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

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Учебное пособие



Владимир 2019

УДК 511.2

ББК 22.13

К93

Рецензенты:

Кандидат физико-математических наук

доцент кафедры общей и теоретической физики

Владимирского государственного университета

имени Александра Григорьевича и Николая Григорьевича Столетовых

*А. А. Мокрова*

Кандидат физико-математических наук

доцент кафедры специальной техники и информационных технологий

Владимирского юридического института ФСИН России

*А. В. Хорошева*

**Куранова, Н. Ю.**

К93 Элементы теории чисел : учеб. пособие / Н. Ю. Куранова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2019. – 80 с. – ISBN 978-5-9984-0959-2

В пособии представлены следующие разделы теории чисел: теория делимости целых чисел, цепные дроби, мультипликативные функции, теория сравнений. В практикуме студентам предложены задания с приведенными типовыми примерами их решения.

Учебное пособие предназначено студентам математических специальностей высших учебных заведений, отдельные его разделы доступны также учащимся старших классов средней школы.

Библиогр.: 17 назв.

УДК 511.2

ББК 22.13

ISBN 978-5-9984-0959-2 © ВлГУ, 2019

 © Куранова Н.Ю., 2019

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 4](#_Toc17942902)

[ГЛАВА 1. ТЕОРИЯ ДЕЛИМОСТИ 6](#_Toc17942903)

[1.1 ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ. ДЕЛЕНИЕ С ОСТАТКОМ 6](#_Toc17942904)

[1.2 НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ 11](#_Toc17942905)

[1.3 АЛГОРИТМ ЕВКЛИДА 13](#_Toc17942906)

[1.4 ПРОСТЫЕ ЧИСЛА. «ОСНОВНАЯ » ТЕОРЕМА АРИФМЕТИКИ 18](#_Toc17942907)

[1.5 ЛИНЕЙНЫЕ ДИОФАНТОВЫ УРАВНЕНИЯ С ДВУМЯ НЕИЗВЕСТНЫМИ 24](#_Toc17942908)

[1.6 ТЕОРЕТИКО-ЧИСЛОВЫЕ ФУНКЦИИ 27](#_Toc17942909)

[1.6.1 ЦЕЛАЯ И ДРОБНАЯ ЧАСТЬ ЧИСЛА 27](#_Toc17942910)

[1.6.2 ЧИСЛО И СУММА ДЕЛИТЕЛЕЙ НАТУРАЛЬНЫХ ЧИСЕЛ 33](#_Toc17942911)

[1.6.3 ФУНКЦИЯ ЭЙЛЕРА 35](#_Toc17942912)

[1.7 ЦЕПНЫЕ ДРОБИ 37](#_Toc17942913)

[ГЛАВА 2. ТЕОРИЯ СРАВНЕНИЙ 50](#_Toc17942914)

[2.1 ОПРЕДЕЛЕНИЯ И ПРОСТЕЙШИЕ СВОЙСТВА 50](#_Toc17942915)

[2.2 ПОЛНАЯ И ПРИВЕДЕННАЯ СИСТЕМА ВЫЧЕТОВ 52](#_Toc17942916)

[2.3 ТЕОРЕМА ЭЙЛЕРА И ТЕОРЕМА ФЕРМА 53](#_Toc17942917)

[2.4 СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ 56](#_Toc17942918)

[2.5 СИСТЕМЫ СРАВНЕНИЙ ПЕРВОЙ СТЕПЕНИ. КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ. 59](#_Toc17942919)

[2.6 СРАВНЕНИЯ ЛЮБОЙ СТЕПЕНИ ПО ПРОСТОМУ МОДУЛЮ 62](#_Toc17942920)

[2.6 СРАВНЕНИЯ ЛЮБОЙ СТЕПЕНИ ПО СОСТАВНОМУ МОДУЛЮ 63](#_Toc17942921)

[2.8 СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ. СИМВОЛ ЛЕЖАНДРА 67](#_Toc17942922)

[2.9 СИМВОЛ ЯКОБИ 71](#_Toc17942923)

[2.10 КВАДРАТИЧНЫЕ СРАВНЕНИЯ ПО ПРОСТОМУ МОДУЛЮ 73](#_Toc17942924)

[2.10 КВАДРАТИЧНЫЕ СРАВНЕНИЯ ПО СОСТАВНОМУ МОДУЛЮ 76](#_Toc17942925)

[ЛИТЕРАТУРА 80](#_Toc17942926)

####

#### ВВЕДЕНИЕ

Установить достоверно, когда зародилась теория чисел, не представляется возможным. Однако точно установлено: на сегодня древнейшим, но не единственным документом, свидетельствующим об интересе древних к теории чисел, является небольшой обломок глиняной таблички 1800 годов до нашей эры. В нем - целый ряд так называемых Пифагоровых троек (натуральных чисел), многие из которых состоят из пяти знаков. Огромное количество таких троек исключает их механический подбор. Это свидетельствует о том, что интерес к теории чисел возник, намного раньше, чем предполагали ученые. История становления и развития теории чисел связана с именами таких выдающихся ученых, как Евклид, Паскаль, Ферма, Эйлер, Гаусс, Лагранж, Абель и мн. др. Этапы исторического развития теории чисел позволяют обратиться к истории и культуре цивилизаций Древней Греции и Востока, Китая, Индии, Европы. Проблемам теории чисел уделяли внимание и отечественные математики — В. Я. Буняковский, П. Л. Чебышев, А. А. Марков, Н. И. Лобачевский, И. М. Виноградов и другие.

Курс теории чисел содержит значительное число задач, как исторических, так и современных, решение которых позволяет взглянуть на эту науку, как на одну из составляющих общечеловеческой культуры. Многие разделы теории чисел обладают значительным гуманитарным потенциалом. Ее практические приложения неисчерпаемы. Разрабатывая и углубляя выкладки и исследования древних математиков, они вывели теорию на новый, значительно более высокий уровень, охватывающий множество областей. Глубокие исследования и поиски новых доказательств привели и к открытию новых проблем, некоторые из которых не изучены до сих пор.

Основу пособия составляют результаты элементарной теории чисел, сформировавшейся в трудах классиков - Ферма, Эйлера, Гаусса и др. Рассматриваются такие вопросы как простые и составные числа, арифметические функции, теория сравнений, цепные дроби, диофантовы уравнения. В каждом разделе приводится теория, примеры и задачи для самостоятельного решения.

Учебное пособие предназначено для подготовки бакалавров по направлению 44.03.05 «Педагогическое образование». Может быть полезно студентам математических специальностей высших учебных заведений при изучении спецкурсов по криптографии.

#### ГЛАВА 1. ТЕОРИЯ ДЕЛИМОСТИ

* 1. ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ. ДЕЛЕНИЕ С ОСТАТКОМ

**Определение.** Пусть *a* , *b* **Z** . Число *а* делится на число *b* если найдется такое число *q* , что *а* = *qb* . Синонимы: *а* кратно *b* ; *b* — делитель *а* .

**Теорема** . Для данного целого отличного от нуля числа *b* , всякое целое число *а* единственным образом представимо в виде *а* = *bq* + *r* , где 0 ≤ *r*<| *b* |.

**Доказательство.** Ясно, что одно представление числа *а* равенством *а = bq + r* мы получим, если возьмем *bq* равным наибольшему кратному числа *b* , не превосходящему *а.*

Тогда, очевидно, 0 ≤ *r* < | *b* |. Докажем единственность такого представления. Ну пусть *а = bq + r* и *а = bq* 1 + *r* 1 — два таких представления. Значит 0 *= а – а = b* ( *q – q* 1 ) + ( *r – r* 1 ). Здесь 0 делится на *b* ; *b* ( *q* – *q* 1 ) делится на *b* , следовательно ( *r – r* 1 ) обязано делиться на *b* . Так как 0 ≤ *r* < *b* и 0 ≤ *r* 1 < *b* , то *r – r* 1 < *b* и *r – r* 1 делится на *b* , значит *r – r* 1 равно нулю, а, значит и *q — q* 1 равно нулю, т. е. два таких представления совпадают.

**Определение.** Число *q* называется неполным частным, а число *r -* остатком от деления *а* на *b*.

Широкое практическое значение имеют следующие свойства:

* *Если остаток от деления  на  равен , а остаток от деления  на  равен , то остаток от деления  на  равен остатку от деления  на .*
* *Если остаток от деления  на  равен , а остаток от деления  на  равен , то остаток от деления  на  равен остатку от деления  на .*

**Пример 1**. Докажите, что квадрат целого числа не может иметь вид

Решение. Заметим, что числа вида при делении на 4 имеют остаток 2.

Рассмотрим всевозможные остатки квадратов целых чисел при делении на 4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 |
|  | 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.

**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 +

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *a* |  | a+1 |  | a+2 |  |  |
| 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 равен 1, если  четно, и 2, если 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  при делении на 3 дает в остатке 1.
* Число  при делении на 3 дает в остатке 1, а  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.
* Число  оканчивается на ту же цифру, что и число N

Используя арифметику остатков, можно получить ценные свойства для теоретико-числовых задач. Составим таблицы квадратов и кубов при делении на различные числа d.

**d=3**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**d=4**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**d=5**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**d=6**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**d=7**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**d=8**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**d=9**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Используя таблицы квадратов и кубов, решите следующие

**ЗАДАНИЯ**

### Может ли число 200...009 быть квадратом целого числа при каком-либо количестве нулей?

### Может ли число 100...004 быть квадратом целого числа?

### Может ли число 100…050…01 быть кубом целого числа?

### На какие цифры может оканчиваться квадрат целого числа?

### Может ли квадрат целого числа иметь вид

### a)5q + 2,

### b)3q − 1,

### c)6q − 1?

### Существует ли натуральное число N такое, что + 1 делится на 3? + 3 делится на 99.

### Докажите, что если делится на 3 (x, y — целые), то x и y делятся на 3.

### Может ли сумма квадратов двух нечетных чисел быть квадратом целого числа? А трех нечетных чисел?

### a, b, c — натуральные числа, причем a + b + c делится на 6. Докажите, что тоже делится на 6

### Докажите, что не является кубом натурального числа при натуральных а и b

###  Докажите, что ваше 28-летие будет отмечаться в тот же день недели, в который вы родились.

### Докажите, что если в трехзначном числе две последние цифры одинаковы, а сумма цифр делится на 7, то и само число делится на 7.

### К числу 15 припишите слева и справа по одной цифре так, чтобы полученное число делилось на 15.

### 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.

### Докажите, что уравнения не имеют решений в целых числах

### ;

### ;

### ;

### ;

### −;

### Докажите, что для любого целого а:

###  делится на 2;

###  делится на 4;

###  делится на 6;

###  делится на 7;

###  делится на 8;

###  делится на 9

### Докажите, что при любом натуральном n

### a) делится на 17;

### b) делится на 133 ;

### c) делится на 14;

### d) делится на 33;

### e) делится на 19.

### Докажите, что число делится на 13 тогда и только тогда, когда сумма числа, полученного отбрасыванием последней цифры и учётверённой последней цифры, делится на 13.

### Докажите, что число делится на 17 тогда и только тогда, когда число его десятков, сложенное с увеличенным в 12 раз числом единиц, кратно 17.

1. Разделите с остатком:

а) 161 на 17;

б) –161 на 17;

в) 161 на –17;

### г) –161 на –17.

### Справедливый ковбой зашел в бар и попросил у бармена стакан виски за 3 доллара, пачку Marlboro за доллар и 11 центов, шесть пачек патронов для своего кольта и дюжину коробков спичек. Услышав итоговую сумму – 28 долларов и 25 центов, ковбой пристрелил бармена. За что?

1.2 НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. НАИМЕНЬШЕЕ

ОБЩЕЕ КРАТНОЕ

**Определение.** Число *d* **Z** , делящее одновременно числа *а* , *b* , *c* , ... , *k* **Z**, называется общим делителем этих чисел. Наибольшее *d* с таким свойством называется наибольшим общим делителем (**НОД**). Обозначение: *d =* ( *a* , *b* , *c* , ..., *k* ) .

**Теорема**. Если ( *a* , *b* ) = *d* , то найдутся такие целые числа *u* и *v* , что *d = au + bv*.

**Доказательство**. Рассмотрим множество **P** *=* {*au + bv; u, v* **Z** }. Очевидно, что **P Z**, а знатоки алгебры могут проверить, что **P** – идеал в **Z**. Очевидно, что *a*, *b*, 0 **P**. Пусть *x*, *y* **P** и *y* 0. Тогда остаток от деления *x* на *y* принадлежит **P**. Действительно:

*x = yq + r*, 0 *r* < *y* ,

*r = x – yq =* ( *au* 1 + *bv* 1 ) – ( *au* 2 + *bv* 2 ) *q = a* ( *u* 1 – *u* 2 *q* )+ *b* ( *v* 1 – *v* 2 *q* ) **P** .

Пусть *d* **P** - наименьшее положительное число из **P**. Тогда *а* делится на *d*. В самом деле, *a = dq + r* 1, 0 ≤ *r* 1 < *d*, *a* **P** , *d* **P** , значит *r* **1 P** , следовательно *r* 1 = 0. Аналогичными рассуждениями получается, что *b* делится на *d* , значит *d* - общий делитель *a* и *b* .

Далее, раз *d* **P**, то *d = au* 0 + *bv* 0. Если теперь *d* 1 - общий делитель *a* и *b*, то *d* 1 | (*au* 0 + *bv* 0 ), т.е. *d* 1 | *d* . Значит *d d* 1 и *d* - наибольший общий делитель.

**Свойство 1**. Для любых целых чисел *а* и *k*, очевидно, справедливо: (*а*, *kа*) = *а*; (1, *а*) = 1.

**Свойство 2**. Если *a = bq + c*, то совокупность общих делителей *a* и *b* совпадает с совокупностью общих делителей *b* и *с*, в частности,

(*a*, *b* ) = ( *b* , *c* ).

**Доказательство.** Пусть *d | a*, *d* | , тогда *d* | *c* . Пусть *d* | *c*, *d* | *b* , тогда *d* | *a* .

**Свойство 3** . Пусть *a*, *b* и *m* - произвольные целые числа. Тогда

( *am* , *bm* ) = *m* ( *a* , *b* ).

**Доказательство.** Если *d* - наибольший общий делитель чисел *а* и *b* , то *dm* | *am* и *dm* | *bm* , т.е. *dm* - делитель *am* и *bm* . Покажем, что *dm* - наибольший общий делитель этих чисел. Поскольку *d* - наибольший общий делитель чисел *а* и *b* , то, согласно свойству 1, для некоторых целых чисел *u* и *v* выполнено равенство *d = au + bv* . Умножив это равенство на *m* , получим равенство:

*dm = amu + bmv* .

