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
доцент кафедры специальной техники и информационных технологий
Владимирского юридического института
Федеральной службы исполнения наказаний
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.

Представлены следующие разделы теории чисел: теория делимости целых чисел, цепные дроби, мультипликативные функции, теория сравнений. Предложены задания, содержащие типовые примеры их решения.

Предназначено для студентов высших учебных заведений, обучающихся по математическим специальностям, а также может быть полезно при изучении спецкурсов по криптографии. Некоторые темы будут интересны учащимся старших классов средней школы.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Библиогр.: 17 назв.

УДК 511.2
ББК 22.13

ISBN 978-5-9984-0959-2

ВВЕДЕНИЕ

Определить достоверно, когда зародилась теория чисел, не представляется возможным. Однако точно установлено: сегодня древнейшим, но не единственным документом, свидетельствующим об интересе древних к теории чисел, является небольшой обломок глиняной таблички, датируемой 1800 г. до н. э. На ней изображен 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 предполагают ученые.

История становления и развития теории чисел связана с именами таких выдающихся ученых, как Евклид, Паскаль, Ферма, Эйлер, Гаусс, Лагранж, Абель и 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 др.

Курс теории чисел содержит значительное число задач, исторических 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, ученые вывели теорию на новый, более высокий уровень, охватывающий множество областей. Поиск новых доказательств привел 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. Рассмотрены такие вопросы, как простые и составные числа, арифметические функции, теория сравнений, цепные дроби, диофантовы уравнения. В каждой главе приводятся теория, примеры и задачи для самостоятельного решения.

Издание предназначено для подготовки бакалавров по направлению 44.03.05 – Педагогическое образование.

Глава 1. ТЕОРИЯ ДЕЛИМОСТИ

1.1. Делимость целых чисел. Деление с остатком

Определение. Пусть a, $b \in \mathbf{Z}$. Число a делится на число b если найдется такое число $q \in$, что $a = qb$. Синонимы: a кратно b; b – делитель a.

Теорема. Для данного целого отличного от нуля числа b, всякое целое число a единственным образом представимо в виде $a = bq + r$, где $0 \leq r < |b|$.

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

Тогда, очевидно, $0 \leq r < |b|$. Докажем единственность такого представления. Ну пусть $a = bq + r$ и $a = bq_1 + r_1$ — два таких представления. Значит $0 = a - a = b\,(q - q_1) + (r - r_1)$. Здесь 0 делится на b; $b\,(q - q_1)$ делится на b, следовательно $(r - r_1)$ обязано делиться на b. Так как $0 \leq$ $\leq r < b$ и $0 \leq r_1 < b$, 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 a на b.

Широкое практическое значение имеют следующие свойства:

- *Если остаток от деления a_1 на b равен r_1, а остаток от деления a_2 на b равен r_2, то остаток от деления $a_1 + a_2$ на b равен остатку от деления $r_1 + r_2$ на b.*
- *Если остаток от деления a_1 на b равен r_1, а остаток от деления a_2 на b равен r_2, то остаток от деления $a_1 \cdot a_2$ на b равен остатку от деления $r_1 \cdot r_2$ на b.*

Пример 1. Докажите, что квадрат целого числа не может иметь вид $4k + 2, k \epsilon Z$

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

Рассмотрим всевозможные остатки квадратов целых чисел при делении на 4

$\boldsymbol{a}$	0	1	2	3
$\boldsymbol{a^2}$	0	1	0	1

Квадраты целых чисел при делении на 4 могут иметь лишь остатки 0 или 1. А потому они не могут иметь вид 4k + 2.

Пример 2. Докажите, что сумма кубов трех последовательных целых чисел делится на 3.

Доказать этот факт можно разными способами. Применим подход, использованный выше. Составим таблицу остатков для трех последовательных чисел $f(a) = a^3 + (a+1)^3 + (a+2)^3$

a	a^3	a+1	$(a+1)^3$	a+2	$(a+2)^3$	$f(a)$
0	**0**	1	**1**	2	**2**	0
1	**1**	2	**2**	0	**0**	0
2	**2**	0	**0**	1	**1**	0

В последнем столбце получен остаток ноль, что означает делимость без остатка на 3 суммы кубов трех последовательных целых чисел.

Нетрудно доказать следующие утверждения:

- Остаток от деления на 3 числа 5^k равен 1, если k четно, и 2, если k нечетно.
- Квадрат любого натурального числа или делится на 2 (на 4), когда само число чётное, или при делении на 2 (на 4) даёт в остатке 1.
- Квадрат любого натурального числа или делится на 3, когда на 3 делится само число, или при делении на 3 даёт в остатке 1.
- Квадрат любого натурального числа или делится на 5, когда на 5 делится само число, или при делении на 5 даёт в остатке 1 или 4.
- Квадрат любого натурального числа или делится на 7, когда на 7 делится само число, или при делении на 7 даёт в остатке 1, 2 или 4.
- Разность квадратов двух целых чисел одинаковой чётности делится на 4.
- Число 4^n при делении на 3 дает в остатке 1.
- Число 5^{2n} при делении на 3 дает в остатке 1, а 5^{2n+1} дает в остатке 2.
- При делении на 3 куб целого числа и само число дают одинаковые остатки (0, 1, 2).
- При делении на 9 куб целого числа дает в остатке 0, 1, 8.
- При делении на 4 куб целого числа дает в остатке 0, 1, 3.
- Число N^5 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

a	a^2	a^3
0	0	0
1	1	1
2	1	2

d=4

a	a^2	a^3
0	0	0
1	1	1
2	0	0
3	1	3

d=5

a	a^2	a^3
0	0	0
1	1	1
2	4	3
3	4	2
4	1	4

d=6

a	a^2	a^3
0	0	0
1	1	1
2	4	2
3	3	3
4	4	4
5	1	5

d=7

a	a^2	a^3
0	0	0
1	1	1
2	4	1
3	2	6
4	2	1
5	4	6

d=8

a	a^2	a^3
0	0	0
1	1	1
2	4	0
3	1	3
4	0	0
5	1	5
6	4	0
7	1	7

d=9

a	a^2	a^3
0	0	0
1	1	1
2	4	8
3	0	0
4	7	1
5	7	8
6	0	0
7	4	1
8	1	8

ЗАДАНИЯ

1. Может ли число 200...009 быть квадратом целого числа при каком-либо количестве нулей?
2. Может ли число 100...004 быть квадратом целого числа?
3. Может ли число 100…050…01 быть кубом целого числа?

4. На какие цифры может оканчиваться квадрат целого числа?

5. Может ли квадрат целого числа иметь вид:

a) 5q + 2,

b) 3q − 1,

c) 6q − 1?

6. Существует ли натуральное число N такое, что $\boldsymbol{N^2}$ + 1 делится на 3? $\boldsymbol{N^3}$ + 3 делится на 99.

7. Докажите, что если $\boldsymbol{x^2 + y^2}$ делится на 3 (x, y — целые), то x и y делятся на 3.

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

9. a, b, c — натуральные числа, причем a + b + c делится на 6. Докажите, что $\boldsymbol{a^3 + b^3 + c^3}$ тоже делится на 6

10. Докажите, что $\boldsymbol{a^3 + b^3 + 4}$ не является кубом натурального числа при натуральных a и b

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

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

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

14. 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.

15. Докажите, что уравнения не имеют решений в целых числах:

a) $\boldsymbol{12x + 5 = y^2}$;

b) $\boldsymbol{x^2 - 5y + 3 = 0}$;

c) $\boldsymbol{x^2 + y^2 = 2007}$;

d) $\boldsymbol{a^2 - 3b^2 = 8}$;

e) $\boldsymbol{-x^2 + 7y^3 + 6 = 0}$;

f) $\boldsymbol{15x^2 - 7y^2 = 9}$.

16. Докажите, что для любого целого a:

a) $\boldsymbol{a^{10} - 9a + 8}$ делится на 2;

b) $\boldsymbol{a^5 + 3a^3 - 12}$ делится на 4;

c) $\boldsymbol{a^3 - 7a + 18}$ делится на 6;

d) $\boldsymbol{a^7 - a - 56}$ делится на 7;

e) $\boldsymbol{a^5 - 17a^3 + 24}$ делится на 8.

17. $\boldsymbol{a^9 + 17a^3 - 18}$ делится на 9.

18. Докажите, что при любом натуральном n:

a) $\boldsymbol{25^{n-2} + 5^n - 13^{n+1}}$ делится на 17;

b) $\boldsymbol{12^{2n+1} + 11^{n+2}}$ делится на 133 ;

c) $\boldsymbol{2^{n+2} + 2^{n+1} + 2^n}$ делится на 14;

d) $\boldsymbol{7^{2n} - 4^{2n}}$ делится на 33;

e) $\boldsymbol{5^{2n+1} + 3^{n+2} \cdot 2^{n-1}}$ делится на 19.

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.

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

21. Разделите с остатком:

а) 161 на 17;

б) –161 на 17;

в) 161 на –17;

г) –161 на –17.

22. 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 $d \in \mathbf{Z}$, делящее одновременно числа $a, b, c, ..., k \in \mathbf{Z}$, 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 $\mathbf{P} = \{au + bv;\ u, v \in \mathbf{Z}\}$. Очевидно, что $\mathbf{P} \in \mathbf{Z}$, а знатоки алгебры могут проверить, что $\mathbf{P}$ – идеал в $\mathbf{Z}$. Очевидно, что $a, b, 0 \in \mathbf{P}$. Пусть $x, y \in \mathbf{P}$ и $y \in 0$. Тогда остаток от деления x на y принадлежит $\mathbf{P}$. Действительно:

$$x = yq + r,\ 0 \le r < y,$$

$$r = x - yq = (au_1 + bv_1) - (au_2 + bv_2)\,q = a\,(u_1 - u_2 q) + b\,(v_1 - v_2 q) \in \mathbf{P}.$$

Пусть $d \in \mathbf{P}$ - наименьшее положительное число из $\mathbf{P}$. Тогда a делится на d. В самом деле, $a = dq + r_1$, $0 \le r_1 < d$, $a \in \mathbf{P}$, $d \in \mathbf{P}$, значит, $r_1 \in \mathbf{P}$, следовательно, $r_1 = 0$. Аналогичными рассуждениями получается, что b делится на d, значит, d - общий делитель a и b.

Далее, раз $d \in \mathbf{P}$, то $d = au_0 + bv_0$. Если теперь d_1 - общий делитель a и b, то $d_1 \mid (au_0 + bv_0)$, т.е. $d_1 \mid d$. Значит $d \in d_1$ и d - наибольший общий делитель.

Свойство 1. Для любых целых чисел a и k, очевидно, справедливо: $(a, ka) = a$; $(1, a) = 1$.

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

Доказательство. Пусть $d \mid a$, $d \mid$, тогда $d \mid c$. Пусть $d \mid c$, $d \mid b$, тогда $d \mid a$.

Свойство 3. Пусть a, b и m - произвольные целые числа. Тогда $(am, bm) = m\,(a, b)$.

Доказательство. Если d - наибольший общий делитель чисел a и b , то $dm \mid am$ и $dm \mid bm$, т.е. dm - делитель am и bm. Покажем, что dm - наибольший общий делитель этих чисел. Поскольку d - наибольший общий делитель чисел a 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. $s \le dm$, следовательно, dm - наибольший общий делитель.

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

Доказательство. Пусть $(c, b) = d$. Имеем: $d \mid b$, $d \mid c$, следовательно $d \mid ac$, т.е. d - делитель ac и b. Пусть теперь $(ac, b) = s$. Имеем: $s \mid b$, $s \mid ac$, s - делитель b, т.е. либо $s = 1$, либо s не делит a. Это означает, что $s \mid c$, значит $s \mid d$. 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 $a_1|b$, $a_2|b$, … , $a_n|b$, то b называется общим кратным чисел $a_1,\ldots,a_n$. Наименьшее положительное общее кратное чисел $a_1,\ldots,a_n$ называется их наименьшим общим кратным (**НОК**).

Пусть НОД$(a,b)=d$, тогда можно записать $a=d\cdot a_1$, $b=d\cdot b_1$, где $(a_1,b_1)=1$.

Пусть $a|M$, $b|M \Rightarrow M=ak$ для некоторого целого k, и тогда число $\frac{M}{b}=\frac{ak}{b}=\frac{a_1k}{b_1}$ – целое. Но, поскольку $(a_1,b_1)=1$, то $b_1\backslash k$, и тогда $k=b_1t$ для некоторого $t \in Z$, и

$$M = \frac{ab}{d}t \ .$$

Очевидно, $\forall\ t \in Z$, M – общее кратное a и b дает формулу всех общих кратных.

При $t=1$ имеем M=НОК(a,b).

$$НОК(a,b) = \frac{a \cdot b}{НОД(a,b)}$$

Формулой M = НОК$(a,b)\cdot t$ можно представить все общие кратные чисел a и b. ($t \in Z$).

