Было: деление по модулю

Делим $\boxed{3/7 \bmod 11}$: $\frac{3}{7} \underset{11}{\equiv} x \iff \boxed{3 \underset{11}{\equiv} 7x}$

приводим к диофантову уравнению:

$$7x - 11y = 3$$

решаем через Расш. АЕ ← универсальный для компьютера способ.

При небольших числах можно решать так:

$$3 \underset{11}{\equiv} 7x \underset{3 \underset{11}{\equiv} 14}{\iff} 14 \underset{11}{\equiv} 7x \iff \boxed{2 \underset{11}{\equiv} x}$$

сокращение на 7, и $(7,11)=1$

т.е. x единственный mod 11, он $x \underset{11}{\equiv} 2$

но по модулю таких x много $x=2, x=13, x=24$ и т.д.

Деление, если делитель не взаимно прост с модулем.

Пытаемся делить:

$$\frac{a}{b} \bmod m, \quad \exists\ (b,m)=d$$

$$a \underset{m}{\equiv} bx \iff a-bx \vdots m \iff \exists y.\ a-bx = my$$

$\iff a = bx+my$ – это диофантово уравнение
a, b, m – знаем
x, y – неизвестные

Чтобы было решение, нужно, чтобы $a \vdots (b,m)=d$
$\exists$ делите, т.е. решения есть. Сколько их?

Общий вид решения: $\begin{cases} x = x_0 + m/d \cdot \xi \\ y = y_0 - b/d \cdot \xi \end{cases}$ $\xi \in \mathbb{Z}$ – не интересно

Итого, по модулю m есть решения:

1) $x \underset{m}{\equiv} x_0$, 2) $x \underset{m}{\equiv} x_0 + m/d$ 3) $x \underset{m}{\equiv} x_0 + 2\,m/d$ ...

$s=1$ $s=2$

при $d=1$

$x \equiv x_0 + m \underset{m}{\equiv} x_0$

d) $x \underset{m}{\equiv} x_0 + \underbrace{(d-1) \cdot m/d}_{<m}$

$x \underset{m}{\equiv} x_0 + d\,m/d = x_0 + m \underset{m}{\equiv} x_0$

– не новое решение

Итого, d решений. Остальные решения сравнимы с одним из предыдущих.

<u>Th.</u> При делении a на b mod m, если $(b, m) = d$, получите

$$\begin{cases} 0 \text{ решений, если } a \not\vdots\, d \\ d \text{ решений, если } a \,\vdots\, d \end{cases}$$

<u>Пример.</u>

1) $7/8 \mod 20$ $a=7$

$d = (8, 20) = 4$

$7 \underset{20}{\equiv} 8x$ $7 \not\vdots\, 4 \Rightarrow 0$ решений

2) $12/8 \mod 20$

$12 \underset{20}{\equiv} 8x \mod 20$

$12-(-8)=20 \,\vdots\, 20$

$x_0 = -1$ – подобрали. $12 \underset{20}{\equiv} -8$

$-1 \underset{20}{\equiv} 19$

Ответы: $x \underset{20}{\equiv} -1$, $x \underset{20}{\equiv} 4$ $x \underset{20}{\equiv} 9$ $x \underset{20}{\equiv} 14$ $x \underset{20}{\equiv} 19$

$m/d = 20/4 = 5$

4 ответа: $12 \underset{20}{\equiv} 8x$

$x=-1$	$x=4$	$x=9$	$x=14$
$12 \underset{20}{\equiv} -8$	$12 \underset{20}{\equiv} 32$	$12 \underset{20}{\equiv} 72$	$12 \underset{20}{\equiv} 112$

Китайская теорема об остатках

Пусть есть система сравнений:

$$\begin{cases} x \underset{m_1}{\equiv} a_1 \\ x \underset{m_2}{\equiv} a_2 \\ \vdots \\ x \underset{m_n}{\equiv} a_n \end{cases}$$

пример

$$\begin{cases} x \underset{5}{\equiv} 2 \\ x \underset{9}{\equiv} 6 \\ x \underset{11}{\equiv} 9 \end{cases}$$

Th. Если $\forall i\ m_i \in \mathbb{N}$, $\underbrace{\forall i, j\ i \neq j\ (m_i, m_j)}_{\text{модули попарно взаимно просты}}$