Видно, что если некоторое число *s* делит одновременно *am* и *bm* , то *s* обязано делить и *dm* , т.е. *s* ≤*dm* , следовательно, *dm* - наибольший общий делитель.

**Свойство 4** . Если ( *a* , *b* ) = 1, то ( *ac* , *b* ) = ( *c* , *b* ).

**Доказательство** . Пусть ( *c, b* ) *= d* . Имеем: *d* | *b* , *d* | *c* , следовательно *d* | *ac* , т.е. *d* - делитель *ас* и *b* . Пусть теперь ( *ac* , *b* ) = *s* . Имеем: *s* | *b* , *s* | *ac* , *s* - делитель *b* , т.е. либо *s* = 1, либо *s* не делит *а* . Это означает, что *s* | *c* , значит *s* | *d* . Итак, *d* и *s* делятся друг на друга, т.е. *d = s*.

**Определение.** Целые числа *a* и *b* называются взаимно простыми, если ( *a* , *b* ) = 1.

Заметим, что два числа *a* и *b* являются взаимно простыми тогда и только тогда, когда найдутся целые числа *u* и *v* такие, что *au + bv* = 1.

Если *a*1*b*, *a*2*b*, … , *anb*, то *b* называется общим кратным чисел *a*1,…,*a*n. Наименьшее положительное общее кратное чисел *a*1,…,*a*n называется их наименьшим общим кратным (**НОК**)*.*

Пусть НОД(*a*,*b*)=*d*, тогда можно записать *a=d∙a*1, *b=d∙b*1, где (*a*1,*b*1)=1.

Пусть *a*∣*M*, *b*∣*M*  *M*=*ak* для некоторого целого *k*, и тогда число  – целое. Но, поскольку (*a*1,*b*1)=1, то *b*1\*k* , и тогда *k=b*1*t* для некоторого , и

.

Очевидно, , *М* – общее кратное *a* и *b* дает формулу всех общих кратных.

При *t=*1 имеем *M*=НОК(*a*,*b*).



Формулой *M* = НОК(*a*,*b*)∙*t*  можно представить все общие кратные чисел *a* и *b*. ().

1.3. АЛГОРИТМ ЕВКЛИДА

*Слово "алгоритм" является русской транскрипцией латинизированного имени выдающегося арабского математика ал-Хорезми Абу Абдуллы Мухаммеда ибн ал-Маджуси (787 - ок.850) и означает в современном смысле некоторые правила, список инструкций или команд, выполняя которые, некто (быть может, тупой, но усердный) достигнет требуемого результата. ".*

*Алгоритм Евклида – алгоритм определения наибольшего общего делителя двух чисел путем последовательного применения теоремы о делении с остатком*.

*Алгоритм нахождения НОД, используемый в компьютерных программах и сейчас, был описан 2300 лет назад Эвклидом. Алгори́тм Евкли́да — эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел (или общей меры двух отрезков). Алгоритм назван в честь греческого математика Евклида, который впервые описал его в VII и X книгах «Начал». В самом простом случае алгоритм Евклида применяется к паре положительных целых чисел и формирует новую пару, которая состоит из меньшего числа и разницы между большим и меньшим числом. Процесс повторяется, пока числа не станут равными. Найденное число и есть наибольший общий делитель исходной пары. Первое описание алгоритма находится в «Началах» Евклида (около 300 лет до н. э.), что делает его одним из старейших численных алгоритмов, используемых в наше время. Оригинальный алгоритм был предложен только для натуральных чисел и геометрических длин (вещественных чисел). Однако в XIX веке он был обобщён на другие типы чисел, такие как целые числа Гаусса и полиномы от одной переменной. Это привело к появлению в современной общей алгебре такого понятия, как евклидово кольцо.*

Пусть даны два числа *a* и *b* ; *a* ≠0, *b* ≠0, считаем, что *a* > *b* . Символом **:=** в записи алгоритма обозначаем присваивание. Алгоритм:

**1. Ввести** *a* и *b* .

**2. Если** *b* = 0 **,** то **Ответ:** *а* . **Конец** .

**3. Заменить** *r* := "остаток от деления *а* на *b* ", *а* := *b* , *b* := *r* .

**4. Идти** на **2.**

В современной буквенной записи, кочующей из одного учебника в другой, алгоритм Евклида выглядит так: *a* > *b; a, b* **Z** .

|  |  |  |
| --- | --- | --- |
| *a = bq* 1 *+ r* 1 *b = r* 1 *q* 2 *+ r* 2 *r* 1 *= r* 2 *q* 3 *+ r* 3 *r* 2 *= r* 3 *q* 4 *+ r* 4  | 0 ≤ *r* 1 <*b* 0 ≤ *r* 2 < *r* 1 0 ≤ *r* 3 < *r* 2 0 ≤ *r* 4 < *r* 3  |  |
|  |
| *r n* -3 *= r n* -2 *q n -1 +r* n-1 *r n -2 = r n* -1 *q n + r n* *r n* -1 = *r n q n +1*  | 0 ≤*r n* -1 < *r n* -2 0 ≤ *r n* < *r n -1* *r n +1* = 0  |

Имеем: *b* > *r* 1 > *r* 2 >... > *r n* > 0, следовательно процесс оборвется максимум через *b* шагов. Очень интересный и практически важный народохозяйственный вопрос о том, когда алгоритм Евклида работает особенно долго, а когда справляется с работой молниеносно, мы рассмотрим в этой книжке чуть позже. Покажем, что *r n* = ( *a* , *b* ). Просмотрим последовательно равенства сверху вниз: всякий делителrь *а* и *b* делит *r* 1 , *r* 2 ,..., *r n* . Если же просматривать эту цепочку равенств от последнего к первому, то видно, что *r n | r n* -1 , *r n | r n* -2 , и т.д., т.е. *r n* делит *а* и *b* . Поэтому *r n* - наибольший общий делитель чисел *а* и *b* .

Доказательство дает практический способ нахождения чисел *u* и *v* из **Z** таких, что *r n = au + bv =*(*a, b* ). Действительно, из цепочки равенств имеем:

*r n = r n* -2 *- r n* -1 *q n = r n* -2 *-* ( *r n* -3 *- r n* -2 *q n* -1 ) *q n =* ...

(идем по цепочке равенств снизу вверх, выражая из каждого следующего равенства остаток и подставляя его в получившееся уже к этому моменту выражение)

... = *au + bv* = ( *a* , *b* ).

**Пример 1.** Пусть *а* = 525, *b* = 231. Отдадим эти числа на растерзание алгоритму Евклида: (ниже приводится запись деления уголком, и каждый раз то, что было в уголке, т.е. делитель, приписывается к остатку от деления с левой стороны, а остаток, как новый делитель, берется в уголок)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \_ \_42| 42 | 0  | \_ 63| 42 | 21 2    | \_ 231| 189 |   42 1      | 525| 462 |   63 3      | 231 2  |

Запись того же самого в виде цепочки равенств:

525 = 231 · 2 + 63
231 = 63 · 3 + 42
63 = 42 · 1 + 21
42 = 21 · 2

Таким образом, (525, 231) = 21. Линейное представление наибольшего общего делителя:

21 = 63 - 42 · 1 = 63 - (231 - 63 · 3) · 1 =
= 525 - 231 · 2 - (231 - (525 - 231 · 2) · 3) =
= 525 · 4 - 231 · 9,

и наши пресловутые *u* и *v* из **Z** равны, соответственно, 4 и - 9.

**Пример 2.**

При любом на туральном *n* найдите НОД чисел : и ; и .

Решение.

По алгоритму Евклида получаем , и . Таким образом, последний ненулевой остаток алгоритма Евклида равен 1.

Во втором случае, следуя алгоритму Евклида, получаем: ; . Далее, , где . При , то есть в случае , последний ненулевой остаток алгоритма Евклида равен 2. При , то есть в случае , последний ненулевой остаток алгоритма Евклида равен 1.

**Пример 3.** Сократите дробь:

Решение.

В первом случае по алгоритму Евклида получаем:

 . Таким образом, последний ненулевой остаток алгоритма Евклида равен 1, и ((6*n*+4), (22*n*+15))=1. То есть дробь несократима.

Во втором случае, следуя алгоритму Евклида, получаем:

При , то есть в случае , последний ненулевой остаток алгоритма Евклида равен 4, то есть ((16*n*+60),(11*n*+41))=4 при , и дробь сократима на 4:

При , то есть в случае , следующий шаг алгоритма имеет вид 4=1∙4+0, и последний ненулевой остаток алгоритма Евклида равен , то есть ((16*n*+60),(11*n*+41))=1 при , и дробь несократима

При , то есть в случае , последний ненулевой остаток алгоритма Евклида равен 2, то есть ((16*n*+60),(11*n*+41))=2 при , и дробь сократима на 2:

Наконец,при , то есть в случае , следующие два шага алгоритма евклидаимеют вид 4=3∙1+1, 3=1∙3+0, и последний ненулевой остаток алгоритма Евклида равен 1, то есть ((16*n*+60),(11*n*+41))=1 при , и дробь несократима.

**Пример 4.** Докажите, что для любого натурального *a* дробь несократима.

Предположим, что . Тогда разность делится на *d.* Следовательно *d=1.* Значит дробь несократима.

*Алгоритм Евклида является одним из старейших известных алгоритмов. Он встречается в «Началах» Евклида около 300 года до нашей эры. Евклид формулировал проблему геометрически, как задачу нахождения общей «меры» для двух отрезков, и его алгоритм состоял в последовательном вычитании меньшего отрезка из большего. Однако вероятно, что алгоритм не был открыт Евклидом, а появился почти на 200 лет раньше. Он был, скорее всего, известен Евдокусу (около 375 года до нашей эры); Аристотель (около 330 года до нашей эры) упоминал о нем в своих трудах. Этот алгоритм может быть использован на любом множестве, где возможно деление с остатком. Такие множества включают в себя кольца многочленов над полем, кольцо гауссовых чисел, Евклидовы области.*

**ЗАДАНИЯ**

1. Вычислить НОД(*a*,*b*) при помощи алгоритма Евклида с делением с остатком и бинарного алгоритма Евклида.

a) *a =* 715, *b =* 195;

d) *a =*1818, *b =* 726;

g) *a =* 2448, *b =* 1632;

b) *a =* 246, *b =* 396;

e) *a=* 6887, *b =* 6319;

h) *a =* 1600, *b =* 1120;

c) *a =* 175, *b =* 14945;

f) *a =* 1763, *b =* 1634;

i) *a =* 2310, *b =* 3388.

1. Сократима ли дробь? Если сократима, то на какое число?

*;*

1.4 ПРОСТЫЕ ЧИСЛА. «ОСНОВНАЯ» ТЕОРЕМА АРИФМЕТИКИ

**Определение.** Число *р* **N** , *р ≠*1, называется простым, если *р* имеет в точности два положительных делителя: 1 и *р* . Остальные натуральные числа (кроме 1) принято называть составными. Число 1 - на особом положении, по договору, оно ни простое, ни составное.

**Свойство 1.** Наименьший делитель любого числа *а* **N** , отличный от 1, есть число простое.

**Доказательство.** Пусть *с | а* , *с* ≠1 и *с* - наименьшее с этим свойством. Если существует *с* 1 такое, что *с* 1 | *с* , то *с* 1 ≤*с* и *с* 1 | *а* , следовательно, *с* 1 *= с* или *с* 1 = 1.

**Свойство 2.** Наименьший отличный от 1 делитель составного числа *а* **N** не превосходит *a* .

**Доказательство.** *с* | *а* , *с* ≠1, *с* - наименьший, следовательно

*а = са* 1 , *а* 1 | *а* , *а* 1 ≥*с* , значит *аа* 1 ≥*с* 2 *а* 1 , *а* ≥*с* 2 и *с* ≤

**Теорема Евклида.** Простых чисел бесконечно много.

**Доказательство.** От противного. Пусть *р* 1 , *р* 2 ,..., *р n* - все простые, какие только есть. Рассмотрим число *а* = *р* 1 *р* 2 ... *р n* + 1. Его наименьший отличный от 1 делитель *с* , будучи простым, не может совпадать ни с одним из *р* 1 *, р* 2 *,..., р n* , так как иначе *с* | 1. Не перестаю удивляться изобретательности ума людей тысячелетней древности!

*Многие учёные-математики, а также любители, занимаются поиском рекордных по величине простых чисел, за нахождение которых организацией [Electronic Frontier Foundation](https://ru.wikipedia.org/wiki/Electronic_Frontier_Foundation%22%20%5Co%20%22Electronic%20Frontier%20Foundation) было предложено несколько наград в зависимости от величины числа. Так, в 2009 году была вручена премия в 100 000 долларов США, назначенная сообществом Electronic Frontier Foundation за нахождение простого числа, десятичная запись которого содержит не менее 10 миллионов цифр. На данный момент рекорд принадлежит простому числу 282 589 933 − 1, открытому в рамках проекта*[*GIMPS*](https://ru.wikipedia.org/wiki/GIMPS)*7 декабря 2018 года. Десятичная запись числа имеет длину 24 862 048 цифр.*

Для составления таблицы простых чисел древний грек Эратосфен придумал процедуру, которая получила название "решето Эратосфена":

2, 3, ~~4~~ , 5, ~~6~~ , 7, ~~8~~ , ~~9~~ , ~~10~~ , 11, ~~12~~ , 13, ~~14~~ , ~~15~~ , ~~16~~ , 17,...

Идем по натуральному ряду слева направо. Подчеркиваем первое неподчеркнутое и невычеркнутое число, а из дальнейшего ряда вычеркиваем кратные только что подчеркнутому. И так много раз. Легко понять, что подчеркнутые числа - простые. Если вспомнить наблюдение 2, то становится понятно, что когда вычеркнуты все кратные простых, меньших *р* , то оставшиеся невычеркнутые, меньшие *р* 2 **-** простые. Это значит, что составление таблицы всех простых чисел меньших *N* закончено сразу, как только вычеркнуты все кратные простых, меньших *a* .

**Основная теорема арифметики.** Всякое целое число, отличное от - 1, 0 и 1, единственным образом (с точностью до порядка сомножителей) разложимо в произведение простых чисел.

**Доказательство.** Будем доказывать утверждение теоремы только для натуральных чисел, ибо знак минус перед числом умеют ставить все умеющие ставить знак минус.

Пусть *а* > 1, *р* 1 **-** его наименьший простой делитель. Значит,

*а = р* 1 *а* 1 . Если, далее, *а* 1 > 1, то пусть *р* 2 **-** его наименьший простой делитель и *а* 1 *= р* 2 *а* 2 , т.е. *а = р* 1 *р* 2 *а* 2 , и так далее, пока *а n* не станет равным единице. Это обязательно произойдет, так как *а* > *а* 1 > *а* 2 ..., а натуральные числа с естественным порядком удовлетворяют условию обрыва убывающих цепей (во как выразился!). Имеем, таким образом,

*a* = *p* 1 *p* 2 ... *p n* , и возможность разложения доказана.