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; $a \neq 0$, $b \neq 0$, считаем, что $a > b$. Символом **:=** в записи алгоритма обозначаем присваивание. Алгоритм:

1. Ввести a и b .
2. Если $b = 0$, то **Ответ:** a . **Конец**.
3. Заменить r := "остаток от деления a на b ", $a := b$, $b := r$.
4. Идти на **2.**

В современной буквенной записи, кочующей из одного учебника в другой, алгоритм Евклида выглядит так: $a > b$; $a, b \in \mathbf{Z}$.

$$a = bq_1 + r_1 \qquad 0 \le r_1 < b$$
$$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2$$
$$r_2 = r_3 q_4 + r_4 \qquad 0 \le r_4 < r_3$$

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \qquad 0 \le r_{n-1} < r_{n-2}$$
$$r_{n-2} = r_{n-1} q_n + r_n \qquad 0 \le r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1} \qquad r_{n+1} = 0$$

Имеем: $b > r_1 > r_2 > \ldots > r_n > 0$, 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 делителгь a и b делит $r_1, r_2, \ldots, r_n$. Если же просматривать эту цепочку равенств от последнего к первому, то видно, что $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$, и т.д., т.е. r_n делит a и b. Поэтому r_n - наибольший общий делитель чисел a 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:

$$r_n = r_{n-2} - r_{n-1} q_n = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n = \ldots$$

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

$$\ldots = au + bv = (a, b).$$

Пример 1. Пусть $a = 525$, $b = 231$. Воспользуемся алгоритмом 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)

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

Запись того же самого в виде цепочки равенств:

$$525 = 231 \cdot 2 + 63$$
$$231 = 63 \cdot 3 + 42$$
$$63 = 42 \cdot 1 + 21$$
$$42 = 21 \cdot 2$$

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

$$21 = 63 - 42 \cdot 1 = 63 - (231 - 63 \cdot 3) \cdot 1 =$$
$$= 525 - 231 \cdot 2 - (231 - (525 - 231 \cdot 2) \cdot 3) =$$
$$= 525 \cdot 4 - 231 \cdot 9,$$

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

Пример 2. При любом на туральном *n* найдите НОД чисел : $6n^4 + n^2 + 3n$ и $2n^3 + 1$; $6n^6 + 10n^5 + 4n^3 + n$ и $3n^3 + 5n^2 + 2$.

Решение.

По алгоритму Евклида получаем $6n^4 + n^2 + 3n = (2n^3 + 1) \cdot (3n) + n^2$, $2n^3 + 1 = n^2 \cdot (2n) + 1$ и $n^2 = 1 \cdot n^2 + 0$. Таким образом, последний ненулевой остаток алгоритма Евклида равен 1.

Во втором случае, следуя алгоритму Евклида, получаем: $6n^6 + 10n^5 + 4n^3 + n = (3n^3 + 5n^2 + 2) \cdot (2n^3) + n$; $3n^3 + 5n^2 + 2 = n \cdot (3n^2 + 5n) + 2$. Далее, $n = 2k + r$, где $r \in \{0, 1\}$. При $r = 0$, то есть в случае $n = 2k$, последний ненулевой остаток алгоритма Евклида равен 2. При $r = 1$, то есть в случае $n = 2k + 1$, последний ненулевой остаток алгоритма Евклида равен 1.

Пример 3. Сократите дробь: $\frac{6n+4}{22n+15}$; $\frac{16n+60}{11n+41}$

Решение. В первом случае по алгоритму Евклида получаем:

$22n+15=(6n+4)\cdot 3+(4n+3), 6n+4=(4n+3)\cdot 1+(2n+1), 4n+3=(2n+1)\cdot 2+1, 2n+1=1\cdot(2n+1)+0.$ Таким образом, последний ненулевой остаток алгоритма Евклида равен 1, и ((6n+4), (22n+15))=1. То есть дробь $\frac{6n+4}{22n+15}$ несократима.

Во втором случае, следуя алгоритму Евклида, получаем:

$6n+60=(11n+41)+(5n+19), 11n+41=(5n+19)\cdot 2+(n+3), 5n+19=(n+3)\cdot 5+4, n+3=4\cdot k+r,$ где $r\epsilon\{0,1,2,3\}$.

При $r=0$, то есть в случае $n+3=4k$, последний ненулевой остаток алгоритма Евклида равен 4, то есть ((16n+60),(11n+41))=4 при $n=4k-3$ или, то то же, при $n=4t+1$, и дробь сократима на 4:

$$\frac{16n+60}{14n+41}=\frac{16(4t+1)+60}{11(4t+1)+41}=\frac{64t+76}{44t+52}=\frac{16t+19}{11t+12}$$

При $r=1$, то есть в случае $n+3=4k+1$, следующий шаг алгоритма имеет вид 4=1·4+0, и последний ненулевой остаток алгоритма Евклида равен , то есть ((16n+60),(11n+41))=1 при $n=4k-2$ или, то то же, при $n=4t+2$, и дробь несократима

При $r=2$, то есть в случае $n+3=4k+2$, последний ненулевой остаток алгоритма Евклида равен 2, то есть ((16n+60),(11n+41))=2 при $n=4k-1$ или, то то же, при $n=4t+3$, и дробь сократима на 2:

$$\frac{16n+60}{14n+41}=\frac{16(4k-1)+60}{11(4k-1)+41}=\frac{64k+44}{44k+30}=\frac{32k+22}{22k+12}$$

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

Пример 4. Докажите, что для любого натурального a дробь $\frac{a+1}{2a+3}$ несократима.

Предположим, что $(a+1,2a+3)=d$. Тогда разность $(2a+3)-2(a+1)=1$ делится на d. Следовательно $d=1$. Значит дробь $\frac{a+1}{2a+3}$ 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;
h) a = 1600, b = 1120;
d) a =1818, b = 726;
c) a = 175, b = 14945;
g) a = 2448, b = 1632;
f) a = 1763, b = 1634;
b) a = 246, b = 396;
i) a = 2310, b = 3388.
e) a= 6887, b = 6319;

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

$$\frac{12n+5}{6n+3};\ \frac{9n+8}{7n+4};\ \frac{7n+5}{3n+2};\ \frac{21n+4}{14n+3}$$

1.4. Простые числа. «Основная» теорема арифметики

Определение. Число $p \in \mathbf{N}$, $p \neq 1$, называется простым, если p имеет в точности два положительных делителя: 1 и p . 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 $a \in \mathbf{N}$, отличный от 1, есть число простое.

Доказательство. Пусть $c \mid a$, $c \neq 1$ и c – наименьшее с этим свойством. Если существует c_1 такое, что $c_1 \mid c$, то $c_1 \leq c$ и $c_1 \mid a$, следовательно, $c_1 = c$ или $c_1 = 1$.

Свойство 2. Наименьший отличный от 1 делитель составного числа $a \in \mathbf{N}$ не превосходит a.

Доказательство. $c \mid a$, $c \neq 1$, c - наименьший, следовательно $a = ca_1$, $a_1 \mid a$, $a_1 \geq c$, значит $aa_1 \geq c^2 a_1$, $a \geq c^2$ и $c \leq \sqrt{a}$

Теорема Евклида. Простых чисел бесконечно много.

Доказательство. От противного. Пусть $p_1, p_2, ..., p_n$ - все простые, какие только есть. Рассмотрим число $a = p_1 p_2 ... p_n + 1$. Его наименьший отличный от 1 делитель c, будучи простым, не может совпадать ни с одним из $p_1, p_2, ..., p_n$, так как иначе $c \mid 1$. 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 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 $2^{82\,589\,933} - 1$, открытому в рамках проекта 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 p, то оставшиеся невычеркнутые, меньшие p^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 $a > 1$, p_1 - его наименьший простой делитель. Значит,

$a = p_1 a_1$. Если, далее, $a_1 > 1$, то пусть p_2 - его наименьший простой делитель и $a_1 = p_2 a_2$, т.е. $a = p_1 p_2 a_2$, и так далее, пока a_n не станет равным единице. Это обязательно произойдет, так как $a > a_1 > a_2 ...$, 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 p_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 $u, v \in \mathbf{Z}$, 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 $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ – каноническое разложение числа a. Тогда все делители a имеют вид

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdot ... \cdot p_k^{\beta_k}, \text{ где } 0 \le \beta_1 \le \alpha_1,\ 0 \le \beta_2 \le \alpha_2,\ \ldots,\ 0 \le \beta_k \le \alpha_k.$$

Доказательство:

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

Следствие 1

Количество различных делителей числа $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ есть $\prod_{i=1}^{k}(1+\alpha_1)$.

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

Следствие 2

НОД($a_1,\ldots,a_n$), где $a_i = p_1^{\alpha_{i1}} \cdot p_2^{\alpha_{i2}} \cdot \ldots \cdot p_k^{\alpha_{ik}}$ $(i=\overline{1,n})$, есть $p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, где $\beta_j = \min_i(\alpha_{ij})$ ($j=\overline{1,k}$).

Пример 1.

$a_1=2\cdot3\cdot5^2=150$, $a_2=2^2\cdot5\cdot7=140$, $a_3=2^3\cdot5=40$.

$p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$.

$a_1= p_1^1 \cdot p_2^1 \cdot p_3^2 \cdot p_4^0$, $a_2= p_1^2 \cdot p_2^0 \cdot p_3^1 \cdot p_4^1$, $a_3= p_1^3 \cdot p_2^0 \cdot p_3^{21} \cdot p_4^0$.

НОД(a_1,a_2,a_3)= $p_1^1 \cdot p_2^0 \cdot p_3^1 \cdot p_4^0=2\cdot5=10$.

Следствие 3

Совокупность общих делителей $a_1,\ldots,a_n$ совпадает с совокупностью делителей НОД($a_1,\ldots,a_n$).

Следствие 4

$НОК(a_1,\ldots,a_n) = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, где $\gamma_j = \max_i(\alpha_i)$, $j=\overline{1,k}$

Пример 2.

НОК(150,140,40)=$2^2 \cdot 3^1 \cdot 5^2 \cdot 7 = 4200$

Следствие 5

Если $a_1,\ldots,a_n$ – попарно простые числа, то НОК($a_1,\ldots,a_n$)= $a_1\cdot\ldots\cdot a_n$

Следствие 6

Совокупность общих кратных чисел $a_1,\ldots,a_n$ совпадает с совокупностью кратных их наименьшего общего кратного.

Задача 1. Найти натуральное число n такое, что числа n, $n+10$, $n+14$ - простые.

Решение. Если $n>3$, то при делении на 3 в остатке может быть 1 или 2. Если $n=3q+1$, то $n+14=3q+15$ - не простое число, т.к. делится на 3. Если $n=3q+2$, то $n+10=3q+12$ - также не простое число. Поэтому $n=3$, $n+10=13$, $n+14=17$.

Задача 2. Если $p > 3$ - простое число, то его можно представить в виде $6n+1$ или $6n-1$, где n - натуральное число.

Решение. Разделим p на 6 с остатком: $p = 6q + r$. Поскольку p простое число, то остаток не может быть равен 2, 3 и 4. Остаются две возможности: $r = 1$ и $r = 5$. В первом случае $p = 6n+1$, где $n = q$, а во втором случае $p = 6n-1$, где $n = q+1$.

Задача 3. Доказать, что среди чисел вида $2p+1$, где p - простое число, только одно является точным кубом.

Решение. Данное число нечетное, поэтому оно является кубом нечетного числа: $2p+1 = (2n+1)^3$. Раскрывая это соотношение, получаем $p = n(4n^2 + 6n + 3)$. Так как p - простое число, то $n = 1$ и $p = 13$.

Задача 4. Доказать, что при $n > 2$ между числами n и $n!$ содержится по крайней мере одно простое число.

Решение. Если это утверждение неверно, то все простые числа, меньшие $n!$, будут также не больше, чем n. Рассмотрим число $n!-1$. Оно составное и поэтому должно делиться на простые числа, которые не превосходят n. На эти же простые числа делится $n!$. 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 m дают остаток 1, то их произведение при делении на m также дает остаток 1.

Решение. Достаточно доказать это для произведения двух чисел. Пусть $a = m \cdot s + 1$ и $b = m \cdot t + 1$. Тогда $a \cdot b = (m \cdot s + 1) \cdot (m \cdot t + 1) = m \cdot (m \cdot s \cdot t + s + t) + 1$, т.е. частным от деления числа $a \cdot b$ на m будет $(m \cdot s \cdot t + s + t)$, 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 a и b, а длина гипотенузы равна c. По теореме Пифагора $a^2 + b^2 = c^2$. 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 a и b делятся на 3. Аналогично, остаток левой части может быть равен 1 только в том случае, когда одно из чисел a или b делится на 3, а другое не делится. Если же оба числа a и b не делятся на 3, то остаток левой части равен 2, и поэтому соотношение $a^2+b^2=c^2$ невозможно.

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

Доказательство. Все множество натуральных чисел разобьем на три подмножества с общими членами: $3u+1$, $3u+1$, $3u+2$; среди чисел первого подмножества имеется лишь одно простое число 3, остальные простые числа входят в два другие подмножества. Допустим P – наибольшее простое число вида $3n+1$; запишем число $N=3\cdot7\cdot13\cdot19\cdot\ldots\cdot P+1$, где в произведение включено число 3 и все простые числа вида $3n+1$; очевидно, число N будет вида $3n+1$ и, следовательно, $N=3s+1$.

Число N не может быть простым, так как $N>P$, но оно не может иметь простыми делителями число 3 и числа вида $3n+1$; следовательно, все его простые делители вида $3u+2$, откуда $N=3t+2$, но равенство $3t+2=3s+1$ невозможно ни при 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 $3n+1$.

Задача 8. Найти простое число p, чтобы числа вида $2p^2+1$ было тоже простым.

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

ЗАДАНИЯ

1. Разложить на простые множители a и b, найти их НОД и НОК

a) *a=1300; b=38808;*

b) *a=44044; b=3220;*

c) *a=4225; b=22015;*

d) *a=38115; b=359;1*

e) *a=2448; b=2430.*

2. Найти все простые p, для которого

a) $p^2 - 1$;

b) $p^2 - 36$;

c) $p^2 - 324$;

d) $p^2 - 900$

является простым.

