

# Элементы теории чисел

кафедра теории чисел  
механико-математического факультета  
МГУ имени М. В. Ломоносова

2 сентября 2023 г.

# Оглавление

<b>Оглавление</b>	<b>i</b>
<b>1 Целые числа</b>	<b>1</b>
1.1 Вводные задачи . . . . .	1
1.2 Наибольший общий делитель . . . . .	2
1.3 Основная теорема арифметики . . . . .	4
1.4 Линейные диофантовы уравнения . . . . .	7
<b>2 Арифметические функции</b>	<b>9</b>
2.1 Мультипликативные функции . . . . .	9
2.2 Функция Мёбиуса . . . . .	10
2.3 Функция Эйлера . . . . .	12
2.4 Свёртка Дирихле . . . . .	13
<b>3 Сравнения: Начало</b>	<b>14</b>
3.1 Задачи для разогрева . . . . .	14
3.2 Линейные сравнения . . . . .	15
3.3 Китайская теорема об остатках . . . . .	16
3.4 Бинарный алгоритм возведения в степень . . . . .	17
3.5 Теоремы Ферма и Эйлера . . . . .	18
3.6 Разное . . . . .	19
<b>4 Полиномиальные сравнения</b>	<b>20</b>
4.1 Предварительные соображения . . . . .	20
4.2 Подъём решений . . . . .	21
4.3 Сравнения второй степени. Символ Лежандра . . . . .	22
<b>5 Первообразные корни (WIP)</b>	<b>25</b>
<b>6 Цепные дроби (TODO)</b>	<b>26</b>
<b>A Примеры задач для контрольных и зачётов</b>	<b>27</b>
<b>Б Подъём решений</b>	<b>29</b>
<b>В Памятка про символ Лежандра (и заодно про символ Якоби)</b>	<b>31</b>

# Тема 1

## Целые числа

### 1.1 Вводные задачи

**Задача 1.1.** Докажите, что для всякого натурального  $n$  справедливы утверждения:

- 1) существуют  $n$  подряд идущих составных чисел;
- 2) существуют  $n$  подряд идущих натуральных чисел, среди которых ровно одно простое.

**Факт.** Каждое натуральное число  $n > 1$  имеет простой делитель.

**Задача 1.2.** Докажите, что при  $n \geq 3$  в интервале  $(n, n!)$  есть простое число. (Подсказка. Рассмотрите число  $n! - 1$ .)

**Задача 1.3.** Объясните, почему простых чисел бесконечно много.

**Задача 1.4.** Занумеруем простые числа в порядке возрастания:  $p_1 = 2, p_2 = 3, p_3 = 5$  и так далее. Докажите, что для любого  $n \geq 2$  справедливо неравенство  $p_{n+1} < p_1 p_2 \cdots p_n$ .

**Задача 1.5.** Найдите все простые числа  $p$ , для которых:

- 1) числа  $p + 10$  и  $p + 14$  также простые;
- 2) числа  $p + 2, p + 8, p + 14$  и  $p + 26$  также простые;
- 3) числа  $4p^2 + 1$  и  $6p^2 + 1$  также простые.

(Подсказка. Используйте деление с остатком.)

**Задача 1.6.** Докажите, что существует бесконечно много простых чисел вида:

- 1)  $4k - 1$ ;
- 2)  $6k - 1$ .

**Задача 1.7.** Пусть  $f(x)$  — непостоянный многочлен с целыми коэффициентами, причём старший коэффициент положителен. Докажите, что найдётся  $n \in \mathbb{N}$ , такое что число  $f(n)$  составное.

**Задача 1.8.** С помощью метода математической индукции докажите, что для произвольного натурального  $n$  справедливы утверждения:

- 1)  $n^3 + 5n \div 6$ ;
- 2)  $6^{2n-1} + 8 \div 7$ ;
- 3)  $2^{5n+3} + 5^n \cdot 3^{n+2} \div 17$ ;
- 4)  $10^n + 18n - 1 \div 27$ ;
- 5)  $2^{3^n} + 1 \div 3^{n+1}$  (однако  $3^{n+2} \nmid 2^{3^n} + 1$ );
- 6)  $\frac{11 \dots 1}{3^n} \div 3^n$  (однако  $3^{n+1} \nmid \frac{11 \dots 1}{3^n}$ ).

**Задача 1.9.** Рассмотрим числа Фибоначчи:  $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2} (n \geq 2)$ . Докажите следующие свойства:

$$1) 2 \mid F_n \iff 3 \mid n; \quad 2) 3 \mid F_n \iff 4 \mid n; \quad 3) 4 \mid F_n \iff 8 \mid F_n.$$

Подумай, бином Ньютона:

$$\begin{aligned} (a+b)^n &= \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \dots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n \\ &= a^n + n a^{n-1} b + \dots + n a b^{n-1} + b^n, \end{aligned}$$

где  $\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!}$  — биномиальные коэффициенты:  $\binom{n}{0} = \binom{n}{n} = 1, \binom{n}{1} = \binom{n}{n-1} = n, \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$ ,  $\binom{n}{3} = \binom{n}{n-3} = \frac{n(n-1)(n-2)}{3!}$  и так далее. Комбинаторный смысл:  $\binom{n}{k}$  — это количество способов выбрать  $k$  предметов из  $n$  без учёта порядка (что это означает при  $k=0$ ?), то есть количество  $k$ -элементных подмножеств у  $n$ -элементного множества.

**Задача 1.10.** Используя бином Ньютона, докажите утверждения:

$$1) 10^n + 18n - 1 \div 27; \quad 2) 2^{3n+2} + 3 \div 7; \quad 3) (2^n - 1)^n - 3 \div 2^n - 3.$$

**Задача 1.11.** Используя комбинаторный смысл биномиальных коэффициентов, найдите количество решений уравнения  $x + y + z = 2023$ :

- 1) в натуральных числах;
- 2) в целых неотрицательных числах. (Подсказка. Сведите к предыдущему пункту.)

**Задача 1.12.** Обобщите задачу 1.11 на уравнение  $x_1 + x_2 + \dots + x_k = n$ .

**Задача 1.13.** Пусть  $d_0, d_1, \dots, d_k$  — все натуральные делители числа  $N$ , упорядоченные по возрастанию (то есть  $1 = d_0 < d_1 < \dots < d_k = N$ ). Докажите, что для всех  $i$  выполнено  $d_i \leq 3d_{i-1}$ , если при некотором  $n \in \mathbb{N}$ :

$$1) N = 2^{2^n} - 1; \quad 2) N = 2^{2^{n+1}} + 2^{2^n} + 1; \quad 3) N = 4^{3^n} - 1.$$

**Сложная задача 1.14.** Целые числа  $a, b > 1$  таковы, что при любом  $n \in \mathbb{N}$  число  $\frac{a^n - 1}{b^n - 1}$  является натуральным. Докажите, что  $a = b^m$  при некотором  $m \in \mathbb{N}$ .

## Ответы

**1.5:** 1)  $p = 3$ ; 2)  $p = 3, 5$ ; 3)  $p = 5$ .

**1.12:** 1)  $\binom{n-1}{k-1}$ ; 2)  $\binom{n+k-1}{k-1}$ .

## 1.2 Наибольший общий делитель

**Задача 1.15.** Пусть  $p$  — простое число. Чему может равняться н.о.д.  $(a, p)$ ?

**Важная лемма.** Пусть  $c \mid ab$ , причём н.о.д.  $(a, c) = 1$ . Тогда  $c \mid b$ .

**Важное следствие.** Пусть  $p$  — простое число,  $p \mid ab$ . Тогда хотя бы одно из чисел  $a, b$  делится на  $p$ .

**Задача 1.16.** Выведите Важное следствие из Важной леммы.

**Задача 1.17.** Обобщите Важное следствие на произвольное число сомножителей:

$$p \mid a_1 a_2 \cdots a_n \implies \exists k: p \mid a_k.$$

**Задача 1.18.** Пусть  $p$  — простое число,  $1 \leq k \leq p-1$ . Используя (обобщённое) Важное следствие, докажите, что биномиальный коэффициент  $\binom{p}{k}$  делится на  $p$ .

**Задача 1.19.** Пусть  $a, b$  — взаимно простые натуральные числа, причём  $a \geq b$ . Докажите, что биномиальный коэффициент  $\binom{a}{b}$  делится на  $a$ . (Подсказка.  $\binom{a}{b} = \frac{a}{b} \cdot \binom{a-1}{b-1}$ .)

**Задача 1.20** (малая теорема Ферма). С помощью математической индукции и задачи 1.18 докажите, что если  $p$  — простое число,  $a \in \mathbb{N}$ , то  $p \mid a^p - a$ .

**Задача 1.21.** Пусть  $p$  — простое число,  $a \in \mathbb{Z}$ . Найдите остаток от деления  $a^{p-1}$  на  $p$ . (Подсказка. Воспользуйтесь малой теоремой Ферма.)

**Задача 1.22.**

1) Пусть  $a, b$  — нечётные целые числа. Докажите равенство

$$\text{н.о.д.}(a, b) = \text{н.о.д.}\left(\frac{a+b}{2}, \frac{a-b}{2}\right).$$

2) Пусть  $a, b, c$  — нечётные целые числа. Докажите равенство

$$\text{н.о.д.}(a, b, c) = \text{н.о.д.}\left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right).$$

**Утверждение.** Пусть  $a, b, c$  — целые числа, причём  $(a, b) \neq (0, 0)$ ,  $d = \text{н.о.д.}(a, b)$ . Уравнение  $ax + by = c$  разрешимо в целых числах, если и только если  $d \mid c$ , причём в этом случае все решения получаются по формулам:

$$\begin{cases} x = x_0 + \frac{b}{d}t, \\ y = y_0 - \frac{a}{d}t, \end{cases}$$

где  $(x_0, y_0)$  — (произвольное) частное решение, а параметр  $t$  пробегает все целые числа.

$\implies$  *Мораль:* чтобы решить уравнение  $ax + by = c$ , достаточно найти какое-то одно решение (а также  $\text{н.о.д.}(a, b)$ ). Это можно сделать с помощью алгоритма Евклида.

