

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
Федеральное государственное бюджетное  
образовательное учреждение  
высшего профессионального образования  
«Пензенский государственный университет» (ПГУ)

---

Н. Д. Никитин, О. Г. Никитина

# Теория чисел

Учебное пособие

Пенза  
Издательство ПГУ  
2016

УДК 511  
Н62

Р е ц е н з е н т ы:

доктор технических наук, профессор,  
заведующий кафедрой математики и математического моделирования  
Пензенского государственного университета  
архитектуры и строительства  
*А. М. Данилов;*

кандидат физико-математических наук,  
доцент кафедры высшей и прикладной математики  
Пензенского государственного университета  
*Т. В. Елисеева*

**Никитин, Н. Д.**

Н62 Теория чисел : учеб. пособие / Н. Д. Никитин, О. Г. Никитина. – Пенза : Изд-во ПГУ, 2016. – 100 с.

ISBN 978-5-906831-63-7

Изложены такие вопросы теории чисел, как отношение делимости в кольце целых чисел, наибольший общий делитель и наименьшее общее кратное целых чисел, основная теорема арифметики, число и сумма натуральных делителей натурального числа, отношение сравнения в кольце целых чисел и его свойства, функция Эйлера, сравнения первой степени и системы сравнений, индексы и их приложения, а также приложения сравнений. Теоретический материал иллюстрируется подробно разобранными примерами. Содержатся задания для индивидуальной работы студентов.

Издание подготовлено на кафедре «Геометрия и математический анализ» Пензенского государственного университета и предназначено для бакалавров, обучающихся по направлению подготовки «Педагогическое образование» (профиль подготовки «Математика»).

УДК 511

*Рекомендовано к изданию методической комиссией  
факультета физико-математических и естественных наук  
Педагогического института им. В. Г. Белинского  
Пензенского государственного университета  
(протокол № 1 от 07.09.2015)*

ISBN 978-5-906831-63-7

© Пензенский государственный  
университет, 2016

## СОДЕРЖАНИЕ

§ 1. Отношение делимости в кольце $Z$ . Теорема о делении с остатком. Наибольший общий делитель целых чисел.....	4
§ 2. Взаимно простые целые числа. Наименьшее общее кратное целых чисел .....	9
§ 3. Простые и составные числа. Основная теорема арифметики.....	14
§ 4. Числовые функции .....	21
§ 5. Систематические числа. Операции над систематическими числами. Перевод записи числа из одной системы счисления в другую.....	27
§ 6. Конечные цепные дроби. Неопределенные уравнения первой степени с двумя неизвестными .....	32
§ 7. Отношение сравнения в кольце $Z$ . Свойства сравнений .....	42
§ 8. Кольцо классов вычетов. Полная и приведенная системы вычетов .....	44
§ 9. Функция Эйлера и ее свойства. Теоремы Эйлера и Ферма .....	48
§ 10. Сравнения с одной неизвестной. Сравнения первой степени .....	53
§ 11. Системы сравнений первой степени .....	59
§ 12. Сравнения высших степеней по простому модулю.....	64
§ 13. Порядок целого числа и класса вычетов по заданному модулю .....	69
§ 14. Первообразные корни и индексы по простому модулю.....	71
§ 15. Арифметические приложения теории сравнений .....	77
§ 16. Алгебраические и трансцендентные числа. Теорема Лиувилля и ее приложения .....	82
Задания для индивидуальной работы.....	85
Список литературы.....	89
ПРИЛОЖЕНИЕ .....	90

## § 1. Отношение делимости в кольце $Z$ .

### Теорема о делении с остатком.

### Наибольший общий делитель целых чисел

Пусть  $(Z, +, \cdot)$  – кольцо целых чисел,  $a, b \in Z$ .

Говорят, что число  $a$  делится на  $b$ , если существует  $c \in Z$  такое, что  $a = b \cdot c$ .

### Свойства отношения делимости

1.  $\forall (a \in Z) a : a$ , так как  $a = a \cdot 1$ .
2.  $a : b \wedge b : c \Rightarrow a : c$ .
3.  $a : c \wedge b : c \Rightarrow (a \pm b) : c$ .
4.  $a : b \wedge b \nmid c \Rightarrow (a \pm b) \nmid c$ .
5.  $a : c \Rightarrow \forall (b \in Z) (ab) : c$ .
6.  $a : b \Rightarrow (-a) : b \wedge a : (-b) \wedge (-a) : (-b)$ .
7.  $\forall (a \in Z) a \neq 0, a \nmid 0$ .
8.  $a \neq 0 \wedge a : b \Rightarrow |a| \geq |b|$ .

**Определение.** Разделить целое число  $a$  на  $b$  ( $b \neq 0$ ) с остатком – это значит, найти такие целые числа  $q, r \in Z$ , чтобы выполнялось равенство:

$$A = bq + r, 0 \leq r < |b|.$$

Имеет место теорема.

**ТЕОРЕМА 1.** Каковы бы ни были  $a, b \in Z, b \neq 0$ , всегда возможно, и притом однозначно, разделить  $a$  на  $b$  с остатком.

Доказательство.

a)  $b \in Z, b > 0$ . Расположим числа, кратные  $b$ , в возрастающем порядке: ...,  $b(-2), b(-1), b \cdot 0, b \cdot 1, b \cdot 2, \dots$

Пусть  $bq \in Z$  – наибольшее целое число, не превосходящее  $a$ . Тогда  $b \cdot q \leq a < b(q+1)$  и  $0 \leq a - b \cdot q < b$ . Обозначим через  $r = a - b \cdot q$ , тогда:

$$a = b \cdot q + r, 0 \leq r < b.$$

Рассмотрим случай б)  $b \in Z, b < 0$ . Тогда  $-b > 0$ . Согласно случаю а), существуют  $q, r \in Z$  такие, что  $a = (-b) \cdot q + r, 0 \leq r < -b$  или  $a = b \cdot (-q) + r, 0 \leq r < -b$ .

**Единственность.** Пусть  $q, r, q_1, r_1$  такие целые числа, что  $a = b \cdot q + r$  и  $a = b \cdot q_1 + r_1, 0 \leq r < |b|$  и  $0 \leq r_1 < |b|$ . Из этих соотношений имеем:

$$b(q - q_1) = r_1 - r, 0 \leq |r_1 - r| < |b| \Rightarrow |b||q - q_1| = |r_1 - r|. \quad (1.1)$$

Если предположить, что  $q \neq q_1$ , то из (1.1)  $\Rightarrow |r_1 - r| \geq |b|$ . Пришли к противоречию с тем, что  $0 \leq |r_1 - r| < |b|$ . Значит,  $q = q_1$ . Тогда из (1.1) следует, что  $r = r_1$ .

## **Наибольший общий делитель целых чисел. Нахождение наибольшего общего делителя двух целых чисел**

**Определение.** Целое число  $\delta$  называется общим делителем целых чисел  $a_1, a_2, \dots, a_n$ , если  $a_i : \delta (i = \overline{1, n})$ .

Число  $d \in Z$  называется наибольшим общим делителем (НОД) целых чисел  $a_1, a_2, \dots, a_n$ , если:

- а)  $d$  – общий делитель этих чисел;
- б)  $d$  делится на любой другой общий делитель этих чисел.

Из определения следует, что НОД целых чисел определен с точностью до знака. Будем рассматривать только положительные значения НОД целых чисел  $a_1, a_2, \dots, a_n$  и будем его обозначать  $(a_1, a_2, \dots, a_n)$  или НОД  $(a_1, a_2, \dots, a_n)$ .

**ЛЕММА.** Если  $a = bq + r$ , то НОД  $(a, b) =$  НОД  $(b, r)$ .

Рассмотрим вопрос о нахождении НОД двух целых чисел.

Пусть  $a, b \in Z, a \not\equiv b$ . Разделим  $a$  на  $b$  с остатком:  $a = bq_0 + r_1, 0 \leq r_1 < |b|$ . Разделим теперь  $b$  на  $r_1 : b = r_1 q_0 + r_2, 0 \leq r_2 < r_1$ . И так далее.

Этот процесс последовательного деления будем продолжать до тех пор, пока не получим нулевой остаток. Так как последовательность натуральных чисел  $r_1 > r_2 > \dots$  не может быть бесконечной, то существует такое натуральное число  $n \in N$ , что  $r_{n-1} : r_n$ . В результате получим цепочку равенств:



3) если  $a \div m \wedge b \div m$ , то  $\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{(a,b)}{m}$ ;

4) если  $d = (a, b)$ , то  $\exists(x, y \in Z) ax + by = d$ .

### Упражнения

1. Найдите частное и остаток от деления:

а) 764 на 13;

б)  $-764$  на  $(-13)$ ;

в) 764 на  $(-13)$ ;

г)  $-764$  на 13.

2. Найдите наибольшее натуральное число, дающее при делении на 13 неполное частное 17.

3. Найдите остаток от деления целого числа  $a = 15n - 4$ ,  $n \in N$ , на 5.

4. Докажите, что квадрат любого нечетного числа при делении на 8 дает остаток 1.

5. Найдите натуральные числа  $n$  такие, что сумма  $S = 1 + 2 + \dots + n$  при делении на 5 дает остаток 1.

6. Докажите, что любая натуральная степень числа 15 при делении на 7 дает остаток 1.

7. Докажите, что числа вида  $3m + 2$  ( $m = 1, 2, \dots$ ) не являются квадратами целых чисел.

8. Докажите, что произведение любых трех последовательных натуральных чисел делится на 6.

9. Докажите, что все числа вида  $2^{2^n} + 1$  ( $n \geq 2$ ) оканчиваются цифрой 7.

10. Докажите, что числа вида  $2^{4^n} - 5$  ( $n \in N$ ) оканчиваются цифрой 1.

11. Докажите, что из  $n$  последовательных чисел одно и только одно число делится на  $n$ .

12. Докажите, что сумма квадратов двух нечетных чисел не является квадратом целого числа.

13. Докажите, что числа вида  $4^n + 15n - 1$  ( $n \in N$ ) кратны 9.

14. Докажите, что  $\forall(m \in N) m \cdot (m^2 + 5) \div 6$ .

15. Найдите НОД чисел 2585 и 7975.

16. Найдите НОД чисел 1073, 3683, 34 481.

17. Найдите НОД чисел 988, 2014, 42 598, 6726.

18. Сократите дробь  $\frac{21\,120}{30\,720}$ .

19. Найдите линейное представление чисел 90 и 35, 549 и 387.

20. Докажите, что  $(a, b) = (5a + 3b, 13a + 8b)$ .

21. Дробь  $\frac{a}{b}$  несократима. Будет ли несократима дробь  $\frac{a}{a+b}$ ?

22. Докажите, что следующие дроби несократимы при всех натуральных значениях  $n$ :

$$а) \frac{2n+13}{n+7}; \quad б) \frac{2n^2-1}{n+1}; \quad в) \frac{n^2-n+1}{n^2+1}.$$

23. Докажите, что НОД двух последовательных четных чисел равен 2, а нечетных 1.

24. Если  $(a, b) = 1$ , то  $(a + b, a - b)$  равен либо 1, либо 2. Докажите это.

25. Докажите, что если  $(a, b) = 1$ , то  $(a + b, a^2 - ab + b^2)$  равен 1 или 3.

26. Докажите, что если  $(a, b) = 1$ , то  $(a + b, a^2 + b^2)$  равен 1 или 2.

27. Числитель дроби – разность квадратов двух нечетных чисел; знаменатель – сумма квадратов тех же чисел. Докажите, что дробь сократима на 2, но несократима на 4.

28. Решите в натуральных числах систему уравнений:

$$а) \begin{cases} xy = 8400, \\ (x, y) = 20; \end{cases} \quad б) \begin{cases} x + y = 150, \\ (x, y) = 30; \end{cases} \quad в) \begin{cases} (x, y) = 150, \\ \frac{x}{y} = \frac{11}{7}. \end{cases}$$

## § 2. Взаимно простые целые числа. Наименьшее общее кратное целых чисел

**Определение.** Целые числа  $a_1, a_2, \dots, a_n$  называются взаимно простыми, если  $\text{НОД}(a_1, a_2, \dots, a_n) = 1$ .

### Свойства взаимно простых чисел

1)  $a, b \in Z$  являются взаимно простыми  $\Leftrightarrow \exists(x, y \in Z) ax + by = 1$ .

Доказательство:

*a)* по условию  $(a, b) = 1$ . В силу свойства 4 НОД целых чисел  $\exists(x, y \in Z) ax + by = 1$ ;

*б)* по условию  $ax + by = 1 (x, y \in Z)$ . Пусть  $(a, b) = d$ . Тогда  $ax + by = 1 \Rightarrow 1 : d, d \in N \wedge 1 : d \Rightarrow d = 1$ . Следовательно,  $a$  и  $b$  взаимно простые целые числа.

*Следствие.* Если  $\text{НОД}(a, b) = 1$  и  $a : a_1, b : b_1 \Rightarrow (a_1, b_1) = 1$ .

Доказательство.  $(a, b) = 1 \Rightarrow \exists(x, y \in Z) ax + by = 1$ . Учитывая, что  $a = a_1 m \wedge b = b_1 n$ , имеем:  $a_1(mx) + b_1(ny) = 1$ . Отсюда следует, что  $a_1, b_1$  взаимно простые числа;

2) если  $(a, b) = d$ , то числа  $\frac{a}{d}, \frac{b}{d}$  взаимно простые;

3) если  $(ab) : c \wedge (a, c) = 1 \Rightarrow b : c$ .

Доказательство. Так как  $(a, c) = 1$ , то  $\exists(x, y \in Z) ax + cy = 1$ . Умножив обе части этого равенства на  $b$ , получим  $(ab)x + (cb)y = b$ . Отсюда следует, что  $b : c$ ;

4) если  $(a, b) = 1$ , то  $c : (ab) \Leftrightarrow c : a \wedge c : b$ ;

5) если  $(a, c) = 1$  и  $(b, c) = 1$ , то  $(ab, c) = 1$ .

### Наименьшее общее кратное целых чисел

Целое число  $k \in Z$  называется общим кратным целых чисел  $a_1, a_2, \dots, a_k$ , если  $k : a_i (i = \overline{1, k})$ .

Целое число  $m \in Z$  называется наименьшим общим кратным (НОК) целых чисел  $a_1, a_2, \dots, a_k$ , если выполняются условия:

*a)*  $m$  – общее кратное целых чисел  $a_1, a_2, \dots, a_k$ ;

*б)* любое общее кратное этих целых чисел делится на  $m$ .

Из определения следует, что НОК целых чисел  $a_1, a_2, \dots, a_k$  определено с точностью до знака. Будем рассматривать только положи-

тельное значение НОК целых чисел и обозначать НОК  $(a_1, a_2, \dots, a_k)$  или  $[a_1, a_2, \dots, a_k]$ .

$$\text{ТЕОРЕМА 1. } \forall(a, b \in N) [a, b] = \frac{a \cdot b}{(a, b)}.$$

Доказательство. Обозначим через  $t = \frac{a \cdot b}{(a, b)}$ . Пусть НОД  $(a, b) = d$ , тогда

$$a = a_1 d, b = b_1 d, a_1, b_1 \in N, (a_1, b_1) = 1.$$

С учетом того, что  $a = a_1 d, b = b_1 d$ , имеем  $t = a_1 b_1 d$ . Отсюда следует, что  $t$  – общее кратное целых чисел  $a$  и  $b$ . Пусть  $l$  общее кратное чисел  $a, b$ . Тогда  $l = l_1 a$ . Из  $l = l_1 a \wedge l : b \Rightarrow (l_1 \cdot a_1) : b_1, (l_1 \cdot a_1) : b_1 \wedge (a_1, b_1) = 1 \Rightarrow l_1 : b_1$ . Существует  $l_2 \in N$  такое, что  $l_1 = l_2 b_1$ . Тогда  $l = l_1 a_1 d = l_2 a_1 b_1 d_1$ . Так как  $t = a_1 b_1 d_1$ , то  $l : t$ . Показано, что  $t$  – наименьшее общее кратное целых чисел  $a, b$ .

*Следствие 1.* Для  $\forall(a, b \in Z), a \neq 0$  и  $b \neq 0$ , существует НОК этих чисел.

*Следствие 2.* Наименьшее положительное общее кратное чисел  $a, b \in Z$  является НОК этих целых чисел.

### Свойства НОК целых чисел

$$1. \forall(a, b \in N) \forall(m \in N) [ma, mb] = m[a, b].$$

$$2. \forall(a, b \in N) \forall(m \in N) \text{ если } a : m \wedge b : m, \text{ то } \left[ \frac{a}{m}, \frac{b}{m} \right] = \frac{[a, b]}{m}.$$

**ТЕОРЕМА 2.** Пусть  $a_1, a_2, \dots, a_n \in Z$ . Если  $[a_1, a_2] = m_1, [a_3, m_1] = m_2, \dots, [a_n, m_{n-2}] = m_{n-1}$ , то  $[a_1, a_2, \dots, a_n] = m_{n-1}$ .

#### Пример 1

Найти наименьшее общее кратное чисел 624, 408 и 748.

#### Решение

Согласно теореме 2  $[624, 408, 748] = [[624, 408], 748]$ . По теореме 1,  $[624, 408] = \frac{624 \cdot 408}{(624, 408)}$ . Найдем  $(624, 408)$ , применив к этим числам алгоритм Евклида:  $624 = 408 \cdot 1 + 216, 408 = 216 \cdot 1 + 192,$

$216 = 192 \cdot 1 + 24$ ,  $192 = 24 \cdot 8$ . Следовательно,  $(624, 408) = 24$ , поэтому  $[624, 408] = \frac{624 \cdot 408}{24} = 10608$ . Тогда

$$[624, 408, 748] = [10608, 748] = \frac{10608 \cdot 748}{(10608, 748)}.$$

Найдем  $(10608, 748)$ :  $10608 = 748 \cdot 14 + 136$ ,  $748 = 136 \cdot 5 + 68$ ,  $136 = 68 \cdot 2$ . Следовательно,  $(10608, 748) = 68$  и  $[624, 408, 748] = \frac{10608 \cdot 748}{(10608, 748)} = \frac{10608 \cdot 748}{68} = 116688$ .

### Пример 2

Решить в натуральных числах систему уравнений

$$\begin{cases} 3x - 10y = 88, \\ [x, y] - 5y = 380. \end{cases}$$

### Решение

Пусть  $(x, y) = d$ , тогда  $x = nd$ ,  $y = md$ , где  $n$  и  $m$  – взаимно простые натуральные числа. Так как  $[x, y] = dnm$ , то систему можно записать в виде

$$\begin{cases} 3nd - 10md = 88, \\ dnm - 5md = 380 \end{cases} \quad \text{или} \quad \begin{cases} d(3n - 10m) = 88, \\ d(nm - 5m) = 380. \end{cases}$$

Из первого уравнения системы следует, что  $88 \div d$ , т.е.  $(2^3 \cdot 11) \div d$ . Из второго уравнения системы следует, что  $380 \div d$ , т.е.  $(2^2 \cdot 5 \cdot 19) \div d$ . Так как числа 88 и 380 имеют общими делителями только 1, 2 и 4, то  $d$  может принимать только одно из этих значений. Рассмотрим эти случаи.

1. Пусть  $d = 1$ , тогда система примет вид

$$\begin{cases} 3n - 10m = 88, \\ nm - 5m = 380. \end{cases}$$

Если умножим первое уравнение на  $m$ , второе – на  $-3$ , а затем их сложим, то получим

$$-10m^2 + 15m = 88m - 1140, \quad \text{или} \quad 10m^2 + 73m - 1140 = 0.$$

Корни этого уравнения не являются натуральными числами. Следовательно, при  $d = 1$  система не имеет решений.

2. Пусть  $d = 2$ , тогда система примет вид

$$\begin{cases} 2(3n - 10m) = 88, \\ 2(nm - 5m) = 380. \end{cases}$$

Аналогично можно показать, что эта система также не имеет решений в натуральных числах.

3. При  $d = 4$  получим систему

$$\begin{cases} 4(3n - 10m) = 88, \\ 4(nm - 5m) = 380 \end{cases} \text{ или } \begin{cases} 3n - 10m = 22, \\ nm - 5m = 95. \end{cases}$$

Найдем ее решения. Если умножим первое уравнение на  $-m$ , второе – на 3, а затем их сложим, то получим

$$10m^2 - 15m = -22m + 285, \text{ или } 10m^2 + 7m - 285 = 0.$$

Корни этого уравнения 5 и  $-5,7$ . Значит,  $m = 5$ . Из первого уравнения системы получим, что  $n = 24$ . Отсюда следует, что  $x = 96$ ,  $y = 20$  – решение системы.

### Упражнения

1. Разность двух нечетных чисел равна  $2^n$ . Докажите, что эти числа взаимно простые.

2. Найдите НОК чисел:

а) 1073, 3683, 34 481;

б) 420, 126, 525;

в) 529, 1541, 1817.

3. Найдите НОД следующих чисел:

а)  $d = (a, b)$  и  $m = [a, b]$ ;

б)  $ab$  и  $m = [a, b]$ ;

в)  $a + b$  и  $m = [a, b]$ .

4. Найдите НОК трех последовательных натуральных чисел.

5. Докажите, что  $\left(\frac{x}{a}, \frac{x}{b}\right) = 1 \Leftrightarrow x = [a, b]$ .

6. Докажите, что если  $(a, c) = (b, c) = 1$ , то  $(a \cdot b, c) = 1$ .

7. Если  $(a, c) = 1$ , то  $b \div (ab, c)$ . Докажите это.

8. Если  $(a, b) = 1$ , то  $(a \cdot c, b) = (c, b)$ . Докажите это.

9. Докажите, что для натуральных чисел  $m, n, k$  имеет место соотношение  $mnk = [m, n, k] \cdot (mn, mk, nk)$ .

10. Решите в натуральных числах следующие системы уравнений:

$$a) \begin{cases} xy = 20, \\ [x, y] = 10; \end{cases} \quad б) \begin{cases} xy = 120, \\ [x, y] = 60; \end{cases}$$

$$в) \begin{cases} \frac{x}{y} = \frac{3}{4}, \\ [x, y] = 84; \end{cases} \quad г) \begin{cases} \frac{x}{y} = \frac{5}{7}, \\ [x, y] = 280. \end{cases}$$

11. Докажите, что если  $(ax - by) : m, (a - b) : m$  и числа  $a, b$  взаимно простые, то  $(x - y) : m$ .

12. Натуральные числа  $a, b$  и  $c$  таковы, что  $\text{НОК}(a, b) = 60$  и  $\text{НОК}(a, c) = 270$ . Найдите  $\text{НОК}(b, c)$  (олимпиада «Ломоносов»).

13. Натуральные числа  $m$  и  $n$  таковы, что  $\text{НОД}(n, m) + \text{НОК}(n, m) = n + m$ . Докажите, что одно из них является делителем другого (олимпиада «Ломоносов»).

14. Решите в натуральных числах следующие системы уравнений:

$$a) \begin{cases} 5x - 2y = 55, \\ [x, y] - 4x = 75; \end{cases} \quad б) \begin{cases} 6x - 7y = 18, \\ [x, y] - 2x = 24; \end{cases}$$

$$в) \begin{cases} 2x - 3y = 8, \\ [x, y] - 5y = 32; \end{cases} \quad г) \begin{cases} 4x - 7y = 6, \\ [x, y] - 8y = 70. \end{cases}$$

### § 3. Простые и составные числа. Основная теорема арифметики

Целое число  $a$ ,  $a \neq 0$ ,  $a \neq \pm 1$ , называется простым целым числом, если его делителями являются только  $\pm 1$  и  $\pm a$ . Целое число  $a$ ,  $a \neq 0$ , называется составным целым числом, если оно имеет делители, отличные от  $\pm 1$  и  $\pm a$ .

**ТЕОРЕМА 1.** Любое число  $n \in N$  ( $n > 1$ ) имеет хотя бы один простой делитель  $p \in N$ .

Доказательство. Доказательство проведем методом математической индукции:

а)  $n = 2$ , 2 – простое число и  $2 : 2$ . Пусть  $a \in N$ ,  $a > 1$ ;

б) предположим, что  $\forall (m \in N)$ ,  $2 \leq m < a$ , имеет хотя бы один простой делитель. Покажем, что  $a \in N$  имеет простой делитель. Если  $a$  простое число, то утверждение верно. Если  $a$  – составное, то  $a$  можно представить в виде

$$a = n_1 \cdot n_2,$$

где  $n_1, n_2 \in N$ .

Так как  $2 \leq n_1 < a$ ,  $2 \leq n_2 < a$ , то по индуктивному предположению числа  $n_1, n_2$  имеют простые делители. Пусть  $p \in N$  – простой делитель  $n_1$ , тогда  $p$  является простым делителем числа  $a$ . Согласно принципу математической индукции,  $\forall (a \in N)$   $a \geq 2$  имеет хотя бы один простой делитель.

**ТЕОРЕМА 2.** Для  $\forall (a_i \in N), i = \overline{1, n}$ , если  $(a_1, a_2, \dots, a_n) : p$ , где  $p$  – простое число, то хотя бы один из сомножителей этого произведения делится на  $p$ .

**ТЕОРЕМА 3 (основная теорема арифметики).** Любое  $n \in N$  ( $n \geq 2$ ) можно представить в виде произведения простых натуральных чисел, и такое представление единственно с точностью до порядка сомножителей в этом произведении.

Доказательство.

I. Возможность представления  $n \in N$  ( $n \geq 2$ ) в виде произведения простых натуральных чисел.

Доказательство проведем методом математической индукции:

а)  $n = 2$ , 2 – простое число. Пусть  $a \in N$ ,  $a > 1$ ;

б) предположим, что  $\forall (m \in N)$ ,  $1 < m < a$ , можно представить в виде произведения простых натуральных чисел. Покажем, что

$a$  можно представить в виде произведения простых чисел. Если  $a$  простое число, то утверждение верно. Если  $a$  – составное, то  $a = n_1 n_2$  ( $n_1, n_2 \in N$ ),  $n_1 \neq 1$ ,  $n_2 \neq 1$ . Так как  $1 < n_1 < a$  и  $1 < n_2 < a$ , то  $n_1, n_2$ , в силу индуктивного предположения, можно представить в виде  $n_1 = p_1 p_2 \dots p_k$ ,  $n_2 = p_{k+1} p_{k+2} \dots p_l$ , где  $p_i$  ( $i = \overline{1, l}$ ) простые натуральные числа. Тогда  $a = p_1 p_2 \dots p_k p_{k+1} p_{k+2} \dots p_l$ . Согласно принципу математической индукции, любое  $n \in N$  ( $n \geq 2$ ) можно представить в виде произведения простых натуральных чисел.

## II. Единственность.

Доказательство проведем также методом математической индукции:

а) при  $n = 2$ , утверждение верно. Пусть  $a \in N$ ,  $1 < a$ ;

б) предположим, что представление  $\forall (m \in N) 2 \leq m < a$  в виде произведения простых натуральных чисел единственно с точностью до порядка сомножителей. Покажем справедливость утверждения для  $a$ .

Пусть  $a$  имеет следующие представления в виде произведения простых натуральных чисел:

$$a = p_1 p_2 \dots p_s \text{ и } a = q_1 q_2 \dots q_k. \quad (3.1)$$

Из равенств (3.1) имеем, что  $p_1 p_2 \dots p_s = q_1 q_2 \dots q_k$ . Отсюда следует, что  $(p_1, p_2, \dots, p_s) : q_1$ . Согласно теореме 2 один из сомножителей произведения делится на  $q_1$ . Пусть  $p_1 : q_1$ . Из того, что  $p_1$  и  $q_1$  – простые натуральные числа и  $p_1 : q_1$ , следует  $p_1 = q_1$ . Тогда из равенства  $p_1 p_2 \dots p_s = q_1 q_2 \dots q_k$  имеем:

$b = p_2 \dots p_s = q_2 \dots q_k$ . Так как  $2 \leq b < a$ , то по индуктивному предположению

$s = k$  и при соответствующей нумерации сомножителей получим, что  $p_2 = q_2, p_3 = q_3, \dots, p_s = q_s$ . Согласно принципу математической индукции, представление  $\forall (n \in N) n \geq 2$  в виде произведения простых натуральных чисел единственно с точностью до порядка сомножителей.

**Определение.** Каноническим разложением целого числа  $n > 1$  называется представление  $n$  в виде

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k},$$

где  $p_1, p_2, \dots, p_k$  – попарно различные простые числа, а  $\alpha_1, \alpha_2, \dots, \alpha_k$  – натуральные числа. Для отрицательных целых чисел  $n < -1$  каноническим представлением считается представление числа  $n$  в виде

$$n = -p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}.$$

Так, например,  $1500 = 2^2 \cdot 3 \cdot 5^3$ .