3. Докажите методом Евклида, что простых чисел вида a, бесконечно много, где $m \epsilon N$.

a) $a = 4m - 1$;

b) $a = 4m + 3$;

c) $a = 6m + 5$;

d) $a = 3m + 2$;

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 $a, b, c \in \mathbf{Z}$; 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:

$$a_1 d \cdot x + b_1 d \cdot y = c, \text{ т.е. } d \cdot (a_1 x + b_1 y) = c.$$

Ясно, что у такого уравнения имеется решение (пара целых чисел x и y) только тогда, когда $d \mid c$. Поскольку очень хочется решать это уравнение дальше, то пусть $d \mid c$. 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 $x = -\frac{b}{a}y$

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 $t = 0; \pm 1; \pm 2;...$ 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 $c \neq 0$. 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:

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at \end{cases}, \text{где } t \in \boldsymbol{Z}$$

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, проверя-

ется 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:

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at \end{cases}, \text{где } t \in \boldsymbol{Z}$$

$(a , b) = 1$. 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. Решить уравнение $7x + 12y = 43$.

Алгоритм Евклида:

$$12 = 7 \cdot 1 + 5$$
$$7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

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

$$1 = 5 - 2 \cdot 2 = 5 - (7 - 5) \cdot 2 = (12 - 7) - (7 - (12 - 7) \cdot 2) = 12 \cdot 3 + 7 \cdot (- 5),$$

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

$$x_0 = uc = (- 5) \cdot 43 = - 215$$
$$y_0 = vc = 3 \cdot 43 = 129.$$

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:

a) $2x + 7y = 20;$

b) $6x - 21y = 21;$

c) $11x + 99y = 41;$

d) $17x + 25y = 117$

2. 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 *x*.

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

Целой частью действительного числа x называется наибольшее целое число, не превосходящее *x*, т.е. целое число n, такое, что $n \leq x < n + 1$. Целая часть числа обозначается *[x]*. Из определения следует, что *[x]* $\leq$ x $<$ *[x] + 1*.

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

Примеры. [4,8] = 4; [5] = 5; [π] = 3; [-6,29] = -7; [-e] = -3; {7} = 0; {π} = 0,1415…; $\{-\frac{23}{7}\} = \frac{5}{7}$.

Рассмотрим свойства функции целой части действительного числа [x].

Свойства целой части действительного числа

1. Пусть *x* – действительное положительное число, *d* – целое положительное. Число положительных чисел, не превосходящих x и делящихся на *d*, равно $[\frac{x}{\mathrm{d}}]$.

Доказательство

Рассмотрим положительные числа, кратные *d* и непревосходящие *x*; пусть наибольшее из них будет равно *sd*, так что (s + 1)d уже больше,

чем x; число таких чисел d, 2d, 3d, …,sd равно s, где sd $\leq x <$ (s + 1)d, следовательно, s $\leq \frac{x}{d} <$ s + 1, т.е. s $= [\frac{x}{d}]$.

2.Для любого действительного числа $x > 0$ и целого $d > 0$

$$[\frac{[x]}{d}] = [\frac{x}{d}].$$

Доказательство

Между $[x]$ и x нет целых чисел, и поэтому число чисел, кратных d, в сегменте $[1, [x]]$, равное согласно предыдущего свойства $[\frac{[x]}{d}]$, равно также величине $[\frac{x}{d}]$, выражающей число чисел, кратных d в сегменте $[1, x]$.

3. Для любого действительного числа x разность $[x] - 2[\frac{x}{2}]$ может равняться только 0 или 1.

Доказательство

Для любого x имеем $x - 1 < [x] \leq x$, так что $[x] - 2[\frac{x}{2}] \leq x - 2\frac{x}{2} = 0$,

$[x] - 2[\frac{x}{2}] > x - 1 - 2(\frac{x}{2} - 1) = x - 1 - x + 2 = 1$, т.е. целое число $[x] - 2[\frac{x}{2}]$ может равняться только 0 или 1.

4. Пусть p – простое число, $n \geq 1$ целое. Для показателя α наивысшей степени p, делящей n!, имеем:

$\alpha = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \ldots$, т.е. при α, равном сумме (3), p^{α} делитель n!, но $p^{\alpha+1}$ 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 $1 \leq n < N$, где N целое ($N \geq 2$).

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

Если $N \geq$ p, то среди множителей 1, 2,…, N произведения N! число делящихся на p будет равно по свойству 1° $[\frac{N}{p}]$. Произведение всех остальных множителей числа $1 \cdot 2 \ldots N$ обозначим через M. Тогда

$N! = p \cdot 2p \cdot \ldots \cdot [\frac{N}{p}]p \cdot M = p^{[\frac{N}{p}]} \cdot [\frac{N}{p}]!M$, где p не является делителем M. Из $N \geq$ p следует $1 \leq [\frac{N}{p}] < N$.

Так что согласно предположению показатель наивысшей степени p, делящей $[\frac{N}{p}]!$, равен:

$$[\frac{[\frac{N}{p}]}{p}] + [\frac{[\frac{N}{p}]}{p^3}] + \ldots = [\frac{N}{p^2}] + [\frac{N}{p^2}]$$

Из формулы получаем, что наибольший показатель степени p, делящий N!, равен $[\frac{N}{p}] + [\frac{N}{p^2}] + [\frac{N}{p^3}] + \ldots$ 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 3^{α} делитель 1000!

Решение. По формуле (2) имеем:

$$\alpha = \left[\frac{1000}{3}\right] + \left[\frac{1000}{9}\right] + \left[\frac{1000}{27}\right] + \left[\frac{1000}{81}\right] + \left[\frac{1000}{243}\right] + \left[\frac{1000}{729}\right] = 498$$

Так что 3^{498} делитель 1000!, но 3^{499} не является делителем 1000!.

2. Найдем наибольшее α, такое, что 643! делится на 5^{α}

Решение. По формуле (3) имеем:

$$\alpha = \left[\frac{643}{5}\right] + \left[\frac{643}{25}\right] + \left[\frac{643}{125}\right] + \left[\frac{643}{625}\right] = 128 + 25 + 5 + 1 = 159$$

643! делится на 5^{159}

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

Решение. Поскольку $45 = 3^2 \cdot 5$, 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 $\left[\frac{1600}{3}\right] = 533$, а делящихся на 5 равно $\left[\frac{1600}{5}\right] = 320$. Количество чисел, не превосходящих 1600 и делящихся и на 3 и на 5, равно $\left[\frac{1600}{15}\right] = 106$. 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

$$\left[\frac{2012}{2}\right] + \left[\frac{2012}{4}\right] + \left[\frac{2012}{8}\right] + \left[\frac{2012}{16}\right] + \left[\frac{2012}{32}\right] + \left[\frac{2012}{64}\right] + \left[\frac{2012}{128}\right] + \left[\frac{2012}{256}\right] +$$
$$\left[\frac{2012}{512}\right] + \left[\frac{2012}{1024}\right] = 1006 + 503 + 251 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 2004.$$

Показатель степени для 5 равен

$$\left[\frac{2012}{5}\right]+\left[\frac{2012}{25}\right]+\left[\frac{2012}{125}\right]+\left[\frac{2012}{625}\right]=402+80+16+3=501.$$

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

Ответ: 2012! оканчивается 501 нулем.

5. Найти наибольшее натуральное число n, при котором дробь $A=\frac{101\cdot 102\cdot ...\cdot 1000}{7^n}$ является целым числом.

Решение. Данную дробь можно представить в виде $\frac{1000!}{7^n\cdot 100!}$.

Число 7 входит в разложение 1000! с показателем $\left[\frac{1000}{7}\right]+\left[\frac{1000}{49}\right]+\left[\frac{1000}{343}\right]=142+20+2=164$, а в разложение 100! с показателем $\left[\frac{100}{7}\right]+\left[\frac{100}{49}\right]=14+2=16$. Таким образом, для того, чтобы дробь A была целым числом, наибольшее возможное значение n должно быть равно

$$n=164-16=48.$$

Ответ. $n=148$.

6. Решить уравнение $\left[\frac{x}{n}\right]=\left[\frac{x}{n+1}\right]$, где n - натуральное число, и найти количество целочисленных решений.

Решение. При $x>0$ имеет место неравенство $\frac{x}{n+1}<\frac{x}{n}$. Пусть $\left[\frac{x}{n}\right]=k\geq 0$. Тогда из условия задачи получаем неравенство $k\leq\frac{x}{n+1}<\frac{x}{n}<k+1$, из которого следует $k\cdot(n+1)\leq x<n\cdot(k+1)$. Последнее неравенство возможно только при $k<n$.

Рассмотрим решение этого неравенства при различных значениях числа k.

k	x	Целочисленные решения	Количество целочисленных решений
0	$0 \le x < n$	$0,1,2,\ldots,\ n-1$	n
1	$n+1 \le x < 2n$	$n+1, n+2, \ldots, 2n-1$	$n-1$
2	$2n+2 \le x < 3n$	$2n+2, 2n+3, \ldots, 3n-1$	$n-2$
……	……	……	……
$n-2$	$n^2-n-2 \le x < n^2-n$	n^2-n-2, n^2-n-1	2
$n-1$	$n^2-1 \le x < n^2$	n^2-1	1

Пусть теперь $\left[\frac{x}{n}\right] = k < 0.$ Тогда из условия задачи получаем неравенство $k \le \frac{x}{n} < \frac{x}{n+1} < k+1$, из которого следует $k \cdot n \le x < (k+1)\cdot(n+1)$. Последнее неравенство возможно только при $k > -(n+1)$.

Рассмотрим решение этого неравенства при отрицательных значениях числа k.

k	x	Целочисленные решения	Кол-во целочисленных решений
-1	$-n \le x < 0$	$-n, -n+1, \ldots, -1$	n
-2	$-2n \le x < -(n+1)$	$-2n, -2n+1, \ldots, -(n+2)$	$n-1$
……	……	……	……
$-n+1$	$n^2+n \le x < -n^2+n+2$	$-n^2+n, -n^2+n+1$	2
$-n$	$-n^2 \le x < n^2+1$	$-n^2$	1

В итоге общее количество целочисленных решений равно $n(n+1)$.

Ответ. Количество целочисленных решений равно $n(n+1)$.

ЗАДАНИЯ

1. Найти каноническое разложение числа *n!*

a) *n=16;*
b) *n=32;*

c) *n=46;*
d) *n=19;*
e) *n=29;*

2. Сколькими нулями заканчивается число *n*! ?

a) *n=160;*
b) *n=264;*
c) *n=167;*
d) *n=234*

3. Найти количество чисел в промежутке $[19; 1000]$, делящихся на 5; 7; 10
4. Найти количество чисел в промежутке $[1; 1000]$, не делящихся ни на одно из чисел : 3, 5, 7

1.6.2. Число и сумма делителей натуральных чисел

Рассмотрим числовые функции число делителей $\boldsymbol{\tau(n)}$ и сумма делителей $\boldsymbol{\sigma(n)}$ натурального числа.

Определение. Число делителей $\boldsymbol{\tau(n)}$ определяется как число положительных делителей натурального n, а сумма делителей $\boldsymbol{\sigma(n)}$ определяется как сумма положительных делителей n, т.е.

$$\tau(n) = \sum_{d/n} 1, \qquad \sigma(n) = \sum_{d/n} d$$

Примеры

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

Заметим, что если p простое, то $\tau(p) = 2$

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

Рассмотрим основные свойства этих функций.

1. Если $p_1{}^{\alpha_1}\, p_2{}^{\alpha_2} \ldots p_k{}^{\alpha_k}$ - каноническое разложение натурального числа, то

$$\tau(p_1{}^{\alpha_1}\, p_2{}^{\alpha_2} \ldots p_k{}^{\alpha_k}) = (\alpha_1+1)\,(\alpha_2+1) \ldots (\alpha_k+1)$$

Доказательство

Любой положительный делитель числа n = $p_1{}^{a_1}.\ p_2{}^{a_2}\ldots p_k{}^{a_k}$ имеет вид $p_1{}^{\beta_1}.p_2{}^{\beta_2}\ldots p_k{}^{\beta_k}$, где $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, …, $0 \le \beta_k \le \alpha_k$,и, таким образом, число положительных делителей n равно числу наборов (β_1,β_2,…,β_k), где β_1 принимает α_1+1 значение от 0 до α_1, β_2 принимает α_2+1 значение от 0 до α_2,..., β_k принимает α_k+1 значений от 0 до α_k. Число таких наборов равно (α_1+1) (α_2+1)… (α_k+1), т. е.

$$\tau(p_1{}^{\alpha_1}\ p_2{}^{\alpha_2}\ldots p_k{}^{\alpha_k}) = (\alpha_1+1)\ (\alpha_2+1)\ldots\ (\alpha_k+1).$$

Примеры

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

τ(1000000) = τ($2^6 \cdot\ 5^6$) = 7 · 7 = 49,
τ(48510) = τ($2\ \cdot 3^2\ \cdot 5\ \cdot 7^2 \cdot 11$) = 2 · 3 · 2 · 3 · 2 = 72.

