

## Числа 1

В этом листке все числа считаются целыми, если не сказано иного.

↪ **Определение 1.** *Простое число* – число, у которого ровно два натуральных делителя - 1 и оно само.

1. Докажите, что простых чисел бесконечно много.
2. Докажите, что при любых  $a$  и  $e$  в арифметической прогрессии вида  $a, a + e, a + 2e \dots$  содержится составное число.

↪ **Определение 2.** *Деление с остатком* числа  $a$  на натуральное число  $b$  называется нахождение таких чисел  $p, r$ , что выполнено  $0 \leq r < b, a = p \cdot b + r$ . Число  $r$  называется остатком. Иногда говорят, что  $a$  сравнимо с  $r$  по модулю  $b$

3. Докажите, что определение выше корректное, то есть для любой пары чисел  $a, b$  подходящая пара  $(p, r)$  существует и единственна.
4. Найдите результат деления с остатком

$$\bullet a = 5, b = 3 \quad \bullet a = 1537, b = 26 \quad \bullet a = -1537, b = 26$$

5. Найдите остаток от деления

- (a)  $8^{100}$  на 5
- (b)  $3^{4^5 6}$  на 7

Фразу  $a$  и  $b$  имеют одинаковые остатки при делении на  $c$  для краткости будем писать так:  $a \equiv b \pmod{c}$ , или  $a \equiv b \pmod{c}$ . Наибольший общий делитель (наибольшее натуральное число, на которое делятся числа) (НОД) будем писать просто как скобки:  $\text{НОД}(a, b) = (a, b)$ . Это обозначения, используемые далее в задачах, в своих решениях используйте что хотите.

6. Докажите, что если  $a \equiv b \pmod{n}, c \equiv d \pmod{n}$ , то:

- $\bullet a + c \equiv b + d \pmod{n}$
- $\bullet a \cdot c \equiv b \cdot d \pmod{n}$

7. Когда для числа  $a$  существует такое число  $b$ , что  $a \cdot b \equiv 1 \pmod{n}$ ?

- (a) Докажите, что  $(a, b) = (b, a - b)$ , теперь постройте алгоритм поиска НОДа двух чисел.
- (b) Найдите алгоритм решения в целых числах уравнения  $ax + by = (a, b)$  (Неизвестные здесь только  $x$  и  $y$ ).

Подсказка: запустите алгоритм из предыдущего пункта.

БОНУС: Напишите общий вид любого решения в целых числах такого уравнения.

с) Решите основную задачу.

8. Докажите, что уравнение  $ax \equiv b \pmod{p}, a \neq 0, p$  - простое, всегда

- (a) имеет решение.
- (b) имеет единственное решение.

- 
9. Докажите, что существует 1000 подряд идущих составных чисел

10. Докажите, что среди любых 10 последовательных чисел найдется число, взаимно простое с остальными.

## Числа 2

↪ **Определение 3.** *Вычетом* называется подмножество целых чисел, дающих одинаковые остатки по какому-либо фиксированному модулю. С ними можно делать те же операции, что и с целыми числами - складывать, умножать, возводить в степень. То, что это не число, а вычет, которому принадлежит это число, показывает черта над числом. При операциях с ними обычно используются т.н. *представители* - просто числа, имеющие нужный остаток. Например:

$$\overline{5} + \overline{7} \equiv \overline{12} \equiv \overline{2} \equiv \overline{-8} \pmod{10}$$

С ними связано множество теорем, используемых в современной криптографии и параллельных вычислениях.

– Это законно вообще?

– Да, в предыдущем листке в задачах доказывается корректность сложения и умножения.

↪ **Определение 4.** *Нулевой вычет:* Вычет чисел, которые делятся на значение модуля.

↪ **Определение 5.** *Обратным вычетом*  $a^{-1}$  для  $a$  называется такой вычет  $b$ , что  $a \cdot b \equiv 1 \pmod{n}$ . Вычет, у которого есть обратный, называется обратимым.

1. Докажите, что у любого ненулевого вычета по простому модулю  $p$  есть обратный.

2. Докажите, что у любого вычета может быть не более одного обратного.

3. Решите уравнения:

$$\bullet \overline{5}x \equiv \overline{3} \pmod{7} \quad \bullet x^2 \equiv \overline{0} \pmod{4} \quad \bullet x^2 \equiv \overline{1} \pmod{24}$$

4. (*Теорема Вильсона*) Пусть  $p$  - простое, тогда:

$$(p-1)! \equiv -1 \pmod{p}$$

5. (*Малая Теорема Ферма*) Пусть  $p$  - простое,  $c$  не кратно  $p$ . Тогда

$$c^{p-1} \equiv 1 \pmod{p}$$

6. (*Китайская Теорема об остатках*) Пусть  $m_1, m_2$  - взаимно простые,  $r_1, r_2$  - вычеты по модулям  $m_1, m_2$  соотв. Тогда существует и единственно такое  $a$ , что

$$\begin{cases} a \equiv r_1 \pmod{m_1} \\ a \equiv r_2 \pmod{m_2} \end{cases}$$

а) Докажите, что такого  $a$  в промежутке чисел  $[0, m_1 \cdot m_2)$  существует не более одного для фиксированного набора остатков  $r_1, r_2$ ;

б) Докажите утверждение теоремы;

с) Обобщите теорему для случая  $n$  чисел.

↪ **Определение 6.** *Функция Эйлера*  $\varphi(n)$  - функция от натурального числа, обозначающая количество чисел от 1 до  $n$ , взаимно простых с  $n$ .

7. Посчитайте значения функции Эйлера:

$$\bullet \varphi(5) \quad \bullet \varphi(16) \quad \bullet \varphi(30) \quad \bullet \varphi(p^n), p - \text{простое}$$

8. Докажите, что для взаимно простых  $a, b$  выполняется:  $\varphi(a) \cdot \varphi(b) = \varphi(ab)$

9. (*Теорема Эйлера*) Докажите, что если  $(a, n) = 1$ , то  $a^{\varphi(n)} \equiv 1 \pmod{n}$

Указание: рассмотрите все вычеты, взаимно простые с  $n$ .