## Бесконечность множества простых чисел

**ТЕОРЕМА 4.** Множество простых натуральных чисел бесконечно.

Доказательство. Достаточно показать, что для каждого конечного множества простых чисел существует такое простое число, которое не принадлежит этому множеству. Пусть  $M = \{p_1, p_2, \dots, p_k\}$  – конечное множество простых чисел. Рассмотрим число  $a = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$ . Так как  $a > 1$ , то по теореме 1 число  $a$  делится хотя бы на одно простое число  $p$ . Если предположим, что  $p \in M$ , то из равенства  $a = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$  следует, что 1 делится на  $p$ . Пришли к противоречию. Значит, простое число  $p \notin M$ . Показано, что множество простых натуральных чисел бесконечно.

**ТЕОРЕМА 5 (теорема Евклида).** Для любого натурального  $n$ ,  $n > 1$ , существует отрезок натуральных чисел длины  $n$ , не содержащий ни одного простого натурального числа.

Доказательство. Рассмотрим последовательность натуральных чисел

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1). \quad (3.2)$$

Число чисел в последовательности (3.2) равно  $n$ , и каждое число этой последовательности составное. Этот пример доказывает утверждение теоремы.

Из теорем 4 и 5 следует сложный характер распределения простых чисел в натуральном ряду.

## Решето Эратосфена

Греческий ученый Эратосфен (ок. 276–194 гг. до н.э.) предложил простой метод нахождения всех простых натуральных чисел, не превосходящих данного натурального числа. Этот метод получил название «решето Эратосфена». Чтобы описать этот метод, докажем следующее утверждение.

**ТЕОРЕМА 6.** Любое составное число  $a$  имеет хотя бы один простой натуральный делитель  $p$ ,  $p \leq \sqrt{a}$ .

Доказательство. Обозначим через  $p$  наименьший положительный делитель числа  $a$ ,  $p \neq 1$ . Покажем, что  $p$  – простое число. Если предположим, что число  $p$  составное, то, согласно теореме 1,  $p$  делится хотя бы на одно простое число  $q$ . Пришли к противоречию с тем,

что  $p$  – наименьший натуральный делитель числа  $a$ . Следовательно,  $p$  – простое число,  $a = pb$ ,  $b \in N$ ,  $p \leq b$ . Если умножим обе части неравенства  $p \leq b$  на  $p$ , то, учитывая, что  $a = pb$ , получим  $p^2 \leq a$ . Отсюда следует, что  $p \leq \sqrt{a}$ .

*Следствие.* Если натуральное число  $a$  не делится ни на одно простое число  $p$ ,  $p \leq \sqrt{a}$ , то число  $a$  является простым.

Опишем теперь метод нахождения всех простых натуральных чисел, не превосходящих данного натурального числа  $a$ .

Для этого рассмотрим последовательность натуральных чисел

$$2, 3, 4, 5, 6, 7, 8, \dots, a. \quad (3.3)$$

Первым простым числом в этой последовательности является число 2. В последовательности (3.3) вычеркнем каждое второе число после числа 2. После числа 2 первым простым числом является число 3. Вычеркнем в последовательности (3.3) каждое третье число после числа 3, считая и вычеркнутые числа. После числа 3 первым простым числом является число 5. Вычеркнем теперь в последовательности (3.3) каждое пятое число после простого числа 5, считая и зачеркнутые числа, и так далее. Этот процесс последовательного вычеркивания будем продолжать до наибольшего простого числа  $p$ ,  $p \leq \sqrt{a}$ . В силу следствия теоремы 6 получим, что незачеркнутыми числами последовательности (3.3) будут только простые числа.

### Пример 1

Найдем все простые числа, не превосходящие 40.

### Решение

Наибольшее простое число, меньшее  $\sqrt{40}$ , это 5. Поэтому в последовательности

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, \\ 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40$$

вычеркнем сначала каждое второе число после числа 2, затем каждое третье число после числа 3, считая и вычеркнутые числа, а затем каждое пятое число после числа 5, считая и вычеркнутые числа. В результате получим

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, \\ 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40.$$

Оставшиеся невычеркнутые числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 – простые.

### Распределение простых чисел в ряду натуральных чисел. Неравенство Чебышева

Пусть  $\pi(x)$  – функция, позволяющая найти число простых чисел, которые не превышают  $x$ .

В работе «Мемуар о простых числах» (1850 г.) П. Л. Чебышев установил границы, в которых заключены значения функции  $\pi(x)$ .

$$0,92129 \cdot \frac{x}{\ln x} < \pi(x) < 1,10555 \cdot \frac{x}{\ln x}.$$

Неравенство Чебышева впервые дало возможность судить о характере возрастания функции  $\pi(x)$  при возрастании  $x$  и доказать теорему, называемую асимптотическим законом распределения простых чисел:

$$\pi(x) \sim \frac{x}{\ln x}.$$

#### Пример 2

Доказать, что для всех простых чисел  $p$ , больших 7,  $p^6 - 1$  делится на 504.

#### Решение

Введём обозначение:  $p^6 - 1 = a$ . Легко видеть, что  $504 = 8 \cdot 9 \cdot 7$ . Так как 8, 9, 7 попарно взаимно простые числа, то  $a$  делится на 504 тогда и только тогда, когда  $a$  делится одновременно на 8, 9 и 7.

Представим число  $a$  в виде произведения:

$$a = p^6 - 1 = (p^3 - 1)(p^3 + 1) = (p - 1)(p + 1)(p^2 - p + 1)(p^2 + p + 1).$$

1. Докажем сначала, что  $a$  делится на 8. Так как  $p$  простое число, то оно нечетное, т.е.  $p = 2k + 1, k \in N$ .

При  $p = 2k + 1, a = 4k(k + 1)(4k^2 + 2k + 1)(4k^2 + 6k + 3)$ . Так как  $k(k + 1)$  как произведение двух последовательных целых чисел делится на 2, то  $a$  делится на 8.

2. Докажем, что  $a$  делится на 9. Так как  $p$  простое число и  $p > 7$ , то  $p$  не делится на 3. Тогда  $p = 3k + r$ , где  $r = 1$  или  $r = 2$ .

При  $p = 3k + 1, a = 9k(3k + 2)(9k^2 + 3k + 1)(3k^2 + 3k + 1)$ . Отсюда следует, что  $a$  делится на 9. Аналогично при  $p = 3k + 2$  получим, что

$$a = 9k(k + 1)(3k + 1)(3k^2 + 3k + 1)(9k^2 + 15k + 7),$$

т.е.  $a$  делится на 9.

3. Докажем, что  $a$  делится на 7. Разделим  $p$  на 7 с остатком:  $p = 7k + r$ , где  $k, r \in \mathbb{N}$ ,  $0 < r < 7$ , так как  $p$  – простое число. Легко видеть, что при  $p = 7k + 1$  первый сомножитель разложения  $a$  делится на 7, аналогично при  $p = 7k + 2$  – четвертый сомножитель делится на 7, при  $p = 7k + 3$  – третий сомножитель, при  $p = 7k + 4$  – четвертый сомножитель, при  $p = 7k + 5$  – третий сомножитель и при  $p = 7k + 6$  второй сомножитель делится на 7.

Таким образом,  $a$  делится на 8, 9, и 7 одновременно. Следовательно, число  $a$  делится на 504.

### Упражнения

1. Напишите каноническое разложение чисел 15754 и 111111. Найдите  $(1575, 11111)$  и  $[1575, 11111]$ .

2. Простыми или составными являются числа 101 и 1001?

3. Выясните, простыми или составными являются числа:  
а) 127;      б) 919;      в) 7429.

4. Используя решето Эратосфена, найдите простые числа, заключенные между:

а) 100 и 110;      б) 240 и 256;      в) 300 и 320;      г) 150 и 180.

5. Докажите, что квадрат числа  $n = 3m + 2$  ( $m = 1, 2, \dots$ ) не может быть представлен в виде суммы квадрата натурального числа и простого числа.

6. Является ли простым число  $43^{111} + 8^{37}$ ?

7. Установите, является ли число  $n^4 + 64$  ( $n \in \mathbb{Z}$ ) простым или составным.

8. Установите, является ли простым или составным число  $n^3 - 6n^2 + 12n + 117$  ( $n \in \mathbb{Z}$ ).

9. Числа  $p$  и  $2p + 1$  простые ( $p > 3$ ). Докажите, что число  $4p + 1$  составное.

10. Пусть  $p > 5$  – простое число. Докажите, что  $p^2 - 1$  делится на 24.

11. Докажите, что между натуральными числами  $n$  и  $n!$ , где  $n > 2$ , существует по крайней мере одно простое число.

12. Найдите целые значения  $n$  такие, чтобы числа были бы простыми:

- а)  $n, n + 10, n + 14$ ;    б)  $n, n + 10, n + 20$ ;    в)  $n, n + 2, n + 16$ ;  
г)  $n, n + 4, n + 14$ ;    д)  $n, n - 10, n - 20$ .

13. Найдите все простые числа  $p$ , для которых числа  $p + 2, p + 6, p + 8, p + 12, p + 14$  являются простыми.

14. Найдите все простые числа  $p$ , чтобы число  $p^2 + 13$  также было простым.

15. Докажите, что указанные ниже числа одновременно не могут быть простыми:

- а)  $n + 5, n + 10$ ;    б)  $n, n + 2$  и  $n + 5$ ;    в)  $2^n - 1, 2^n + 1$ ,  
где  $n$  – натуральное число,  $n > 2$ .

16. Найдите все простые числа вида  $\frac{n(n+1)}{2} - 1, n \in N$ .

17. Сколько существует способов разложения числа  $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_l^{k_l}$  в произведение двух взаимно простых множителей, отличных от 1 и  $n$ ?

## § 4. Числовые функции

### Число и сумма натуральных делителей натурального числа

Пусть  $n \in N$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  – каноническое разложение числа  $n$  на произведение простых множителей.

Любой натуральный делитель  $d$  числа  $n$  можно представить в виде

$$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k},$$

где  $\delta_i \in M_i$ ,  $M_i = \{0, 1, 2, \dots, \alpha_i\}$ ,  $i = \overline{1, k}$ .

**ТЕОРЕМА 1.** Пусть  $n \in N$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  – каноническое разложение числа  $n$  на произведение простых множителей. Для числа  $n$  число его натуральных делителей

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

Доказательство. Любой натуральный делитель  $d$  числа  $n$  можно представить в виде

$$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k},$$

где  $\delta_i \in M_i$ ,  $M_i = \{0, 1, 2, \dots, \alpha_i\}$ ,  $i = \overline{1, k}$ .

Обозначим  $M = M_1 \times M_2 \times \dots \times M_k$ . Так как  $|M_1| = \alpha_1 + 1$ ,  $|M_2| = \alpha_2 + 1$ , ...,  $|M_k| = \alpha_k + 1$  ( $|M_i|$  – число элементов конечного множества  $M_i$ ), то  $|M| = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ . Обозначим через  $T$  множество всех натуральных делителей числа  $n$ . Построим отображение  $f: T \rightarrow M$ , полагая для любого  $d \in T$   $d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k}$ ,  $f(d) = (\delta_1, \delta_2, \dots, \delta_k)$ . Покажем, что  $f$  – биективное отображение. Так как для любого набора  $(v_1, v_2, \dots, v_k) \in M$  число  $d = p_1^{v_1} \cdot p_2^{v_2} \cdot \dots \cdot p_k^{v_k}$  является натуральным делителем числа  $n$ , то  $f(d) = (v_1, v_2, \dots, v_k)$ . Значит,  $f$  сюръективно.

Если  $d_1 = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k}$ ,  $d_2 = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_k^{s_k}$  – натуральные делители числа  $n$  и  $d_1 \neq d_2$ , то  $(\delta_1, \delta_2, \dots, \delta_k) \neq (s_1, s_2, \dots, s_k)$ , т.е.  $f(d) \neq f(d_2)$ . Следовательно, отображение  $f$  инъективно.

Так как множества  $T$  и  $M$  конечные и отображение  $f: T \rightarrow M$  биективное, то  $|T| = |M|$ . Значит,  $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ .

**ТЕОРЕМА 2.** Пусть  $n \in N$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  – каноническое разложение числа  $n$  на произведение простых множителей. Сумма всех натуральных делителей числа  $n$ :

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

Доказательство. Любой натуральный делитель  $d$  числа  $n$  можно представить в виде

$$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k},$$

где  $\delta_i \in M_i$ ,  $M_i = \{0, 1, 2, \dots, \alpha_i\}$ ,  $i = \overline{1, k}$ . Рассмотрим произведение

$$(1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \dots (1 + p_k + p_k^2 + \dots + p_k^{\alpha_k}). \quad (4.1)$$

Если найдем произведение всех сомножителей в (4.1), то получим сумму слагаемых, каждое из которых является натуральным делителем числа  $n$ , причем каждый делитель числа  $n$  входит в качестве слагаемого в эту сумму только один раз. Так как по формуле для суммы членов геометрической прогрессии

$$1 + p_i + p_i^2 + \dots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \quad (i = \overline{1, k}),$$

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

### Пример 1

Найти натуральное число  $m$ , имеющее девять натуральных делителей, сумма которых равна 217.

### Решение

Пусть  $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , тогда  $\tau(m) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ . Так как по условию  $\tau(m) = 9$ , т.е.  $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) = 9 = 3 \cdot 3$ , то  $k = 2$  (случай  $k = 1$  не возможен). Из равенства  $(\alpha_1 + 1)(\alpha_2 + 1) = 3 \cdot 3$  следует, что  $\alpha_1 = 2, \alpha_2 = 2$ . Значит,  $m = p_1^2 p_2^2$ . Так как

$$\sigma(m) = \frac{p_1^3 - 1}{p_1 - 1} \cdot \frac{p_2^3 - 1}{p_2 - 1} = (p_1^2 + p_1 + 1)(p_2^2 + p_2 + 1)$$

и по условию  $\sigma(m) = 217$ , то  $(p_1^2 + p_1 + 1)(p_2^2 + p_2 + 1) = 217 = 7 \cdot 31$ . Отсюда с учетом того, что  $\alpha_1 = \alpha_2$ , получим  $p_1^2 + p_1 + 1 = 7$  и  $p_2^2 + p_2 + 1 = 31$ . Эти равенства возможны только тогда, когда  $p_1 = 2, p_2 = 5$ . Таким образом,  $m = 2^2 \cdot 5^2 = 100$ .

### Функция $E(x)$ и ее применение в теории чисел

Функция  $E(x)$  каждому действительному числу  $x$  ставит в соответствие наибольшее целое число  $m$ , удовлетворяющее условию  $m \leq x < m + 1$ . Это целое число обозначают  $[x]$ .

#### Пример 2

$$E(-5,6) = -6, E(5,75) = 5, \text{ т.е. } [-5,6] = -6, [5,75] = 5.$$

Разность  $x - E(x)$  называется дробной частью числа  $x$ ,  $0 \leq x - E(x) < 1$ . Дробную часть числа  $x$  обозначают  $\{x\}$ . Например,  $\{-5,6\} = 0,4$ ,  $\{5,75\} = 0,75$ .

Любое действительное число  $x$  можно представить в виде  $x = [x] + \{x\}$ .

Справедливы утверждения.

**ТЕОРЕМА 3.** Пусть  $m, n \in N$ . Число натуральных чисел, кратных  $m$  и не превосходящих  $n$ , равно  $E\left(\frac{n}{m}\right)$ .

Доказательство. Пусть  $m, n \in N$ . Разделим  $n$  на  $m$  с остатком:

$$n = mq + r, 0 \leq r < m. \quad (4.2)$$

Натуральные числа  $m, 2m, \dots, mq$ , кратные числу  $m$ , не превосходят числа  $n$ . Разделив обе части равенства (4.2) на  $m$ , получим  $\frac{n}{m} = q + \frac{r}{m}$ . Так как  $0 \leq \frac{r}{m} < 1$ , то  $E\left(\frac{n}{m}\right) = q$ .

**ТЕОРЕМА 4.** Пусть  $n$  – натуральное число,  $n > 1$ ,  $p$  – простое натуральное число и  $p^k \leq n < p^{k+1}$ . Простое число  $p$  входит в каноническое разложение числа  $n!$  с показателем

$$m = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + \dots + E\left(\frac{n}{p^{k-1}}\right) + E\left(\frac{n}{p^k}\right).$$

Доказательство. В силу теоремы 3, среди чисел  $1, 2, \dots, n$  имеется  $E\left(\frac{n}{p}\right)$  чисел, кратных  $p$ ,  $E\left(\frac{n}{p^2}\right)$  чисел, кратных  $p^2$ , ...,  $E\left(\frac{n}{p^k}\right)$  чисел, кратных  $p^k$ . Поэтому среди этих чисел существует  $E\left(\frac{n}{p}\right) - E\left(\frac{n}{p^2}\right)$  чисел, кратных  $p$ , но не кратных  $p^2$ ,  $E\left(\frac{n}{p^2}\right) - E\left(\frac{n}{p^3}\right)$  чисел, кратных  $p^2$ , но не кратных  $p^3$ , ...,  $E\left(\frac{n}{p^{k-1}}\right) - E\left(\frac{n}{p^k}\right)$  чисел, кратных  $p^{k-1}$ , но не кратных  $p^k$ . Каждое число  $1, 2, \dots, n$ , кратное  $p$ , но не кратное  $p^2$ , дает в произведении  $n! = 1 \cdot 2 \cdot \dots \cdot n$  один простой множитель, равный  $p$ . Числа, кратные  $p^2$ , но не кратные  $p^3$ , дают в произведении  $n!$  два таких множителя, ..., числа, кратные  $p^{k-1}$ , но не кратные  $p^k$ , дают в произведении  $n!$   $k-1$  таких множителей. Числа, кратные  $p^k$ , дают в произведении  $n!$   $k$  простых множителей, каждый из которых равен  $p$ . Поэтому число  $p$  входит в каноническое разложение числа  $n!$  с показателем

$$m = \left( E\left(\frac{n}{p}\right) - E\left(\frac{n}{p^2}\right) \right) + \dots + (k-1) \left( E\left(\frac{n}{p^{k-1}}\right) - E\left(\frac{n}{p^k}\right) \right) + k \cdot E\left(\frac{n}{p^k}\right).$$

Если раскроем скобки и приведем подобные слагаемые, то получим

$$m = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + \dots + E\left(\frac{n}{p^{k-1}}\right) + E\left(\frac{n}{p^k}\right).$$

Теорема доказана.

Нахождение чисел  $E\left(\frac{n}{p}\right), E\left(\frac{n}{p^2}\right), \dots, E\left(\frac{n}{p^k}\right)$  удобно проводить по следующей схеме:

$$\begin{array}{r|l} n & p \\ \hline r_1 & q_1 \quad p \\ & \hline & r_2 \quad q_2 \\ & \dots \\ & \dots \\ & q_k \quad p \\ & \hline & q_k \quad 0 \end{array}$$

Этот процесс последовательного деления следует проводить до тех пор, пока не получим неполное частное, меньшее  $p$ . Тогда показатель  $t$ , с которым простое число  $p$  входит в каноническое разложение числа  $n!$ , равен  $q_1 + q_2 + \dots + q_k$ .

### Пример 3

Выяснить, с каким показателем входит число 7 в каноническое разложение числа  $351!$ .

Решение. Найдем числа  $E\left(\frac{351}{7}\right)$ ,  $E\left(\frac{351}{7^2}\right)$ ,  $E\left(\frac{351}{7^3}\right)$  по приведенной схеме:

$$\begin{array}{r|l} 351 & 7 \\ \hline 1 & 50 \quad 7 \\ & 1 \quad 7 \quad 7 \\ & & 0 \quad 1 \end{array}$$

Из данной таблицы следует, что  $q_1 = 50$ ,  $q_2 = 7$ ,  $q_3 = 1$  и показатель, с которым простое число 7 входит в каноническое разложение числа  $351!$ , равен  $50 + 7 + 1 = 58$ .

### Упражнения

1. Найдите число натуральных чисел, не превосходящих 100 и не делящихся ни на одно из простых чисел 5, 7, 11.

2. Найдите число и сумму натуральных делителей числа:

а) 468; б) 572; в) 288; г) 999; д) 753; е) 2015.

3. Найдите каноническое разложение  $\tau(n)$ ,  $\sigma(n)$ , если  $n = 8211$ .

4. Найдите натуральное число, если оно делится на 3 и на 4 и имеет 14 делителей.

5. а) найдите натуральное число  $n$ , которое делится на 2 и на 9 и имеет всего 14 делителей;

б) докажите, что если заменить 14 на 15, то задача будет иметь несколько решений, а при замене 14 на 17 решений вообще не будет.

6. Найдите все натуральные числа, последняя цифра которых 0 и которые имеют 15 различных натуральных делителей.

7. Натуральное число  $a$  имеет ровно четыре различных натуральных делителя. Натуральное число  $b$  имеет ровно шесть натураль-

ных делителей. Может ли число  $c = a \cdot b$  иметь ровно 15 различных натуральных делителей?

8. Найдите натуральное число, которое делится точно на два различных простых числа, если  $\tau(n) = 6$ ,  $\sigma(n) = 28$ .

9. Найдите натуральное число, имеющее 6 делителей, сумма которых равна 104.

10. Найдите наименьшее число вида  $2^a \cdot p_1 \cdot p_2$ , где  $p_1$  и  $p_2$  – нечетные простые числа, сумма делителей которого втрое больше самого числа.

11. Некоторое натуральное число имеет два простых делителя. Его квадрат имеет всего 15 делителей. Сколько делителей имеет куб этого числа?

12. Найдите  $E(2 + \sqrt[3]{987})$ ;  $E(2 - \lg 2512)$ .

13. С каким показателем степени число 7 входит в каноническое разложение числа  $43!$ ?

14. Найдите показатель, с которым простое число  $p$  входит в произведение  $n!$ , если:

а)  $p = 3$ ,  $n = 110$ ;      б)  $p = 11$ ,  $n = 2015$ ;      в)  $p = 13$ ,  $n = 70256$ .

15. Сколькими нулями оканчивается число  $2015!$ ?

16. Запишите каноническое разложение чисел:

а)  $50!$ ;      б)  $87!$ ;      в)  $92!$ .

## § 5. Систематические числа.

### Операции над систематическими числами.

#### Перевод записи числа из одной системы счисления в другую

Любой способ наименования и записи числа называется системой счисления. Все системы счисления делятся на два класса: непозиционные и позиционные. Знаки, используемые для записи числа, называются цифрами. В непозиционной системе счисления значение знака в записи числа не зависит от места этого знака в записи числа. В позиционной системе счисления значение знака в записи числа зависит от расположения этого знака в записи числа.

В непозиционной римской системе счисления всего 7 знаков: I, V, X, L – 50, C – 100, D – 500, M – 1000. При записи числа в римской системе счисления используются следующие правила:

1) если знак, имеющий меньшее значение стоит перед знаком, имеющим большее значение, то производится вычитание;

2) если знак, имеющий меньшее значение стоит после знака, имеющего большее значение, то производится сложение.

Например: CLV – 155, CM – 900.

#### Позиционные системы счисления

Пусть  $M = \{0, 1, 2, \dots, q-1\}$ ,  $q \in N$ ,  $q \geq 2$ . Представление числа  $a \in N$  в виде

$$a = a_s q^s + a_{s-1} q^{s-1} + \dots + a_1 q + a_0, \quad (5.1)$$

где  $a_i \in M$  ( $i = \overline{1, s}$ ),  $a_s \neq 0$ , называется записью числа  $a$  в системе счисления с основанием  $q$ . Представление числа  $a \in N$  в виде (5.1) кратко записывают

$$a = (a_s a_{s-1} \dots a_0)_q.$$

Например,  $589_{12} = 5 \cdot 12^2 + 8 \cdot 12 + 9$ .

**ТЕОРЕМА.** Любое натуральное число  $a$  в системе счисления с основанием  $q$  может быть представлено в виде (5.1), и такое представление однозначно.

Доказательство. I. Возможность представления  $\forall (a \in N)$  в виде (5.1) докажем методом математической индукции:

a) пусть  $a \in N$ ,  $a < q$ . Тогда равенство  $a = a$  – представление  $a$  в виде (5.1);

б) пусть  $a \in N$ ,  $a \geq q$ . Предположим, что  $\forall(m \in N), 1 \leq m < a$ , может быть представлено в виде (5.1).

Разделим  $a$  на  $q$  с остатком:  $a = bq + a_0$  ( $a_0 \in M$ ), так как  $b < a$ , то согласно индуктивному предположению  $b$  можно представить в виде

$$b = a_s q^{s-1} + a_{s-1} q^{s-2} + \dots + a_2 q + a_1, a_i \in M, a_s \neq 0 (i = \overline{1, s}). \quad (5.2)$$

Учитывая (5.2), из равенства  $a = bq + a_0$  получим:

$$a = a_s q^s + a_{s-1} q^{s-1} + \dots + a_1 q + a_0.$$

Согласно принципу математической индукции  $\forall(a \in N)$  можно представить в виде (5.1).

II. Единственность представления  $\forall(a \in N)$  в виде (5.1) также докажем методом математической индукции:

а)  $a \in N$ ,  $a < q$ . Тогда представление  $a$  в виде  $a = a$  единственно;

б) пусть  $a \in N$ ,  $a \geq q$ . Предположим  $\forall(m \in N), 1 \leq m < a$ , представление  $a$  в виде (5.1) единственно.

Пусть  $a \in N$ , кроме представления в виде (5.1), может быть представлено так же, как

$$a = b_t q^t + b_{t-1} q^{t-1} + \dots + b_1 q + b_0 \quad (5.3)$$

в системе с основанием  $q$ .

Из (5.1) и (5.3) имеем:

$$a = (a_s q^{s-1} + a_{s-1} q^{s-2} + \dots + a_1)q + a_0 = (b_t q^{t-1} + b_{t-1} q^{t-2} + \dots + b_1)q + b_0.$$

Из этого равенства в силу теоремы о делении с остатком получаем, что

$$a_0 = b_0, b = a_s q^{s-1} + a_{s-1} q^{s-2} + \dots + a_1 = b_t q^{t-1} + b_{t-1} q^{t-2} + \dots + b_1.$$

Так как  $b < a$ , то согласно индуктивному предположению б)  $t = s$ ,  $a_s = b_s, \dots, a_1 = b_1$ .

Таким образом, представление  $\forall(a \in N)$  в виде (5.1) единственно.

## Операции над систематическими числами

Сложение, вычитание, умножение, деление чисел в различных системах счисления проводятся по тем же правилам, что и в системе счисления с основанием 10.

Рассмотрим примеры.

1. Сложение и вычитание.

$$\begin{array}{r} 5768_9 \\ + 6832_9 \\ \hline 13711_9 \end{array} \quad \begin{array}{r} 7632_9 \\ - 6858_9 \\ \hline 663_9 \end{array}$$

2. Умножение, деление.

$\begin{array}{r} \times 465_8 \\ \quad 76_8 \\ \hline 3476 \\ + 4163 \\ \hline 45326_8 \end{array}$	$\begin{array}{l} 30 = 3 \cdot 8 + 6 \\ 39 = 4 \cdot 8 + 7 \\ 28 = 3 \cdot 8 + 4 \\ 35 = 4 \cdot 8 + 3 \\ 46 = 5 \cdot 8 + 6 \\ 33 = 4 \cdot 8 + 1 \end{array}$	$\begin{array}{r} - 33162_8 \overline{)457_8} \\ \quad 2753 \\ \hline \quad 3432 \\ - \quad 3432 \\ \hline \quad \quad 0 \end{array}$	$\begin{array}{l} 35 = 4 \cdot 8 + 3 \\ 29 = 3 \cdot 8 + 5 \\ 23 = 2 \cdot 8 + 7 \\ 42 = 5 \cdot 8 + 2 \\ 35 = 4 \cdot 8 + 3 \\ 28 = 3 \cdot 8 + 4 \end{array}$
--	---	---	---

### Перевод записи числа из одной системы счисления в другую

Пусть число  $a \in N$  записано в системе счисления с основанием  $p$ . Требуется записать число  $a$  в системе счисления с основанием  $q$ .

Предположим, что запись числа  $a$  в системе счисления  $q$  имеет вид

$$a = a_k q^k + a_{k-1} q^{k-1} + \dots + a_1 q + a_0.$$

Необходимо найти числа  $a_0, a_1, a_2, \dots, a_k$ . Для этого в системе счисления с основанием  $p$  разделим  $a$  на  $q$  с остатком:  $a = b_0 q + a_0$ .