2°. Если $p_1{}^{\alpha_1}\ p_2{}^{\alpha_2}\ldots p_k{}^{\alpha_k}$ - каноническое разложение натурального числа, то

$$\sigma(p_1{}^{\alpha_1}\ p_2{}^{\alpha_2}\ \ldots p_k{}^{\alpha_k}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot\cdot\ \frac{p_2^{\alpha_2+1}-1}{p_2-1}\ \cdot \ldots \cdot$$

Доказательство

$$\sigma(p_1{}^{\alpha_1}\ p_2{}^{\alpha_2}\ \ldots p_k{}^{\alpha_k}) = \sum_{d\,|\,p_1{}^{\alpha_1}\ p_2{}^{\alpha_2}\ldots p_k{}^{\alpha_k}} d = \sum_{\substack{0 \le \beta_1 \le \alpha \\ \cdots\cdots\cdots \\ 0 \le \beta_2 \le \alpha_2}} p_1{}^{\beta_1}.p_2{}^{\beta_2}\ \ldots p_k{}^{\beta_k} =$$

$$=\left(1 + \mathrm{p}_1 + \mathrm{p}_1^2 + \cdots + \mathrm{p}_1^{\alpha_1}\right) \cdot \left(1 + \mathrm{p}_2 + \mathrm{p}_2^2 + \cdots + \mathrm{p}_2^{\alpha_2}\right) \cdot$$
$$\cdots \cdot (1+p_k+p_k{}^2+p_k{}^{\alpha_k}).\ (4)$$

Действительно, перемножая числа, стоящие в скобках, в правой части, мы получим слагаемые вида $p_1{}^{\beta_1}.p_2{}^{\beta_2}\ldots p_k{}^{\beta_k}$, где β_1 принимает значение от 0 до α_1, β_2 принимает значение от 0 до α_2,..., β_k принимает значений от 0 до α_k, 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: $1+ p_{\mathrm{I}} + p_{\mathrm{I}}^2 + p_{\mathrm{I}}^{\alpha_{\mathrm{I}}} = \dfrac{p_{\mathrm{I}}^{\alpha_{\mathrm{I}}+1}-1}{p_{\mathrm{I}}-1}$

Пример

$\sigma(19800) = \sigma(2^3 \cdot 3^2 \cdot 5^2 \cdot 11) = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^3-1}{5-1} \cdot \frac{11^2-1}{11-1} = 72540.$

σ (504) = σ ($2^3.3^2.7^1$) = $\frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{7^2-1}{7-1} = 1560.$

3°.Числовые функции - число делителей $\tau(n)$ и сумма делителей $\sigma(n)$ натурального числа - мультипликативные функции.

Доказательство

Если a = ${p_1}^{\alpha_1}\ldots{p_k}^{\alpha_k}$ и b = ${q_1}^{\beta_1}\ldots{q_s}^{\beta_s}$ – каноническое разложение взаимно простых чисел a и b (все p_i и q_j - простые числа), то ${p_1}^{\alpha_1}\ldots{p_k}^{\alpha_k}\ {q_1}^{\beta_1}\ldots{q_s}^{\beta_s}$ - каноническое разложение a b и τ(ab) = (α_1+1) … (α_k+1) (β_1+1) … (β_s+1) = = τ(a)τ(b),

$$\sigma(\mathrm{ab}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}\cdot\frac{q_1^{\beta_k+1}-1}{q_1-1}\cdot\ldots\cdot\frac{q_s^{\beta_s+1}-1}{q_s-1} = \tau(\mathrm{a})\tau(\mathrm{b}).$$

ЗАДАНИЯ

Вычислите:

a)	$\tau(100)$;	e)	$\tau(\sigma(100))$;	i)	$\tau(10!)$;
b)	$\tau(123)$;	f)	$\sigma(\tau(100))$;	j)	$\sigma(\tau(10!))$;
c)	$\sigma(100)$;	g)	$\tau(100!)$;	k)	$\sigma(\tau(100)!)$;
d)	$\sigma(123)$;	h)	$\sigma(10!)$;	l)	$\sigma(\tau(3!)!)$;

1.6.3. Функция Эйлера

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

Пример

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

$\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$,
$\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$.

Замечание

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

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

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

1°. Функция Эйлера мультипликативная.

$$\varphi\ (a\ b) = \varphi\ (a)\ (b) \text{ при } (a\ b) = 1.$$

Пусть x пробегает значения $r_1, r_2, \ldots, r_{\varphi(b)}$, образующие приведенную систему вычетов по модулю b, а y пробегает значения $s_1, s_2, \ldots, s_{\varphi(a)}$, образующие приведенную систему вычетов по модулю a. Составим всевозможные числа вида $ar_i + bs_j$, соответствующие различным парам r_i, s_j ;число таких чисел будет равно φ (b) φ (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 φ (ab). Произведение φ (b) φ (a) и φ (a b) и выражают одну и ту же величину, т. е. φ (a b) = φ (a)(b).

Примеры

1) φ (3) = 2, φ (10) = 4, φ (30) = 8;
2) φ (5) = 4, φ (8) = 4, φ(40) = 16;
3) φ (3) = 2, φ (6) = 2, φ (18) = 6.

В примере $\varphi\ (3 \cdot 6) \neq \varphi\ (3)\ (6)$, так как φ (3,6) = 2.

2°. Пусть p-простое число, $\alpha \geq 1$- любое натуральное, тогда

$$\varphi\ (p^a) = p^{a-1}(p - 1).$$

Доказательство

Число взаимно просто с p^a тогда и только тогда, когда оно не делится на p. Среди первых p^a натуральных чисел имеется $\frac{p^a}{p} = p^{a-1}$ чисел, делящихся на p; остальные p^a-p^{a-1}чисел взаимно просты с p^a,т. е. $\varphi\ (p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.

3°. Если $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$- каноническое разложение числа n, то φ (n) = $p_1^{a_1-1} p_2^{a_2-1} \ldots p_s^{a_s-1}(p_1 - 1)(p_2 - 1) \ldots (p_s - 1)$.

Доказательство

$p_1, p_2, \ldots, p_s$ в каноническом разложении обозначают различные простые числа, поэтому $p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$-попарно взаимно простые числа и согласно свойствам 1, 2 и 3 имеем:

$$\varphi\ (p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}) = \varphi\ (p_1^{a_1})\ \varphi\ (p_2^{a_2}) \ldots \varphi\ (p_s^{a_s}) =$$
$$= p_1^{a_1-1}\ (p_1 - 1) p_2^{a_2-1}(p_2 - 1) \ldots p_s^{a_s-1}(p_s - 1).$$

Примеры

1. φ (270)= φ (2 · 3^3 ·5)= 3^2 (2-1) (3-1) (5-1) = 72;
2. φ (700000)= φ (2^5 · 5^5 · 7) = 2^4 · 5^4(2-1) (5-1) (7-1)=240000;
3. Вычислить значения функции Эйлера для чисел $n = 1000, 125, 360$.
4. φ (45375)= φ (3 · 5^3 · 11^2)= 5^2 ·11 · 2 · 10=22000

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

$$\varphi(p^k) = (p^k - p^{k-1}).$$

Отсюда получаем:

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400,$$

$$\varphi(125) = \varphi(5^3) = (5^3 - 5^2) = 100,$$

$$\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) = (2^3 - 2^2) \cdot (3^2 - 3) \cdot (5 - 1) = 4 \cdot 6 \cdot 4 = 96$$

Задача. Найти значение $\varphi(2m)$, если известно значение $\varphi(m)$.

Решение. Если число m нечетное, то в силу мультипликативности функции Эйлера $\varphi(2m) = \varphi(2) \cdot \varphi(m) = 1 \cdot \varphi(m) = \varphi(m)$. Если же число m четное, $m = 2^k \cdot n$, где n - нечетное, то
$\varphi(2m) = \varphi(2^{k+1} \cdot n) = \varphi(2^{k+1}) \cdot \varphi(n) = (2^{k+1} - 2^k) \cdot \varphi(n) = 2^k \cdot \varphi(n).$

Но $\varphi(m) = \varphi(2^k \cdot n) = \varphi(2^k) \cdot \varphi(n) = (2^k - 2^{k-1}) \cdot \varphi(n) = 2^{k-1} \cdot \varphi(n)$. Таким обра-зом, в этом случае $\varphi(2m) = 2 \cdot \varphi(n)$.

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 $a_1, a_2, ..., a_n$, называется общим делителем этих чисел. Общий делитель этих чисел называется их наибольшим общим делителем, если он делится на всякий общий делитель данных чисел.

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

$$\left.\begin{array}{l} a = bq_1 + r_2, \\ b = r_2 q_2 + r_3, \\ r_2 = r_3 q_3 + r_4, \\ \dots\dots\dots\dots, \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, \\ r_{n-1} = r_n q_n, \end{array}\right\} (1)$$

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

Системе равенств (1) соответствует равносильная система

$$\left.\begin{array}{l} \frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{b/r_2}, \\ \frac{b}{r_2} = q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{r_2/r_3}, \\ \dots\dots\dots\dots\dots\dots\dots\dots, \\ \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n}, \\ \frac{r_{n-1}}{r_n} = q_n, \end{array}\right\} (2)$$

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

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

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

Имеются различные формы записи цепных дробей:

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

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

Числа $q_1, q_2, \ldots, q_n$ называются элементами цепной дроби.

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

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

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

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

Доказательство: 1) Заметим, что при отказе от указанного условия единственность представления отпадает. В самом деле, при $q_n > 1$: $q_n = (q_n - 1) + \frac{1}{1}$, так что представление можно удлинить:

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

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

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

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

где $q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}} > 1$, т.к. $q_2 \geq 1$.

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

Пусть $\frac{a}{b} = (q_1, q_2, ..., q_n) = (q'_1, q'_2, ..., q'_{n'})$ с условием $q_n > 1$, $q'_{n'} > 1$. Тогда $\left[\frac{a}{b}\right] = q_1 = q'_1$, так что $(q_2, ..., q_n) = (q'_2, ..., q'_{n'})$. Повторным сравнением целых частей получаем $q_2 = q'_2$, а следовательно $(q_3, ..., q_n) = (q'_3, ..., q'_{n'})$ и так далее. Если $n = n'$, то в продолжении указанного процесса получим также $q_n = q'_n$. Если же $n \neq n'$, например $n' > n$, то получим $0 = \frac{1}{(q'_{n+1}, ..., q'_{n'})}$, что невозможно.

Замечания:

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

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

Пример: $-\frac{95}{42} = -3 + \frac{1}{42/31}$, а так как $\frac{42}{31} = (1,2,1,4,2)$, то $-\frac{95}{42} = (-3,1,2,1,4,2)$

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

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

Подходящие дроби. Их свойства

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

Основную роль играют дроби вида:

$$\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, ...$$

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

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

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

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

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

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

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

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

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

$$\delta_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}, \text{ причем } P_k = q_k P_{k-1} + P_{k-2};\ Q_k = q_k Q_{k-1} + Q_{k-2} \quad (3)$$

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 P_k и знаменателей Q_k подходящих дробей по формулам удобно располагать по схеме:

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

Пример

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

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

Подходящие дроби $\frac{P_n}{Q_n}$ равны соответственно $\frac{2}{1}$; $\frac{5}{2}$; $\frac{7}{3}$; $\frac{26}{11}$; $\frac{33}{14}$; $\frac{59}{25}$; $\frac{269}{114}$; $\frac{866}{367}$.

Представление действительных иррациональных чисел правильными бесконечными цепными дробями

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

Выражение $q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots}}$ (где $q_i \in Z, i=\overline{1,\dots}$, $q_2,\dots>0$) (2)

возникающее в таком процессе или заданное формально, называется *правильной бесконечной цепной*, или *непрерывной дробью*, или *дробью*

бесконечной длины и обозначают кратко через $(q_1, q_2, q_3, \ldots)$, а числа $q_1, q_2, \ldots$ – ее элементами или неполными частными.

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

Рассмотрим пример разложения иррационального числа α. Пусть $\alpha = \sqrt{11}$. Выделим из $\sqrt{11}$ его целую часть. $[\sqrt{11}]$=3, а дробную часть $\sqrt{11}$–3, которая меньше 1, представим в виде $\frac{1}{\alpha_2}$, где $\alpha_2 = \frac{1}{\sqrt{11}-3} > 1$.

Повторяя операцию выделения целой части и перевертывания дробной, получаем:

$$\alpha = \alpha_1 = \sqrt{11} = 3 + \frac{1}{\alpha_2}, \alpha_2 > 1;$$

$$\alpha_2 = \frac{1}{\sqrt{11}-3} = \frac{\sqrt{11}+3}{2} = 3 + \frac{1}{\alpha_3}, \alpha_3 > 1;$$

$$\alpha_3 = \frac{2}{\sqrt{11}-3} = \frac{2(\sqrt{11}+3)}{2} = 6 + \frac{1}{\alpha_4}, \alpha_4 > 1.$$

Если остановиться на этом шаге, то можно записать:

$$\alpha = 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{\alpha_4}}}$$

С другой стороны, из формулы для α_3 видно, что $\sqrt{11}$=3+$\frac{1}{\alpha_4}$. Поэтому $\alpha_4 = \alpha_3$, 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, $\sqrt{11}$ разлагается в смешанную периодическую дробь (3, 3, 6, 3, 6, …) или (3, (3, 6)).

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

$$\left.\begin{array}{l} \alpha = \alpha_1 = q_1 + \dfrac{1}{\alpha_2}, где: q_1 = [\alpha_1], \alpha_2 > 1, \\ \alpha_2 = q_2 + \dfrac{1}{\alpha_3}, где: q_2 = [\alpha_2], \alpha_3 > 1, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_k = q_k + \dfrac{1}{\alpha_{k+1}}, где: q_k = [\alpha_k], \alpha_{k+1} > 1, \end{array}\right\}$$

так что $\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_k + \cfrac{1}{\alpha_{k+1}}}}}$.

Числа α_k называются остаточными числами порядка k разложения α. В формуле (4) имеем кусок разложения до остаточного числа α_{k+1}.

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

$$\delta_1 = q_1, \delta_2 = (q_1, q_2), \dots, \delta_k = (q_1, q_2, \dots, q_k), \dots$$

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 $q_1, q_2, \dots, q_k$ и совершенно не зависит от того, является ли q_k последним элементом или за ним следует еще элемент q_{k+1}.

Примеры

1. Записать в виде конечной цепной дроби

a) $\frac{135}{279}$; b) $\frac{103993}{33102}$; c) 2,98976; d) $-\frac{187}{63}$

Решение:

a) $\frac{135}{279}$=(0, 2, 15);

b) $\frac{103993}{33102}$=(3, 7, 15, 1, 292);

c) 2,98976=$\frac{298976}{10^5}$=(2, 1, 96, 1, 1, 1, 10);

d) $-\frac{187}{63}$=–(2, 1, 30, 2)=(-2, 1, 30, 2)

2. Разложить простую дробь в цепную дробь и найти ее подходящие дроби.

a) $\frac{247}{74}$; b) $\frac{333}{100}$; c) $\frac{103993}{33102}$.