**Задача 1.23.** Используя алгоритм Евклида, решите в целых числах уравнения:

1)  $17x - 57y = 2$ ;

4)  $17x - 27y = 1$ ;

7)  $23x - 32y = 3$ ;

2)  $183x - 141y + 6 = 0$ ;

5)  $37x + 17y = 1$ ;

8)  $24335x - 3588y = 1$ ;

3)  $183x + 141y = 45$ ;

6)  $104x + 39y = 25$ ;

9)  $24335x + 3588y = 928$ .

**Задача 1.24.** Решите в целых числах уравнение  $123x + 456y = 123456$ .

**Задача 1.25.** Пусть  $a_1, \dots, a_n$  — целые числа, не все равные 0. Докажите утверждения:

1) найдутся такие целые  $\lambda_1, \dots, \lambda_n$ , что

$$\text{н.о.д.}(a_1, \dots, a_n) = \lambda_1 a_1 + \dots + \lambda_n a_n;$$

- 2) любой общий делитель чисел  $a_1, \dots, a_n$  является делителем  $\text{н.о.д.}(a_1, \dots, a_n)$  и наоборот;  
 3) для всякого целого  $a$  справедливо равенство

$$\text{н.о.д.}(a_1, \dots, a_n, a) = \text{н.о.д.}(\text{н.о.д.}(a_1, \dots, a_n), a).$$

(Подсказка. Доказывайте все три утверждения одновременно, используя индукцию по  $n$ .)

**Задача 1.26.** Докажите Важную лемму с помощью п. 1 задачи 1.25.

**Задача 1.27.** Пусть  $c$  делится на  $a$  и  $b$ , причём  $\text{н.о.д.}(a, b) = 1$ . Докажите, что  $c$  делится на  $ab$ .

**Задача 1.28.** Пусть  $m, n \in \mathbb{N}$ . Докажите равенства:

- 1)  $\text{н.о.д.}(\underbrace{11 \dots 1}_m, \underbrace{11 \dots 1}_n) = \underbrace{11 \dots 1}_{\text{н.о.д.}(m, n)}$ ;  
 2)  $\text{н.о.д.}(a^m - 1, a^n - 1) = a^{\text{н.о.д.}(m, n)} - 1$ , где  $a \in \mathbb{N}$ ,  $a > 1$ ;  
 3\*)  $\text{н.о.д.}(F_m, F_n) = F_{\text{н.о.д.}(m, n)}$ , где  $F_k$  —  $k$ -е число Фибоначчи. (Подсказка. Например, докажите и используйте тождество  $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$ .)

**Задача 1.29.**

- 1) Докажите, что для всякого простого  $p > 2$  числитель  $m$  дроби  $\frac{m}{n} = \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1}$  делится на  $p$ .  
 2\*\*) Докажите, что при  $p > 3$  число  $m$  делится на  $p^2$ .

## Ответы

**1.21:** 0, если  $p \mid a$ , и 1 в противном случае.

**1.23:** 1)  $x = -20 + 57t$ ,  $y = -6 + 17t$ ,  $t \in \mathbb{Z}$ ; 2)  $x = 20 + 47t$ ,  $y = 26 + 61t$ ,  $t \in \mathbb{Z}$ ; 3)  $x = -9 + 47t$ ,  $y = 12 - 61t$ ,  $t \in \mathbb{Z}$ ; 4)  $x = 8 + 27t$ ,  $y = 5 + 17t$ ,  $t \in \mathbb{Z}$ ; 5)  $x = 6 + 17t$ ,  $y = -13 - 37t$ ,  $t \in \mathbb{Z}$ ; 6) нет решений; 7)  $x = 21 + 32t$ ,  $y = 15 + 23t$ ,  $t \in \mathbb{Z}$ ; 8)  $x = 2807 + 3588t$ ,  $y = 19038 + 24335t$ ,  $t \in \mathbb{Z}$ ; 9)  $x = 8 + 3588t$ ,  $y = -54 - 24335t$ ,  $t \in \mathbb{Z}$ .

**1.24:**  $x = 1000 + 152t$ ,  $y = 1 - 41t$ ,  $t \in \mathbb{Z}$ .

## 1.3 Основная теорема арифметики

**Основная теорема арифметики.** Каждое натуральное число  $n > 1$  можно представить в виде произведения простых чисел, причём такое представление единственно с точностью до порядка сомножителей. (Простое число является «произведением» из одного сомножителя. Удобно также считать, что число 1 раскладывается в «пустое» произведение простых сомножителей.)

Представление  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , где  $p_1 < p_2 < \dots < p_k$  — простые числа,  $\alpha_i \in \mathbb{N}$ , называется каноническим разложением натурального числа  $n$  на простые сомножители. Для каждого  $n$  оно единственно. Если простое число  $p$  входит в каноническое разложение числа  $n$  в степени  $\alpha$ , то положим  $v_p(n) = \alpha$ . Условимся также, что  $v_p(n) = 0$ , если  $p \nmid n$ . (Функцию  $v_p$  будем обзывать ( $p$ -адическим) показателем.)

Некоторые свойства показателей  $v_p(\cdot)$ :

- 1)  $n = \prod_{p \mid n} p^{v_p(n)} = \prod_p p^{v_p(n)}$  (первое произведение берётся по всем простым делителям  $p$  числа  $n$ , второе — по всем простым числам  $p$ );

- 2)  $v_p(ab) = v_p(a) + v_p(b)$ ;
- 3)  $v_p(n)$  — это такое целое  $\alpha \geq 0$ , что  $p^\alpha \parallel n$ , то есть  $p^\alpha \mid n$ , но  $p^{\alpha+1} \nmid n$ ;
- 4)  $a \mid b \iff$  для всех простых  $p$  выполнено  $v_p(a) \leq v_p(b)$ ; при этом  $v_p(b/a) = v_p(b) - v_p(a)$ .

**Задача 1.30.** Пусть  $a_1, \dots, a_n \in \mathbb{N}$ ,  $p$  — простое число. Докажите равенства:

- 1)  $v_p(\text{н.о.д.}(a_1, \dots, a_n)) = \min\{v_p(a_1), \dots, v_p(a_n)\}$ ;
- 2)  $v_p(\text{н.о.к.}(a_1, \dots, a_n)) = \max\{v_p(a_1), \dots, v_p(a_n)\}$ .

**Задача 1.31.**

- 1) Пусть  $a, b \in \mathbb{N}$ . Докажите равенство  $ab = \text{н.о.д.}(a, b) \cdot \text{н.о.к.}(a, b)$ .
- 2) Пусть  $a_1, \dots, a_n \in \mathbb{N}$ . Докажите равенства

$$\begin{aligned} a_1 \cdots a_n &= \text{н.о.д.}(a_1, \dots, a_n) \cdot \text{н.о.к.}\left(\frac{a_1 \cdots a_n}{a_1}, \dots, \frac{a_1 \cdots a_n}{a_n}\right) \\ &= \text{н.о.к.}(a_1, \dots, a_n) \cdot \text{н.о.д.}\left(\frac{a_1 \cdots a_n}{a_1}, \dots, \frac{a_1 \cdots a_n}{a_n}\right). \end{aligned}$$

**Задача 1.32.** Рассмотрим числа  $a = 2^7 \cdot 3^3 \cdot 7^2 \cdot 13^4 \cdot 21^5$  и  $b = 3^2 \cdot 5^6 \cdot 7^3 \cdot 15^2 \cdot 20^4$ . Найдите:

- 1)  $\text{н.о.д.}(a, b)$ ;
- 2)  $\text{н.о.к.}(a, b)$ ;
- 3) количество (натуральных) общих делителей чисел  $a$  и  $b$ ;
- 4) количество чётных общих делителей чисел  $a$  и  $b$ ;
- 5) произведение всех общих делителей чисел  $a$  и  $b$ .

**Задача 1.33.** Пусть  $n \in \mathbb{N}$ ,  $p$  — простое число. Докажите утверждения:

- 1)  $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$  (где  $\lfloor x \rfloor$  — целая часть числа  $x \in \mathbb{R}$ , то есть наибольшее целое число, не превосходящее  $x$ , то бишь такое  $n \in \mathbb{Z}$ , что  $n \leq x < n + 1$ );
- 2)  $v_p(n!) < \frac{n}{p-1}$ ;
- 3)  $(n!)^{\frac{1}{n}} < \prod_{p \leq n} p^{\frac{1}{p-1}}$  при  $n > 1$ , где произведение берётся по всем простым  $p$ , не превосходящим  $n$ ;
- 4)  $v_p(n!) = \frac{n - S_p(n)}{p-1}$ , где  $S_p(n)$  — сумма цифр числа  $n$  в  $p$ -ичной системе счисления (то есть  $S_p(n) = a_0 + a_1 + \dots + a_k$ , где  $n = a_0 + a_1 p + \dots + a_k p^k$ ,  $a_i \in \{0, 1, \dots, p-1\}$ ).

**Задача 1.34.** Сколькими нулями оканчивается десятичная запись числа  $1000!$ ?

**Задача 1.35.** Посчитайте количество делителей числа  $16!$ .

**Задача 1.36.**

- 1) Докажите, что для любых вещественных чисел  $x, y$  выполнено  $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$ .
- 2) Докажите, что  $\binom{n}{k} \in \mathbb{N}$ , используя явную формулу  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$  и свойства показателей.

**Задача 1.37.**

- 1) Докажите, что для любого  $x \in \mathbb{R}$  справедливо неравенство  $[6x] + [x] \geq [3x] + 2[2x]$ .
- 2) Докажите, что при любом  $n \in \mathbb{N}$  число  $\frac{(6n)!n!}{(3n)!(2n)!^2}$  является целым.

**Задача 1.38.**

- 1) Пусть  $N, n \in \mathbb{N}$ ,  $N > 2^{n-1}\sqrt{N}$ . Докажите, что среди чисел  $1, \dots, N$  не менее  $n$  простых. (Подсказка. Каждое натуральное число можно представить в виде  $ab^2$ , где  $a$  бесквадратно.)
- 2) Докажите, что среди чисел  $1, \dots, N$  не менее  $\log_4 N$  простых.
- 3) Докажите, что  $n$ -е простое число удовлетворяет неравенству  $p_n < 4^n$ .

**Задача 1.39.** Пусть  $a, b, c, k \in \mathbb{N}$ ,  $ab = c^k$ , н.о.д. $(a, b) = 1$ . Докажите, что  $a = c_1^k$ ,  $b = c_2^k$  для некоторых  $c_1, c_2 \in \mathbb{N}$ .