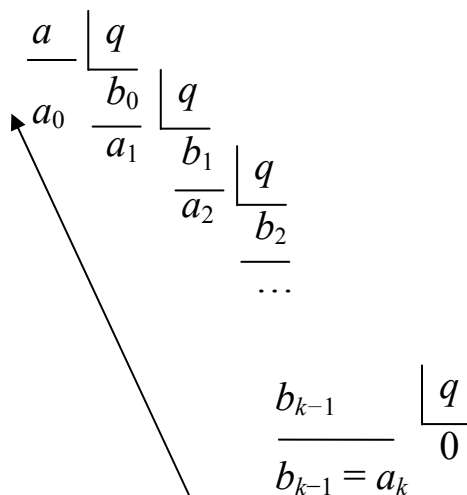
Разделим теперь  $b_0$  на  $q$  с остатком в этой же системе счисления:

$$b_0 = b_1 q + a_1.$$

И так далее. Этот процесс последовательного деления будем продолжать до тех пор, пока не получим нулевое неполное частное:

$$b_{k-2} = b_{k-1} q + a_{k-1}, b_{k-1} = 0 \cdot q + b_{k-1}, b_{k-1} = a_k.$$

Последовательность деления  $a$  на  $q$  в системе счисления с основанием  $p$  удобно приводить по следующей схеме:



Стрелка указывает направление разрядов.

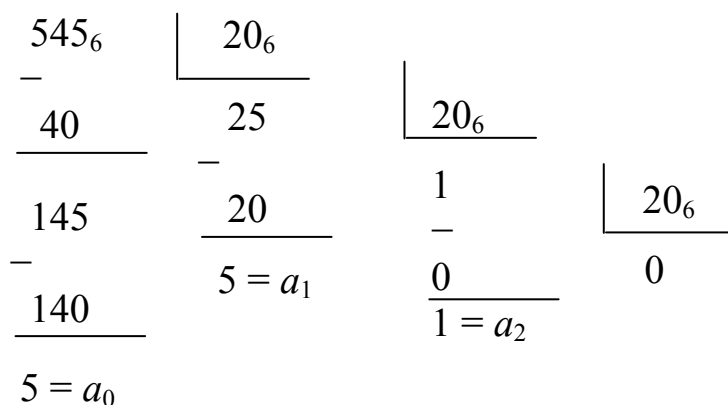
Если  $q < p$ , то остатки  $a_0, a_1, \dots, a_k$  при последовательном делении  $a$  на  $q$  в системе счисления с основанием  $p$  обозначаются одной цифрой. Эти цифры и будут цифрами в записи числа  $a$  в системе счисления с основанием  $q$ .

Если же  $q \geq p$ , то  $q$  и некоторые из остатков  $a_0, a_1, \dots, a_k$  в системе счисления с основанием  $p$  запишутся более чем одной цифрой. Эти числа нужно записать с помощью цифр в  $q$ -ичной системе счисления.

### Пример

Записать число  $545_6$  в системе счисления с основанием 12. Запишем число 12 в системе счисления с основанием 6:

$$12 = 2 \cdot 6 + 0 = (20)_6.$$



Значит,  $545_6 = 155_{12}$ .

## Упражнения

1. Выполните сложение чисел:

- а)  $1001010_2 + 1101001_2$ ; б)  $1543_6 + 42_6$ ;  
в)  $65004_8 + 70645_8$ ; г)  $7489(12)_{13} + 5762_{13}$ ;  
д)  $43(10)(11)7_{12} + 3(10)6_{12} + 5(11)38_{12}$ ; е)  $47(10)9_{11} + 84567_{11}$ ;  
ж)  $(12)724(11)(10)_{13} + 478(10)953_{13}$ .

2. Выполните вычитание чисел:

- а)  $10101011_2 - 110111_2$ ; б)  $1131043_5 - 342144_5$ ;  
в)  $23042_6 - 5354_6$ ; г)  $783041_9 - 27605_9$ ;  
д)  $46(10)37_{12} - 72(11)48_{12}$ ; е)  $1(11)(10)9(10)_{13} - (12)(11)9(11)_{13}$ .

3. Выполните умножение чисел:

- а)  $4203_5 \cdot 42_5$ ; б)  $5034_6 \cdot 545_6$ ; в)  $50624_7 \cdot 56_7$ ;  
г)  $42(11)3_{12} \cdot 789_{12}$ ; д)  $343224_7 \cdot 1256_7$ ; е)  $258(10)3_{11} \cdot 56_{11}$ .

4. Выполните деление чисел:

- а)  $111100011_2 : 10101_2$ ; б)  $1141043_5 : 23_5$ ;  
в)  $471222_8 : 27_8$ ; г)  $51(10)3406_{11} : 548_{11}$ .

5. Выведите признак делимости на  $g - 1$  в  $g$ -ичной системе счисления.

6. Замените звездочки цифрами так, чтобы:

- а) число  $7 * 8(10)5_2$  делилось на 11;  
б) число  $36 * 05_7$  делилось на 6;  
в) число  $51 * 2_6$  делилось на 4;  
г) число  $25 * *_8$  делилось на 32.

7. Осуществите переход:

- а)  $37051_8 = x_6$ ; б)  $42013_5 = x_7$ ; в)  $890721 = x_8$ ;  
г)  $45253_7 = x_{12}$ ; д)  $6785_9 = x_{12}$ ; е)  $(11)89(10)_{12} = x_{14}$ ;  
ж)  $6276_8 = x_{13}$ ; з)  $(10)983_{11} = x_{13}$ ; и)  $9(12)34_{13} = x_{15}$ .

8. Запишите числа  $m$  и  $n$  в системе счисления с основанием  $g$  и разделите  $m$  на  $n$  с остатком:

- а)  $m = 54326_9, n = 35_7, g = 8$ ; б)  $m = 70463_8, n = 124_5, g = 7$ ;  
в)  $m = 23012_4, n = 158_9, g = 5$ .

9. Найдите основание  $x$  системы счисления, в которой справедливо равенство:

- а)  $53_x = 33$ ; б)  $400_x = 64$ ; в)  $201_x = 51$ ;  
г)  $231_x = 45$ ; д)  $10302_x = 2550$ ; е)  $400_x = 32$ .

## § 6. Конечные цепные дроби. Неопределенные уравнения первой степени с двумя неизвестными

**Определение.** Конечной цепной дробью называется выражение вида

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_n}}}}, \quad (6.1)$$

где  $q_0 \in \mathbb{Z}$ ,  $q_i \in \mathbb{N}$  ( $i = \overline{1, n}$ ),  $q_n \neq 1$ . Так как конечное число рациональных операций над рациональными числами дает рациональное число, то любая конечная цепная дробь является рациональным числом. Цепную дробь (6.1) сокращенно записывают  $[q_0, q_1, q_2, \dots, q_n]$ .

**ТЕОРЕМА 1.** Любое рациональное число представимо конечной цепной дробью.

Доказательство. Пусть  $t \in \mathbb{Q}$ ,  $t = \frac{a}{b}$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}$ . Если  $t \in \mathbb{Z}$ , то  $[t] = t$ . Если же  $t \notin \mathbb{Z}$ , то к числам  $a, b$  применим алгоритм Евклида:

$$\begin{aligned} a &= bq_0 + r_1, \quad b = r_1q_1 + r_2, \quad r_1 = r_2q_2 + r_3, \quad \dots, \quad r_{n-2} = \\ &= r_{n-1}q_{n-1} + r_n, \quad r_{n-1} = r_nq_n, \end{aligned} \quad (6.2)$$

где  $b > r_1 > r_2 > \dots > r_n$ ,  $q_n \neq 1$ , так как  $r_{n-1} > r_n$ . Из (6.2) имеем:

$$\frac{a}{b} = q_0 + \frac{1}{\frac{b}{r_1}}, \quad \frac{b}{r_1} = q_1 + \frac{1}{\frac{r_1}{r_2}}, \quad \frac{r_1}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}}, \quad \dots, \quad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}}, \quad \frac{r_{n-1}}{r_n} = q_n. \quad (6.3)$$

Из первых двух равенств (6.3) следует, что  $\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{r_1}{r_2}}}$ .

Если в это равенство вместо дроби  $\frac{r_1}{r_2}$  подставим ее выражение из (6.3), то получим

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{r_2 + \frac{1}{r_3}}}}$$

Продолжая этот процесс, получим, что

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots + \frac{1}{q_n}}}$$

### Пример 1

Представить в виде конечной цепной дроби рациональное число  $t = -\frac{27}{25}$ . Применим к числам  $-27, 25$  алгоритм Евклида:

$$-27 = 25 \cdot (-2) + 23, 25 = 23 \cdot 1 + 2, 23 = 2 \cdot 11 + 1, 2 = 1 \cdot 2 + 0.$$

Из этих равенств следует, что

$$-\frac{27}{25} = -2 + \frac{1}{1 + \frac{1}{11 + \frac{1}{2}}}$$

**ТЕОРЕМА 2.** Представление любого рационального числа в виде конечной цепной дроби единственно.

### Подходящие дроби. Числа

$$\delta_0 = q_0, \delta_1 = q_0 + \frac{1}{q_1}, \delta_2 = q_0 + \frac{1}{q_1 + \frac{1}{q_2}}, \dots$$

называются подходящими дробями к цепной дроби (6.1).

Рассмотрим последовательности

$$P_0, P_1, \dots, P_{n-1}, P_n; Q_0, Q_1, \dots, Q_{n-1}, Q_n,$$

определенные рекуррентными соотношениями:

$$\left. \begin{aligned} P_k &= P_{k-1}q_k + P_{k-2} \\ Q_k &= Q_{k-1}q_k + Q_{k-2} \end{aligned} \right] , k = \overline{2, n}, \quad (6.4)$$

с начальными условиями:  $P_0 = q_0$ ,  $P_1 = q_0q_1 + 1$  и  $Q_0 = 1$ ,  $Q_1 = q_1$ , где  $q_0, q_1, \dots, q_n$  – элементы цепной дроби (6.1). Справедливо утверждение.

**ТЕОРЕМА 3.** Для подходящей дроби  $\delta_k$  к цепной дроби (6.1) справедливо равенство

$$\delta_k = \frac{P_k}{Q_k}, k = \overline{0, n}. \quad (6.5)$$

Доказательство. Доказательство проведем методом математической индукции.

1. Докажем, что равенство (6.5) справедливо при  $k = 0, 1, 2$ .

При  $k = 0$  подходящая дробь

$$\delta_0 = \frac{q_0}{1} = \frac{P_0}{Q_0},$$

при  $k = 1$

$$\delta_1 = q_0 + \frac{1}{q_1} = \frac{q_0q_1 + 1}{q_1} = \frac{P_1}{Q_1},$$

при  $k = 2$

$$\begin{aligned} \delta_2 &= q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = q_0 + \frac{q_2}{q_1q_2 + 1} = \\ &= \frac{(q_0q_1 + 1)q_2 + q_0}{q_1q_2 + 1} = \frac{P_1q_2 + P_0}{Q_1q_2 + Q_0} = \frac{P_2}{Q_2}. \end{aligned}$$

Показано, что утверждение теоремы верно при  $k = 0, 1, 2$ .

2. Предположим, что равенство (6.5) верно при  $k = m$ ,  $m < n$ . Докажем справедливость равенства (6.5)  $k = m + 1$ .

По индуктивному предположению

$$\delta_m = \frac{P_m}{Q_m} = \frac{P_{m-1}q_m + P_{m-2}}{Q_{m-1}q_m + Q_{m-2}}. \quad (6.6)$$

Заметим, что  $(m + 1)$ -я подходящая дробь

$$\delta_{m+1} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots + \frac{1}{q_{m-1} + \frac{1}{q_m + \frac{1}{q_{m+1}}}}}}$$

получается из подходящей дроби  $\delta_m$  посредством замены  $q_m$  на  $q_m + \frac{1}{q_{m+1}}$ . Поэтому, если в равенство (6.6) вместо  $q_m$  подставим  $q_m + \frac{1}{q_{m+1}}$ , получим

$$\delta_{m+1} = \frac{P_{m-1} \left( q_m + \frac{1}{q_{m+1}} \right) + P_{m-2}}{Q_{m-1} \left( q_m + \frac{1}{q_{m+1}} \right) + Q_{m-2}} = \frac{P_{m-1}q_m + P_{m-2} + \frac{P_{m-1}}{q_{m+1}}}{Q_{m-1}q_m + Q_{m-2} + \frac{Q_{m-1}}{q_{m+1}}} =$$

$$\frac{P_m q_{m+1} + P_{m-1}}{Q_m q_{m+1} + Q_{m-1}} = \frac{P_{m+1}}{Q_{m+1}}.$$

Из пунктов 1 и 2 следует, что для любого  $k \in \{0, 1, \dots, n\}$  справедливо равенство  $\delta_k = \frac{P_k}{Q_k}$ .

**Определение.** Числа  $P_k$  и  $Q_k$ , определенные рекуррентными соотношениями (6.4), с начальными условиями:  $P_0 = q_0$ ,  $P_1 = q_0 q_1 + 1$  и  $Q_0 = 1$ ,  $Q_1 = q_1$ , называются, соответственно, числителем и знаменателем  $k$ -й подходящей дроби  $\delta_k$  цепной дроби (6.1).

Вычисление числителей и знаменателей подходящих дробей удобно проводить по следующей схеме.

$s$	0	1	2	...	$n - 1$	$n$
$q_s$	$q_0$	$q_1$	$q_2$	...	$q_{n-1}$	$q_n$
$P_s$	$P_0 = q_0$	$P_1 = q_0 q_1 + 1$	$P_2 = P_1 q_2 + P_0$	...	$P_{n-1} = P_{n-2} q_{n-1} + P_{n-3}$	$P_n = P_{n-1} q_n + P_{n-2}$
$Q_s$	$Q_0 = 1$	$Q_1 = q_1$	$Q_2 = Q_1 q_2 + Q_0$	...	$Q_{n-1} = Q_{n-2} q_{n-1} + Q_{n-3}$	$Q_n = Q_{n-1} q_n + Q_{n-2}$

## Пример 2

Найдем подходящие дроби для цепной дроби  $[2; 1, 2, 2, 3, 4]$ .

**Решение.** Составим таблицу для определения числителей и знаменателей подходящих дробей.

$s$	0	1	2	2	4	5
$q_s$	2	1	2	2	3	4
$P_s$	2	3	8	19	65	279
$Q_s$	1	1	3	7	24	103

Из таблицы следует, что  $\delta_0 = \frac{2}{1}$ ,  $\delta_1 = \frac{3}{1}$ ,  $\delta_2 = \frac{8}{3}$ ,  $\delta_3 = \frac{19}{7}$ ,  
 $\delta_4 = \frac{65}{24}$ ,  $\delta_5 = \frac{279}{103} = [2; 1, 2, 2, 3, 4]$ .

### Свойства подходящих дробей

1. Числители и знаменатели двух соседних подходящих дробей  $\frac{P_{s-1}}{Q_{s-1}}$  и  $\frac{P_s}{Q_s}$  связаны соотношением

$$P_{s-1}Q_s - Q_{s-1}P_s = (-1)^s, \quad s = \overline{1, n}. \quad (6.7)$$

**Доказательство.** Доказательство проведем методом математической индукции.

1. При  $s = 1$  имеем:  $P_0Q_1 - Q_0P_1 = q_0q_1 - 1 \cdot (q_0q_1 + 1) = (-1) = (-1)^1$ .

2. Предположим, что равенство (6.7) верно при  $s = k, k < n$ . Докажем справедливость (6.7) при  $s = k + 1$ :

$$\begin{aligned} P_kQ_{k+1} - Q_kP_{k+1} &= P_k(Q_k \cdot q_{k+1} + Q_{k-1}) - Q_k(P_k \cdot q_{k+1} + P_{k-1}) = \\ &= P_kQ_{k-1} - Q_kP_{k-1} = -(P_{k-1}Q_k - P_kQ_{k-1}) = -(-1)^k = (-1)^{k+1}. \end{aligned}$$

Согласно принципу математической индукции равенство (6.7) верно для любого  $s = \{1, 2, \dots, n\}$ .

2. Числители и знаменатели подходящих дробей – целые числа. Знаменатели подходящих дробей – натуральные числа и, начиная с первого знаменателя, образуют возрастающую последовательность.

3. Числители и знаменатели подходящих дробей взаимно простые целые числа.

Доказательство. При  $s = 0$   $\delta_s = \frac{q_0}{1}, (q_0, 1) = 1$ . Пусть теперь  $s \geq 1$ .

Покажем, что числитель и знаменатель дроби  $\frac{P_s}{Q_s}$  – взаимно простые целые числа. Предположим, что  $(P_s, Q_s) = d$ . В силу свойства 1 имеет место равенство

$$P_{s-1} Q_s - P_s Q_{s-1} = (-1)^s. \quad (6.8)$$

Так как  $P_s \div d, Q_s \div d$ , то из (6.8) следует, что  $(-1)^s \div d$ . Значит,  $d = 1, (P_s, Q_s) = 1$ .

4. Подходящие дроби четного порядка образуют возрастающую последовательность, а нечетного порядка – убывающую последовательность.

Доказательство. Учитывая соотношения (6.4) и свойство 1 подходящих дробей, имеем:

$$\begin{aligned} \frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} &= \frac{P_{k-2}Q_k - P_kQ_{k-2}}{Q_kQ_{k-2}} = \frac{P_{k-2}(Q_{k-1}q_k + Q_{k-2}) - (P_{k-1}q_k + P_{k-2})Q_{k-2}}{Q_kQ_{k-2}} = \\ &= \frac{(P_{k-2}Q_{k-1} - P_{k-1}Q_{k-2})q_k}{Q_kQ_{k-2}} = \frac{(-1)^{k-1}q_k}{Q_kQ_{k-2}}. \end{aligned} \quad (6.9)$$

Если  $k$  четное число, то из (6.9) следует, что  $\frac{P_{k-2}}{Q_{k-2}} < \frac{P_k}{Q_k}$ , если же

$k$  нечетное число, то из (6.9) следует, что  $\frac{P_{k-2}}{Q_{k-2}} > \frac{P_k}{Q_k}$ .

5. Из двух соседних подходящих дробей  $\frac{P_{k-1}}{Q_{k-1}}, \frac{P_k}{Q_k}$  данной цепной дроби дробь четного порядка меньше дроби нечетного порядка.

6. Каждая подходящая дробь нечетного порядка данной цепной дроби больше любой подходящей дроби четного порядка.

7. Подходящая дробь четного порядка является приближенным значением числа  $\frac{a}{b}$  с недостатком, а нечетного порядка – с избытком (за исключением последней подходящей дроби, совпадающей с дробью  $\frac{a}{b}$ ).

8. Если  $\frac{a}{b}$  рациональное число и  $\frac{P_s}{Q_s}$  –  $s$ -я подходящая дробь разложения  $\frac{a}{b}$  в цепную дробь, то  $\left| \frac{a}{b} - \frac{P_s}{Q_s} \right| < \frac{1}{Q_s^2}$ .

### Решение в целых числах линейного уравнения с двумя неизвестными

Рассмотрим уравнение

$$ax + by = c, \quad a, b, c \in Z. \quad (6.10)$$

Поставим вопрос о нахождении всех решений уравнения (6.10) в целых числах. Если  $(a, b) = d$ ,  $d > 1$ ,  $c$  не делится на  $d$ , то уравнение (6.10) не имеет решения. Пусть  $c : d$ , тогда уравнение (6.10) равносильно уравнению

$$a_1x + b_1y = c_1,$$

где  $a_1 = \frac{a}{d}$ ,  $b_1 = \frac{b}{d}$ ,  $(a_1, b_1) = 1$ , которое имеет решение в целых числах. Действительно, так как  $(a_1, b_1) = 1$ , то  $\exists(m, n \in Z), a_1m + b_1n = 1$ . Умножив это равенство на  $c_1$ , получим  $a_1(mc_1) + b_1(nc_1) = c_1$ . Пара  $(mc_1, nc_1)$  целых чисел – решение уравнения.

**ТЕОРЕМА 4.** Если  $(x_0, y_0)$  целочисленное решение уравнения (6.10), где  $(a, b) = 1$ , то

$$x = x_0 + bt, \quad y = y_0 - at, \quad (6.11)$$

где  $t$  – произвольное целое число, общее решение этого уравнения.

Доказательство. Для  $\forall(t \in Z)$  формулы (6.11) дают решение уравнения (6.10), так как  $a(x_0 + bt) + b(y_0 - at) = c$ . Пусть теперь  $(x_1, y_1)$  – решение уравнения (6.10). Покажем, что это решение получается из формул (6.11) при  $t \in Z$ . Если из уравнения (6.10) вычтем равенство  $ax_0 + by_0 = c$ , то получим равносильное уравнение

$$a(x - x_0) + b(y - y_0) = 0. \quad (6.12)$$

Так как  $(x_1, y_1)$  – решение уравнения (6.12), то имеет место равенство

$$a(x_1 - x_0) = -b(y_1 - y_0). \quad (6.13)$$

Учитывая что  $(a, b) = 1$ , из (6.13) имеем:  $(x_1 - x_0) \div b$ . Существует  $t_1 \in Z$  такое, что  $x_1 - x_0 = bt_1$ ,  $x_1 = x_0 + bt_1$ . Учитывая, что  $x_1 - x_0 = bt_1$ , из (6.13) получим  $y_1 = y_0 - at_1$ . Показано, что произвольное решение  $(x_1, y_1)$  уравнения (6.10) получается из формул (6.11) при  $t = t_1$ ,  $t_1 \in Z$ . Теорема доказана.

Из теоремы следует: чтобы найти общее решение линейного уравнения  $ax + by = c$ ,  $a, b, c \in Z$ ,  $(a, b) = 1$ , в целых числах, достаточно найти какое-либо его частное решение в целых числах. Частное решение уравнения (6.10) в целых числах можно найти, используя теорию конечных цепных дробей. Для этого разложим  $\frac{a}{b}$  в конечную

цепную дробь. Пусть  $\frac{a}{b} = [q_0, q_1, \dots, q_n]$  и  $\frac{P_s}{Q_s}$  ( $s = \overline{1, n}$ ) подходящие

дроби этой цепной дроби. Из условий  $(a, b) = 1$ ,  $(P_n, Q_n) = 1$ ,  $\frac{P_n}{Q_n} = \frac{a}{b}$

следует, что  $P_n = a$ ,  $Q_n = b$ . В силу свойства 1 подходящих дробей имеет место равенство  $P_{n-1}Q_n - Q_{n-1}P_n = (-1)^n$  или  $P_{n-1}b - aQ_{n-1} = (-1)^n$ .

Если обе части последнего равенства умножим на  $(-1)^n c$ , то получим

$$a((-1)^{n+1}Q_{n-1}c) + b((-1)^n P_{n-1}c) = c. \quad (6.14)$$

Из (6.14) следует, что пара  $((-1)^{n+1}Q_{n-1}c, (-1)^n P_{n-1}c)$  есть частное решение уравнения (6.10) при условии  $(a, b) = 1$ . Таким образом, справедливо утверждение.

**ТЕОРЕМА 5.** Общее решение в целых числах уравнения  $ax + by = c$ ,  $a, b, c \in Z$ ,  $(a, b) = 1$ , можно представить в виде

$$\begin{cases} x = (-1)^{n+1}Q_{n-1}c + bt, \\ y = (-1)^n P_{n-1}c - at, \end{cases}$$

где  $t$  – произвольное целое число.

### Пример 3

Найти общее решение уравнения  $8x + 19y = 10$  в целых числах.

**Решение.** Так как  $(8, 19) = 1$ , то уравнение имеет решение в целых числах. Представим  $\frac{8}{19}$  в виде конечной цепной дроби:

$\frac{8}{19} = [0; 2, 2, 1, 2]$ . Для нахождения  $P_3, Q_3$  составим таблицу:

$s$	0	1	2	3	4
$q_s$	0	2	2	1	2
$P_s$	0	1	2	3	8
$Q_s$	1	2	5	7	19

Из таблицы следует, что  $P_3 = 3, Q_3 = 7$ .  $x = -70 + 19t, y = 30 - 8t, t \in Z$ , общее решение уравнения.

### Упражнения

1. Представьте в виде цепной дроби:

$$\frac{127}{52}, \frac{24}{35}, \frac{135}{279}, -\frac{187}{63}, \frac{96}{79}, \frac{151}{121}, -\frac{55}{117}.$$

2. Найдите действительные числа, которые обращаются в данные цепные дроби:  $[2; 1, 3, 4, 1, 5]$ ,  $[2; 1, 1, 7, 6]$ ,  $[0; 1, 4, 3, 2]$ ,  $[0; 3, 1, 2, 7]$ ,  $[-2; 1, 4, 1, 2, 5]$ ,  $[-5; 4, 1, 1, 2]$ ,  $[-4; 1, 6, 4, 1, 2]$ .

3. При помощи разложения в цепную дробь сократите:

$$\begin{array}{lll} \text{а) } \frac{3587}{2743}; & \text{б) } \frac{1043}{3427}; & \text{в) } \frac{1491}{2247}; \\ \text{г) } \frac{3577}{2555}; & \text{д) } \frac{5726}{6240}; & \text{е) } \frac{1857}{9153}; \\ \text{ж) } \frac{70757}{491209}; & \text{з) } \frac{326129}{3270977}; & \text{и) } \frac{798551}{858819}. \end{array}$$

4. Докажите, что дробь вида  $\frac{a^4 + 3a^2 + 1}{a^3 + 2a^2}$ , где  $a$  – натуральное число, несократима.

5. Решите уравнения:

$$\text{а) } [2; 1, 2, x] = \frac{19}{7}; \quad \text{б) } [x; 2, 3, 4] = \frac{73}{30}; \quad \text{в) } [4; 3, 9, x] = \frac{62}{13}.$$

6. Решите в целых числах уравнения:

$$\begin{array}{lll} \text{а) } 70x + 33y = 1; & \text{б) } 275x + 145y = 10; & \text{в) } 23x + 49y = 53; \\ \text{г) } 12x + 7y = 41; & \text{д) } 35x + 37y = 12; & \text{е) } 39x - 22y = 10; \\ \text{ж) } 81x - 48y = 33; & \text{з) } 45x + 37y = 25; & \text{и) } 25x - 19y = 117; \\ \text{к) } 42x + 31y = 67; & \text{л) } 17x - 25y = 117; & \text{м) } 42x + 37y = 21; \\ \text{н) } 60x - 91y = 2; & \text{о) } 12x - 7y = 29. \end{array}$$

7. Из имеющихся резисторов сопротивлением по 1,2 и 1,7 Ом требуется составить последовательным соединением цепь сопротивлением 11,1 Ом. Сколько резисторов того и другого типа потребуется?

8. Для проведения эстафеты по бегу требуется разделить дистанцию в 6,7 км на участки размером по 175 м для женщин и по 300 м для мужчин. Из скольких спортсменов, как мужчин, так и женщин, должны состоять команды, участвующие в эстафете?

9. Сколько потребуется сосудов емкостью по 0,5 л и по 0,8 л для разлива 12 л жидкости так, чтобы все взятые сосуды были наполнены?

10. В населенный пункт, с которым установлено лишь авиационное сообщение, требуется отправить 150 контейнеров груза. В распоряжении отправителей имеются транспортные самолеты грузоподъемностью в 8 и 13 контейнеров. Сколько понадобится самолетов того и другого типа для того, чтобы перевезти указанный груз одним рейсом? Грузоподъемность каждого самолета должна быть использована полностью.

11. При каких целых числах выражение  $\frac{7-11x}{10}$  равно такому целому положительному числу, при делении которого на 4 получается остаток, равный 3?

12. Найдите общий вид целых чисел, кратных 8, которые при делении на 5 дают в остатке 3.

13. Число  $\frac{1261}{881}$  замените подходящей дробью, чтобы погрешность не превышала 0,0001.

14. Число  $\frac{245}{38}$  замените подходящей дробью, чтобы погрешность не превышала 0,001.

## § 7. Отношение сравнения в кольце $Z$ . Свойства сравнений

Целые числа  $a, b \in Z$  называются сравнимыми по  $\text{mod } m$ , где  $m \in N, m > 1$ , если  $(a - b) \div m$ . Если целые числа  $a, b$  сравнимы по  $\text{mod } m$ , то будем этот факт записывать  $a \equiv b(\text{mod } m)$ .

**ТЕОРЕМА 1.**  $a \equiv b(\text{mod } m)$  тогда и только тогда, когда целые числа  $a, b$  при делении на  $m$  имеют одинаковые остатки.

Справедливы следующие свойства сравнений.

1.  $\forall (a \in Z) a \equiv a(\text{mod } m)$ .
2.  $a \equiv b(\text{mod } m) \Rightarrow b \equiv a(\text{mod } m)$ .
3.  $a \equiv b(\text{mod } m) \wedge b \equiv c(\text{mod } m) \Rightarrow a \equiv c(\text{mod } m)$ .
4.  $a \equiv b(\text{mod } m) \wedge c \equiv d(\text{mod } m) \Rightarrow a \pm c \equiv b \pm d(\text{mod } m)$ .
5.  $a \equiv b(\text{mod } m) \wedge c \equiv d(\text{mod } m) \Rightarrow ac \equiv bd(\text{mod } m)$ .
6.  $a \equiv b(\text{mod } m)$ , то  $\forall (n \in N) a^n \equiv b^n(\text{mod } m)$ .
7.  $a \equiv b(\text{mod } m)$ , то  $\forall (k \in Z) ak \equiv bk(\text{mod } m)$ .
8.  $a \equiv b(\text{mod } m)$ , то  $\forall (k \in N) ak \equiv bk(\text{mod } mk)$ .
9.  $\forall (k \in Z) ak \equiv kb(\text{mod } m) \wedge (k, m) = 1 \Rightarrow a \equiv b(\text{mod } m)$ .
10.  $\forall (k \in N) ak \equiv bk(\text{mod } mk) \Rightarrow a \equiv b(\text{mod } m)$ .