Покажем единственность. Ну пусть *a* = *q* 1 *q* 2 ... *q n* **-** другое разложение, т.е. *p* 1 *p* 2 *...p n = q* 1 *q* 2 *...q s* . В последнем равенстве правая часть делится на *q* 1 , следовательно, левая часть делится на *q* 1 . Покажем, что если произведение *p* 1 *p* 2 *...p n* делится на *q* 1 , то один из сомножителей *р k* обязан делиться на *q* 1 .

Действительно, если *q* 1 | *p* 1 , то все доказано. Пусть *q* 1 не делит *p* 1 . Так как *q* 1 - простое число, то ( *q* 1 , *p* 1 ) = 1. Значит найдутся такие *u* , *v* **Z** , что *up* 1 + *vq* 1 = 1. Умножим последнее равенство на *p* 2 *...p n* , получим: *p* 2 ... *p n* = *p* 1 ( *p* 2 ... *p n* ) *u* + *q* 1 ( *p* 2 ... *p n* ) *v* . Оба слагаемых справа делятся на *q* 1 , следовательно, *p* 2 *...p n* делится на *q* 1 . Далее рассуждаем по индукции.

Теперь пусть, например, *q* 1 | *p* 1 . Значит *q* 1 *= p* 1 , так как *p* 1 **-** простое. Из равенства *p* 1 *p* 2 *...p n = q* 1 *q* 2 *...q s* банальным сокращением моментально получим равенство *p* 2 *...p n = q* 2 *...q s* . Снова рассуждая по индукции, видим, что *n = s* , и каждый сомножитель левой части равенства *p* 1 *p* 2 *...p n = q* 1 *q* 2 *...q n* обязательно присутствует в правой и наоборот.

**Теорема о делителях числа.**

Пусть  – каноническое разложение числа *a*. Тогда все делители *а* имеют вид

, где 0≤*β*1≤*α*1, 0≤*β*2≤*α*2, …, 0≤*βk*≤*αk*.

Доказательство:

Пусть *q*\*a*  *a* представимо в виде *a=dq*, тогда все простые делители числа *d* входят в каноническое разложение числа *а* с показателями, не меньшими тех, с которыми они входят в каноническое разложение числа *а*.

**Следствие 1**

Количество различных делителей числа  есть .

Доказательство очевидно, оно следует из числа всевозможных сочетаний в формуле делителя в теореме о делителях числа.

**Следствие 2**

НОД(*a*1,…,*an*), где  (), есть , где  ().

**Пример** 1.

*a*1=2∙3∙52=150, *a*2=22∙5∙7=140, *a*3=23∙5=40.

*p*1=2, *p*2=3, *p*3=5, *p*4=7.

*a*1=, *a*2=, *a*3=.

НОД(*a*1,*a*2,*a*3)= =2∙5=10.

**Следствие 3**

Совокупность общих делителей *a*1,…,*an* совпадает с совокупностью делителей НОД(*a*1,…,*an*).

**Следствие 4**

*НОК,* где , 

**Пример 2.**

НОК(150,140,40)=

**Следствие 5**

Если *a*1,…,*an* – попарно простые числа, то НОК(*a*1,…,*an*)*= a*1∙…∙*an*

**Следствие 6**

Совокупность общих кратных чисел *a*1,…,*an* совпадает с совокупностью кратных их наименьшего общего кратного*.*

**Задача 1** Найти натуральное число  такое, что числа , ,  - простые.

Решение. Если , то при делении на 3 в остатке может быть 1 или 2. Если , то  - не простое число, т.к. делится на 3. Если , то  - также не простое число. Поэтому , , .

**Задача 2**. Если  - простое число, то его можно представить в виде  или , где  - натуральное число.

Решение. Разделим  на 6 с остатком: . Поскольку  простое число, то остаток не может быть равен 2, 3 и 4. Остаются две возможности:  и . В первом случае , где , а во втором случае , где .

**Задача 3.** Доказать, что среди чисел вида , где  - простое число, только одно является точным кубом.

Решение. Данное число нечетное, поэтому оно является кубом нечетного числа: . Раскрывая это соотношение, получаем . Так как  - простое число, то  и .

**Задача 4.** Доказать, что при  между числами  и  содержится по крайней мере одно простое число.

Решение. Если это утверждение неверно, то все простые числа, меньшие , будут также не больше, чем . Рассмотрим число . Оно составное и поэтому должно делиться на простые числа, которые не превосходят . На эти же простые числа делится . Но два последовательных натуральных числа не могут иметь общих простых делителей, т.к. они взаимно простые.

**Задача 5.** Доказать, что если натуральные числа при делении на  дают остаток 1, то их произведение при делении на  также дает остаток 1.

Решение. Достаточно доказать это для произведения двух чисел. Пусть  и . Тогда , т.е. частным от деления числа  на  будет , а остатком 1.

**Задача 6.** В прямоугольном треугольнике длины всех сторон являются целыми числами. Доказать, что длина хотя бы одного катета делится на 3.

Решение. Пусть длины катетов равны  и , а длина гипотенузы равна . По теореме Пифагора . Рассуждая так же, как и в предыдущей задаче, находим, что остаток от деления на 3 правой части этого соотношения равен 0 или 1. Остаток левой части может быть равен 0 только в том случае, когда оба числа  и  делятся на 3. Аналогично, остаток левой части может быть равен 1 только в том случае, когда одно из чисел  или  делится на 3, а другое не делится. Если же оба числа  и  не делятся на 3, то остаток левой части равен 2, и поэтому соотношение  невозможно.

**Задача 7.** Методом Евклида докажите, что простых чисел вида 3*n*+1 бесконечно.

Доказательство. Все множество натуральных чисел разобьем на три подмножества с общими членами: 3*u*+1, 3*u*+1, 3*u*+2; среди чисел первого подмножества имеется лишь одно простое число 3, остальные простые числа входят в два другие подмножества. Допустим *Р* – наибольшее простое число вида 3*n*+1; запишем число *N*=3·7·13·19·…·*P+1,* где в произведение включено число 3 и все простые числа вида 3*n*+1; очевидно, число *N* будет вида 3*n*+1 и ,следовательно, *N=*3*s*+1.

Число *N* не может быть простым, так как *N,* но оно не можетиметь простыми делителями число 3 и числа вида 3*n*+1; следовательно, все его простые делители вида 3*u*+2, откуда *N*=3*t*+2, но равенство 3*t+2=3s+1* невозможно ни при каикх целых положительных значениях *t* и *s*, так как последнее равенство может быть переписано в виде 3(*t-s*)=-1. Полеченное противоречие доказывает существование бесконечного множества простых числе вида 3*n*+1.

**Задача 8**. Найти простое число *p*, чтобы числа вида было тоже простым.

Решение. Разобьем множество простых чисел на три класса: класс простых чисел 3*q (*q=1), класс проостых чисел 3*q*+1 (*q*=2,4,…) и класс простых чисе 3*q*+2 (*q*=1,3,…). Единственное простое число первого класса *p*=3 удовлетворяет требованиям задачи. При *p*=3*q*+1 или *p*=3*q*+2 , число является составным – кратным трем.

**ЗАДАНИЯ**

1. Разложить на простые множители *а* и *b*, найти их НОД и НОК
2. *а=1300; b=38808;*
3. *а=44044; b=3220;*
4. *а=4225; b=22015;*
5. *а=38115; b=359;1*
6. *а=2448; b=2430.*
7. Найти все простые *р*, для которого

является простым.

1. Докажите методом Евклида, что простых чисел вида *а*, бесконечно много, где .

1.5 ЛИНЕЙНЫЕ ДИОФАНТОВЫ УРАВНЕНИЯ С ДВУМЯ НЕИЗВЕСТНЫМИ

*Решение уравнений в целых числах является одной из древнейших математических задач. Наибольшего расцвета эта область математики достигла в Древней Греции. Основным источником, дошедшим до нашего времени, является произведение Диофанта – «Арифметика». Диофант суммировал и расширил накопленный до него опыт решения неопределенных уравнений в целых числах*

Пусть требуется решить линейное диофантово уравнение:

*ax + by = c* ,

где *a* , *b* , *c* **Z** ; *a* и *b* - не нули.

Попробуем порассуждать, глядя на это уравнение.

Пусть ( *a* , *b* ) = *d* . Тогда *a* = *a* 1 *d* ; *b* = *b* 1 *d* и уравнение выглядит так:

*a* 1 *d· x* + *b* 1 *d· y* = *c* , т.е. *d·* ( *a* 1 *x* + *b* 1 *y* ) = *c* .

Ясно, что у такого уравнения имеется решение (пара целых чисел *x* и *y* ) только тогда, когда *d* | *c* . Поскольку очень хочется решать это уравнение дальше, то пусть *d* | *c* . Поделим обе части уравнения на *d* , успокоимся, и всюду далее будем считать, что ( *a* , *b* ) = 1. Так можно.

Рассмотрим несколько случаев.

|  |  |  |
| --- | --- | --- |
| *Случай 1.* Пусть *c* = 0, уравнение имеет вид *ax + by* = 0 **- "** однородное линейное диофантово уравнение". Немножко потрудившись, находим, что  |  |  |

Так как *x* должен быть целым числом, то *y = at* , где *t* - произвольное целое число. Значит *x = - bt* и решениями однородного диофантова уравнения *ax + by =* 0 являются все пары вида {- *bt* , *at* }, где *t* = 0; ±1; ±2;... Множество всех таких пар называется общим решением линейного однородного диофантова уравнения, любая же конкретная пара из этого множества называется частным решением.

*Случай 2.*

Пусть теперь *c* **≠**0. Этот случай закрывается следующей теоремой.

**Теорема.** Пусть ( *a* , *b* ) = 1, { *x* 0 , *y* 0 } - частное решение диофантова уравнения *ax + by = c* . Тогда его общее решение задается формулами:

|  |  |
| --- | --- |
|  |  |

Таким образом, в теории линейных диофантовых уравнений общее решение неоднородного уравнения есть сумма общего решения соответствующего однородного уравнения и некоторого (любого) частного решения неоднородного уравнения.

**Доказательство.** То, что правые части указанных в формулировке теоремы равенств действительно являются решениями, проверяется их непосредственной подстановкой в исходное уравнение. Покажем, что любое решение уравнения *ax + by = c* имеет именно такой вид, какой указан в формулировке теоремы. Пусть { *x* \* *, y* \*} - какое-нибудь решение уравнения *ax + by = c* . Тогда *ax* \* *+ by* \* *= c* , но ведь и *ax* 0 *+ by* 0 *= c* . Следуя многолетней традиции доказательства подобных теорем, вычтем из первого равенства второе и получим:

*a* ( *x* \*- *x* 0 ) *+ b* ( *y* \*- *y* 0 ) = 0

- однородное уравнение. Далее, глядя на случай 1, рассмотрение которого завершилось несколькими строками выше, пишем сразу общее решение: *x* \*- *x* 0 *= - bt* , *y* \*- *y* 0 *= at* , откуда моментально, используя навыки третьего класса средней школы, получаем:

|  |  |
| --- | --- |
|  |  |

( *a* , *b* ) = 1. Это означает, что найдутся такие *u* и *v* из **Z** , что *au + bv =* 1 (если вы это забыли, вернитесь в пункт 4), причем эти *u* и *v* мы легко умеем находить с помощью алгоритма Евклида. Умножим теперь равенство *au + bv =* 1 на *c* и получим: *a* ( *uc* ) + *b* ( *vc* ) = *c* , т.е. *x* 0 *= uc* , *y* 0 *= vc* .

**Пример.**

7 *x* + 12 *y* = 43

алгоритм Евклида:

12 = 7· 1 + 5
7 = 5· 1 + 2
5 = 2· 2 + 1
2 = 1· 2

Значит, наибольший общий делитель чисел 7 и 12 равен 1 **,** а его линейное выражение таково:

1 = 5 - 2· 2 = 5 - (7 - 5) · 2 = (12 - 7) - (7 - (12 - 7) · 2) = 12· 3 + 7· (- 5),

т.е. *u* = - 5, *v* = 3. Частное решение:

*x* 0 = *uc* = (- 5) · 43 = - 215
*y* 0 = *vc* = 3 · 43 = 129.

*В августе 1900 г. в Париже состоялся II Международный конгресс математиков. 8 августа Д.Гильберт прочитал на нем доклад "Математические проблемы". Среди 23 проблем, решение которых (по мнению Д.Гильберта) совершенно необходимо было получить в наступающем XX в., десятую проблему он определил следующим образом:*

*"Пусть задано диофантово уравнение с произвольным числом неизвестных и рациональными числовыми коэффициентами. Указать способ, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых числах".*

*Гипотезу, что такого способа нет, первым выдвинул (с достаточным на то основанием) американский математик М.Дэвис в 1949 г. Доказательство этой гипотезы растянулось на 20 лет - последний шаг был сделан только в 1970 г. Юрием Владимировичем Матиясеевичем, на первом году аспирантуры он показал алгоритмическую неразрешимость 10 проблемы Гильберта.*

**ЗАДАНИЯ**

1. Решите диофантовы уравнения:
2. *2x + 7y = 20;*
3. *6 x - 21y = 21;*

### *11x + 99y = 41;*

### *17x + 25y = 117*

### Тема сделал несколько мелких покупок в супермаркете, имея при себе сто рублей. Давая сдачу с этой суммы, кассир ошиблась, перепутав местами цифры, и выплатила рублями то, что должна была вернуть копейками, и, наоборот, копейками то, что должна была вернуть рублями. Купив в аптеке набор пипеток за 1 руб.40 коп., Тема обнаружил ошибку кассира и, пересчитав деньги, нашел, что оставшаяся у него сумма втрое превышает ту, которую ему должны были вернуть в супермаркете. Какова стоимость всех покупок Темы?

1.6 ТЕОРЕТИКО-ЧИСЛОВЫЕ ФУНКЦИИ

1.6.1 Целая и дробная часть числа

В теории чисел рассматриваются разнообразные функции *f(n)*, значения которых при натуральных *n* связаны с арифметичесикми свойствами *n*.

*Определение*. Функция *f(n)* назывется числовой, если она определена при всех натуральных значениях аргумента *х*.

Важную роль в теории чисел играет функция *y = [х];* она определяется для всех вещественных х и представляет собой наибольшее целое, не превосходящее *х*. Эта функция называется целой частью от *х*. Наряду с функцией *y = [x*] существует функция *{x}=х - [*x], которая называется дробной частью от х.Функции целая и дробная часть числа находят широкое применение в дискретной математике и теории чисел.

