решение уравнения $21m - 2s = -7$. Таким образом, $m = -7 - 2t, \quad s = -70 - 21t, t \in \mathbb{Z}$.

Все решения исходного уравнения в целых числах x, y, z определяются формулами: $x = 4z - 21t - 70$, $y = -z - 2t - 7$, $t \in \mathbb{Z}$.

Так как $-3 \le x \le 5$, $-4 \le y \le 4$, $-3 \le z \le 3$, то внутри треугольника $X_1X_2X_3$ лежит только одна точка $(1; -3; 2)$.

Ответ. $(1; -3; 2)$.

□

Задачи для самостоятельного решения

1. Решите уравнения в целых числах.

1.1. $10x - 15y = 25$, $6x + 10y + 15z = 7$.

1.2. $14x + 21y = -49$, $4x - 6y + 11z = 7$.

1.3. $12x - 8y = -24$, $6x + 10y - 7z = 11$.

1.4. $15x - 18y = 21$, $-7x + 4y + 9z = 19$.

1.5. $22x + 4y = -16$, $5x + 12y + 8z = 14$.

1.6. $39x - 22y = 10$, $10x - 6y + 13z = 8$.

1.7. $17x - 25y = 117$, $7x - 4y + 8z = 11$.

1.8. $53x + 47y = 11$, $5x + 3y - 6z = 12$.

1.9. $43x + 37y = 21$, $6x + 5y - 3z = 7$.

1.10. $17x - 16y = 31$, $-3x + 7y + 6z = 15$.

1.11. $23x + 15y = 19$, $3x + 6y - 5z = 11$.

1.12. $12x - 37y = -3$, $11x - 3y + 6z = -5$.

1.13. $18x + 31y = 26$, $4x + 3y + 7z = -10$.

1.14. $11x + 16y = 156$, $-7x + 5y + 12z = 3$.

1.15. $45x - 37y = 25$, $3x - 7y + 2z = 5$.

2. Решите диофантовы уравнения с использованием цепной дроби.

2.1.	$45x - 37y = 25.$	2.2.	$2x - 3y = 5.$
2.3.	$2x + 3y = -7.$	2.4.	$3x - 2y = -6.$
2.5.	$5x - 6y = 7.$	2.6.	$11x + 2y = -8.$
2.7.	$39x - 22y = 10.$	2.8.	$17x - 25y = 117.$
2.9.	$53x + 47y = 11.$	2.10.	$43x + 37y = 21.$
2.11.	$17x - 16y = 31.$	2.12.	$23x + 15y = 19.$
2.13.	$12x - 37y = -3.$	2.14.	$18x + 31y = 26.$
2.15.	$11x + 16y = 156.$		

3. Через какие целые точки проходит отрезок с концами $X_1 = (x_1; y_1)$ и $X_2 = (x_2; y_2)$.

3.1.	$x_1 = 2,$	$y_1 = 7,$	$x_2 = 50,$	$y_2 = 49.$
3.2.	$x_1 = 5,$	$y_1 = 5,$	$x_2 = 17,$	$y_2 = 11.$
3.3.	$x_1 = 4,$	$y_1 = 8,$	$x_2 = 37,$	$y_2 = 32.$
3.4.	$x_1 = 3,$	$y_1 = 7,$	$x_2 = 15,$	$y_2 = 15.$
3.5.	$x_1 = 2,$	$y_1 = 5,$	$x_2 = 32,$	$y_2 = 30.$
3.6.	$x_1 = 3,$	$y_1 = 7,$	$x_2 = 21,$	$y_2 = 37.$
3.7.	$x_1 = 4,$	$y_1 = 5,$	$x_2 = 32,$	$y_2 = 27.$
3.8.	$x_1 = 5,$	$y_1 = 7,$	$x_2 = 41,$	$y_2 = 33.$
3.9.	$x_1 = 3,$	$y_1 = 8,$	$x_2 = 33,$	$y_2 = 50.$
3.10.	$x_1 = 6,$	$y_1 = 11,$	$x_2 = 20,$	$y_2 = 51.$

3.11. $x_1 = 7, \quad y_1 = 13, \quad x_2 = 43, \quad y_2 = 27.$
3.12. $x_1 = 7, \quad y_1 = 11, \quad x_2 = 32, \quad y_2 = 41.$
3.13. $x_1 = 5, \quad y_1 = 11, \quad x_2 = 47, \quad y_2 = 60.$
3.14. $x_1 = 5, \quad y_1 = 6, \quad x_2 = 45, \quad y_2 = 31.$
3.15. $x_1 = 4, \quad y_1 = 6, \quad x_2 = 49, \quad y_2 = 31.$

4. Плоскость проходит через три точки $X_1 = (x_1; y_1; z_1)$, $X_2 = (x_2; y_2; z_2)$ и $X_3 = (x_3; y_3; z_3)$. Найдите все внутренние целые точки плоскости, ограниченной треугольником $X_1X_2X_3$.

4.1. $X_1 = (1; 4; 3), \quad X_2 = (-1; 5; 2), \quad X_3 = (-3; 0; -2).$
4.2. $X_1 = (2; -2; 1), \quad X_2 = (7; -8; 3), \quad X_3 = (-3; 4; 1).$
4.3. $X_1 = (5; -4; 3), \quad X_2 = (2; 4; -3), \quad X_3 = (-3; -2; 3).$
4.4. $X_1 = (5; 7; 3), \quad X_2 = (3; 2; -1), \quad X_3 = (-3; 4; 1).$
4.5. $X_1 = (1; 4; 2), \quad X_2 = (3; 5; 4), \quad X_3 = (-3; -1; -3).$
4.6. $X_1 = (3; -4; 3), \quad X_2 = (2; 4; -3), \quad X_3 = (-2; -2; 1).$
4.7. $X_1 = (-1; -2; 3), \quad X_2 = (2; 5; -3), \quad X_3 = (-2; -1; 1).$
4.8. $X_1 = (-5; -3; 4), \quad X_2 = (3; 3; -3), \quad X_3 = (-1; -2; 2).$
4.9. $X_1 = (5; -4; 3), \quad X_2 = (2; 4; -3), \quad X_3 = (-2; -2; 1).$
4.10. $X_1 = (-3; -3; 3), \quad X_2 = (4; -2; -3), \quad X_3 = (2; 2; 1).$
4.11. $X_1 = (3; -2; 3), \quad X_2 = (2; 4; -3), \quad X_3 = (-2; -2; 1).$
4.12. $X_1 = (-2; -3; 4), \quad X_2 = (3; 4; -3), \quad X_3 = (-1; -2; 2).$
4.13. $X_1 = (-4; -3; 4), \quad X_2 = (3; 2; -3), \quad X_3 = (-2; -2; 1).$

4.14. $X_1 = (3; -2; 3)$, $X_2 = (2; 5; -3)$, $X_3 = (-2; -1; 1)$.

4.15. $X_1 = (-5; -3; 4)$, $X_2 = (3; 3; -3)$, $X_3 = (-1; -2; 1)$.

5.1. Имеются задачи «стоимостью» 7 и 9 баллов. Для получения зачета надо набрать не менее 213 баллов. Какое минимальное количество задач надо решить?

5.2. Для выполнения одной контрольной работы по алгебре студент затрачивает 54 минуты, а по аналитической геометрии — 48 минут. Сколько контрольных работ и по каким дисциплинам студент выполнит за 5 часов?

5.3. Определите дату рождения, зная, что сумма произведений числа месяца на 12 и номера месяца на 31 равна 436.

5.4. Пол шириной 3 метра нужно изготовить из досок шириной 11 и 13 сантиметров. Сколько необходимо досок того и другого размера?

5.5. Один мастер делает на длинной ленте метки синим фломастером от ее начала через каждые 34 сантиметров, другой мастер делает метки красным фломастером через каждые 27 сантиметров. Может ли синяя пометка оказаться на расстоянии 2 сантиметров от красной?

5.6. Для прокладки газопровода длиной 450 метров имеются трубы длиной 9 и 13 метров, причем не более 25 штук каждой длины. Сколько потребуется труб той и другой длины, чтобы число сварных швов было минимальным? Трубы резать нельзя.

5.7. В первом сплаве золото и серебро находится в отношении 4 : 7, а во втором — 7 : 9. Каков вес серебра в первом сплаве, если общий вес

двух сплавов — 277 грамм?

5.8. Фирма продавала чай в центре города по 1000 руб., а кофе по 1300 руб. за чашку; на вокзале — по 750 руб. и 950 руб. соответственно. Всего было продано за час 20 чашек чая и 20 чашек кофе, при этом выручка в центре и на вокзале оказалась одинаковой. Сколько чашек кофе продано в центре?

5.9. Два студента вместе получили надбавку к стипендии в размере 200 000 руб. Первый студент $\frac{5}{9}$ своей надбавки потратил на поездку в Минск, а второй $\frac{7}{11}$ своей надбавки потратил на дискотеку. Какую надбавку получил каждый студент?

5.10. Если двузначное число разделить на некоторое целое число, то в частном получится 3, а в остатке 8. Если же в делимом поменять местами цифры, а делитель оставить прежним, то в частном получится 2, а в остатке 5. Найдите первоначальное значение делимого.

5.11. Найдите трехзначное число, если сумма его цифр равна 9 и оно равно 47/36 от числа, записываемого теми же цифрами, но в обратном порядке.

5.12. На поле имеется два участка под посев зерновых. После применения новых методов агрономии урожай на первом участке повысился на 80%, а на втором — на 24%, и с этих участков было собрано 25 центнеров зерна. Сколько зерна стали собирать с каждого участка?

5.13. На ремонт объекта поставили две бригады. Одной первой бригаде для выполнения 40% всей работы потребовалось бы на 2 дня больше,

чем одной второй для выполнения 17% всей работы. За сколько дней могла бы отремонтировать каждая бригада отдельно весь объект?

5.14. При стрельбе по мишени стрелок выбивает только по 8, 9 и 10 очков. Всего он, сделав более 11 выстрелов, выбил 100 очков. Сколько выстрелов сделал стрелок и какие были попадания?

5.15. В магазине имеется мастика в ящиках по 16, 17 и 21 кг. Как одной организации купить ровно 185 кг мастики, не вскрывая ящики? Найдите все способы, которыми можно это сделать.

6. При каких значениях $u, v \in \mathbb{Z}$ числа a_1, a_2 и a_3 образуют арифметическую прогрессию?

6.1. $a_1 = 2, \quad a_2 = 3u, \quad a_3 = 5v.$

6.2. $a_1 = 2u, \quad a_2 = 3, \quad a_3 = 7v.$

6.3. $a_1 = 3u, \quad a_2 = 2v, \quad a_3 = 1.$

6.4. $a_1 = 5, \quad a_2 = 2u, \quad a_3 = 5v.$

6.5. $a_1 = 2, \quad a_2 = 5u, \quad a_3 = 3v.$

6.6. $a_1 = 6u, \quad a_2 = 5, \quad a_3 = 5v.$

6.7. $a_1 = 7, \quad a_2 = 3u, \quad a_3 = 11v.$

6.8. $a_1 = 8u, \quad a_2 = 5v, \quad a_3 = 6.$

6.9. $a_1 = 3v, \quad a_2 = 13, \quad a_3 = 4u.$

6.10. $a_1 = 11v, \quad a_2 = 5u, \quad a_3 = 2.$

6.11. $a_1 = 14, \quad a_2 = 5v, \quad a_3 = 6u.$

6. 12. $a_1 = 8u, \quad a_2 = 3v, \quad a_3 = 12.$

6. 13. $a_1 = 12, \quad a_2 = 5u, \quad a_3 = 11v.$

6. 14. $a_1 = 16, \quad a_2 = 4v, \quad a_3 = 13u.$

6. 15. $a_1 = 3, \quad a_2 = 5u, \quad a_3 = 11v.$

Кафедра
ФМО и ИТ

4. Практическое занятие по теме «Сравнения в кольце целых чисел. Кольцо классов вычетов по данному модулю»

Пример 1. *Пусть n — натуральное число. Найдите остаток от деления числа 20^{6n+5} на 9.*

Доказательство. Напомним, что согласно свойствам сравнений, можно вычитать и прибавлять к любой части сравнения числа, кратные модулю. Так как $20 \equiv 2 \pmod 9$, то

$$20^{6n+5} \equiv 2^{6n+5} = (2^3)^{2n} \cdot 2^5 \equiv (-1)^{2n} \cdot 5 \equiv 5 \pmod 9.$$

Ответ. 5. □

Пример 2. *Найдите последние две цифры десятичной записи числа 5^n, $n \geq 2$.*

Доказательство. Последние две цифры числа совпадают с остатком от деления этого числа на 100. Проверим, что при любом $n \geq 2$ последние две цифры десятичной записи числа 5^n будут 2 и 5. Воспользуемся индукцией по n. При $n = 2$ утверждение справедливо. Пусть $n \geq 3$. Предположим, что утверждение верно для $n-1$ и докажем его для n. Так как $5^{n-1} \equiv 25 \pmod{100}$, то

$$5^n = 5^{n-1} \cdot 5 \equiv 25 \cdot 5 = 125 \equiv 25 \pmod{100},$$

значит утверждение справедливо для любого $n \geq 2$.
Ответ. 2 и 5.

Пример 3. *В аддитивной группе кольца $\mathbb{Z}_5$ найдите порядки всех элементов. Для каждого элемента укажите противоположный.*

Доказательство. Составим таблицу сложения элементов в кольце $\mathbb{Z}_5$.

$(\mathbb{Z}_5, +)$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

На пересечении строки a и столбца b в таблице сложения ставится остаток от деления суммы $a + b$ на 5.

Ясно, что порядок 0 как элемента аддитивной группы $\mathbb{Z}_5$ равен 1, т. е. $|0| = 1$. Так как $1 + 1 + 1 + 1 + 1 = 0$, то $|1| = 5$. Аналогично, $|2| = |3| = |4| = 5$.

Из таблицы сложения для $\mathbb{Z}_5$ противоположные элементы определяем следующим образом. В строке a находим нулевой элемент 0. Если он

стоит в столбце b, то $a + b = 0$ и b — противоположный элемент для a. Итак, $-0 = 0$, $-1 = 4$, $-2 = 3$, $-3 = 2$, $-4 = 1$.

Ответ. $|0| = 1$, $|1| = |2| = |3| = |4| = 5$, $-0 = 0$, $-1 = 4$, $-2 = 3$, $-3 = 2$, $-4 = 1$.

□

Пример 4. *В кольце $\mathbb{Z}_{24}$ перечислите обратимые элементы и делители нуля. Для каждого обратимого элемента укажите обратный.*

Доказательство. Поскольку НОД$(24, x) \neq 1$ для каждого $x \in \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22\}$, то соответствующие классы вычетов будут делителями нуля. Обратимыми элементами будут элементы 1, 5, 7, 11, 13, 17, 19, 23. Число обратимых элементов равно 8 и совпадает со значением функции Эйлера

$$\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3)\varphi(3) = (2^3 - 2^2)(3 - 1) = 8.$$

Составим таблицу умножения обратимых элементов.

Из таблицы обратные элементы определяем следующим образом. В строке a находим единичный элемент 1. Если он стоит в столбце b, то $ab = 1$ и b — обратный элемент для a. Из таблицы видно, что каждый элемент совпадает со своим обратным.

$(\mathbb{U}_{24}, \cdot)$	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	19	17	13	11	7	5	1

□

Напомним, что элемент a кольца K называется *идемпотентом*, если $a^2 = a$.

Пример 5. *Найдите все идемпотенты в кольце* $\mathbb{Z}_{242}$.

Доказательство. Очевидно, что 0 и 1 являются идемпотентами. Согласно определению элемент $a \in \mathbb{Z}_{2 \cdot 11^2}$ является идемпотентом, если для числа a выполняется сравнение

$$a(a-1) \equiv 0 \pmod{2 \cdot 11^2}, \tag{3.1}$$

причем

$$2 \leq a < 2 \cdot 11^2. \tag{3.2}$$

Ясно, что $d = \text{НОД}(a, 2 \cdot 11^2) \in \{1, 2, 11, 2 \cdot 11, 11^2\}$.

Если $d = 1$, то из (3.1) следует, что $2 \cdot 11^2$ делит $a - 1$, противоречие с (3.2).

Если $d = 2$, то из (3.1) следует, что 11^2 делит $a-1$, т. е. $a-1 = 11^2 s$ для некоторого целого s. Теперь из (3.2) заключаем что $s = 1$ и $a = 122$ — идемпотент кольца $\mathbb{Z}_{2 \cdot 11^2}$.

Если $d = 11^2$, то $a = 11^2 k$ для некоторого целого k, а из (3.2) получаем, что $k = 1$ и $a = 121$ — идемпотент кольца $\mathbb{Z}_{2 \cdot 11^2}$.

Случаи $d = 11$ и $d = 2 \cdot 11$ невозможны, так как в этих случаях из (3.1) следует, что 11 одновременно делит a и $a - 1$, противоречие.

Ответ. $\{0, 1, 121, 122\}$. □

Напомним, что элемент a кольца K называется *нильпотентным*, если существует $t \in \mathbb{N}$ такое, что $a^t = 0$, где 0 — нулевой элемент кольца K.

Пример 6. *Найдите все нильпотентные элементы в* $\mathbb{Z}_{242}$. *Доказательство.* Согласно определению элемент $a \in \mathbb{Z}_{2 \cdot 11^2}$ является нильпотентным, если существует $t \in \mathbb{N}$ такое, что для числа a выполняется сравнение

$$a^t \equiv 0 \pmod{2 \cdot 11^2}, \tag{3.3}$$

Так как простые делители чисел a и a^t совпадают, то сравнению (3.3) удовлетворяют числа, кратные 22, и только они.

Ответ. $\{22s \mid 0 \leq s < 11\}$. □

Пример 7. *Найдите значения $t \in \mathbb{Z}_{19}$, при которых отношение корней уравнения $x^2 + (t+3)x + 5 = 0$ равно 6.*

Доказательство. Поскольку $\mathbb{Z}_{19}$ — поле, то можно воспользоваться теоремой Виета: $x_1 + x_2 = -(t+3)$, $x_1 \cdot x_2 = 5$. По условию $x_1 = 6x_2$ и $6x_2^2 = 5 = 24$ в поле $\mathbb{Z}_{19}$. Поэтому $x_2^2 = 4$ и $x_2 = \pm 2$.