**ТЕОРЕМА 2.** Пусть  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  многочлен с целыми коэффициентами. Если  $a \equiv b(\text{mod } m)$ , то  $f(a) \equiv f(b)(\text{mod } m)$ .

Покажем применение теоремы 2 к выводу признака делимости на 11. Пусть  $a \in N, a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$ . Так как  $10 \equiv -1(\text{mod } m)$ , то согласно теореме 2

$$a \equiv a_n (-1)^n + a_{n-1} (-1)^{n-1} + \dots + a_1 (-1) + a_0 (\text{mod } 11). \quad (7.1)$$

Из (7.1) следует, что

$$a \div 11 \Leftrightarrow (a_n (-1)^n + a_{n-1} (-1)^{n-1} + \dots + a_1 (-1) + a_0) \div 11.$$

### Классы вычетов по заданному модулю

Из свойств 1–3 сравнения следует, что отношение сравнения на  $Z$  по модулю  $m$  является отношением эквивалентности.

Пусть  $a \in Z, m \in N, m > 1$ . Класс эквивалентности, порожденный целым числом  $a$ , относительно отношения сравнения по заданному модулю  $m$ , называется классом вычетов по  $\text{mod } m$  и обозначается  $\bar{a}$ .

Из определения следует, что  $\bar{a} = \{x \in Z \mid x \equiv a(\text{mod } m)\}$ .

## Свойства классов вычетов

1. Любые два класса вычетов по модулю  $m$  либо совпадают, либо их пересечение – пустое множество. Объединение всех классов по модулю  $m$  есть множество  $Z$ .

$$2. \bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}.$$

3. Пусть  $A$  – класс вычетов по  $\text{mod } m$ ,  $a \in A$ . Тогда

$$A = \{a + mt | t \in Z\}.$$

Доказательство. Пусть  $b \in A$ , тогда  $b \equiv a \pmod{m}$ .  $\exists(t_1 \in Z)$   
 $b = a + mt_1$ .

Отсюда следует, что  $b \in \{a + mt | t \in Z\}$ . Так как  $\forall(t \in Z)$   
 $a + mt \equiv a \pmod{m}$ , то  $a + mt \in A$ . Таким образом,  $A = \{a + mt | t \in Z\}$ .

4. Пусть  $A$  – класс вычетов по  $\text{mod } m$  и  $r$  – остаток от деления какого-либо целого числа, принадлежащего  $A$ , на  $m$ , тогда  $A = \{r + mt | t \in Z\}$ .

### Пример

Пусть  $m = 4$ . Согласно теореме 1 число всех классов вычетов по модулю 4 равно 4.  $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  – множество всех классов вычетов по модулю 4,  $\bar{0} = \{4t | t \in Z\}$ ,  $\bar{1} = \{4t + 1 | t \in Z\}$ ,  $\bar{2} = \{4t + 2 | t \in Z\}$ ,  $\bar{3} = \{4t + 3 | t \in Z\}$ .

## § 8. Кольцо классов вычетов.

### Полная и приведенная системы вычетов

#### Кольцо классов вычетов

На множестве  $Z_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$  классов вычетов по заданному модулю  $m$  введем операции сложения и умножения классов вычетов следующим образом:

$$\overline{a} \oplus \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Покажем, что введенные операции не зависят от выбора представителей из классов вычетов.

Пусть  $a' \in \overline{a}, b' \in \overline{b}$ , тогда  $a' \equiv a \pmod{m}, b' \equiv b \pmod{m}$ . Сложив и умножив эти сравнения, получим  $a' + b' \equiv a + b \pmod{m}, a' \cdot b' \equiv a \cdot b \pmod{m}$ . Из этих сравнений следует, что

$$\overline{a' + b'} = \overline{a + b}, \quad \overline{a' \cdot b'} = \overline{a \cdot b}.$$

Справедливо утверждение.

**ТЕОРЕМА 1.** Алгебра  $(Z_m, \oplus, \cdot)$  является коммутативным кольцом с единицей.

Доказательство.

I. Покажем, что алгебра  $(Z_m, \oplus)$  – абелева группа. Для этого проверим выполнимость аксиом группы для этой алгебры.

1. Так как для любых  $\overline{a}, \overline{b}, \overline{c} \in Z_m$

$$(\overline{a} \oplus \overline{b}) \oplus \overline{c} = \overline{(a+b)} \oplus \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} \oplus \overline{(b+c)} = \overline{a} \oplus (\overline{b} \oplus \overline{c}),$$

то сложение классов вычетов ассоциативно.

2. Для любого  $\overline{a} \in Z_m$   $\overline{a} \oplus \overline{0} = \overline{a}$ ,  $\overline{0}$  – нейтральный элемент.

3. Для любого  $\overline{a} \in Z_m$   $\overline{a} \oplus \overline{(-a)} = \overline{0}$ ,  $\overline{-a}$  – класс вычетов, противоположный классу  $\overline{a}$ .

4. Очевидно, что сложение классов вычетов коммутативно.

Из 1–4 следует, что алгебра  $(Z_m, \oplus)$  – абелева группа.

II. Покажем, что умножение классов вычетов дистрибутивно относительно сложения и что умножение ассоциативно.

5. Для любых  $\overline{a}, \overline{b}, \overline{c} \in Z_m$

$$\overline{a} \cdot (\overline{b} \oplus \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} \oplus \overline{ac} = \overline{a} \cdot \overline{b} \oplus \overline{a} \cdot \overline{c}.$$

Так как  $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$ , то

$$(\bar{b} \oplus \bar{c}) \cdot \bar{a} = \bar{a} \cdot (\bar{b} \oplus \bar{c}) = \bar{b} \cdot \bar{a} \oplus \bar{c} \cdot \bar{a}.$$

$$6. \bar{a}, \bar{b}, \bar{c} \in Z_m \quad \bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot \overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}.$$

Из 1–6 следует, алгебра  $(Z_m, \oplus, \cdot)$  – коммутативное кольцо. Класс вычетов  $\bar{1}$  – единица этого кольца.

**ТЕОРЕМА 2.** Если  $p \in N$  – простое число, то кольцо  $(Z_p, \oplus, \cdot)$  является полем.

Доказательство. Покажем, что для любого элемента кольца  $(Z_p, \oplus, \cdot)$ , отличного от  $\bar{0}$ , существует обратный элемент. Пусть  $\bar{a} \in Z_p$ ,  $\bar{a} \neq \bar{0}$ . Так как  $(a, p) = 1$ , то по свойству 4 НОД целых чисел существуют целые числа  $x_0, y_0$  такие, что  $a \cdot x_0 + p \cdot y_0 = 1$ . Из этого равенства следует  $\bar{a} \cdot \overline{x_0} + \bar{p} \cdot \overline{y_0} = \bar{1}$ . Так как  $\bar{p} = \bar{0}$ , то  $\bar{a} \cdot \overline{x_0} = \bar{1}$ . Значит, класс  $\overline{x_0}$  целых чисел является обратным элементом для класса  $\bar{a}$ . Показано, что кольцо  $(Z_p, \oplus, \cdot)$  является полем.

### Полная и приведенная системы вычетов

Множество  $Z_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$  – множество всех классов вычетов по модулю  $m$ . Совокупность целых чисел, содержащая по одному целому числу из каждого класса вычетов по модулю  $m$ , называется полной системой вычетов (ПСВ) по модулю  $m$ .

#### Пример 1

Системы чисел  $0, 1, 2, 3, 4; -8, -7, -6, -5, 1$  – ПСВ по модулю 5.

**ТЕОРЕМА 3.** Любая совокупность  $m$  целых чисел, попарно не сравнимых по модулю  $m$ , является ПСВ по модулю  $m$ .

**ТЕОРЕМА 4.** Пусть  $a_1, a_2, \dots, a_m$  – полная система вычетов по модулю  $m$  и  $b, c \in Z$ ,  $(c, m) = 1$ , тогда  $ca_1 + b, ca_2 + b, \dots, ca_m + b$  – полная система вычетов по модулю  $m$ .

Если  $(a, m) = 1$ , то класс вычетов  $\bar{a}$  по модулю  $m$  называется классом вычетов взаимно простым с  $m$ .

Пусть  $n \in N$ . Обозначим через  $\varphi(n)$  число, равное числу натуральных чисел, не превосходящих  $n$  и взаимно простых с  $n$ .

Так, например,  $\varphi(5) = 4$ ,  $\varphi(8) = 4$ .

**ТЕОРЕМА 5.** Число классов вычетов по модулю  $m$ , взаимно простых с  $m$ , равно  $\varphi(m)$ .

Доказательство. Выпишем из ПСВ  $1, 2, 3, \dots, m$  по модулю  $m$  целые числа, взаимно простые с  $m$ :

$$a_1, a_2, \dots, a_{\varphi(m)}. \quad (8.1)$$

Так как целые числа в (8.1) попарно несравнимы, то классы вычетов

$$\overline{a_1}, \overline{a_2}, \dots, \overline{a_{\varphi(m)}} \quad (8.2)$$

различны. Любой класс вычетов  $\overline{a}$  по модулю  $m$ , не входящий в (8.1), содержит целое число из множества  $\{1, 2, \dots, m\} \setminus \{a_1, a_2, \dots, a_{\varphi(m)}\}$ , поэтому не является взаимно простым с  $m$ .

Следовательно, число всех классов вычетов по модулю  $m$ , взаимно простых с  $m$ , равно  $\varphi(m)$ .

Совокупность целых чисел, содержащая по одному целому числу из каждого класса вычетов по модулю  $m$ , взаимно простого с  $m$ , называется приведенной системой вычетов по модулю  $m$ .

### Пример 2

Пусть  $m = 8$ .  $0, 1, 2, 3, 4, 5, 6, 7$  – ПСВ по модулю  $m$ ;  $1, 3, 5, 7$  – приведенная система вычетов по модулю 8.

**ТЕОРЕМА 6.** Любая совокупность  $\varphi(m)$  целых чисел, попарно несравнимых по модулю  $m$  и взаимно простых с  $m$ , есть приведенная система вычетов по  $\text{mod } m$ .

**ТЕОРЕМА 7.** Пусть  $a_1, a_2, \dots, a_{\varphi(m)}$  – приведенная система вычетов по модулю  $m$  и  $c \in \mathbb{Z}$ ,  $(c, m) = 1$ , тогда  $ca_1, ca_2, \dots, ca_{\varphi(m)}$  – приведенная система вычетов по модулю  $m$ .

## Упражнения

1. Какие из следующих высказываний истинны?

а)  $1 \equiv -5 \pmod{6}$ ;

б)  $546 \equiv 0 \pmod{13}$ ;

в)  $2^3 \equiv 1 \pmod{4}$ ;

г)  $3m \equiv -1 \pmod{m}$ ;

д)  $(m-1)^2 \equiv 1 \pmod{m}$ ;

е)  $2m+1 \equiv (m+1)^2 \pmod{m}$ .

2. Если  $3^n \equiv 1 \pmod{10}$ ,  $n \in \mathbb{N}$ , то  $3^{n+1} \equiv -1 \pmod{10}$ . Докажите это.

3. Докажите, что  $(2^{5n} - 1) \div 31$ ,  $n \in \mathbb{N}$ .

4. Докажите, что  $(1 + 3^x + 9^x) \div 13$ , если  $x = 3n + 1$  ( $n = 0, 1, 2, \dots$ ).

5. Докажите, что число вида  $\frac{18a + 5b}{19}$  – целое, если  $\frac{11a + 2b}{19}$  – целое число ( $a, b \in \mathbb{Z}$ ).

6. Образуют ли данные числа полную систему вычетов по указанному модулю:

а) 13, 8, -3, 10, 35, 60 по mod 6;

б) 20, 31, -8, -5, 25, 14, 8, -1, 13, 6 по mod 10?

7. По какому модулю числа 20, -4, 22, 18, -1 составляют полную систему вычетов?

8. Некоторый класс вычетов по модулю 7 содержит число  $a = 11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ . Каков абсолютно наименьший вычет этого класса?

9. Известно, что  $a^{1000} \equiv 5 \pmod{7}$ ;  $a^{1001} \equiv 45 \pmod{7}$ . Вычислите остаток от деления  $a$  на 7.

10. Найдите остаток от деления  $1532^5 + 899$  на 9.

11. Почему система чисел -5, 13, 11, -21, 5 не является приведенной системой вычетов по модулю 6?

12. Докажите, что система чисел 5,  $5^2$ ,  $5^3$ ,  $5^4$ ,  $5^5$ ,  $5^6$  является приведенной системой вычетов по модулю 7.

13. Используя метод математической индукции, докажите, что  $2^{3^n} \equiv -1 \pmod{3^{n+1}}$ , где  $n \in \mathbb{N}$ .

14. Найдите все делители нуля в кольце классов вычетов  $(\mathbb{Z}_{12}, \oplus, \cdot)$ .

15. Решите уравнения  $\bar{2} \cdot \bar{x} + \bar{7} = \bar{3}$ ,  $\bar{4} \cdot \bar{x} + \bar{9} = \bar{4}$ ,  $\bar{5} \cdot \bar{x} - \bar{8} = \bar{2}$  над полем  $(\mathbb{Z}_{17}, \oplus, \cdot)$ .

## § 9. Функция Эйлера и ее свойства. Теоремы Эйлера и Ферма

Числовая функция  $\varphi$ , заданная на множестве  $N$  и ставящая  $\forall(n \in N)$  в соответствие число натуральных чисел, не превосходящих  $n$  и взаимно простых с  $n$ , называется функцией Эйлера.

**Пример 1**

$$\varphi(6) = 2, \quad \varphi(8) = 4.$$

**Определение.** Числовая функция  $f$ , заданная на множестве  $N$ , называется мультипликативной, если для любых взаимно простых натуральных чисел  $m, n$  выполняется равенство  $f(m \cdot n) = f(m) \cdot f(n)$ .

**ТЕОРЕМА 1.** Функция Эйлера мультипликативная.

Доказательство. Пусть  $m, n \in N, (m, n) = 1$ . Покажем, что  $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ . Полную систему вычетов по модулю  $m \cdot n$  запишем в виде таблицы:

$$\begin{array}{cccccc}
 1 & 2 & 3 & \dots & m \\
 m+1 & m+2 & m+3 & \dots & 2m \\
 2m+1 & 2m+2 & 2m+3 & \dots & 3m \\
 \vdots & \vdots & \vdots & \ddots & \vdots \\
 (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \dots & n \cdot m
 \end{array} \quad (9.1)$$

Так как  $\forall(x \in N)(x, mn) = 1 \Leftrightarrow (x, m) = 1 \wedge (x, n) = 1$ , то число натуральных чисел в (9.1), взаимно простых с  $m \cdot n$ , равно числу натуральных чисел, каждое из которых является взаимно простым как с  $m$ , так и с  $n$ . Так как  $(km + r, m) = 1 \Leftrightarrow (r, m) = 1$ , то столбцы в (9.1) с такими номерами  $r$ , что  $(r, m) = 1$ , состоят из натуральных чисел взаимно простых с  $m$ . Число таких столбцов в (9.1)  $\varphi(m)$ . Каждый такой столбец состоит из чисел вида

$$r, m + r, 2m + r, \dots, (n - 1)m + r, \quad (9.2)$$

где  $r \in \{1, 2, \dots, m - 1\}$ . Так как совокупность целых чисел  $0, 1, 2, \dots, n - 1$  – ПСВ по  $\text{mod } n$  и  $(m, n) = 1$ , то согласно теореме 4 § 8 совокупность целых чисел (9.2) есть полная система вычетов по  $\text{mod } n$ . Следовательно, она содержит  $\varphi(n)$  натуральных чисел, взаимно простых с  $n$ . Значит, в таблице (9.1) имеется  $\varphi(m)$  столбцов натуральных чисел, взаимно простых с  $m$ , и в каждом таком столбце имеется только

$\varphi(n)$  натуральных чисел, взаимно простых с  $n$ . Следовательно, в таблице (9.1) содержится  $\varphi(m) \cdot \varphi(n)$  натуральных чисел, взаимно простых с  $m \cdot n$ . Значит,  $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ . Теорема доказана.

**ТЕОРЕМА 2.** Пусть  $n = p^\alpha$ , где  $p$  – простое натуральное число,  $\alpha \in N$ , тогда  $\varphi(n) = p^\alpha \left(1 - \frac{1}{p}\right)$ .

Доказательство. Пусть  $x \in N$ ,  $(x, n) = d$ . Если  $d > 1$ , то  $d$  является степенью с основанием  $p$ , показатель которой  $k$ ,  $k \leq \alpha$ . Отсюда следует, что  $x \in N$ ,  $(x, n) = 1$  тогда и только тогда, когда  $x \not\equiv 0 \pmod{p}$ . Так как число чисел, кратных  $n$  и не превосходящих  $n$ , равно  $E\left(\frac{n}{p}\right) = p^{\alpha-1}$ , то число чисел, взаимно простых с  $n$  и не превосходящих  $n$ , равно  $p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$ .

**ТЕОРЕМА 3.** Пусть  $n \in N$  имеет следующее каноническое разложение на произведение простых множителей

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

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

Доказательство. Так как  $p_1, p_2, \dots, p_k$  – простые числа, то  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$  – взаимно простые натуральные числа. Методом математической индукции нетрудно доказать, что если  $f$  – мультипликативная функция на  $N$  и  $n_1, n_2, \dots, n_k$  – попарно взаимно простые натуральные числа, то имеет место равенство  $f(n_1 \cdot n_2 \cdot \dots \cdot n_k) = f(n_1) f(n_2) \dots f(n_k)$ . Тогда, с учетом теоремы 3, имеем:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

### Пример 2

$$120 = 2^3 \cdot 3 \cdot 5, \quad \varphi(120) = 120 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 32.$$

ТЕОРЕМА ЭЙЛЕРА. Пусть  $a, m \in \mathbb{Z}, m > 1$ . Если  $(a, m) = 1$ , то  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

Доказательство. Пусть

$$r_1, r_2, \dots, r_{\varphi(m)} \quad (9.3)$$

приведенная система вычетов по  $\text{mod } m$ . Так как  $(a, m) = 1$ , то

$$ar_1, ar_2, \dots, ar_{\varphi(m)} \quad (9.4)$$

приведенная система вычетов по  $\text{mod } m$ . Каждому целому числу из (9.4) поставим в соответствие целое число из (9.3), сравнимое с ним по  $\text{mod } m$ . В результате получим:

$$\left. \begin{array}{l} ar_1 \equiv r_\alpha \pmod{m}, \\ ar_2 \equiv r_\beta \pmod{m}, \\ \dots \\ ar_{\varphi(m)} \equiv r_\gamma \pmod{m}. \end{array} \right] \quad (9.5)$$

Найдем произведение сравнений в (9.5):

$$a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_\alpha r_\beta \dots r_\gamma \pmod{m}. \quad (9.6)$$

Заметим, что  $r_1 r_2 \dots r_{\varphi(m)} = r_\alpha r_\beta \dots r_\gamma$ . Учитывая, что  $(r_1 r_2 \dots r_{\varphi(m)}, m) = 1$ , из (9.6) получим  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

ТЕОРЕМА ФЕРМА. Пусть  $a \in \mathbb{Z}, p \in \mathbb{N}, p$  – простое число. Если  $(a, p) = 1$ , то  $a^{p-1} \equiv 1 \pmod{p}$ .

Теорема Ферма является следствием теоремы Эйлера.

### Пример 3

Найти остаток от деления числа  $a = 18^{125}$  на 15.

Решение

Пусть  $r$  остаток от деления числа  $a$  на 15,  $a = 15g + r, 0 \leq r < 15$ . Тогда  $r \equiv 18^{125} \pmod{15}$ .  $(r - 18^{125}) : 15 \wedge (18, 15) = 3 \Rightarrow r : 3$ . Пусть  $r = 3r_1$ ,

$r_1 \in N$ . Тогда из сравнения  $3r_1 \equiv 18 \cdot 18^{124} \pmod{15}$  следует, что  $r_1 \equiv 6 \cdot 18^{124} \pmod{5}$ . Так как  $(18, 5) = 1$ , то по теореме Эйлера  $18^{\varphi(5)} \equiv 1 \pmod{5}$ ,  $18^4 \equiv 1 \pmod{5}$ .  $18^4 \equiv 1 \pmod{5} \Rightarrow 18^{124} \equiv 1 \pmod{5}$ .  $18^{124} \equiv 1 \pmod{5} \wedge 6 \equiv 1 \pmod{5} \Rightarrow 6 \cdot 18^{124} \equiv 1 \pmod{5}$ . Из условий  $r_1 \equiv 6 \cdot 18^{124} \pmod{5}$ ,  $6 \cdot 18^{124} \equiv 1 \pmod{5}$ ,  $0 \leq r_1 < 5$  следует, что  $r_1 = 1$ . Так как  $r = 3r_1$ , то  $r = 3$ .

#### Пример 4

Найти две последние цифры в записи числа  $a = 28^{122}$ .

#### Решение

Пусть  $r$  остаток от деления числа  $a$  на 100,  $a = 100g + r$ ,  $0 \leq r < 100$ . Тогда  $r \equiv 28^{122} \pmod{100}$ .

Две последние цифры в записи числа  $r$  являются двумя последними цифрами числа  $a$ . Так как  $(r - 28^{122}) : 100 \wedge (100, 28) = 4$ , то  $r : 4$ . Пусть  $r = 4r_1$ ,  $0 \leq r_1 < 25$ . Тогда из сравнения  $4r_1 \equiv 28^{122} \pmod{100}$  следует, что  $r_1 \equiv 7 \cdot 28^{121} \pmod{25}$ . Так как  $(28, 25) = 1$ , то по теореме Эйлера

$$28^{\varphi(25)} \equiv 1 \pmod{25}, \quad 28^{20} \equiv 1 \pmod{25}. \quad 28^{20} \equiv 1 \pmod{25} \Rightarrow 28^{120} \equiv 1 \pmod{25}.$$

$$28^{120} \equiv 1 \pmod{25} \wedge 7 \cdot 28 \equiv 21 \pmod{25} \Rightarrow 7 \cdot 28^{121} \equiv 21 \pmod{25}.$$

Из условий  $r_1 \equiv 7 \cdot 28^{121} \pmod{25}$ ,  $7 \cdot 28^{121} \equiv 21 \pmod{25}$ ,  $0 \leq r_1 < 25$  следует, что  $r_1 = 21$ . Так как  $r = 4r_1$ , то  $r = 84$ . Следовательно, 8 и 4 две последние цифры в записи числа  $a = 28^{122}$ .

### Упражнения

1. Сколько натуральных чисел, взаимно простых с числом 520 и не превосходящих этого числа?

Вычислите:

- |                     |                      |                     |
|---------------------|----------------------|---------------------|
| a) $\varphi(800)$ ; | б) $\varphi(125)$ ;  | в) $\varphi(360)$ ; |
| г) $\varphi(128)$ ; | д) $\varphi(1001)$ ; | е) $\varphi(80)$ .  |

2. Найдите число классов вычетов, взаимно простых с модулем  $m = 1225$ .

3. Докажите, что  $(a^{12} - 1) : 7$ , если  $(a, 7) = 1$ .

4. Докажите, что  $a^{p-1} + p - 1$ , где  $a \not\equiv 0 \pmod{p}$ , является составным.

5. Докажите, что  $(a^{12} - b^{12}) : 65$ , если  $(a, 65) = (b, 65) = 1$ .

6. Решите уравнения:

а)  $\varphi(5^x) = 100$ ;      б)  $\varphi(7^x) = 294$ ;      в)  $\varphi(3^x 5^y) = 600$ .

7. Решите уравнения:

а)  $\varphi(m) = 3600$ , где  $m = 3^\alpha 5^\beta 7^\gamma$ ;

б)  $\varphi(m) = 11424$ , где  $m = p_1^2 p_2^2$  и  $p_1, p_2$  – простые натуральные числа.

8. Найдите остаток от деления:

а)  $66^{17}$  на 7;      б)  $22^{2342}$  на 14;

в)  $34^{3741}$  на 26;      г)  $64^{728}$  на 6;

д)  $7^{100} + 11^{100}$  на 13;      е)  $8^{80} + 13^{90}$  на 17;

ж)  $(85^{70} + 19^{32})^{17}$  на 21;      з)  $(84^{80} + 23^{40})^{15}$  на 25;

и)  $(15728 + 19^{30})^7$  на 57;      к)  $5^{70} + 7^{50}$  на 12.

9. Докажите, что:

а)  $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} + 1$  делится на 7;

б) число  $7^{40} - 5^{30}$  делится на 11;

в) число  $13^{176} - 1$  делится на 89.

10. Найдите последнюю цифру в десятичном представлении чисел:

а)  $3^{105}$ ;      б)  $13^{219}$ ;      в)  $17^{501}$ ;      г)  $243^{402}$ ;

д)  $473^{1971}$ ;      е)  $23^{2010}$ ;      ж)  $66^{210}$ .

11. Найдите две последние цифры в десятичном представлении чисел предыдущей задачи.

## § 10. Сравнения с одной неизвестной. Сравнения первой степени

### Сравнения с одной неизвестной

Сравнение вида

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{m}, \quad (10.1)$$

где  $f(x)$  – многочлен с целыми коэффициентами, называется сравнением с одной неизвестной. Если  $a_n \not\equiv 0 \pmod{m}$ , то  $n$  называется степенью сравнения (10.1).

Если  $a \in Z$  удовлетворяет сравнению (10.1), т.е.  $f(a) \equiv 0 \pmod{m}$ , то  $\forall (b \in \bar{a})$ , где  $\bar{a}$  – класс вычетов по  $\text{mod } m$ , удовлетворяет сравнению (10.1). Действительно, из  $a \equiv b \pmod{m}$  следует, что  $f(a) \equiv f(b) \pmod{m}$ . Так как  $f(a) \equiv 0 \pmod{m}$ , то в силу свойства транзитивности сравнения имеем:  $f(b) \equiv 0 \pmod{m}$ .

**Определение.** Класс вычетов по  $\text{mod } m$ , целые числа из которого удовлетворяют сравнению (10.1), называется решением сравнения (10.1).

Решить данное сравнение можно следующим образом: выписать полную систему вычетов по  $\text{mod } m$

$$x_1, x_2, \dots, x_m. \quad (10.2)$$

Классы вычетов по  $\text{mod } m$ , порожденные теми целыми числами из (10.2), которые удовлетворяют сравнению (10.1), являются решениями сравнения (10.1).

**Пример 1**

Решить сравнение

$$f(x) = x^2 + x + 1 \equiv 0 \pmod{3}.$$

**Решение**

$-1, 0, 1$  – полная система вычетов по  $\text{mod } 3$ . Так как  $f(0) = 1 \not\equiv 0 \pmod{3}$ ,  $f(-1) = 1 \not\equiv 0 \pmod{3}$ ,  $f(1) = 3 \equiv 0 \pmod{3}$ , то класс вычетов  $\bar{1}$  является решением сравнения.

**Определение.** Сравнения  $f(x) \equiv 0 \pmod{m}$ ,  $g(x) \equiv 0 \pmod{m_1}$  называются равносильными, если множество целых чисел, удовлетворяющих одному из сравнений, совпадает со множеством целых чисел, удовлетворяющих другому сравнению.

## Свойства равносильности сравнений

1. Если в сравнении  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{m}$  заменить коэффициенты многочлена  $f(x)$  целыми числами, сравнимыми с коэффициентами по  $\text{mod } m$  (например,  $a_n \equiv b_n \pmod{m}$ ,  $a_{n-1} \equiv b_{n-1} \pmod{m}$ , ...,  $a_0 \equiv b_0 \pmod{m}$ ), то получим сравнение  $b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0 \equiv 0 \pmod{m}$ , равносильное исходному сравнению.

2. Если обе части сравнения  $f(x) \equiv 0 \pmod{m}$  умножим на число  $k \in \mathbb{Z}$ ,  $k \neq 0$ ,  $(k, m) = 1$ , то получим равносильное сравнение  $kf(x) \equiv 0 \pmod{m}$ .

3. Если обе части сравнения  $f(x) \equiv 0 \pmod{m}$  и модуль  $m$  умножим на  $k \in \mathbb{N}$ , то получим сравнение  $kf(x) \equiv 0 \pmod{mk}$ , которое равносильно исходному сравнению.