Решение:

a) $\frac{247}{74}$= (3, 2, 1, 24);

Находим подходящие дроби:

		3	2	1	24
P_k	**1**	3	7	10	247
Q_k	**0**	**1**	2	3	74

$\frac{P_2}{Q_2}=\frac{2\cdot 3+1}{2\cdot 1+0}=\frac{7}{2}$; $\frac{P_3}{Q_3}=\frac{1\cdot 7+3}{1\cdot 2+1}=\frac{10}{3}$; $\frac{P_4}{Q_4}=\frac{24\cdot 10+7}{24\cdot 3+2}=\frac{247}{74}$

b) $\frac{333}{100}$= (3, 3, 33);

		3	3	33
P_k	**1**	3	10	333
Q_k	**0**	**1**	3	100

$\frac{P_2}{Q_2}=\frac{3\cdot 3+1}{3\cdot 1+0}=\frac{10}{3}$; $\frac{P_3}{Q_3}=\frac{33\cdot 10+3}{33\cdot 3+1}=\frac{333}{100}$

c) $\frac{103993}{33102}$ = 3, 7, 15, 1, 292);

		3	7	15	1	292
P_k	**1**	3	22	333	355	103993
Q_k	**0**	**1**	7	106	113	33102

$\frac{P_2}{Q_2}=\frac{7\cdot 3+1}{7\cdot 1+0}=\frac{22}{7}$; $\frac{P_3}{Q_3}=\frac{15\cdot 22+3}{15\cdot 7+1}=\frac{333}{106}$; $\frac{P_4}{Q_4}=\frac{1\cdot 333+22}{1\cdot 106+7}=\frac{355}{113}$; $\frac{P_5}{Q_5}=\frac{292\cdot 355+333}{292\cdot 113+106}=\frac{103993}{33102}$;

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

$$\text{a) } \sqrt{5}\text{; b) } \sqrt{32}\text{; c) } \frac{1+\sqrt{3}}{2}.$$

Решение: **a)** $\alpha=\sqrt{5}$. Выделим из $\sqrt{5}$ его целую часть: $\lfloor\sqrt{5}\rfloor=2$, а дробную часть $\sqrt{5}$-2, которая <1, представим в виде $\frac{1}{\alpha_2}$, где $\alpha_2=\frac{1}{\sqrt{5}-2}>1$. Повторяя эту операцию выделения целой части и переворачивания дробной, получаем:

$$\alpha=\alpha_1=\sqrt{5}=2+\frac{1}{\alpha_2};$$

$$\alpha_2=\frac{1}{\sqrt{5}-2}=\frac{\sqrt{5}+2}{1}=\sqrt{5}+2=4+\frac{1}{\alpha_3};$$

$$\alpha_3=\frac{1}{\sqrt{5}+2-4}=\frac{\sqrt{5}+2}{1}=\sqrt{5}+2=4+\frac{1}{\alpha_4}.$$

Мы получили, что $\alpha_2=\alpha_3$, следовательно, неполные частные, начиная с α_2 будут повторяться и $\sqrt{5}$=(2, (4)).

Составим таблицу подходящих дробей:

		2	4	4	4	
P_k	**1**	2	9	38		
Q_k	**0**	**1**	4	17	72	

Нам необходимо найти такую подходящую дробь $\delta_k = \frac{P_k}{Q_k}$, чтобы $Q_k Q_{k+1} > \frac{1}{0{,}001} = 1000$. Очевидно, что это $\delta_3 = \frac{38}{17}$, так как 17·72>1000.

Ответ: $\frac{38}{17}$.

b) $\alpha = \sqrt{32}$; $\left[\sqrt{32}\right]$=5

$$\alpha = \alpha_1 = \sqrt{32} = 5 + \frac{1}{\alpha_2};$$

$$\alpha_2 = \frac{1}{\sqrt{32}-5} = \frac{\sqrt{32}+5}{7} = 1 + \frac{1}{\alpha_3};$$

$$\alpha_3 = \frac{1}{\frac{1}{\sqrt{32}-5} - 1} = \frac{\sqrt{32}-5}{1-\sqrt{32}+5} = \frac{\sqrt{32}-5}{6-\sqrt{32}} = \frac{\sqrt{32}+2}{4} = 1 + \frac{1}{\alpha_4};$$

$$\alpha_4 = \frac{1}{\frac{\sqrt{32}+2}{4} - 1} = \frac{4}{\sqrt{32}-2} = \frac{4\sqrt{32}+8}{28} = \frac{\sqrt{32}+2}{7} = 1 + \frac{1}{\alpha_5};$$

$$\alpha_5 = \frac{1}{\frac{\sqrt{32}+2}{7} - 1} = \frac{7}{\sqrt{32}-5} = \frac{7\sqrt{32}+35}{7} = \sqrt{32}+5 = 10 + \frac{1}{\alpha_6};$$

$$\alpha_6 = \frac{1}{\sqrt{32}+5-10} = \frac{\sqrt{32}+5}{7} = 1 + \frac{1}{\alpha_7}.$$

Мы получили $\alpha_2 = \alpha_6 \Rightarrow$ неполные частные, начиная с α_2 будут повторяться и $\sqrt{32}$=(5, (1, 1, 1, 10)).

	5	1	1	1	10	1	…
P_k	5	6	11	17	181	198	
Q_k	1	1	2	3	32	35	

$\frac{181}{32}$, так как 32·35>1000. Ответ: $\frac{181}{32}$.

c) $\frac{1+\sqrt{3}}{2} = \alpha$; $\left[\frac{1+\sqrt{3}}{2}\right]$=1

$$\alpha_1 = \frac{1+\sqrt{3}}{2} = 1 + \frac{1}{\alpha_2};$$

$$\alpha_2 = \frac{1}{\frac{1+\sqrt{3}}{2} - 1} = \frac{2}{\sqrt{3}-1} = \frac{2\sqrt{3}+2}{2} = \sqrt{3}+1 = 2 + \frac{1}{\alpha_3};$$

$$\alpha_3 = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = 1 + \frac{1}{\alpha_4};$$

$\alpha_1 = \alpha_3 \Rightarrow \alpha = ((1, 2))$

	1	2	1	2	1	2	1	2	1
P_k	1	3	4	11	15	41	56	153	
Q_k	1	2	3	8	11	30	41	102	

$\frac{41}{30}$, так как 30·41>1000.

Ответ: $\frac{41}{30}$.

ЗАДАНИЯ

1. Разложить в конечную цепную дробь число

a) $\alpha = \frac{312}{175}$;

b) $\alpha = \frac{3885}{2306}$;

c) $\alpha = \frac{27899}{36823}$.

2. Разложить в бесконечную цепную дробь число

a) $\alpha = \sqrt{13}$;

b) $\alpha = 3\sqrt{3}$;

c) $\alpha = \frac{2+\sqrt{13}}{5}$;

d) $\alpha = \frac{2-\sqrt{13}}{5}$.

Глава 2. ТЕОРИЯ СРАВНЕНИЙ

2.1. 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 $a, b \in \boldsymbol{Z}$, $m \in \boldsymbol{N}$. Говорят, что число a сравнимо с b по модулю m, если a и b при делении на m дают одинаковые остатки. Записывается это так: $a \equiv b(mod\ m)$.

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.

$$a_1 \equiv b_1 (\text{mod } m),\ a_2 \equiv b_2 (\text{mod } m),\ \dots,\ a_k \equiv b_k (\text{mod } m) \Rightarrow a_1 + \dots + a_k \equiv b_1 + \dots b_k (\text{mod } m)$$

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

$$a+b \equiv c\ (\text{mod } m) \Rightarrow a \equiv c-b\ (\text{mod } m)$$

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

$$a \equiv b\ (\text{mod } m) \Rightarrow a+mt \equiv b+mk (\text{mod } m)\ (t, k \in Z)$$

Свойство 4. Сравнения по одинаковому модулю можно почленно перемножать

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

и, следовательно,

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

$$a \equiv b\ (mod\ m) \Rightarrow a^k \equiv b^k (mod\ m)$$

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

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

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

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

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

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

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

$$a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2},\ \ldots,\ a \equiv b \pmod{m_k} \Rightarrow$$

$$a \equiv b \pmod{НОК(m_1,\ldots,m_k)}$$

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

$$a \equiv b \pmod{m},\ d \backslash m \Rightarrow a \equiv b \pmod{d}$$

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

2.2. Полная и приведенная система вычетов

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

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

Пример. Пусть $m = 5$. Тогда:

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

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

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

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

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

Доказательство. Утверждение 1) – очевидно. Докажем утверждение 2). Чисел $ax+b$ ровно m штук. Покажем, что они между собой не сравнимы по модулю m . Ну пусть для некоторых различных x_1 и x_2 из полной системы вычетов оказалось, что $ax_1 + b \equiv ax_2 + b (mod\ m)$. Тогда, по свойствам сравнений из предыдущего пункта, получаем:

$ax_1 \equiv ax_2 (mod m)$ $x_1 \equiv x_2 (mod\ m)$ – противоречие с тем, что x_1 и x_2 различны и взяты из полной системы вычетов.

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

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

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

2.3. Теорема Эйлера и теорема Ферма

Теорема (Эйлер). Пусть $m>1$, $(a,m)=1$, $\varphi(m)$ – функция Эйлера. Тогда:

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

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

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

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

$$\rho_1, \rho_2, \ldots, \rho_c$$

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

$$a r_1 \equiv \rho_1 (mod\ m)$$
$$a r_2 \equiv \rho_2 (mod\ m)$$
$$\ldots$$
$$a r_c \equiv \rho_c (mod\ m)$$

Перемножим эти c штук сравнений. Получится:

$$a^c r_1 r_2 \ldots r_c \equiv \rho_{j1} \rho_{j2} \ldots \rho_{jc} (mod\ m)$$

Так как $r_1 r_2 \ldots r_c = \rho_1 \rho_2 \ldots \rho_c \neq 0$ и взаимно просто с модулем m, то, поделив последнее сравнение на $r_1 r_2 \ldots r_c$, получим $a^{\varphi(m)} \equiv 1 (mod\ m)$.

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

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

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

Доказательство. Положим в условии теоремы Эйлера $m=p$, тогда $\varphi(m)=p-1$ (см. пункт 14) . Получаем $a^{p-1} \equiv 1 (mod\ p)$.

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

легко подправить формулировку теоремы Ферма, чтобы снять ограничение взаимной простоты.

Следствие. Без всяких ограничений на $a \in \mathbf{Z}$,

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

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

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

Решение**.** $a^{9} \equiv 7(\mathrm{mod}\ 10)$ – это дано. Кроме того, очевидно, что (7, 10)=1 и (a , 10)=1. По теореме Эйлера, $a^{\varphi(10)} \equiv 1(\mathrm{mod}\ 10)$. Следовательно, $a^{4} \equiv 1(\mathrm{mod}\ 10)$ и, после возведения в квадрат, $a^{8} \equiv 1(\mathrm{mod}\ 10)$. Поделим почленно $a^{9} \equiv 7(\mathrm{mod}\ 10)$ на $a^{8} \equiv 1(\mathrm{mod}\ 10)$ и получим $a \equiv 7(\mathrm{mod}\ 10)$. Это означает, что a=7.

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

Решение. Число 101 – простое, (7, 101)=1, следовательно, по теореме Ферма: $7^{100} \equiv 1(\mathrm{mod}\ 101)$. Возведем это сравнение в четвертую степень: $7^{400} \equiv 1(\mathrm{mod}\ 101)$, домножим его на очевидное сравнение $7^{2} \equiv 49(\mathrm{mod}\ 101)$, получим: $7^{402} \equiv 49(\mathrm{mod}\ 101)$. 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; $200+43 \equiv 43(\mathrm{mod}\ 100)$ 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 $243^{402} \equiv 43^{402}(\mathrm{mod}\ 100)$. Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера, $43^{\varphi(100)} \equiv 1(\mathrm{mod}\ 100)$. Считаем:

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

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

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

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

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

$$73^{2}\equiv 1 \pmod 3$$
$$73^{4}\equiv 1 \pmod 5$$
$$73^{6}\equiv 1 \pmod 7$$

Перемножая, получаем:

$$73^{12}\equiv 1 \pmod 3, \pmod 5, \pmod 7,$$

откуда, по свойствам сравнений следует:

$$73^{12}-1\equiv 0 \pmod{105},$$

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) $1^{19}+2^{19}+4^{19}+5^{19}+7^{19}+8^{19}\equiv 0 \pmod 9$;
б) $1^{14}+3^{14}+7^{14}+9^{14}\equiv 0 \pmod{10}$.
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) 90^{42} mod 41;	d) 8^{485} mod 187;	g) 3^{161613} mod 16;
b) 34^{160003} mod 15;	e) $(-2)^{634178}$ mod 117;	h) 5^{186609} mod 9;
c) $(-5)^{100016}$ mod 11;	f) 50^{190021} mod 38;	i) 347^{174007} mod 349;

2.4. Сравнения первой степени

Решить сравнение – значит найти все те x , 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

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

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

Случай 1. Пусть a 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):

$$-aP_{n-1} \equiv (-1)^n (mod\ m) \text{ т.е.}$$

$$aP_{n-1} \equiv (-1)^{n-1} (mod\ m) \text{ т.е.}$$

$$a[(-1)^{n-1} P_{n-1} b] \equiv b(mod\ m)$$

и единственное решение исходного сравнения есть:

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

Пример. Решить сравнение 111x ≡75(mod 322).
Решение**.** (111, 322)=1. Включаем алгоритм Евклида:

$$322 = 11 \cdot 2 + 100$$

$$111 = 100 \cdot 1 + 11$$

$$100 = 11 \cdot 9 + 1$$

$$11 = 1 \cdot 11$$

(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: $x \equiv (-1)^3 29\ 75 - 2175 \equiv 79 (mod\ 322)$

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

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

$t \in \mathbf{Z}$, 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 $xa_1 d \equiv b_1 d(mod\ m_1 d)$ и его модуль поделим на d:

$$xa_1 \equiv b_1 (mod\ m_1),$$

где уже a_1 и m_1 взаимно просты. Согласно случаю 1 этого пункта, такое сравнение имеет единственное решение x_0:

$$x \equiv x_0 (mod\ m_1)$$

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 $x=x_0+tm$ 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 $ax \equiv b(mod\ m)$ не имеет решений. Если b кратно d, сравнение $ax \equiv b(mod\ m)$ имеет d штук решений.