Если $x_2 = 2$, то $x_1 = 12$, $12 + 2 = -(t+3)$ и $t = -17 = 2$ в поле $\mathbb{Z}_{19}$.

Если $x_2 = -2$, то $x_1 = -12$, $-12 - 2 = -(t+3)$ и $t = 11$.

Ответ. $t \in \{2, 11\}$. □

Задачи для самостоятельного решения

1. Пусть $n \in \mathbb{N}$. Найдите последние две цифры десятичной записи числа a и остаток от деления числа b на m.

1.1. $a = 5^{40}$, $b = 48^{5n+3}$, $m = 11$.

1.2. $a = 6^{32}$, $b = 48^{5n+4}$, $m = 11$.

1.3. $a = 8^{18}$, $b = 7 \cdot 3^{3n+1} - 2^{3n+1}$, $m = 19$.

1.4. $a = 3^{12}$, $b = 25 \cdot 7^{2n} + 2^{3n+4}$, $m = 41$.

1.5. $a = 2^{33}$, $b = 11 \cdot 3^{5n} + 2 \cdot 13^{2n+1}$, $m = 37$.

1.6. $a = 4^{20}$, $b = 75^{6n+7}$, $m = 13$.

1.7. $a = 2^{78}$, $b = 40^{3n+3}$, $m = 9$.

1.8. $a = 3^{63}$, $b = 128^{6n+7}$, $m = 9$.

1.9. $a = 5^{37}$, $b = 88^{9n+5}$, $m = 9$.

1.10. $a = 6^{47}$, $b = 104^{8n+3}$, $m = 7$.
1.11. $a = 8^{39}$, $b = 261^{3n+5}$, $m = 7$.
1.12. $a = 4^{28}$, $b = 180^{3n+1}$, $m = 7$.
1.13. $a = 2^{56}$, $b = 130^{10n+3}$, $m = 11$.
1.14. $a = 3^{73}$, $b = 180^{5n+2}$, $m = 11$.
1.15. $a = 7^{32}$, $b = 36^{20n+3}$, $m = 11$.

2. Укажите полную систему неотрицательных вычетов и полную систему наименьших по абсолютной величине вычетов по модулю m.

2.1. $m = 5$. 2.2. $m = 6$. 2.3. $m = 7$.
2.4. $m = 8$. 2.5. $m = 9$. 2.6. $m = 10$.
2.7. $m = 11$. 2.8. $m = 12$. 2.9. $m = 13$.
2.10. $m = 14$. 2.11. $m = 9$. 2.12. $m = 16$.
2.13. $m = 17$. 2.14. $m = 18$. 2.15. $m = 19$.

3. Составьте из чисел, кратных p, полную систему вычетов по модулю m.

3.1. $m = 11$, $p = 3$. 3.2. $m = 12$, $p = 5$.
3.3. $m = 14$, $p = 3$. 3.4. $m = 10$, $p = 7$.
3.5. $m = 6$, $p = 5$. 3.6. $m = 9$, $p = 4$.
3.7. $m = 13$, $p = 8$. 3.8. $m = 15$, $p = 4$.
3.9. $m = 13$, $p = 7$. 3.10. $m = 17$, $p = 6$.
3.11. $m = 12$, $p = 7$. 3.12. $m = 13$, $p = 5$.
3.13. $m = 15$, $p = 7$. 3.14. $m = 11$, $p = 6$.
3.15. $m = 14$, $p = 5$.

4. В аддитивной группе кольца $\mathbb{Z}_m$ найдите порядки всех элементов. Для каждого элемента укажите противоположный.

4.1. $m = 16$. 4.2. $m = 18$. 4.3. $m = 12$.
4.4. $m = 21$. 4.5. $m = 20$. 4.6. $m = 19$.
4.7. $m = 15$. 4.8. $m = 13$. 4.9. $m = 17$.
4.10. $m = 11$. 4.11. $m = 14$. 4.12. $m = 10$.
4.13. $m = 23$. 4.14. $m = 22$. 4.15. $m = 24$.

5. В кольце $\mathbb{Z}_m$ перечислите обратимые элементы и делители нуля. Для каждого обратимого элемента укажите обратный.

5.1. $m = 12$. 5.2. $m = 10$. 5.3. $m = 21$.
5.4. $m = 14$. 5.5. $m = 15$. 5.6. $m = 27$.
5.7. $m = 28$. 5.8. $m = 30$. 5.9. $m = 16$.
5.10. $m = 18$. 5.11. $m = 20$. 5.12. $m = 26$.
5.13. $m = 36$. 5.14. $m = 42$. 5.15. $m = 22$.

6. Найдите все идемпотенты в кольце $\mathbb{Z}_m$.

6.1. $m = 1\,183$. 6.2. $m = 507$. 6.3. $m = 605$.
6.4. $m = 147$. 6.5. $m = 245$. 6.6. $m = 363$.
6.7. $m = 845$. 6.8. $m = 847$. 6.9. $m = 539$.
6.10. $m = 867$. 6.11. $m = 637$. 6.12. $m = 175$.
6.13. $m = 1083$. 6.14. $m = 275$. 6.15. $m = 325$.

7. Найдите все нильпотентные элементы в кольце $\mathbb{Z}_m$.

7.1. $m = 147$. 7.2. $m = 224$. 7.3. $m = 448$.

7.4. $m = 136$. 7.5. $m = 441$. 7.6. $m = 550$.
7.7. $m = 220$. 7.8. $m = 490$. 7.9. $m = 726$.
7.10. $m = 650$. 7.11. $m = 882$. 7.12. $m = 408$.
7.13. $m = 900$. 7.14. $m = 440$. 7.15. $m = 980$.

8. Найдите порядки всех обратимых элементов в $\mathbb{Z}_m$. Является ли циклической мультипликативная группа $\mathbb{U}_m$?

8.1. $m = 22$. 8.2. $m = 18$. 8.3. $m = 21$.
8.4. $m = 20$. 8.5. $m = 12$. 8.6. $m = 26$.
8.7. $m = 24$. 8.8. $m = 27$. 8.9. $m = 42$.
8.10. $m = 28$. 8.11. $m = 36$. 8.12. $m = 15$.
8.13. $m = 10$. 8.14. $m = 30$. 8.15. $m = 16$.

9. Укажите разложение мультипликативной группы $\mathbb{U}_m$ в прямое произведение примарных циклических подгрупп.

9.1. $m = 24$. 9.2. $m = 15$. 9.3. $m = 12$.
9.4. $m = 21$. 9.5. $m = 20$. 9.6. $m = 28$.
9.7. $m = 33$. 9.8. $m = 16$. 9.9. $m = 32$.
9.10. $m = 45$. 9.11. $m = 36$. 9.12. $m = 48$.
9.13. $m = 40$. 9.14. $m = 44$. 9.15. $m = 39$.

10. Найдите значения $t \in \mathbb{Z}_m$, при которых отношение корней уравнения равно k.

10.1. $2x^2 + (t-10)x + 6 = 0$, $m = 5$, $k = 13$.
10.2. $x^2 + tx + 7 = 0$, $m = 19$, $k = 6$.

10. 3. $x^2 + (t+1)x + 30 = 0, \quad m =$

10. 4. $x^2 + 6x + t = 0, \quad m =$

10. 5. $3x^2 - 18x + t + 1 = 0, \quad m =$

10. 6. $x^2 - (t+3)x + 1 = 0, \quad m =$

10. 7. $x^2 - 4x + 2t = 0, \quad m =$

10. 8. $x^2 + 3tx + 3 = 0, \quad m =$

10. 9. $x^2 + 2x + t - 2 = 0, \quad m =$

10. 10. $x^2 + (t-6)x + 8 = 0, \quad m =$

10. 11. $x^2 - 8x - t = 0, \quad m =$

10. 12. $x^2 + 2tx + 2 = 0, \quad m =$

10. 13. $x^2 - 4x - t - 1 = 0, \quad m =$

10. 14. $x^2 + (t+3)x - 1 = 0, \quad m =$

10. 15. $2x^2 - x + t = 0, \quad m =$

7, $k = 4$.
11, $k = 9$.
11, $k = 13$.
5, $k = 24$.
7, $k = 5$.
11, $k = 9$.
7, $k = 9$.
7, $k = 4$.
13, $k = 10$.
13, $k = 5$.
11, $k = 8$.
7, $k = 3$.
7, $k = 3$.

5. Практическое занятие по теме «Числовые функции. Функция Эйлера»

Пример 1. *Вычислите значения функций Эйлера, $\tau(n)$ и $\sigma(n)$ от числа* 113400.

Доказательство. Воспользуемся тем, что если $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ — каноническое разложение числа n, то значения функций Эйлера, $\sigma(n)$ и $\tau(n)$ вычисляются по следующим формулам:

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_t^{\alpha_t - 1}(p_t - 1),$$

$$\tau(n) = (\alpha_1 + 1) \dots (\alpha_t + 1),$$

$$\sigma(n) = \left(\frac{p_1^{\alpha_1 + 1} - 1}{p_1 - 1}\right) \dots \left(\frac{p_t^{\alpha_t + 1} - 1}{p_t - 1}\right).$$

Так как $113400 = 2^3 \cdot 3^4 \cdot 5^2 \cdot 7$, то имеем:

$\varphi(113400) = (2^3 - 2^2)(3^4 - 3^3)(5^2 - 5)(7 - 7^0) = 2^6 \cdot 3^4 \cdot 5$,

$\tau(113400) = (3 + 1)(4 + 1)(2 + 1)(1 + 1) = 2^3 \cdot 3 \cdot 5$,

$\sigma(113400) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^5 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 31$.

Ответ. $\varphi(113400) = 2^6 \cdot 3^4 \cdot 5$, $\tau(113400) = 2^3 \cdot 3 \cdot 5$, $\sigma(113400) = 2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 31$. □

Пример 2. *Сколькими нулями заканчивается десятичная запись числа $\varphi(111!)$?*

Доказательство. Каноническое разложение числа 111! и значение функции Эйлера имеют вид: $111! = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5} \dots 109$,

$$\varphi(111!) = 2^{\alpha_2 - 1} \cdot 3^{\alpha_3 - 1}(3-1) \cdot 5^{\alpha_5 - 1}(5-1) \dots (109-1).$$

Число нулей, которыми заканчивается десятичная запись, совпадает с количеством 5 в каноническом разложении $\varphi(111!)$. К значению

$$\alpha_5 - 1 = \left[\frac{111}{5}\right] + \left[\frac{111}{5^2}\right] - 1 = 22 + 4 - 1 = 25$$

необходимо добавить число простых чисел p_i, для которых $p_i - 1$ делится на 5. Такими простыми числами будут числа 11, 31, 41, 61, 71, 101: $11 - 1 = 10$, $31 - 1 = 30$, $41 - 1 = 40$, $61 - 1 = 60$, $71 - 1 = 70$, $101 - 1 = 100$ делятся на 10, то десятичная запись числа $\varphi(111!)$ заканчивается 32 нулями.

Ответ. 32 нуля.

□

Пример 3. *Решите уравнения* $\varphi(x) = i$, $i \in \{1, 2, 3, 4\}$. *Доказательство.* Напомним, что если $x = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $p_1 < \dots < p_k$, то $\varphi(x) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1)$.

Ясно, что решениями уравнения $\varphi(x) = 1$ будут только 1 и 2. Несложно проверить, что решениями уравнения $\varphi(x) = 2$ будут только числа 3, 4 и 6.

Пусть $\varphi(x) = 3$. Так как $p_i - 1 \neq 3$, то $p_j = 3$ для некоторого j и $p_j(p_j - 1)$ делит $\varphi(x) = 3$, что невозможно. Значит уравнение $\varphi(x) = 3$ не имеет решений.

Пусть $\varphi(x) = 4$. Если $x = 2^\alpha$, то $\varphi(2^\alpha) = 2^{\alpha-1} = 4$ и $x = 8$. Пусть теперь $x \neq 2^\alpha$, т. е. x делится на нечетное простое число p_i. Тогда $p_i - 1$ делит 4 и $p_i \in \{3, 5\}$. Если x делится на 3, то $x = 3m$, 3 не делит m, $\varphi(3m) = 2\varphi(m)$, $\varphi(m) = 2$, $m = 4$, $x = 12$. Если x делится на 5, то $x = 5m$, 5 не делит m, $\varphi(5m) = 4\varphi(m)$, $\varphi(m) = 1$, $m \in \{1, 2\}$, $x \in \{5, 10\}$.
Ответ. Уравнение $\varphi(x) = 1$ имеет два решения: $x_1 = 1$, $x_2 = 2$. Уравнение $\varphi(x) = 2$ имеет три решения: $x_1 = 3$, $x_2 = 4$, $x_3 = 6$. Уравнение $\varphi(x) = 3$ решений не имеет. Уравнение $\varphi(x) = 4$ имеет четыре решения: $x_1 = 5$, $x_2 = 8$, $x_3 = 10$, $x_4 = 12$. □

Пример 4. *Решите уравнение* $\varphi(x) = 10$.

Доказательство. Пусть $x = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $p_1 < \dots < p_k$. Тогда $\varphi(x) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) = 2 \cdot 5$.

Если $p_i = 5$ для некоторого i, то $p_i - 1 = 5 - 1 = 4$ и 4 делит 10, что невозможно. Поэтому 5 не делит x и $p_j - 1$ делится на 5 для некоторого j. Так как $p_j - 1$ — четное число, то $p_j - 1 = 2 \cdot 5$ и $p_j^{\alpha_j} = 11$. Теперь $x = 11m$, причем 11 не делит m. Из равенства $10 = \varphi(11m) = 10\varphi(m)$ получаем, что $\varphi(m) = 1$ и $m \in \{1, 2\}$.
Ответ. Уравнение имеет два решения: $x_1 = 11$, $x_2 = 22$.

□

Пример 5. *Решите уравнение* $\varphi(x) = 40$.

Доказательство. Опять считаем, что $x = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $p_1 < \dots < p_k$, $\varphi(x) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) = 2^3 \cdot 5$.

Предположим, что 5^2 делит x. Тогда $x = 5^2 m$, 5 не делит m, и $\varphi(x) = \varphi(5^2)\varphi(m) = 40$, $\varphi(m) = 2$, $m \in \{3, 4, 6\}$, $x \in \{75, 100, 150\}$.

Пусть теперь 5^2 не делит x. Тогда 5 делит $p_i - 1$ для некоторого i. Ясно, что $p_i - 1 = 2^k 5$, где $1 \leq k \leq 3$, т. е. $p_i \in \{11, 41\}$. Если $p_i = 11$, то $x = 11m$, 11 не делит m, $\varphi(m) = 4$, $m \in \{5, 8, 10, 12\}$ и $x \in \{55, 88, 110, 132\}$. Если $p_i = 41$, то $x = 41m$, 41 не делит m, $\varphi(m) = 1$, $m \in \{1, 2\}$ и $x \in \{41, 82\}$.

Ответ. Уравнение имеет девять решений:
$x \in \{41, 55, 75, 82, 88, 100, 110, 132, 150\}$. □

Пример 6. *Перечислите все натуральные числа a такие, что количество натуральных чисел не превышающих a и имеющих с a наибольший общий делитель 15, равно* 10.

Доказательство. Пусть b — произвольное натуральное число такое, что $b < a$ и $(a, b) = 15$. Тогда $(\frac{a}{15}, \frac{b}{15}) = 1$. Поэтому число натуральных чисел, не превышающих a и имеющих с a наибольшим общим делителем число 15, равно $\varphi(\frac{a}{15})$. Остается решить уравнение $\varphi(\frac{a}{15}) = 10$. Используя пример 2.4, получим $\frac{a}{15} \in \{11, 22\}$.

Ответ. $a \in \{165, 330\}$.

□

Задачи для самостоятельного решения

1. Вычислите значения функций Эйлера, σ и τ от числа a.

1.1. $a = 142560$. 1.2. $a = 421200$.
1.3. $a = 539000$ 1.4. $a = 476000$.
1.5. $a = 105840$. 1.6. $a = 273000$.
1.7. $a = 853776$. 1.8. $a = 794976$.
1.9. $a = 702702$. 1.10. $a = 343035$.
1.11. $a = 798525$. 1.12. $a = 606375$.
1.13. $a = 268125$. 1.14. $a = 523908$.
1.15. $a = 548856$.

2. Сколькими нулями заканчивается десятичная запись числа $\varphi(a!)$?

2.1. $a = 92$. 2.2. $a = 72$. 2.3. $a = 88$.
2.4. $a = 104$. 2.5. $a = 64$. 2.6. $a = 90$.
2.7. $a = 69$. 2.8. $a = 80$. 2.9. $a = 100$.
2.10. $a = 60$. 2.11. $a = 85$. 2.12. $a = 70$.
2.13. $a = 98$. 2.14. $a = 109$. 2.15. $a = 79$.

3. Пусть $a! = 2^{\alpha_2}3^{\alpha_3}5^{\alpha_5}\ldots$ — каноническое разложение $a!$. Вычислите $\tau(2^{\alpha_2}3^{\alpha_3}5^{\alpha_5})$.

3.1. $a = 23$. 3.2. $a = 16$. 3.3. $a = 18$.
3.4. $a = 27$. 3.5. $a = 20$. 3.6. $a = 28$.

3.7. $a = 24$. 3.8. $a = 30$. 3.9. $a = 25$.
3.10. $a = 29$. 3.11. $a = 32$. 3.12. $a = 22$.
3.13. $a = 21$. 3.14. $a = 31$. 3.15. $a = 33$.

4. Пусть $a! = 2^{\alpha_2}3^{\alpha_3}5^{\alpha_5}\ldots$ — каноническое разложение $a!$. Вычислите $\sigma(5^{\alpha_5}7^{\alpha_7}11^{\alpha_{11}})$.