## Сравнение первой степени с одной неизвестной

Любое сравнение первой степени с одной неизвестной можно привести к виду  $ax \equiv b \pmod{m}$ .

ТЕОРЕМА. Пусть дано сравнение

$$ax \equiv b \pmod{m} \quad (10.3)$$

и  $(a, m) = d$ . Если  $d = 1$ , то сравнение (10.3) имеет единственное решение; если  $d > 1$  и  $b \not\equiv d$ , то сравнение (10.3) не имеет решений; если  $d > 1$  и  $b \equiv d$ , то сравнение (10.3) имеет  $d$  различных решений, образующих один класс вычетов по  $\text{mod } \frac{m}{d}$ .

Доказательство. 1. По условию  $(a, m) = 1$ . Выпишем ПСВ по  $\text{mod } m$ :  $x_1, x_2, \dots, x_m$ . Так как  $(a, m) = 1$ , то

$$ax_1, ax_2, \dots, ax_m \pmod{m} \quad (10.4)$$

ПСВ по  $\text{mod } m$ . Целое число  $b$  сравнимо только с одним из целых чисел в (10.4). Пусть  $ax_i \equiv b \pmod{m}$ . Тогда класс вычетов  $\overline{x_i}$  по  $\text{mod } m$  является решением сравнения (10.3) и притом единственным.

2. По условию  $(a, m) = d$ ,  $b \not\equiv d$ . Предположим, что класс вычетов  $\overline{x_0}$  по  $\text{mod } m$  является решением сравнения (10.3). Тогда  $ax_0 \equiv b \pmod{m}$  или  $ax_0 - b = mt$ ,  $t \in \mathbb{Z}$ . Из этого равенства следует, что  $b \equiv d$  (противоречие). В этом случае сравнение (10.3) не имеет решений.

3. По условию  $(a, m) = d$ ,  $b \div d$ . Пусть  $a = a_1 d$ ,  $b = b_1 d$ ,  $m = m_1 d$ . Если обе части сравнения (10.3) и модуль  $m$  разделим на  $d$ , то получим сравнение

$$a_1 x \equiv b_1 \pmod{m_1}. \quad (10.5)$$

Нетрудно показать, что сравнения (10.3) и (10.5) равносильны. Так как  $(a_1, m_1) = 1$ , то сравнение (10.5) имеет единственное решение. Пусть класс вычетов  $\bar{x}_0$  по  $\text{mod } m_1$  является решением сравнения (10.5),

$$\bar{x}_0 = \{\dots, x_0 - 2m_1, x_0 - m_1, x_0, x_0 + m_1, x_0 + 2m_1, \dots, x_0 + (d-1)m_1, \dots\}.$$

Так как сравнения (10.3) и (10.5) равносильны, то только целые числа из класса вычетов  $\bar{x}_0$  удовлетворяют сравнению (10.3). Покажем, что целые числа из класса вычетов  $\bar{x}_0$  по  $\text{mod } m_1$  образуют  $d$  различных классов вычетов по  $\text{mod } m$ . Рассмотрим последовательность

$$x_0, x_0 + m_1, x_0 + 2m_1, \dots, x_0 + (d-1)m_1. \quad (10.6)$$

Целые числа в (10.6) попарно несравнимы по  $\text{mod } m$ . Действительно, если предположить, что  $x_0 + km_1 \equiv x_0 + lm_1 \pmod{m}$ , где  $0 \leq k < l \leq d-1$ , то из этого сравнения получаем  $k \equiv l \pmod{d}$ , т.е.  $(k-l) \div d$ . Пришли к противоречию, так как  $0 \leq k < l \leq d-1 \Rightarrow (k-l) \nmid d$ . Покажем, что любое целое число  $x_0 + sm_1$ ,  $s \in \mathbb{Z}$ , сравнимо с одним из целых чисел в (10.6). Разделим  $s$  на  $d$  с остатком:  $s = t \cdot d + r$ ,  $0 \leq r \leq d-1$ . Тогда из равенства  $x_0 + sm_1 = x_0 + rm_1 + mt$  следует, что  $x_0 + sm_1 \equiv x_0 + rm_1 \pmod{m}$ ,  $0 \leq r \leq d-1$ . Показано, что любое целое число из класса вычетов  $\bar{x}_0$  по  $\text{mod } m_1$  сравнимо с одним из целых чисел в (10.6) по  $\text{mod } m$ . Таким образом, классы вычетов по  $\text{mod } m$ , порожденные целыми числами в (10.6), являются решениями сравнения (10.3):  $x \equiv x_0 \pmod{m}$ ,  $x \equiv x_0 + m_1 \pmod{m}$ , ...,  $x \equiv x_0 + (d-1)m_1 \pmod{m}$ . Теорема доказана.

## Способы решения сравнений первой степени

1. *Подстановка в сравнение первой степени целых чисел из ПСВ.*

Этот способ применяется при небольших модулях.

Пусть задано сравнение  $ax \equiv b \pmod{m}$ . Выпишем ПСВ по  $\text{mod } m$ :

$$x_1, x_2, \dots, x_m. \quad (10.7)$$

Классы вычетов по  $\text{mod } m$ , порожденные теми целыми числами из ПСВ (10.7), которые удовлетворяют сравнению  $ax \equiv b \pmod{m}$ , являются решениями этого сравнения.

## **2. Приведение сравнения первой степени к равносильному сравнению с коэффициентом при $x$ , равном единице.**

Этот способ основан на проведении ряда равносильных преобразований заданного сравнения, основанных на свойствах равносильности сравнений.

**Пример 2**

Решить сравнение  $24x \equiv 27 \pmod{37}$ .

**Решение**

Так как  $(24, 37) = 1$ , то сравнение имеет единственное решение.

$$(3, 37) = 1 \wedge 24x \equiv 27 \pmod{37} \Leftrightarrow 72x \equiv 81 \pmod{37}.$$

Так как  $72 \equiv -2 \pmod{37} \wedge 81 \equiv 7 \pmod{37}$ , то  $72x \equiv 81 \pmod{37} \Leftrightarrow -2x \equiv 7 \pmod{37}$ . Умножив обе части этого сравнения на 18 и учитывая, что  $-36 \equiv 1 \pmod{37} \wedge 126 \equiv 15 \pmod{37}$ , получим сравнение  $x \equiv 15 \pmod{37}$ . Класс целых чисел  $x \equiv 15 \pmod{37}$  является решением сравнения.

## **3. Способ Эйлера.**

Пусть задано сравнение

$$ax \equiv b \pmod{m}, \quad (10.8)$$

где  $(a, m) = 1$ . Сравнение имеет единственное решение. По теореме Эйлера,  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . Если обе части этого сравнения умножим на  $b$ , то получим  $a(a^{\varphi(m)-1}b) \equiv b \pmod{m}$ . Отсюда следует, что класс целых чисел  $x \equiv (a^{\varphi(m)-1}b) \pmod{m}$  является решением сравнения.

**Пример 3**

Решить сравнение  $5x \equiv 7 \pmod{8}$ .

**Решение**

Так как  $(5, 8) = 1$ , то сравнение имеет единственное решение.

Так как  $\varphi(8) = 4$ , то класс целых чисел  $x \equiv 5^3 \cdot 7 \pmod{8}$  или  $x \equiv 3 \pmod{8}$  решение сравнения.

## **4. Решение сравнения первой степени при помощи конечных цепных дробей.**

Пусть задано сравнение (10.8). Разложим  $\frac{m}{a}$  в конечную цепную дробь.

Если  $\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} = \frac{m}{a}$  являются последними подходящими дробями, то по свойству подходящих дробей имеем:  $P_{n-1}Q_n - Q_{n-1}P_n = (-1)^n$  или  $aP_{n-1} - Q_{n-1}m = (-1)^n$ . Если обе части последнего равенства умножим на  $(-1)^n b$ , то получим

$$a(-1)^n P_{n-1}b - b(-1)^n Q_{n-1}m = b.$$

Отсюда следует, что  $a((-1)^n P_{n-1}b) \equiv b \pmod{m}$ . Значит, класс целых чисел  $x \equiv (-1)^n P_{n-1}b \pmod{m}$  является решением сравнения.

**Пример 4**

Решить сравнение  $55x \equiv 7 \pmod{87}$ .

**Решение**

Так как  $(55, 87) = 1$ , то сравнение имеет единственное решение. Разложим  $\frac{m}{a} = \frac{87}{55}$  в конечную цепную дробь:  $\frac{87}{55} = [1; 1, 1, 2, 1, 1, 4]$ .

Для нахождения числителя предпоследней подходящей дроби составим таблицу.

$S$	0	1	2	3	4	5	6
$q_s$	1	1	1	2	1	1	4
$P_s$	1	2	3	8	11	19	87

Из таблицы следует, что  $P_5 = 19$ . Класс целых чисел  $x \equiv (-1)^6 19 \cdot 7 \pmod{87}$  или  $x \equiv 46 \pmod{87}$  является решением сравнения.

**Пример 5**

Решить сравнение  $82x \equiv 14 \pmod{202}$ .

**Решение**

Так как  $(82, 14) = 2$ ,  $14 \div 2$ , то сравнение имеет два решения. Поделив обе части сравнения на 2, получим равносильное сравнение  $41x \equiv 7 \pmod{101}$ , которое имеет одно решение, так как  $(41, 101) = 1$ .

Решим это сравнение с помощью цепных дробей. Разложим  $\frac{m}{a} = \frac{101}{41}$

в конечную цепную дробь:  $\frac{101}{41} = [2; 2, 6, 3]$ . Для нахождения числителя предпоследней подходящей дроби составим таблицу:

$s$	0	1	2	3
$q_s$	2	2	6	3
$P_s$	2	5	32	101

Из таблицы следует, что  $P_2 = 32$ . Класс целых чисел  $x \equiv (-1)^3 32 \cdot 7 \pmod{101}$  или  $x \equiv 79 \pmod{101}$  – решение сравнения  $41x \equiv 7 \pmod{101}$ . Решением сравнения  $82x \equiv 14 \pmod{202}$  являются классы вычетов:  $x \equiv 79 \pmod{202}$ ,  $x \equiv 180 \pmod{202}$ .

### Упражнения

1. Решите следующие сравнения:

- а)  $5x \equiv 6 \pmod{9}$ ;    б)  $39x \equiv 5 \pmod{11}$ ;    в)  $37x \equiv 16 \pmod{11}$ ;  
 г)  $16x \equiv 9 \pmod{14}$ ;    д)  $11x \equiv 15 \pmod{24}$ ;    е)  $5x \equiv 15 \pmod{25}$ ;  
 ж)  $75x \equiv 54 \pmod{21}$ ;    з)  $12x \equiv 16 \pmod{28}$ ;    и)  $20x \equiv 35 \pmod{45}$ .

2. Решите следующие сравнения с помощью цепных дробей:

- а)  $37x \equiv 25 \pmod{107}$ ;    б)  $95x \equiv 59 \pmod{308}$ ;  
 в)  $185x \equiv 125 \pmod{535}$ ;    г)  $221x \equiv 111 \pmod{360}$ ;  
 д)  $41x \equiv 7 \pmod{101}$ ;    е)  $271x \equiv 25 \pmod{119}$ ;  
 ж)  $23x \equiv 5 \pmod{71}$ ;    з)  $59x \equiv 5 \pmod{201}$ ;  
 и)  $341x \equiv 15 \pmod{127}$ ;    к)  $73x \equiv 6 \pmod{113}$ .

3. Решите сравнения:

- а)  $5x \equiv 7 \pmod{8}$ ;    б)  $13x \equiv 19 \pmod{29}$ ;  
 в)  $13x \equiv 178 \pmod{153}$ ;    г)  $12x \equiv 15 \pmod{20}$ ;

д) измените правую часть последнего сравнения так, чтобы полученное сравнение имело четыре решения. Найдите их.

## § 11. Системы сравнений первой степени

Рассмотрим систему сравнений

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1}, \\ f_2(x) \equiv 0 \pmod{m_2}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_k(x) \equiv 0 \pmod{m_k}, \end{cases} \quad (11.1)$$

где  $f_i(x)$  ( $i = \overline{1, k}$ ) – многочлены с целыми коэффициентами. Обозначим  $M = [m_1, m_2, \dots, m_k]$ . Если  $a \in Z$  удовлетворяет системе (11.1), т.е.

$$f_i(a) \equiv 0 \pmod{m_i} \quad (i = \overline{1, k}), \quad (11.2)$$

то любое  $b \in Z$  такое, что  $b \equiv a \pmod{M}$ , удовлетворяет системе (11.1). Действительно, из того, что  $b \equiv a \pmod{M}$ , следует согласно теореме 1 § 1, что  $f_i(b) \equiv f_i(a) \pmod{M}$ . Так как  $M : m_i$  ( $i = \overline{1, k}$ ), то из сравнения  $f_i(b) \equiv f_i(a) \pmod{M}$  получим, что  $f_i(b) \equiv f_i(a) \pmod{m_i}$ . Но тогда, в силу (11.2),  $f_i(b) \equiv 0 \pmod{m_i}$ . Таким образом, если  $a \in Z$  удовлетворяет системе сравнений (11.1), то  $\forall (b \in \bar{a})$ , где  $\bar{a}$  – класс целых чисел по модулю  $M$ , удовлетворяет системе сравнений (11.1).

**Определение.** Решением системы сравнений (11.1), где  $f_i(x)$  ( $i = \overline{1, k}$ ) – многочлены с целыми коэффициентами, называется класс чисел по модулю  $M$ ,  $M = [m_1, m_2, \dots, m_k]$ , целые числа из которого удовлетворяют сравнению (11.1).

Решить систему (11.1) можно следующим образом.

1. Выписать полную систему вычетов по модулю  $M$ .
2. Проверить, какие числа из этой системы удовлетворяют системе сравнений (11.1).

Классы вычетов по модулю  $M$ , порожденные теми целыми числами из полной системы вычетов по модулю  $M$ , которые удовлетворяют системе сравнений (11.1), образуют множество решений системы (11.1).

**Пример 1**

Найти решение системы сравнений

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

## Р е ш е н и е

В данном случае  $M = [4, 6] = 12$ . Полная система наименьших по абсолютной величине вычетов:  $-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6$ . Только  $-2$  и  $2$  удовлетворяют системе сравнений. Поэтому решения системы сравнений – это два класса по модулю 12:  $x \equiv -2 \pmod{12}$  и  $x \equiv 2 \pmod{12}$ .

## Системы сравнений первой степени

Рассмотрим систему вида

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}. \end{cases} \quad (11.3)$$

**ТЕОРЕМА 1.** Пусть  $d = (m_1, m_2)$ ,  $M = [m_1, m_2]$ . Тогда если  $(c_2 - c_1) \not\equiv d$ , то система (11.3) не имеет решений, а если  $(c_2 - c_1) \equiv d$ , то система (11.3) имеет одно решение, представляющее класс целых чисел по модулю  $M$ .

Доказательство. Первому уравнению системы (11.3) удовлетворяют целые числа вида  $x = c_1 + m_1 t, t \in Z$ . Необходимо выбрать такие целые  $t$ , при которых  $x$  удовлетворяет второму сравнению. Отыскание таких  $t$  сводится к решению сравнения

$$m_1 t \equiv c_2 - c_1 \pmod{m_2}. \quad (11.4)$$

Если  $(c_2 - c_1) \not\equiv d$ , то сравнение (11.4) не имеет решений. В этом случае среди всех целых значений  $x$ , удовлетворяющих первому сравнению  $x \equiv c_1 \pmod{m_1}$  нет ни одного, которое бы удовлетворяло второму уравнению системы. Значит, в этом случае система не совместна.

Если  $(c_2 - c_1) \equiv d$ , то система имеет  $d$  различных решений, которые образуют один класс целых чисел по модулю  $\frac{m_2}{d}$ . Этот класс

можно записать в виде  $t \equiv \alpha \pmod{\frac{m_2}{d}}$ . Значит, сравнению (11.4) удов-

летворяют целые числа вида  $t = \alpha + \frac{m_2}{d} y, y \in Z$ . Из множества значений  $x$ , удовлетворяющих первому сравнению, выделим те, которые удовлетворяют второму сравнению системы:

$$x = c_1 + \left(\alpha + \frac{m_2}{d} y\right)m_1 = c_1 + \alpha m_1 + \frac{m_1 m_2}{d} y = \beta + M y, y \in Z.$$

Целые числа вида  $x = \beta + My$ ,  $y \in Z$ , образуют класс вычетов по модулю  $M$ , т.е.  $x \equiv \beta \pmod{M}$ . Система (11.3) имеет одно решение.

**ТЕОРЕМА 2.** Система

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots \\ x \equiv c_k \pmod{m_k} \end{cases} \quad (11.5)$$

либо не имеет решений, либо имеет одно решение.

**ТЕОРЕМА 3.** Если в системе сравнений (11.5)  $m_1, m_2, \dots, m_k$  попарно взаимно простые числа, то система (11.5) совместна и имеет одно решение, представляющее класс целых чисел по модулю  $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$ .

**Пример 2**

Решить систему сравнений

$$\begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 7 \pmod{6}, \\ x \equiv 4 \pmod{15}. \end{cases} \quad (11.6)$$

**Решение**

Решим сначала систему, состоящую из первых двух сравнений:

$$\begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 7 \pmod{6}. \end{cases}$$

Так как  $(8,6) = 2$  и  $(3-7):2$ , то система имеет одно решение. Первому сравнению системы удовлетворяют числа вида  $x = 3 + 8t$ ,  $t \in Z$ . Чтобы определить такие целые значения  $t$ , при которых число  $x$  удовлетворяет второму сравнению системы, решим сравнение  $x = 3 + 8t \equiv 7 \pmod{6}$ ,  $8t \equiv 4 \pmod{6}$ . Так как  $(8,6) = 2$  и  $4:2$ , то это сравнение имеет два решения, образуя один класс вычетов по модулю 3. Разделив обе части сравнения  $8t \equiv 4 \pmod{6}$  и модуль на 2, получим равносильное сравнение  $4t \equiv 2 \pmod{3}$  или  $t \equiv 2 \pmod{3}$ , так как  $4 \equiv 1 \pmod{3}$ . Числа вида  $t = 2 + 3k$ ,  $k \in Z$ , удовлетворяют сравнению  $t \equiv 2 \pmod{3}$ . Тогда целые числа  $x = 19 + 24k$ ,  $k \in Z$ , удовлетво-

ряют системе, состоящей из первых двух сравнений, и класс целых чисел  $x \equiv 19 \pmod{24}$  – решение этой системы.

Таким образом, система сравнений (11.6) эквивалентна системе

$$\begin{cases} x \equiv 19 \pmod{24}, \\ x \equiv 4 \pmod{15}. \end{cases}$$

Так как  $(24, 15) = 3$  и  $(19 - 4) : 3$ , то система совместна. Найдем ее решение. Определим такие целые значения  $k$ , чтобы число  $x = 19 + 24k$  удовлетворяло сравнению  $x \equiv 4 \pmod{15}$ ,  $x = 19 + 24k \equiv 4 \pmod{15}$ ,  $24k \equiv -15 \pmod{15}$ . Так как  $24 \equiv 9 \pmod{15}$  и  $-15 \equiv 0 \pmod{15}$ , то сравнение  $24k \equiv -15 \pmod{15}$  равносильно сравнению  $9k \equiv 0 \pmod{15}$  или  $3k \equiv 0 \pmod{5}$ . Умножив обе части этого сравнения на 2 и учитывая, что  $6 \equiv 1 \pmod{5}$ , получим сравнение  $k \equiv 0 \pmod{5}$ . Этому сравнению удовлетворяют числа  $k = 5l$ ,  $l \in \mathbb{Z}$ . Но тогда  $x = 19 + 120l$ ,  $l \in \mathbb{Z}$ . Класс целых чисел  $x \equiv 19 \pmod{120}$  – решение системы (11.6).

**ТЕОРЕМА 4.** Пусть  $m_1, m_2, \dots, m_k$  попарно взаимно простые числа,  $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$  и  $y_1, y_2, \dots, y_k$  подобраны так, что

$$\frac{M}{m_1} y_1 \equiv 1 \pmod{m_1}, \quad \frac{M}{m_2} y_2 \equiv 1 \pmod{m_2}, \quad \dots, \quad \frac{M}{m_k} y_k \equiv 1 \pmod{m_k}$$

и  $x_0 = \frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + \dots + \frac{M}{m_k} y_k c_k$ . Тогда решением системы

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots \\ x \equiv c_k \pmod{m_k} \end{cases}$$

является класс целых чисел  $x \equiv x_0 \pmod{M}$ .

**Пример 3**

Решить систему

$$\begin{cases} x \equiv 5 \pmod{13}, \\ x \equiv 2 \pmod{9}, \\ x \equiv 6 \pmod{7}. \end{cases}$$

## Решение

Найдем целые числа  $y_1, y_2, y_3$ , удовлетворяющие, соответственно, сравнениям  $9 \cdot 7y \equiv 1(\text{mod } 13)$ ,  $13 \cdot 7y \equiv 1(\text{mod } 9)$ ,  $13 \cdot 9y \equiv 1(\text{mod } 7)$ . Так как  $63 \equiv -2(\text{mod } 13)$ , то сравнение  $9 \cdot 7y \equiv 1(\text{mod } 13)$  равносильно сравнению  $-2y \equiv 1(\text{mod } 13)$  или  $2y \equiv -1(\text{mod } 13)$ . Этому сравнению удовлетворяет число  $y_1 = 6$ . Сравнение  $13 \cdot 7y \equiv 1(\text{mod } 9)$  равносильно сравнению  $y \equiv 1(\text{mod } 9)$ , поэтому  $y_1 = 1$ . Так как  $117 \equiv -2(\text{mod } 7)$ , то сравнение  $13 \cdot 9y \equiv 1(\text{mod } 7)$  равносильно сравнению  $-2y \equiv 1(\text{mod } 7)$  или  $2y \equiv -1(\text{mod } 7)$ . Число  $y_3 = 3$  удовлетворяет сравнению  $2y \equiv -1(\text{mod } 7)$ .

Согласно теореме 4 число  $x_0 = 63 \cdot 6 \cdot 5 + 91 \cdot 1 \cdot 2 + 117 \cdot 3 \cdot 6 = 4178$  удовлетворяет каждому сравнению системы. Так как  $4178 \equiv 83(\text{mod } 819)$ , то класс целых чисел  $x \equiv 83(\text{mod } 819)$  – решение системы.

## Упражнения

1. Решите системы сравнений:

$$\begin{array}{lll} a) \begin{cases} x \equiv 12(\text{mod } 17), \\ x \equiv 10(\text{mod } 11); \end{cases} & б) \begin{cases} x \equiv 20(\text{mod } 23), \\ x \equiv 21(\text{mod } 25); \end{cases} & в) \begin{cases} x \equiv 15(\text{mod } 17), \\ x \equiv 7(\text{mod } 20); \end{cases} \\ г) \begin{cases} x \equiv 9(\text{mod } 16), \\ x \equiv 7(\text{mod } 25); \end{cases} & д) \begin{cases} x \equiv 15(\text{mod } 23), \\ x \equiv 12(\text{mod } 29); \end{cases} & е) \begin{cases} 3x \equiv 5(\text{mod } 4), \\ 5x \equiv 2(\text{mod } 7); \end{cases} \\ ж) \begin{cases} 5x \equiv 3(\text{mod } 4), \\ 7x \equiv 2(\text{mod } 5); \end{cases} & з) \begin{cases} 9x \equiv 7(\text{mod } 13), \\ 5x \equiv 2(\text{mod } 12). \end{cases} & \end{array}$$

2. Решите системы сравнений:

$$\begin{array}{lll} a) \begin{cases} 3x \equiv 2(\text{mod } 13), \\ 5x \equiv 11(\text{mod } 16), \\ 5x \equiv 2(\text{mod } 9); \end{cases} & б) \begin{cases} 3x \equiv 5(\text{mod } 13), \\ 2x \equiv 17(\text{mod } 21), \\ 5x \equiv 31(\text{mod } 32); \end{cases} & в) \begin{cases} 2x \equiv 5(\text{mod } 21), \\ 5x \equiv 22(\text{mod } 31), \\ 4x \equiv 5(\text{mod } 29); \end{cases} \\ г) \begin{cases} x \equiv 8(\text{mod } 15), \\ x \equiv 9(\text{mod } 13), \\ x \equiv 5(\text{mod } 14); \end{cases} & д) \begin{cases} 3x \equiv 8(\text{mod } 20), \\ 5x \equiv 8(\text{mod } 9), \\ 4x \equiv 1(\text{mod } 21); \end{cases} & е) \begin{cases} 2x \equiv 9(\text{mod } 15), \\ 5x \equiv 4(\text{mod } 7), \\ 7x \equiv 3(\text{mod } 9); \end{cases} \\ ж) \begin{cases} 3x \equiv 1(\text{mod } 25), \\ 6x \equiv 3(\text{mod } 33), \\ 4x \equiv 5(\text{mod } 9); \end{cases} & з) \begin{cases} 8x \equiv 1(\text{mod } 13), \\ 5x \equiv 7(\text{mod } 18), \\ 2x \equiv 1(\text{mod } 9). \end{cases} & \end{array}$$

## § 12. Сравнения высших степеней по простому модулю

### Число решений сравнений $n$ -й степени по простому модулю

Имеет место утверждение.

ТЕОРЕМА 1. Любое сравнение  $n$ -й степени

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p} \quad (12.1)$$

по простому модулю  $p$  имеет не более  $n$  решений.

Доказательство. Доказательство проведем методом математической индукции по  $n$ .

1. При  $n = 1$  сравнение  $a_1 x + a_0 \equiv 0 \pmod{p}$  имеет единственное решение, так как  $(a_1, p) = 1$ .

2. Предположим, что любое сравнение  $(n - 1)$  степени имеет не более  $(n - 1)$  решений. Докажем, что сравнение (12.1) имеет не более  $n$  решений.

Если сравнение (12.1) не имеет решений, то утверждение теоремы верно. Предположим, что сравнение (12.1) имеет решение и класс вычетов  $\bar{x}_1$  по простому модулю  $p$  является решением сравнения (12.1). Тогда имеет место сравнение

$$a_n x_1^n + a_{n-1} x_1^{n-1} + \dots + a_1 x_1 + a_0 \equiv 0 \pmod{p}. \quad (12.2)$$

Если из сравнения (12.1) вычтем сравнение (12.2), то получим сравнение

$$a_n (x^n - x_1^{n-1}) + a_{n-1} (x^{n-1} - x_1^{n-1}) + \dots + a_1 (x - x_1) \equiv 0 \pmod{p}. \quad (12.3)$$

Представляя каждое слагаемое  $a_l (x^l - x_1^l)$ , где  $l = \overline{2, n}$ , в сравнении (12.3) в виде

$$a_l (x^l - x_1^l) = (x - x_1)(x^{l-1} + x^{l-2} x_1 + \dots + x x_1^{l-2} + x_1^{l-1}),$$

вынеся затем  $(x - x_1)$  за скобку, получим сравнение вида

$$(x - x_1)(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_1 x + b_0) \equiv 0 \pmod{p}. \quad (12.4)$$

Сравнение (12.1) равносильно сравнению (12.4). Покажем теперь, что если сравнение (12.1) имеет решение, отличное от класса вычетов  $\bar{x}_1$ , то оно является решением сравнения

$$b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x + b_0 \equiv 0 \pmod{p}, \quad (12.5)$$

где  $b_{n-2}, \dots, b_1, b_0$  – некоторые целые числа,  $b_{n-1} = a_n$ . Пусть класс вычетов  $\bar{x}_2$  по простому модулю  $p$  – решение сравнения (12.4) и  $\bar{x}_2 \neq \bar{x}_1$ . Тогда имеет место сравнение

$$(x_2 - x_1)(b_{n-1}x_2^{n-1} + b_{n-2}x_2^{n-2} + \dots + b_1x_2 + b_0) \equiv 0 \pmod{p}. \quad (12.6)$$

Так как  $(x_2 - x_1, p) = 1$ , то из сравнения (12.6) следует, что

$$b_{n-1}x_2^{n-1} + b_{n-2}x_2^{n-2} + \dots + b_1x_2 + b_0 \equiv 0 \pmod{p}.$$

Показано, что любое решение сравнения (12.1), отличное от класса вычетов  $\bar{x}_1$ , является решением сравнения (12.5). Так как по индуктивному предположению 2-е сравнение (12.5) имеет не более  $n - 1$  решения, то сравнение (12.1) имеет не более  $n$  решений.