Пример. Решить сравнение $111x \equiv 75 (mod\ 321)$.

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

$$37x \equiv 25 (mod\ 107) \text{ и уже } (37,107)=1 .$$

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: $\frac{107}{37} = 2 + \frac{1}{1+\frac{1}{8+\frac{1}{4}}}$

Таблица для нахождения числителей подходящих дробей:

q_n	0	2	1	8	4
P_n	1	2	3	26	107

Значит, $x \equiv (-1)^3 26\ 25 \equiv -650 (mod\ 107) \equiv -8 (mod\ 107) \equiv 99 (mod\ 107)$. Три решения исходного сравнения:

$$x \equiv 99 (mod\ 321),\ x \equiv 206 (mod\ 321),\ x \equiv 313 (mod\ 321),$$

и других решений нет.

Теорема 2. Пусть $m>1$, $(a,m)=1$ Тогда сравнение $ax \equiv b (mod\ m)$ имеет решение: $x \equiv ba^{\varphi(m)-1} (mod\ m)$.

Доказательство. По теореме Эйлера, имеем: $a^{\varphi(m)} \equiv 1 (mod\ m)$, следовательно, $a\ ba^{\varphi(m)-1} \equiv b (mod\ m)$.

Пример. Решить сравнение $7x \equiv 3 (mod\ 10)$. Вычисляем:

$$\varphi(10)=4;\ x \equiv 3 \cdot 7^{4-1} (mod\ 10) \equiv 1029 (mod\ 10) \equiv 9 (mod\ 10) .$$

ЗАДАНИЯ

Решить сравнения:

a) $5x \equiv 3 (mod\ 11)$; d) $6x \equiv 15 (mod\ 21)$; g) $13x \equiv 8 (mod\ 16)$;
b) $8x \equiv 5 (mod\ 13)$; e) $16x \equiv 26 (mod\ 62)$; h) $25x \equiv 50 (mod\ 125)$;
c) $15x \equiv 25 (mod\ 17)$; f) $21x \equiv 14 (mod\ 42)$; i) $13x \equiv 37 (mod\ 29)$.

2.5. Системы сравнений первой степени

Рассмотрим систему сравнений

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

Китайская теорема об остатках

Пусть $m_1,\dots, m_k$ – попарно простые числа $\Rightarrow$ система сравнений (*) имеет единственное решение $x_0 \equiv \sum_{i=1}^{k} b_i M_i M_i^{'} \pmod{M}$ **,

где $M = \prod_{i=1}^{k} m_i = НОК(m_i)$, $M_i = \frac{M}{m_i}$, $M_i' = M_i^{-1} \pmod{m_i}$.

Доказательство

Т.к. $m_s \backslash M_j$ $\forall j \neq s,\ j = \overline{1,k} \Rightarrow x_0 \equiv M_s M_s^{'} b_s \equiv b_s \pmod{m_s}$ $\forall s \in \{1,\dots,k\}$

$\Rightarrow$ система (*) равносильна системе

$$\begin{cases} x \equiv x_0 \pmod{m_1} \\ x \equiv x_0 \pmod{m_2} \\ x \equiv x_0 \pmod{m_k} \end{cases} \quad ***$$

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 ** $b_1, b_2, \dots, b_k$ независимо друг от друга пробегают полные системы вычетов по модулям $m_1, m_2, \dots, m_k$ соответственно, то x_0 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:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases}$$

Вычислим параметры, необходимые для нахождения решения. Составим таблицу

m_i	3	4	5
M_i	20	15	12
M_i'	2	3	3

Согласно китайской теореме об остатках, решением будет являться

$x_0 \equiv 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \pmod{60} \equiv 40 + 90 + 144 \pmod{60} \equiv 34 \pmod{60}$.

Ответ: $x \equiv 34 \pmod{60}$.

Пример

Решить систему сравнений:

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

$$b_1 = 1 \; ; \; b_2 = 3 \; ; \; b_3 = 2 \; ;$$

$$M_1 = 35, \; M_2 = 28, \; M_3 = 20 \; .$$

$$35 \cdot 3 \equiv 1 \pmod 4$$
$$28 \cdot 2 \equiv 1 \pmod 5$$
$$20 \cdot 6 \equiv 1 \pmod 7$$

т.е. $M_1^{-1}=3$, $M_2^{-1}=2$, $M_3^{-1}=6$.

Значит $x_0 = 35 \cdot 3 \cdot 1 + 28 \cdot 2 \cdot 3 + 20 \cdot 6 \cdot 2 = 513$. Получим ответ: $x \equiv 513 \pmod{140} \equiv 93 \pmod{140}$, т.е. наименьшее положительное число равно 93.

ЗАДАНИЯ

Решить системы сравнений.

a) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 8 \pmod 7 \end{cases}$; c) $\begin{cases} 2x \equiv 18 \pmod{22} \\ 3x \equiv 5 \pmod 7 \end{cases}$; e) $\begin{cases} 5x \equiv 3 \pmod{25} \\ x \equiv 8 \pmod{13} \end{cases}$;

b) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$; d) $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 9 \\ x \equiv 1 \pmod 5 \end{cases}$; f) $\begin{cases} 3x \equiv 18 \pmod{30} \\ x \equiv 2 \pmod 3 \\ 5x \equiv 1 \pmod 7 \end{cases}$.

2.6. Сравнения любой степени по простому модулю

В этом пункте мы рассмотрим сравнения вида $f(x) \equiv 0 \pmod p$, где p - простое число, $f(x)=ax^n+a_1x^{n-1}+\ldots+a_n$ - многочлен с целыми коэффициентами, и попытаемся научиться решать такие сравнения. Не отвлекаясь на посторонние природные явления, сразу приступим к работе.

Лемма 1. Произвольное сравнение $f(x) \equiv 0 \pmod p$, где p - 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: $f(x)=(x^p-x)\cdot Q(x)+R(x)$, где, как известно, степень остатка $R(x)$ не превосходит $p-1$. Но ведь, по теореме Ферма, $x^p-x \equiv 0 \pmod p$. Это означает, что $f(x) \equiv R(x) \pmod p$, а исходное сравнение равносильно сравнению $R(x) \equiv 0 \pmod p$.

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

Лемма 2. Если сравнение $ax^n+a_1x^{n-1}+\ldots+a_n \equiv 0 \pmod p$ степени n по простому модулю p имеет более n различных решений, то все коэффициенты $a, a_1, \ldots, a_n$ кратны p.

Доказательство. Пусть сравнение $ax^n+a_1x^{n-1}+\ldots+a_n \equiv 0 \pmod p$, имеет $n+1$ решение и $x_1, x_2, \ldots, x_n, x_{n+1}$ – наименьшие неотрицательные вычеты этих решений. Тогда, очевидно, многочлен $f(x)$ представим в виде:

$$f(x)=a(x-x_1)(x-x_2)\ldots(x-x_n-2)(x-x_{n-1})(x-x_n)+$$
$$+b(x-x_1)(x-x_2)\ldots(x-x_n-2)(x-x_{n-1})+$$
$$+c(x-x_1)(x-x_2)\ldots(x-x_n-2)+$$
$$+\ldots+$$
$$+k(x-x_1)(x-x_2)+$$
$$+l(x-x_1)+$$
$$+m.$$

Действительно, коэффициент b нужно взять равным коэффициенту при x^{n-1} в разности $f(x)-a(x-x_1)(x-x_2)\ldots(x-x_n)$; коэффициент c – это коэффициент перед x^{n-2} в разности $f(x)-a(x-x_1)(x-x_2)\ldots(x-x_n-b(x-x_1)(x-x_2)\ldots(x-x_{n-1})$, и т.д.

Теперь положим последовательно $x=x_1, x_2,\ldots,x_n,x_{n+1}$. Имеем:

1) $f(x_1)=m\equiv 0(mod\ p)$, следовательно, p делит m .

2) $f(x_2)=m+l(x_2-x_1)\equiv l(x_2-x_1)\equiv 0(mod\ p)$, следовательно, p делит l , ибо p не может делить x_2-x_1, так как $x_2<p$, $x_1<p$.

3) $f(x_3)\equiv k(x_3-x_1)(x_3-x_2)\equiv 0(mod\ p)$, следовательно, p делит k .

И т.д.

Получается, что все коэффициенты $a, b, c,\ldots,k, l$ кратны p . Это означает, что все коэффициенты $a,a_1,\ldots,a_n$ тоже кратны p , ведь они являются суммами чисел, кратных p .

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

Пример:

Сравнение второй степени $x^2\equiv 1(mod\ 16)$ имеет четыре различных решения:

$$x\equiv 1(mod\ 16),\ x\equiv 7(mod\ 16),\ x\equiv 9(mod\ 16),\ x\equiv 15(mod\ 16).$$

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

2.7. 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 $m_1, m_2, \ldots m_k$ попарно взаимно просты, то сравнение $f(x) \equiv 0 (\mathrm{mod}\ m_1 m_2 \ldots m_k)$ равносильно системе сравнений:

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\ m_1) \\ f(x) \equiv 0 (\mathrm{mod}\ m_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f(x) \equiv 0 (\mathrm{mod}\ m_k) \end{cases}$$

При этом, если $T_1, T_2, \ldots, T_к$ – числа решений отдельных сравнений этой системы по соответствующим модулям, то число решений T исходного сравнения равно $T_1 T_2 \ldots T_к$.

Доказательство. Первое утверждение теоремы (о равносильности системы и сравнения) очевидно, т.к. если $a \equiv b$ (mod m), то $a \equiv b$ (mod d), где d делит m. Если же $a \equiv b$ (mod m_1) и $a \equiv b$ (mod m_2), то $a \equiv b$ (mod $НОК(m_1, m_2)$), 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 $f(x) \equiv 0 (\mathrm{mod}\ m_s)$ выполняется тогда и только тогда, когда выполняется одно из T_s штук сравнений вида $x \equiv b_s$ (mod m_s), где b_s пробегает вычеты решений сравнения $f(x) \equiv 0 (\mathrm{mod}\ m_s)$. Всего различных комбинаций таких простейших сравнений

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\ m_1) \\ x \equiv b_2 (\mathrm{mod}\ m_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k (\mathrm{mod}\ m_k) \end{cases}$$

$T_1 T_2 \ldots T_к$ штук. Все эти комбинации, по лемме 2 из пункта 19, приводят к различным классам вычетов по mod($m_1 m_2 \ldots m_k$).

Итак, решение сравнения $f(x) \equiv 0 \left(\mathrm{mod}\ p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}\right)$ сводится к решению сравнений вида $f(x) \equiv 0(\mathrm{mod}\ p^a)$. Оказывается, что решение этого последнего сравнения, в свою очередь, сводится к решению некоторого сравнения $g(x) \equiv 0(\mathrm{mod}\ p)$ с 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 $f(x) \equiv 0(\mathrm{mod}\ p^a)$ к решению сравнения $g(x) \equiv 0(\mathrm{mod}\ p)$.

Процесс сведения

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

Пусть $x \equiv x_1(\mathrm{mod}\ p)$ – решение сравнения $f(x) \equiv 0(\mathrm{mod}\ p)$. Тогда x можно представить в виде

$$x = x_1 + pt_1, \text{ где } t_1 \in Z.$$

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

$$f(x_1) + pt_1 f'(x_1) \equiv 0(\mathrm{mod}\ p^2).$$

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

$$\frac{f(x_1)}{p} + t_1 f'(x_1) \equiv 0(\mathrm{mod}\ p)$$

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

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

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

$$f(x_2) + p^2 t_2 f'(x_2) \equiv 0(\mathrm{mod}\ p^3),$$

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

$$\frac{f(x_2)}{p} + t_2 f'(x_2) \equiv 0(\mathrm{mod}\ p)$$

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

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

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

Итак:

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

Пример 1. Требуется решить сравнение $x^3+9x—1\equiv 0$ (mod 125).

Решение. Известно, что сравнение $x^3+9x—1\equiv 0$ (mod 5) имеет одно решение:

$$x\equiv 2(\mathrm{mod}\ 5),\ \text{или}\ x=2+5t_1.$$

Подставим получившееся x в сравнение по модулю 25:

$$(2+5t_1)^3+9(2+5t_1)—1\equiv 0\ (\mathrm{mod}\ 25).$$

Решим это сравнение.

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

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

$$13\cdot 5t_1\equiv 0\ (\mathrm{mod}\ 25)$$

$$13t_1\equiv 0\ (\mathrm{mod}\ 5)$$

$$t_1\equiv 0\ (\mathrm{mod}\ 5)$$

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

$$(2+25t_2)^3+9(2+25t_2)—1\equiv 0\ (\mathrm{mod}\ 125)$$

Решим это сравнение.

