Лекция 4. Введение в теорию чисел. Функция Эйлера. Малая теорема Ферма.

#вшпи #дискретная_математика #теория

Автор конспекта: Гридчин Михаил

Общие понятия о числах

1. Делимость (a делится на $b \iff a = bc$)
2. Деление с остатком ($a = bq + r, \quad q, r \in \mathbb{Z}, \quad 0 \le r < |b|$). Например, $-5 = 2(-3) + 1$.
3. Простое число p - нет натуральных делителей кроме 1 и p. 1 - не простое число.
4. $\text{НОД}(a, b) = d, d \in \mathbb{N}$: 1) $a = da', b = db'$. 2) d - наибольший. 2') Любой общий делитель a и b является делителем d.
5. Числа a и b - взаимно просты, если $\text{НОД}(a, b) = 1$.
6. Если $\text{НОД}(a, b) = 1$ и $ac \mid b$. (ac делится на b), то $c \mid b$.
7. $\text{НОК}(a, b)$ - наименьшее $m \in \mathbb{N} : m \mid a, m \mid b$. $\text{НОК}(a, b) = \frac{ab}{\text{НОД}(a,b)}$
8. ***Теорема (основная теорема арифметики)***. Любое $m \in \mathbb{N}$ представимо единственным образов в виде произведения простых делителей.

$$m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

   Где p_i - простое, $k_i \in \mathbb{N}$.

p - простые числа

Утверждение. Количество простых чисел на $[1, n]$ обозначим, как $\pi(n)$. Тогда

$$\frac{\pi(n)}{n / \ln n} \to 1, n \to \infty$$

То есть $\pi(n) \sim \frac{1}{\ln n}$.

Def. $a \equiv b \pmod m \iff a - b \mid m$.
Свойства.

$$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod m \\ ac \equiv bd \pmod m \end{cases}$$

$$\begin{cases} ac \equiv bc \pmod m \\ \boxed{(c, m) = 1} \end{cases} \implies ac - bc \mid m \implies (a - b)c \mid m \implies a - b \mid m \implies \boxed{a \equiv b \pmod m}$$

Из алгоритма Евклида $(a, b) = (a - b, b) = \ldots = d = xa + yb$

Обратимость остатков. Рассмотрим уравнение

$$ax \equiv 1 \pmod p \iff \begin{cases} a \mid p \implies \varnothing \\ a \nmid p \implies (a,p) = 1 \implies \exists x, y \in \mathbb{Z} : ax + py = 1 \end{cases}$$

Рассмотрим последнее по модулю p:

$$ax \equiv 1 \pmod p$$

Другой способ решения: $a \nmid p \implies (a,p) = 1$. Рассмотрим различные ненулевые остатки от деления на p и всевозможные умножения a на $x < p$:

$$\begin{matrix} 1, & 2, & 3, & \dots, & p-1 \\ 1a, & 2a, & 3a, & \dots, & a(p-1) \end{matrix}$$

Докажем, что $\nexists i, j : ai \equiv aj \pmod p$. Действительно, тогда $a(i-j) \equiv 0 \pmod p$. Но $(a,p) = 1 \implies (i-j) \mid p$, но $i < p$ и $j < p$. Следовательно, $i = j$, что и требовалось. Следовательно, все остатки от деления ax на p - это какая-то перестановка чисел от 1 до p. То есть найдётся такое число $t \in \{1, 2, \dots, p\} : ta \equiv 1 \pmod p$ - что и требовалось доказать.

Последний способ доказательства можно применить для лёгкого доказательства малой теоремы Ферма.

Теорема (малая теорема Ферма). $a^{p-1} \equiv 1 \pmod p$.
□ Поскольку $1a, 2a, \dots, a(p-1)$ дают все остатки от деления на p, то

$$1 \cdot 2 \cdot \ldots (p-1) \equiv a \cdot 2a \cdot \ldots (p-1)a \equiv a^{p-1} \cdot 1 \cdot 2 \ldots (p-1) \pmod p$$

Но из свойства арифметики по модулю поскольку $(1 \cdot 2 \cdot \ldots (p-1), p) = 1$, то $a^{p-1} \equiv 1 \pmod p$ ■

Теорема (теорема Вильсона).