**Задача 1.40** (примитивные пифагоровы тройки). Найдите все натуральные решения уравнения  $x^2 + y^2 = z^2$  с условием н.о.д. $(x, y, z) = 1$ . Утверждения-подсказки:

- 1) Числа  $x, y, z$  попарно взаимно просты.
- 2) Числа  $x, y$  разной чётности,  $z$  нечётно.
- 3) Пусть  $x$  чётно, а  $y$  нечётно. Тогда числа  $(z \pm y)/2$  взаимно просты.
- 4) Все решения с чётным  $x$  получаются по формулам:  $x = 2ab$ ,  $y = a^2 - b^2$ ,  $z = a^2 + b^2$ , где  $a, b$  — взаимно простые натуральные числа разной чётности,  $a > b$ .

**Задача 1.41.** Докажите, что уравнение  $x^4 + y^4 = z^2$  не имеет решений в натуральных числах. Для этого предположите противное и получите противоречие. Утверждения-подсказки:

- 1) Найдётся решение с попарно взаимно простыми  $x, y, z$ , причём  $x$  чётно.
- 2) Справедливы равенства  $x^2 = 2ab$ ,  $y^2 = a^2 - b^2$ ,  $z = a^2 + b^2$ , где  $a > b$  — взаимно простые натуральные числа, причём  $a$  нечётно, а  $b$  чётно.
- 3) Найдутся  $z_1, c_2 \in \mathbb{N}$ , такие что  $a = z_1^2$ ,  $b = 2c_2^2$ .
- 4) Найдутся взаимно простые  $a_1, b_1 \in \mathbb{N}$ , такие что  $a = a_1^2 + b_1^2$ ,  $b = 2a_1b_1$ .
- 5) Найдутся взаимно простые  $x_1, y_1 \in \mathbb{N}$ , такие что  $a_1 = x_1^2$ ,  $b_1 = y_1^2$ .
- 6) Справедливо равенство  $x_1^4 + y_1^4 = z_1^2$ , причём числа  $x_1, y_1, z_1$  попарно взаимно просты и  $z_1 < z$ .

**Задача 1.42.** Докажите, что уравнение  $x^2 + y^4 = z^4$  не имеет решений в натуральных числах.

**Ответы**

**1.32:** 1)  $2^7 \cdot 3^4 \cdot 7^3$ ; 2)  $2^8 \cdot 3^8 \cdot 5^{12} \cdot 7^7 \cdot 13^4$ ; 3) 160; 4) 140; 5)  $2^{560} \cdot 3^{320} \cdot 7^{240}$ .

**1.34:** 249.

**1.35:** 5376.

## 1.4 Линейные диофантовы уравнения

Пусть  $a_1, \dots, a_n, b \in \mathbb{Z}$ , причём  $|a_1| + \dots + |a_n| > 0$ . Чтобы решить в целых числах уравнение

$$a_1x_1 + \dots + a_nx_n = b,$$

можно использовать следующий алгоритм:

о) Составляем матрицу (размера  $(n+1) \times n$ )

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

1) Со *столбцами* матрицы разрешается проделывать следующие махинации:

а) к любому столбцу матрицы можно прибавить любой другой, умноженный на целое число, например:

$$\begin{pmatrix} e_1 & e_2 \\ f_1 & f_2 \\ g_1 & g_2 \end{pmatrix} \rightarrow \begin{pmatrix} e_1 + \lambda e_2 & e_2 \\ f_1 + \lambda f_2 & f_2 \\ g_1 + \lambda g_2 & g_2 \end{pmatrix}$$

(к первому столбцу прибавили второй, умноженный на  $\lambda$ , *второй столбец при этом не меняется*);

б) любой столбец матрицы можно умножить на  $-1$  (то есть тупо меняем знаки у всех элементов столбца);

в) можно поменять любые два столбца местами.

2) С помощью этих преобразований приводим матрицу к виду

$$\begin{pmatrix} d & 0 & \dots & 0 \\ c_{1,0} & c_{1,1} & \dots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,0} & c_{n,1} & \dots & c_{n,n-1} \end{pmatrix}.$$

Тогда:

а)  $|d| = \text{н.о.д.}(a_1, \dots, a_n)$ .

б) Если  $d \nmid b$ , то (целых) решений нет. В противном случае общее решение имеет вид

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \underbrace{\frac{b}{d} \begin{pmatrix} c_{1,0} \\ \vdots \\ c_{n,0} \end{pmatrix}}_{\text{частное решение}} + \underbrace{t_1 \begin{pmatrix} c_{1,1} \\ \vdots \\ c_{n,1} \end{pmatrix} + \dots + t_{n-1} \begin{pmatrix} c_{1,n-1} \\ \vdots \\ c_{n,n-1} \end{pmatrix}}_{\text{общее решение однородного уравнения}},$$

где  $t_1, \dots, t_{n-1} \in \mathbb{Z}$ .

*Замечание.* В произвольный момент работы алгоритма для любого столбца  $\begin{pmatrix} s \\ u_1 \\ \vdots \\ u_n \end{pmatrix}$  матрицы выполнено

$$a_1u_1 + \dots + a_nu_n = s.$$

Это наблюдение можно использовать для проверки вычислений, а также для нахождения частных решений уравнения, любое из которых можно использовать вместо  $\frac{b}{d} \begin{pmatrix} c_{1,0} \\ \vdots \\ c_{n,0} \end{pmatrix}$ .

**Задача 1.43.** Решите уравнения из задачи 1.23 с помощью матричного алгоритма.

**Задача 1.44.** Решите в целых числах уравнения:

1)  $3x + 5y + 7z = 1$ ;

4)  $179x + 65y - 8z = 7$ ;

2)  $8x - 15y + 29z = -2$ ;

5)  $66x + 108y - 150z - 36 = 0$ ;

3)  $85x - 13y - 8z + 3 = 0$ ;

6)  $9x + 33y - 21z - 12w = 6$ .

**Сложная задача 1.45.** Обоснуйте алгоритм.

## Ответы

Ответы приводить бессмысленно, так как их внешний вид слишком сильно зависит от используемых преобразований.

## Тема 2

# Арифметические функции

### 2.1 Мультипликативные функции

*Арифметической* функцией называется произвольная функция  $f : \mathbb{N} \rightarrow \mathbb{C}$  (если не знаем про комплексные числа, то под  $\mathbb{C}$  можно понимать  $\mathbb{R}$ ). Арифметическая функция  $f$  называется *мультипликативной*, если, во-первых, она не является тождественно нулевой и, во-вторых, для любых взаимно простых  $a, b \in \mathbb{N}$  выполнено  $f(ab) = f(a)f(b)$ .

**Задача 2.1.** Докажите, что для любой мультипликативной функции  $f$  выполнено  $f(1) = 1$ . (Следовательно, вместо условия  $f \not\equiv 0$  в определении мультипликативной функции можно потребовать  $f(1) = 1$ .)

**Задача 2.2.** Пусть  $f$  — мультипликативная функция. Докажите, что для любых попарно взаимно простых  $a_1, \dots, a_n$  выполнено

$$f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n).$$

**Задача 2.3.** Пусть  $f$  — мультипликативная функция. Докажите, что для любого натурального  $n$  выполнено

$$\sum_{d|n} f(d) = \prod_{p|n} (f(1) + f(p) + f(p^2) + \cdots + f(p^{\nu_p(n)})),$$

где сумма берётся по всем натуральным, а произведение — по всем простым делителям числа  $n$ . (При  $n = 1$  произведение полагается равным 1.)

**Задача 2.4.** Докажите, что арифметическая функция  $f$  является мультипликативной тогда и только тогда, когда для любого  $n \in \mathbb{N}$  справедливо равенство

$$f(n) = \prod_{p|n} f(p^{\nu_p(n)}).$$

**Задача 2.5.** Пусть для каждого простого числа  $p$  и каждого натурального числа  $\alpha$  выбрано число  $c(p, \alpha) \in \mathbb{C}$ . Докажите, что существует единственная мультипликативная функция  $f$ , такая что при всех  $p$  и  $\alpha$  выполнено  $f(p^\alpha) = c(p, \alpha)$ .

**Задача 2.6.** Пусть  $f$  — мультипликативная функция,  $m \in \mathbb{N}$ , причём  $f(m) \neq 0$ . Докажите, что функция  $g(n) = \frac{f(mn)}{f(m)}$  мультипликативна.

**Задача 2.7.** Пусть  $f$  — арифметическая функция,  $F(n) = \sum_{d|n} f(d)$ . Докажите утверждения:

- 1) Если  $f$  мультипликативна, то  $F$  также мультипликативна.
- 2) Если  $F$  мультипликативна, то  $f$  также мультипликативна. (*Подсказка.* Воспользоваться математической индукцией.)

Для  $n \in \mathbb{N}$  обозначим:  $\tau(n)$  — количество (натуральных) делителей числа  $n$ ,  $\sigma(n)$  — сумма делителей числа  $n$ .

**Задача 2.8.** Докажите, что функции  $\tau$  и  $\sigma$  мультипликативны, и выведите явные формулы для  $\tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$  и  $\sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$ .

**Задача 2.9.** Докажите, что для всякого  $n \in \mathbb{N}$  справедливо равенство

$$\sum_{d|n} \tau(d^2) = (\tau(n))^2.$$

**Задача 2.10.**

- 1) Число  $n \in \mathbb{N}$  называется *совершенным*, если оно удовлетворяет равенству  $\sigma(n) = 2n$  (то есть равно сумме своих собственных делителей). Докажите, что все *чётные* совершенные числа  $n$  задаются формулой  $n = 2^{p-1}(2^p - 1)$ , где  $p \in \mathbb{N}$  таково, что число  $2^p - 1$  простое (теорема Евклида–Эйлера). (Простые числа вида  $2^p - 1$  называются простыми числами Мерсенна; очевидно, что само число  $p$  при этом тоже простое.)
- 2) Число  $n \in \mathbb{N}$  называется *суперсовершенным*, если оно удовлетворяет равенству  $\sigma(\sigma(n)) = 2n$ . Докажите, что все *чётные* суперсовершенные числа  $n$  описываются формулой  $n = 2^{p-1}$ , где  $2^p - 1$  — простое число Мерсенна.