4.1. $a = 21$. 4.2. $a = 31$. 4.3. $a = 33$.
4.4. $a = 23$. 4.5. $a = 16$. 4.6. $a = 18$.
4.7. $a = 27$. 4.8. $a = 20$. 4.9. $a = 28$.
4.10. $a = 24$. 4.11. $a = 30$. 4.12. $a = 25$.
4.13. $a = 29$. 4.14. $a = 32$. 4.15. $a = 22$.

5. Решите уравнение.

5.1. $\varphi(x) = 8$. 5.2. $\varphi(x) = 12$.
5.3. $\varphi(x) = 24$. 5.4. $\varphi(x) = 16$.
5.5. $\varphi(x) = 18$. 5.6. $\varphi(x) = 36$.
5.7. $\varphi(x) = 40$. 5.8. $\varphi(x) = 42$.
5.9. $\varphi(x) = 56$. 5.10. $\varphi(x) = 60$.
5.11. $\varphi(x) = 84$. 5.12. $\varphi(x) = 88$.
5.13. $\varphi(x) = 100$. 5.14. $\varphi(x) = 108$.
5.15. $\varphi(x) = 112$.

6. Найдите все простые делители числа x из уравнения.

6.1. $11\varphi(x) = 4x$. 6.2. $35\varphi(x) = 12x$.
6.3. $31\varphi(x) = 12x$. 6.4. $19\varphi(x) = 9x$.
6.5. $65\varphi(x) = 24x$. 6.6. $13\varphi(x) = 4x$.

6.7. $77\varphi(x) = 30x$. 6.8. $15\varphi(x) = 4x$.
6.9. $23\varphi(x) = 20x$. 6.10. $29\varphi(x) = 12x$.
6.11. $33\varphi(x) = 16x$. 6.12. $51\varphi(x) = 16x$.
6.13. $31\varphi(x) = 8x$. 6.14. $37\varphi(x) = 12x$.
6.15. $41\varphi(x) = 16x$.

7. Решите уравнение.

7.1. $\varphi(3^x5^y7^z) = 720$. 7.2. $\varphi(3^x13^y) = 12168$.
7.3. $\varphi(3^x5^y) = 600$. 7.4. $\varphi(5^x7^y) = 600$.
7.5. $\varphi(3^x5^y7^z) = 25200$. 7.6. $\varphi(5^x7^y11^z) = 18480$.
7.7. $\varphi(5^x7^y11^z) = 4200$. 7.8. $\varphi(5^x11^y) = 2200$.
7.9. $\varphi(2^x13^y) = 1248$. 7.10. $\varphi(3^x17^y) = 4896$.
7.11. $\varphi(3^x7^y11^z) = 1980$. 7.12. $\varphi(2^x17^y) = 2176$.
7.13. $\varphi(3^x5^y) = 5400$. 7.14. $\varphi(5^x7^y) = 5880$.
7.15. $\varphi(3^x7^y13^z) = 4056$.

8. Найдите n, если известен его делитель m и значение $\tau(n)$.

8.1. $m = 135$, $\tau(n) = 21$. 8.2. $m = 104$, $\tau(n) = 15$.
8.3. $m = 88$, $\tau(n) = 21$. 8.4. $m = 75$, $\tau(n) = 14$.
8.5. $m = 99$, $\tau(n) = 10$. 8.6. $m = 40$, $\tau(n) = 33$.
8.7. $m = 36$, $\tau(n) = 21$. 8.8. $m = 56$, $\tau(n) = 22$.
8.9. $m = 52$, $\tau(n) = 26$. 8.10. $m = 68$, $\tau(n) = 22$.
8.11. $m = 175$, $\tau(n) = 10$. 8.12. $m = 98$, $\tau(n) = 15$.
8.13. $m = 117$, $\tau(n) = 14$. 8.14. $m = 80$, $\tau(n) = 15$.
8.15. $m = 45$, $\tau(n) = 14$.

9. Пусть $n = p^\alpha q^\beta$, где p и q — различные простые числа, α и β — натуральные числа. Найдите $\tau(n^3)$, если известно значение $\tau(n^2)$.

9. 1. $\tau(n^2) = 77$. 9. 2. $\tau(n^2) = 75$.
9. 3. $\tau(n^2) = 85$. 9. 4. $\tau(n^2) = 91$.
9. 5. $\tau(n^2) = 93$. 9. 6. $\tau(n^2) = 95$.
9. 7. $\tau(n^2) = 99$. 9. 8. $\tau(n^2) = 105$.
9. 9. $\tau(n^2) = 111$. 9. 10. $\tau(n^2) = 115$.
9. 11. $\tau(n^2) = 117$. 9. 12. $\tau(n^2) = 119$.
9. 13. $\tau(n^2) = 121$. 9. 14. $\tau(n^2) = 133$.
9. 15. $\tau(n^2) = 135$.

10. Перечислите все натуральные числа a такие, что количество натуральных чисел не превышающих a и имеющих с a наибольший общий делитель 15, равно b.

10. 1. $b = 16$. 10. 2. $b = 18$. 10. 3. $b = 36$.
10. 4. $b = 40$. 10. 5. $b = 42$. 10. 6. $b = 56$.
10. 7. $b = 60$. 10. 8. $b = 84$. 10. 9. $b = 88$.
10. 10. $b = 100$. 10. 11. $b = 108$. 10. 12. $b = 112$.
10. 13. $b = 8$. 10. 14. $b = 12$. 14. 15. $b = 24$.

6. Практическое занятие по теме «Решение сравнений»

Пример 1. *Решите сравнение* $7x \equiv 16 \pmod{23}$.

Доказательство. Первый способ. Так как $16 \equiv -7 \pmod{23}$, то $7x \equiv -7 \pmod{23}$ и можно обе части сравнения поделить на 7. Тогда $x \equiv -1 \equiv 22 \pmod{23}$. Таким образом, решением данного сравнения будет любое число из класса $\overline{22} = \{22 + 23t \mid t \in \mathbb{Z}\}$.

Второй способ. Так как 7 и 23 взаимно просты, то по теореме Эйлера $7^{\varphi(23)} \equiv 1 \pmod{23}$. Число 23 — простое, поэтому $\varphi(23) = 22$. Следовательно, $7^{22} \equiv 1 \pmod{23}$. Умножим обе части сравнения $7x \equiv 16 \pmod{23}$ на 7^{21}, получим $x \equiv 7^{21} \cdot 16 \pmod{23}$. Найдем остаток при делении $7^{21} \cdot 16$ на 23. Так как $7^2 = 49 \equiv 3 \pmod{23}$, то $7^{21} = (7^2)^{10} \cdot 7 \equiv 3^{10} \cdot 7 \pmod{23}$. Поскольку $3^3 = 27 \equiv 4 \pmod{23}$, то $3^{10} \cdot 7 = (3^3)^3 \cdot 3 \cdot 7 \equiv 4^3 \cdot 21 \pmod{23}$. Так как $4^3 = 64 \equiv -5 \pmod{23}$ и $21 \equiv -2 \pmod{23}$, то $4^3 \cdot 21 \equiv (-5) \cdot (-2) \pmod{23}$. Итак, $7^{21} \equiv 10 \pmod{23}$. Тогда $7^{21} \cdot 16 \equiv 10 \cdot 16 \pmod{23}$. Поскольку $160 \equiv 22 \pmod{23}$, то $7^{21} \cdot 16 \equiv 22 \pmod{23}$. Таким образом, $x \equiv 22 \pmod{23}$.

Ответ. $x \equiv 22 \pmod{23}$. □

Пример 2. Решите сравнение $22x \equiv 29 \pmod{32}$.

Доказательство. Так как $\text{НОД}(22, 32) = 2$ и 29 не делится на 2, то сравнение решений не имеет.

Ответ: решений нет. □

Пример 3. Решите сравнение $15x \equiv 5 \pmod{25}$.

Доказательство. Здесь НОД$(15, 25) = 5$ и 5 делится на 5. Следовательно, сравнение имеет 5 решений.

После деления обеих частей сравнения и модуля на 5 получим сравнение $3x \equiv 1 \pmod 5$. Полученное сравнение имеет единственное решение, так как НОД$(3, 5) = 1$. Его решением является $x \equiv 2 \pmod 5$. Тогда $\overline{2}, \overline{7}, \overline{12}$ — решения исходного сравнения.
Ответ: $\overline{2}, \overline{7}, \overline{12}$. □

Пример 4. *В кольце* $\mathbb{Z}_{14}$ *решите уравнение* $6 \cdot \overline{x} = \overline{10}$.

□ Вначале решим сравнение $6x \equiv 10 \pmod{14}$. Так как $2 =$ НОД$(6, 14)$ делит 10, то сравнение имеет два решения. Разделим сравнение на 2. Получим $3x \equiv 5 \pmod 7$. Так как 3 и 7 взаимно просты, то это сравнение имеет единственное решение по модулю 7. Подставляя числа 0, 1, 2, 3, 4, 5, 6, получаем, что $x \equiv 4 \pmod 7$. Итак, решениями исходного сравнения будут целые числа $x = 4 + 7t$, $t \in \mathbb{Z}$, которые составляют класс вычетов по модулю 7. Этот класс распадается на два класса вычетов $\overline{4} = \{4 + 14t \mid t \in \mathbb{Z}\}$ и $\overline{11} = \{11 + 14t \mid t \in \mathbb{Z}\}$ по модулю 14. Таким образом, сравнение имеет два решения: $x_1 \equiv 4 \pmod{14}$, $x_2 \equiv 11 \pmod{14}$. В кольце $\mathbb{Z}_{14}$ этим решениям соответствуют классы вычетов $\overline{4}$ и $\overline{11}$.
Ответ. Уравнение имеет два решения: $x_1 = \overline{4}$, $x_2 = \overline{11}$. ⊠

Пример 5. *В кольце* $\mathbb{Z}_5$ *решите уравнение* $x^2 + x - \overline{2} = \overline{0}$.

□ Проверка показывает, что среди элементов кольца $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ уравнению удовлетворяют только два: $\overline{1}$ и $\overline{3}$.
Ответ. Уравнение имеет два решения: $x_1 = \overline{1}$, $x_2 = \overline{3}$. ⊠

Пример 6. *Найдите все целочисленные решения уравнения*

$$54x - 42y = -18.$$

□ Выразим одну из неизвестных через другую:

Чтобы y было целым, x должно удовлетворять сравнению

$$54x + 18 \equiv 0 \pmod{42},\ 54x \equiv -18 \pmod{42}.$$

Так как НОД$(54, 42) = 6$ делит (-18), то последнее сравнение имеет 6 решений по модулю 42. Разделив обе части сравнения и модуль на 6, получим: $9x \equiv -3 \pmod 7$. Перебирая возможные остатки от делении на 7, получаем: $x \equiv 2 \pmod 7$. Решениями сравнения $54x + 18 \equiv 0 \pmod{42}$ будут целые числа из следующих классов вычетов по модулю 42: $\overline{2}$, $\overline{9}$, $\overline{16}$, $\overline{23}$, $\overline{30}$, $\overline{37}$. Все числа этих классов можно записать в виде: $x = 2 + 7t$, где $t \in \mathbb{Z}$. Найдем значения y:

$$y = \frac{126 + 378t}{42} = 3 + 9t, \quad t \in \mathbb{Z}.$$

Ответ. $x = 2 + 7t$, $y = 3 + 9t$, $t \in \mathbb{Z}$. ⊠

Задачи для самостоятельного решения

1. Решите сравнения.

1.1. $3x \equiv 1 \pmod 7$, $15x \equiv 9 \pmod{11}$, $42x \equiv 12 \pmod{90}$.

1.2. $5x \equiv 9 \pmod 6$, $29x \equiv 15 \pmod{19}$, $55x \equiv 35 \pmod{75}$.

1.3. $13x \equiv 20 \pmod 4$, $6x \equiv 22 \pmod{13}$, $20x \equiv 12 \pmod{72}$.

1.4. $16x \equiv -6 \pmod 9$, $14x \equiv -9 \pmod{17}$, $25x \equiv 45 \pmod{60}$.

1.5. $17x \equiv -20 \pmod 3$, $9x \equiv -8 \pmod{23}$, $21x \equiv 7 \pmod{49}$.

1.6. $5x \equiv 7 \pmod 8$, $10x \equiv 15 \pmod{17}$, $10x \equiv 25 \pmod{35}$.

1.7. $7x \equiv 6 \pmod{15}$, $18x \equiv 12 \pmod{19}$, $10x \equiv 12 \pmod{14}$.

1.8. $27x \equiv -14 \pmod{25}$, $21x \equiv 14 \pmod{23}$, $26x \equiv 2 \pmod{30}$.

1.9. $13x \equiv 10 \pmod{11}$, $24x \equiv 16 \pmod{25}$, $15x \equiv 21 \pmod{24}$.

1.10. $5x \equiv -2 \pmod{11}$, $15x \equiv 10 \pmod{19}$,
$10x \equiv 14 \pmod{22}$.

1.11. $4x \equiv 7 \pmod{17}$, $14x \equiv 35 \pmod{37}$,
$15x \equiv 25 \pmod{35}$.

1.12. $7x \equiv 5 \pmod{8}$, $22x \equiv 33 \pmod{39}$,
$12x \equiv 21 \pmod{27}$.

1.13. $5x \equiv 6 \pmod{7}$, $21x \equiv 35 \pmod{37}$,
$10x \equiv -4 \pmod{22}$.

1.14. $3x \equiv -8 \pmod{13}$, $26x \equiv 39 \pmod{41}$,
$14x \equiv 12 \pmod{30}$.

1.15. $3x \equiv -7 \pmod{11}$, $15x \equiv 20 \pmod{23}$,
$16x \equiv 28 \pmod{36}$.

2. Решите сравнение первой степени.

2.1. $114x \equiv 42 \pmod{87}$.

2.2. $39x \equiv 84 \pmod{93}$.

2.3. $111x \equiv 81 \pmod{447}$.

2.4. $186x \equiv 374 \pmod{422}$.

2.5. $375x \equiv 195 \pmod{501}$.

2.6. $129x \equiv 321 \pmod{471}$.

2.7. $117x \equiv 168 \pmod{186}$.

2.8. $132x \equiv 147 \pmod{189}$.

2.9. $112x \equiv 140 \pmod{252}$.

2.10. $176x \equiv 196 \pmod{252}$.
2.11. $273x \equiv 161 \pmod{343}$.
2.12. $294x \equiv 132 \pmod{450}$.
2.13. $210x \equiv 180 \pmod{270}$.
2.14. $195x \equiv 147 \pmod{264}$.
2.15. $126x \equiv 210 \pmod{147}$.

3. Решите уравнение в кольце $\mathbb{Z}_m$.

3.1. $\overline{2}x^3 - \overline{3}x^2 + \overline{2}x - \overline{1} = \overline{0}$, $m = 7$.
3.2. $x^4 - \overline{4}x^2 - \overline{2} = \overline{0}$, $m = 5$.
3.3. $x^3 - \overline{2}x^2 + x + \overline{1} = \overline{0}$, $m = 3$.
3.4. $\overline{4}x^4 + x^2 + \overline{2}x + \overline{2} = \overline{0}$, $m = 5$.
3.5. $x^3 + \overline{5}x^2 - \overline{15}x + \overline{22} = \overline{0}$, $m = 7$.
3.6. $\overline{5}x^4 + x^2 - x + \overline{2} = \overline{0}$, $m = 7$.
3.7. $\overline{3}x^4 + \overline{2}x^2 - \overline{1} = \overline{0}$, $m = 5$.
3.8. $\overline{7}x^3 - \overline{5}x + \overline{1} = \overline{0}$, $m = 13$.
3.9. $\overline{4}x^3 - \overline{7}x^2 + \overline{10} = \overline{0}$, $m = 11$.
3.10. $\overline{2}x^4 + \overline{5}x + \overline{3} = \overline{0}$, $m = 6$.
3.11. $\overline{3}x^3 + \overline{2}x^2 - \overline{2} = \overline{0}$, $m = 5$.
3.12. $\overline{5}x^3 + \overline{3}x + \overline{3} = \overline{0}$, $m = 7$.
3.13. $\overline{4}x^3 + \overline{7}x - \overline{1} = \overline{0}$, $m = 8$.
3.14. $\overline{4}x^4 + \overline{3}x^2 + \overline{2} = \overline{0}$, $m = 6$.
3.15. $\overline{2}x^3 - \overline{7}x + \overline{3} = \overline{0}$, $m = 5$.

Кафедра
ФМО и ИТ

4. Решите уравнение в кольце $\mathbb{Z}_m$.

4.1. $\overline{132}x^3 + \overline{143}x^2 + \overline{23}x - \overline{19} = \overline{5}$, $m = 11$.
4.2. $\overline{117}x^3 + \overline{143}x^2 + \overline{3}x - \overline{19} = \overline{5}$, $m = 13$.
4.3. $\overline{153}x^3 + \overline{187}x^2 + \overline{11}x - \overline{9} = \overline{5}$, $m = 17$.
4.4. $\overline{361}x^3 + \overline{209}x^2 + \overline{23}x - \overline{11} = \overline{5}$, $m = 19$.
4.5. $\overline{253}x^3 + \overline{115}x^2 + \overline{12}x - \overline{9} = \overline{5}$, $m = 23$.
4.6. $\overline{164}x^3 - \overline{205}x^2 + \overline{26}x - \overline{30} = \overline{9}$, $m = 41$.
4.7. $\overline{273}x^3 + \overline{195}x^2 + \overline{22}x - \overline{22} = \overline{11}$, $m = 39$.
4.8. $\overline{289}x^3 - \overline{272}x^2 + \overline{10}x - \overline{10} = \overline{5}$, $m = 17$.
4.9. $\overline{342}x^3 - \overline{228}x^2 + \overline{18}x - \overline{18} = -\overline{6}$, $m = 19$.
4.10. $\overline{437}x^3 - \overline{184}x^2 + \overline{21}x - \overline{21} = -\overline{7}$, $m = 23$.
4.11. $\overline{225}x^3 + \overline{325}x^2 + \overline{24}x - \overline{16} = \overline{0}$, $m = 25$.
4.12. $\overline{152}x^3 - \overline{323}x^2 + \overline{15}x - \overline{15} = -\overline{5}$, $m = 19$.
4.13. $\overline{444}x^3 + \overline{333}x^2 + \overline{14}x - \overline{35} = \overline{0}$, $m = 37$.
4.14. $\overline{228}x^3 - \overline{304}x^2 + \overline{29}x - \overline{10} = \overline{5}$, $m = 19$.
4.15. $\overline{529}x^3 + \overline{437}x^2 + \overline{9}x - \overline{9} = -\overline{17}$, $m = 23$.