Целой частью действительного числа х называется наибольшее целое число, не превосходящее *х*, т.е. целое число , такое, что + 1. Целая часть числа обозначается *[х].* Из определения следует, что *[х] [х] + 1*.

Дробной частью действительного числа х называется разность *х* - [*х*]. Дробная часть числа *х* обозначается {*x*}. Таким образом, {*x*} = *х* - [*х*] и 0 {*x*}< 1

**Примеры.** [4,8] = 4; [5] = 5; [π] = 3; [-6,29] = -7; [-e] = -3; {7} = 0; {π} = 0,1415…; {} = .

Рассмотрим свойства функции целой части действительного числа [х].

**Свойства целой части действительного числа**

**1.** Пусть *х* – действительное положительное число, *d* – целое положительное. Число положительных чисел, не превосходящих х и делящихся на *d*, равно [].

**Доказательство**

Рассмотрим положительные числа, кратные *d* и непревосходящие *х*; пусть наибольшее из них будет равно *sd*, так что (s + 1)d уже больше, чем *х*; число таких чисел d, 2d, 3d, …,sd равно s, где sd< (s + 1)d, следовательно, s< s + 1, т.е. s].

**2.**Для любого действительного числа *х* > 0 и целого *d* > 0

] = ].

**Доказательство**

Между [*х*] и *х* нет целых чисел, и поэтому число чисел, кратных d, в сегменте , равное согласно предыдущего свойства ], равно также величине ], выражающей число чисел, кратных d в сегменте .

**3.** Для любого действительного числа х разность [*х*] - 2] может равняться только 0 или 1.

**Доказательство.**

Для любого *х* имеем *х* - 1< [*х*] *х*, так что [*х*] - 2] ≤ х - 2 = 0,

[*х*] - 2] > х – 1 - 2 -1) = *x* – 1 – *x* + 2 = 1, т.е. целое число [*х*] - 2] может равняться только 0 или 1.

**4.** Пусть *p* – простое число, *n*  1 целое. Для показателя α наивысшей степени p, делящей n, имеем:

α = ] + ] + ] + …, т.е. при α, равном сумме (3), делитель n, но не является делителем n.

**Доказательство.**

При *n < p* все слагаемые в ряде равны нулю, и вместе с тем действительно в этом случае показатель наивысшей степени p, делящей *n*, равен нулю, так что для таких *p* и *n* свойство верно.

Возьмем теперь произвольное простое число p и применим метод индукции по *n*. При *n* = 1 свойство верно, так как в этом случае n = 1< *p*. Предположим, что утверждение верно при всех *n*, таких, что 1 *n < N*, где *N* целое (*N* 2).

Если *N <* p, то утверждение свойства верно для *N*, как это было отмечено выше.

Если *N*  p, то среди множителей 1, 2,…, *N* произведения *N* число делящихся на p будет равно по свойству 1° ]. Произведение всех остальных множителей числа 1 · 2… *N* обозначим через *М*. Тогда

*N* = p · 2 p ·…· ]*p* · *М* = · ]*М*, где p не является делителем *М.* Из *N* p следует 1 ] < *N*.

Так что согласно предположению показатель наивысшей степени p, делящей ], равен:

] + ] + … = ] + ]

Из формулы получаем, что наибольший показатель степени *p*, делящий *N*, равен ] + ] + ] + … Таким образом, свойство верно для *N* и в этом случае. По принципу полной математической индукции свойство при произвольном простом p верно для любого натурального n.

**Примеры**

**1.** Найдем наибольшее α, такое, что  делитель 1000!

Решение. По формуле (2) имеем:



Так что  делитель 1000!, но  не является делителем 1000!.

**2.** Найдем наибольшее α, такое, что 643! делится на 

Решение. По формуле (3) имеем:



 643! делится на 

**3.** Найти количество натуральных чисел, не превосходящих 1600 и взаимно простых с 45.

Решение. Поскольку , взаимно простыми числами с 45 являются те, которые не делятся ни на 3, ни на 5. Количество чисел, не превосходящих 1600 и делящихся на 3, равно , а делящихся на 5 равно . Количество чисел, не превосходящих 1600 и делящихся и на 3 и на 5, равно . Поэтому количество чисел, не превосходящих 1600 и делящихся либо на 3, либо на 5, равно 533+320-106=747. Остальные числа не делятся ни на 3, ни на 5, т.е. они взаимно просты с числом 1600. Их количество равно 1600-747=853.

Ответ: 853

**4.**Сколькими нулями оканчивается число 2012!?

Решение. Надо вычислить, сколько раз это число делится на 10. Для этого надо найти, с каким показателем степени входят числа 2 и 5 в разложение числа 2012! Показатель степени для 2 равен



Показатель степени для 5 равен



Поэтому 2012! делится на 10 в степени 501, т.е. оканчивается 501 нулем.

Ответ: 2012! оканчивается 501 нулем.

**5.** Найти наибольшее натуральное число , при котором дробь  является целым числом.

Решение. Данную дробь можно представить в виде .

Число 7 входит в разложение  с показателем

, а в разложение  с показателем . Таким образом, для того, чтобы дробь  была целым числом, наибольшее возможное значение  должно быть равно



Ответ. 

**6.**Решить уравнение , где  - натуральное число, и найти количество целочисленных решений.

Решение. При  имеет место неравенство  Пусть  Тогда из условия задачи получаем неравенство , из которого следует  Последнее неравенство возможно только при 

 Рассмотрим решение этого неравенства при различных значениях числа 

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Целочисленные решения | Количество целочисленных решений |
| 0 |  | 0,1,2,…,  |  |
| 1 |  |  |  |
| 2 |  |  |  |
| …… | …… | …… | …… |
|  |  |  | 2 |
|  |  |  | 1 |

Пусть теперь  Тогда из условия задачи получаем неравенство , из которого следует  Последнее неравенство возможно только при 

Рассмотрим решение этого неравенства при отрицательных значениях числа 

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Целочисленные решения | Кол-во целочисленных решений |
| -1 |  |  |  |
| -2 |  |  |  |
| …… | …… | …… | …… |
|  |  |  | 2 |
|  |  |  | 1 |

В итоге общее количество целочисленных решений равно 

Ответ. Количество целочисленных решений равно 

**ЗАДАНИЯ**

1. Найти каноническое разложение числа *n!*
2. *n=16;*
3. *n=32;*
4. *n=46;*
5. *n=19;*
6. *n=29;*
7. Сколькими нулями заканчивается число *n*! ?
8. *n=160;*
9. *n=264;*
10. *n=167;*
11. *n=234*
12. Найти количество чисел в промежутке , делящихся на 5; 7; 10
13. Найти количество чисел в промежутке , не делящихся ни на одно из чисел : 3, 5, 7

1.6.2 ЧИСЛО И СУММА ДЕЛИТЕЛЕЙ НАТУРАЛЬНЫХ ЧИСЕЛ

Рассмотрим числовые функциичисло делителей и сумма делителей натурального числа.

**Определение.** Число делителей определяется как число положительных делителей натурального n, а сумма делителей определяется как сумма положительных делителей n, т.е.

 =, = 

**Примеры**

1) = 1, = 6, так как у числа 18 шесть положительных делителей: 1, 2, 3, 6, 9, 18.

Заметим, что если p простое, то = 2

2) = 1+2+3+6+9+18=39 Очевидно, что для простых p = 1+p.

Рассмотрим основные свойства этих функций.

**1**. Если … - каноническое разложение натурального числа, то

 … = (+1) (+1)… (+1)

**Доказательство**

Любой положительный делитель числа n = . … имеет вид .…, где 0 ≤≤, 0 ≤ ≤, …, 0 ≤ ≤ ,и, таким образом, число положительных делителей n равно числу наборов ,,…,), где принимает +1 значение от 0 до , принимает +1 значение от 0 до ,..., принимает +1 значений от 0 до Число таких наборов равно (+1) (+1)… (+1), т. е.

 … = (+1) (+1)… (+1).

**Примеры**

Пусть n=504= · · 7; тогда τ(504)=4 · 3 · 2=24.

τ(1000000) = τ() = 7 · 7 = 49,

τ(48510) = τ( · 11) = 2 · 3 · 2 · 3 · 2 = 72.

**2**. Если … - каноническое разложение натурального числа, то

 = · 

**Доказательство**

=(1+++). (4)

Действительно, перемножая числа, стоящие в скобках, в правой части, мы получим слагаемые вида .…, где принимает значение от 0 до , принимает значение от 0 до ,..., принимает значений от 0 до причем каждое такое слагаемое суммы в левой части (4) получится один и только один раз. Чтобы получить формулу , остается только каждый множитель правой части записать в виде дроби: 

**Пример.**

 = · · · 11) = · · · = 72540.

 (504) = (..) = · · = 1560.

**3.**Числовые функции **-** число делителей и сумма делителей натурального числа - мультипликативные функции.

**Доказательство**

Если a = … и b = … – каноническое разложение взаимно простых чисел а и b ( все - простые числа), то …… - каноническое разложение а b и = (+1) … (+1) (+1) … (+1) = =

 =     =

**ЗАДАНИЯ**

 Вычислите:

1.6.3 ФУНКЦИЯ ЭЙЛЕРА

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

**Пример**

(8) = 4, так как существуют 4 неотрицательных числа, меньших 8 и взаимно простых с 8, а именно числа 1,3,5,7.

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

(5) = 4, (6) = 2, (7) = 6.

**Замечание**

Отметим, что (1) = 1, ибо существует одно неотрицательное число – нуль, для которого (0,1) = 1.

Очевидно, число (*n*) равно количеству чисел, которые образуют приведенную систему вычетов по модулю n.

Рассмотрим основные свойства функции Эйлера (*n*) . В соответствии с определением этой функции ее аргумент всегда считают натуральным числом.

Функция Эйлера мультипликативная.

 (a b) = (a) (b) при (a b) = 1.

Пусть *x* пробегает значения ,,…, образующие приведенную систему вычетов по модулю b, а y пробегает значения образующие приведенную систему вычетов по модулю a. Составим всевозможные числа вида a+bсоответстввующие различным парам ;число таких чисел будет равно (b) (a).

С другой стороны, поскольку (a,b)=1, то эти числа образуют приведенную систему вычетов по модулю ab, т. е. число таких чисел должно равняться (ab). Произведение (b) (a) и (a b) и выражают одну и ту же величину, т. е. (a b) (а)(b).

**Примеры**

1) (3) = 2, (10) = 4, (30) = 8;

2) (5) = 4, (8) = 4, (40) = 16;

3) (3) = 2, (6) = 2, (18) = 6.

В примере (3 · 6) ≠ (3) (6) , так как (3,6) = 2.

**2** Пусть p-простое число, α ≥ 1- любое натуральное, тогда

 ( )=(p -1).

**Доказательство**

Число взаимно просто с тогда и только тогда, когда оно не делится на p. Среди первых натуральных чисел имеется = чисел, делящихся на p; остальные -чисел взаимно просты с ,т. е. () =-=(p-1).

**3** Если n =….- каноническое разложение числа n, то (n) =…((-1)…..(-1).

**Доказательство**

,,…, в каноническом разложении обозначают различные простые числа, поэтому….-попарно взаимно простые числа и согласно свойствам 1, 2 и 3 имеем:

 (….)= ()=

-1)…(-1).

**Примеры**

1. (270)= (2 · ·5)=(2-1) (3-1) (5-1) = 72;
2. (700000)= (7) =(2-1) (5-1) (7-1)=240000;
3. Вычислить значения функции Эйлера для чисел 
4. (45375)= (3 · · )= ·11 · 2 · 10=22000

Решение. Для решения надо воспользоваться свойством мультипликативности функции Эйлера и формулой её значения для степени простого числа:

.

Отсюда получаем:

,

,



**Задача**. Найти значение , если известно значение .

Решение. Если число  нечетное, то в силу мультипликативности функции Эйлера  Если же число  четное, , где  - нечетное, то 

Но . Таким обра-зом, в этом случае .

1.7 ЦЕПНЫЕ ДРОБИ

*Цепные дроби были введены в 1572 году итальянским математиком Бомбелли. Современное обозначение непрерывных дробей встречается у итальянского математика Катальди в 1613 году. Величайший математик XVIII века Леонардо Эйлер первый изложил теорию цепных дробей, поставил вопрос об их использовании для решения дифференциальных уравнений, применил их к разложению функций, представлению бесконечных произведений, дал важное их обобщение.*

*Работы Эйлера по теории цепных дробей были продолжены М. Софроновым (1729-1760), академиком В.М. Висковатым (1779-1819), Д. Бернулли (1700-1782) и др. Многие важные результаты этой теории принадлежат французскому математику Лагранжу, который нашел метод приближенного решения с помощью цепных дробей дифференциальных уравнений.*

 Представление рациональных чисел цепными дробями.

Целое число, являющееся делителем каждого из целых чисел , называется общим делителем этих чисел. Общий делитель этих чисел называется их наибольшим общим делителем, если он делится на всякий общий делитель данных чисел.

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



где неполным частным последовательных делений  соответствуют остатки  с условием b>>>…>>0, а соответствует остаток 0.

Системе равенств (1) соответствует равносильная система



из которой последовательной заменой каждой из дробей  и т.д. ее соответствующим выражением из следующей строки получается представление дроби  в виде:







Такое выражение называется правильной (конечной) цепной или правильной непрерывной дробью, при этом предполагается, что  – целое число, а , …,  - натуральные числа.

Имеются различные формы записи цепных дробей:













Числа , , …,  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  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 .

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

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



так что представление можно удлинить:



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

2) Принимая условие , можно утверждать, что целая часть цепной дроби  равна ее первому неполному частному . В самом деле:

1. если *n=*1, то
2. если *n=*2, то ; поэтому 
3. если *n>*2, то =



,

где  >1, т.к. 





Поэтому и здесь . Докажем то, что рациональное число  однозначно представляется цепной дробью , если .

Пусть  с условием , . Тогда , так что . Повторным сравнением целых частей получаем , а следовательно  и так далее. Если , то в продолжении указанного процесса получим также . Если же , например , то получим , что невозможно.

Замечания:

1. В случае разложения правильной положительной дроби первый элемент , например, .
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**: , а так как , то 

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

**Пример**: 5=(5); .

***Подходящие дроби. Их свойства***.

Задаче разложения обыкновенной дроби в непрерывную дробь противостоит обратная задача – обращения или свертывания цепной дроби  в простую дробь .

Основную роль играют дроби вида:  или  которые называются подходящими дробями данной непрерывной дроби или соответствующего ей числа .

Заметим, что ==. Считается, что подходящая дробь  имеет порядок *k*.

Прежде чем приступить к вычислению подходящих дробей заметим, что  переходит в , если в первой заменить  выражением .

Имеем ,

,

, …,

при этом принимается, что , , , , ,  и так далее.