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

$$25+13\cdot 25t_2+625\cdot(25t_2^3+2t_2^2)\equiv 0\ (\mathrm{mod}\ 125)$$

$$25+13\cdot 25t_2\equiv 0\ (\mathrm{mod}\ 125)$$

$$1+13t_2\equiv 0\ (\mathrm{mod}\ 5)$$

$$13t_2\equiv -1\ (\mathrm{mod}\ 5)$$

$$3t_2\equiv 4\ (\mathrm{mod}\ 5)$$

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

$$5=3+2$$

$$3=2+1$$

$$2=1+0$$

$$1=3-2=3-(5-3)=2\cdot 3-1\cdot 5.$$

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

Тогда решением сравнения относительно t_2 будет

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

$$t_2 \equiv 3 \pmod 5$$

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

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

Пример 2. Решить сравнение $x^4+7x+4 \equiv 0 \pmod{27}$.

Решение. $27=3^3$.

процесс решения должен быть таким:

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

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

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

Ищем t_1: $3+3t_1 \cdot 2 \equiv 0 \pmod 9$, после деления на $p=3$:

$1+2t_1 \equiv 0 \pmod 3$,

$t_1 \equiv 1 \pmod 3$ - единственное решение. Далее: $t_1=1+3t_2$,

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

$18+9\,20t_2 \equiv 0 \pmod{27}$,

и, после деления на $p^2=9$, ищем t_2: $2+20t_2 \equiv 0 \pmod 3$, $t_2 \equiv 2 \pmod 3$, $t_2=2+3t_3$,

откуда $x=4+9(2+3t_3)=22+27t_3$.

Значит, решением сравнения является $x \equiv 22 \pmod{27}$.

ЗАДАНИЯ

1. Сколько решений имеет сравнение $x^5+x+1 \equiv 0 \pmod{105}$?

2. Решите сравнения:

а) $7x^4+19x+25 \equiv 0 \pmod{27}$;

б) $9x^2+29x+62 \equiv 0 \pmod{64}$;

в) $6x^3+27x^2+17x+20 \equiv 0 \pmod{30}$;

г) $31x^4+57x^3+96x+191 \equiv 0 \pmod{225}$;

д) $x^3+2x+2 \equiv 0 \pmod{125}$;

е) $x^4+4x^3+2x^2+2x+12 \equiv 0 \pmod{625}$.

2.8. Сравнения второй степени. Символ Лежандра

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

$$x^2 \equiv a \pmod{p},$$

где a и p взаимно просты, а p - нечетное простое число.

Ясно, что сравнение $x^2 \equiv a \pmod 2$ имеет решение при любых a, т.к. вместо a достаточно подставлять только 0 или 1, а числа 0 и 1 являются квадратами. Именно поэтому случай $p=2$ не представляет особого интереса и выводится из дальнейшего рассмотрения.

Что касается сравнения $x^2 \equiv 0 \pmod p$, то оно, очевидно, всегда имеет решение $x=0$. Итак, интерес представляет только ситуация с нечетным простым модулем и $a \neq 0$.

Определение. Если сравнение $x^2 \equiv a \pmod p$ имеет решения, то число a называется квадратичным вычетом по модулю p. В противном случае, число a называется квадратичным невычетом по модулю p.

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

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

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

Простое наблюдение: Если a - квадратичный вычет по модулю p, то сравнение $x^2 \equiv a \pmod p$ имеет в точности два решения. Действительно, если a - квадратичный вычет по модулю p, то у сравнения $x^2 \equiv a \pmod p$ есть хотя бы одно решение $x \equiv x_1 \pmod p$. Тогда $x_2 = -x_1$ – тоже решение, ведь $(-x_1)^2 = x_1^2$. Эти два решения не сравнимы по модулю $p > 2$, так как из $x_1 \equiv -x_1 \pmod p$ следует $2x_1 \equiv 0 \pmod p$, т.е. (поскольку $p \neq 2$) $x_1 \equiv 0 \pmod p$, что невозможно, ибо $a \neq 0$.

Поскольку сравнение $x^2 \equiv a \pmod p$ есть сравнение второй степени по простому модулю, то больше двух решений оно иметь не может.

Введя в рассмотрение удобный символ ($\frac{a}{p}$), заменяющий длинную фразу. Этот символ носит теперь фамилию Лежандра и читается: “символ Лежандра а по пэ”.

Определение. Пусть a не кратно p . Тогда символ Лежандра определяется как:

$$\left(\frac{a}{p}\right)=\begin{cases} 1, \text{а - квадратичный вычет по модулю р} \\ -1, \text{а - квадратичный невычет по модулю р} \end{cases}$$

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 a простейшее двучленное сравнение второй степени имеет решение, а при каких – не имеет ?).

Теорема. (Критерий Эйлера) Пусть a не кратно p . Тогда:

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\pmod p$$

Доказательство

По теореме Ферма, $a^{p-1}\equiv 1 \pmod p$. В этом сравнении перенесем единицу в левую часть: $a^{p-1}-1\equiv 0 \pmod p$. Поскольку р – простое, а значит нечетное число, значит р-1 – число четное. Тогда можем разложить левую часть сравнения на множители: $\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-2}{2}}+1\right)\equiv 0 \pmod p$.

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

$$a^{\frac{p-1}{2}}\equiv 1 \pmod p \text{ *, либо } a^{\frac{p-1}{2}}\equiv -1 \pmod p \text{ **}$$

Если a – квадратичный вычет по модулю p, то a при некотором x удовлетворяет сравнению $a\equiv x^2 \pmod p$, тогда $a^{\frac{p-1}{2}}\equiv x^{p-1} \pmod p$, а учитывая (по теореме Ферма), что $x^{p-1}\equiv 1 \pmod p$, получаем сравнение (*).

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

Свойство 1. Если $a \equiv b \pmod p$, то $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

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

Свойство 2. $\left(\frac{1}{p}\right) = 1$

Доказательство очевидно, ведь единица является квадратом.

Свойство 3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, p \equiv 1 \pmod 4 \\ -1, p \equiv 3 \pmod 4 \end{cases}$

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

Свойство 4. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

Действительно, $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}} (b)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ (mod\ p)$

Свойство 5. $\left(\frac{a^2}{p}\right) = 1$

Свойство 6. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, т.е. в числителе символа Лежандра можно отбросить квадратный множитель.

Действительно, $\left(\frac{ab^2}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot 1 \equiv \left(\frac{a}{p}\right) (mod\ p)$

Примеры

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{5}{13}\right) = (-1)^{\frac{13^2-1}{8}} \cdot \left(\frac{5}{13}\right) = -\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = -\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = 1$$

10 – квадратичный вычет по модулю 13.

$$\left(\frac{1350}{1381}\right) = \left(\frac{2}{1381}\right) \cdot \left(\frac{3}{1381}\right)^3 \cdot \left(\frac{5}{1381}\right)^2 = \left(\frac{2}{1381}\right) \cdot \left(\frac{3}{1381}\right) = (-1) \cdot \left(\frac{3}{1381}\right) =$$

$$= -(-1)^{\frac{1381-1}{2}\cdot\frac{3-1}{2}}\left(\frac{1381}{3}\right) = -(-1)^{90}\left(\frac{1381}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

1350является квадратичным вычетом по модулю 1381.

2.9. Символ Якоби

Пусть n – составное число, каноническое разложение которого есть $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Положим $(a,n)=1$. Тогда символ Якоби определяется равенством: $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} ... \left(\frac{a}{p_k}\right)^{\alpha_k}$

Свойства символа Якоби

1. $a \equiv a_1 (\mathrm{mod}\ n) \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{a_1}{n}\right)$

2. $\left(\frac{1}{n}\right) = 1$

3. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

4. $\left(\frac{a \cdot b \cdot ... \cdot l}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)...\left(\frac{l}{n}\right)$

5. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

6. Закон взаимности:

$(n,m)=1$, n, $m>0$, n, m — нечетные числа $\Rightarrow \left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$

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:

$$\left(\frac{n}{m}\right)=\left(\frac{2}{m}\right)^{k}\left(\frac{n_1}{m}\right)$$

2. Пользуясь св-вом 4, понижаем степень k:

$$\left(\frac{n}{m}\right)=\left(\frac{2}{m}\right)^{k \bmod 2}\left(\frac{n_1}{m}\right)$$

3. Если k mod 2=1, то вычисляем $\left(\frac{2}{m}\right)$ пользуясь свойством 5.

4. Символ $\left(\frac{n_1}{m}\right)$ 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 $(n,m)\neq 1$, то s:=0. Идти на Выход.

Ш.2: n:=n mod m. Ш.3.

Ш.3: Представить n как $n=2^k n_1$. 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: $n\leftrightarrow m$. s:=$s\cdot(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$. Идти на Ш.2.

Выход. s – символ Якоби.

Пример

$$\left(\frac{219}{383}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{4}{219}\right)\left(\frac{41}{219}\right)=-\left(\frac{41}{219}\right)=-\left(\frac{219}{41}\right)=-\left(\frac{14}{41}\right)=$$

$$=-\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{6}{7}\right)=-\left(\frac{-1}{7}\right)=1.$$

Вычислить, пользуясь свойствами символа Якоби:

a) $\left(\frac{5}{7}\right)$; c) $\left(\frac{38}{11}\right)$; e) $\left(\frac{25}{30}\right)$; g) $\left(\frac{385}{927}\right)$; i) $\left(\frac{331}{221}\right)$; k) $\left(\frac{203}{313}\right)$;

b) $\left(\frac{2}{13}\right)$; d) $\left(\frac{150}{19}\right)$; f) $\left(\frac{343}{585}\right)$; h) $\left(\frac{54}{101}\right)$; j) $\left(\frac{222}{431}\right)$; l) $\left(\frac{928}{385}\right)$.

2.10. Квадратичные сравнения по простому модулю

Пусть дано сравнение $x^2 \equiv a \pmod p$, $p>2$ – простое и $\left(\frac{a}{p}\right)=1$.

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

Для p возможны следующие случаи:

а) Пусть $p \equiv 3 \pmod 4$, т.е. $p=4k+3$.

По критерию Эйлера, $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Подставляя сюда p, получим

$$a^{\frac{4k+2}{2}} \equiv 1 \pmod p$$

$$a^{2k+1} \equiv 1 \pmod p$$

$$a^{2k+2} \equiv a \pmod p$$

Вернувшись сравнению, которое требуется решить, заметим, что $x^2 \equiv a^{2k+2} \pmod p$, и тогда $x \equiv \pm a^{k+1} \pmod p$ – искомое решение.

б) $p \equiv 5 \pmod 8$, т.е. $p=8k+5$.

Найдем какой-нибудь квадратичный невычет по модулю р. Согласно св-ву 7 для символа Лежандра, таким невычетом в случае $p=8k+5$ будет являться «2». Тогда, согласо критерию Эйлера, $2^{4k+2} \equiv -1 \pmod p$.

Так как а – квадратичный вычет по модулю р, то по критерию Эйлера, $a^{\frac{p-1}{2}} \equiv 1 \pmod p \Rightarrow a^{\frac{3k+4}{2}} = a^{4k+2} \equiv 1 \pmod p$.

Тогда возможны два варианта: $a^{2k+1} \equiv 1 \pmod p$ или $a^{2k+1} \equiv -1 \pmod p$.

В первом случае дальнейшие рассуждения проводим как в пункте а, и получаем $x \equiv \pm a^{k+1} \pmod p$.

Рассмотрим подробнее второй случай. Имеем:

$$a^{2k+1} \equiv -1 \pmod p$$

Для того, чтобы избавиться от знака (—) в правой части, домножим левую часть этого сравнения на 2^{4k+2}, а левую – на –1.

$$2^{4k+2}a^{2k+1}\equiv 1(\text{mod } p)$$
$$2^{4k+2}a^{2k+2}\equiv a(\text{mod } p)$$
$$x\equiv\pm 2^{2k+1}a^{k+1}(\text{mod } p)$$

Таким образом, имеются два кандидата на решение:

$$x\equiv\pm a^{k+1}(\text{mod } p).$$
$$x\equiv\pm 2^{2k+1}a^{k+1}(\text{mod } p)$$

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

в) $p\equiv 9(\text{mod } 16)$, т.е. $p=16k+9$.

Найдем N – какой-нибудь квадратичный невычет по модулю p. Тогда по критерию Эйлера, $N^{\frac{p-1}{2}} = N^{8k+4} = -1$.

С другой стороны, поскольку a – квадратичный вычет по модулю p, то по критерию Эйлера, $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p) \Rightarrow a^{\frac{16k+8}{2}} = a^{8k+4} \equiv 1(\text{mod } p)$.

Тогда возникают два случая: $a^{4k+2}\equiv 1(\text{mod } p)$ или $a^{4k+2}\equiv -1(\text{mod } p)$.

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

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

Рассмотрим первый из вариантов:

$$N^{4k+2}a^{2k+1}\equiv 1(\text{mod } p)$$
$$N^{4k+2}a^{2k+2}\equiv a(\text{mod } p)$$
$$x\equiv\pm N^{2k+1}a^{k+1}(\text{mod } p).$$

Рассмотрим второй из вариантов:

$$N^{4k+2}a^{2k+1}\equiv -1(\mathrm{mod}\ p)$$
$$N^{12k+6}a^{2k+1}\equiv 1(\mathrm{mod}\ p)$$
$$N^{12k+6}a^{2k+2}\equiv a(\mathrm{mod}\ p)$$
$$x\equiv\pm N^{6k+3}a^{k+1}(\mathrm{mod}\ p)$$

Итак, получили четыре пары – кандидата на решение:

$$x\equiv\pm a^{k+1}(\mathrm{mod}\ p)$$
$$x\equiv\pm N^{2k+1}a^{k+1}(\mathrm{mod}\ p)$$
$$x\equiv\pm N^{4k+2}a^{k+1}(\mathrm{mod}\ p)$$
$$x\equiv\pm N^{6k+3}a^{k+1}(\mathrm{mod}\ p)$$

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

Рассмотренным способом можно построить решение для любого простого модуля p. Если $p=2^h k+2^{h-1}+1$, то при решении сравнения возникнет 2^{h-2} пар – кандидатов в решение, каждая из которых будет иметь вид $x\equiv\pm N^{z(2k+1)}a^{k+1}(\mathrm{mod}\ p)$, где $z=\overline{1,h-2}$.