5. Найдите при каких $\overline{a}$ и $\overline{b}$ уравнение в кольце $\mathbb{Z}_m$: имеет единственное решение; не имеет решений; имеет ровно m решений; имеет нулевое решение.

5.1. $\overline{a}x + \overline{b} = x$, $m = 3$.
5.2. $\overline{2}x - \overline{b} = \overline{a}x$, $m = 5$.
5.3. $\overline{(a-1)}x - \overline{a} = \overline{b}$, $m = 7$.

5.4. $\overline{a}x + \overline{2b} = \overline{3}x$, $m = 5$.

5.5. $\overline{a}x + \overline{a} = -\overline{b}x$, $m = 11$.

5.6. $\overline{(a+1)}x - \overline{2a} = \overline{b-1}$, $m = 7$.

5.7. $\overline{(b+3)}x = \overline{(a-3)}x + \overline{1}$, $m = 5$.

5.8. $\overline{b}x - \overline{2} = \overline{2}x$, $m = 11$.

5.9. $\overline{ab}x = \overline{b}$, $m = 13$.

5.10. $\overline{(a-1)}x = \overline{(ab-1)}x + \overline{a}$, $m = 17$.

5.11. $\overline{b}x + \overline{a} = x$, $m = 5$.

5.12. $\overline{3}x - \overline{a} = \overline{b}x$, $m = 7$.

5.13. $\overline{(2a-1)}x - \overline{ab} = \overline{b}$, $m = 11$.

5.14. $\overline{b}x + \overline{ab} = -\overline{a}x$, $m = 7$.

5.15. $-\overline{a}x = -\overline{b}x + \overline{a}$, $m = 5$.

6. Решите, используя сравнения, задачу 3 и 4 из темы «Линейные диофантовы уравнения».

7. Практическое занятие по теме «Системы сравнений»

Пример 1. При каких значениях a имеет решение система сравнений

$$\begin{cases} x \equiv 5 \pmod{18} \\ x \equiv 8 \pmod{21} \\ x \equiv a \pmod{35}. \end{cases}$$

Доказательство. Из первого сравнения находим: $x = 18t + 5$. Подставим x во второе сравнение t: $18t + 5 \equiv 8 \pmod{21}$, $18t \equiv 3 \pmod{21}$, $6t \equiv 1 \pmod{7}$, $t \equiv 6 \pmod{7}$. Удобнее взять $t \equiv -1 \pmod{7}$, откуда $t = 7t_1 - 1$. Подставим найденное значение t в первое равенство: $x = 18(7t_1 - 1) + 5 = 126t_1 - 13$. Это значение x подставим в третье сравнение системы: $126t_1 - 13 \equiv a \pmod{35}$, т. е. $21t_1 \equiv a + 13 \pmod{35}$. Так как НОД$(21, 35) = 7$, то по теореме о существовании решения 7 должно делить $a + 13 = a - 1 + 14$, или $a \equiv 1 \pmod{7}$.

Ответ. При $a \equiv 1 \pmod{7}$.

□

Пример 2. Найдите наибольшее трехзначное натуральное число, которое при делении на 3, 5, 7 дает остаток 2, 4, 3 соответственно.

Доказательство. Пусть x — искомое число. Тогда имеем систему

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod 7. \end{cases}$$

Решим ее вторым способом. Так как $m = 3 \cdot 5 \cdot 7$, то $M_1 = 35$, $M_2 = 21$, $M_3 = 15$. Решаем сравнения:

$35x \equiv 1 \pmod 3$, $x = 2 = a_1$,
$21x \equiv 1 \pmod 5$, $x = 1 = a_2$,
$15x \equiv 1 \pmod 7$, $x = 1 = a_3$.

Вычисляем $c = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 3 \cdot 1 = 269 \equiv 59 \pmod{105}$. Теперь $x = 59 + 105t$, $t \in \mathbb{Z}$. Так как $59 + 105 \cdot 8 = 899$, а $59 + 105 \cdot 9 = 1004$, то $x = 899$.

Ответ. 899. □

Пример 3. *Найдите остаток от деления числа* 19^{14} *на* 70.

Доказательство. Так как $70 = 2 \cdot 5 \cdot 7$, $19 \equiv 1 \pmod 2$, $19 \equiv (-1) \pmod 5$, $19 \equiv (-2) \pmod 7$, то $19^{14} \equiv 1 \pmod{10}$, $19^{14} \equiv 2^{14} = 2^{2 \cdot 6} + 2 \equiv 2^2 \pmod 7$. Здесь применили малую теорему Ферма: $2^6 \equiv 1 \pmod 7$. Остаток является решением системы

$$\begin{cases} x \equiv 1 \pmod{10} \\ x \equiv 4 \pmod 7. \end{cases}$$

Решая эту систему, получим: $x = 11$.
Ответ. 11. □

Пример 4. *Решите систему сравнений*

$$\begin{cases} 2x + 3y \equiv 1 \pmod 6 \\ 3x - 4y \equiv 3 \pmod 6. \end{cases}$$

Доказательство. Умножим обе части первого сравнение системы на 3, а второго — на 2:

$$\begin{cases} 6x + 9y \equiv 3 \pmod 6 \\ 6x - 8y \equiv 6 \pmod 6. \end{cases}$$

Вычтем из первого сравнения системы второе:

$$17y \equiv -3 \pmod 6,\ y \equiv 3 \pmod 6.$$

Подставим $y = 3 + 6t$, $t \in \mathbb{Z}$ в первое сравнение исходной системы: $2x + 9 + 18t \equiv 1 \pmod 6$, $x \equiv 5 \pmod 6$.
Ответ. $x = 5 + 6s$, $y = 3 + 6t$, $t, s \in \mathbb{Z}$.

□

Напомним, что запись

$$A = \overline{a_n a_{n-1} \dots a_1 a_0},$$

означает натуральное число A, которое в десятичной системе счисления представимо в виде:

$$A = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots + 10 \cdot a_1 + a_0,$$

здесь $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{N} \cup \{0\}$, $a_n \neq 0$.

Пример 5. *Число* $\overline{13xy45z}$ *делится на* 792. *Найдите* x, y *и* z.

Доказательство. Так как $792 = 8 \cdot 9 \cdot 11$ и

$$\overline{13xy45z} = 13 \cdot 10^5 + x \cdot 10^4 + y \cdot 10^3 + 450 + z,$$

то можно записать систему:

$$\begin{cases} 13 \cdot 10^5 + x \cdot 10^4 + y \cdot 10^3 + 450 + z \equiv 0 \pmod 8 \\ 13 \cdot 10^5 + x \cdot 10^4 + y \cdot 10^3 + 450 + z \equiv 0 \pmod 9 \\ 13 \cdot 10^5 + x \cdot 10^4 + y \cdot 10^3 + 450 + z \equiv 0 \pmod{11}. \end{cases}$$

Так как 10^5, 10^4 и 10^3 делятся на 8, а $450 = 8 \cdot 56 + 2$, то из первого сравнения имеем:

$$2 + z \equiv 0 \pmod 8, \; z \equiv -2 \equiv 6 \pmod 8.$$

Но $0 \leq z \leq 9$, поэтому $z = 6$ и $\overline{13xy45z} = \overline{13xy456}$. Поскольку $10 \equiv 1 \pmod 9$, то $10^n \equiv 1 \pmod 9$ для любого натурального n и из второго сравнения имеем:

$$13 + x + y + 456 \equiv 0 \pmod 9, \; x + y + 1 \equiv 0 \pmod 9.$$

Поскольку $10 \equiv -1 \pmod{11}$, то $10^n \equiv (-1)^n \pmod{11}$ для любого n и из третьего сравнения имеем:

$$-13 + x - y + 456 \equiv 0 \pmod{11},\ x - y + 3 \equiv 0 \pmod{11}.$$

Получаем новую систему:

$$\begin{cases} x + y + 1 \equiv 0 \pmod{9} \\ x - y + 3 \equiv 0 \pmod{11}, \end{cases} \qquad \begin{cases} x + y \equiv 8 \pmod{9} \\ x - y \equiv 8 \pmod{11}, \end{cases}$$

где $0 \leq x + y \leq 18$. Из первого сравнения получаем две возможности: $x + y = 8$ или $x + y = 17$. Но теперь из второго сравнения вытекает, что система имеет единственное решение: $x = 8$ и $y = 0$.
Ответ. $x = 8$, $y = 0$, $z = 2$. □

Пример 6. *Перпендикуляр к оси абсцисс пересекает прямые*

$$4x - 7y = 9,\ 2x + 9y = 15,\ 5x - 13y = 12$$

в точках с целочисленными координатами. Найдите координаты точек пересечения. В ответ запишите координаты с наименьшим натуральным значением абсциссы.

Доказательство. Поскольку точки пересечения лежат на одном перпендикуляре к оси абсцисс, то их координаты имеют одинаковые абсциссы. Но точки пересечения имеют целочисленные координаты, поэтому абсцисса точек пересечения является решением системы сравнений:

$$\begin{cases} 4x \equiv 9 \pmod 7 \\ 2x \equiv 15 \pmod 9 \\ 5x \equiv 12 \pmod{13}, \end{cases} \quad \begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 3 \pmod 9 \\ x \equiv 5 \pmod{13}. \end{cases}$$

Решая ее, получим: $x = 291 + 819t$, $t \in \mathbb{Z}$. Соответствующие ординаты будут равны:

$$y_1 = \frac{4 \cdot (291 + 819t) - 9}{7} = 165 + 468t,$$

$$y_2 = \frac{2 \cdot (291 + 819t) - 15}{-9} = -63 - 182t,$$

$$y_3 = \frac{5 \cdot (291 + 819t) - 12}{13} = 111 + 315t.$$

Искомые координаты точек: $(291 + 819t; 165 + 468t)$, $(291 + 819t; -63 - 182t)$, $(291 + 819t; 111 + 315t)$, $t \in \mathbb{Z}$.

Ответ. $(291; 165)$, $(291; -63)$, $(291; 111)$.

□

Пример 7. *При каких целых k число $a = k^2 + 3k + 1$ делится на 55?*

Доказательство. Так как $55 = 5 \cdot 11$, то значение a должно делится на 5 и на 11. Разделим k с остатком на 5: $k = 5q_1 + r_1$, $r_1 \in \{0, 1, 2, 3, 4\}$. Подставляя $k = 5q_1 + r_1$ в a, получим по модулю 5 сравнение:

$$a \equiv r_1^2 + 3r_1 + 1 \in \{\overline{1}, \overline{0}, \overline{1}, \overline{4}, \overline{4}\}.$$

Итак, a делится на 5 при $k = 5q_1 + 1$.

Разделим k с остатком на 11:

$$k = 11q_2 + r_2,\ r_2 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

Подставляя $k = 11q_2 + r_2$ в a, получим по модулю 11 сравнение:

$$a \equiv r_2^2 + 3r_2 + 1 \in \{\overline{1}, \overline{5}, \overline{0}, \overline{8}, \overline{7}, \overline{8}, \overline{0}, \overline{5}, \overline{1}, \overline{10}, \overline{10}\}.$$

Итак, a делится на 11 при $k = 11q_2 + 2$ и $k = 11q_2 + 6$.

Таким образом, получаем две системы:

$$\begin{cases} k \equiv 1 \pmod 5 \\ k \equiv 2 \pmod{11}, \end{cases} \qquad \begin{cases} k \equiv 1 \pmod 5 \\ k \equiv 6 \pmod{11}. \end{cases}$$

Решаем первую систему. Из первого сравнения получаем: $k = 1 + 5t$. Подставляем во второе сравнение: $1 + 5t \equiv 2 \pmod{11}$, $5t \equiv 1 \pmod{11}$, $t \equiv 9 \pmod{11}$, $t = 9 + 11l$, $k = 1 + 5(9 + 11l) = 46 + 55l$.

Решаем вторую систему. Из первого сравнения получаем: $k = 1 + 5t$. Подставляем во второе сравнение: $1 + 5t \equiv 6 \pmod{11}$, $5t \equiv 5 \pmod{11}$, $t \equiv 1 \pmod{11}$, $t = 1 + 11s$, $k = 1 + 5(1 + 11s) = 6 + 55s$.

Проверка. При $k = 6 + 55s$ имеем: $a \equiv 6^2 + 3 \cdot 6 + 1 = 36 + 18 + 1 = 55$ делится на 55.

При $k = 46 + 55l$ имеем: $a \equiv 46^2 + 3 \cdot 46 + 1 = 2116 + 138 + 1 = 2255 = 55 \cdot 41$ делится на 55.

Ответ. Число k^2+3k+1 делится на 55 в двух случаях: k при делении на 55 дает остаток 6 и k при делении на 55 дает остаток 46. $\square$

Задачи для самостоятельного решения

1. Решите системы сравнений.

1.1. $\begin{cases} 7x \equiv 3 \pmod{11} \\ 3x \equiv 1 \pmod{7} \\ 3x \equiv 2 \pmod{5}, \end{cases} \quad \begin{cases} x \equiv 13 \pmod{16} \\ x \equiv 3 \pmod{10} \\ x \equiv 9 \pmod{14}. \end{cases}$

1.2. $\begin{cases} x \equiv 1 \pmod{3} \\ 3x \equiv 5 \pmod{7} \\ 2x \equiv 3 \pmod{5}, \end{cases} \quad \begin{cases} 3x \equiv 5 \pmod{10} \\ 2x \equiv 5 \pmod{15} \\ 7x \equiv 5 \pmod{13}. \end{cases}$

1.3. $\begin{cases} 3x \equiv 2 \pmod{7} \\ x \equiv 8 \pmod{11} \\ 2x \equiv 9 \pmod{15}, \end{cases} \quad \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{14}. \end{cases}$

1.4. $\begin{cases} 7x \equiv 10 \pmod{11} \\ 12x \equiv 7 \pmod{13} \\ 7x \equiv 11 \pmod{15}, \end{cases} \quad \begin{cases} 4x \equiv 1 \pmod{9} \\ 5x \equiv 3 \pmod{7} \\ 5x \equiv 5 \pmod{12}. \end{cases}$

1.5. $\begin{cases} 2x \equiv 1 \pmod{3} \\ 2x \equiv 2 \pmod{7} \\ 17x \equiv 7 \pmod{11}, \end{cases} \quad \begin{cases} 5x \equiv 3 \pmod{8} \\ 7x \equiv 3 \pmod{11} \\ 5x \equiv 1 \pmod{6}. \end{cases}$

1.6. $\begin{cases} 4x \equiv 7 \pmod{13} \\ x \equiv 2 \pmod{17} \\ 5x \equiv 3 \pmod{9}, \end{cases} \quad \begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 18 \pmod{21} \\ x \equiv 3 \pmod{12}. \end{cases}$

1.7. $\begin{cases} 4x \equiv 3 \pmod 7 \\ 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13}, \end{cases}$

1.8. $\begin{cases} 2x \equiv 7 \pmod{13} \\ 5x \equiv 8 \pmod{17} \\ 14x \equiv 35 \pmod{19}, \end{cases}$

1.9. $\begin{cases} 2x \equiv 5 \pmod{11} \\ 7x \equiv 6 \pmod{13} \\ 3x \equiv 7 \pmod{17}, \end{cases}$

1.10. $\begin{cases} 2x \equiv 3 \pmod 7 \\ 3x \equiv 6 \pmod{11} \\ x \equiv 2 \pmod 5, \end{cases}$

1.11. $\begin{cases} 3x \equiv 2 \pmod 7 \\ 3x \equiv 1 \pmod 5 \\ 7x \equiv 3 \pmod{11}, \end{cases}$

1.12. $\begin{cases} 7x \equiv 7 \pmod{13} \\ 2x \equiv 1 \pmod 3 \\ 3x \equiv 2 \pmod 5, \end{cases}$

1.13. $\begin{cases} x \equiv 2 \pmod 9 \\ 5x \equiv 3 \pmod{13} \\ 4x \equiv 7 \pmod{11}, \end{cases}$

$x \equiv 13 \pmod{14}$
$x \equiv 6 \pmod{35}$
$x \equiv 26 \pmod{45}$.
$x \equiv 19 \pmod{56}$
$x \equiv 3 \pmod{24}$
$x \equiv 7 \pmod{20}$.
$x \equiv 19 \pmod{22}$
$x \equiv 8 \pmod{33}$
$x \equiv 14 \pmod{21}$.
$3x \equiv 7 \pmod{10}$
$2x \equiv 3 \pmod{7}$
$7x \equiv 8 \pmod{15}$.
$3x \equiv 1 \pmod{10}$
$4x \equiv 3 \pmod{5}$
$2x \equiv 7 \pmod{9}$.
$7x \equiv 3 \pmod{15}$
$3x \equiv 7 \pmod{10}$
$3x \equiv 2 \pmod{7}$.
$3x \equiv 4 \pmod{5}$
$x \equiv 3 \pmod{10}$
$7x \equiv 2 \pmod{11}$.

1.14. $\begin{cases} 2x \equiv 7 \pmod{17} \\ 5x \equiv 3 \pmod{13} \\ 14x \equiv 12 \pmod{5}, \end{cases} \quad \begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 8 \pmod{15} \\ x \equiv 3 \pmod{11}. \end{cases}$

1.15. $\begin{cases} 11x \equiv 5 \pmod{17} \\ 6x \equiv 1 \pmod{11} \\ 3x \equiv 4 \pmod{7}, \end{cases} \quad \begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 13 \pmod{15} \\ 7x \equiv 9 \pmod{11}. \end{cases}$

2. При каких целых a система сравнений имеет решение?