(В настоящий момент неизвестно, существуют ли *нечётные* совершенные/суперсовершенные числа.)

## Ответы

$$2.8: \tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1), \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

## 2.2 Функция Мёбиуса

Функция Мёбиуса:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если найдётся простое } p, \text{ такое что } p^2 \mid n, \\ (-1)^k, & \text{если } n = p_1 \cdots p_k, \text{ где } p_1 < \cdots < p_k \text{ — простые.} \end{cases}$$

**Формула обращения Мёбиуса.** Пусть  $f, F$  — арифметические функции. Тогда следующие два условия эквивалентны:

- 1)  $F(n) = \sum_{d|n} f(d)$  (для всех  $n \in \mathbb{N}$ );
- 2)  $f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right)$  (для всех  $n \in \mathbb{N}$ ).

**Задача 2.11.** Докажите, что функция Мёбиуса мультипликативна.

**Задача 2.12.** Докажите равенства:

$$1) \sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1; \end{cases} \quad 2) \sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

**Задача 2.13.** Пусть арифметическая функция  $f$  такова, что при всех  $n \in \mathbb{N}$  справедливо равенство

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \frac{\mu(n) \sigma(n)}{\tau(n^2)}.$$

Найдите все натуральные решения уравнения  $f(x) = 0$ .

**Задача 2.14.**

1) Докажите, что для любого  $x \in [1, +\infty)$  выполнено

$$\sum_{n \leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1,$$

где сумма берётся по всем натуральным числам  $n$ , не превосходящим  $x$ . (Подсказка. Воспользуйтесь п. 1 задачи 2.12.)

2) Докажите, что при  $N \geq 2$  справедливо неравенство

$$\left| \sum_{n=1}^N \frac{\mu(n)}{n} \right| < 1.$$

(На самом деле  $\lim_{N \rightarrow \infty} \sum_{n=1}^N \frac{\mu(n)}{n} = 0$ , но доказать это очень сложно.)

**Задача 2.15.** Пусть  $n \in \mathbb{N}$ . Вычислите произведения:

$$1) \prod_{d|n} d^{\mu(n/d)}; \quad 2) \prod_{d|n} d^{\mu(d)}.$$

**Сложная задача 2.16.** Используя п. 1 задачи 2.12, докажите формулу обращения Мёбиуса.

**Сложная задача 2.17.**

1) Обобщите формулу обращения Мёбиуса на функции  $f, F: [1, +\infty) \rightarrow \mathbb{C}$ :

$$F(x) = \sum_{n \leq x} f\left(\frac{x}{n}\right) \iff f(x) = \sum_{n \leq x} \mu(n) F\left(\frac{x}{n}\right).$$

2) Выведите из утверждения п. 1 обычную формулу обращения Мёбиуса.

## Ответы

**2.13:**  $x = 2n$ , где  $n \in \mathbb{N}$ .

**2.15:** 1)  $p$ , если  $n = p^\alpha$  ( $p$  — простое число,  $\alpha \in \mathbb{N}$ ), и 1 в противном случае; 2)  $1/p$ , если  $n = p^\alpha$ , и 1 в противном случае.



**Задача 2.25.**

1) Докажите, что для любых  $a, b \in \mathbb{N}$  справедливо равенство

$$\varphi(ab) = \varphi(a) \varphi(b) \frac{\text{н.о.д.}(a, b)}{\varphi(\text{н.о.д.}(a, b))}.$$

2) Докажите, что если  $\text{н.о.д.}(a, b) > 1$ , то  $\varphi(ab) > \varphi(a) \varphi(b)$ .

**Ответы**

**2.18:**  $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1)$ .

**2.20:** 1) 40; 2) 1980; 3) 192.

**2.21:** 1)  $x = 4$ ; 2) нет решений; 3)  $x = 3$ ; 4)  $(x, y) = (2, 2)$ ; 5)  $(x, y) = (3, 2)$ ; 6)  $(x, y) = (4, 2)$ ; 7)  $(x, y, z) = (1, 2, 1)$ ; 8)  $(x, y, z) = (t, t + 1, 2t)$ ,  $t \in \mathbb{N}$ ; 9)  $(x, y, z) = (t + 1, 2^{t-1}, 3^t)$ ,  $t \in \mathbb{N}$ .

**2.22:** 1)  $\varphi(n/d)$ , если  $d \mid n$ , и 0 в противном случае; 2) обе суммы равны  $n$ .

**2.4 Свёртка Дирихле**

Не нужна.

## Тема 3

# Сравнения: Начало

### Напоминание

Эквивалентные определения:  $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$  найдётся  $k \in \mathbb{Z}$ , такое что  $a = b + mk \iff a$  и  $b$  дают один и тот же остаток при делении на  $m$ .

Некоторые свойства:

- 1)  $a \equiv a \pmod{m}$  (рефлексивность);
- 2) если  $a \equiv b \pmod{m}$ , то  $b \equiv a \pmod{m}$  (симметричность);
- 3) если  $a \equiv b \pmod{m}$  и  $b \equiv c \pmod{m}$ , то  $a \equiv c \pmod{m}$  (транзитивность; вместе свойства 1, 2 и 3 означают, что при фиксированном модуле  $m$  получаем отношение эквивалентности);
- 4) если  $a_1 \equiv b_1 \pmod{m}$  и  $a_2 \equiv b_2 \pmod{m}$ , то

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m},$$

$$a_1 - a_2 \equiv b_1 - b_2 \pmod{m},$$

$$a_1 a_2 \equiv b_1 b_2 \pmod{m};$$

- 5) если  $a \equiv b \pmod{m}$ ,  $n \in \mathbb{N}$ , то  $a^n \equiv b^n \pmod{m}$ ;
- 6) если  $a \equiv b \pmod{m}$ ,  $f(x) \in \mathbb{Z}[x]$ , то  $f(a) \equiv f(b) \pmod{m}$ ;
- 7) если  $c \neq 0$ , то  $a \equiv b \pmod{m} \iff ac \equiv bc \pmod{mc}$ ;
- 8) если  $\text{н.о.д.}(c, m) = 1$ , то  $a \equiv b \pmod{m} \iff ac \equiv bc \pmod{m}$ ;
- 9) если  $a \equiv b \pmod{m}$ ,  $d \mid m$ , то  $a \equiv b \pmod{d}$ ;
- 10)  $a \equiv b \pmod{m_i}, i = 1, \dots, n \iff a \equiv b \pmod{\text{н.о.к.}(m_1, \dots, m_n)}$ ;
- 11) если  $a \equiv b \pmod{m}$ , то  $\text{н.о.д.}(a, m) = \text{н.о.д.}(b, m)$ .

### 3.1 Задачи для разогрева

**Задача 3.1.** Используя свойства сравнений, докажите, что при произвольном целом  $n \geq 0$  число  $12^{n+2} \cdot 34^{3n+4} - 43^{4n+3} \cdot 21^{2n+1}$  делится на 11.

**Задача 3.2.** Обоснуйте «школьные» признаки делимости на 3, 9 и 11:

- 1) При делении на 3 натуральное число даёт такой же остаток, что и сумма его (десятичных) цифр (в частности, натуральное число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3).
- 2) При делении на 9 натуральное число даёт такой же остаток, что и сумма его цифр.
- 3) Натуральное число делится на 11 тогда и только тогда, когда на 11 делится разность между суммой цифр с чётными номерами и суммой цифр с нечётными номерами. (Как определить остаток при делении на 11?)

**Задача 3.3.** Допустим, что длины сторон прямоугольного треугольника суть целые числа. Докажите, что:

- 1) длина хотя бы одного из катетов делится на 3;
- 2) длина хотя бы одной из сторон делится на 5.

**Задача 3.4.** Докажите утверждения:

- 1) Существует бесконечно много натуральных чисел, не представимых в виде суммы двух квадратов целых чисел.
- 2) Существует бесконечно много натуральных чисел, не представимых в виде суммы трёх квадратов целых чисел.

## 3.2 Линейные сравнения

**Утверждение.** Пусть  $a, b, m \in \mathbb{Z}$ ,  $m \neq 0$ ,  $d = \text{н.о.д.}(a, m)$ . Сравнение  $ax \equiv b \pmod{m}$  разрешимо, если и только если  $d \mid b$ , причём в этом случае общее решение имеет вид  $x \equiv x_0 \pmod{m/d}$ , где  $x_0$  — (произвольное) частное решение.

**Задача 3.5.** Обоснуйте утверждение.

**Задача 3.6.** Используя алгоритм Евклида или матричный алгоритм, решите сравнения:

- |                                |                                    |                                      |
|--------------------------------|------------------------------------|--------------------------------------|
| 1) $23x \equiv 19 \pmod{18}$ ; | 3) $23x + 13 \equiv 0 \pmod{73}$ ; | 5) $141x \equiv 45 \pmod{183}$ ;     |
| 2) $25x \equiv 9 \pmod{52}$ ;  | 4) $91x \equiv 26 \pmod{133}$ ;    | 6) $340x + 90 \equiv 0 \pmod{445}$ . |

**Задача 3.7.** Решите сравнение  $66x + 108y \equiv 36 \pmod{150}$ .

*Важный частный случай:* если  $\text{н.о.д.}(a, m) = 1$ , то сравнение  $ax \equiv b \pmod{m}$  разрешимо при любом  $b$ , в частности при  $b = 1$ . Решением сравнения  $ax \equiv 1 \pmod{m}$  является класс вычетов по модулю  $m$ , который будем обозначать через  $a^{-1} \pmod{m}$  (под  $a^{-1}$  ниже понимается произвольный представитель этого класса вычетов).

**Задача 3.8.** Найдите  $47^{-1} \pmod{61}$ .

**Задача 3.9.** Докажите, что если сравнение  $ax \equiv 1 \pmod{m}$  разрешимо, то  $\text{н.о.д.}(a, m) = 1$ .

**Задача 3.10.** Пусть  $\text{н.о.д.}(a, m) = 1$ . Решите сравнение  $ax \equiv b \pmod{m}$ , используя  $a^{-1} \pmod{m}$ .

**Задача 3.11.** Пусть  $\text{н.о.д.}(a, m) = 1$ . Докажите, что  $\text{н.о.д.}(a^{-1}, m) = 1$  и  $(a^{-1})^{-1} \equiv a \pmod{m}$ .