Закономерность, которую мы замечаем в построении формулы для  (ее числителя  и знаменателя ), сохраняется при переходе к  и сохранится также при переходе от *k* к (*k*+1).

Поэтому, на основании принципа математической индукции, для любого *k*, где , имеем

, причем ;  (3)

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  и знаменателей  подходящих дробей по формулам удобно располагать по схеме:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | … |  |  |  | … |  |
|  |  |  |  | … |  |  |  | … |  |
|  |  |  |  | … |  |  |  | … |  |

**Пример**:

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

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

Подходящие дроби  равны соответственно ; ; ; ; ; ; ; .

***Представление действительных иррациональных чисел правильными бесконечными цепными дробями***.

Для иррационального числа  указанный процесс должен быть бесконечным, так как конечная цепная дробь равна рациональному числу.

Выражение  (где , ) (2)



возникающее в таком процессе или заданное формально, называется *правильной бесконечной цепной*, или *непрерывной дробью*, или *дробью бесконечной длины* и обозначают кратко через (), а числа  – ее элементами или неполными частными.

Разложение  возможно только в единственном виде, так как процесс выделения целой части – процесс однозначный.

Рассмотрим пример разложения иррационального числа . Пусть . Выделим из  его целую часть. =3, а дробную часть –3, которая меньше 1, представим в виде , где .

Повторяя операцию выделения целой части и перевертывания дробной, получаем:

;

;

.

Если остановиться на этом шаге, то можно записать:



С другой стороны, из формулы для  видно, что =3+. Поэтому , вследствие чего, начиная с этого момента, неполные частные станут повторяться.

Бесконечная непрерывная дробь, в которой определенная последовательность неполных частных, начиная с некоторого места, периодически повторяется, называется *периодической непрерывной дробью*.

Если, в частности, периодическое повторение начинается с первого звена, то цепная дробь называется чисто периодической, в противном случае – смешанной периодической.

Итак,  разлагается в смешанную периодическую дробь (3, 3, 6, 3, 6, …) или (3, (3, 6)).

В общем случае разложения действительного иррационального числа  поступаем так же, как в примере. Останавливаясь при этом в процессе выделения целой части после *k*–го шага, будем иметь:



так что 



.

Числа  называются остаточными числами порядка *k* разложения . В формуле (4) имеем кусок разложения до остаточного числа .

Для бесконечной цепной дроби можно построить бесконечную последовательность конечных непрерывных дробей.



Эти дроби называют *подходящими дробями*. Закон образования соответствующих им простых дробей будет такой же, как и для подходящих дробей в случае конечных непрерывных дробей, так как этот закон зависит только от неполных частных  и совершенно не зависит от того, является ли  последним элементом или за ним следует еще элемент .

**Примеры**.

1. Записать в виде конечной цепной дроби

a) ; b) ; c) 2,98976; d) 

Решение:

1. =(0, 2, 15);
2. =(3, 7, 15, 1, 292);
3. 2,98976==(2, 1, 96, 1, 1, 1, 10);
4. =–(2, 1, 30, 2)=(-2, 1, 30, 2)
5. Разложить простую дробь в цепную дробь и найти ее подходящие дроби.

a) ; b) ; c) .

Решение:

a) =(3, 2, 1, 24);

Находим подходящие дроби:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | 3 | 2 | 1 | 24 |
|  | **1** | 3 | 7 | 10 | 247 |
|  | **0** | **1** | 2 | 3 | 74 |

=; =; =

b) =(3, 3, 33);

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | 3 | 3 | 33 |
|  | **1** | 3 | 10 | 333 |
|  | **0** | **1** | 3 | 100 |

=; =

c) =(3, 7, 15, 1, 292);

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | 3 | 7 | 15 | 1 | 292 |
|  | **1** | 3 | 22 | 333 | 355 | 103993 |
|  | **0** | **1** | 7 | 106 | 113 | 33102 |

=; =; =; =;

3. Разложить в цепную дробь и заменить подходящей дробью с точностью до 0,001 следующие числа:

a) ; b) ;c) .

Решение: a) =. Выделим из  его целую часть: , а дробную часть -2, которая <1, представим в виде , где . Повторяя эту операцию выделения целой части и переворачивания дробной, получаем:

;

;

.

Мы получили, что , следовательно, неполные частные, начиная с  будут повторяться и =(2, (4)).

Составим таблицу подходящих дробей:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | 2 | 4 | 4 | 4 | … |
|  | **1** | 2 | 9 | 38 |  |  |
|  | **0** | **1** | 4 | 17 | 72 |  |

Нам необходимо найти такую подходящую дробь , чтобы . Очевидно, что это , так как 17·72>1000.

Ответ: .

b) =; =5

;

;

;

;

;

.

Мы получили  неполные частные, начиная с  будут повторяться и =(5, (1, 1, 1, 10)).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 5 | 1 | 1 | 1 | 10 | 1 | … |
|  | 5 | 6 | 11 | 17 | 181 | 198 |  |
|  | 1 | 1 | 2 | 3 | 32 | 35 |  |

, так как 32·35>1000. Ответ: .

c) =; =1

;

;

;

=((1, 2))

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 |
|  | 1 | 3 | 4 | 11 | 15 | 41 | 56 | 153 |  |
|  | 1 | 2 | 3 | 8 | 11 | 30 | 41 | 102 |  |

, так как 30·41>1000.

Ответ: .

**ЗАДАНИЯ**

1. Разложить в конечную цепную дробь число
2. ;
3. ;
4. .
5. Разложить в бесконечную цепную дробь число
6. ;
7. ;
8. ;
9. .

#### Глава 2. ТЕОРИЯ СРАВНЕНИЙ

* 1. Определения и простейшие свойства

*Понятие сранения было введено впервые Гауссом. Несмотря на свою кажущуюся простоту, это понятие достаточно глубокое, очень важно и имеет много приложений*.

Определение. Пусть *а, b* ***Z*** , m ***N*** . Говорят, что число *а* сравнимо с *b* по модулю *m* , если *а* и *b* при делении на m дают одинаковые остатки. Записывается это так: *a ≡b(mod m)* .

Число *a* сравнимо с *b* по модулю *m* тогда и только тогда, когда *a-b* делится на *m* нацело. Очевидно, это бывает тогда и только тогда, когда найдется такое целое число *t* , что *a=b+mt* . Сравнимость *a* с *b* по модулю *m* означает, что *a* и *b* представляют один и тот же элемент в кольце Z m .

**Свойство 1.** Сравнения по одинаковому модулю можно почленно складывать.

*a*1≡*b*1(mod *m*), *a*2*≡ b*2(mod *m*), … , *a*k≡*b*k(mod *m*)=>*a*1+…+*a*k ≡*b*1+…*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 ≡ c* (mod *m*) * a ≡ c–b* (mod *m*)

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

*a ≡ b* (mod *m*) * a+mt ≡ b+mk*(mod *m*) (*t*, *k*  Z)

**Свойство 4.** Сравнения по одинаковому модулю можно почленно перемножать

*a ≡ b (mod m), c ≡ d (mod m)  ac ≡ bd (mod m)*

и, следовательно,

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

*a ≡ b (mod m)  ak ≡ bk(mod m)*

**Свойство 6.** Если *a0 ≡b0 (mod m)* , *a1 ≡b1 (mod m)* ,..., *an ≡bn (mod m)* , *x≡y(mod m)* , то *a0 x n +a1 x n-1 +...+a n ≡b0 y n +b1 yn-1 +...+bn (mod m)*

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

*a b* (mod *m*), (*a*, *b*) = *c*, (*c*, *m*) = 1  (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≡b* (mod *m*)  *ak≡bk* (mod *mk*)

*a=a*1*d*, *b=b*1*d*, *m=m*1*d  a*1≡*b*1(mod *m*1)

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

*a*≡*b* (mod *m*1), *a*≡b(mod *m*2), …, *a*≡*b*(mod *m*k) 

*a*≡*b* (mod *НОК*(*m*1,…,*m*k))

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

*a*≡*b* (mod *m*), *d*\*m*  *a*≡*b*(mod *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. ПОЛНАЯ И ПРИВЕДЕННАЯ СИСТЕМА ВЫЧЕТОВ

Отношение *≡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 *≡m* ("индекс эквивалентности *≡m* ") в точности равно *m* .

**Определение.** Любое число из класса эквивалентности *≡m* будем называть вычетом по модулю *m* . Совокупность вычетов, взятых по одному из каждого класса эквивалентности *≡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.** 1) Любые *m* штук попарно несравнимых по модулю *m* чисел образуют полную систему вычетов по модулю *m* .

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

**Доказательство.** Утверждение 1) – очевидно. Докажем утверждение 2). Чисел *аx+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 ≡ax 2 +b(mod m)* . Тогда, по свойствам сравнений из предыдущего пункта, получаем:

*ax1 ≡ax2 (modm) x1 ≡x2 (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 φ(*m)*  штук вычетов, где φ( *m* )– функция Эйлера – число чисел, меньших *m* и взаимно простых с *m* . Если к этому моменту вы уже забыли функцию Эйлера, загляните в пункт 14 и убедитесь, что про нее там кое-что говорилось.

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

**Лемма 2.** 1) Любые φ(*m*) чисел, попарно не сравнимые по модулю *m* и взаимно простые с модулем, образуют приведенную систему вычетов по модулю *m* .

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

2.3 ТЕОРЕМА ЭЙЛЕРА И ТЕОРЕМА ФЕРМА

**Теорема (Эйлер).** Пусть *m>1 , (a,m)=1* , φ( *m* ) – функция Эйлера. Тогда:

*a φ( m ) ≡1(mod m)* .

**Доказательство.** Пусть *х* пробегает приведенную систему вычетов по *mod m* :

*x=r 1 ,r 2 ,...,r c*

где *c= φ(m)* их число, *r 1 ,r 2 ,..., r c* - наименьшие неотрицательные вычеты по *mod m* . Следовательно, наименьшие неотрицательные вычеты, соответствующие числам *ax* суть соответственно:

*ρ1 , ρ2 ,..., ρc*

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

*a r 1 ≡ ρ1 (mod m)*
 *a r 2 ≡ ρ2 (mod m)*
...
 *a r c ≡ ρс (mod m)*

Перемножим эти *с* штук сравнений. Получится:

*a c r 1 r 2 ...r c ≡ρj 1 ρj 2 ... ρj c (mod m)*

Так как *r 1 r 2 ...r c = ρ1 ρ2 ... ρc ≠0* и взаимно просто с модулем *m* , то, поделив последнее сравнение на *r 1 r 2 ...r c* , получим *a φ( m ) ≡1(mod m)* .

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

**Теорема (Ферма).** Пусть *р* – простое число, *р* не делит *a* . Тогда:

*a p-1 ≡1(mod p)* .

**Доказательство.** Положим в условии теоремы Эйлера *m=p* , тогда *φ(m)=p-1* (см. пункт 14 ) . Получаем *a p-1 ≡1(mod p)* .



Необходимо отметить важность условия взаимной простоты модуля и числа *a* в формулировках теорем Эйлера и Ферма. Простой пример: сравнение 6 2 ≡1(mod 3) очевидно не выполняется. Однако можно легко подправить формулировку теоремы Ферма, чтобы снять ограничение взаимной простоты.

**Следствие .** Без всяких ограничений на *a* **Z** ,

*a p ≡a(mod p)* .

**Доказательство.** Умножим обе части сравнения *a p-1 ≡1(mod p)* на *a* . Ясно, что получится сравнение, справедливое и при *a* , кратном *р* .

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

Решение**.** a 9 ≡7(mod 10) – это дано. Кроме того, очевидно, что (7, 10)=1 и ( *a* , 10)=1. По теореме Эйлера, a φ(10) ≡1(mod 10). Следовательно, a 4 ≡1(mod 10) и, после возведения в квадрат, a 8 ≡1(mod 10). Поделим почленно a 9 ≡7(mod 10) на a 8 ≡1(mod 10) и получим a ≡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 ≡1(mod 101). Возведем это сравнение в четвертую степень: 7 400 ≡1(mod 101), домножим его на очевидное сравнение 7 2 ≡49(mod 101), получим: 7 402 ≡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-ую степень, раскроем его левую часть по биному Ньютона (мысленно, конечно). В этом гигантском 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 43 402 (mod 100). Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера, 43 φ(100) ≡1(mod 100). Считаем:

φ(100)= φ(2 2 5 2 )=(10–5)(10–2)=40.

Имеем сравнение: 43 40 ≡1(mod 100), которое немедленно возведем в десятую степень и умножим почленно на очевидное сравнение, проверенное на калькуляторе: 43 2 ≡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 ≡1(mod 3)
73 4 ≡1(mod 5)
73 6 ≡1(mod 7)

Перемножая, получаем:

73 12 ≡1(mod 3),(mod 5),(mod 7),

откуда, по свойствам сравнений следует:

73 12 -1 ≡0(mod 105),

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

**ЗАДАНИЯ**

**1** . Докажите, что:

а) 13 176 -1 делится на 89 ; б) 52 60 -1 делится на 385.

**2** . Докажите, что 3 100 -3 60 -3 40 +1 делится на 77.

**3** . Докажите, что:

а) 1 19 +2 19 +4 19 +5 19 +7 19 +8 19 ≡0(mod 9);

б) 1 14 +3 14 +7 14 +9 14 ≡0(mod 10).

**4** . Найдите две последние цифры десятичной записи числа:

а) 19 321 ; б) 131 161 .

**5** . Найдите остаток от деления:

а) числа 3 200 +7 200 на 101 ; б) числа 7 65 +11 65 на 80.

**6** . Докажите, что существует такая степень числа 2, все последние 1000 цифр которой в десятичной записи будут единицами и двойками.

**7**. Пользуясь теоремой Эйлера, вычислить:

a) 9042 mod 41; d) 8485 mod 187; g) 3161613 mod 16;

b) 34160003 mod 15; e) (-2)634178 mod 117; h) 5186609 mod 9;

c) (-5)100016 mod 11; f) 50190021 mod 38; i) 347174007 mod 349;

2.4 СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

Решить сравнение – значит найти все те х , которые удовлетворяют данному сравнению, при этом весь класс чисел по mod m считается за одно решение

Таким образом, число решений сравнения есть число вычетов из полной системы, которые этому сравнению удовлетворяют.

В этом пункте детально рассмотрим только сравнения первой степени вида

*ax ≡b(mod m),*

оставив более высокие степени на съедение следующим пунктам. Как решать такое сравнение? Рассмотрим два случая.

**Случай 1.** Пусть *а* и *m* взаимно просты. Тогда несократимая дробь *m/a* сама просится разложиться в цепную дробь:

Эта цепная дробь, разумеется, конечна, так как *m/a* - рациональное число. Рассмотрим две ее последние подходящие дроби:

. Вспоминаем важное свойство числителей и знаменателей подходящих дробей: *mQ n-1 -aP n-1 =(-1) n* . Далее (слагаемое *mQ n-1* , кратное *m* , можно выкинуть из левой части сравнения):

*-aP n-1 ≡(-1) n (mod m)* т.е.

