Билет 8. Модульная арифметика. Сравнимость по модулю, полная и приведенная системы вычетов. Теоремы Эйлера и Ферма.

Определение

Числа a и b **сравнимы по модулю** m ($a \equiv b \pmod{m}$), если:

- Они дают одинаковый остаток при делении на m
- $a = b + mt$ для некоторого целого t
- $m \mid (a - b)$ (m делит $a - b$)

Полная система вычетов

Определение

Класс вычетов — множество всех чисел, сравнимых по модулю m.
Полная система вычетов — набор из m чисел, взятых по одному из каждого класса.

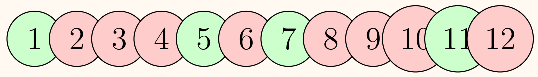
Приведенная система вычетов

Определение

Приведенная система вычетов — набор из $\phi(m)$ чисел, взаимно простых с m, взятых по одному из каждого соответствующего класса.

Пример

Приведенная система вычетов по модулю 12:
Числа, взаимно простые с 12: 1, 5, 7, 11
$\phi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4$



Взаимно простые с 12
Не взаимно простые с 12

Теорема Эйлера

Теорема

Если $m > 1$ и $(a, m) = 1$, то:

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

Доказательство

Доказательство:
Пусть $r_1, r_2, \ldots, r_{\phi(m)}$ — приведенная система вычетов.
Тогда $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ — тоже приведенная система (возможно, в другом порядке).
Следовательно:

$$(a \cdot r_1)(a \cdot r_2) \cdots (a \cdot r_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

$$a^{\phi(m)} \cdot (r_1 r_2 \cdots r_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

Так как $(r_i, m) = 1$, можем сократить:

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

Пример

Вычислить $11^{219} \pmod{91}$**:**
$91 = 7 \cdot 13$, $\phi(91) = 6 \cdot 12 = 72$
$(11, 91) = 1$, тогда по теореме Эйлера:

$$11^{72} \equiv 1 \pmod{91}$$

$$
\begin{aligned}
11^{219} &= 11^{72\cdot 3+3} \\
&= (11^{72})^3 \cdot 11^3 \\
&\equiv 1^3 \cdot 11^3 \pmod{91} \\
&= 1331 \equiv 57 \pmod{91}
\end{aligned}
$$

Ответ: 57

$$\boxed{11^{219}} \longrightarrow \boxed{11^{72\cdot 3+3}} \longrightarrow \boxed{(11^{72})^3 \cdot 11^3} \longrightarrow \boxed{1 \cdot 1331} \longrightarrow \boxed{57}$$

Теорема Ферма

Теорема

Если p — простое и p не делится на a, то:

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

Доказательство

Доказательство: Следует из теоремы Эйлера, так как для простого p:

$$\phi(p) = p - 1$$

Пример

Пример для $p = 7$, $a = 3$:

$$3^6 = 729 \equiv 1 \pmod{7}$$

Проверка: $729 \div 7 = 104$ остаток 1