Лекция 6, ДМиТИ

Вспоминаем: $x \underset{m}{\equiv} y$ (опр: $x - y \vdots m$, $x \bmod m = y \bmod m$)

Вычисления по модулю

Пример $2^{100} \bmod 3 = ?$

$2 \underset{3}{\equiv} -1$ (-3; $2-(-1)=3 \vdots 3$)

$2 \underset{3}{\equiv} 2$

$4 = 2^2 \underset{3}{\equiv} 1$

$8 = 2^3 \underset{3}{\equiv} 2$

закономерная

$\Rightarrow$ (св-ва степ) $2^{100} \underset{3}{\equiv} (-1)^{100} = 1 \Rightarrow 2^{100} \underset{3}{\equiv} 1 \Rightarrow 2^{100} \bmod 3 = 1 \bmod 3 = 1$

Ответ: $2^{100} \bmod 3 = 1$

Или $2^{100} \underset{3}{\equiv} 4^{50} \underset{3}{\equiv} 1^{50} \equiv 1$.

Пример 2 $1^{10} + 2^{10} + 3^{10} \bmod 5 = ?$

$1^{10} \underset{5}{\equiv} 1 \quad 2^{10} \underset{5}{\equiv} (2^2)^5 \underset{5}{\equiv} 4^5 \underset{5}{\equiv} (-1)^5 \underset{5}{\equiv} -1$

т.к. $4 \underset{5}{\equiv} -1$

$3^{10} \underset{5}{\equiv} (3^2)^5 \underset{5}{\equiv} 9^5 \underset{5}{\equiv} (-1)^5 \underset{5}{\equiv} -1$

неполное частное, ост

$1^{10} + 2^{10} + 3^{10} \underset{5}{\equiv} 1 + (-1) + (-1) \underset{5}{\equiv} -1 \underset{5}{\equiv} 4$

$-1 = 5(-1) + 4$

$\Rightarrow 1^{10} + 2^{10} + 3^{10} \bmod 5 = -1 \bmod 5 = 4$

Ответ: 4

Алгоритм быстрого возведения в степень

Дано $a \in \mathbb{Z}$, $n, m \in \mathbb{N}$ Посчитать $a^n \bmod m = ?$

Надо вычислить $a^n \bmod m = ?$

$A^N \cdot B \underset{m}{\equiv} C$ — будет инвариант

(утверждение, которое верно на каждом шаге)

Сначала: $A := a$, $N := n$, $B := 1$

C - неизвестное число, ответ в задаче

Проверим, что сначала инвариант выполняется:

$A^N \cdot B \underset{m}{\equiv} C \iff a^n \cdot 1 \underset{m}{\equiv} C$ ✓ т.к. c - ответ

Шаг алгоритма.

Если N - чёт, то $A_{k+1} := A_k^2 \bmod m$, $B_{k+1} := B_k \bmod m$, $N_{k+1} := N_k / 2$

Проверяем, что Инвариант не испортился

Было: $A_k^{N_k} \cdot B_k \underset{m}{\equiv} C$ - верно

Стало $A_{k+1}^{N_{k+1}} \cdot B_{k+1} \underset{m}{\equiv} (A_k^2)^{N_k/2} \cdot B_k \underset{m}{\equiv} A_k^{N_k} \cdot B_k \underset{m}{\equiv} C$

Если N-нечет, то $A_{k+1} := A_k \bmod m$, $B_{k+1} := B_k \cdot A_k \bmod m$, $N_{k+1} := N_k - 1$

Проверяем.

Было $A_k^{N_k} \cdot B_k \underset{m}{\equiv} C$ - верно

Стало $A_{k+1}^{N_{k+1}} B_{k+1} \underset{m}{\equiv} A_k^{N_k - 1} \cdot B_k \cdot A_k \underset{m}{\equiv} A_k^{N_k} B_k \underset{m}{\equiv} C$

Продолжаем, пока N_k не станет равен 0.

(Натуральные числа не могут постоянно уменьшаться)

$A_k^{N_k} \cdot B_k \underset{m}{\equiv} C \Rightarrow B_k \underset{m}{\equiv} C$

Ответ: B_k.