**ТЕОРЕМА 2.** Сравнение  $x^{p-1} - 1 \equiv 0 \pmod{p}$ , где  $p$  – простое число, имеет точно  $p - 1$  решений.

Доказательство. Согласно теореме Ферма любое целое число  $a$ ,  $(a, p) = 1$ , удовлетворяет этому сравнению. В частности, сравнению удовлетворяет каждое число из приведенной системы вычетов  $1, 2, 3, \dots, p-1$  по модулю  $p$ . Отсюда следует, что классы вычетов  $\bar{1}, \bar{2}, \bar{3}, \dots, \overline{p-1}$  по модулю  $p$  являются решениями сравнения  $x^{p-1} - 1 \equiv 0 \pmod{p}$ . Но тогда в силу теоремы (12.1) сравнение  $x^{p-1} - 1 \equiv 0 \pmod{p}$  имеет точно  $p - 1$  решений.

**ТЕОРЕМА 3.** Пусть  $p$  простое натуральное число. Если  $d$  натуральный делитель числа  $p - 1$ , то сравнение  $x^d - 1 \equiv 0 \pmod{p}$  имеет точно  $d$  решений.

Доказательство. Пусть  $p - 1 = d \cdot k, k \in \mathbb{N}$ . Сравнение  $x^{p-1} - 1 \equiv 0 \pmod{p}$  запишем в виде

$$(x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1) \equiv 0 \pmod{p}. \quad (12.7)$$

Из (12.7) следует, что любое решение сравнения  $x^{p-1} - 1 \equiv 0 \pmod{p}$  является, по крайней мере, решением одного из сравнений

$$x^d - 1 \equiv 0 \pmod{p}, \quad (12.8)$$

$$x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1 \equiv 0 \pmod{p}. \quad (12.9)$$

Согласно теореме 1 сравнение (12.9) имеет не более  $d(k-1) = p-d-1$  решений. Так как сравнение  $x^{p-1} - 1 \equiv 0 \pmod{p}$  имеет точно  $p-1$  решений и каждое его решение является решением, по крайней мере, одного из сравнений, то сравнение (12.8) имеет точно  $d$  решений.

### Построение равносильных сравнений

ТЕОРЕМА 4. Любое сравнение  $n$ -й степени

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p} \quad (12.10)$$

по простому модулю  $p$  можно заменить сравнением равносильным данному сравнению с коэффициентом при  $x^n$ , равным 1.

Доказательство. Рассмотрим сравнение  $a_n y \equiv 1 \pmod{p}$ . Так как  $(a_n, p) = 1$ , то это сравнение имеет единственное решение. Пусть класс вычетов  $\bar{y}_0$  по модулю  $p$  – решение сравнения  $a_n y \equiv 1 \pmod{p}$ , тогда  $a_n y_0 \equiv 1 \pmod{p}$ . Из сравнения  $a_n y_0 \equiv 1 \pmod{p}$  следует, что  $(y_0, p) = 1$ . Умножив обе части сравнения (12.10) на  $y_0$ , получим равносильное сравнение

$$y_0 a_n x^n + y_0 a_{n-1} x^{n-1} + \dots + y_0 a_1 x + y_0 a_0 \equiv 0 \pmod{p}. \quad (12.11)$$

Заменив теперь коэффициенты в сравнении (12.11) целыми числами из полной системы вычетов по  $\text{mod } p$ , наименьших по абсолютной величине, сравнимыми с этими коэффициентами, получим равносильное сравнение

$$x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 \equiv 0 \pmod{p}.$$

ТЕОРЕМА 5. Любое сравнение  $n$ -й степени по простому модулю  $p$ ,  $p \leq n$ , можно заменить сравнением, равносильным данному сравнению, степень которого меньше, чем  $p$ .

Доказательство. Пусть  $f(x) \equiv 0 \pmod{p}$  сравнение  $n$ -й степени по простому модулю  $p$ ,  $p \leq n$ . Разделим многочлен  $f(x)$  на  $x^p - x$ :  $f(x) = (x^p - x)g(x) + r(x)$ , где  $g(x), r(x)$  – многочлены с целыми коэффициентами, степень многочлена  $r(x)$  меньше  $p$ . Покажем что сравнения  $f(x) \equiv 0 \pmod{p}$  и  $r(x) \equiv 0 \pmod{p}$  равносильны. Пусть целое число  $a$  удовлетворяет сравнению  $f(x) \equiv 0 \pmod{p}$ , т.е.

$$f(a) = (a^p - a)g(a) + r(a) \equiv 0 \pmod{p}. \quad (12.12)$$

Так как в силу следствия теоремы Ферма  $(a^p - a)g(a) \equiv 0 \pmod{p}$ , то из сравнения (12.12) получим  $r(a) \equiv 0 \pmod{p}$ . С другой стороны, если  $b$  такое целое число, что  $r(b) \equiv 0 \pmod{p}$ , то, учитывая сравнение  $(b^p - b)g(b) \equiv 0 \pmod{p}$ , получим  $f(b) \equiv 0 \pmod{p}$ . Показано, что сравнения  $f(x) \equiv 0 \pmod{p}$  и  $r(x) \equiv 0 \pmod{p}$  равносильны.

**Пример**

Решить сравнение  $5x^5 + 4x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{3}$ .

**Решение**

Так как  $5 \equiv 2 \pmod{3}$ ,  $4 \equiv 1 \pmod{3}$ ,  $3 \equiv 0 \pmod{3}$ , то сравнение

$$5x^5 + 4x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{3}$$

равносильно сравнению  $2x^5 + x^4 + x^2 + x + 1 \equiv 0 \pmod{3}$ . Разделим многочлен  $5x^5 + 4x^4 + 3x^3 + x^2 + x + 1$  на  $x^3 - x$  с остатком:

$$\begin{array}{r|l} 2x^5 + x^4 + x^2 + x + 1 & x^3 - x \\ - 2x^5 - 2x^3 & \hline x^4 + 2x^3 + x^2 & \\ - x^4 - x^2 & \\ \hline 2x^3 + 2x^2 + x + 1 & \\ - 2x^3 - 2x & \\ \hline 2x^2 + 3x + 1 & \end{array}$$

Согласно теореме 5 исходное сравнение равносильно сравнению  $2x^2 + 3x + 1 \equiv 0 \pmod{3}$ . Так как из полной системы вычетов  $-1, 0, 1$  по модулю 3 только целые числа  $-1$  и  $1$  удовлетворяют сравнению  $2x^2 + 3x + 1 \equiv 0 \pmod{3}$ , то классы вычетов  $\bar{1}, \bar{2}$  по модулю 3 являются решениями исходного сравнения.

### Упражнения

1. Убедитесь, что следующие сравнения не имеют решений:

а)  $x^2 - 2x + 3 \equiv 0 \pmod{4}$ ;

б)  $x^3 + x + 4 \equiv 0 \pmod{5}$ ;

в)  $x^4 + 2 \equiv 0 \pmod{5}$ ;

г)  $x^5 - 2x^3 + 13x - 1 \equiv 0 \pmod{4}$ .

2. Убедитесь, что следующим сравнениям удовлетворяют любые целые значения неизвестного:

а)  $x^2 - x + 6 \equiv 0 \pmod{2}$ ;

б)  $x(x^2 - 1) \equiv 0 \pmod{6}$ ;

в)  $x^4 + 2x^3 - x^2 - 2x \equiv 0 \pmod{4}$ ;

г)  $x^p - x \equiv 0 \pmod{p}$ ,

где  $p$  – простое число.

3. Решите сравнения:

а)  $x^5 + 2x^4 - 2x^3 - 2x^2 + 2x - 1 \equiv 0 \pmod{3}$ ;

б)  $x^6 + x^5 - 2x^2 - x \equiv 0 \pmod{5}$ ;

в)  $x^7 - 3x^6 + x^5 - x^3 + 4x^2 - 4x + 2 \equiv 0 \pmod{5}$ ;

г)  $x^{12} + x^{11} - x^2 - 1 \equiv 0 \pmod{11}$ ;

д)  $x^{14} - x^{13} - x^2 + 2x + 1 \equiv 0 \pmod{13}$ ;

е)  $x^{10} + x^8 + x^7 - x^4 - x^2 + 4x - 3 \equiv 0 \pmod{7}$ ;

ж)  $x^{12} - 2x^7 + x^3 + 1 \equiv 0 \pmod{5}$ .

## § 13. Порядок целого числа и класса вычетов по заданному модулю

Пусть  $a, m$  – целые числа,  $m > 1$ ,  $(a, m) = 1$ .

**Определение.** Наименьшее натуральное число  $d$  такое, что  $a^d \equiv 1 \pmod{m}$ , называется порядком числа  $a$  по модулю  $m$  и обозначается  $O_m(a)$ .

Если  $b \equiv a \pmod{m}$ , то  $b$  имеет тот же порядок по модулю  $m$ , что и  $a$ . Таким образом, если  $O_m(a) = d$ , то любое целое число из класса вычетов  $\bar{a}$  по модулю  $m$  имеет порядок  $d$ .

**Определение.** Порядком класса вычетов  $\bar{a}$  по модулю  $m$  называется порядок целого числа  $a$  по модулю  $m$ .

**ТЕОРЕМА 1.** Если  $O_m(\bar{a}) = d$ , то целые числа  $a, a^2, a^3, \dots, a^d$  попарно не сравнимы по модулю  $m$ .

Доказательство. Предположим, что  $a^k \equiv a^l \pmod{m}$ ,  $1 \leq l < k \leq d$ . Так как  $(a^l, m) = 1$ , то из сравнения  $a^k \equiv a^l \pmod{m}$  следует, что  $a^{k-l} \equiv 1 \pmod{m}$ . Пришли к противоречию с условием, так как  $1 \leq k-l < d$ .

**ТЕОРЕМА 2.** Пусть  $O_m(\bar{a}) = d$  и  $n$  – неотрицательное целое число. Тогда сравнение  $a^n \equiv 1 \pmod{m}$  выполняется тогда и только тогда, когда  $n$  делится на  $d$ .

Доказательство. По условию  $O_m(\bar{a}) = d$  и  $a^d \equiv 1 \pmod{m}$ . Покажем, что  $n$  делится на  $d$ . Для этого разделим  $n$  на  $d$  с остатком:  $n = dq + r$ ,  $0 \leq r < d$ . Так как  $a^d \equiv 1 \pmod{m}$ , то  $a^{dq} \equiv 1 \pmod{m}$ . Умножив обе части этого сравнения на  $a^r$ , получим  $a^{dq+r} \equiv a^r \pmod{m}$ . Отсюда, в силу транзитивности отношения сравнения,  $a^r \equiv 1 \pmod{m}$ . Так как по условию  $a^r \not\equiv 1 \pmod{m}$ , если  $0 < r < d$ , то сравнение  $a^r \equiv 1 \pmod{m}$  возможно лишь при  $r = 0$ . Следовательно,  $n$  делится на  $d$ .

Пусть теперь  $n$  делится на  $d$ ,  $n = d \cdot k$ ,  $k \in \mathbb{N}$ . Тогда из сравнения  $a^d \equiv 1 \pmod{m}$  следует, что  $a^{dk} \equiv 1 \pmod{m}$ , т.е.  $a^n \equiv 1 \pmod{m}$ .

**ТЕОРЕМА 3.** Если  $O_m(\bar{a}) = d$ , то  $a^s \equiv a^t \pmod{m}$  тогда и только тогда, когда  $s \equiv t \pmod{d}$ .

Доказательство. По условию  $O_m(\bar{a}) = d$  и  $a^s \equiv a^t \pmod{m}$ . Покажем, что  $s \equiv t \pmod{d}$ . Предположим, что  $t \leq s$ . Из условий  $(a^t, m) = 1$  и  $a^s \equiv a^t \pmod{m}$  следует  $a^{s-t} \equiv 1 \pmod{m}$ . Так как  $O_m(\bar{a}) = d$ , то согласно теореме 2  $s - t$  делится на  $d$ , т.е.  $s \equiv t \pmod{d}$ .

Пусть теперь  $s \equiv t \pmod{d}$  и  $t \leq s$ . Покажем, что  $a^s \equiv a^t \pmod{m}$ . Так как  $s \equiv t \pmod{d}$ , то существует  $k \in \mathbb{Z}, k \geq 0$ , что  $s = t + k \cdot d$ . Из условия, что  $a^d \equiv 1 \pmod{m}$ , следует  $a^{dq} \equiv 1 \pmod{m}$ . Умножив обе части последнего сравнения на  $a^t$ , получим  $a^{t+dq} \equiv a^t \pmod{m}$ , т.е.  $a^s \equiv a^t \pmod{m}$ .

**ТЕОРЕМА 4.** Если  $O_m(\bar{a}) = n$  и  $k \in \mathbb{Z}, k \geq 0, (k, n) = d$ , то  $O_m(a^k) = \frac{n}{d}$ .

Доказательство. Пусть  $O_m(a^k) = f$  и  $k = k_1 d, n = n_1 d$ . Тогда  $(a^k)^f = a^{kf}, a^{kf} \equiv 1 \pmod{m}$ . Так как  $O_m(a) = n$ , то согласно теореме 2  $(k \cdot f)$  делится на  $n$ . Из условий  $k_1 \cdot f$  делится на  $n_1$  и  $(k_1, n_1) = 1$  следует, что  $f$  делится на  $n_1$ . Так как  $(a^k)^{n_1} = (a^n)^{k_1}$  и  $a^n \equiv 1 \pmod{m}$ , то  $(a^k)^{n_1} \equiv 1 \pmod{m}$ . Из этого сравнения, учитывая, что  $O_m(a^k) = f$ , согласно теореме 2 следует, что  $n_1$  делится на  $f$ . Следовательно,  $f = n_1 = \frac{n}{d}$ .

*Следствие 1.* Если  $(k, n) = 1$  и  $O_m(\bar{a}) = n$ , то  $O_m(a^k) = n$ .

*Следствие 2.* Если  $O_m(\bar{a}) = n$ , то среди классов вычетов  $\bar{a}, \bar{a}^2, \dots, \bar{a}^n$  по модулю  $m$  имеется  $\varphi(n)$  классов, имеющих порядок  $n$ .

## § 14. Первообразные корни и индексы по простому модулю

Пусть  $a \in Z$ ,  $p \in N$  простое число,  $(a, p) = 1$ .

**Определение.** Целое число  $a$  называется первообразным корнем по простому модулю  $p$ , если  $O_p(a) = p - 1$ .

Если  $b \equiv a \pmod{p}$  и  $O_p(a) = p - 1$ , то  $b$  первообразный корень по простому модулю  $p$ . Таким образом, если  $a$  первообразный корень по простому модулю  $p$ , то любое целое число  $b$  из класса вычетов  $\bar{a}$  по модулю  $p$  является первообразным корнем по этому модулю.

**Определение.** Класс вычетов  $\bar{a}$  по простому модулю  $p$  называется первообразным корнем по этому модулю, если  $O_p(\bar{a}) = p - 1$ .

Из теорем 1, 3 § 13 следует, что если целое число  $a$  является первообразным корнем по простому модулю  $p$ , то числа  $a, a^2, a^3, \dots, a^{p-1}$  образуют приведенную систему вычетов по модулю  $p$  и  $a^s \equiv a^t \pmod{p}$  тогда и только тогда, когда  $s \equiv t \pmod{p-1}$ .

**ТЕОРЕМА.** Пусть  $p \in N$  – простое число,  $d$  – натуральный делитель числа  $p - 1$ . Тогда в приведенной системе вычетов по модулю  $p$  содержится  $\varphi(d)$  целых чисел, имеющих порядок  $d$ .

**Доказательство.** Обозначим через  $B$  приведенную систему вычетов по модулю  $p$ , а через  $\psi(d)$  число целых чисел из множества  $B$ , имеющих порядок  $d$ . Допустим, что существует хотя бы одно целое число  $a \in B$ , имеющее порядок  $d$ , т.е.  $\psi(d) > 0$ . Тогда, согласно теореме 1 § 13, числа

$$a, a^2, a^3, \dots, a^d \tag{14.1}$$

попарно не сравнимы по модулю  $p$ . Каждое из целых чисел последовательности (14.1) удовлетворяет сравнению

$$x^d - 1 \equiv 0 \pmod{p}. \tag{14.2}$$

Так как сравнение (14.2) имеет точно  $d$  решений, то любое целое число из приведенной системы вычетов  $B$ , имеющее порядок  $d$  по модулю  $p$ , принадлежит множеству  $M = \{a, a^2, a^3, \dots, a^d\}$ . Число  $a^k$  имеет порядок  $d$  по простому модулю  $p$  тогда и только тогда, когда  $(k, d) = 1$ . Поэтому число чисел в множестве  $M$ , имеющих порядок  $d$  по простому модулю  $p$ , равно  $\varphi(d)$ .

Таким образом, если существует хотя бы одно целое число из приведенной системы вычетов  $B$ , имеющее порядок  $d$  по простому модулю  $p$ , то  $\psi(d) = \varphi(d)$ .

Следовательно,  $\psi(d) \leq \varphi(d)$  для любого натурального делителя  $d$  числа  $p - 1$ .

Покажем, что сумма  $\sum_{d|p-1} \psi(d) = p - 1$ , где  $\psi(d)$  – число целых

чисел в приведенной системе вычетов  $B$  по модулю  $p$ , имеющих порядок  $d$ . Выпишем все натуральные делители числа  $p - 1$ :  $d_1, d_2, \dots, d_s = p - 1$ . В приведенной системе вычетов  $B$  по модулю  $p$  каждое целое число имеет в качестве порядка одно из целых чисел  $d_1, d_2, \dots, d_s$ . Обозначим через  $\psi(d_1)$  число целых чисел из  $B$ , имеющих порядок  $d_1$ , через  $\psi(d_2)$  число целых чисел из  $B$ , имеющих порядок  $d_2$ , ...,  $\psi(d_s)$  число целых чисел из  $B$ , имеющих порядок  $d_s$ . Тогда

$$\psi(d_1) + \psi(d_2) + \dots + \psi(d_s) = p - 1. \quad (14.3)$$

По тождеству Гаусса [3]

$$\varphi(d_1) + \varphi(d_2) + \dots + \varphi(d_s) = p - 1. \quad (14.4)$$

Если из равенства (14.4) вычтем равенство (14.3), то получим

$$(\varphi(d_1) - \psi(d_1)) + (\varphi(d_2) - \psi(d_2)) + \dots + (\varphi(d_s) - \psi(d_s)) = 0. \quad (14.5)$$

Так как  $\psi(d_i) \leq \varphi(d_i)$ ,  $i = \overline{1, s}$ , то из (14.5) следует, что  $\psi(d_i) = \varphi(d_i)$ ,  $i = \overline{1, s}$ .

Показано, что если  $d$  – натуральный делитель числа  $p - 1$ , то в приведенной системе вычетов по модулю  $p$  содержится  $\varphi(d)$  целых чисел, имеющих порядок  $d$ .

*Следствие.* По любому простому модулю  $p$  существует  $\varphi(p - 1)$  классов вычетов первообразных корней по модулю  $p$ .

**Пример 1**

Найдем все первообразные классы вычетов по модулю 17.

**Решение**

Согласно следствию число первообразных классов вычетов равно  $\varphi(16) = 8$ . Так как 3 и 17 взаимно простые числа, то по теореме Эйлера  $3^{\varphi(17)} \equiv 1 \pmod{17}$ , т.е.  $3^{16} \equiv 1 \pmod{17}$ . Выпишем все делите-

ли числа 16: 1, 2, 4, 8, 16. Из условий  $3^1 \not\equiv 1 \pmod{17}$ ,  $3^2 \not\equiv 1 \pmod{17}$ ,  $3^4 \equiv 13 \pmod{17}$ ,  $3^8 \equiv 13^2 \equiv -1 \pmod{17}$ ,  $3^{16} \equiv 1 \pmod{17}$  следует  $O_{17}(3) = 16$ . Значит, 3 – первообразный корень по простому модулю 17. В силу теоремы 1 § 13 целые числа  $3, 3^2, 3^3, \dots, 3^{16}$  образуют приведенную систему вычетов по модулю 17. Согласно следствию 1 теоремы 4 § 13  $O_{17}(3^k) = 16$  тогда и только тогда, когда  $(k, 16) = 1$ . Отсюда следует, что числа  $3, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15}$  из приведенной системы вычетов – первообразные корни по модулю 17. Заменяя эти числа наименьшими натуральными числами, сравнимыми с ними по модулю 17, получим  $3, 10, 5, 11, 14, 7, 12, 6$ . Классы вычетов  $\overline{3}, \overline{5}, \overline{6}, \overline{7}, \overline{10}, \overline{11}, \overline{12}, \overline{14}$  – первообразные корни по модулю 17.

### Индексы. Свойства индексов

Пусть  $a \in Z$  – первообразный корень по простому модулю  $p$ . Тогда последовательность целых чисел

$$a, a^2, a^3, \dots, a^{p-1} \quad (14.6)$$

является приведенной системой вычетов по модулю  $p$ . Любое целое число  $b \in Z$ , взаимно простое с  $p$ , сравнимо только с одним числом из последовательности (14.6).

**Определение.** Неотрицательное целое число  $s$  называется индексом целого числа  $b$  по простому модулю  $p$  и основанию  $a$ , если  $b \equiv a^s \pmod{p}$ .

Индекс числа  $b$  по простому модулю  $p$  и основанию  $a$  обозначается  $ind_a b$ .

Если целое число  $c \equiv b \pmod{p}$  и индекс  $ind_a b = s$ , то индекс  $ind_a c = s$ . Таким образом, если  $ind_a b = s$ , то для любого целого числа  $c \in \overline{b}$  (где  $\overline{b}$  – класс вычетов по простому модулю  $p$ ) индекс  $ind_a c = s$ .

**Определение.** Неотрицательное целое число  $s$  называется индексом классов вычетов  $\overline{b}$  по простому модулю  $p$  и основанию  $\overline{a}$  ( $\overline{a}$  – первообразный корень по простому модулю  $p$ ), если  $\overline{b} = \overline{a}^s$ .

### Свойства индексов

Пусть  $g$  – первообразный корень по простому модулю  $p$ .

1. Если  $ind_g b = v$ , то неотрицательное число  $v'$  является индексом целого числа  $b$  по основанию  $g$  тогда и только тогда, когда  $v \equiv v' \pmod{p-1}$ .

$$2. a \equiv b \pmod{p} \Leftrightarrow \text{ind}_g a \equiv \text{ind}_g b \pmod{p-1}.$$

3. Пусть  $a, b \in Z$ ,  $(a, p) = 1$ ,  $(b, p) = 1$ . Тогда

$$\text{ind}_g ab \equiv \text{ind}_g a + \text{ind}_g b \pmod{p-1}.$$

$$4. \text{ind}_g b^n \equiv n \cdot \text{ind}_g b \pmod{p-1}.$$

5. Пусть  $a, b \in Z$ ,  $(a, p) = 1$ ,  $(b, p) = 1$ ,  $b = ma$ . Тогда

$$\text{ind}_g \frac{b}{a} \equiv \text{ind}_g b - \text{ind}_g a \pmod{p-1}.$$

6. Пусть  $g, q$  – первообразные корни по простому модулю  $p$ ,  $b \in Z$ ,  $(b, p) = 1$ . Тогда  $\text{ind}_g b \equiv \text{ind}_q b \cdot \text{ind}_g q \pmod{p-1}$ .

### Пример 2

Покажем, что число 2 является первообразным корнем по простому модулю 13, и найдем индексы чисел 1, 2, ..., 12 по модулю 13 и основанию 2.

#### Решение

Так как 2 и 13 взаимно простые числа, то по теореме Эйлера  $2^{\varphi(13)} \equiv 1 \pmod{13}$ , т.е.  $2^{12} \equiv 1 \pmod{13}$ . Выпишем все натуральные делители числа 12: 1, 2, 3, 4, 6, 12. Из условий, что  $2^1 \not\equiv 1 \pmod{13}$ ,  $2^2 \not\equiv 1 \pmod{13}$ ,  $2^3 \not\equiv 1 \pmod{13}$ ,  $2^4 \not\equiv 1 \pmod{13}$ ,  $2^6 \not\equiv 1 \pmod{13}$ ,  $2^{12} \equiv 1 \pmod{13}$ , следует  $O_{13}(2) = 12$ . Значит, 2 – первообразный корень по простому модулю 13.

Так как  $2^0 \equiv 1 \pmod{13}$ ,  $2^1 \equiv 2 \pmod{13}$ ,  $2^2 \equiv 4 \pmod{13}$ ,  $2^3 \equiv 8 \pmod{13}$ ,  $2^4 \equiv 3 \pmod{13}$ ,  $2^5 \equiv 6 \pmod{13}$ ,  $2^6 \equiv 12 \pmod{13}$ ,  $2^7 \equiv 11 \pmod{13}$ ,  $2^8 \equiv 9 \pmod{13}$ ,  $2^9 \equiv 5 \pmod{13}$ ,  $2^{10} \equiv 10 \pmod{13}$ ,  $2^{11} \equiv 7 \pmod{13}$ ,  $2^{12} \equiv 1 \pmod{13}$ , то индексы чисел 1, 2, ..., 12 таковы:

$a$	1	2	3	4	5	6	7	8	9	10	11	12
$\text{inda}$	0	1	4	2	9	5	11	3	8	10	7	6

### Пример 3

Найдем теперь индексы чисел 323 и 426 по модулю 13, используя построенную таблицу.

## Решение

Для нахождения индекса числа 323 заменим его сравнимым с ним наименьшим неотрицательным вычетом по модулю 13. Имеем:  $323 \equiv 11 \pmod{13}$ ; тогда  $\text{ind } 323 = \text{ind } 11 = 7$ . Так как  $423 \equiv 7 \pmod{13}$ , то  $\text{ind } 423 = \text{ind } 7 = 11$ .

## Применение индексов

### 1. Решение сравнений первой степени.

#### Пример 4

Решить сравнение  $6x \equiv 7 \pmod{13}$ .

#### Решение

Так как  $(6, 13) = 1$ , то сравнение имеет единственное решение.  $6x \equiv 7 \pmod{13} \Leftrightarrow \text{ind } 6 + \text{ind } x \equiv \text{ind } 7 \pmod{12}$ . Тогда  $\text{ind } x \equiv \text{ind } 7 - \text{ind } 6 \pmod{12}$ . Учитывая, что  $\text{ind } 7 = 11$ , а  $\text{ind } 6 = 5$ , получим  $\text{ind } x \equiv 6 \pmod{12}$ . Следовательно,  $x \equiv 12 \pmod{13}$  – решение сравнения.

**2. Решение двучленных сравнений  $n$ -й степени.** Сравнение вида  $ax^n \equiv b \pmod{m}$ , где  $a \not\equiv 0 \pmod{m}$ , называется двучленным сравнением  $n$ -й степени с одной неизвестной.

Ограничимся рассмотрением двучленных сравнений по простому модулю  $p$ , т.е. сравнений вида

$$ax^n \equiv b \pmod{p}, (a, p) = 1. \quad (14.7)$$

$ax^n \equiv b \pmod{p} \Leftrightarrow \text{ind } a + n \cdot \text{ind } x \equiv \text{ind } b \pmod{p-1}$ . Введем обозначение:  $\text{ind } x = y$ . Тогда предыдущее сравнение запишется в виде

$$ny = \text{ind } b - \text{ind } a \pmod{p-1} \quad (14.8)$$

Пусть  $d = (n, p-1)$ .

Если  $d = 1$ , то сравнение (14.8) имеет единственное решение.

Если  $d > 1$  и  $(\text{ind } b - \text{ind } a)$  не делится на  $d$ , то сравнение не имеет решений.

Если  $d > 1$  и  $(\text{ind } b - \text{ind } a)$  делится на  $d$ , то сравнение (14.8) имеет  $d$  решений.

#### Пример 5

Решить сравнение  $6x^8 \equiv 7 \pmod{13}$ .

#### Решение

$6x^8 \equiv 7 \pmod{13} \Leftrightarrow \text{ind } 6 + 8 \cdot \text{ind } x \equiv \text{ind } 7 \pmod{12}$ . Введем обозначение:  $\text{ind } x = y$ . Тогда предыдущее сравнение запишется в виде

$8y \equiv \text{ind } 5 - \text{ind } 6 \pmod{12}$ . Учитывая, что  $\text{ind } 5 = 9$ , а  $\text{ind } 6 = 5$ , получим  $8y \equiv 4 \pmod{12}$ . Сравнение  $8y \equiv 4 \pmod{12}$  имеет четыре решения. Разделив обе части сравнения и модуль на 4, получим сравнение  $2y \equiv 1 \pmod{3}$ , имеющее единственное решение  $y \equiv 2 \pmod{3}$ . Тогда классы целых чисел  $y \equiv 2 \pmod{12}$ ,  $y \equiv 5 \pmod{12}$ ,  $y \equiv 8 \pmod{12}$ ,  $y \equiv 11 \pmod{12}$  – решения сравнения  $8y \equiv 4 \pmod{12}$ . Так как  $\text{ind } x \equiv 2 \pmod{12} \Leftrightarrow x \equiv 4 \pmod{13}$ ,  $\text{ind } x \equiv 5 \pmod{12} \Leftrightarrow x \equiv 6 \pmod{13}$ ,  $\text{ind } x \equiv 8 \pmod{12} \Leftrightarrow x \equiv 9 \pmod{13}$ ,  $\text{ind } x \equiv 11 \pmod{12} \Leftrightarrow x \equiv 7 \pmod{13}$ , то классы целых чисел  $x \equiv 4 \pmod{13}$ ,  $x \equiv 6 \pmod{13}$ ,  $x \equiv 9 \pmod{13}$ ,  $x \equiv 7 \pmod{13}$  – решения сравнения.