$a_i \in \mathbb{Z}$

Тогда $\exists!$ решение системы mod M, где $M = m_1 m_2 \dots m_n$

В примере: $\exists!$ решение mod $M = 5 \cdot 9 \cdot 11 = 45 \cdot 11 = 495$

Подберём. попробуем 42 - подходит

$x \underset{495}{\equiv} 42$ $\left(\begin{array}{ll} x = 42 & x = 42 + 2 \cdot 495 \\ x = 42 + 495 & \dots \end{array} \right)$

Д-во. конструктивно

1) $M_i := M / m_i$

$M_1 = \frac{m_1 m_2 m_3}{m_1} = m_2 m_3 = 9 \cdot 11 = 99$

$M_2 = m_1 m_3 = 5 \cdot 11 = 55$

$M_3 = m_1 \cdot m_2 = 5 \cdot 9 = 45$

2) Делим $\frac{a_i}{M_i}$ mod m_i

$M_i x_i \underset{m_i}{\equiv} a_i$

деление однозначно определено, т.к. $(m_i, M_i) = 1$

i) $99 x_1 \underset{5}{\equiv} 2$ $\Rightarrow$ $x_1 \underset{5}{\equiv} -2$

$-1 \cdot x_1 \underset{5}{\equiv} 2$, т.к. $99 \underset{5}{\equiv} -1$

$55 x_2 \underset{9}{\equiv} 6$ $\Rightarrow$ $x_2 \underset{9}{\equiv} 6$

$1 x_2 \underset{9}{\equiv} 6$ т.к. $55 \underset{9}{\equiv} 1$

$45 x_3 \underset{11}{\equiv} 9$

объяснение:

$\exists\,(m_i, \underbrace{m_1 m_2 \ldots \cancel{m_i} \ldots m_n}) = d \,\vdots\, p > 1$ простое

$d \neq 1$

$1x_3 \equiv_{11} 9 \Rightarrow x_3 \equiv_{11} 9$

$m_i \,\vdots\, p \quad m_1 m_2 \ldots m_n \,\vdots\, p \Rightarrow \exists j \quad m_j \,\vdots\, p$

$\Rightarrow (m_i, m_j) \,\vdots\, p$?? – противоречие

3) Ответ $X \equiv_M M_1 x_1 + M_2 x_2 + \ldots + M_n x_n$

3) $X \equiv_{495} 99 \cdot (-2) + 55 \cdot 6 + 45 \cdot 9$

$= -198 + 330 + (360 + 45) =$

$= 132 + 360 + 45 = 132 + 405$

$= \underline{\underline{537}}. \quad (42 + 495)$

I Поймем, что

$M_1 x_1 + \ldots + M_n x_n$ подходит:

$\forall i$

$$\underset{\substack{\vdots m_i \\ m_i \,|||\, 0}}{M_1 x_1} + \ldots + \underset{m_i \,|||\, a_i}{M_i x_i} + \ldots + \underset{m_i \,|||\, 0}{M_n x_n} \equiv_{m_i} 0 + \ldots + a_i + \ldots + 0 = a_i$$

это ровно система из 2)

II Единственность. $\exists$ есть решения x и y:

$$\begin{cases} x \equiv_{m_1} a_1 \\ \\ x \equiv_{m_n} a_n \end{cases} \qquad \begin{cases} y \equiv_{m_1} a_1 \\ \vdots \\ y \equiv_{m_n} a_n \end{cases} \Rightarrow \begin{cases} x - y \equiv_{m_1} 0 \\ \ldots \\ x - y \equiv_{m_n} 0 \end{cases}$$

$\Rightarrow x - y \,\vdots\, m_1, \quad x - y \,\vdots\, m_2, \ldots \quad x - y \,\vdots\, m_n$

$$\frac{\begin{matrix} x - y \,\vdots\, m_1 \\ x - y \,\vdots\, m_2 \end{matrix}}{} \Rightarrow x - y \,\vdots\, \overset{\text{НОК}}{[m_1, m_2]} = \frac{m_1 m_2}{(m_1, m_2)} = \frac{m_1 m_2}{1} = m_1 m_2$$

$x - y \,\vdots\, m_1 m_2$

$x - y \,\vdots\, m_3$ $\Big|$ $\xRightarrow{\text{аналогично}}$ $x - y \,\vdots\, m_1 m_2 m_3$

и т.д. $\Rightarrow x-y \vdots m_1 m_2 \dots m_n = M$

(другими словами, если $A \vdots m_1 \dots A \vdots m_n$, где m_i попарно взаимно просты, то $A \vdots m_1 m_2 \dots m_n$)