**Ответы**

- 3.6: 1)  $x \equiv 11 \pmod{18}$ ; 2)  $x \equiv 17 \pmod{52}$ ; 3)  $x \equiv 28 \pmod{73}$ ; 4) нет решений; 5)  $x \equiv 12 \pmod{61}$ ; 6)  $x \equiv 39 \pmod{89}$ .  
 3.8:  $13 \pmod{61}$ .  
 3.10:  $x \equiv a^{-1}b \pmod{m}$ .

**3.3 Китайская теорема об остатках**

**Китайская теорема об остатках.** Допустим, что модули  $m_1, \dots, m_n \in \mathbb{N}$  попарно взаимно просты. Тогда для любых чисел  $a_1, \dots, a_n \in \mathbb{Z}$  система сравнений

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \dots\dots\dots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{3.1}$$

разрешима, причём общее решение имеет вид  $x \equiv x_0 \pmod{M}$ , где  $x_0$  — (произвольное) частное решение,  $M = m_1 \cdots m_n$ .

Частное решение  $x_0$  системы сравнений (3.1) можно искать в виде

$$x_0 = M_1x_1 + \dots + M_nx_n,$$

где  $M_i = M/m_i = m_1 \cdots m_{i-1}m_{i+1} \cdots m_n$ ; при этом для неизвестных  $x_i$  получаем независимые условия

$$M_ix_i \equiv a_i \pmod{m_i}, \quad i = 1, \dots, n.$$

(Почему эти сравнения разрешимы?) Если рассмотреть  $M_i^* \in \mathbb{Z}$ , такие что  $M_iM_i^* \equiv 1 \pmod{m_i}$  (то есть  $M_i^* \equiv M_i^{-1} \pmod{m_i}$ ), то в качестве частного решения сходится

$$x_0 = M_1M_1^*a_1 + \dots + M_nM_n^*a_n.$$

(Эта формула удобна, если (и только если) нужно решать много систем с одними и теми же модулями  $m_1, \dots, m_n$  и разными правыми частями  $a_1, \dots, a_n$ .)

Аналогичные соображения можно применять и в случае, когда сравнения системы имеют вид  $a_ix \equiv b_i \pmod{m_i}$ , н.о.д.( $a_i, m_i$ ) = 1.

**Задача 3.12.** Решите системы сравнений:

- |   |   |  |
|---|---|--|
| 1) $\begin{cases} x \equiv 1 \pmod{8}, \\ x \equiv 2 \pmod{13}; \end{cases}$  | 3) $\begin{cases} x \equiv 1 \pmod{5}, \\ x \equiv 2 \pmod{6}, \\ x \equiv 3 \pmod{7}; \end{cases}$         | 5) $\begin{cases} 2x \equiv 1 \pmod{7}, \\ 3x \equiv 2 \pmod{11}, \\ 5x \equiv 3 \pmod{13}; \end{cases}$ |
| 2) $\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 4 \pmod{7}; \end{cases}$ | 4) $\begin{cases} x \equiv 3 \pmod{999}, \\ x \equiv 2 \pmod{1000}, \\ x \equiv 1 \pmod{1001}; \end{cases}$ | 6) $\begin{cases} 4x \equiv 7 \pmod{9}, \\ 3x \equiv 5 \pmod{16}, \\ 7x \equiv 2 \pmod{25}. \end{cases}$ |

**Задача 3.13.**

- Точка  $(a, b) \in \mathbb{Z}^2 \setminus \{0\}$  называется невидимой, если н.о.д.( $a, b$ ) > 1. Докажите, что для любого  $N \in \mathbb{N}$  найдётся такая пара чисел  $(u, v) \in \mathbb{N}^2$ , что все точки  $(u + i, v + j)$ ,  $0 \leq i < N$ ,  $0 \leq j < N$ , невидимы.
- Обобщите утверждение п. 1 на  $\mathbb{Z}^d$  с произвольным  $d \geq 2$ .

**Задача 3.14.** Решите системы сравнений:

$$1) \begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 19 \pmod{25}, \\ x \equiv 69 \pmod{125}; \end{cases} \quad 2) \begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 6 \pmod{9}, \\ x \equiv 15 \pmod{108}; \end{cases} \quad 3) \begin{cases} x \equiv 23 \pmod{120}, \\ x \equiv 143 \pmod{150}, \\ x \equiv 83 \pmod{180}. \end{cases}$$

**Задача 3.15.** Пусть модули  $m_1, \dots, m_n$  произвольны. Докажите, что система (3.1) разрешима тогда и только тогда, когда при всех  $i, j$  выполнено  $a_i \equiv a_j \pmod{\text{н.о.д.}(m_i, m_j)}$ , причём в этом случае общее решение имеет вид  $x \equiv x_0 \pmod{M}$ . Чему здесь равно  $M$ ?

## Ответы

**3.12:** 1)  $x \equiv 41 \pmod{104}$ ; 2)  $x \equiv 53 \pmod{210}$ ; 3)  $x \equiv -4 \pmod{210}$ ; 4)  $x \equiv 1002 \pmod{999\,999\,000}$ ; 5)  $x \equiv 921 \pmod{1001}$ ; 6)  $x \equiv 1111 \pmod{3600}$ .

**3.14:** 1)  $x \equiv 69 \pmod{125}$ ; 2)  $x \equiv 123 \pmod{216}$ ; 3)  $x \equiv 1343 \pmod{1800}$ .

**3.15:**  $M = \text{н.о.к.}(m_1, \dots, m_n)$ .

## 3.4 Бинарный алгоритм возведения в степень

**Задача 3.16.** Обоснуйте следующий алгоритм «быстрого» возведения в степень (по модулю).

**Дано:** целые числа  $a, N > 1, m \neq 0$ .

**Надо:** вычислить  $a^N \pmod{m}$ .

- 1) Представить  $N$  в двоичном виде:  $N = c_0 2^n + c_1 2^{n-1} + \dots + c_n, c_i \in \{0, 1\}, c_0 = 1$ .
- 2) Вычислить последовательно  $a_0, a_1, \dots, a_n$ :

$$\begin{aligned} a_0 &\equiv a \pmod{m}, \\ a_i &\equiv a_{i-1}^2 \cdot a^{c_i} \pmod{m}, \quad i = 1, \dots, n. \end{aligned}$$

- 3) Выполнено  $a^N \equiv a_n \pmod{m}$ .

Покажите, что для вычисления  $a^N \pmod{m}$  алгоритму требуется не более  $2 \log_2 N$  умножений (по модулю  $m$ ).

**Задача 3.17.** Вычислите с помощью алгоритма быстрого возведения в степень:

- 1)  $3^{13} \pmod{31}$ ;
- 2)  $2^{37} \pmod{101}$ ;
- 3)  $7^{49} \pmod{125}$ .

**Задача 3.18.** Придумайте алгоритм вычисления  $F_N \pmod{m}$  (где  $F_N$  —  $N$ -е число Фибоначчи), требующий не более  $C \log_2 N$  умножений и сложений по модулю  $m$ , где  $C$  — некоторая постоянная. (Подсказка. Подберите матрицу  $M$ , чтобы выполнялось  $\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = M \begin{pmatrix} F_{n-1} \\ F_{n-2} \end{pmatrix}$ .)

## Ответы

**3.17:** 1)  $24 \pmod{31}$ ; 2)  $55 \pmod{101}$ ; 3)  $107 \pmod{125}$ .

### 3.5 Теоремы Ферма и Эйлера

**Теорема Эйлера.** Пусть  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ , причём  $\text{н.о.д.}(a, m) = 1$ . Тогда

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

**Малая теорема Ферма.** Пусть  $p$  — простое число,  $a \in \mathbb{Z}$ , причём  $p \nmid a$ . Тогда

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Малая теорема Ферма** (альтернативная формулировка). Пусть  $p$  — простое число,  $a \in \mathbb{Z}$ . Тогда

$$a^p \equiv a \pmod{p}.$$

**Задача 3.19.** Докажите эквивалентность двух формулировок малой теоремы Ферма.

**Задача 3.20.** Докажите, что если  $a^{\varphi(m)} \equiv 1 \pmod{m}$ , то  $\text{н.о.д.}(a, m) = 1$ .

**Задача 3.21.** Пусть  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $\text{н.о.д.}(a, m) = 1$ . С помощью теоремы Эйлера получите формулу для  $a^{-1} \pmod{m}$ .

**Задача 3.22.** Убедитесь, что число  $2222^{5555} + 5555^{2222}$  делится на 7.

**Задача 3.23.** Докажите, что для произвольного целого  $n \geq 0$  справедливо сравнение

$$2^{2^{6n+2}} + 3 \equiv 0 \pmod{19}.$$

**Задача 3.24.** Посчитайте остатки от деления:

- |                           |                           |                            |
|---------------------------|---------------------------|----------------------------|
| 1) $3^{999}$ на 17;       | 3) $14^{24242}$ на 72;    | 5) $5^{14^{23}}$ на 37;    |
| 2) $41^{99999999}$ на 99; | 4) $123^{11111}$ на 2700; | 6) $12^{34^{56}}$ на 2925. |

**Задача 3.25.** Найдите три последние цифры числа  $2^{3^{57}}$  (в десятичной системе счисления).

**Задача 3.26** (малая теорема Ферма для многочленов). Пусть  $p$  — простое число,  $x_1, \dots, x_n$  — переменные. Докажите утверждения:

- 1) Справедливо сравнение

$$(x_1 + \dots + x_n)^p \equiv x_1^p + \dots + x_n^p \pmod{p},$$

то есть все коэффициенты многочлена  $(x_1 + \dots + x_n)^p - (x_1^p + \dots + x_n^p)$  делятся на  $p$ .

- 2) Для любого многочлена  $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$  справедливо сравнение

$$(f(x_1, \dots, x_n))^p \equiv f(x_1^p, \dots, x_n^p) \pmod{p}.$$

**Задача 3.27.**

- Допустим, что справедливо сравнение  $a \equiv b \pmod{p^n}$ , где  $a, b \in \mathbb{Z}$ ,  $p, n \in \mathbb{N}$ . Докажите, что  $a^p \equiv b^p \pmod{p^{n+1}}$ .
- Более того, пусть  $p$  — простое число,  $p^n \geq 3$  (то есть либо  $p > 2$ , либо  $p = 2$  и  $n > 1$ ),  $p \nmid a$ ,  $a \neq b$ . Докажите, что  $v_p(a^p - b^p) = v_p(a - b) + 1$ .
- Выведите из малой теоремы Ферма теорему Эйлера для  $m = p^n$  ( $p$  — простое число).