Пример $3^{22} \bmod 7 = ?$

$A^N \cdot B = 3^{22} \cdot 1 \underset{7}{\equiv} 2^{11} \cdot 1 \underset{7}{\equiv} 2^{10} \cdot 2 \underset{7}{\equiv} 4^5 \cdot 2 \underset{7}{\equiv} 4^4 \cdot 1 \underset{7}{\equiv} 2^2 \cdot 1 \underset{7}{\equiv} 4^1 \cdot 1 \underset{7}{\equiv} 4^0 \cdot 4$

22-чет
$3^2 \bmod 7 = 2$

11-Нечет
$1 \cdot 2 = 2$

10-чет
$2^2 \bmod 7 = 4$

5-Нечет
$4 \cdot 2 \bmod 7 = 8 \bmod 7 = 1$

4-чет
$4^2 \bmod 7 = 16 \bmod 7 = 2$

2-чёт

1-Нечет
$4 \cdot 1 \bmod 7 = 4$

Теперь $N = 0$. Ответ: 4 ■

Посчитаем кол-во шагов алгоритма (быстрого возведения в степень.

За каждые два шага N уменьшается в 2 раза.

т.е. $N_{k+2} < N_k / 2$

Значит, $N < 2^{\lceil \log_2 N \rceil}$

округлил вверх

$N = 2^{\log_2 N}$

1) N_k - чёт
$N_{k+1} = N_k / 2$
$N_{k+2} < N_k / 2$

2) N_k - Нечет
$N_{k+1} = N_k - 1$ - чет
$N_{k+2} = \frac{N_k - 1}{2} < \frac{N_k}{2}$

$N_{1+2\lceil \log_2 n \rceil} < N_1 / 2^{\lceil \log_2 n \rceil} < n / n = 1$

т.е. $2\lceil \log_2 n \rceil$ шагов точно хватает

$3 \log_2 n \approx \log_{10} n \approx$ кол-во цифр

$2 \log_2 n \approx 2/3$ кол-ва цифр числа

$n = N_1$

$N_3 < N_1 / 2$

$N_5 < N_3 / 2 < n / 4$

$N_7 < N_5 / 2 < n / 8$

$N_9 < N_7 / 2 < n / 16$

$N_{1+2a} < n / 2^a \le 1$

$N_{1+2\lceil \log_2 n \rceil} < n / 2^{\lceil \log_2 n \rceil}$

обычное возведение в степень, умножение в цикле n раз — n шагов. $n \gg 2\log_2 n$

Теперь,

Деление по модулю

Обычное деление x/y : Найти z : $x = yz$

Деление по модулю $\frac{x}{y} \bmod m$ Найти z : $x \underset{m}{\equiv} yz$

Пример $\frac{1}{2} \bmod 3$ $1 \underset{3}{\equiv} 2z$ ответ $z=2$ $1 \equiv 2 \cdot 2$

~~$z = 5$~~ $\not\equiv_3$ $1 \underset{3}{\equiv} 2 \cdot 5 = 10$

Пример $\frac{5}{7} \bmod 9$ $5 \underset{9}{\equiv} 7z$ Ответ: $z=2$ $5 \underset{9}{\equiv} 7 \cdot 2$

Утв. Делим x на y mod m

Ищем z: $x \underset{m}{\equiv} yz$

Если $(m, y) = 1$, то

модуль и делитель

$\exists z : x \underset{m}{\equiv} yz$ и $\forall z_1, z_2$ — выходят $z_1 \underset{m}{\equiv} z_2$

Другими словами $\exists!$ результат деления по модулю m

Округление

ceil $\lceil x \rceil$ - вверх

floor $\lfloor x \rfloor$ - вниз

$[x]$ - вниз "целая часть"

$\lceil 2{,}5 \rceil = 3$

$\lfloor 2{,}5 \rfloor = 2$

$[2{,}5] = 2$

$\lfloor -2{,}5 \rfloor = -3$

$\lceil -2{,}5 \rceil = -2$

$[-2{,}5] = -3$

Д-во. $x \underset{m}{\equiv} yz \iff x - yz \vdots m$

$\iff \exists k : x - yz = km \iff$

$\iff x = km + yz$

m, x, y — известны

k, z — не известны

— это диофантово уравнение

если $(m, y) = 1 \Rightarrow x : 1 \Rightarrow$ решение есть

(это условие ∃ решения диоф ур-ия)

Общий вид решения: $\begin{cases} z = z_0 + \xi \cdot {}^{n}/_{1} \\ k = k_0 - \xi \cdot {}^{y}/_{1} \end{cases}$ $\xi \in \mathbb{Z}$ – не интересно

т.е. $z = z_0 + \xi n \Rightarrow z \underset{n}{\equiv} z_0$ ∎