*aP n-1 ≡(-1) n-1 (mod m)* т.е.

*a[(-1) n-1 P n-1 b] ≡b(mod m)*

и единственное решение исходного сравнения есть:

*x ≡(-1) n-1 P n-1 b(mod m)*



**Пример.** Решить сравнение 111x ≡75(mod 322).

Решение**.** (111, 322)=1. Включаем алгоритм Евклида:

322=11 · 2+100

111=100 · 1+11

100=11 · 9+1

11=1 · 11

(В равенствах подчеркнуты неполные частные.) Значит, *n=4* , а соответствующая цепная дробь такова:

Посчитаем числители подходящих дробей, составив для этого стандартную таблицу:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|    | 0  | 2  | 1  | 9  | 11  |
| *P n*  | 1  | 2  | 3  | 29  | 322  |

Числитель предпоследней подходящей дроби равен 29, следовательно, готовая формула дает ответ: *x ≡(-1) 3 29 75 -2175 ≡79(mod 322)*

**Случай 1.** Дано сравнение *ax ≡b(mod m)* , где *a* и *m* взаимно просты. По алгоритму Евклида, найдите *u* , *v* **Z** такие, что *au+vm=1* , умножьте это равенство на *b* : *aub+vmb=b* , откуда следует: *aub ≡b(mod m)* . Значит решением исходного сравнения является *x ≡ub(mod m)* .

**Случай 2.** Пусть *(a,m)=d* . В этом случае, для разрешимости сравнения *ax ≡b(mod m)* необходимо, чтобы *d* делило *b* , иначе сравнение вообще выполняться не может. Действительно, *ax ≡b(mod m)* бывает тогда, и только тогда, когда *ax- b* делится на *m* нацело, т.е. *ax- b=t · m* ,

*t* **Z** , откуда *b=ax- t m* , а правая часть последнего равенства кратна *d* .

Пусть *b=db 1* , *a=da 1* , *m=dm 1* . Тогда обе части сравнения *xa 1 d ≡b 1 d(mod m 1 d)* и его модуль поделим на *d* :

*xa 1 ≡b 1 (mod m 1 )* ,

где уже *а 1* и *m 1* взаимно просты. Согласно случаю 1 этого пункта, такое сравнение имеет единственное решение *x0* :

*x ≡x 0 (mod m 1 )*

По исходному модулю *m* , числа (\*) образуют столько решений исходного сравнения, сколько чисел вида (\*) содержится в полной системе вычетов: 0,1,2,..., *m-2, m-1* . Очевидно, что из чисел *x=x 0 +t m* в полную систему наименьших неотрицательных вычетов попадают только *x 0 , x 0 +m 1 , x 0 +2m 1 , ..., x 0 +(d-1)m 1* , т.е. всего *d* чисел. Значит у исходного сравнения имеется *d* решений.

**Теорема 1.** Пусть *(a,m)=d* . Если *b* не делится на *d* , сравнение *ax ≡b(mod m)* не имеет решений. Если *b* кратно *d* , сравнение *ax ≡b(mod m)* имеет *d* штук решений.

**Пример.** Решить сравнение *111x ≡75(mod 321)* .

Решение**.** *(111,321)=3* , поэтому поделим сравнение и его модуль на 3:

*37x ≡25(mod 107)* и уже *(37,107)=1* .

Включаем алгоритм Евклида (как обычно, подчеркнуты неполные частные):

107=37 2+33

37=33 1+4

33=4 8+1

4=1 4

Имеем *n=4* и цепная дробь такова:

Таблица для нахождения числителей подходящих дробей:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| q n  | 0  | 2  | 1  | 8  | 4  |
| P n  | 1  | 2  | 3  | 26  | 107  |

Значит, *x≡(-1)326 25 ≡-650(mod 107) ≡-8(mod 107) ≡99(mod 107)*.

Три решения исходного сравнения:

*x ≡99(mod 321), x ≡206(mod 321), x ≡313(mod 321)* ,

и других решений нет.

**Теорема 2.** Пусть *m>1, (a,m)=1* Тогда сравнение *ax ≡b(mod m)* имеет решение: *x ≡baφ(m)-1 (mod m)* .

**Доказательство.** По теореме Эйлера, имеем: *a φ(m) ≡1(mod m)* , следовательно, *a ba φ(m)-1 ≡b(mod m)* .

**Пример.** Решить сравнение *7x ≡3(mod 10)* . Вычисляем:

*φ(10)=4; x ≡3·7 4-1 (mod 10)≡1029(mod 10) ≡9(mod 10)* .

**ЗАДАНИЯ**

Решить сравнения:

a) 5*x* ≡ 3(mod 11); d) 6*x* ≡15(mod 21); g) 13*x*≡8(mod 16);

b) 8*x* ≡ 5(mod 13); e) 16*x*≡26(mod 62); h) 25*x*≡50(mod 125);

c) 15*x*≡25(mod 17); f) 21*x*≡14(mod 42); i) 13*x*≡37(mod 29).

* 1. СИСТЕМЫ СРАВНЕНИЙ ПЕРВОЙ СТЕПЕНИ. КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ.

Рассмотрим систему сравнений



**Китайская теорема об остатках**

Пусть *m*1,…, *mk* – попарно простые числа ** система сравнений (\*) имеет единственное решение *x*0 ≡ \*\*,

где *M=*, *Mi*=, .

Доказательство:

Т.к. *ms*\*Mj*     

  система (\*) равносильна системе

 \*\*\*

т.е. системам (\*) и (\*\*\*) удовлетворяют одни и те же значения *x*. Системе (\*\*\*) (в силу свойств 12 и 13 сравнений) удовлетворяют те и только те значения, которые заданы теоремой (т.е. *x*0).

Следствие.

Если в системе \*\*  независимо друг от друга пробегают полные системы вычетов по модулям  соответственно, то  пробегает полную систему вычетов по модулю *M*.

Доказательство: в силу свойства 13 сравнений, *x*0 пробегает ровно *M* не сравнимых по модулю *M* значений.

*Эта теорема 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.*

**Пример**

Решить систему сравнений:



|  |  |  |  |
| --- | --- | --- | --- |
| *mi* | 3 | 4 | 5 |
| *Mi* | 20 | 15 | 12 |
|  | 2 | 3 | 3 |

Вычислим параметры, необходимые для нахождения решения. Составим таблицу

Согласно китайской теореме об остатках, решением будет являться

*x*0≡1∙20∙2+2∙15∙3+4∙12∙3(mod 60)≡40+90+144(mod 60)≡34(mod 60).

Ответ: *x*≡34(mod 60).

**Пример.**

Решить систему сравнений:



*b 1 =1* ; *b 2 =3* ; *b 3 =2* ;

 *M 1 =35, M 2 =28, M 3 =20* .

35 ·3 ≡1(mod 4)
28 ·2 ≡1(mod 5)
20 ·6 ≡1(mod 7)

т.е. *M 1 -1*=3, *M 2 -1*=2, *M 3 -1*=6.

Значит *x 0* =35 ·3 ·1+28 ·2 ·3+20 ·6 ·2=513.

Получим ответ: *x* ≡513(mod 140) ≡93(mod 140),

т.е. наименьшее положительное число равно 93.

**ЗАДАНИЯ**

Решить системы сравнений.

a) ; c) ; e)  ;

b) ; d) ; f).

2.6 СРАВНЕНИЯ ЛЮБОЙ СТЕПЕНИ ПО ПРОСТОМУ МОДУЛЮ

В этом пункте мы рассмотрим сравнения вида *f(x) 0(mod p)* , где *р* - простое число, *f(x)=ax n +a 1 x n-1 +…+a n* - многочлен с целыми коэффициентами, и попытаемся научиться решать такие сравнения. Не отвлекаясь на посторонние природные явления, сразу приступим к работе.

**Лемма 1.** Произвольное сравнение *f(x) ≡0(mod p)* , где *р* - простое число, равносильно некоторому сравнению степени не выше *p-1* .

**Доказательство.** Разделим *f(x)* на многочлен *x p -x* (такой многочлен алгебраисты иногда называют "многочлен деления круга") с остатком: *f(x)=(x p -x) ·Q(x)+R(x),* где, как известно, степень остатка *R(x)* не превосходит *р-1* . Но ведь, по теореме Ферма, *x p -x ≡0(mod p)* . Это означает, что *f(x) ≡R(x)(mod p)* , а исходное сравнение равносильно сравнению *R(x) ≡0(mod p).*

С ее помощью можно свести решение сравнения высокой степени к решению сравнения меньшей степени.

**Лемма 2.** Если сравнение *ax n +a 1 x n-1 +…+a n ≡0(mod p)* степени *n* по простому модулю *р* имеет более *n* различных решений, то все коэффициенты *a,a 1 ,…,a n* кратны *р* .

**Доказательство.** Пусть сравнение *ax n +a 1 x n-1 +…+a n ≡0(mod p)* , имеет *n+1* решение и *x 1 ,x 2 ,…,x n ,x n+1* – наименьшие неотрицательные вычеты этих решений. Тогда, очевидно, многочлен *f(x)* представим в виде:

|  |
| --- |
| *f(x)=a(x-x 1 )(x-x 2 )…(x-x n -2)(x-x n-1 )(x-x n )+ +b(x-x 1 )(x-x 2 )…(x-x n -2)(x-x n-1 )+ +c(x-x 1 )(x-x 2 )…(x-x n -2)+ +…+ + k(x-x 1 )(x-x 2 )+ +l(x-x 1 )+ +m.*  |

Действительно, коэффициент *b* нужно взять равным коэффициенту при *x n-1* в разности *f(x)-a(x-x1)(x-x2)…(x-xn)* ;
коэффициент *с* – это коэффициент перед *x n-2* в разности *f(x)-a(x-x1)(x-x 2 )…(x-xn - b(x-x1)(x-x2)…(x-xn-1) ,* и т.д.

Теперь положим последовательно *x=x1 ,x2 ,…,xn ,xn+1* . Имеем:

1) *f(x1)=m≡0(mod p)*, следовательно, *р* делит *m* .

2) *f(x2 )=m+l(x2 -x1 ) ≡l(x2 -x1) ≡0(mod p)* , следовательно, *р* делит *l* , ибо *р* не может делить *x2-x1*, так как *x2 <p, x1 <p* .

3) *f(x3 ) ≡k(x3 -x1 )(x3 -x2 ) ≡0(mod p)* , следовательно, *р* делит *k* .

И т.д.

Получается, что все коэффициенты *a, b, c,...,k, l* кратны *р* . Это означает, что все коэффициенты *a,a 1 ,…,a n* тоже кратны *р* , ведь они являются суммами чисел, кратных *р* .

Если модуль- число составное, то сравнение *n* -ой степени может иметь и более *n* решений, при этом, коэффициенты многочлена не обязаны быть кратными *р* .

 Пример:

сравнение второй степени *x 2 ≡1(mod 16)* имеет четыре различных решения:

*x ≡1(mod 16), x ≡7(mod 16), x ≡9(mod 16) , x ≡15(mod 16).*

Всякое нетривиальное сравнение по *mod p* равносильно сравнению степени не выше *p-1* и имеет не более *p-1* решений.

* 1. СРАВНЕНИЯ ЛЮБОЙ СТЕПЕНИ ПО СОСТАВНОМУ МОДУЛЮ

Переход от решения сравнений по простому модулю к a priori более сложной задаче — решению сравнений по составному модулю (переход от пункта 20 к пункту 21) осуществляется быстро и без лишних затей с помощью следующей теоремы:

**Теорема 1.** Если числа *m* 1 , *m* 2 ,… *m k* попарно взаимно просты, то сравнение *f* ( *x* ) ≡0(mod *m* 1 *m* 2 … *m k* ) равносильно системе сравнений:



При этом, если Т 1 , Т 2 , ..., Т к  — числа решений отдельных сравнений этой системы по соответствующим модулям, то число решений Т исходного сравнения равно Т 1 Т 2 ...Т к .

**Доказательство.** Первое утверждение теоремы (о равносильности системы и сравнения) очевидно, т.к. если *a* ≡b (mod *m* ) , то *a* ≡*b* (mod *d* ), где *d* делит *m* . Если же *a* ≡*b* (mod *m* 1 ) и *a* ≡*b* (mod *m* 2 ), то *a* ≡*b* (mod *HOK* ( *m* 1 , *m* 2 )), где *НОК* ( *m* 1 ,  *m* 2 )– наименьшее общее кратное *m* 1 и *m* 2 . (Вспомните простейшие свойства сравнений из пункта 16).

Обратимся ко второму утверждению теоремы (о числе решений сравнения).

Каждое сравнение *f* (*x* ) ≡0(mod *m s* ) выполняется тогда и только тогда, когда выполняется одно из T s штук сравнений вида *x* ≡*b s* (mod *m s* ), где *b s* пробегает вычеты решений сравнения *f* ( *x* ) ≡0(mod *m s* ). Всего различных комбинаций таких простейших сравнений



Т 1 Т 2 ...Т к штук. Все эти комбинации, по лемме 2 из пункта 19, приводят к различным классам вычетов по mod( *m* 1 *m* 2 … *m* k ).

Итак, решение сравнения  сводится к решению сравнений вида *f* ( *x* ) ≡0(mod *p a* ). Оказывается, что решение этого последнего сравнения, в свою очередь, сводится к решению некоторого сравнения *g* ( *x* ) ≡0(mod *p* ) c другим многочленом в левой части, но уже с простым модулем, а это, просто напросто, приводит нас в рамки предыдущего пункта. Сейчас я расскажу процесс сведения решения сравнения *f* ( *x* ) ≡0(mod *p a* ) к решению сравнения *g* ( *x* ) ≡0(mod *p* ).

**Процесс сведения.**

Решение сравнение вида *f*(*x*)≡0(mod *p*α) может быть найдено, если известно решение сравнения *f*(*x*)≡0(mod *p*). Покажем это.

Пусть *x≡x*1(mod *p*) – решение сравнения *f*(*x*)≡0(mod *p*). Тогда *x* можно представить в виде

*x=x*1+*pt*1, где .

Подставляя такое *x* в сравнение *f*(*x*)≡0(mod *p*2) и применяя формулу Тейлора (учитывая, что *f*(*x*) – многочлен, *x*1 – целое число, поэтому  ), получаем

*f*(*x*1)+*pt*1*f* '(*x*1)≡0(mod *p*2).