- 4) Покажите, что из справедливости теоремы Эйлера для  $m = p^n$  следует теорема Эйлера с произвольным  $m$ .
- 5) Пусть целое  $m \geq 8$  не имеет вид  $p^\alpha$  или  $2p^\alpha$ , где  $p > 2$  — простое число,  $\alpha \in \mathbb{N}$ . Докажите, что для любого  $a \in \mathbb{Z}$ , взаимно простого с  $m$ , справедливо сравнение

$$a^{\varphi(m)/2} \equiv 1 \pmod{m}.$$

**Задача 3.28.** Докажите, что для произвольных  $m \in \mathbb{N}$  и  $a \in \mathbb{Z}$  справедливо сравнение

$$\sum_{d|m} \mu(d) a^{m/d} \equiv 0 \pmod{m}.$$

**Задача 3.29.** Докажите, что для произвольных натуральных  $a_1, \dots, a_m$  справедливо сравнение

$$a_1^{a_2 \dots a_m} \equiv a_1^{a_2 \dots a_{m-1}} \pmod{m}.$$

## Ответы

**3.21:**  $a^{\varphi(m)-1} \pmod{m}$ .

**3.24:** 1) 11; 2) 62; 3) 16; 4) 27; 5) 12; 6) 2016.

**3.25:** 208.

## 3.6 Разное

**Задача 3.30.**

- 1) Пусть простое число  $p > 2$  делит число  $a^2 + 1$  при некотором  $a \in \mathbb{Z}$ . Докажите, что  $p \equiv 1 \pmod{4}$ . (*Подсказка.* Используйте малую теорему Ферма.)
- 2) Используя утверждение п. 1, докажите, что существует бесконечно много простых чисел вида  $4k + 1$  ( $k \in \mathbb{N}$ ).

**Теорема Вильсона.** Целое число  $n > 1$  является простым в том и только в том случае, когда справедливо сравнение

$$(n-1)! \equiv -1 \pmod{n}.$$

**Задача 3.31.** Пусть  $p > 2$  — простое число. Используя теорему Вильсона, докажите, что:

- 1) если  $p = 4k + 1$  ( $k \in \mathbb{N}$ ), то  $p \mid ((2k)!)^2 + 1$ ;
- 2) если  $p = 4k - 1$  ( $k \in \mathbb{N}$ ), то  $p \mid ((2k-1)!)^2 - 1$ .

## Тема 4

# Полиномиальные сравнения

### 4.1 Предварительные соображения

#### Понятие решения. Количество решений

**Задача 4.1.** Решите сравнения:

- |  |   |
|--|---|
| 1) $x^2 \equiv 0 \pmod{128}$ ;                                 | 4) $x^2 + 4x + 4 \equiv 0 \pmod{243}$ ;       |
| 2) $x^3 \equiv 0 \pmod{11^{11} \cdot 13^{31} \cdot 31^{13}}$ ; | 5) $x^3 - x \equiv 0 \pmod{343}$ ;            |
| 3) $x^5 \equiv 0 \pmod{12^{12}}$ ;                             | 6) $(x + 2)^3(x + 3)^2 \equiv 0 \pmod{5^5}$ . |

**Задача 4.2.** Сколько решений имеют сравнения из задачи 4.1?

#### Использование теоремы Эйлера

**Задача 4.3.** Используя теорему Эйлера (или малую теорему Ферма), решите сравнения:

- |  |  |
|--|--|
| 1) $x^6 + x^3 + x + 1 \equiv 0 \pmod{3}$ ;   | 4) $x^{100} + x^{50} + x^5 + 4 \equiv 0 \pmod{5}$ ;        |
| 2) $x^6 + x^3 + x + 2 \equiv 0 \pmod{3}$ ;   | 5) $x^{239} + x^{97} + 2 \equiv 0 \pmod{45}$ ;             |
| 3) $x^{42} + x^{13} + 1 \equiv 0 \pmod{9}$ ; | 6) $x^{141} + 3x^{94} + 3x^{47} + 1 \equiv 0 \pmod{144}$ . |

**Задача 4.4.** Пусть  $f(x_0) \equiv 0 \pmod{m}$  (где  $f(x) \in \mathbb{Z}[x]$ ,  $m \in \mathbb{N}$ ,  $x_0 \in \mathbb{Z}$ ), причём  $\text{н.о.д.}(f(0), m) = 1$ . Докажите, что  $\text{н.о.д.}(x_0, m) = 1$ .

#### Использование китайской теоремы об остатках

**Задача 4.5.** Пусть  $f(x) \in \mathbb{Z}[x]$ ,  $m_1, \dots, m_k \in \mathbb{N}$ , причём  $\text{н.о.д.}(m_i, m_j) = 1$  при всех  $i \neq j$ . Обозначим через  $N_i$  количество решений сравнения  $f(x) \equiv 0 \pmod{m_i}$ ,  $i = 1, \dots, k$ . Сколько решений имеет сравнение  $f(x) \equiv 0 \pmod{m}$  при  $m = m_1 \cdots m_k$ ?

**Задача 4.6.** Сколько решений имеет сравнение  $x^3 + 2x^2 - 3x \equiv 0 \pmod{75}$ ?

**Задача 4.7.** Используя китайскую теорему об остатках, решите сравнения:

- |   |   |
|---|---|
| 1) $x^2 + 2x + 12 \equiv 0 \pmod{15}$ ; | 3) $x^6 + 3x + 6 \equiv 0 \pmod{35}$ ;      |
| 2) $x^3 + 8x + 12 \equiv 0 \pmod{21}$ ; | 4) $x^{41} + x^4 + 1 \equiv 0 \pmod{105}$ . |

**Ответы**

**4.1:** 1)  $x \equiv 0 \pmod{16}$ ; 2)  $x \equiv 0 \pmod{11^4 \cdot 13^{11} \cdot 31^5}$ ; 3)  $x \equiv 0 \pmod{2^5 \cdot 3^3}$ ; 4)  $x \equiv -2 \pmod{27}$ ; 5)  $x \equiv 0, \pm 1 \pmod{343}$ ; 6)  $x \equiv -2 \pmod{25}$  или  $x \equiv -3 \pmod{125}$ .

**4.2:** 1) 8 решений; 2)  $11^7 \cdot 13^{20} \cdot 31^8$  решений; 3)  $2^{19} \cdot 3^9$  решений; 4) 9 решений; 5) 3 решения; 6) 150 решений.

**4.3:** 1)  $x \equiv 2 \pmod{3}$ ; 2) нет решений; 3)  $x \equiv 7 \pmod{9}$ ; 4)  $x \equiv 4 \pmod{5}$ ; 5)  $x \equiv -1 \pmod{15}$ ; 6)  $x \equiv -1 \pmod{12}$ .

**4.5:**  $N_1 \cdots N_k$  решений.

**4.6:** 6 решений.

**4.7:** 1)  $x \equiv 1, 6, 7, 12 \pmod{15}$ ; 2)  $x \equiv 1, 3 \pmod{7}$ ; 3) нет решений; 4)  $x \equiv 58, 88 \pmod{105}$ .

**4.2 Подъём решений**

Итак, благодаря китайской теореме об остатках, нам достаточно научиться решать сравнения вида  $f(x) \equiv 0 \pmod{p^n}$ , где  $p$  — простое число,  $n \in \mathbb{N}$ . Это можно делать с помощью метода *подъёма решений*. Краткое напоминание о том, как он работает, можно найти в приложении Б. Более внятно и подробно вам рассказывают на лекциях.

**Задача 4.8.** Используя метод подъёма решений, решите сравнения:

1)  $x^5 + x^3 + 3x + 1 \equiv 0 \pmod{32}$ ;

5)  $x^4 + x^2 + 3x + 13 \equiv 0 \pmod{27}$ ;

2)  $x^3 - 4x^2 + x - 6 \equiv 0 \pmod{81}$ ;

6)  $x^4 + x^2 + 3x + 13 \equiv 0 \pmod{81}$ ;

3)  $x^4 + x^2 + 6x + 1 \equiv 0 \pmod{27}$ ;

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

4)  $x^4 + x^2 + 6x + 1 \equiv 0 \pmod{81}$ ;

8)  $x^2 - 37 \equiv 0 \pmod{343}$ .

**Задача 4.9.** Используя все свои знания и умения, решите сравнения:

1)  $2x^2 + x + 21 \equiv 0 \pmod{432}$ ;

3)  $x^5 + 3x^3 + 56x + 15 \equiv 0 \pmod{75}$ ;

2)  $x^3 + 7x^2 + 5x + 29 \equiv 0 \pmod{270}$ ;

4)  $x^{3^{1001}} + 2 \equiv 0 \pmod{375}$ .

**Задача 4.10.** Решите системы сравнений:

$$1) \begin{cases} 2x^2 + 3x + 5 \equiv 0 \pmod{8}, \\ 5x^2 + 2x + 3 \equiv 0 \pmod{9}, \\ 3x^2 + 5x + 2 \equiv 0 \pmod{25}; \end{cases}$$

$$2) \begin{cases} x \equiv 3 \pmod{7}, \\ x^2 \equiv 44 \pmod{7^2}, \\ x^3 \equiv 111 \pmod{7^3}. \end{cases}$$

**Ответы**

**4.8:** 1)  $x \equiv 27 \pmod{32}$ ; 2)  $x \equiv 42 \pmod{81}$ ; 3)  $x \equiv 4 \pmod{9}$ ; 4) нет решений; 5)  $x \equiv 4, 7 \pmod{9}$ ; 6)  $x \equiv 16, 22 \pmod{27}$ ; 7)  $x \equiv 2 \pmod{3^{10}}$ ; 8)  $x \equiv \pm 123 \pmod{343}$ .

**4.9:** 1)  $x \equiv 25, 393 \pmod{432}$ ; 2)  $x \equiv 49, 157 \pmod{270}$ ; 3)  $x \equiv 10 \pmod{25}$  или  $x \equiv 1 \pmod{5}$ ; 4)  $x \equiv 322 \pmod{375}$ .