2.1. $\begin{cases} x \equiv a \pmod{10} \\ x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{14}. \end{cases}$

2.2. $\begin{cases} 4x \equiv 1 \pmod{9} \\ 5x \equiv a \pmod{14} \\ 5x \equiv 5 \pmod{12}. \end{cases}$

2.3. $\begin{cases} 5x \equiv 3 \pmod{8} \\ 7x \equiv 3 \pmod{11} \\ 5x \equiv a \pmod{6}. \end{cases}$

2.4. $\begin{cases} x \equiv a \pmod{15} \\ x \equiv 18 \pmod{21} \\ x \equiv 3 \pmod{12}. \end{cases}$

2.5. $\begin{cases} x \equiv 13 \pmod{14} \\ x \equiv a \pmod{35} \\ x \equiv 26 \pmod{45}. \end{cases}$

2.6. $\begin{cases} x \equiv 19 \pmod{56} \\ x \equiv 3 \pmod{24} \\ x \equiv a \pmod{20}. \end{cases}$

2.7. $\begin{cases} x \equiv a \pmod{22} \\ x \equiv 8 \pmod{33} \\ x \equiv 14 \pmod{21}. \end{cases}$

2.8. $\begin{cases} 3x \equiv 7 \pmod{10} \\ 2x \equiv a \pmod{21} \\ 7x \equiv 8 \pmod{15}. \end{cases}$

2.9. $\begin{cases} 3x \equiv 1 \pmod{10} \\ 4x \equiv 3 \pmod{5} \\ x \equiv a \pmod{18}. \end{cases}$

2.10. $\begin{cases} 7x \equiv a \pmod{15} \\ 3x \equiv 7 \pmod{10} \\ 3x \equiv 2 \pmod{7}. \end{cases}$

2.11. $\begin{cases} 3x \equiv 4 \pmod 5 \\ x \equiv a \pmod{10} \\ 7x \equiv 2 \pmod{11}. \end{cases}$ 2.12. $\begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 8 \pmod{15} \\ x \equiv a \pmod{22}. \end{cases}$

2.13. $\begin{cases} x \equiv a \pmod{10} \\ x \equiv 13 \pmod{15} \\ 7x \equiv 9 \pmod{11}. \end{cases}$ 2.14. $\begin{cases} x \equiv 13 \pmod{16} \\ x \equiv a \pmod{10} \\ x \equiv 9 \pmod{14}. \end{cases}$

2.15. $\begin{cases} 3x \equiv 5 \pmod{10} \\ 2x \equiv 5 \pmod{15} \\ 7x \equiv a \pmod{26}. \end{cases}$

3. Найдите наибольшее трехзначное натуральное число, которое при делении на a_1, a_2, a_3 дает соответственно остатки b_1, b_2, b_3.

3.1. $\{a_1, a_2, a_3\} = \{13, 5, 12\}$, $\{b_1, b_2, b_3\} = \{5, 1, 7\}$.
3.2. $\{a_1, a_2, a_3\} = \{7, 11, 13\}$, $\{b_1, b_2, b_3\} = \{3, 2, 5\}$.
3.3. $\{a_1, a_2, a_3\} = \{7, 11, 17\}$, $\{b_1, b_2, b_3\} = \{3, 5, 13\}$.
3.4. $\{a_1, a_2, a_3\} = \{7, 13, 17\}$, $\{b_1, b_2, b_3\} = \{4, 9, 1\}$.
3.5. $\{a_1, a_2, a_3\} = \{3, 5, 8\}$, $\{b_1, b_2, b_3\} = \{2, 4, 1\}$.
3.6. $\{a_1, a_2, a_3\} = \{5, 7, 9\}$, $\{b_1, b_2, b_3\} = \{4, 6, 1\}$.
3.7. $\{a_1, a_2, a_3\} = \{15, 14, 11\}$, $\{b_1, b_2, b_3\} = \{11, 3, 5\}$.
3.8. $\{a_1, a_2, a_3\} = \{13, 21, 23\}$, $\{b_1, b_2, b_3\} = \{9, 1, 13\}$.
3.9. $\{a_1, a_2, a_3\} = \{16, 10, 14\}$, $\{b_1, b_2, b_3\} = \{13, 3, 9\}$.
3.10. $\{a_1, a_2, a_3\} = \{5, 12, 14\}$, $\{b_1, b_2, b_3\} = \{4, 1, 7\}$.
3.11. $\{a_1, a_2, a_3\} = \{15, 21, 12\}$, $\{b_1, b_2, b_3\} = \{6, 18, 3\}$.

3. 12. $\{a_1, a_2, a_3\} = \{12, 15, 11\}$, $\{b_1, b_2, b_3\} =$
3. 13. $\{a_1, a_2, a_3\} = \{10, 15, 11\}$, $\{b_1, b_2, b_3\} =$
3. 14. $\{a_1, a_2, a_3\} = \{7, 11, 5\}$, $\{b_1, b_2, b_3\} =$
3. 15. $\{a_1, a_2, a_3\} = \{3, 7, 5\}$, $\{b_1, b_2, b_3\} =$

4. Найдите остаток от деления числа a на b.

4. 1. $a = 15^7$, $b = 55$. 4. 2. $a = 19^{10}$, $b =$
4. 3. $a = 17^9$, $b = 48$. 4. 4. $a = 16^{16}$, $b =$
4. 5. $a = 14^{14}$, $b = 100$. 4. 6. $a = 12^{11}$, $b =$
4. 7. $a = 19^5$, $b = 92$. 4. 8. $a = 15^{16}$, $b =$
4. 9. $a = 24^7$, $b = 86$. 4. 10. $a = 32^{12}$, $b =$
4. 11. $a = 18^{10}$, $b = 70$. 4. 12. $a = 22^{15}$, $b =$
4. 13. $a = 17^{23}$, $b = 92$. 4. 14. $a = 26^5$, $b =$
4. 15. $a = 28^{11}$, $b = 82$.

5. Решите систему сравнений.

5. 1. $\begin{cases} x + 2y \equiv 3 \pmod{13} \\ 4x + y \equiv 5 \pmod{13}. \end{cases}$
5. 2. $\begin{cases} 4x - 6y \equiv 1 \pmod{13} \\ 5x - 7y \equiv 3 \pmod{13}. \end{cases}$
5. 3. $\begin{cases} x + 2y \equiv 0 \pmod{13} \\ 3x + 2y \equiv 2 \pmod{13}. \end{cases}$
5. 4. $\begin{cases} x - 7y \equiv 12 \pmod{16} \\ 4x + 3y \equiv 13 \pmod{16}. \end{cases}$

$\{5, 8, 3\}$.
$\{3, 13, 9\}$.
$\{3, 6, 2\}$.
$\{1, 5, 3\}$.

$= 66$.
$= 85$.
$= 78$.
$= 112$.
$= 80$.
$= 76$.
$= 68$.

5. 5. $\begin{cases} 5x - y \equiv 3 \pmod{16} \\ 2x + 3y \equiv -1 \pmod{16}. \end{cases}$

5. 6. $\begin{cases} 2x + 3y \equiv 1 \pmod{16} \\ 3x - 4y \equiv 3 \pmod{16}. \end{cases}$

5. 7. $\begin{cases} 9x - 3y \equiv 5 \pmod{14} \\ 5x + 6y \equiv 3 \pmod{14}. \end{cases}$

5. 8. $\begin{cases} 8x - 3y \equiv 1 \pmod{14} \\ 2x + 5y \equiv 7 \pmod{14}. \end{cases}$

5. 9. $\begin{cases} 3x + 7y \equiv 13 \pmod{14} \\ 4x - 5y \equiv 12 \pmod{14}. \end{cases}$

5. 10. $\begin{cases} 2x - y \equiv 4 \pmod{15} \\ x + 5y \equiv 3 \pmod{15}. \end{cases}$

5. 11. $\begin{cases} 5x - y \equiv 9 \pmod{15} \\ 2x + 4y \equiv 7 \pmod{15}. \end{cases}$

5. 12. $\begin{cases} x - 5y \equiv 10 \pmod{15} \\ 2x - 2y \equiv -3 \pmod{15}. \end{cases}$

5. 13. $\begin{cases} 3x + y \equiv 3 \pmod{17} \\ 4x - 13y \equiv 1 \pmod{17}. \end{cases}$

5. 14. $\begin{cases} 7x + 5y \equiv 12 \pmod{17} \\ 2x - 7y \equiv 4 \pmod{17}. \end{cases}$

5. 15. $\begin{cases} 6x - 8y \equiv 5 \pmod{17} \\ 3x + 5y \equiv 7 \pmod{17}. \end{cases}$

Кафедра
ФМО и ИТ

6. Найдите все числа a, делящиеся на b.

6.1. $a = \overline{xy9z}$, $b = 132$. 6.2. $a = \overline{8xyz}$, $b = 154$.
6.3. $a = \overline{xyz4}$, $b = 252$. 6.4. $a = \overline{x6yz}$, $b = 308$.
6.5. $a = \overline{7xyz}$, $b = 156$. 6.6. $a = \overline{x4yz}$, $b = 273$.
6.7. $a = \overline{xy86z}$, $b = 693$. 6.8. $a = \overline{3x5yz}$, $b = 132$.
6.9. $a = \overline{x67yz}$, $b = 264$. 6.10. $a = \overline{42xyz}$, $b = 792$.
6.11. $a = \overline{4x8yz6}$, $b = 504$. 6.12. $a = \overline{x395yz}$, $b = 168$.
6.13. $a = \overline{x5y6z6}$, $b = 252$. 6.14. $a = \overline{xy35z2}$, $b = 231$.
6.15. $a = \overline{xyz444}$, $b = 693$.

7. В кольце $\mathbb{Z}_m$ найдите обратные к элементам a и b.

7.1. $n = 2020$. $a = 7$, $b = 13$.
7.2. $n = 2019$. $a = 17$, $b = 19$.
7.3. $n = 2016$. $a = 23$, $b = 11$.
7.4. $n = 2015$. $a = 17$, $b = 23$.
7.5. $n = 2013$. $a = 13$, $b = 19$.
7.6. $n = 2012$. $a = 7$, $b = 17$.
7.7. $n = 2009$. $a = 17$, $b = 5$.
7.8. $n = 2008$. $a = 19$, $b = 5$.
7.9. $n = 2007$. $a = 5$, $b = 10$.
7.10. $n = 2005$. $a = 11$, $b = 13$.
7.11. $n = 2004$. $a = 7$, $b = 11$.

7.12. $n = 2\,001$. $a = 19$, $b = 25$.
7.13. $n = 2\,000$. $a = 23$, $b = 13$.
7.14. $n = 1\,996$. $a = 29$, $b = 7$.
7.15. $n = 1\,992$. $a = 7$, $b = 23$.

8. Найдите все значения x и y, при которых числа a и b делятся на m.

8.1. $a = \overline{1xy2}$, $b = \overline{x12y}$, $m = 7$.
8.2. $a = \overline{1x4y}$, $b = \overline{3xy2}$, $m = 11$.
8.3. $a = \overline{27xy}$, $b = \overline{3x5y}$, $m = 11$.
8.4. $a = \overline{2xy3}$, $b = \overline{x3y2}$, $m = 13$.
8.5. $a = \overline{81xy}$, $b = \overline{9xy5}$, $m = 17$.
8.6. $a = \overline{9xy4}$, $b = \overline{53xy}$, $m = 17$.
8.7. $a = \overline{xy21}$, $b = \overline{3x5y}$, $m = 17$.
8.8. $a = \overline{x53y}$, $b = \overline{xy57}$, $m = 19$.
8.9. $a = \overline{xy38}$, $b = \overline{4xy9}$, $m = 19$.
8.10. $a = \overline{3x7y}$, $b = \overline{92xy}$, $m = 19$.
8.11. $a = \overline{x56y}$, $b = \overline{5xy6}$, $m = 23$.
8.12. $a = \overline{5xy9}$, $b = \overline{6x7y}$, $m = 23$.
8.13. $a = \overline{7x3y}$, $b = \overline{55xy}$, $m = 23$.
8.14. $a = \overline{3xy2}$, $b = \overline{xy51}$, $m = 23$.
8.15. $a = \overline{7xy5}$, $b = \overline{xy38}$, $m = 23$.

9. Перпендикуляр к оси абцисс пересекает три прямые в точках с целочисленными координатами. Найдите координаты точек пересечения. В ответ запишите координаты с наименьшим натуральным значением

абциссы.

9. 1. $3x - 5y = 4$, $2x + 3y = 10$, $5x - 7y = 6$.
9. 2. $2x + 7y = 9$, $5x - 4y = -1$, $4x + 3y = 3$.
9. 3. $4x - 5y = -3$, $2x - 3y = -6$, $5x + 2y = 7$.
9. 4. $7x - 2y = -3$, $5x - 3y = -6$, $3x + 5y = 4$.
9. 5. $2x + 3y = 8$, $9x - 5y = 12$, $3x + 2y = 4$.
9. 6. $x - 5y = 2$, $x - 8y = 1$, $x - 11y = 3$.
9. 7. $4x - 7y = 9$, $2x + 9y = 15$, $5x - 17y = 12$.
9. 8. $3x + 7y = 6$, $2x - 11y = 4$, $7x + 6y = 5$.
9. 9. $11x + 13y = 5$, $7x + 5y = 1$, $5x + 3y = 7$.
9. 10. $6x + 7y = 2$, $13x - 2y = 3$, $7x - 11y = 2$.
9. 11. $13x + 3y = 5$, $17x + 13y = 7$, $3x + 5y = 7$.
9. 12. $3x - 13y = 7$, $5x + 17y = 3$, $5x - 3y = 11$.
9. 13. $x - 7y = 5$, $3x + 13y = 2$, $7x - 3y = 6$.
9. 14. $5x + 3y = 7$, $-5x + 7y = 3$, $6x - 5y = 11$.
9. 15. $4x - 5y = 11$, $3x + 11y = 7$, $-2x + 7y = 13$.

10. При каких целых k число a делится на m?

10. 1. $a = k^2 - 3k + 23$, $m = 63$.
10. 2. $a = k^2 + 42k + 21$, $m = 105$.
10. 3. $a = k^2 + 7k + 5$, $m = 91$.
10. 4. $a = 9k^2 + 13k + 4$, $m = 85$.
10. 5. $a = 3k^2 - 3k + 15$, $m = 77$.

10.6. $a = 5k^2 + 4k - 9, \quad m = 119.$

10.7. $a = 5k^2 - 3k + 7, \quad m = 117.$

10.8. $a = -k^2 + 5k - 4, \quad m = 143.$

10.9. $a = 2k^2 + 23k - 13, \quad m = 104.$

10.10. $a = 10k^2 - 5k + 12, \quad m = 136.$

10.11. $a = 5k^2 - 13k + 6, \quad m = 162.$

10.12. $a = -3k^2 + 14k + 3, \quad m = 171.$

10.13. $a = 3k^2 - 10k - 6, \quad m = 133.$

10.14. $a = 7k^2 - 6k + 3, \quad m = 147.$

10.15. $a = -7k^2 + k + 16, \quad m = 184.$

Кафедра
ФМО и ИТ

8. Практическое занятие по теме «Порядок числа по данному модулю. Первообразные корни. Индексы по простому модулю»

Пример 1. Найдите $\theta(5 \mod 11)$ и $\theta(5 \mod 10)$.

Доказательство. 1. Поскольку $\varphi(11) = 10$, то $\theta(5 \mod 11)$ делит 10. То есть $\theta(5 \mod 11) \in \{1, 2, 5, 10\}$. При этом

$5^1, 5^2 \not\equiv 1 \pmod{11}, 5^5 \equiv 5^2 \cdot 5^2 \cdot 5 \equiv 3 \cdot 3 \cdot 5 \equiv -10 \equiv 1 \pmod{11}$.

Значит, $\theta(5 \mod 11) = 5$.

2. Числа 5 и 10 не являются взаимно простыми. Поэтому $\theta(5 \mod 10)$ не существует.

Ответ: 5. □

Пример 2. Найдите наименьший первообразный корень по модулю 13.

Доказательство. Первообразные корни будем искать среди чисел $\{1, 2, \ldots, 11, 12\}$. Так как $\theta(1 \mod 13) = 1$, то 1 не является первообразным корнем.

Способ 1. Поскольку $\varphi(13) = 12$, то $\theta(2 \mod 13)$ делит 12. То есть $\theta(2 \mod 13) \in \{1, 2, 3, 4, 6, 12\}$. При этом

$2^1, 2^2, 2^3, 2^4, 2^6 \not\equiv 1 \pmod{11}$. По теореме Эйлера $2^{12} \equiv 1 \pmod{13}$. Значит, $\theta(2 \mod 13) = 12$ и число 2 является первообразным корнем по модулю 13.

Способ 2. Простыми делителями числа $13-1=12$ являются числа 2 и 3.

Так как $2^2 \equiv 4 \pmod{13}$, $2^3 \equiv 8 \pmod{13}$, то число 2 является первообразным корнем по модулю 13.

Ответ: 2. □

Пример 3. Найдите все попарно несравнимые первообразные корни по модулю 11.

Доказательство. Число попарно несравнимых по модулю 11 первообразных корней равно $\varphi(11-1)=\varphi(10)=4$. Найдём сначала наименьший положительный первообразный корень, испытывая числа из приведённой системы наименьших положительных вычетов по модулю 11:

$$2^{\frac{11-1}{2}} \equiv 2^5 \equiv 32 \equiv -1 \not\equiv 1 \pmod{11},$$

$$2^{\frac{11-1}{5}} \equiv 2^2 \equiv 4 \not\equiv 1 \pmod{11},$$

т.е. достаточное условие выполняется и 2 — первообразный корень по модулю 11. Остальные первообразные корни найдём, как наименьшие положительные вычеты степеней 2^k по модулю 11, где $\text{НОД}(k,10)=1$, $1<k<10$.

$$k=3,\ 7,\ 9:\ 2^3 \equiv 8 \pmod{11},$$

$$2^7 \equiv 7 \pmod{11}$$

$$2^9 \equiv 6 \pmod{11}.$$

Ответ: $2, 6, 7, 8$ — попарно несравнимые первообразные корни по модулю 11. □

Пример 4. Постройте таблицы индексов и антииндексов по модулю $p = 11$.

Доказательство. В качестве основания a возьмём наименьший положительный первообразный корень по модулю 11.