 Поскольку *f*(*x*1)≡0(mod *p*), то p\*f*(*x*1), а значит можно сократить в получившемся выражении на *p* правую, левую части и модуль. Получим:



Если *f* '(*x*1) не делится на *р*, то данное сравнение имеет одно решение:

 (т.е. )  

Подставляя полученное *x* в сравнение *f*(*x*)≡0(mod *p*3), имеем

*f*(*x*2)+*p*2*t*2*f* '(*x*2)≡0(mod *p*3),

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



[Здесь *f* '(*x*2) не может быть кратно *р*, если *f* '(*x*1) не кратно *p*, т.к. *x*2≡*x*1(mod *p*), а значит, *f* '(*x*2) ≡ *f* '(*x*1) (mod *p*)]

Тогда сравнение имеет одно решение , или, что то же самое,  , откуда получаем решение по модулю *p*3 : *x=x*3+*p*3*t*3.

Продолжим этот процесс до тех пор, пока не будет решено сравнение по модулю *pα.* Итак, по данному решению сравнения *f*(*x*)≡0(mod *p*) можно найти решение сравнения *f*(*x*)≡0(mod *p*α).

Итак:

***Всякое решение*** *x* ≡*x* 1 (mod *p* ) ***сравнения*** *f* ( *x* ) ≡0(mod *p* ), ***при условии*** p/ *f ′′*( *x* 1 ), ***дает одно решение сравнения*** *f* ( *x* ) ≡0(mod *p a* ) ***вида*** *x* ≡*x* a + *p* a *t* a , т.е. *x* ≡*x* a (mod *p a* ).

**Пример 1.** Требуется решить сравнение *x*3+9*x*—1≡0 (mod 125).

Решение. Известно, что сравнение *x*3+9*x*—1≡0 (mod 5) имеет одно решение:

*x*≡2(mod 5), или *x=*2+5*t*1.

Подставим получившееся *x* в сравнение по модулю 25:

(2+5*t*1)3+9(2+5*t*1)—1≡0 (mod 25).

Решим это сравнение.

8+4·5*t*1+2·(5*t*1)2+(5*t*1)3+18+9·5*t*1—1≡0 (mod 25)

25+13·5*t*1+25·(5*t*13+2 *t*12) ≡0 (mod 25)

13·5*t*1≡0 (mod 25)

13*t*1≡0 (mod 5)

*t*1≡0 (mod 5)

Или, что то же самое, *t*1=0+5*t*2, откуда решение по модулю 25 есть *x=*2+25*t*2. Подставим полученное *x* в сравнение по модулю 125:

(2+25*t*2)3+9(2+25*t*2)—1≡0 (mod 125)

Решим это сравнение.

8+4·25*t*2+2·(25*t*2)2+(25*t*1)3+18+9·25*t*1—1≡0 (mod 125)

25+13·25*t*2+625·(25*t*23+2*t*22) ≡0 (mod 125)

25+13·25*t*2≡0 (mod 125)

1+13*t*2≡0 (mod 5)

13*t*2≡-1 (mod 5)

3*t*2≡4 (mod 5)

Получили сравнение первой степени. Решим его. Найдем 3-1(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)=2·3-1·5.

2≡3-1(mod 5).

Тогда решением сравнения относительно *t*2 будет

*t*2≡2·4 (mod 5)

*t*2≡3 (mod 5)

Или, что то же самое, *t*2=3+5*t*3, откуда решение по модулю 125 есть *x=*2+25(3+5*t*3)=2+75+125*t*3=77+125*t*3, или, что то же самое,

x≡77 (mod 125).

**Пример 2 .** Решить сравнение *x* 4 +7 *x* +4 ≡0(mod27).

Решение.27=3 3 .

процесс решения должен быть таким:

*f ′*( *x* )=(4 *x* 3 +7) |*x* ≡1 ≡2(mod 3),

т.е. не делится на *р* = 3. Далее: *x* 1 =1+3 *t* 1

*f* (1)+ *f ′*(1) 3 *t* 1 ≡0(mod3 2 )

Ищем *t* 1 : 3+3 *t* 1·2≡0(mod 9), после деления на *р* =3:

1+2 *t* 1 ≡0(mod 3),

*t* 1 ≡1(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) ≡0(mod *p* 3 =27),

18+9 20 *t* 2 ≡0(mod27),

и, после деления на *p* 2 =9, ищем *t* 2 : 2+20 *t* 2 ≡0(mod3), *t* 2 ≡2(mod3), *t* 2 =2+3 *t* 3 ,

откуда *x* =4+9 (2+3 *t* 3 )=22+27 *t* 3 .

Значит, решением сравнения является *x* ≡22(mod27).

**ЗАДАНИЯ**

**1.** Сколько решений имеет сравнение *x* 5 + *x* +1 ≡0(mod105) ?

**2.** Решите сравнения:

а) 7 *x* 4 +19 *x* +25 ≡0(mod27);

б) 9 *x* 2 +29 *x* +62 ≡0(mod64);

 в) 6 *x* 3 +27 *x* 2 +17 *x* +20 ≡0(mod30);

 г) 31 *x* 4 +57 *x* 3 +96 *x* +191 ≡0(mod225);

 д) *x* 3 +2 *x* +2 ≡0(mod125);

е) *x* 4 +4 *x* 3 +2 *x* 2 +2 *x* +12 ≡0(mod625).

* 1. СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ. СИМВОЛ ЛЕЖАНДРА

В этом пункте мы будем подробно рассматривать простейшие двучленные сравнения второй степени вида

*x* 2 ≡*a* (mod *p* ),

где *а* и *р* взаимно просты, а *р* - нечетное простое число.

Ясно, что сравнение *x* 2 ≡*a* (mod 2) имеет решение при любых *а* , т.к. вместо *а* достаточно подставлять только 0 или 1, а числа 0 и 1 являются квадратами. Именно поэтому случай *р* =2 не представляет особого интереса и выводится из дальнейшего рассмотрения.

Что касается сравнения *x* 2 ≡0(mod *p* ), то оно, очевидно, всегда имеет решение *х* =0. Итак, интерес представляет только ситуация с нечетным простым модулем и *а* ≠0.

**Определение.** Если сравнение *x* 2 ≡*a* (mod *p* ) имеет решения, то число *а* называется квадратичным вычетом по модулю *р* . В противном случае, число *а* называется квадратичным невычетом по модулю *р* .

Итак, если *а* – квадрат некоторого числа по модулю *р* , то *а* -“квадратичный вычет”, если же никакое число в квадрате не сравнимо с *а* по модулю *р* , то *а* - “квадратичный невычет”.

**Пример.** Число 2 является квадратом по модулю 7 , т.к.

4 2 ≡16 ≡2(mod7). Значит, 2 - квадратичный вычет. (Сравнение *x* 2 ≡2(mod7) имеет еще и другое решение: 3 2 ≡9 ≡2(mod7).) Напротив, число 3 является квадратичным невычетом по модулю 7 , т.к. сравнение *x* 2 ≡3(mod7) решений не имеет, в чем нетрудно убедиться последовательным перебором полной системы вычетов: *x* = 0,1,2,3,4,5,6.

**Простое наблюдение:** Если *а* - квадратичный вычет по модулю *р* , то сравнение *x* 2 ≡*a* (mod *p* ) имеет в точности два решения. Действительно, если *а* - квадратичный вычет по модулю *р* , то у сравнения *x* 2 ≡*a* (mod *p* ) есть хотя бы одно решение *x* ≡*x* 1 (mod *p* ). Тогда *x* 2 = - *x* 1 – тоже решение, ведь (- *x* 1 ) 2 =x 1 2 . Эти два решения не сравнимы по модулю *р* >2 , так как из *x* 1 ≡- *x* 1 (mod *p* ) следует 2 *x* 1 ≡0(mod *p* ), т.е. (поскольку *р* ≠2) *x* 1 ≡0(mod *p* ), что невозможно, ибо *а* ≠0.

Поскольку сравнение *x* 2 ≡*a* (mod *p* ) есть сравнение второй степени по простому модулю, то больше двух решений оно иметь не может.

Введя в рассмотрение удобный символ ( ), заменяющий длинную фразу. Этот символ носит теперь фамилию Лежандра и читается: “символ Лежандра а по пэ”.

**Определение.** Пусть *а* не кратно *р* . Тогда символ Лежандра определяется как:

|  |  |
| --- | --- |
|  |  |

Оказывается, что символ Лежандра есть не просто удобное обозначение. Он имеет много полезных свойств и глубокий смысл, уходящий корнями в теорию конечных полей. Далее в этом пункте мы рассмотрим некоторые простейшие свойства символа Лежандра и, прежде всего, научимся его вычислять ( т.е. , тем самым, научимся отвечать на вопрос, проставленный в начале пункта: при каких *а* простейшее двучленное сравнение второй степени имеет решение, а при каких – не имеет ? ).

**Теорема. (Критерий Эйлера)** Пусть *а* не кратно *р* . Тогда:



**Доказательство.**

По теореме Ферма, *ap*-1≡1(mod *p*). В этом сравнении перенесем единицу в левую часть: *ap*-1-1≡0(mod *p*). Поскольку p – простое, а значит нечетное число, значит p-1 – число четное. Тогда можем разложить левую часть сравнения на множители: .

Из множителей в левой части один и только один делится на *p*, то есть либо

 \*, либо  \*\*

Если *а* – квадратичный вычет по модулю *р*, то *а* при некотором *x* удовлетворяет сравнению *a≡x*2(mod *p*) , тогда , а учитывая (по теореме Ферма), что *xp*—1≡1(mod *p*), получаем сравнение (\*).

При этом решения сравнения \* исчерпываются квадратичными вычетами по модулю *р*. Следовательно, если *а* – квадратичный невычет по модулю *р*, то сравнение \* не выполняется, а значит выполняется сравнение \*\*.

**Свойство 1.** Если *a* ≡*b* (mod *p* ), то 

Это свойство следует из того, что числа одного и того же класса по модулю *р* будут все одновременно квадратичными вычетами либо квадратичными невычетами.

**Свойство 2.** 

Доказательство очевидно, ведь единица является квадратом.

**Свойство 3**. 

Доказательство свойства следует из критерия Эйлера при а=-1. Так как (р-1)/2 четное, если р вида 4n+1, и нечетное, если р вида 4n+3, то число -1 является квадратичным вычетом по модулю р тогда и только тогда, когда р вида 4n+1

**Свойство 4**.

Действительно,

**Свойство 5**. 

**Свойство 6**., т.е. в числителе символа Лежандра можно отбросить квадратный множитель.

Действительно,

**Примеры:**



10 – квадратичный вычет по модулю 13.



 .

1350 не является квадратичным вычетом по модулю 1381.

* 1. СИМВОЛ ЯКОБИ

Пусть *n* – составное число, каноническое разложение которого есть . Положим (*a*,*n*)=1. Тогда символ Якоби определяется равенством:

**Свойства символа Якоби:**

1. *a*≡*a*1(mod *n*)  

2. 

3. 

4. 

5. 

6. 3акон взаимности:

(*n*,*m*)=1, *n*, *m*>0, *n*, *m* — нечетные числа  

Эти свойства нетрудно доказать, воспользовавшись определением символа Якоби и свойствами символа Лежандра.

Очевидно, для символа Якоби выполняются те же свойства, что и для символа Лежандра, за исключением только критерия Эйлера. Критерий Эйлера для символа Якоби не выполняется.

Приведенные свойства символа Якоби позволяют составить **алгоритм для вычисления символа Якоби и символа Лежандра**:

1. Выделяем из числителя все степени двойки:



1. Пользуясь св-вом 4, понижаем степень *k*:



1. Если *k* mod 2=1, то вычисляем пользуясь свойством 5.
2. Символ преобразуем, пользуясь законом взаимности, и затем приводим числитель *m* по модулю знаменателя *n*1 и повторяя для получившегося символа Якоби шаги 1-4, пока в числителе не останется 1 или —1.

В более формализованном виде алгоритм выглядит следующим образом:

**Алгоритм вычисления символа Якоби:**

Вход: *n* - числитель, *m* – знаменатель символа Якоби. *m* – нечетное число,

 *n*, *m*>0, *s*=1.

Ш.1: Если (*n*,*m*)≠1, то *s*:=0. Идти на Выход.

Ш.2: *n*:=*n* mod *m*. Ш.3.

Ш.3: Представить *n* как *n*=2*kn*1 . *k*:=*k* mod 2, *n*:=*n*1.

Ш.4: Если *k*=1, то если *m* mod 8 = 3 или *m* mod 8 = 5, то *s*:=—*s* .

Ш.5: Если n=1, то идти на Выход.

Ш.6: Если *n=m*—1, и *m* mod 4 = 1, то идти на Выход.

 Если *n=m*—1, и *m* mod 4 = 3, то *s*:=—*s.* Идти на Выход.

Ш.7: *n↔m*. *s*:=*s*·(—1) . Идти на Ш.2.

Выход. *s* – символ Якоби.

Пример:



.

Вычислить, пользуясь свойствами символа Якоби:

a); c); e) ; g) ; i) ; k) ;

b); d); f) ; h) ; j) ; l) .

2.10 КВАДРАТИЧНЫЕ СРАВНЕНИЯ ПО ПРОСТОМУ МОДУЛЮ

Пусть дано сравнение *x*2≡*a*(mod *p*), *p*>2 – простое и .

Данное сравнение имеет 2 решения. Укажем, как найти эти решения.

Для *p* возможны следующие случаи:

а)Пусть *p*≡3(mod 4), т.е. *p*=4*k*+3.

По критерию Эйлера, . Подставляя сюда *p*, получим



*a*2*k*+1≡1(mod *p*)

*a*2*k*+2≡*a*(mod *p*)

Вернувшись сравнению, которое требуется решить, заметим, что *x*2≡*a*2*k*+2(mod *p*), и тогда *x*≡±*ak*+1(mod *p*) – искомое решение.

б) *p*≡5(mod 8), т.е. *p*=8*k*+5.

Найдем какой-нибудь квадратичный невычет по модулю p. Согласно св-ву 7 для символа Лежандра, таким невычетом в случае *p*=8*k*+5 будет являться «2». Тогда, согласо критерию Эйлера, 24k+2≡—1(mod *p*).

Так как a – квадратичный вычет по модулю p, то по критерию Эйлера,   .

Тогда возможны два варианта: *a*2*k*+1≡1(mod *p*) или *a*2*k*+1≡—1(mod *p*).

В первом случае дальнейшие рассуждения проводим как в пункте а, и получаем *x*≡±*ak*+1(mod *p*).

Рассмотрим подробнее второй случай. Имеем:

*a*2*k*+1≡—1(mod *p*)

Для того, чтобы избавиться от знака (—) в правой части, домножим левую часть этого сравнения на 24k+2, а левую – на –1.

24*k*+2*a*2*k*+1≡1(mod *p*)

24*k*+2*a*2*k*+2≡*a*(mod *p*)

*x*≡±22*k*+1*ak*+1(mod *p*)

Таким образом, имеются два кандидата на решение:

*x*≡±*ak*+1(mod *p*).