**4.10:** 1)  $x \equiv 291, 299, 1091, 1299 \pmod{1800}$ ; 2)  $x \equiv 17 \pmod{343}$ .

### 4.3 Сравнения второй степени. Символ Лежандра

В этом параграфе предполагается крепкое знание определений и основных свойств *квадратичных вычетов* и *квадратичных невычетов* (по нечётному простому модулю), а также *символа Лежандра*. Свойства символа Лежандра можно найти в приложении В. (Там же можно немного узнать про обобщение — *символ Якоби*.)

**Задача 4.11.** Вычислите символы Лежандра:

$$1) \left(\frac{111}{541}\right); \quad 2) \left(\frac{529}{601}\right); \quad 3) \left(\frac{2108}{2003}\right); \quad 4) \left(\frac{19525}{1847}\right).$$

**Задача 4.12.** Пусть  $a, b, c \in \mathbb{Z}$ ,  $m \in \mathbb{N}$ , причём  $\text{н.о.д.}(2a, m) = 1$ . Докажите, что сравнения  $ax^2 + bx + c \equiv 0 \pmod{m}$  и  $y^2 \equiv b^2 - 4ac \pmod{m}$  имеют одинаковое количество решений. (Подсказка. Выделите полный квадрат.)

**Задача 4.13.** Выясните, разрешимы ли сравнения (все модули простые):

$$\begin{array}{ll} 1) x^2 \equiv 68 \pmod{113}; & 3) x^2 + 7x + 45 \equiv 0 \pmod{409}; \\ 2) x^2 \equiv 219 \pmod{383}; & 4) 5x^2 + 11x - 91 \equiv 0 \pmod{379}. \end{array}$$

**Задача 4.14.** Пусть  $p > 2$  — простое число,  $a \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ . Докажите утверждения:

- 1) Для любого  $a$  сравнение  $x^2 \equiv a \pmod{p}$  имеет  $1 + \left(\frac{a}{p}\right)$  решений.
- 2) Если  $p \nmid a$ , то сравнение  $x^2 \equiv a \pmod{p^n}$  разрешимо тогда и только тогда, когда  $a$  является квадратичным вычетом по модулю  $p$ , причём в этом случае сравнение имеет два решения.

**Задача 4.15.** Выясните, сколько решений имеют сравнения:

$$\begin{array}{ll} 1) x^2 \equiv 881 \pmod{3125}; & 4) 6x^2 + x + 9 \equiv 0 \pmod{343}; \\ 2) x^2 \equiv 2 \pmod{65}; & 5) x^2 + 26 \equiv 0 \pmod{3150}; \\ 3) x^2 + 122 \equiv 0 \pmod{189}; & 6) x^2 \equiv 451 \pmod{900}. \end{array}$$

**Задача 4.16.** Опишите все простые числа  $p$ , для которых разрешимы сравнения:

$$\begin{array}{ll} 1) x^2 + 1 \equiv 0 \pmod{p}; & 5) x^2 + x + 1 \equiv 0 \pmod{p}; \\ 2) x^2 - 2 \equiv 0 \pmod{p}; & 6) x^2 + x - 1 \equiv 0 \pmod{p}; \\ 3) x^2 + 2 \equiv 0 \pmod{p}; & 7) x^2 + x + 2 \equiv 0 \pmod{p}; \\ 4) x^2 - 3 \equiv 0 \pmod{p}; & 8) 3x^2 + 2x + 1 \equiv 0 \pmod{p}. \end{array}$$

**Задача 4.17.**

- 1) Используя результат п. 1 задачи 4.16, докажите, что существует бесконечно много простых  $p \equiv 1 \pmod{4}$ . (См. также задачу 3.30.)
- 2) Используя результат п. 2 задачи 4.16, докажите, что существует бесконечно много простых  $p \equiv -1 \pmod{8}$ .
- 3) Используя результат п. 3 задачи 4.16, докажите, что существует бесконечно много простых  $p \equiv 3 \pmod{8}$ .
- 4) Используя результат п. 4 задачи 4.16, докажите, что существует бесконечно много простых  $p \equiv -1 \pmod{12}$ .

- 5) Используя результат п. 5 задачи 4.16, докажите, что существует бесконечно много простых  $p \equiv 1 \pmod{6}$ .
- 6) Используя результат п. 6 задачи 4.16, докажите, что существует бесконечно много простых  $p \equiv -1 \pmod{10}$ .

**Задача 4.18.** Пусть  $a, n$  — целые числа, причём  $a$  нечётно,  $n \geq 3$ . Докажите утверждения:

- Сравнение  $x^2 \equiv a \pmod{2^n}$  разрешимо тогда и только тогда, когда  $a \equiv 1 \pmod{8}$ . (Подсказка. Для доказательства достаточности используйте «подъём» в виде  $x_{n+1} = x_n + 2^{n-1}t$ .)
- Если сравнение  $x^2 \equiv a \pmod{2^n}$  разрешимо, то оно имеет четыре решения вида  $\pm x_0, \pm x_0 + 2^{n-1}$ . (Подсказка. Перепишите сравнение в виде  $x^2 \equiv x_0^2 \pmod{2^n}$ .)

*Замечание.* Попробуйте доказать достаточность в п. 1, используя п. 2.

**Задача 4.19.** Найдите количество решений сравнения

$$x^2 + 2x + 72 \equiv 0 \pmod{2^{2023} \cdot 151^{9000} \cdot 199^{100500}}$$

(числа 151 и 199 простые).

**Задача 4.20.** Пусть  $a, b, c \in \mathbb{Z}$ . Докажите, что сравнение  $(x^2 - ab)(x^2 - ac)(x^2 - bc) \equiv 0 \pmod{p}$  разрешимо при любом простом  $p$ .

**Задача 4.21.** Пусть  $p$  — простое число,  $a, b, c \in \mathbb{Z}$ , причём  $p \nmid ab$ . Докажите, что сравнение  $ax^2 + by^2 + c \equiv 0 \pmod{p}$  разрешимо (относительно переменных  $x, y$ ). (Подсказка. Перепишите сравнение в виде  $ax^2 \equiv -by^2 - c \pmod{p}$ .)

*Замечание.* Следующие задачи так или иначе связаны с символами Лежандра и Якоби.

**Задача 4.22.** Пусть  $p > 2$  — простое число. Докажите, что справедливо сравнение

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

**Задача 4.23.** Пусть  $p > 2$  — простое число,  $a, b \in \mathbb{Z}$ , причём  $p \nmid a$ . Докажите, что

$$\sum_{x=0}^{p-1} \left( \frac{ax+b}{p} \right) = 0.$$

**Задача 4.24.** Пусть  $P$  — нечётное натуральное число, не являющееся квадратом целого числа.

- Докажите, что найдётся целое  $a$ , такое что  $\left( \frac{a}{P} \right) = -1$ . (Подсказка. Используйте китайскую теорему об остатках.)
- Докажите, что в (любой) приведённой системе вычетов по модулю  $P$  ровно для половины чисел  $a$  выполняется  $\left( \frac{a}{P} \right) = -1$ . (Подсказка. Укажите явную биекцию между искомыми вычетами и всеми прочими.)
- (Правильно) обобщите утверждение задачи 4.23 на сумму символов Якоби  $\sum_{x=0}^{P-1} \left( \frac{ax+b}{P} \right)$ .

**Задача 4.25.** Вычислите сумму символов Якоби

$$\sum_{n=1}^{500} \left( \frac{1001}{2n-1} \right).$$

**Задача 4.26.** Докажите, что при любых  $a, b, c \in \mathbb{N}$  число  $c^2 + a$  не делится на  $4ab - 1$ . (Подсказка. Воспользуйтесь символом Якоби.)

**Ответы**

**4.11:** 1)  $-1$ ; 2)  $1$ ; 3)  $1$ ; 4)  $-1$ .

**4.13:** 1) нет; 2) да; 3) да; 4) нет.

**4.15:** 1) 2 решения; 2) нет решений; 3) 4 решения; 4) 2 решения; 5) 8 решений; 6) нет решений.

**4.16:** 1)  $p = 2$  или  $p \equiv 1 \pmod{4}$ ; 2)  $p = 2$  или  $p \equiv \pm 1 \pmod{8}$ ; 3)  $p = 2$  или  $p \equiv 1, 3 \pmod{8}$ ; 4)  $p = 2, 3$  или  $p \equiv \pm 1 \pmod{12}$ ; 5)  $p = 3$  или  $p \equiv 1 \pmod{3}$ ; 6)  $p = 5$  или  $p \equiv \pm 1 \pmod{5}$ ; 7)  $p = 7$  или  $p \equiv 1, 2, 4 \pmod{7}$ ; 8)  $p = 2$  или  $p \equiv 1, 3 \pmod{8}$ .

**4.19:** 16 решений.

**4.25:** 0.

## **Тема 5**

# **Первообразные корни (WIP)**

Как-нибудь потом.

## Тема 6

# Цепные дроби (TODO)

Мне лень.

# Приложение А

## Примеры задач для контрольных и зачётов

**Задача 1.** Решите в целых числах уравнение  $19x - 91y + 9 = 0$ .

**Задача 2.** Найдите количество (натуральных) делителей числа  $16!$  («16 факториал»).

**Задача 3.** Найдите количество общих (натуральных) делителей трёх чисел  $2^2 \cdot 3^3 \cdot 5^5 \cdot 7^7$ ,  $2^3 \cdot 3^7 \cdot 7^{11} \cdot 11^2$  и  $3^{11} \cdot 5^7 \cdot 7^5 \cdot 11^3$ .

**Задача 4.** Решите в целых числах уравнение  $66x + 108y - 150z - 36 = 0$ .

**Задача 5.** Является ли функция  $f(n) = \varphi(\varphi(n))$  мультипликативной?

**Задача 6.** Решите в натуральных числах уравнение  $\varphi(4^x 6^y) = 2 \varphi(35^z)$ .

**Задача 7.** Вычислите сумму  $\sum_{d|n} \mu(d) \sigma(d)$  при  $n = pq^{10}r^{100}s^{1000}t^{2023}$ , где  $p, q, r, s, t$  — различные простые числа.