### Упражнения

1. Найдите порядок числа 2 по модулю 29.
2. Найдите порядок числа 2 по простому модулю 11.
3. Найдите порядок класса вычетов  $\bar{7}$  по модулю 43, а также все классы вычетов по модулю 43, имеющие такой же порядок.
4. Найдите все классы первообразных корней по модулю 11.
5. Найдите число классов и сами классы первообразных корней по модулю 7.
6. Решите сравнения с помощью индексов:
 

а) $13x^{21} \equiv 5 \pmod{31}$ ;	б) $40x^{10} \equiv 3 \pmod{17}$ ;
в) $3x^8 \equiv 5 \pmod{13}$ ;	г) $17 \cdot 13^{3x} + 27 \equiv 0 \pmod{29}$ ;
д) $12^{7x} \equiv 15 \pmod{31}$ ;	е) $15 \cdot x^9 + 29 \equiv 0 \pmod{47}$ ;
ж) $7x^{13} \equiv 24 \pmod{47}$ ;	з) $25x^7 \equiv -7 \pmod{41}$ ;
и) $25^{5x} \equiv 47 \pmod{61}$ ;	к) $13 \cdot 7^{5x} + 1 \equiv 0 \pmod{67}$ .
7. При помощи индексов найдите показатель, которому принадлежит 6 по модулю 23.
8. При помощи индексов покажите, что 2 есть первообразный корень по модулю 37.
9. При каких целых значениях  $a$   $(3a^2 - 5) \div 7$ ?

## § 15. Арифметические приложения теории сравнений

**1. Нахождение остатков при делении на данное число.** Пусть  $r_1, r_2, \dots, r_n$  остатки от деления чисел  $a_1, a_1, \dots, a_n$  на  $m$ . Тогда

$$\begin{cases} a_1 \equiv r_1 \pmod{m} \\ a_2 \equiv r_2 \pmod{m} \\ \dots\dots\dots \\ a_n \equiv r_n \pmod{m} \end{cases} \quad (15.1)$$

А. Сложив сравнения (15.1), получим:

$$a_1 + a_1 + \dots + a_n \equiv r_1 + r_2 + \dots + r_n \pmod{m}. \quad (15.2)$$

Из (15.2) следует, что числа  $a_1 + a_1 + \dots + a_n, r_1 + r_2 + \dots + r_n$  имеют одинаковые остатки при делении на  $m$ . Если  $r_1 + r_2 + \dots + r_n < m$ , то число  $r_1 + r_2 + \dots + r_n$  будет искомым остатком.

Б. Умножив сравнения (15.1), получим сравнение

$$a_1 \cdot a_2 \cdot \dots \cdot a_n \equiv r_1 \cdot r_2 \cdot \dots \cdot r_n \pmod{m}. \quad (15.3)$$

Из (15.3) следует, что нахождение остатка от деления числа  $a_1 \cdot a_2 \cdot \dots \cdot a_n$  на  $m$  можно заменить нахождением остатка от деления числа  $r_1 \cdot r_2 \cdot \dots \cdot r_n$  на  $m$ .

В. Если в сравнении (15.3)  $a_1 = a_2 = \dots = a_n = a$ , то получим сравнение

$$a^n \equiv r^n \pmod{m}.$$

Рассмотрим некоторые возможные приемы нахождения остатка от деления  $r^n$  на  $m$ .

1. Последовательное возведение в степень сравнения  $r \equiv r \pmod{m}$  с последовательной заменой правой части получающегося сравнения абсолютно наименьшими вычетами по модулю  $m$ .

2. Если  $(r, m) = 1$ , то можно воспользоваться теоремой Эйлера. По теореме Эйлера  $r^{\varphi(m)} \equiv 1 \pmod{m}$ . Разделим теперь  $n$  на  $\varphi(m)$ :  $n = \varphi(m)q + k$ . Тогда получим

$$r^n = r^{\varphi(m)q+k} = r^{\varphi(m)q} \cdot r^k \equiv r^k \pmod{m}.$$

Из этого сравнения следует, что задача отыскания остатка от деления числа  $r^n$  на  $m$  сводится к задаче нахождения остатка от деления числа  $r^k$  на  $m$ , где  $k < \varphi(m)$ .

### Пример 1

Найти наименьший неотрицательный остаток от деления числа  $(6459 + 5387 - 1254) \cdot 2934$  на 33.

### Решение

Найдем остатки от деления чисел  $6459 + 5387 - 1254 = 10592$ , 2934 на 33:  $10592 = 33 \cdot 320 + 32$ ,  $2934 = 33 \cdot 88 + 30$ . Так как остатком от деления числа  $32 \cdot 30 = 960$  на 33 является число 3, то искомым остаток  $r = 3$ .

### Пример 2

Найти остаток от деления числа  $a = 15^{125}$  на 12.

### Решение

Пусть  $r$  остаток от деления числа  $a$  на 12,  $a = 12g + r$ ,  $0 \leq r < 12$ . Тогда  $r \equiv 15^{125} \pmod{12}$ .  $(r - 15^{125}) : 12 \wedge (12, 15) = 3 \Rightarrow r : 3$ . Пусть  $r = 3r_1$ ,  $r_1 \in \mathbb{N}$ . Тогда из сравнения  $3r_1 \equiv 15 \cdot 5^{124} \pmod{12}$  следует, что  $r_1 \equiv 5 \cdot 5^{124} \pmod{4}$ . Так как  $(15, 4) = 1$ , то по теореме Эйлера  $15^{\varphi(4)} \equiv 1 \pmod{4}$ ,  $15^2 \equiv 1 \pmod{4}$ .  $15^2 \equiv 1 \pmod{4} \Rightarrow 15^{124} \equiv 1 \pmod{4}$ .  $15^{124} \equiv 1 \pmod{4} \wedge 5 \equiv 1 \pmod{4} \Rightarrow 5 \cdot 15^{124} \equiv 1 \pmod{4}$ . Из условий  $r_1 \equiv 5 \cdot 15^{124} \pmod{4}$ ,  $5 \cdot 15^{124} \equiv 1 \pmod{4}$ ,  $0 \leq r_1 < 4$  следует, что  $r_1 = 1$ . Так как  $r = 3r_1$ , то  $r = 3$ .

**2. Признаки делимости.** Критерий, устанавливающий необходимое и достаточное условие делимости произвольного натурального числа  $n$  на данное натуральное число  $m$ , называется признаком делимости на  $m$ .

Французский математик Блез Паскаль (1623–1662) нашел общий признак делимости, который в терминах сравнений может быть сформулирован следующим образом.

**Теорема (общий признак делимости Паскаля).** Для того, чтобы число  $n$ , записанное в произвольной  $g$ -ичной системе счисления в виде

$$n = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0,$$

делилось на число  $m$ , необходимо и достаточно, чтобы число  $q = a_n r_n + a_{n-1} r_{n-1} + \dots + a_1 r_1 + a_0$  делилось на  $m$  (здесь  $a_i$  – цифры числа  $n$ , а  $r_i$  – абсолютно наименьшие вычеты соответствующих степеней  $g^i$  по модулю  $m$ ,  $i = \overline{1, n}$ ).

В качестве следствий из общего признака Паскаля вытекают различные частные признаки делимости. Приведем некоторые из них, наиболее часто используемые.

*Следствие 1.* Пусть  $m$  – делитель числа  $g - 1$ . Для того, чтобы число, записанное в  $g$ -ичной системе счисления, делилось на  $m$ , необходимо и достаточно, чтобы сумма его цифр делилась на  $m$ .

**З а м е ч а н и е.** Для чисел, записанных в десятичной системе счисления, из сформулированного признака вытекают известные признаки делимости на 9 и на 3.

*Следствие 2.* Пусть  $m$  – делитель числа  $g + 1$ . Для того, чтобы число, записанное в  $g$ -ичной системе счисления, делилось на  $m$ , необходимо и достаточно, чтобы разность между суммами цифр на четных и нечетных местах делилась на  $m$ .

**З а м е ч а н и е.** Для чисел, записанных в десятичной системе счисления, получается известный признак делимости на 11: для того, чтобы число делилось на 11, необходимо и достаточно, чтобы разность между суммами цифр на четных и нечетных местах делилась на 11.

*Следствие 3.* Пусть  $m$  – делитель числа  $g^k$ . Для того, чтобы число, записанное в  $g$ -ичной системе счисления, делилось на  $m$ , необходимо и достаточно, чтобы число, записанное последними  $k$  цифрами данного числа, делилось на  $m$ .

**3. Проверка результатов арифметических действий.** Результат действия сложения, вычитания и умножения целых чисел есть целое число. Поэтому, если вместо данных чисел взять наименьшие положительные или наименьшие абсолютные вычеты по какому-либо модулю, то результат действий над этими вычетами будет сравним по тому же модулю с наименьшим вычетом проверяемого результата. Если сравнение не имеет места, то в результате действий над данными целыми числами была допущена ошибка. В качестве модуля удобно брать число, по которому наименьшие вычеты легко вычисляются (например, в десятичной системе счисления – 9 или 10). Правильность соответствующего сравнения лишь подтверждает, но не гарантирует правильность результата.

### Пример 3

Проверим правильность выполнения действия с помощью 9 и 11:

$$54319363 - 32897891 = 21421472.$$

А. Модуль  $m = 9$ .

$$54319363 \equiv 34 \pmod{9}, 32897891 \equiv 47 \pmod{9}, 21421472 \equiv 23 \pmod{9},$$

$$34 - 47 = -13, -13 \equiv 23 \pmod{9}.$$

Сравнение  $-13 \equiv 23 \pmod{9}$  подтверждает правильность результата, но не гарантирует.

Б. Модуль  $m = 11$ .

$$(3 + 3 + 1 + 4) - (5 + 3 + 9 + 6) = -12, (1 + 8 + 9 + 2) - (3 + 8 + 7 + 9) = -7,$$

$$(2 + 4 + 2 + 1) - (2 + 4 + 1 + 7) = -5, -12 - (-7) = -5.$$

Сравнение  $-5 \equiv -5 \pmod{11}$  подтверждает также правильность полученного результата.

### Пример 4

Проверим правильность выполнения действия

$$542678 \cdot 65328 = 35452068382$$

с помощью модуля 9.

$$542678 \equiv 32 \pmod{9}, 65328 \equiv 24 \pmod{9},$$

$$35452068382 \equiv 46 \pmod{9}, 32 \cdot 24 \not\equiv 46 \pmod{9}.$$

Так как сравнение  $32 \cdot 24 \not\equiv 46 \pmod{9}$  неверно, то действие выполнено неправильно.

## Упражнения

1. Найдите остаток от деления:

- |                             |                               |                              |
|-----------------------------|-------------------------------|------------------------------|
| а) $66^{17}$ на 7;          | б) $11^{802}$ на 1000;        | в) $19^{2402}$ на 100;       |
| г) $1967^{2014}$ на 11;     | д) $5^{80} + 7^{100}$ на 13;  | е) $2^{100} + 3^{100}$ на 5; |
| ж) $5^{70} + 7^{50}$ на 12; | з) $5^{50} + 13^{100}$ на 18; | и) $12^{2751}$ на 10;        |
| к) $178^{2741}$ на 22.      |                               |                              |

2. При помощи свойств сравнений выведите признаки делимости на следующие числа:

- |               |               |               |
|---------------|---------------|---------------|
| а) $m = 11$ ; | б) $m = 3$ ;  | в) $m = 9$ ;  |
| г) $m = 4$ ;  | д) $m = 6$ ;  | е) $m = 8$ ;  |
| ж) $m = 12$ ; | з) $m = 15$ ; | и) $m = 18$ . |

3. Проверьте результаты действий с помощью чисел 9, 11:

- a)*  $25045 \cdot 1487 = 37240915$ ;      *б)*  $13547 - 9862 = 3685$ ;  
*в)*  $8264 \cdot 5201 = 42981064$ ;      *г)*  $25041 + 91382 = 116423$ ;  
*д)*  $3745 \cdot 8067 = 30210915$ ;      *е)*  $24667 + 18265 = 42932$ ;  
*ж)*  $141811 + 17128 = 158939$ ;      *з)*  $37918 - 13207 = 24711$ ;  
*и)*  $42932 - 18265 = 24667$ ;      *к)*  $4371 \cdot 1243 = 5433153$ ;  
*л)*  $4237 \cdot 27925 = 118275855$ .

## § 16. Алгебраические и трансцендентные числа. Теорема Лиувилля и ее приложения

**Определение.** Комплексное число  $\alpha$  называется алгебраическим числом, если оно является корнем некоторого многочлена  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  с рациональными коэффициентами.

**Пример 1**

Числа  $\sqrt[3]{3}$ ,  $1 + \frac{\sqrt{3}}{2}$ ,  $2 + \sqrt{3}i$  – алгебраические числа.

**Определение.** Многочлен  $g(x)$  с рациональными коэффициентами наименьшей степени, корнем которого является число  $\alpha$ , называется минимальным многочленом алгебраического числа  $\alpha$ .

**ТЕОРЕМА 1.** Если  $g(x)$  минимальный многочлен алгебраического числа  $\alpha$  и  $f(x)$  такой многочлен с рациональными коэффициентами, что  $f(\alpha) = 0$ , то  $f(x)$  делится на  $g(x)$ .

Доказательство. Разделим  $f(x)$  на  $g(x)$  с остатком:

$$f(x) = g(x)q(x) + r(x), \quad (16.1)$$

где либо  $r(x) = 0$ , либо степень многочлена  $r(x)$  меньше степени многочлена  $g(x)$ . Предположим, что  $r(x) \neq 0$ . Если в равенство (16.1) вместо  $x$  подставим  $\alpha$  и учтем, что  $f(\alpha) = 0$ ,  $g(\alpha) = 0$ , то получим  $r(\alpha) = 0$ . Отсюда следует, что  $\alpha$  является корнем многочлена  $r(x)$  с рациональными коэффициентами, степень которого меньше степени  $g(x)$ .

**ТЕОРЕМА 2.** Минимальный многочлен  $g(x)$  алгебраического числа  $\alpha$  является неприводимым многочленом над полем рациональных чисел.

Доказательство. Предположим, что  $g(x)$  является приводимым многочленом над полем рациональных чисел, т.е.  $g(x) = \varphi(x) \cdot \psi(x)$ , где  $\varphi(x)$ ,  $\psi(x)$  – многочлены с рациональными коэффициентами, степени которых меньше степени многочлена  $g(x)$ . Из равенства  $0 = \varphi(\alpha) \cdot \psi(\alpha)$  следует, что либо  $\varphi(\alpha) = 0$ , либо  $\psi(\alpha) = 0$ . Пусть, например,  $\varphi(\alpha) = 0$ , тогда  $\alpha$  – корень многочлена  $\varphi(x)$  с рациональными коэффициентами, степень которого меньше степени многочлена  $g(x)$ . Пришли к противоречию.

ТЕОРЕМА 3. Множество всех алгебраических чисел относительно операции сложения и операции умножения является полем.

ТЕОРЕМА 4 (теорема Лиувилля). Для любого действительного числа  $\alpha$  степени  $n$  можно подобрать положительное число  $c$ , зависящее только от  $\alpha$ , такое, что для всех рациональных чисел  $\frac{a}{b} \neq \alpha$  будет иметь место равенство

$$\left| \alpha - \frac{a}{b} \right| \geq \frac{c}{b^n}.$$

Из теоремы 4 следует утверждение.

ТЕОРЕМА 5. Пусть  $\alpha$  – действительное число. Если для любого натурального  $n$  и любого действительного числа  $c$  существует хотя бы одна рациональная дробь  $\frac{a}{b}$ ,  $\frac{a}{b} \neq \alpha$ , такая, что

$$\left| \alpha - \frac{a}{b} \right| < \frac{c}{b^n},$$

то число  $\alpha$  трансцендентное.

Пример 2

$$\alpha = \frac{1}{10^1!} + \frac{1}{10^2!} + \frac{1}{10^3!} + \dots - \text{трансцендентное число.}$$

Доказательство. Возьмем произвольные действительные числа  $n \geq 1$  и  $c > 0$ . Возьмем числа  $a = 10^{k!} \left( \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \dots + \frac{1}{10^{k!}} \right)$ ,  $b = 10^{k!}$ , где  $k$  выбрано настолько большим, что  $10^{k!} \geq \frac{2}{c}$  и  $k \geq n$ . Тогда

$$\left| \alpha - \frac{a}{b} \right| = \frac{1}{10^{(k+1)!}} + \frac{1}{10^{(k+2)!}} + \dots < \frac{1}{10^{(k+1)!}} \left( 1 + \frac{1}{2} + \frac{1}{2^2} + \dots \right) = \frac{2}{10^{k!}} \cdot \frac{1}{10^{k! \cdot k}} \leq \frac{c}{b^n}.$$

Так как для произвольных  $c > 0$  и  $n \geq 1$  можно найти дробь  $\frac{a}{b}$  такую, что  $\left| \alpha - \frac{a}{b} \right| < \frac{c}{b^n}$ , то  $\alpha$  – трансцендентное число.

Теорема Лиувилля дает возможность строить трансцендентные числа определенной природы, но является недостаточной для доказа-

тельности трансцендентности числа  $e$ . Трансцендентность числа  $e$  была доказана в 1873 г. Ш. Эрмитом.

### Упражнения

1. Докажите, что следующие числа являются алгебраическими:

а)  $\sqrt[4]{4 - \sqrt[3]{2}}$ ;                      б)  $\sqrt{2} + \sqrt[3]{3}$ ;                      в)  $a + \sqrt[n]{b}$ ;  
г)  $a + i\sqrt{b}$  ( $a, b \in \mathbb{Q}$ );                      д)  $\sin 10^\circ$ ;                      е)  $\cos 20^\circ$ .

2. Докажите, что всякое число, получающееся из рациональных чисел при помощи действий сложения, вычитания, умножения, деления и извлечения корня, будет алгебраическим.

3. Укажите степень алгебраических чисел:

а)  $a + bi$  ( $a, b \in \mathbb{Q}$ );                      б)  $\sqrt[3]{3}$ ;  
в)  $\sqrt[3]{2} - 1$ ;                      г)  $\sqrt{2} - \sqrt{3}$ .

4. Докажите, что корни уравнений  $x^3 + 2\sqrt{2}x^2 + 2 = 0$  и  $x^2 + 2ix + 10 = 0$  являются алгебраическими числами.

5. Докажите, что корни уравнения  $x^5 - 3x^2 + 12x - 6 = 0$  есть алгебраические числа пятого порядка.

6. Докажите, что число  $\alpha = \frac{1}{10^{11}} + \frac{1}{10^{21}} + \frac{1}{10^{31}} + \dots$  является трансцендентным.

7. Определите степень числа  $-\frac{\sqrt[3]{2}}{2} + i\frac{\sqrt{3}}{\sqrt[3]{4}}$  относительно поля  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ .

## Задания для индивидуальной работы

1. Найдите остаток от деления числа  $a$  на указанное число:

а)  $a = 8n - 3$  на 4;

б)  $a = 15n - 5$  на 5;

в)  $a = 6n - 1$  на 3;

г)  $a = 12n - 5$  на 6.

2. Представьте НОД ( $a, b$ ) в виде линейной комбинации этих целых чисел:

а)  $a = 628, b = -1024$ ;

б)  $a = 468, b = -11280$ ;

в)  $a = 336, b = -1308$ ;

г)  $a = 468, b = -1470$ .

3. Найдите все натуральные  $n$ , для которых дробь  $\frac{3n^3 - 8n^2 + 14n - 8}{3n - 5}$  сократима.

4. Решите систему уравнений в натуральных числах:

а) 
$$\begin{cases} x + y = 36, \\ (x, y) = 9; \end{cases}$$

б) 
$$\begin{cases} \frac{x}{y} = \frac{4}{9}, \\ (x, y) = 35; \end{cases}$$

в) 
$$\begin{cases} x \cdot y = 72, \\ (x, y) = 6; \end{cases}$$

г) 
$$\begin{cases} 2x + y = 60, \\ (x, y) = 12. \end{cases}$$

5. Решите систему уравнений в натуральных числах:

а) 
$$\begin{cases} 6x - 7y = 21, \\ [x, y] - 3y = 60; \end{cases}$$

б) 
$$\begin{cases} 4x - 3y = 22, \\ [x, y] + 5y = 182; \end{cases}$$

в) 
$$\begin{cases} 7x - 5y = 128, \\ [x, y] - 8y = 108; \end{cases}$$

г) 
$$\begin{cases} 8x - 9y = 10, \\ [x, y] + 6y = 418. \end{cases}$$

6. Найдите все целые значения  $n$ , для каждого из которых числа  $a, b, c$  являются простыми:

а)  $a = n, b = n + 8, c = n + 16$ ;

б)  $a = n, b = n + 14, c = n + 28$ ;

в)  $a = n, b = n - 2, c = n + 14$ ;

г)  $a = n, b = n - 8, c = n + 20$ .

7. Найдите простое число  $p$  такое, что натуральные числа  $3n + 2$  и  $8n + 3$  делятся на  $p$ .

8. Произведение нескольких различных простых чисел делится на каждое из этих чисел, уменьшенное на 1. Чему может быть равно это произведение?

9. Пусть  $p$  – простое число. Докажите, что  $8p^2 + 1$  является простым числом лишь при  $p = 3$ .

10. Найдите наибольший общий делитель всех чисел вида  $p^2 - 1$ , где  $p$  – простое число, большее 3, но меньшее 2010.

11. Найдите число и сумму натуральных делителей данного числа:

а) 624;      б) 728;      в) 420;      г) 672.

12. Найдите натуральное число, которое делится на 2 и на 6 и имеет 15 натуральных делителей.

13. Некоторое число имеет всего два простых делителя. Его квадрат имеет всего 81 делитель. Сколько делителей имеет куб этого числа?

14. Найдите натуральное число, имеющее 6 натуральных делителей, сумма которых равна 171.

15. Найдите натуральное число, имеющее 9 натуральных делителей, сумма которых равна 403.

16. С каким показателем входит число 3 в каноническое разложение числа  $71!$ ?

17. Сколькими нулями заканчивается число  $1273!$ ?

18. Запишите каноническое разложение данного числа:

а)  $45!$ ;      б)  $62!$ ;      в)  $87!$ ;      г)  $95!$ .

19. Постройте график функции:

а)  $y = [x]$ ;      б)  $y = \left[-\frac{x}{2}\right]$ ;      в)  $y = \left[\frac{x^2}{2} - 1\right]$ ;      г)  $y = [\cos x]$ .

20. Решите уравнение:

а)  $\left[\frac{8x+19}{7}\right] = \frac{16(x+1)}{11}$ ;      б)  $\left[\frac{2x-1}{3}\right] = \left[\frac{x+1}{2}\right]$ ;

в)  $[x^2] = 2$ ;      г)  $[3x^2 - x] = x + 1$ .

21. Покажите, что решением уравнения

$$[x] + \left[ x + \frac{1}{100} \right] + \left[ x + \frac{2}{100} \right] + \dots + \left[ x + \frac{99}{100} \right] = [100x]$$

является любое действительное число.

22. Разложите число в цепную дробь:

$$a) \frac{91}{23}; \quad б) -\frac{627}{43}; \quad в) \frac{734}{15}; \quad г) -\frac{638}{49}.$$

23. Решите уравнение:

$$a) [x; 5, 2, 3] = \frac{45}{38}; \quad б) [2; x, 3, 4] = \frac{73}{30};$$
$$в) [3; 2, x, 6] = \frac{109}{32}; \quad г) [-2; 3, 5, x] = -\frac{59}{35}.$$

24. При помощи разложения в цепную дробь сократите данную рациональную дробь:

$$a) \frac{13464}{12672}; \quad б) \frac{11232}{4896}; \quad в) \frac{8712}{1692}; \quad г) \frac{2499}{4998}.$$

25. Решите уравнение в целых числах:

$$a) 3x + 17y = 5; \quad б) 15x + 19y = 2;$$
$$в) 21x - 13y = 8; \quad г) 25x - 16y = 3.$$

26. Докажите, что  $(a + b)^p \equiv a^p + b^p \pmod{p}$ , где  $p$  – простое число.

27. Найдите две последние цифры числа:

$$a) 9^{9^9}; \quad б) 7^{9^{9^9}}.$$

28. Докажите, что числа  $-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -1, 0, 1, \dots, \frac{p-3}{2}, \frac{p-1}{2}$  попарно не сравнимы по модулю  $p$ , где  $p$  – простое число.

29. Докажите, что  $\varphi(m^n) = m^{n-1}\varphi(m)$ , где  $m, n \in \mathbb{N}$  ( $\varphi$  – функция Эйлера).

30. Докажите справедливость равенств:

$$a) \varphi(4n + 2) = \varphi(2n + 1); \quad б) \varphi(4n) = \begin{cases} 2\varphi(n) & \text{при } (n, 2) = 1, \\ 2\varphi(2n) & \text{при } (n, 2) = 2. \end{cases}$$

**31.** Решите уравнения:

а)  $\varphi(11^x) = 1210$ ;

б)  $\varphi(7^x) = 2058$ ;

в)  $\varphi(p^x) = p^{x-1}$ ;

г)  $\varphi(5^x \cdot 7^y) = 4200$ .

**32.** Решите уравнения:

а)  $\varphi(x) = \frac{x}{2}$ ;

б)  $\varphi(x) = \frac{x}{3}$ ;

в)  $\varphi(x) = \frac{x}{4}$ .

**33.** Найдите остаток от деления числа:

а)  $24^{103}$  на 15;

б)  $35^{242}$  на 18;

в)  $44^{133}$  на 46;

г)  $178^{52}$  на 11;

д)  $5^{88} + 7^{109}$  на 13;

е)  $5^{50} + 13^{10}$  на 18;

ж)  $(11^{57} + 13^{82})^{100}$  на 15; з)  $(12^{50} + 11^{20})^{80}$  на 7.

**34.** Решите сравнения:

а)  $39x \equiv 19 \pmod{53}$ ;

б)  $12x \equiv 15 \pmod{35}$ ;

в)  $64x \equiv 21 \pmod{13}$ ;

г)  $29x \equiv 35 \pmod{123}$ ;

д)  $37x \equiv 16 \pmod{11}$ ;

е)  $15x \equiv 21 \pmod{6}$ .

**35.** Решите сравнения с помощью цепных дробей:

а)  $92x \equiv 20 \pmod{284}$ ;

б)  $14x \equiv 50 \pmod{62}$ ;

в)  $25x \equiv 7 \pmod{31}$ ;

г)  $91x \equiv 1 \pmod{132}$ ;

д)  $14x \equiv 50 \pmod{62}$ ;

е)  $13x \equiv 178 \pmod{153}$ .

**36.** Решите системы сравнений:

а) 
$$\begin{cases} 5x \equiv 2 \pmod{12}, \\ 7x \equiv 2 \pmod{8}, \\ 3x \equiv 1 \pmod{5}; \end{cases}$$

б) 
$$\begin{cases} 7x \equiv 4 \pmod{15}, \\ 3x \equiv 23 \pmod{28}, \\ 5x \equiv 8 \pmod{11}; \end{cases}$$

в) 
$$\begin{cases} 3x \equiv 5 \pmod{12}, \\ 7x \equiv 3 \pmod{25}, \\ 3x \equiv 2 \pmod{17}; \end{cases}$$

г) 
$$\begin{cases} 3x \equiv 5 \pmod{14}, \\ 5x \equiv 1 \pmod{9}, \\ 7x \equiv 2 \pmod{25}. \end{cases}$$

**37.** Решите сравнения с помощью индексов:

а)  $17x^5 + 3 \equiv 0 \pmod{37}$ ;

б)  $10x^9 + 7 \equiv 0 \pmod{13}$ ;

в)  $19^{7x} \equiv 15 \pmod{59}$ ;

г)  $11 \cdot 5^{3x} \equiv -70 \pmod{13}$ ;

д)  $13^x \equiv 25 \pmod{43}$ ;

е)  $x^{17} \equiv 31 \pmod{67}$ .