Из примера 3. следует, что $a = 2$ — первообразный корень по модулю 11. Последовательно приводим по модулю 11 все степени 2 до $p - 2 = 9$ включительно:

$2^0 \equiv 1 \pmod{11}$ $2^1 \equiv 2 \pmod{11}$ $2^2 \equiv 4 \pmod{11}$
$2^3 \equiv 8 \pmod{11}$ $2^4 \equiv 5 \pmod{11}$ $2^5 \equiv 10 \pmod{11}$
$2^6 \equiv 9 \pmod{11}$ $2^7 \equiv 7 \pmod{11}$ $2^8 \equiv 3 \pmod{11}$
$2^9 \equiv 6 \pmod{11}$

Получим таблицы:

а) таблица индексов

b	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2 b$	0	1	8	2	4	9	7	3	6	5

б) таблица антииндексов

$\mathrm{ind}_2 b$	0	1	2	3	4	5	6	7	8	9
b	1	2	4	8	5	10	9	7	3	6

□

Пример 5. Найдите остаток от деления 300^{304} на 11.

Доказательство. Для нахождения отстатка от деления 300^{304} на 11 мы должны найти целое число x такое, что $300^{304} \equiv x \pmod{11}$ и $0 \leq x < 11$. Заменив число 300 его остатком от деления на 11 и воспользовавшись свойствами индексов, мы получим, что

$$300^{304} \equiv x \pmod{11} \Leftrightarrow 3^{304} \equiv x \pmod{11} \Leftrightarrow$$

$$\operatorname{ind} 3^{304} \equiv \operatorname{ind} x \pmod{10} \Leftrightarrow 304 \operatorname{ind} 3 \equiv \operatorname{ind} x \pmod{10} \Leftrightarrow$$

$$304 \cdot 8 \equiv \operatorname{ind} x \pmod{10} \Leftrightarrow \operatorname{ind} x \equiv 2 \pmod{10} \Leftrightarrow x \equiv 4 \pmod{11}.$$

Таким образом, остаток от деления 300^{304} на 11 равен 4. □

Задачи для самостоятельного решения

1. Найдите порядок числа a по модулю m, т.е. $\theta(a \mod m)$.

1.1. $a = 13$, $m = 27$.
1.2. $a = 12$, $m = 25$.
1.3. $a = 10$, $m = 21$.
1.4. $a = 12$, $m = 17$.
1.5. $a = 11$, $m = 18$.
1.6. $a = 9$, $m = 25$.
1.7. $a = 14$, $m = 15$.
1.8. $a = 15$, $m = 16$.
1.9. $a = 5$, $m = 31$.
1.10. $a = 8$, $m = 23$.
1.11. $a = 7$, $m = 22$.
1.12. $a = 6$, $m = 17$.
1.13. $a = 13$, $m = 27$.
1.14. $a = 8$, $m = 21$.
1.15. $a = 7$, $m = 26$.

2. Найдите наименьший первообразный корень по модулю m.

1.1. $m = 27$. 1.2. $m = 25$. 1.3. $m = 13$.
1.4. $m = 18$. 1.5. $m = 14$. 1.6. $m = 22$.
1.7. $m = 54$. 1.8. $m = 34$. 1.9. $m = 26$.
1.10. $m = 50$. 1.11. $m = 23$. 1.12. $m = 19$.
1.13. $m = 37$. 1.14. $m = 31$. 1.15. $m = 29$.

3. Найдите все попарно несравнимые первообразные корни по модулю m.

1.1. $m = 37$. 1.2. $m = 31$. 1.3. $m = 29$.
1.4. $m = 27$. 1.5. $m = 25$. 1.6. $m = 13$.
1.7. $m = 18$. 1.8. $m = 14$. 1.9. $m = 22$.
1.10. $m = 54$. 1.11. $m = 34$. 1.12. $m = 26$.
1.13. $m = 50$. 1.14. $m = 23$. 1.15. $m = 19$.

4. Постройте таблицы индексов и антииндексов по модулю p.

1.1. $p = 37$. 1.2. $p = 31$. 1.3. $p = 41$.
1.4. $p = 43$. 1.29. $p = 47$. 1.6. $p = 13$.
1.7. $p = 19$. 1.8. $p = 17$. 1.9. $p = 53$.
1.10. $p = 59$. 1.61. $p = 67$. 1.12. $p = 71$.
1.13. $p = 73$. 1.14. $p = 79$. 1.15. $p = 83$.

5. Найдите остаток от деления a на b.

1.1. $a = 100^{300}$, $b = 37$. 1.2. $a = 200^{600}$, $b = 31$.
1.3. $a = 100^{400}$, $b = 41$. 1.4. $a = 200^{700}$, $b = 43$.

1.5. $a = 100^{500}$, $b = 47$.
1.6. $a = 200^{800}$, $b =$
1.7. $a = 300^{900}$, $b = 19$.
1.8. $a = 400^{300}$, $b =$
1.9. $a = 300^{100}$, $b = 53$.
1.10. $a = 400^{400}$, $b =$
1.11. $a = 300^{200}$, $b = 67$.
1.12. $a = 400^{500}$, $b =$
1.13. $a = 500^{600}$, $b = 73$.
1.14. $a = 500^{800}$, $b =$
1.15. $a = 500^{700}$, $b = 83$.

13.
17.
= 59.
= 71.
= 79.

9. Практическое занятие по теме «Двучленные сравнения. Квадратичные вычеты. Показательные двучленные сравнения. Символ Лежандра»

Пример 1. Решите сравнение $7x \equiv 9 \pmod{11}$.

Доказательство. Пользуясь свойствами индексов, мы получим, что

$$7x \equiv 9 \pmod{11} \Leftrightarrow \operatorname{ind} 7x \equiv \operatorname{ind} 9 \pmod{10} \Leftrightarrow$$
$$\operatorname{ind} 7 + \operatorname{ind} x \equiv \operatorname{ind} 9 \pmod{10} \Leftrightarrow 7 + \operatorname{ind} x \equiv 6 \pmod{10} \Leftrightarrow$$
$$\operatorname{ind} x \equiv 9 \pmod{10} \Leftrightarrow x \equiv 6 \pmod{11}.$$

Таким образом, сравнение $7x \equiv 9 \pmod{11}$ имеет единственное решение $x \equiv 6 \pmod{11}$. В кольце $\mathbb{Z}_{11}$ этому решению соответствует класс вычетов $x = \overline{6}$.

Ответ. Сравнение имеет единственное решение: $x = \overline{6}$.

Пример 2. Решите сравнение $7x^4 \equiv 10 \pmod{11}$.

Доказательство. Индексируем обе части сравнения по модулю 11.

$$\operatorname{ind} 7 + 4\operatorname{ind} x \equiv \operatorname{ind} 10 \pmod{10}.$$

Из таблицы индексов для простого числа 11 находим, что $\operatorname{ind} 7 = 7$, $\operatorname{ind} 10 = 5$. Тогда получим сравнение первой степени относительно $\operatorname{ind} x$, а именно, $4\operatorname{ind} x \equiv 8 \pmod{10}$.

Последнее сравнение имеет два решения $\operatorname{ind} x \equiv 2;\ 7 \pmod{10}$.

Теперь из таблицы антииндексов для простого числа 11 находим, что $x \equiv 4; 7 \pmod{11}$ — два решения данного сравнения.

Ответ. Сравнение имеет два решения: $x_1 = \overline{4}$, $x_2 = \overline{7}$. □

Пример 3. Решите сравнение $9^x \equiv 5 \pmod{11}$.

Доказательство. Индексируем обе части сравнения по модулю 11.

$$x\operatorname{ind} 9 \equiv \operatorname{ind} 5 \pmod{10}.$$

Из таблицы индексов для простого числа 11, см. пример 3.9.4 находим, что $\operatorname{ind} 9 = 6,\ \operatorname{ind} 5 = 4$. Тогда получим сравнение первой степени относительно x, а именно, $6x \equiv 4 \pmod{10}$.

Последнее сравнение имеет два решения $x \equiv 4;\ 9 \pmod{10}$.

Ответ. Сравнение имеет два решения: $x_1 \equiv 4 \pmod{10}$, $x_2 \equiv 9 \pmod{10}$. □

Пример 4. Вычислите символ Лежандра $\left(\dfrac{-125}{47}\right)$.

Доказательство.

$$\left(\frac{-125}{47}\right) = \left(\frac{-5 \cdot 25}{47}\right) = \left(\frac{-5}{47}\right) \cdot \left(\frac{5^2}{47}\right) =$$

$$\left(\frac{-5}{47}\right) = \left(\frac{-1}{47}\right) \cdot \left(\frac{5}{47}\right) = (-1) \cdot \left(\frac{5}{47}\right) =$$

$$(-1)\cdot\left(\frac{47}{5}\right)=(-1)\cdot\left(\frac{2}{5}\right)=(-1)\cdot(-1)=1.$$

Ответ. 1. □

Пример 5. Установите количество решений сравнения

$$x^2\equiv 7 \pmod{19}.$$

Доказательство. Пользуясь критерием Эйлера, исследуем, с чем сравнимо $7^{\frac{19-1}{2}}$ по модулю 19. Очевидно, что $7^{\frac{19-1}{2}}=7^9=(7\cdot 7^2)^3\equiv(7\cdot 11)^3\equiv 1^3=1 \pmod{19}$. Значит, $\left(\frac{7}{19}\right)=1$. Поэтому сравнение разрешимо и имеет два решения.

Ответ. Сравнение имеет два решения. □

Задачи для самостоятельного решения

1. Решите сравнения.

1.1. $15x\equiv 20 \pmod{23}$, $16x\equiv 28 \pmod{36}$.

1.2. $15x\equiv 9 \pmod{11}$, $42x\equiv 12 \pmod{90}$.

1.3. $29x\equiv 15 \pmod{19}$, $55x\equiv 35 \pmod{75}$.

1.4. $6x\equiv 22 \pmod{13}$, $20x\equiv 12 \pmod{72}$.

1.5. $14x \equiv -9 \pmod{17}$, $25x \equiv 45 \pmod{60}$.
1.6. $9x \equiv -8 \pmod{23}$, $21x \equiv 7 \pmod{49}$.
1.7. $10x \equiv 15 \pmod{17}$, $10x \equiv 25 \pmod{35}$.
1.8. $18x \equiv 12 \pmod{19}$, $10x \equiv 12 \pmod{14}$.
1.9. $21x \equiv 14 \pmod{23}$, $26x \equiv 2 \pmod{30}$.
1.10. $24x \equiv 16 \pmod{25}$, $15x \equiv 21 \pmod{24}$.
1.11. $15x \equiv 10 \pmod{19}$, $10x \equiv 14 \pmod{22}$.
1.12. $14x \equiv 35 \pmod{37}$, $15x \equiv 25 \pmod{35}$.
1.13. $22x \equiv 33 \pmod{39}$, $12x \equiv 21 \pmod{27}$.
1.14. $21x \equiv 35 \pmod{37}$, $10x \equiv -4 \pmod{22}$.
1.15. $26x \equiv 39 \pmod{41}$, $14x \equiv 12 \pmod{30}$.

2. Решите двучленные сравнения с помощью индексов.

2.1. $25x^7 \equiv -7 \pmod{31}$. 2.2. $8x^9 \equiv -17 \pmod{41}$.
2.3. $7x^{13} \equiv -23 \pmod{47}$. 2.4. $9x^{11} \equiv -1 \pmod{43}$.
2.5. $19x^5 \equiv -13 \pmod{53}$. 2.6. $17x^5 \equiv -3 \pmod{37}$.
2.7. $5x^{11} \equiv -19 \pmod{29}$. 2.8. $15x^9 \equiv -29 \pmod{47}$.
2.9. $6x^7 \equiv -19 \pmod{23}$. 2.10. $13x^8 \equiv -36 \pmod{61}$.
2.11. $3x^8 \equiv 5 \pmod{13}$. 2.12. $40x^{10} \equiv 3 \pmod{17}$.
2.13. $2x^{13} \equiv 5 \pmod{19}$. 2.14. $3x^{12} \equiv 31 \pmod{41}$.
2.15. $12x^{18} \equiv 54 \pmod{13}$.

3. Решите показательные двучленные сравнения с помощью индексов.

3.1. $3^x \equiv 7 \pmod{11}$. 3.2. $6^x \equiv -3 \pmod{13}$.
3.3. $15^{2x} \equiv -3 \pmod{61}$. 3.4. $8^x \equiv -3 \pmod{47}$.

3.5. $32^x \equiv 15 \pmod{37}$.
3.6. $25^{5x} \equiv 47 \pmod{61}$.
3.7. $8 \cdot 7^x \equiv -4 \pmod{83}$.
3.8. $13 \cdot 7^{5x} \equiv -1 \pmod{67}$.
3.9. $22 \cdot 12^{13x} \equiv -6 \pmod{31}$.
3.10. $23^x \equiv 37 \pmod{41}$.
3.11. $7 \cdot 5^x \equiv -1 \pmod{73}$.
3.12. $11 \cdot 5^{3x} \equiv -70 \pmod{79}$.
3.13. $17 \cdot 13^{3x} \equiv -27 \pmod{29}$.
3.14. $13^x \equiv 25 \pmod{43}$.
3.15. $19^{7x} \equiv 15 \pmod{59}$.

4. Вычислите символ Лежандра.

4.1. $\left(\frac{102}{17}\right)$.
4.2. $\left(\frac{-88}{23}\right)$.
4.3. $\left(\frac{125}{47}\right)$.
4.4. $\left(\frac{204}{311}\right)$.
4.5. $\left(\frac{219}{383}\right)$.
4.6. $\left(\frac{63}{131}\right)$.
4.7. $\left(\frac{47}{73}\right)$.
4.8. $\left(\frac{241}{593}\right)$.
4.9. $\left(\frac{251}{577}\right)$.
4.10. $\left(\frac{35}{97}\right)$.
4.11. $\left(\frac{29}{383}\right)$.
4.12. $\left(\frac{257}{571}\right)$.
4.13. $\left(\frac{342}{677}\right)$.
4.14. $\left(\frac{401}{757}\right)$.
4.15. $\left(\frac{215}{761}\right)$.

5. Установите количество решений сравнения.

5.1. $x^2 \equiv 200 \pmod{79}$.
5.2. $x^2 \equiv 56 \pmod{87}$.
5.3. $x^2 \equiv 15 \pmod{209}$.
5.4. $x^2 \equiv -27 \pmod{91}$.

5.5. $x^2 \equiv 215 \pmod{47}$.
5.6. $x^2 \equiv 200 \pmod{61}$.
5.7. $x^2 \equiv 69 \pmod{307}$.
5.8. $x^2 \equiv 5 \pmod{19}$.
5.9. $x^2 \equiv 5 \pmod{29}$.
5.10. $x^2 \equiv 2 \pmod{97}$.
5.11. $x^2 \equiv 241 \pmod{587}$.
5.12. $x^2 \equiv 151 \pmod{587}$.
5.13. $x^2 \equiv 300 \pmod{151}$.
5.14. $x^2 \equiv -53 \pmod{253}$.
5.15. $x^2 \equiv 304 \pmod{299}$.

Итоговый тест

К итоговому тесту можно перейти по следующей ссылке Тест.

Задача 1. Решить сравнение $ax = b \pmod{m}$.

	a	b	m
1.	251,	28,	1053
2.	394,	23,	1619
3.	173,	26,	1071
4.	194,	28,	1185
5.	71,	22,	510
6.	406,	11,	2899
7.	59,	30,	253
8.	82,	27,	339
9.	447,	23,	1837
10.	222,	17,	1375
11.	305,	39,	1863
12.	110,	18,	791
13.	123,	12,	874
14.	265,	29,	1097
15.	94,	9,	593
15.	127,	14,	779
17.	38,	36,	277
18.	251,	6,	1806
19.	394,	27,	2801
20.	203,	28,	877
21.	292,	35,	1209
22.	117,	17,	739
23.	210,	40,	1289
24.	59,	26,	430
25.	82,	33,	585
26.	447,	32,	3178
27.	231,	31,	949
28.	82,	13,	507
29.	463,	30,	2843
30.	128,	34,	937
31.	265,	35,	1892
32.	94,	28,	875
33.	253,	30,	1061
34.	284,	7,	1167
35.	131,	10,	811
36.	142,	17,	867
37.	203,	21,	1486
38.	292,	27,	2085
39.	45,	21,	193

Задача 2. Решить сравнение $ax =$

	a	b	m
1.	52,	34,	847
2.	81,	4,	1483
3.	294,	21,	1269
4.	544,	8,	3436
5.	284,	4,	2324
6.	356,	41,	1492
7.	68,	4,	973
8.	94,	21,	1533
9.	117,	37,	2143
10.	120,	20,	502
11.	328,	12,	2028
12.	393,	30,	3219
13.	516,	25,	2164
14.	573,	30,	4695
15.	268,	5,	1108
16.	60,	24,	851
17.	82,	39,	1327
18.	131,	19,	2383
19.	640,	12,	2684
20.	444,	12,	2750
21.	291,	18,	2367
22.	492,	33,	2036
23.	110,	37,	1561
24.	152,	35,	2461
25.	191,	6,	3475
26.	328,	32,	1356

b (mod **m**).

	a	b	m
27.	97,	4,	1759
28.	608,	12,	2516
29.	420,	16,	2578
30.	1060,	32,	8628
31.	93,	7,	678
32.	82,	34,	1159
33.	112,	6,	1807
34.	181,	4,	3283
35.	666,	6,	2757
36.	616,	8,	3782
37.	135,	7,	579
38.	220,	41,	1608

Задача 3. Решить систему сравнений

$$a_1x \equiv b_1 \pmod{m_1}$$
$$a_2x \equiv b_2 \pmod{m_2}$$
$$a_3x \equiv b_3 \pmod{m_3}$$

с коэффициентами $[a_1, b_1, m_1]; [a_2, b_2, m_2]; [a_3, b_3, m_3]$.