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 $x^2\equiv 8(\mathrm{mod}\ 17)$.

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

$\left(\frac{8}{17}\right)=\left(\frac{2}{17}\right)^3=\left(\frac{2}{17}\right)=1$. Сравнение имеет 2 решения. Отыщем их.

$17=2\cdot 8+1=4\cdot 4+1=8\cdot 2+1=16\cdot 1+1=32\cdot 0+17=2^5\cdot 0+17$.

$h=5$, $k=0$. Имеется $2^3=8$ пар-кандидатов в решения.

Найдем какой-нибудь невычет по модулю 17:

$\left(\frac{3}{17}\right)=(-1)^{1\cdot 8}\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1$.

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

Имеются следующие кандидаты в решения сравнения:

1) $x\equiv\pm 8(\mathrm{mod}\ 17)$
2) $x\equiv\pm 3\cdot 8(\mathrm{mod}\ 17)$
3) $x\equiv\pm 3^2 8(\mathrm{mod}\ 17)$
4) $x\equiv\pm 3^3 8(\mathrm{mod}\ 17)$
5) $x\equiv\pm 3^4 8(\mathrm{mod}\ p)$
6) $x\equiv\pm 3^5 8(\mathrm{mod}\ p)$
7) $x\equiv\pm 3^6 8(\mathrm{mod}\ p)$
8) $x\equiv\pm 3^7 8(\mathrm{mod}\ p)$

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

1) $x \equiv \pm 8 \pmod{17}$. Тогда $x^2 \equiv 64 \equiv 13 \pmod{17}$.

2) $x \equiv \pm 3 \cdot 8 \equiv \pm 24 \equiv \pm 7 \pmod{17}$. Тогда $x^2 \equiv 49 \equiv 15 \pmod{17}$.

3) $x \equiv \pm 3^2 8 \equiv \pm 72 \equiv \pm 4 \pmod{17}$. Тогда $x^2 \equiv 16 \pmod{17}$.

4) $x \equiv \pm 3^3 8 \equiv \pm 216 \equiv \pm 12 \pmod{17}$. Тогда $x^2 \equiv 144 \equiv 8 \pmod{17}$.

Ответ: $x \equiv \pm 12 \pmod{17}$, или $x \equiv \pm 5 \pmod{17}$.

ЗАДАНИЯ

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

a) $x^2 \equiv 17 \pmod{19}$;	d) $x^2 \equiv 2 \pmod{7}$;	g) $x^2 \equiv 3 \pmod{41}$;
b) $x^2 \equiv 3 \pmod{13}$;	e) $x^2 \equiv 3 \pmod{11}$;	h) $x^2 \equiv 2 \pmod{17}$;
c) $x^2 \equiv 8 \pmod{41}$;	f) $2x^2 \equiv 10 \pmod{11}$;	i) $3x^2 \equiv 15 \pmod{31}$.

2.11. Квадратичные сравнения по составному модулю

Рассмотрим сравнение вида $x^2 \equiv a \pmod{p^\alpha}$, где p – простое нечетное число. Как было показано в п.4 §4, решение этого сравнения можно отыскать, решив сравнение $x^2 \equiv a \pmod{p}$. Причем сравнение $x^2 \equiv a \pmod{p^\alpha}$ будет иметь два решения, если a является квадратичным вычетом по модулю p.

Пример

Решить квадратичное сравнение $x^2 \equiv 86 \pmod{125}$.

$125 = 5^3$, 5 – простое число. Проверим, является ли 86 квадратом по модулю 5.

$\left(\frac{86}{5}\right) = \left(\frac{1}{5}\right) = 1$. Исходное сравнение имеет 2 решения.

Найдем решение сравнения $x^2 \equiv 86 \pmod{5}$.

$$x^2 \equiv 1 \pmod{5}.$$

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

$$x \equiv \pm 1 \pmod{5} \text{ или, иначе, } x = \pm(1 + 5t_1).$$

Подставим получившееся решение в сравнение по модулю $5^2=25$:

$$x^2\equiv 86 \pmod{25}$$
$$x^2\equiv 11 \pmod{25}$$
$$(1+5t_1)^2\equiv 11 \pmod{25}$$
$$1+10\,t_1+25\,t_1^2\equiv 11 \pmod{25}$$
$$10\,t_1\equiv 10 \pmod{25}$$
$$2\,t_1\equiv 2 \pmod 5$$
$$t_1\equiv 1 \pmod 5,\text{ или, что то же самое, } t_1=1+5t_2.$$

Тогда решение сравнения по модулю 25 есть $x=\pm(1+5(1+5t_2))=\pm(6+25t_2)$. Подставим получившееся решение в сравнение по модулю $5^3=125$:

$$x^2\equiv 86 \pmod{125}$$
$$(6+25t_2)^2\equiv 86 \pmod{125}$$
$$36+12\cdot 25t_2+625t_2^2\equiv 86 \pmod{125}$$
$$12\cdot 25t_2\equiv 50 \pmod{125}$$
$$12t_2\equiv 2 \pmod 5$$
$$2t_2\equiv 2 \pmod 5$$
$$t_2\equiv 1 \pmod 5,\text{ или } t_2=1+5t_3.$$

Тогда решение сравнения по модулю 125 есть $x=\pm(6+25(1+5t_3))=\pm(31+125t_3)$.

Ответ: $x\equiv\pm 31 \pmod{125}$.

Рассмотрим теперь сравнение вида $x^2\equiv a \pmod{2^\alpha}$. Такое сравнение не всегда имеет два решения. Для такого модуля возможны случаи:

1) $\alpha=1$. Тогда сравнение имеет решение только тогда, когда $a\equiv 1 \pmod 2$, и решением будет $x\equiv 1 \pmod 2$ (одно решение).

2) $\alpha=2$. Сравнение имеет решения только тогда, когда $a\equiv 1 \pmod 4$, и решением будет $x\equiv\pm 1 \pmod 4$ (два решения).

3) $\alpha\geq 3$. Сравнение имеет решения только тогда, когда $a\equiv 1 \pmod 8$, и таких решений будет четыре. Сравнение $x^2\equiv a \pmod{2^\alpha}$ при $\alpha\geq 3$ решается так же, как сравнения вида $x^2\equiv a \pmod{p^\alpha}$, только в качестве начального решения выступают решения по модулю 8: $x\equiv\pm 1 \pmod 8$ и $x\equiv\pm 3 \pmod 8$. Их следует подставить в сравнение по модулю 16, затем по модулю 32 и т. д. вплоть до модуля 2^α.

Пример

Решить сравнение $x^2\equiv 33 \pmod{64}$

$64=2^6$. Проверим, имеет ли исходное сравнение решения. $33\equiv 1 \pmod 8$, значит сравнение имеет 4 решения.

По модулю 8 эти решения будут: $x\equiv\pm1(\mathrm{mod}\ 8)$ и $x\equiv\pm3(\mathrm{mod}\ 8)$, что можно представить как $x=\pm(1+4t_1)$. Подставим это выражение в сравнение по модулю 16

$$x^2\equiv33(\mathrm{mod}\ 16)$$
$$(1+4t_1)^2\equiv1(\mathrm{mod}\ 16)$$
$$1+8t_1+16t_1^2\equiv1(\mathrm{mod}\ 16)$$
$$8t_1\equiv0\ (\mathrm{mod}\ 16)$$
$$t_1\equiv0\ (\mathrm{mod}\ 2)$$

Тогда решение примет вид $x=\pm(1+4t_1)=\pm(1+4(0+2t_2))=\pm(1+8t_2)$. Подставим получившееся решение в сравнение по модулю 32:

$$x^2\equiv33(\mathrm{mod}\ 32)$$
$$(1+8t_2)^2\equiv1(\mathrm{mod}\ 32)$$
$$1+16t_2+64t_2^2\equiv1(\mathrm{mod}\ 32)$$
$$16t_2\equiv0\ (\mathrm{mod}\ 32)$$
$$t_2\equiv0\ (\mathrm{mod}\ 2)$$

Тогда решение примет вид $x=\pm(1+8t_2)=\pm(1+8(0+2t_3))=\pm(1+16t_3)$. Подставим получившееся решение в сравнение по модулю 64:

$$x^2\equiv33(\mathrm{mod}\ 64)$$
$$(1+16t_3)^2\equiv33(\mathrm{mod}\ 64)$$
$$1+32t_3+256t_3^2\equiv33(\mathrm{mod}\ 64)$$
$$32t_3\equiv32\ (\mathrm{mod}\ 64)$$
$$t_3\equiv1\ (\mathrm{mod}\ 2)$$

Тогда решение примет вид $x=\pm(1+16t_3)=\pm(1+16(1+2t_4))=\pm(17+32t_4)$. Итак, по модулю 64 исходное сравнение имеет четыре решения: $x\equiv\pm17(\mathrm{mod}\ 64)$ и $x\equiv\pm49(\mathrm{mod}\ 64)$.

Теперь рассмотрим сравнение общего вида: $x^2\equiv a(\mathrm{mod}\ m)$, $(a,m)=1$, $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ - каноническое разложение модуля m. Согласно Теореме из п.4 §4, данному сравнению равносильна система

$$\begin{cases} x^2\equiv a(\mathrm{mod}\ 2^{\alpha}) \\ x^2\equiv a(\mathrm{mod}\ p_1^{\alpha_1}) \\ x^2\equiv a(\mathrm{mod}\ p_2^{\alpha_2}) \\ \ldots \\ x^2\equiv a(\mathrm{mod}\ p_k^{\alpha_k}) \end{cases}$$

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 $\alpha=1$, 2^{k+1}, если $\alpha=2$, 2^{k+2}, если $\alpha\geq 3$.

Пример

Решить сравнение $x^2\equiv 4 \pmod{21}$.

21 – составное число. Факторизуем его: $21=3\cdot 7$. Проверим разрешимость исходного сравнения:

$\left(\frac{4}{3}\right)=\left(\frac{1}{3}\right)=1$, $\left(\frac{4}{7}\right)=\left(\frac{2}{7}\right)^2=1$. Сравнение разрешимо и имеет $2^2=4$ решения.

Составим систему: $\begin{cases} x^2\equiv 4 \pmod 3 \\ x^2\equiv 4 \pmod 7 \end{cases}$. Решим каждое из уравнений этой системы. Получим $\begin{cases} x\equiv \pm 1 \pmod 3 \\ x\equiv \pm 2 \pmod 7 \end{cases}$. Итак, имеем 4 системы:

1) $\begin{cases} x\equiv 1 \pmod 3 \\ x\equiv 2 \pmod 7 \end{cases}$ 2) $\begin{cases} x\equiv 1 \pmod 3 \\ x\equiv -2 \pmod 7 \end{cases}$ 3) $\begin{cases} x\equiv -1 \pmod 3 \\ x\equiv 2 \pmod 7 \end{cases}$ 4) $\begin{cases} x\equiv -1 \pmod 3 \\ x\equiv -2 \pmod 7 \end{cases}$

Решая каждую из этих систем по китайской теореме об остатках, получим четыре решения: $x\equiv\pm 2 \pmod{21}$, $x\equiv\pm 5 \pmod{21}$.

ЗАДАНИЯ

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

a) $x^2\equiv 7 \pmod 9$;	g) $x^2\equiv 1 \pmod{32}$;	m) $x^2\equiv 11 \pmod{35}$;
b) $x^2\equiv -1 \pmod{25}$;	h) $x^2\equiv 67 \pmod{81}$;	n) $x^2\equiv 5 \pmod{12}$;
c) $x^2\equiv 32 \pmod{49}$;	i) $x^2\equiv 59 \pmod{125}$;	o) $x^2\equiv 9 \pmod{20}$;
d) $x^2\equiv 1 \pmod 4$;	j) $x^2\equiv 4 \pmod 6$;	p) $x^2\equiv 31 \pmod{105}$;
e) $x^2\equiv 3 \pmod 8$;	k) $x^2\equiv 1 \pmod{15}$;	q) $x^2\equiv 4 \pmod{105}$;
f) $x^2\equiv 9 \pmod{16}$;	l) $x^2\equiv 1 \pmod{24}$;	r) $x^2\equiv 16 \pmod{75}$.

2. Определить, сколько решений имеют сравнения.

a) $x^2\equiv -1 \pmod{59}$;	d) $x^2\equiv 17 \pmod{32}$;	g) $x^2\equiv 1 \pmod{150}$;
b) $x^2\equiv 3 \pmod{83}$;	e) $x^2\equiv 25 \pmod{96}$;	h) $x^2\equiv 4 \pmod{343}$;
c) $x^2\equiv 1 \pmod 8$;	f) $x^2\equiv 2 \pmod{315}$;	i) $x^2\equiv 1 \pmod 2$.

ЗАКЛЮЧЕНИЕ

Изучение теории чисел играет важную роль при подготовке специалистов-математиков. Большинство проблем теории чисел непосредственно или косвенно связано с понятием делимости числа. Поэтому все темы пособия заслуживают полного и глубокого изучения. Теория чисел изучает числа с точки зрения их строения и внутренних связей, рассматривает возможности представить одни числа через другие, более простые по своим свойствам.

Безусловно, настоящее издание не сможет заменить учебники по теории чисел по полноте представленного материала. Однако студентам математических специальностей оно будет интересно тем, что в одном пособии изложен как теоретический материал, так и решение примеров и задач, приведены исторические сведения. Обучающиеся могут использовать этот материал в других научных областях: теории корректирующих кодов, криптографии, методах сжатия информации и управления роботами, распознавании образов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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 XIX 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.

ОГЛАВЛЕНИЕ

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. 4,65. Тираж 50 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.