**Задача 8.** Арифметическая функция  $f$  такова, что для всех  $n \in \mathbb{N}$  выполнено

$$\sum_{d|n} (-1)^d \mu\left(\frac{n}{d}\right) f(d) = n \mu(n).$$

Определите знак числа  $f(11!)$ .

**Задача 9.** Решите сравнение  $266x + 126 \equiv 0 \pmod{637}$ .

**Задача 10.** Найдите  $19^{-1} \pmod{101}$ .

**Задача 11.** Решите сравнение  $66x + 108y + 114 \equiv 0 \pmod{150}$ .

**Задача 12.** Решите систему сравнений

$$\begin{cases} x \equiv 6 \pmod{7}, \\ x \equiv 1 \pmod{8}, \\ x \equiv 7 \pmod{9}. \end{cases}$$

**Задача 13.** Найдите остаток от деления  $111^{22222}$  на 828.

**Задача 14.** Используя китайскую теорему об остатках и метод подъёма решений, решите сравнение  $x^3 + 11x^2 + 9x + 39 \equiv 0 \pmod{375}$ .

**Задача 15.** Сколько решений имеет сравнение  $x^4 - 5x - 6 \equiv 0 \pmod{100^{100}}$ ?

**Задача 16.** Разрешимо ли сравнение  $x^2 \equiv 2 \pmod{65}$ ?

**Задача 17.** Разрешимо ли сравнение  $x^2 + 6 \equiv 0 \pmod{987654323}$ ? (Число 987654323 простое.)

**Задача 18.** Найдите количество решений сравнения

$$x^2 + 2x + 72 \equiv 0 \pmod{2^{2023} \cdot 151^{9000} \cdot 199^{100500}}$$

(числа 151 и 199 простые).

**Задача 19.** Для каких простых чисел  $p$  разрешимо сравнение  $2x^2 + x + 1 \equiv 0 \pmod{p}$ ?

**Задача 20.** Вычислите сумму символов Лежандра

$$\sum_{x=1}^{316} \left( \frac{5x + 97}{317} \right).$$

**Задача 21.** Найдите первообразный корень по модулю 41.

**Задача 22.** Найдите первообразный корень по модулю 1250.

**Задача 23.** Докажите, что 123 — первообразный корень по модулю  $11^{11}$ .

**Задача 24.** Убедитесь, что 3 — первообразный корень по модулю 257, и с помощью этого знания решите в натуральных числах сравнение  $3^{10x-7} \equiv 27 \pmod{257}$ . (Число 257 простое.)

**Задача 25.** Решите сравнение  $x^{37} \equiv 27 \pmod{257}$ .

## Ответы

**1:**  $x = 57 + 91t, y = 12 + 19t, t \in \mathbb{Z}$ .

**2:** 5376.

**3:** 24.

**4:** мне лень решать.

**5:** нет.

**6:**  $(x, y, z) = (1, 2, 1)$ .

**7:**  $-pqrst$ .

**8:**  $f(11!) < 0$ .

**9:**  $x \equiv 57 \pmod{91}$ .

**10:**  $16 \pmod{101}$ .

**11:** см. задачу 4.

**12:**  $x \equiv 97 \pmod{504}$ .

**13:** 729.

**14:**  $x \equiv 61, 186 \pmod{375}$ .

**15:** 8 решений.

**16:** нет.

**17:** да.

**18:** 16 решений.

**19:**  $p \equiv 0, 1, 2, 4 \pmod{7}$ .

**20:** 1.

**21:** например, 6.

**22:** например, 627 или 3.

**24:**  $x = 1 + 128t, t \in \mathbb{N}_0$ .

**25:**  $x \equiv 3^7 \equiv 131 \pmod{257}$ .

# Приложение Б

## Подъём решений

Пусть  $f(x) \in \mathbb{Z}[x]$ . Мы хотим научиться решать сравнения вида

$$f(x) \equiv 0 \pmod{p^n}, \quad (\text{Б.1})$$

где  $p$  — простое число (для простоты),  $n \in \mathbb{N}$ .

Сравнение по простому модулю (то есть при  $n = 1$ ) мы будем решать простым (или не очень) перебором (число  $p$  у нас всегда будет небольшим).

Допустим, что мы как-то нашли все решения сравнения (Б.1) для некоторого  $n$ . Тогда решения  $x_{n+1}$  сравнения по модулю  $p^{n+1}$  нужно искать в виде

$$x_{n+1} = x_n + p^n t,$$

где  $x_n$  — какое-то решение сравнения по модулю  $p^n$ , а  $t$  пробегает полную систему вычетов по модулю  $p$  (например,  $0 \leq t \leq p-1$  или  $-p/2 < t \leq p/2$ ). *Важно*: нижний индекс  $n$  у  $x_n$  — это не номер решения; он просто указывает на то, для какого модуля это решение (разные решения можно обозначать через  $x_n, y_n, z_n$ , или  $x_n, x'_n, x''_n$ , или ещё как-нибудь). В итоге получаем сравнение (относительно переменной  $t$ )

$$f(x_n + p^n t) \equiv 0 \pmod{p^{n+1}}.$$

Оказывается, что это сравнение всегда линейно (решать линейные сравнения легко по любому модулю), а именно:

$$f(x_n) + f'(x_n)p^n t \equiv 0 \pmod{p^{n+1}} \iff \frac{f(x_n) \bmod p^{n+1}}{p^n} + f'(x_n)t \equiv 0 \pmod{p}, \quad (\text{Б.2})$$

где  $f(x_n) \bmod p^{n+1}$  значит, что  $f(x_n)$  достаточно вычислять по модулю  $p^{n+1}$ .

Отсюда уже можно сделать некоторые выводы:

- 1) Если  $f'(x_n) \not\equiv 0 \pmod{p}$ , то сравнение (Б.2) имеет единственное решение, то есть в этом случае решение  $x_n$  однозначно «поднимается» до решения  $x_{n+1}$ .
- 2) Если  $f'(x_n) \equiv 0 \pmod{p}$ , то сравнение (Б.2) не содержит  $t$ , поэтому всё зависит от  $f(x_n)$ :
  - а) если  $f(x_n) \not\equiv 0 \pmod{p^{n+1}}$ , то решений нет, то есть  $x_n$  «не поднимается» до решения сравнения по модулю  $p^{n+1}$ ;
  - б) если  $f(x_n) \equiv 0 \pmod{p^{n+1}}$ , то годится любое  $t$ , то есть решение  $x_n$  порождает  $p$  различных решений по модулю  $p^{n+1}$ .

Эту процедуру нужно проделать для каждого решения  $x_n$  сравнения (Б.1).

*Заключительное замечание:* если цепочка решений  $x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow \dots$  получена с помощью описанной выше процедуры *подъёма решений* (то есть  $x_2$  произошло из  $x_1$ ,  $x_3$  — из  $x_2$ , и т. д.), то  $x_1 \equiv x_2 \equiv x_3 \equiv \dots \pmod{p}$ , поэтому

$$f'(x_1) \equiv f'(x_2) \equiv f'(x_3) \equiv \dots \pmod{p},$$

то есть *производную достаточно считать только для  $x_1$* , а сравнение (Б.2) окончательно принимает вид

$$\overbrace{\frac{f(x_n) \bmod p^{n+1}}{p^n}}^{\text{считать нужно только это}} + \underbrace{f'(x_1)t}_{\text{не меняется}} \equiv 0 \pmod{p}, \quad x_1 \equiv x_n \pmod{p}.$$

В частности, если  $f'(x_1) \not\equiv 0 \pmod{p}$ , то решение  $x_1$  однозначно поднимается до решения по модулю  $p^n$  для любого  $n$ , то есть в классе вычетов  $x \equiv x_1 \pmod{p}$  сравнение (Б.1) имеет единственное решение.

*Замечание.* На самом деле от модуля  $p^n$  можно перейти сразу к  $p^{2n}$ :

$$\begin{aligned} f(x_n + p^n t) \equiv 0 \pmod{p^{2n}} &\iff f(x_n) + f'(x_n)p^n t \equiv 0 \pmod{p^{2n}} \\ &\iff \frac{f(x_n) \bmod p^{2n}}{p^n} + f'(x_n)t \equiv 0 \pmod{p^n}. \end{aligned}$$

Здесь  $t$  пробегает полную систему вычетов по модулю  $p^n$ , а производную нужно пересчитывать на каждом шаге. Для маленьких  $n$  игра не стоит свеч.

## Приложение В

# Памятка про символ Лежандра (и заодно про символ Якоби)

Пусть  $p > 2$  — простое число,  $a \in \mathbb{Z}$ . Символ Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } p \nmid a \text{ и сравнение } x^2 \equiv a \pmod{p} \text{ разрешимо,} \\ -1, & \text{если } (p \nmid a) \text{ сравнение } x^2 \equiv a \pmod{p} \text{ неразрешимо,} \\ 0, & \text{если } p \mid a. \end{cases}$$

Пусть  $P = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  — нечётное натуральное число,  $a \in \mathbb{Z}$ . Символ Якоби:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Избранные свойства символа Якоби (в частности символа Лежандра):

- 1)  $\left(\frac{a}{P}\right) = 0 \iff \text{н.о.д.}(a, P) > 1$ ;
- 2) если  $a \equiv b \pmod{P}$ , то  $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$ ;
- 3)  $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$ ;
- 4)  $\left(\frac{1}{P}\right) = 1$  (более общо:  $\left(\frac{a^2}{P}\right) = 1$  при  $\text{н.о.д.}(a, P) = 1$ );
- 5)  $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}} = \begin{cases} 1, & P \equiv 1 \pmod{4}, \\ -1, & P \equiv -1 \pmod{4}; \end{cases}$
- 6)  $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} = \begin{cases} 1, & P \equiv \pm 1 \pmod{8}, \\ -1, & P \equiv \pm 3 \pmod{8}; \end{cases}$
- 7) **квадратичный закон взаимности**: если  $P, Q$  — нечётные натуральные числа, то

$$\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \left(\frac{Q}{P}\right) = \begin{cases} -\left(\frac{Q}{P}\right), & P \equiv Q \equiv -1 \pmod{4}, \\ \left(\frac{Q}{P}\right) & \text{иначе;} \end{cases}$$

- 8) **критерий Эйлера для символа Лежандра**: если  $p > 2$  — простое число, то для произвольного  $a \in \mathbb{Z}$  выполнено  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ . (Для составного  $p$  это утверждение неверно!)