1. [5, 3, 4], [6, 2, 5], [6, 13, 19]
2. [5, 1, 4], [8, 3, 7], [4, 13, 17]
3. [5, 3, 4], [8, 10, 11], [6, 9, 13]
4. [5, 3, 4], [12, 10, 11], [4, 12, 19]
5. [5, 5, 6], [12, 1, 5], [6, 9, 17]
6. [7, 1, 6], [6, 4, 7], [4, 4, 13]
7. [5, 1, 4], [6, 6, 7], [4, 3, 13]
8. [5, 1, 4], [6, 5, 7], [6, 15, 19]
9. [5, 1, 4], [8, 9, 11], [4, 6, 17]
10. [5, 1, 6], [8, 4, 5], [6, 10, 13]
11. [5, 5, 6], [12, 2, 5], [4, 4, 19]

Задача 4. Решить в целых неотрицательных числах уравнение $ax + by = c$.

a	b	c
1. 14,	47,	1905
2. 18,	41,	2283
3. 24,	37,	2464
4. 28,	31,	2615
5. 35,	29,	3438
6. 42,	23,	2639
7. 20,	37,	2160
8. 25,	31,	2469
9. 30,	29,	2458
10. 36,	23,	1817
11. 45,	19,	2862
12. 12,	17,	442
13. 27,	29,	2419
14. 32,	23,	2008
15. 40,	19,	2802
16. 48,	17,	2265
17. 14,	13,	418
18. 18,	11,	519

Задача 5. С помощью таблицы индексов решить сравнение $ax \equiv b \pmod{m}$.

	a	b	m
1.	30,	8,	73
2.	32,	5,	59
3.	13,	37,	67
4.	30,	22,	31
5.	16,	10,	17
6.	7,	1,	13
7.	19,	1,	47
8.	36,	11,	97
9.	18,	19,	71
10.	2,	3,	17
11.	1,	7,	13
12.	3,	9,	47
13.	5,	25,	53
14.	25,	16,	53
15.	57,	74,	97
16.	23,	4,	29
17.	4,	8,	13
18.	4,	2,	17
19.	13,	6,	59
20.	11,	23,	29
21.	13,	36,	47
22.	32,	10,	59
23.	3,	18,	71

Задача 6. С помощью таблицы индексов решить сравнение $ax^k \equiv b \pmod{m}$.

	a	k	b	m
1.	30,	197,	52,	89
2.	21,	173,	25,	43
3.	39,	197,	71,	79
4.	64,	163,	66,	97
5.	60,	177,	33,	89
6.	78,	157,	91,	97
7.	38,	179,	2,	79
8.	45,	167,	27,	53
9.	9,	191,	14,	19
10.	7,	199,	16,	19
11.	12,	151,	6,	13
12.	8,	127,	10,	41
13.	5,	117,	20,	47
14.	25,	159,	8,	47
15.	17,	137,	40,	43

Задача 7. С помощью таблицы индексов решить сравнение $a \cdot b^x \equiv c \pmod{m}$.

	a	b	c	m
1.	30	83	4	97
2.	32	50	16	59
3.	19	34	35	43
4.	15	79	12	83
5.	75	15	62	83
6.	2	17	20	23
7.	30	22	18	31
8.	12	45	20	73
9.	18	29	16	43
10.	57	33	68	71
11.	9	2	3	19
12.	7	7	9	11
13.	6	11	41	67
14.	73	14	19	97
15.	59	31	34	61
16.	21	7	38	41
17.	10	11	7	13
18.	13	80	11	83
19.	3	6	8	13
20.	76	56	49	83
21.	13	28	12	43
22.	48	26	16	53
23.	38	53	13	83

ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ПО ТЕМЕ «АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ»

Кафедра ФМО и ИТ

Вариант 1

1. С помощью числа 9 проверить результат арифметических действий 115403365:23845=48417.
2. Найти длину периода и количество цифр между запятой и перио дом десятичной дроби, в которую обращается обыкновенная несокра тимая дробь со знаменателем 860.
3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 53.
4. Используя таблицы индексов, найти остаток от деления числа 19^{32} на число 67.
5. Используя соответствующий признак делимости, проверить дели мость чисел 90585 и 254925 на число 165.
6. С помощью таблиц индексов найти показатель, которому принадле жит число 23 по модулю 53.
7. С помощью таблиц индексов решить сравнение $5x^3 \equiv 38 \pmod{47}$.
8. Найти все первообразные корни по модулю 71.

Вариант 2

1. С помощью числа 9 проверить результат арифметических действий

$$421767:3429=123.$$

2. Найти длину периода и количество цифр между запятой и перио дом десятичной дроби, в которую обращается обыкновенная несократи мая дробь со знаменателем 850.

3. Используя понятие числа, принадлежащего показателю, найти дли ну периода при обращении в десятичные дроби обыкновенных несо кратимых дробей со знаменателем 71.

4. Используя таблицы индексов, найти остаток от деления числа 11^{37} на число 61.

5. Используя соответствующий признак делимости, проверить дели мость чисел 111888, 121878 и 145854 на число 111.

6. С помощью таблиц индексов найти показатель, которому принадле жит число 15 по модулю 47.

7. С помощью таблиц индексов решить сравнение $2x^4 \equiv 33 (\mathrm{mod}\ 43)$.

8. Найти наименьший первообразный корень по модулю 67.

Вариант 3

1. С помощью числа 9 проверить результат арифметических действий

$$1042 \cdot 1011 = 1053462.$$

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 620.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 89.

4. Используя таблицы индексов, найти остаток от деления числа 7^{23} на число 59.

5. Используя соответствующий признак делимости, проверить делимость чисел 121878, 141858 и 145854 на число 37.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 19 по модулю 43.

7. С помощью таблиц индексов решить сравнение $7x^3 \equiv 14 \pmod{41}$.

8. Найти наименьший первообразный корень по модулю 61.

Вариант 4

1. С помощью числа 9 проверить результат арифметических действий
$$4371 \cdot 1243 = 5433153.$$
2. Найти длину периода и количество цифр между запятой и перио дом десятичной дроби, в которую обращается обыкновенная несокра тимая дробь со знаменателем 208.
3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 83.
4. Используя таблицы индексов найти остаток от деления числа 17^{19} на число 53.
5. Используя соответствующий признак делимости, проверить дели мость чисел 11934, 52434 и 111888 на число 54.
6. С помощью таблиц индексов найти показатель, которому принадле жит число 17 по модулю 41.
7. С помощью таблиц индексов решить сравнение $3x^5 \equiv 16 \pmod{31}$.
8. Найти наименьший первообразный корень по модулю 59.

Вариант 5

1. С помощью числа 9 проверить результат арифметических действий

$$42932-18265=24667.$$

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 210.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 97.

4. Используя таблицы индексов, найти остаток от деления числа 31^{18} на

5. Используя соответствующий признак делимости, проверить делимость чисел 52434, 79974 и 111888 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 10 по модулю 37.

7. С помощью таблиц индексов решить сравнение $2x^6 \equiv 5 (\mathrm{mod}\ 31)$.

8. Найти наименьший первообразный корень по модулю 83.

Вариант 6

1. С помощью числа 9 проверить результат арифметических действий 37918-13207=24711.
2. Найти длину периода и количество цифр между запятой и перио дом десятичной дроби, в которую обращается обыкновенная несокра тимая дробь со знаменателем 760.
3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 59.
4. Используя таблицы индексов, найти остаток от деления числа 29^{17} на число 41.
5. Используя соответствующий признак делимости, проверить дели мость чисел 3038035 и 3539635 на число 65.
6. С помощью таблиц индексов найти показатель, которому принадле жит число 8 по модулю 31.
7. С помощью таблиц индексов решить сравнение $23x^3 \equiv 58 \pmod{97}$.
8. Найти наименьший первообразный корень по модулю 79.

Вариант 7

1. С помощью числа 9 проверить результат арифметических действий

$$115403365:23845=48417.$$

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 385.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократи мых дробей со знаменателем 47.

4. Используя таблицы индексов, найти остаток от деления числа 17^{19} на число 53.

5. Используя соответствующий признак делимости, проверить делимость чисел 52434, 79974 и 111888 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 8 по модулю 31.

7. С помощью таблиц индексов решить сравнение $3x^5\equiv 18 (\mathrm{mod}\ 71)$.

8. Найти наименьший первообразный корень по модулю 73.

Вариант 8

1. С помощью числа 9 проверить результат арифметических действий

$$421767:3429=123.$$

2. Найти длину периода и количество цифр между запятой и период десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 410.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 67.

4. Используя таблицы индексов, найти остаток от деления числа 19^{19} на число 97.

5. Используя соответствующий признак делимости, проверить делимость чисел 86670, 79974 и 333777 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 16 по модулю 53.

7. С помощью таблиц индексов решить сравнение $3^{x^2} \equiv 25 (\mathrm{mod}\ 31)$.

8. Найти наименьший первообразный корень по модулю 89.

Вариант 9

1. С помощью числа 11 проверить результат арифметических действий

$$864368582:77=11225566.$$

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 510.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 61.

4. Используя таблицы индексов, найти остаток от деления числа 27^{29} на число 89.

5. Используя соответствующий признак делимости, проверить делимость чисел 52434, 79974 и 111888 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 12 по модулю 59.

7. С помощью таблиц индексов решить сравнение $26x^2\equiv 67 (\mathrm{mod}\ 73)$.

8. Найти наименьший первообразный корень по модулю 79.

Кафедра ФМО и ИТ

Вариант 10

1. С помощью числа 9 проверить результат арифметических действий
$$13250100:4569=2800.$$
2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 760.
3. Используя понятие числа, принадлежащего показателю, найти дли ну периода при обращении в десятичные дроби обыкновенных несокра тимых дро бей со знаменателем 71.
4. Используя таблицы индексов, найти остаток от деления числа 25^{31} на число 83.
5. Используя соответствующий признак делимости, проверить дели мость чисел 3038035 и 3539635 на число 65.
6. С помощью таблиц индексов найти показатель, которому принадлежит число 14 по модулю 59.
7. С помощью таблиц индексов решить сравнение $13x^{11}\equiv 8(\mathrm{mod}\ 61)$.
8. Найти наименьший первообразный корень по модулю 53.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ ПО ТЕМЕ «РЕШЕНИЕ СРАВНЕНИЙ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ»

Вариант 1

1. Решить сравнения:
   a) методом Эйлера $5x \equiv 2(\mathrm{mod}8)$;
   b) методом подходящих дробей $13x \equiv 19(\mathrm{mod}215)$.
2. Решить неопределенное уравнение $73x+85y=-7$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 7(\mathrm{mod}11), \\ 6x \equiv 3(\mathrm{mod}15), \\ x \equiv 2(\mathrm{mod}19). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже p, где p - модуль

$$x^{14} - x^{12} + 3x^5 - 6x^2 + x + 1 \equiv 0(\mathrm{mod}11).$$

5. С помощью символа Лежандра установить, имеет ли решение срав нение

$$x^2 \equiv 42(\mathrm{mod}251).$$

Вариант 2

1. Решить сравнения:
   a) методом Эйлера $7x \equiv 2(\mathrm{mod}13)$;
   b) методом подходящих дробей $41x \equiv 32(\mathrm{mod}101)$.
2. Решить неопределенное уравнение $253x\text{-}449y=3$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 3(\mathrm{mod}5), \\ 3x \equiv 5(\mathrm{mod}11), \\ 3x \equiv 12(\mathrm{mod}15). \end{cases}$$

4. Решить сравнение

$$x^{14} - 4x^{13} - x + 6 \equiv 0(\mathrm{mod}13).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 30(\mathrm{mod}269).$$

Вариант 3

1. Решить сравнения:
   a) методом Эйлера $5x \equiv 4(\mathrm{mod}7)$;
   b) методом подходящих дробей $25x \equiv 17(\mathrm{mod}151)$.
2. Решить неопределенное уравнение $172x+152y=-300$.
3. Решить систему сравнений

$$\begin{cases} 7x \equiv 9(\mathrm{mod}12), \\ x \equiv 6(\mathrm{mod}15), \\ 3x \equiv 5(\mathrm{mod}127). \end{cases}$$

4. Разложить на множители многочлен $x^4 + 6x^3 - 3x^2 + x + 2$ по модулю *13*.
5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 26(\mathrm{mod}241).$$

Вариант 4

1. Решить сравнения:
   a) методом Эйлера $3x \equiv 5(\mathrm{mod}11)$;
   b) методом подходящих дробей $23x \equiv 14(\mathrm{mod}109)$.
2. Решить неопределенное уравнение $24x\text{-}56y=72$.
3. Решить систему сравнений

$$\begin{cases} 7x \equiv 3(\mathrm{mod}9), \\ 3x \equiv 9(\mathrm{mod}12), \\ x \equiv 11(\mathrm{mod}13). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже p, где p - модуль

$$x^{10} + 3x^5 - 4x^3 + x^2 - 3 \equiv 0(\mathrm{mod}7).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 20(\mathrm{mod}101).$$

Вариант 5

1. Решить сравнения:
   a) методом Эйлера $3x \equiv 4(\mathrm{mod}\,7)$;
   b) методом подходящих дробей $11x \equiv 26(\mathrm{mod}\,107)$.
2. Решить неопределенное уравнение $162x+104y=-10$.
3. Решить систему сравнений

$$\begin{cases} 9x \equiv 3(\mathrm{mod}\,14), \\ 4x \equiv 20(\mathrm{mod}\,18), \\ x \equiv 5(\mathrm{mod}\,11). \end{cases}$$

4. Решить сравнение

$$x^{12} + 2x^{11} - 2x - 1 \equiv 0(\mathrm{mod}\,11).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 65(\mathrm{mod}\,193).$$

Вариант 6

1. Решить сравнения:
   a) методом Эйлера $2x \equiv 9 (\mathrm{mod} 15)$;
   b) методом подходящих дробей $45x \equiv 8 (\mathrm{mod} 113)$.
2. Решить неопределенное уравнение $39x\text{-}45y=21$.
3. Решить систему сравнений

$$\begin{cases} 5x \equiv 3 (\mathrm{mod} 17), \\ x \equiv 1 (\mathrm{mod} 12), \\ 8x \equiv 2 (\mathrm{mod} 6). \end{cases}$$

4. Разложить на множители многочлен $x^4 - 4x^3 + 4x - 1$ по модулю 7.
5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 33 (\mathrm{mod} 179).$$

Вариант 7

1. Решить сравнения:
   a) методом Эйлера $4x \equiv 7(\mathrm{mod}9)$;
   b) методом подходящих дробей $19x \equiv 42(\mathrm{mod}163)$.
2. Решить неопределенное уравнение $107x+84y=1$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 7(\mathrm{mod}113), \\ 7x \equiv 8(\mathrm{mod}9), \\ 3x \equiv 4(\mathrm{mod}19). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже p, где p - модуль

$$x^9 - 3x^4 + 2x^3 - x + 3 \equiv 0(\mathrm{mod}7).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 28(\mathrm{mod}251).$$

Вариант 8

1. Решить сравнения:
   a) методом Эйлера $7x \equiv 2(\mathrm{mod}11)$;
   b) методом подходящих дробей $12x \equiv 31(\mathrm{mod}137)$.
2. Решить неопределенное уравнение $37x\text{-}256y=1$.
3. Решить систему сравнений

$$\begin{cases} x \equiv 2(\mathrm{mod}103), \\ 3x \equiv 9(\mathrm{mod}21), \\ 2x \equiv 6(\mathrm{mod}12). \end{cases}$$

4. Решить сравнение $x^8 - 2x^7 + 3x^6 + x^5 - 2x^2 - x - 3 \equiv 0(\mathrm{mod}5)$.
5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 12(\mathrm{mod}269).$$

Вариант 9

1. Решить сравнения:
   a) методом Эйлера $4x \equiv 5(\mathrm{mod}13)$;
   b) методом подходящих дробей $8x \equiv 17(\mathrm{mod}127)$.
2. Решить неопределенное уравнение $571x+359y=-10$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 3(\mathrm{mod}7), \\ 3x \equiv 5(\mathrm{mod}131), \\ 2x \equiv 10(\mathrm{mod}14). \end{cases}$$

4. Разложить на множители многочлен $x^4 - 3x^3 - x + 4$ по модулю 7.
5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 48(\mathrm{mod}193).$$

Вариант 10

1. Решить сравнения:
   a) методом Эйлера $5x \equiv 12 (\mathrm{mod} 13)$;
   b) методом подходящих дробей $6x \equiv 31 (\mathrm{mod} 149)$.
2. Решить неопределенное уравнение $60x - 91y = 2$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 3 (\mathrm{mod} 5), \\ 24x \equiv 14 (\mathrm{mod} 26), \\ 3x \equiv 5 (\mathrm{mod} 11). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже p, где p - модуль

$$x^8 - 2x^7 + 3x^6 + x^5 - 2x^2 - x - 3 \equiv 0 (\mathrm{mod} 5).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 56 (\mathrm{mod} 241).$$

Иога́нн Карл Фри́дрих Га́усс
(нем. *Johann Carl Friedrich Gauß*)
(1777–1855)

Немецкий математик, механик, физик, астроном и геодезист. Считается од ним из величайших математиков всех времен, «королем математиков».
Отличительными чертами его исследо ваний являются необычайная широта проблематики, глубокая органическая связь между теоретической и приклад ной математикой.
Все опубликованные им труды содер жат значительные результаты. Он публиковал только тогда, когда считал свою работу над темой завершенной.
Работы Гаусса оказали большое влияние на развитие высшей ал гебры, теории чисел, дифференциальной геометрии, теории при тяжения, классической теории электричества и магнетизма.
Внес фундаментальный вклад также в астрономию и геодезию; разработал вычислительные методы, приведшие к созданию но вого научного направления – высшей геодезии.
В 1832 г. создал абсолютную систему мер (СГС), введя три основные единицы: единицу длины – сантиметр, единицу массы – грамм, единицу времени – секунду. Гаусс на 10 лет раньше Лоба чевского пришел к идее неевклидовой геометрии, но не стал зани маться этой темой глубже. Узнав о работе Лобачевского, начал в 62 года изучать русский язык, чтобы прочитать эти работы в оригинале.

Евкли́д
(др.-греч. Εὐκλείδης)
(III в. до н. э.)