*x*≡±22*k*+1*ak*+1(mod *p*)

Вычислив и подставив каждое из них в исходное сравнение, выберем ту пару, которая удовлетворяет исходному сравнению.

в) *p*≡9(mod 16), т.е. *p*=16*k*+9.

Найдем *N* – какой-нибудь квадратичный невычет по модулю *p*. Тогда по критерию Эйлера, .

С другой стороны, поскольку *a* – квадратичный вычет по модулю *p*, то по критерию Эйлера,   .

Тогда возникают два случая: *a*4*k*+2≡1(mod *p*) или *a*4*k*+2≡-1(mod *p*).

Рассмотрим первый случай: *a*4*k*+2≡1(mod *p*). Поскольку показатель степени в левой части сравнения – четный, то вновь возникают два варианта: *a*2*k*+1≡1(mod *p*) или *a*2*k*+1≡—1(mod *p*), первый из которых приводит, как ранее, к кандидату в решение *x*≡±*ak*+1(mod *p*), а второй вариант, рассуждая как в пункте б, приведем к кандидату в решения *x*≡±*N*4*k*+2*ak*+1(mod *p*).

Рассмотрим второй случай: *a*4*k*+2≡-1(mod *p*). Для того, чтобы избавиться от знака (—) в правой части сравнения, домножим правую часть на *N*8*k*+4, а левую – на –1. Получим *N*8*k*+4*a*4*k*+2≡1(mod *p*). Поскольку показатели степеней в левой части получившегося сравнения четны, то отсюда возникают два варианта: *N*4*k*+2*a*2*k*+1≡1(mod *p*) или *N*4*k*+2*a*2*k*+1≡-1(mod *p*).

Рассмотрим первый из вариантов:

*N*4*k*+2*a*2*k*+1≡1(mod *p*)

*N*4*k*+2*a*2*k*+2≡*a*(mod *p*)

*x*≡±*N*2*k*+1*ak*+1(mod *p*).

Рассмотрим второй из вариантов:

*N*4*k*+2*a*2*k*+1≡-1(mod *p*)

*N*12*k*+6*a*2*k*+1≡1(mod *p*)

*N*12*k*+6*a*2*k*+2≡*a*(mod *p*)

*x*≡±*N*6*k*+3*ak*+1(mod *p*)

Итак, получили четыре пары – кандидата на решение:

*x*≡±*ak*+1(mod *p*)

*x*≡±*N*2*k*+1*ak*+1(mod *p*)

*x*≡±*N*4*k*+2*ak*+1(mod *p*)

*x*≡±*N*6*k*+3*ak*+1(mod *p*)

Вычислив и подставив в исходное сравнение, выберем ту пару, которая удовлетворяет исходному сравнению.

Рассмотренным способом можно построить решение для любого простого модуля *p*. Если *p*=2*hk*+2*h*—1+1, то при решении сравнения возникнет 2*h*—2 пар – кандидатов в решение, каждая из которых будет иметь вид *x*≡±*Nz*(2*k*+1)*ak*+1(mod *p*), где .

 Главная проблема здесь – отыскание квадратичного невычета *N*, но поскольку, как было доказано ранее, квадратичных вычетов и невычетов по простому модулю – одинаковое количество, то невычет обязательно найдется.

**Пример**:

Решить сравнение x2≡8(mod 17).

17 – простое число. Выясним, имеет ли данное сравнение решение:

. Сравнение имеет 2 решения. Отыщем их.

17=2·8+1=4·4+1=8·2+1=16·1+1=32·0+17=25·0+17.

*h*=5, *k*=0. Имеется 23=8 пар-кандидатов в решения.

Найдем какой-нибудь невычет по модулю 17:

.

Итак, *N*=3 – кв. невычет по модулю 17.

Имеются следующие кандидаты в решения сравнения:

1) *x*≡±8(mod 17) 5) *x*≡±*3*48(mod *p*)

2) *x*≡±3·8(mod 17) 6) *x*≡±*3*58(mod *p*)

3) *x*≡±328(mod 17) 7) *x*≡±*3*68(mod *p*)

4) *x*≡±338(mod 17) 8) *x*≡±*3*78(mod *p*)

Будем проверять каждую пару решений, пока не найдем верное решение.

1) *x*≡±8(mod 17). Тогда *x*2≡64≡13(mod 17).

2) *x*≡±3·8≡±24≡±7(mod 17). Тогда *x*2≡49≡15(mod 17).

3) *x*≡±328≡±72≡±4(mod 17). Тогда *x*2≡16(mod 17).

4) *x*≡±338≡±216≡±12(mod 17). Тогда *x*2≡144≡8(mod 17).

Ответ: *x*≡±12(mod 17), или *x*≡±5(mod 17).

**ЗАДАНИЯ**

Решить следующие квадратичные сравнения по простому модулю, если решение существует.

a) *x*2≡17(mod 19); d) *x*2≡2 (mod 7); g) *x*2≡3 (mod 41);

b) *x*2≡3 (mod 13); e) *x*2≡3 (mod 11); h) *x*2≡2 (mod 17);

c) *x*2≡8 (mod 41); f) 2*x*2≡10 (mod 11); i) 3*x*2≡15(mod 31).

* 1. КВАДРАТИЧНЫЕ СРАВНЕНИЯ ПО СОСТАВНОМУ МОДУЛЮ

Рассмотрим сравнение вида *x*2≡*a*(mod *p*α), где *p* – простое нечетное число. Как было показано в п.4 §4, решение этого сравнения можно отыскать, решив сравнение *x*2≡*a*(mod *p*). Причем сравнение *x*2≡*a*(mod *p*α) будет иметь два решения, если *a* является квадратичным вычетом по модулю *p*.

**Пример:**

Решить квадратичное сравнение *x*2≡86(mod 125).

125 = 53, 5 – простое число. Проверим, является ли 86 квадратом по модулю 5.

. Исходное сравнение имеет 2 решения.

Найдем решение сравнения *x*2≡86(mod 5).

*x*2≡1(mod 5).

Это сравнение можно было бы решить способом, указанным в предыдущем пункте, но мы воспользуемся тем, что квадратный корень из 1 по любому модулю есть ±1, а сравнение имеет ровно два решения. Таким образом, решение сравнения по модулю 5 есть

*x*≡±1(mod 5) или, иначе, *x*=±(1+5*t*1).

Подставим получившееся решение в сравнение по модулю 52=25:

*x*2≡86(mod 25)

*x*2≡11(mod 25)

(1+5*t*1)2≡11(mod 25)

1+10 *t*1+25 *t*12≡11(mod 25)

10 *t*1≡10(mod 25)

2 *t*1≡2(mod 5)

*t*1≡1(mod 5), или, что то же самое, *t*1=1+5*t*2.

Тогда решение сравнения по модулю 25 есть *x*=±(1+5(1+5*t*2))=±(6+25*t*2). Подставим получившееся решение в сравнение по модулю 53=125:

*x*2≡86(mod 125)

(6+25*t*2)2≡86(mod 125)

36+12·25*t*2+625*t*22≡86(mod 125)

12·25*t*2≡50(mod 125)

12*t*2≡2(mod 5)

2*t*2≡2(mod 5)

*t*2≡1(mod 5), или *t*2=1+5*t*3.

Тогда решение сравнения по модулю 125 есть *x*=±(6+25(1+5*t*3))=±(31+125*t*3).

Ответ: *x*≡±31(mod 125).

Рассмотрим теперь сравнение вида *x*2≡*a*(mod 2α). Такое сравнение не всегда имеет два решения. Для такого модуля возможны случаи:

1. α=1. Тогда сравнение имеет решение только тогда, когда *a*≡1(mod 2), и решением будет *x*≡1(mod 2) (одно решение).
2. α=2. Сравнение имеет решения только тогда, когда *a*≡1(mod 4), и решением будет *x*≡±1(mod 4) (два решения).
3. α≥3. Сравнение имеет решения только тогда, когда *a*≡1(mod 8), и таких решений будет четыре. Сравнение *x*2≡*a*(mod 2α) при α≥3 решается так же, как сравнения вида *x*2≡*a*(mod *p*α), только в качестве начального решения выступают решения по модулю 8: *x*≡±1(mod 8) и *x*≡±3(mod 8). Их следует подставить в сравнение по модулю 16, затем по модулю 32 и т. д. вплоть до модуля 2α.

**Пример:**

Решить сравнение *x*2≡33(mod 64)

64=26. Проверим, имеет ли исходное сравнение решения. 33≡1(mod 8), значит сравнение имеет 4 решения.

По модулю 8 эти решения будут: *x*≡±1(mod 8) и *x*≡±3(mod 8), что можно представить как *x*=±(1+4*t*1). Подставим это выражение в сравнение по модулю 16

*x*2≡33(mod 16)

(1+4*t*1)2≡1(mod 16)

1+8*t*1+16*t*12≡1(mod 16)

8*t*1≡0 (mod 16)

*t*1≡0 (mod 2)

Тогда решение примет вид *x*=±(1+4*t*1)=±(1+4(0+2*t*2))=±(1+8*t*2). Подставим получившееся решение в сравнение по модулю 32:

*x*2≡33(mod 32)

(1+8*t*2)2≡1(mod 32)

1+16*t*2+64*t*22≡1(mod 32)

16*t*2≡0 (mod 32)

*t*2≡0 (mod 2)

Тогда решение примет вид *x*=±(1+8*t*2) =±(1+8(0+2t3)) =±(1+16*t*3). Подставим получившееся решение в сравнение по модулю 64:

*x*2≡33(mod 64)

(1+16*t*3)2≡33(mod 64)

1+32*t*3+256*t*32≡33(mod 64)

32*t*3≡32 (mod 64)

*t*3≡1 (mod 2)

Тогда решение примет вид *x*=±(1+16*t*3) =±(1+16(1+2t4)) =±(17+32*t*4). Итак, по модулю 64 исходное сравнение имеет четыре решения: *x*≡±17(mod 64)и *x*≡±49(mod 64).

Теперь рассмотрим сравнение общего вида: *x*2≡*a*(mod *m*), (*a*,*m*)=1,  - каноническое разложение модуля *m*. Согласно Теореме из п.4 §4, данному сравнению равносильна система



Если каждое сравнение этой системы разрешимо, то разрешима и вся система. Найдя решение каждого сравнения этой системы, мы получим систему сравнений первой степени, решив которую по китайской теореме об остатках, получим решение исходного сравнения. При этом количество различных решений исходного сравнения (если оно разрешимо) есть 2*k*, если α=1, 2*k*+1, если α=2, 2*k*+2, если α≥3.

**Пример:**

Решить сравнение *x*2≡4(mod 21).

21 – составное число. Факторизуем его: 21=3·7. Проверим разрешимость исходного сравнения:

, . Сравнение разрешимо и имеет 22=4 решения.

Составим систему: . Решим каждое из уравнений этой системы. Получим . Итак, имеем 4 системы:

1)  2)  3)  4)

Решая каждую из этих систем по китайской теореме об остатках, получим четыре решения: *x*≡±2(mod 21), *x*≡±5(mod 21).

**ЗАДАНИЯ**

**1**. Решить следующие квадратичные сравнения по составному модулю, если решение существует.

a) *x*2≡7(mod 9); g) *x*2≡1 (mod 32); m) *x*2≡11 (mod 35);

b) *x*2≡-1(mod 25); h) *x*2≡67 (mod 81); n) *x*2≡5 (mod 12);

c) *x*2≡32(mod 49); i) *x*2≡59 (mod 125); o) *x*2≡9 (mod 20);

d) *x*2≡1(mod 4); j) *x*2≡4(mod 6); p) *x*2≡31 (mod 105);

e) *x*2≡3(mod 8); k) *x*2≡1(mod 15); q) *x*2≡4 (mod 105);

f) *x*2≡9(mod 16); l) *x*2≡1(mod 24); r) *x*2≡ 16 (mod 75).

**2**. Определить, сколько решений имеют сравнения.

a) *x*2≡—1(mod 59); d) *x*2≡ 17(mod 32); g) x2≡1(mod 150);

b) *x*2≡ 3(mod 83); e) *x*2≡ 25(mod 96); h) x2≡4(mod 343);

c) *x*2≡ 1(mod 8); f) *x*2≡ 2(mod 315); i) x2≡1(mod 2).

#### ЛИТЕРАТУРА

1. С.В. Сизый. Лекции по теории чисел: Учебное пособие для математических специальностей. Екатеринбург: Уральский государственный университет им. А. М. Горького, 1999
2. И. М. Виноградов. "Основы теории чисел". М., Наука, 1981.
3. А. Б. Шидловский. "Трансцендентные числа". М., Наука, 1987.
4. А. Я. Хинчин. "Цепные дроби". М., Гос. Изд-во Физ.-Мат. Лит., 1961.
5. А. А. Карацуба. "Основы аналитической теории чисел". М., Наука, 1975.
6. В. Боро, Д. Цагир, Ю. Рольфс, Ч. Крафт, Е. Янцен. "Живые числа". М., Мир, 1985.
7. Д. Кнут. "Искусство программирования для ЭВМ", том 2 - "Получисленные алгоритмы". М., Мир, 1977.
8. Д. Я. Стройк. "Краткий очерк истории математики". М., Наука, 1990.
9. Ф. Клейн. "Элементарная математика с точки зрения высшей". М., Наука, 1987.
10. Н. И. Фельдман. "Седьмая проблема Гильберта". Изд-во МГУ, 1982.
11. Д. Пойа. "Математика и правдоподобные рассуждения". М., Наука, 1975.
12. Г. Вилейтнер. "История математики от Декарта до середины ХIX столетия". М., Наука, 1966.
13. Ж. П. Серр. "Курс арифметики". М., Мир, 1982.
14. А. И. Маркушевич. "Краткий курс теории аналитических функций". М., Наука, 1978.
15. Д. О. Шклярский, Н. Н. Ченцов, И. М. Яглом. "Избранные задачи и теоремы элементарной математики". М., Наука, 1976.
16. С. В. Сизый, В. Б. Савинов, Е. Л. Сафронович, Л. Ф. Спевак, М. В. Дунаев. "Книжка, прочитанная вслух". Екатеринбург, УрГУ, 1995.
17. Р. Грэхем. "Начала теории Рамсея". М., Мир, 1984.

Учебное издание

КУРАНОВА Наталья Юрьевна

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Учебное пособие

*Издается в авторской редакции*

Подписано в печать 30.08.19

Формат 60×84/16. Усл. печ. л. 5. Тираж 50 экз.

Заказ

Издательство

Владимирского государственного университета

имени Александра Григорьевича и Николая Григорьевича Столетовых.

600000, Владимир, ул. Горького, 87.