## Список литературы

1. Александров, В. А. Задачник-практикум по теории чисел / В. А. Александров, С. М. Горшенин. – М. : Просвещение, 1972.
2. Алгебра и теория чисел / под ред. Н. Я. Виленкина. – М. : Просвещение, 1972. – Ч. III.
3. Бухштаб, А. А. Теория чисел / А. А. Бухштаб. – М. : Просвещение, 1966.
4. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – М.–Л. : ГИТТЛ, 1952.
5. Грибанов, Б. У. Сборник упражнений по теории чисел / Б. У. Грибанов, П. И. Титов. – М. : Просвещение, 1964. – 144 с.
6. Деза, Л. Сборник задач по теории чисел / Л. Деза, Л. Котова. – М. : Лирком, 2012.
7. Завало, С. Т. Алгебра и теория чисел / С. Т. Завало, В. Н. Костарчук, Б. И. Хацет. – Киев : Вища шк., 1980. – Ч. 2.
8. Кочева, А. А. Задачник-практикум по алгебре и теории чисел / А. А. Кочева. – М. : Просвещение, 1984. – Ч. III.
9. Кудреватов, Г. А. Сборник задач по теории чисел / Г. А. Кудреватов. – М. : Просвещение, 1979.
10. Куликов, Л. Я. Алгебра и теория чисел / Л. Я. Куликов. – М. : Высш. шк., 1979.
11. Михелович, Ш. Х. Теория чисел / Ш. Х. Михелович. – М. : Высш. шк., 1962.
12. Практические занятия по алгебре и теории чисел / М. П. Лельчук, И. И. Полевченко, А. М. Радьков, Б. Д. Чеботаревский. – Минск : Выш. шк., 1986. – 302 с.
13. Шнеперман, Л. Б. Курс алгебры и теории чисел в задачах и упражнениях / Л. Б. Шнеперман. – Минск : Выш. шк., 1986. – Ч. 1.
14. Шнеперман, Л. Б. Курс алгебры и теории чисел в задачах и упражнениях / Л. Б. Шнеперман. – Минск : Выш. шк., 1987. – Ч. 2.

## ПРИЛОЖЕНИЕ

### Элементы теории чисел в олимпиадных задачах для школьников

1. Найдите все простые числа, которые являются одновременно суммой двух простых чисел и разностью двух простых чисел (Всероссийская олимпиада по математике, 11-й класс).

Р е ш е н и е

Обозначим искомое простое число через  $p$ . Так как  $p$  – сумма двух простых чисел, то  $p > 2$ , следовательно,  $p$  нечетно. Значит, одно из слагаемых в представлении числа  $p$  в виде суммы двух простых чисел четно, т.е. равно двум. Итак,  $p = q + 2$  и  $p = r - 2$ , где  $q$  и  $r$  – простые числа, следовательно, числа  $p - 2$ ,  $p$  и  $p + 2$  – простые. Из трех последовательных нечетных чисел, по крайней мере, одно делится на 3. Значит, одно из чисел  $p - 2$ ,  $p$ ,  $p + 2$  равно трем. Ясно, что этим числом может быть только число  $p - 2$ . Тогда условию задачи удовлетворяет число  $p = 5$  и только оно.

2. К натуральному числу  $N$  прибавили наибольший его делитель, меньший  $N$ , и получили степень десятки. Найдите все такие  $N$  (Всероссийская олимпиада по математике, 9-й класс; автор – Агаханов Н. Х.).

Р е ш е н и е

Пусть  $m$  – наибольший делитель числа  $N$ , меньший, чем  $N$ . Тогда  $N = mp$ , где  $p$  – наименьший простой делитель числа  $N$ . Имеем  $m(p + 1) = N + m = 10^k$ . Число в правой части не делится на 3, поэтому  $p > 2$ . Отсюда следует, что  $N$  нечетно, а тогда и  $m$  нечетно. Так как  $10^k$  делится на  $m$ , то  $m = 5^s$ . Если  $m = 1$ , то  $N = p = 10^k - 1$ , что невозможно, так как  $10^k - 1$  делится на 9, т.е. не является простым. Значит,  $s \geq 1$ , число  $N$  кратно 5, и потому  $p \leq 5$ . Если  $p = 3$ , то  $4 \cdot 5^s = 10^k$ , откуда  $k = 2$ ,  $m = 25$  и  $N = 75$ . Если же  $p = 5$ , то  $p + 1 = 6$ , и число  $10^k$  делится на 3, что невозможно. Таким образом, условию задачи удовлетворяет только число  $N = 75$ .

3. При каких натуральных  $n$  найдутся такие целые числа  $a$ ,  $b$  и  $c$ , что их сумма равна нулю, а число  $a^n + b^n + c^n$  – простое? (Всероссийская олимпиада по математике, 11-й класс; автор – Сендеров В. А.)

П е р в о е р е ш е н и е

Если  $n$  четно, то  $1^n + (-1)^n + 0^n = 2$  – простое число. Пусть  $x$  – целое, а  $n$  – нечетное. Представив  $x$  в виде  $x = 3t$  или  $x = 3t \pm 1$  для це-

лого  $t$ , в любом случае получим, что  $x^n - x$  делится на 3. Кроме того,  $x^n - x$  четно. Отсюда вытекает, что  $a^n + b^n + c^n = (a^n - a) + (b^n - b) + (c^n - c)$  делится на  $2 \cdot 3$  и, значит, не является простым.

### Второе решение

Докажем другим способом, что при нечетном  $n$  число  $d = a^n + b^n + c^n$  не является простым. Пусть  $d$  – простое число, тогда  $n > 1$  и  $a, b, c$  отличны от 0. Поскольку  $b^n + c^n$  делится на  $b + c = -a$ , то число  $d$  делится на  $a$ . Аналогично,  $d$  делится на  $b$  и на  $c$ . Отсюда следует, что каждое из чисел  $a, b, c$  равно одному из чисел  $\pm 1, \pm d$ . Так как среди чисел  $a, b, c$  нет двух противоположных (иначе третье было бы нулем), то среди них найдутся два равных числа; пусть они равны  $m$ , тогда третье число равно  $-2m$ . Получаем, что  $d = 2m^n - 2^n m^n$  – четное число, делящееся на  $2^n - 2 > 2$ . Противоречие.

Получили, что при всех четных  $n$  найдутся такие целые числа  $a, b$  и  $c$ , что их сумма равна нулю, а число  $a^n + b^n + c^n$  – простое.

**4.** Натуральное число  $n$  таково, что  $3n + 1$  и  $10n + 1$  являются квадратами натуральных чисел. Докажите, что число  $29n + 11$  – составное (Московская математическая олимпиада, 10-й класс).

### Решение

Пусть  $3n + 1 = a^2$ ,  $10n + 1 = b^2$ , где  $a, b \in \mathbb{N}$ , и пусть  $p = 29n + 11$  – простое число. Далее можно рассуждать по-разному.

*Первый способ.* Перемножив указанные равенства, в результате получим  $30n^2 + 13n + 1 = (ab)^2$ . Следовательно,  $29n^2 + 11n = (ab)^2 - (n + 1)^2$ . Отсюда  $np = (ab - n - 1)(ab + n + 1)$ . Хотя бы один из множителей в правой части делится на  $p$  и потому не меньше  $p$ . Значит,  $ab + n + 1 \geq p$ , где  $p = 29n + 11$ . Тогда  $ab \geq 28n + 10$ ,  $(ab)^2 \geq 784n^2 + 560n + 100$ . С другой стороны,  $(ab)^2 = 30n^2 + 13n + 1$ , что противоречит предыдущему. Следовательно, предположение неверно и число  $p = 29n + 11$  является составным.

*Второй способ.*  $(9a + 2b)(9a - 2b) = 81a^2 - 4b^2 = 81(3n + 1) - 4(10n + 1) = 243n + 77 = 7(29n + 11) = 7p$ . Значит,  $9a + 2b \geq p > 29n$ . Так как  $9a - 2b > 0$ , то  $18a > 9a + 2b > 29n$ , откуда  $a > n$ ,  $3n + 1 = a^2 > n^2$ ,  $n < 3$ . Непосредственно можно проверить, что значения  $n = 1$  и  $n = 2$  не подходят.

**5.** Пусть  $p$  – простое число. Набор из  $p + 2$  натуральных чисел (необязательно различных) назовем «интересным», если сумма любых  $p$  из них делится на каждое из двух оставшихся чисел. Найдите

все «интересные» наборы (Турнир городов, 8–9-е классы; автор – Полянский А.).

**Р е ш е н и е**

Пусть  $S$  – сумма всех чисел «интересного» набора,  $c$  – наибольшее число в наборе,  $a$  и  $b$  – еще два каких-то числа из набора. Суммы  $S - a - c$  и  $S - b - c$  делятся на  $c$ , значит, и их разность  $b - a$  кратна  $c$ . Поскольку эта разность по модулю меньше  $c$ , то она равна нулю. Итак, все числа набора, кроме наибольшего числа  $c$ , равны  $a$ .  $S - a - a = (p - 1)a + c$  делится на  $a$ , следовательно,  $c = ka$ .  $S - a - c = pa$  делится на  $c$ , что равносильно делимости  $p$  на  $k$ . Итак,  $k = 1$  или  $k = p$ . Таким образом, все «интересные» наборы имеют вид  $(pt, t, \dots, t)$  и  $(t, t, \dots, t)$ , где  $t$  – натуральное число.

**6.** Для каждого натурального  $n$  обозначим через  $S_n$  сумму первых  $n$  простых чисел:  $S_1 = 2$ ,  $S_2 = 2 + 3 = 5$ ,  $S_3 = 2 + 3 + 5 = 10$ , .... Могут ли два подряд идущих члена последовательности  $(S_n)$  оказаться квадратами натуральных чисел? (Всероссийская олимпиада по математике, 9-й класс; автор – Шарич В.).

**Р е ш е н и е**

Обозначим  $n$ -е простое число через  $p_n$ . Предположим, что нашлось  $m > 1$ , для которого  $S_{m-1} = k^2$ ,  $S_m = l^2$ , где  $k$  и  $l$  – натуральные числа. Числа  $S_2 = 5$ ,  $S_3 = 10$  квадратами не являются, так что  $m > 4$ . Заметим, что  $p_m = S_m - S_{m-1} = (l - k)(l + k)$ ; ввиду простоты  $p_m$  получим  $l - k = 1$ ,  $p_m = l + k = 2l - 1 = 2\sqrt{S_m} - 1$ . Таким образом,

$$S_m = \left(\frac{p_m + 1}{2}\right)^2.$$

Заметим, что  $p_m$  нечётно (так как  $m > 2$ ) и  $1 + 3 + 5 + \dots + p_m = (1^2 - 0^2) + (2^2 - 1^2) + \dots + \left(\frac{p_m + 1}{2}\right)^2 - \left(\frac{p_m - 1}{2}\right)^2 = \frac{p_m + 1}{2}$ . С другой стороны, в сумму  $S_m = 2 + p_2 + \dots + p_m$ , кроме двойки, входят лишь нечётные числа и при  $m > 4$  не входят нечётное составное число 9 и число 1, поэтому  $S_m \leq (1 + 3 + 5 + \dots + p_m) + 2 - 1 - 9 < \frac{p_m + 1}{2}$ . Противоречие.

**З а м е ч а н и е.** В последовательности  $(S_n)$  встречаются квадраты натуральных чисел. Кроме  $S_9 = 100$ , известны еще несколько; минимальный из них — это  $S_{2474} = 25633969 = 5063^2$ .

7. Найдите все простые числа  $p, q, r$ , удовлетворяющие равенству  $p^q + q^p = r$  (Московская математическая олимпиада, 10-й класс).

Р е ш е н и е

Среди чисел  $p, q, r$  должно быть хотя бы одно чётное. Действительно, если  $p$  и  $q$  нечётны, то  $p^q$  и  $q^p$  нечётны, а значит,  $r = p^q + q^p$  чётно. С другой стороны, единственное чётное простое число – это число 2. Следовательно, одно из чисел  $p, q, r$  равно двум. Если  $r = 2$ , то  $p = q = 1$  – не простые числа. Таким образом, одно из чисел  $p, q$  равно двум. Пусть это число  $p$ . Получим:  $2^q + q^2 = r$ .

Поскольку  $2^2 + 2^2 = 8$  – не простое число, то  $q \neq 2$ , а значит, число  $q$  нечётно, откуда  $2^q$  даёт остаток 2 при делении на три. Если  $q \neq 3$ , то число  $q$  не делится на три, а значит, число  $q^2$  даёт остаток 1 при делении на три. Итак, при  $q \neq 3$  получим  $r = 3$ , что невозможно, так как  $r > q > 3$ . Таким образом, остаётся только вариант  $p = 2, q = 3, r = 2^3 + 3^2 = 17$  или  $p = 3, q = 2, r = 3^2 + 2^3 = 17$ .

8. Приведённый квадратный трёхчлен с целыми коэффициентами в трёх последовательных целых точках принимает простые значения. Докажите, что он принимает простое значение, по крайней мере, еще в одной целой точке (Всероссийская олимпиада по математике, 10-й класс; автор – Агаханов Н. Х.).

Р е ш е н и е

Пусть трёхчлен  $f(x)$  принимает простые значения в точках  $n-1, n$  и  $n+1$ . Те же значения он принимает в точках, симметричных указанным относительно оси параболы  $y = f(x)$ . Эти симметричные точки также целые, так как по условию абсцисса вершины параболы целая или полуцелая. Отсюда следует утверждение задачи, если точка  $K(n, f(n))$  не является вершиной параболы. Если же  $K(n, f(n))$  – вершина параболы, то  $f(x) = (x - n)^2 + p$ , причём числа  $f(n) = p$  и  $f(n+1) = p+1$  – простые. Значит,  $p = 2, p+1 = 3$ . Но тогда и  $f(n+3) = 3^2 + 2 = 11$  – простое число.

9. Найдите все простые числа  $p, q$  и  $r$ , для которых выполняется равенство:  $p + q = (p - q)^r$  (Московская математическая регата, 9-й класс).

Р е ш е н и е

Из условия видно, что  $p + q$  делится на  $p - q$ , следовательно,  $(p + q) - (p - q) = 2q$  также делится на  $p - q$ . Делителями числа  $2q$  могут являться только числа 1, 2,  $q$  и  $2q$ . Если  $p - q = 1$ , то левая часть

исходного равенства больше правой части. Если  $p - q$  равно  $q$  или  $2q$ , то  $p$  равно  $2q$  или  $3q$ , т.е. число  $p$  – не простое. Значит,  $p - q = 2$ . Тогда исходное равенство примет вид:  $2q + 2 = 2^r \Leftrightarrow q = 2^{r-1} - 1$ . Если  $r = 2$ , то  $q = 1$  – не простое число. Значит,  $r$  нечетно и  $r - 1 = 2k$ . Далее можно рассуждать по-разному.

*Первый способ.*  $2^{r-1} - 1 = 4^k - 1$  делится на  $4 - 1 = 3$ . Таким образом,  $q = 3$ . Тогда  $p = 5$  и  $r = 3$ .

*Второй способ.* Так как  $q = 2^{2k} - 1 = (2^k - 1)(2^k + 1)$ , то  $q$  может оказаться простым числом только в случае, когда  $2^k - 1 = 1$ . Значит,  $k = 1$ ,  $r = 3$ ,  $q = 3$ ,  $p = 5$ .

**10.** Какова наибольшая длина арифметической прогрессии из натуральных чисел  $a_1, a_2, \dots, a_n$ , с разностью 2, обладающей свойством:  $a_k^2 + 1$  является простым числом при всех  $k = 1, 2, \dots, n$ ? (Все-российская олимпиада по математике, 2002, 10-й класс; автор – Агаханов Н. Х.).

**Р е ш е н и е**

Натуральные числа вида  $a = 5m \pm 2$  таковы, что  $a^2 + 1 \div 5$ , поэтому они не дают простых чисел  $p = a^2 + 1$ , кроме случая  $p = 5$  при  $a = 2$ . С другой стороны, среди чисел  $b, b + 2, b + 4$  – не более двух подряд идущих чисел, не имеющих вид  $5m \pm 2$ . Значит, если в прогрессии не содержится число 2, то  $n \leq 2$ . Если  $a_1 = 2$ , то  $n \leq 3$ , так как  $a_4 = 8 = 5 \cdot 2 - 2$ . Числа  $a_1 = 2, a_2 = 4, a_3 = 6$  дают искомую тройку, так как 5, 17, 37 – простые числа. Следовательно, наибольшая длина арифметической прогрессии из натуральных чисел  $a_1, a_2, \dots, a_n$ , с разностью 2, обладающей нужным свойством, равна трем.

**11.** При каких натуральных  $n$  число  $n^2 - 1$  является степенью простого числа? (Московская математическая регата, 11-й класс).

**Р е ш е н и е**

$n^2 - 1 = (n + 1)(n - 1)$ , а НОД  $(n + 1, n - 1) = d \leq 2$ . Если  $d = 2$ , то  $n^2 - 1$  – степень двойки:  $n + 1 = 2^k$  и  $n - 1 = 2^m$ , причём значения этих степеней различаются на 2. Значит,  $k = 2, m = 1, n = 3$ . Если же  $d = 1$ , то  $n - 1 = 1$ , т.е.  $n = 2$ . Таким образом, число  $n^2 - 1$  является степенью простого числа при  $n = 2$  и  $n = 3$ .

**12.** Найдите все такие натуральные  $k$ , что произведение первых  $k$  простых чисел, уменьшенное на 1, является точной степенью натурального числа (большей, чем первая) (Все-российская олимпиада по математике, 10-й класс; автор – Сендеров В. А.).

### Решение

Пусть  $n \geq 2$ , и  $2 = p_1 < \dots < p_k$  – первые  $k$  простых чисел. Предположим, что

$$p_1 p_2 \dots p_k = a^n + 1. \quad (*)$$

Если  $a = 1$ , то  $a^n + 1 = 2$  и, следовательно,  $k = 1$ .

Предположим теперь, что  $a > 1$ ; тогда  $k > 1$ . Число  $a$  нечётно, поэтому у него существует нечётный простой делитель  $q$ . Тогда  $q > p_k$ , иначе левая часть равенства (\*) делилась бы на  $q$ , что не так. Поэтому и  $a > p_k$ .

Без ограничения общности можно считать, что  $n$  – простое число (если  $n = st$ , то можно заменить  $n$  на  $t$ , а  $a$  – на  $a^s$ ). Заметим, что  $n > 2$ , поскольку  $a^2 + 1$  не может делиться на  $3 = p_2$ . Покажем, что  $n > p_k$ . Действительно, в противном случае  $n = p_i$ , где  $i \leq k$ . Тогда  $a^{p_i} + 1$  кратно  $p_i$ ; с другой стороны, по малой теореме Ферма  $a^{p_i} - a$  кратно  $p_i$ . Так как  $a^{p_i} + 1 = (a + 1)(a^{p_i-1} - a^{p_i-2} + \dots - a + 1)$ , причём  $a + 1 = (a^{p_i} + 1) - (a^{p_i} - a)$  кратно  $p_i$  и  $a^{p_i-1} - a^{p_i-2} + \dots - a + 1 \equiv 1 + 1 + \dots + 1 = p_i \equiv 0 \pmod{p_i}$ , то  $a^{p_i} + 1$  делится на  $p_i^2$ , что противоречит условию.

Итак,  $a > p_k$  и  $n > p_k$ , откуда  $a^n + 1 > p_k^{p_k} > p_1 p_2 \dots p_k$ , что противоречит равенству (\*). Таким образом, условию задачи удовлетворяет только  $k = 1$ .

**13.** Известно, что  $a^n - b^n$  делится на  $n$  ( $a, b, n$  – натуральные числа,  $a \neq b$ ). Доказать, что  $\frac{a^n - b^n}{a - b}$  делится на  $n$  (Московская математическая олимпиада, 9-й класс).

### Решение

Воспользуемся методом математической индукции.

*База.* Пусть  $n$  – простое число. Если число  $a - b$  не делится на  $n$ , то всё ясно. Если же  $a \equiv b \pmod{n}$ , то

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1} \equiv nb^{n-1} \equiv 0 \pmod{n}.$$

*Шаг индукции.* Пусть для всех показателей, меньших  $n$ , утверждение доказано. Обозначим  $d = \text{НОД}(n, a - b)$ , тогда  $n = kd$ .

Если  $d = 1$ , то всё ясно. Если  $d = n$ , то  $a \equiv b \pmod{n}$  и можно повторить вышеприведенное доказательство. Если же  $1 < d < n$ , то

$\frac{a^n - b^n}{a - b} = \frac{(a^d)^k - (b^d)^k}{a^d - b^d} \cdot \frac{a^d - b^d}{a - b}$  делится на  $n$ , так как первый множитель делится на  $k$ , а второй – на  $d$  (у последней дроби знаменатель, а тем более числитель делится на  $d$ ).

**14.** Сумма десяти натуральных чисел равна 1001. Какое наибольшее значение может принимать НОД (наибольший общий делитель) этих чисел? (Окружная олимпиада (Москва), 9-й класс).

**Р е ш е н и е**

*Пример.* Рассмотрим девять чисел, равных 91, и число 182. Их сумма равна 1001.

*Оценка.* Докажем, что значение, большее 91, НОД принимать не может. Заметим, что  $1001 = 7 \cdot 11 \cdot 13$ . Так как каждое слагаемое в данной сумме делится на НОД, то НОД является делителем числа 1001. С другой стороны, меньшее слагаемое в сумме (а значит и НОД) не больше, чем  $1001 : 10$ , т.е. не больше 101. Осталось заметить, что 91 – наибольший из делителей числа 1001, удовлетворяющий этому условию.

Таким образом, наибольшее значение, которое может принимать НОД десяти натуральных чисел с суммой 1001, равно 91.

**15.** Найдите все натуральные числа, имеющие ровно шесть делителей, сумма которых равна 3500 (Всероссийская олимпиада по математике, 9-й класс. Автор – Женодаров Р. Г.).

**Р е ш е н и е**

Если у числа  $n$  шесть делителей, то  $n = p^5$  ( $p$  – простое) или  $n = p^2q$ , где  $p$  и  $q$  – различные простые числа.

В первом случае  $1 + p + p^2 + p^3 + p^4 + p^5 = 3500$  или  $p(1 + p + p^2 + p^3 + p^4) = 3500 - 1 = 3499$ . Число 3499 не делится на 2, 3, 5 и 7, поэтому  $p > 10$ , но в этом случае  $p + (1 + p + p^2 + p^3 + p^4) > 10^5 > 3499$ . Поэтому это уравнение решений в простых числах не имеет. Во втором случае  $1 + p + p^2 + q + pq + p^2q = 3500$ , т.е.  $(1 + p + p^2)(1 + q) = 5^3 \cdot 7 \cdot 4^2$ . Первый множитель нечетный и не кратен 5 (чтобы убедиться в этом, достаточно проверить это утверждение для соответствующих остатков числа  $p$ ). Отсюда, учитывая, что  $1 + p + p^2 > 1$ , имеем  $1 + p + p^2 = 7$ . Значит,  $p = 2$  ( $p = -3$  – не подходит) и  $q = 499$ . Числа 2 и 499 – простые. Искомое число  $n = 2^2 \cdot 499 = 1996$ .

**16.** Найдите все пары натуральных чисел  $(a, b)$ , для которых выполняется равенство  $\text{НОК}(a, b) - \text{НОД}(a, b) = \frac{ab}{5}$  (Московская математическая регата, 11-й класс).

**Решение**

Воспользуемся тем, что  $\text{НОК}(a, b)$  делится на  $\text{НОД}(a, b)$ , и тождеством  $\text{НОК}(a, b) \cdot \text{НОД}(a, b) = ab$ . Пусть  $\text{НОД}(a, b) = n$ , тогда  $\text{НОК}(a, b) = kn$  ( $n$  и  $k$  – натуральные числа). Тогда  $5(kn - n) = kn^2$ , или  $k(5 - n) = 5$ . Это уравнение имеет единственное решение:  $k = 5, n = 4$ . Значит,  $\text{НОД}(a, b) = 4$ ,  $\text{НОК}(a, b) = 20$ ,  $ab = 80$ . Оба числа не меньше 4, и одно из них кратно 5, т.е. не меньше 20. Отсюда получаем, что данное равенство выполняется для пар  $(4, 20)$  и  $(20, 4)$ .

**17.** Наибольший общий делитель натуральных чисел  $a, b$  будем обозначать  $(a, b)$ . Пусть натуральное число  $n$  таково, что  $(n, n + 1) < (n, n + 2) < \dots < (n, n + 35)$ . Докажите, что  $(n, n + 35) < (n, n + 36)$  (Турнир городов, 8–9-е классы; автор – Френкин Б. Р.).

**Решение**

Заметим, что

$$(n, n + k) = (n, k) \leq k, \text{ т.е. } (n, n + 1) \leq 1, (n, n + 2) \leq 2, \dots, (n, n + 35) \leq 35.$$

Поэтому неравенства из условия задачи могут выполняться тогда и только тогда, когда  $(n, n + 1) = 1, (n, n + 2) = 2, \dots, (n, n + 35) = 35$ . Но тогда  $(n, n + 4) = 4, (n, n + 9) = 9$ , т.е.  $n$  делится на  $4 \cdot 9 = 36$ , откуда  $(n, n + 36) = 36 > 35 = (n, n + 35)$ .

**18.** Натуральные числа  $a, b, c, d$  таковы, что наименьшее общее кратное этих чисел равно  $a + b + c + d$ . Докажите, что  $abcd$  делится на 3 или на 5 (или на то и другое) (Турнир городов, 8–9-е классы; автор – Сендеров В. А.).

**Решение**

Пусть  $m = \text{НОК}(a, b, c, d) = a + b + c + d$ . Достаточно доказать, что  $m$  делится на 3 или на 5. Можно считать, что  $a \geq b \geq c \geq d$ . Если все четыре числа равны, то  $m = a$ , что противоречит условию. Следовательно, число  $b + c + d$  меньше  $3a$  и делится на  $a$ . Если  $b + c + d = 2a$ , то  $m = 3a$  кратно 3. Пусть  $b + c + d = a, m = 2a = 2(b + c + d)$ . Тогда  $2(c + d)$  делится на  $b$ . Если  $b = c = d$ , то  $a = 3b$  кратно 3. Если  $c + d < 2b$ , то  $2(c + d)$  равно  $3b, 2b$  или  $b$ , при этом  $m = 5b, 4b$  или  $3b$ . В первом и последнем случаях  $m$  кратно 3 или 5. Остался случай

$a = 2b$ ,  $c + d = b$ . При этом  $m = 4(c + d)$  делится на  $c$ , следовательно,  $4d$  равно  $4c$ ,  $3c$ ,  $2c$  или  $c$ . Во втором случае  $d$  кратно 3, в остальных  $c = d$ ,  $2d$  или  $4d$ . Соответственно,  $b = 2d$ ,  $3d$  или  $5d$ . В последних двух случаях  $b$  кратно 3 или 5. Случай же  $a = 2b = 4c = 4d$  невозможен, так как снова НОК  $(a, b, c, d) = a$ .

**19.** Найдите наибольшее натуральное  $n$ , для которого число  $6500!$  делится на каждое из чисел  $k^k$  при  $k = 1, 2, \dots, n$  (олимпиада «Физтех», дистанционный этап, 10-й класс).

**Р е ш е н и е**

Так как  $80^2 < 6500 < 81^2$ , то число  $6500!$  точно делится на  $k^k$  при  $k \leq 80$  (так как среди чисел от 1 до 6500 есть, по крайней мере,  $k$  чисел, делящихся на  $k$ ) и точно не делится на  $83^{83}$  (так как 83 – простое число и среди чисел от 1 до 6500 меньше 83 чисел, делящихся на 83, нет ни одного числа, которое делится на  $83^2$ ). Остается проверить, делится ли число  $6500!$  на  $81^{81}$  и  $82^{82}$ .

Заметим, что  $81^{81} = 3^{324}$ . Но  $\left[ \frac{6500}{3} \right] = 2166$ , поэтому число  $6500!$  делится на  $3^{2166}$  и, следовательно, делится на  $81^{81} = 3^{324}$ .

Проверим, делится ли число  $6500!$  на  $82^{82}$ .  $82 = 2 \cdot 41$ . Число  $6500!$  делится на  $2^{82}$  и  $\left[ \frac{6500}{41} \right] = 158$ . Следовательно, число  $6500!$  делится на  $41^{158}$  и тем более делится на  $41^{82}$ . Значит, число  $6500!$  делится на  $82^{82}$ .

Таким образом, наибольшее натуральное  $n$ , для которого число  $6500!$  делится на каждое из чисел  $k^k$  при  $k = 1, 2, \dots, n$ , равно 82.

*Учебное издание*

**Никитин Николай Дмитриевич,  
Никитина Ольга Геннадьевна**

## Теория чисел

Редактор *Т. Н. Судовчихина*  
Компьютерная верстка *Н. В. Ивановой*  
Дизайн обложки *А. А. Стаценко*

Подписано в печать 20.01.2016.  
Формат  $60 \times 84 \frac{1}{16}$ . Усл. печ. л. 5,81.  
Тираж 50. Заказ № 4.

---

Издательство ПГУ.  
440026, Пенза, Красная, 40.  
Тел./факс: (8412) 56-47-33; e-mail: [iic@pnzgu.ru](mailto:iic@pnzgu.ru)