$$(m-1)! \equiv -1 \pmod m \iff \text{m - простое}$$

□
ШАГ1. Доказательство слева направо. Пусть m - составное. Это значит, что среди $(m-1)!$ есть делители m. То есть $(m, (m-1)!) =: d \neq 1$. Перепишем формулировку теоремы в следующем виде:

$$(m-1)! + 1 = mk$$

Получаем, что $(m-1)! \mid d$, $mk \mid d$, но $1 \nmid d \implies$ противоречие.
ШАГ2. Доказательство справа налево. Пусть m - простое. Рассмотрим все ненулевые остатки от деления на m:

$$1, 2, 3, \dots, (m-1) \quad (*)$$

Из обратимости остатков по простому модулю
$\forall a \in \{1, \dots, m-1\} \exists x : a \cdot x \equiv 1 \pmod{m-1}$.
Начнём сопоставлять эти остатки. Числу $a = 1$ сопоставим $x = 1$, числу $a = 2$ сопоставим $x = x_2$, ..., числу $a = (m-1)$ сопоставим $x = (m-1)$. Несколько утверждений, связанные с сопоставлением:

1. x определён однозначно для любого a. Потому что если
$$ax \equiv ay \pmod{m} \implies x \equiv y \pmod{m} \implies x = y$$
2. Разным a соответствуют разные x. Аналогично если
$$a_1 x \equiv a_2 x \pmod{m} \implies a_1 \equiv a_2 \pmod{m} \implies a_1 = a_2$$
3. Если $t^2 \equiv 1 \pmod{m}$, то
$$(t-1)(t+1) \equiv 0 \pmod{m} \implies \left[\begin{array}{c} t \equiv 1 \pmod{m} \\ t \equiv m-1 \pmod{m} \end{array}\right.$$
Это значит, что кроме $a = 1$ и $a = (m-1)$ абсолютно все остальные остатки разбились на пары, причём взаимно однозначно. Это значит, что если мы возьмём произведение всех остатков, то каждый из остатков $\in \{2, 3, \dots, (m-2)\}$ при умножении на свою пару даст 1. То есть
$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (m-2) \cdot (m-1) \equiv 1 \cdot (m-1) \equiv m-1 \equiv -1 \pmod{m}$$
■

Def. Функция Эйлера $\phi(n)$ - количество чисел ($\mathbb{N}$), меньших n и взаимно простых с ним.
Свойства.

- $\phi(p) = p - 1$.
- $\phi(p^2) = p^2 - p = p(p-1)$
- $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
- Если $(m, n) = 1$, то $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

□
ШАГ1. Рассмотрим сначала два простых p_1, p_2. Заметим, что среди чисел $1, 2, \dots p_1 p_2$ нет чисел, которые делятся и на p_1, и на p_2 одновременно кроме $p_1 p_2$.
То есть $\phi p_1 p_2 = p_1 p_2 - p_1 - p_2 + 1 = \phi(p_1)\phi(p_2)$.

ШАГ2. Докажем теперь в общем случае. Поскольку $(m, n) = 1$, то $\exists x, y \in \mathbb{Z} : mx + ny = 1$.
Тогда $\forall a \in \mathbb{Z}, \exists x_a, y_a \in \mathbb{Z} : mx_a + ny_a = a$.
Рассмотрим $mx + ny$ по-другому. Пусть $x \in \{0, \dots, n-1\}$, $y \in \{0, \dots, m-1\}$. Тогда выражение примет nm значений. Покажем, что это все возможные остатки от деления nm
.

Пусть $mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{mn}$. Но тогда
$m(x_1 - x_2) + n(y_1 - y_2) \equiv 0 \pmod{mn} \implies (x_1 - x_2) \mid n, (y_1 - y_2) \mid m$. Но тогда
$x_1 = x_2, y_1 = y_2$
Значит, не может быть так, что разные пары чисел (x, y) дают одинаковый остаток на
$mn \implies mx + ny$ - все возможные остатки от деления на mn.
Рассмотрим ряд чисел:

$$1, 2, 3, \dots, t, \dots, mn$$

Рассмотрим среди всех чисел от 1 до mn произвольное число t. Из только что доказанного

$$t \equiv mx + ny \pmod{mn}$$

То есть такие x, y существуют. Осталось понять, является ли t таким, что $(t, mn) = 1$.
От противного пусть

$$(t, mn) =: d \neq 1 \implies \left[\begin{array}{l}(t, m) \neq 1 \\ (t, n) \neq 1\end{array}\right.$$

$(t, n) = 1 \iff (x, n) = 1$. $((m, n) = 1 \implies x \text{ не имеет ни одного делителя с n})$.
$(t, m) = 1 \iff (y, m) = 1$.
Значит, чтобы $(t, mn) = 1$, требуется, чтобы $(x, n) = 1$ и $(y, m) = 1$. Таких чисел x ровно $\phi(n)$, таких чисел y ровно $\phi(m) \implies$ таких чисел t всего $phi(n) \cdot \phi(m)$. ∎