Древнегреческий математик, автор первого из дошедших до нас теорети ческих трактатов по математике. Трактат Евклида «Начала» состоит из тринадцати книг, Евклид включил в него многое из того, что было создано его предшественниками, обработав этот материал и сведя его воедино. «Начала» Евклида оставались основ ным учебником по математике в тече ние более чем двух тысячелетий.

Рассуждение Евклида укладывается в одну фразу: если бы имелось лишь конечное число простых чисел, то можно было бы их перемножить и, прибавив единицу, получить число, которое не делится ни на одно простое, что невозможно.

Леона́рд Э́йлер
(нем. *Leonhard Euler*)
(1707–1783)

Швейцарский, немецкий и российский математик и механик, внесший фундаментальный вклад в развитие этих наук, а также физики, астрономии и ряда прикладных наук. В математике Эйлер впервые увязал анализ, алгебру, геометрию, тригонометрию, теорию чисел и другие дисциплины в единую систему, добавив при этом немало собственных открытий. Был виртуозным алгоритми-стом и всегда старался довести свои открытия до уровня конкретных вычислительных методов.

Автор более чем 850 работ (включая два десятка фундаментальных монографий). В его работах использовались продуманная терминология и математическая символика, в большой мере сохранившиеся до наших дней. Почти полжизни провел в России, куда приехал в возрасте 20 лет по приглашению Петра I в период организации Российской академии наук. Уже через год пребывания в России он хорошо знал русский язык и часть своих сочинений (особенно учебники) публиковал на русском.

По отзывам современников, Эйлер был жизнерадостен, общителен, практически ни с кем не ссорился, охотно помогал коллегам и молодежи.

Пьер де Ферма́
(фр. *Pierre de Fermat*)
(1601–1665)

Французский математик, один из создателей аналитической геометрии, математического анализа, теории вероятностей и теории чисел. По профессии юрист, с 1631 г. – советник парламента в Тулузе. Блестящий полиглот.

Наиболее известен формулировкой ***Великой теоремы Ферма****: для любого натурального числа $n > 2$ уравнение $x^n + y^n = z^n$ не имеет натуральных решений x, y, z.*

Ферма сформулировал эту теорему в 1637 г. на полях «Арифметики» Диофанта с припиской, что найденное им удивительное доказательство этого утверждения слишком длинно, чтобы привести его на полях книги. Строгое доказательство Великой теоремы Ферма было получено американским математиком Эндрю Уайл-сом и опубликовано в журнале «Annals of Mathematics» в 1995 г., занимая 129 с.

Цинь Цзю-шао
(кит. 秦九韶)
(XIII в.)

Китайский математик и астроном, автор трактата «Сунь Цзы Суань Цзин» («Математическое наставление Сунь Цзы»). Считается одним из великих алгебраистов 18-19 в.в. Занимаясь разработкой календаря, он открыл утверждение, известное как китайская теорема об остатках.

孫子算經卷上
唐朝議大夫行太史令上輕車都尉臣李淳風等奉勅注釋
度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Адриен Мари Лежа́ндр
(фр. *Adrien-Marie Legendre*)
(1752–1833)

Французский математик.
Его имя внесено в список 72 величайших ученых Франции, помещенный на первом этаже Эйфелевой башни.
В годы французской революции активно участвовал в Комиссии по введению метрической системы.
Двухтомный труд Лежандра «Теория чисел» (1798) был самым полным изложением теории чисел в то время. Книга выдержала три переиздания еще при жизни автора.

Карл Гу́став Я́коб Яко́би
(нем. *Carl Gustav Jacob Jacobi*)
(1804–1851)

Немецкий математик и механик. Внес огромный вклад в комплексный анализ, ли нейную алгебру, динамику и другие разде лы математики и механики.
Карл Якоби имел незаурядный преподава тельский талант. По общему мнению, как педагогу ему не было равных, и рас цвет немецкой математической школы в конце XIX в. – также и его заслуга. Поми мо других качеств, Якоби отличало ис ключительное трудолюбие и полное от сутствие завистливости.
Якоби первый применил в теории чисел эллиптические функции; именно на этом пути спустя полтора века была доказана Вели кая теорема Ферма.

Джон Вильсон
(англ. John Wilson)
(1847–1896))

Жил и творил в Великобритании во второй половине 18 века, совмещая занятия математикой с работой судьей по общим искам. Главный вклад Вильсона в математику - это теорема, названная в его честь, которая является одновременно необходимым и достаточным условиям для проверки числа на простоту. Но он никак не мог доказать свою гипотезу. В итоге он заявил, что для доказательства потребуется ввести новую нотацию теории чисел.

Первое доказательство нашел Лагранж. Гаусс весьма едко отозвался о попытках Вильсона доказать гипотезу: «Вильсону требовалась не новая нотация, а некоторое представление, о чем идет речь».

Однако же, тест простоты с помощью этой теоремы не выгоден с алгоритмической точки зрения, ведь факториалы больших чисел вычислять очень затратно. Если все простые числа подчиняются теореме Вильсона, то сами простые числа Вильсона - более витиеватому условию.

Блез Паскаль
(фр. Blaise Pascal)
(1623–1662)

Родился в семье высокообразованного юриста, занимавшегося математикой и воспитывавшего своих детей под влиянием педагогических идей М. Монтеня, рано проявил выдающиеся математические способности, войдя в историю науки как классический пример отроческой гениальности. Первый математический трактат Паскаля «Опыт теории конических сечений» (1639, издан 1640) являлся развитием трудов Ж. Дезарга, содержал одну из основных теорем проективной геометрии – «Паскаля» теорему. В 1641 (по другим сведениям, в 1642) Паскаль сконструировал суммирующую машину. К 1654 закончил ряд работ по арифметике, теории чисел, алгебре и теории вероятностей (опубликованных в 1665). Паскаль нашел общий алгоритм для нахождения признаков делимости любого целого числа на любое другое целое число (трактат «О характере делимости чисел»), способ вычисления биномиальных коэффициентов

Мартин Хэллман
(англ. Martin Hellman)
(1945)

Американский криптограф. Получил известность благодаря разработке первой асимметричной криптосистемы в соавторстве с Уитфилдом Диффи и Ральфом Мерклем. Один из активных сторонников либерализации в сфере криптографии. Хеллман долгое время являлся участником конференции компьютерной конфиденциальности, работает над анализом рисков ядерной угрозы.

Работа Хеллмана и Уитфилда Диффи была опубликована в 1976 под названием «Новые направления в криптографии». Статья повлекла за собой немедленное развитие нового класса алгоритмов шифрования, алгоритмы с асимметричным ключом. Хеллман и Уитфилд Диффи были награждены Обществом Маркони в 2000 году за работу над криптографией с открытым ключом и помощи в становлении криптографии самостоятельным разделом науки.

Бейли Уитфилд Диффи
(англ. Bailey Whitfield Diffie)
(1944)

Диффи - один из самых известных американских криптографов, заслуживший мировую известность за концепцию криптографии с открытым ключом. В 1975 году Диффи, Хеллман и Меркл начали работать над концепцией шифрования с открытым ключом.

Система была основана на разбиении ключа на две части — известный открытый ключ и закрытый ключ. Это обеспечивало безопасность общения без необходимости встречи, чтобы обменяться ключами, и также предоставляло возможность цифровой подписи сообщений, чтобы понять от кого сообщение пришло. Шифрование с открытым ключом позволило использовать криптографию в повседневной жизни обычным людям. Решение Диффи и Мартина создало много проблем для правительственных структур, чьей задачей было отслеживание переговоров.

Эдуард Варинг
(англ. Edward Waring)
(1736-1798)

Варнинг - английский математик. Его необычайные математические способности были отмечены ещё во время обучения в Кол ледже святой Магдалины Кембриджского университета.Занимался в основном вопро сами теории чисел и алгебраическими уравне ниями. В 1760 году стал профессором в Кем бриджском университете. В 1782 году издал работу «Meditationes algebraicae», в кото рой сформулировал гипотезу, ставшую из вестной как проблема Варинга:

"Существует ли для каждого натурального n такое число g(n), что любое натуральное число n является суммой не более чем g(n) слагае мых, являющихся n-ми степенями натуральных чисел."

ПРИЛОЖЕНИЕ

Таблицы индексов по простым модулям, меньшим 100

Числа	Модули																							Числа
	3	**5**	**7**	**11**	**13**	**17**	**19**	**23**	**29**	**31**	**37**	**41**	**43**	**47**	**53**	**59**	**61**	**67**	**71**	**73**	**79**	**83**	**89**	**97**	
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
2	1	3	4	3	7	14	7	12	17	24	11	14	27	18	49	15	31	17	6	8	4	79	16	34	**2**
3		1	5	4	4	1	1	8	1	1	34	25	1	20	1	54	6	3	26	6	1	30	1	70	**3**
4		2	2	6	2	12	14	2	6	18	22	28	12	36	46	30	2	34	12	16	8	76	32	68	**4**
5			1	2	3	5	4	17	10	20	1	18	25	1	15	32	22	57	28	1	62	1	70	1	**5**
6			3	7	11	15	8	20	18	25	9	39	28	38	50	11	37	20	32	14	5	27	17	8	**6**
7				1	5	11	6	15	8	28	28	1	35	32	10	38	19	61	1	33	53	58	81	31	**7**
8				9	9	10	3	14	23	12	33	2	39	8	43	45	33	51	18	24	12	73	48	6	**8**
9				8	8	2	2	16	2	2	32	10	2	40	2	50	12	6	52	12	2	60	2	44	**9**
10				5	10	3	11	7	27	14	12	32	10	19	12	47	53	8	34	9	66	80	86	35	**10**
11					1	7	12	21	5	23	6	37	30	7	34	27	45	13	31	55	68	10	84	6	**11**
12					6	13	15	10	7	19	20	13	13	10	47	26	8	37	38	22	9	24	33	42	**12**
13						4	17	18	26	11	13	9	32	11	32	37	40	59	39	59	34	15	23	25	**13**
14						9	13	5	25	22	3	15	20	4	7	53	50	12	7	41	57	55	9	65	**14**
15						6	5	3	11	21	35	3	26	21	16	28	28	60	54	7	63	31	71	71	**15**
16						8	10	4	12	6	8	16	24	26	40	2	4	2	24	32	16	70	64	40	**16**
17							16	9	21	7	5	7	38	16	22	20	17	32	49	21	21	78	6	89	**17**
18							9	6	19	26	7	24	29	12	51	7	43	23	58	20	6	57	18	78	**18**
19								13	13	4	25	31	19	45	45	48	26	38	16	62	32	23	35	81	**19**
20								19	16	8	23	6	37	37	9	4	24	25	40	17	70	77	14	69	**20**
21								1	9	29	26	26	36	6	11	34	25	64	27	39	54	6	82	5	**21**
22								11	22	17	17	11	15	25	31	42	16	30	37	63	72	7	12	24	**22**
23									4	27	21	4	16	5	39	51	27	14	15	46	26	66	57	77	**23**
24									24	13	31	27	40	28	44	41	39	54	44	30	13	21	49	76	**24**
25									20	10	2	36	8	2	30	6	44	48	56	2	46	2	52	2	**25**

Числа	Модули																	Числа
26			15	5	24	23	17	29	29	52	11	10	45	67	38	12	39	59	**26**
27			3	3	30	35	3	14	3	46	18	9	8	18	3	8	3	18	**27**
28			14	16	14	29	5	22	4	10	21	29	13	49	61	52	25	3	**28**
29				9	15	33	41	35	18	14	5	22	68	35	11	46	59	13	**29**
30				15	10	17	11	39	13	43	59	11	60	15	67	28	87	9	**30**
31					27	12	34	3	5	39	29	7	11	11	56	50	31	46	**31**
32					19	30	9	44	37	17	35	19	30	40	20	67	80	74	**32**
33					4	22	31	27	35	23	51	16	57	61	69	40	85	60	**33**
34					16	21	23	34	19	35	48	49	55	29	25	75	22	27	**34**
35					29	19	18	33	25	12	41	52	29	34	37	59	63	32	**35**
36					18	38	14	30	48	22	14	40	64	28	10	54	34	16	**36**
37						8	7	42	14	13	9	44	20	64	19	22	11	91	**37**
38						5	4	17	42	5	57	55	22	70	36	20	51	19	**38**
39						34	33	31	33	33	46	62	65	65	35	45	24	95	**39**
40						20	22	9	6	19	55	42	46	25	74	74	30	7	**40**
41							6	15	21	36	54	43	25	4	75	44	21	85	**41**
42							21	24	8	49	56	15	33	47	58	3	10	39	**42**
43								13	38	31	13	21	48	51	49	33	29	4	**43**
44								43	28	57	47	47	43	71	76	4	28	58	**44**
45								41	17	24	34	63	10	13	64	61	72	45	**45**
46								23	36	8	58	31	21	54	30	63	73	15	**46**
47									24	55	20	58	9	31	59	13	54	84	**47**
48									41	56	10	5	50	38	17	18	65	14	**48**
49									20	18	38	56	2	66	28	34	74	62	**49**
50									27	21	15	65	62	10	50	81	68	36	**50**
51									23	16	23	35	5	27	22	26	7	63	**51**
52									26	9	42	27	51	3	42	9	55	93	**52**
53										40	3	45	23	53	77	69	78	10	**53**
54										3	49	26	14	26	7	5	19	52	**54**
55										1	7	4	59	56	52	11	66	87	**55**

Числа	Модули									Числа
56	25	52	46	19	57	65	49	41	37	**56**
57	44	32	41	42	68	33	53	36	55	**57**
58	29	36	39	4	43	15	43	75	47	**58**
59		1	18	3	5	31	62	43	67	**59**
60		30	28	66	23	71	25	15	43	**60**
61			53	69	58	45	48	69	64	**61**
62			24	17	19	60	47	47	80	**62**
63			1	53	45	55	36	83	75	**63**
64			36	36	48	24	64	8	12	**64**
65			50	67	60	18	16	5	26	**65**
66			33	63	69	73	37	13	94	**66**
67				47	50	48	29	56	57	**67**
68				61	37	29	72	38	61	**68**
69				41	52	27	14	58	51	**69**
70				35	42	41	56	79	66	**70**
71					44	51	65	62	11	**71**
72					36	14	51	50	50	**72**
73						44	39	20	28	**73**
74						23	19	27	29	**74**
75						47	32	53	72	**75**
76						40	17	67	53	**76**
77						43	68	77	21	**77**
78						39	42	40	33	**78**
79							35	42	30	**79**
80							71	46	41	**80**
81							38	4	88	**81**
82							41	37	23	**82**
83								61	17	**83**
84								26	73	**84**
85								76	90	**85**

ЗАКЛЮЧЕНИЕ

Изучение теории сравнений играет важную роль при подготовке специалистов-математиков. Большинство проблем теории сравнений непосредственно или косвенно связано с понятием делимости числа, поэтому все темы пособия заслуживают полного и глубокого изучения. Теория сравнений изучает числа с точки зрения их строения и внутренних связей, рассматривает возможности представления одних чисел через другие, более простые по своим свойствам.

Безусловно, настоящее издание не сможет заменить учебники по теории чисел по полноте представленного материала. Однако студентам математических специальностей оно будет интересно тем, что в одном пособии изложены как теоретический материал, так и решение примеров и задач, приведены исторические сведения. Обучающиеся могут использовать этот материал в других научных областях: теории корректирующих кодов, криптографии, методах сжатия информации и управления роботами, распознавании образов.

ЛИТЕРАТУРА

1. Бэйкер, А. Введение в теорию чисел / А. Бэйкер. — Минск : Выш-эйш. шк., 1995.

2. Бухштаб, А.А. Теория чисел / А.А. Бухштаб. — СПб.: Издательство “Лань”, 2008.

3. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. — М.: Наука, 1972.

4. Куликов, Л.Я. Алгебра и теория чисел / Л.Я. Куликов. — М.: Высш. шк., 1979.

5. Матысик, О.В. Теория чисел : курс лекций / О.В. Матысик, А.А. Трофимук; Брест. гос. университет им. А.С. Пушкина. – Брест : БрГУ, 2013. – 108 с.

6. Монахов, В.С. Алгебра и теория чисел : учебное пособие / В.С. Монахов, А.В. Бузланов. – Минск : Изд. центр БГУ, 2007.

7. Монахов, В. С. Числовые функции и классы вычетов : практикум

/ В.С. Монахов, А.А. Трофимук – Брест : Изд-во БрГУ имени А.С. Пушкина 2012. – 88 с.

8. Кочева, А.А. Задачник-практикум по алгебре и теории чисел. Часть III: Учебное пособие для студентов-заочников физико-математических факультетов педагогических институтов / А.А. Кочева. — М.: Просвещение, 1984.

9. Боревич, З.И. Теория чисел. / З.И. Боревич, И.Р. Шафаревич. — М.: Наука, 1972.

10. Воробьёв, Н.Н. Признаки делимости / Н.Н. Воробьёв. — М.: На-ука, 1980.

11. Степанов, С.А. Сравнения / С.А. Степанов. — М.: Знание, 1975.

12. Швецкий, М.В. Упражнения по теории чисел: элементы теории сравнений / М.В. Швецкий, Е.Ю. Яшина. — Спб. : Изд-во РГПУ им. Герцена, 2013.

13. Шмигирев, А.Э. Теория чисел: тексты лекций и индивидуальные задания / А.Э. Шмигирев, Э.Ф. Шмигирев, М.И. Ефремова. — Мозырь : УО МГПУ им. И.П. Шамякина, 2006.

14. Кудреватов, Г.А. Сборник задач по теории чисел / Г.А. Кудрева-тов. — М.: Просвещение, 1970.

15. Михелович, Ш.Х. Теория чисел / Ш.Х. Михелович. — М.: Просвещение, 1967.

Учебное электронное издание

КУРАНОВА Наталья Юрьевна

ТЕОРИЯ СРАВНЕНИЙ И ЕЁ АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ

Учебно-практическое пособие

Издается в авторской редакции

Системные требования: Intel от 1,3 ГГц; Windows XP/7/8/10; Adobe Reader; дисковод DVD-ROM.

Тираж 25 экз.

Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых
Изд-во ВлГУ
rio.vlgu@yandex.ru

Педагогический институт
кафедра физико-математического образования и информационных технологий
natali_math@mail.ru

Кафедра ФМО и ИТ