Итого $x-y \vdots M \Rightarrow x \underset{M}{\equiv} y$ ∎

Функция Эйлера

Опр. $\varphi(n)$, где $n \in \mathbb{N}$ — это кол-во натуральных чисел от 1 до n, которые взаимно просты с n.

$$\varphi(n) = \left| \{ i : 1 \le i \le n,\ (i,n)=1 \} \right|$$

Пример $\varphi(10) = 4$

1 2 3 4 5 6 7 8 9 10

1) 2) 3) 4)

$\varphi(8) = 4$ 1 2 3 4 5 6 7 8

$\varphi(1) = 1$ 1

$\varphi(2) = 1$ 1 2

Утв. $\boxed{\varphi(p) = p-1}$, если $p \in \mathbb{P}$.

Д-во Если $1 \le i < p$, т.е. $1 \le i \le p-1$

$\Rightarrow i \not\vdots p \Rightarrow (i,p)=1. \Rightarrow$ все подходят

Пример $\varphi(7)=6$ 1 2 3 4 5 6 7

Утв $\boxed{\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}}$

Δ-во $\quad$ Пусть $(i, p^k) \neq 1 \qquad (i, p^k) = d > 1$.

$1 \le i \le p^k - 1$. $\qquad p^k \vdots p^l \vdots p$, где $l \le k$

$\Rightarrow d \vdots p \Rightarrow i \vdots p$.

Вывод $(i, p^k) \neq 1 \Leftrightarrow i \vdots p$

Сколько не взаимно просты с p^k?

= сколько чисел $\vdots p$

– это $\underbrace{1\cdot p, 2p, 3p, 4p, \ldots - p^{k-1} \cdot p}_{p^{k-1} \text{ шт.}} = p^k$

Сколько не взаимно просто:

все остальные

$p^k - p^{k-1}$ ∎

Пример: $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$

$= 2 \cdot 3^3 = 2 \cdot 27 = 54$

Утв Пусть $a, b \in \mathbb{N}$, $\boxed{\text{Пусть } (a,b) = 1}$

тогда $\boxed{\varphi(ab) = \varphi(a)\varphi(b)}$

(т.е. φ „мультипликативна")

Пример $\qquad \varphi(10) = \underset{\underset{1}{\parallel}}{\varphi(2)} \cdot \underset{\underset{4}{\parallel}}{\varphi(5)} = 4$

$\varphi(12) = \varphi(4) \cdot \varphi(3) = 4$

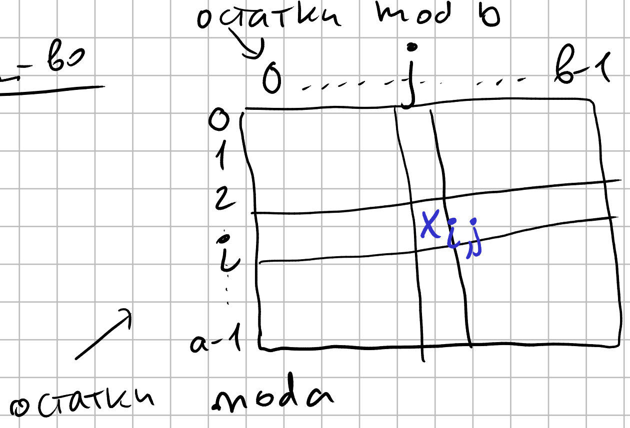
$\varphi(4) = \varphi(2^2) = 1 \cdot 2^1$, $\quad \varphi(3) = 2$

1 2 3 4 5 6

$\varphi(12) \neq \underset{\underset{1}{\parallel}}{\varphi(2)} \cdot \underset{\underset{2}{\parallel}}{\varphi(6)} = 2 \neq 4$

$(2,6) \neq 1$

Д-во



Пример $a=3$ $b=4$

	0	1	2	3
0	0	9	6	3
1	4	1	10	7
2	8	5	2	11

$9 \underset{3}{\equiv} 0$

$9 \underset{4}{\equiv} 1$

$6 \underset{3}{\equiv} 0$

$6 \underset{4}{\equiv} 2$

x_{ij} – число в строке i, столбце j:

$$\begin{cases} x_{i,j} \underset{a}{\equiv} i \\ x_{i,j} \underset{b}{\equiv} j \end{cases}$$

← как в китайской теореме об остатках $(a,b)=1$

x_{ij} единственный mod $a \cdot b$