Ждём слушателей!

Напоминание! Альтернативный экзамен, см. pozdnikov.vm2-leti.spb.ru

Было: уравнение диофантово (в целых числах)

$$ax+by=c \qquad (a,b,c\in\mathbb{Z} \quad a\neq 0 \text{ или } b\neq 0)$$

Теорема $\exists\, x_0\ y_0$ - частное решение ур-вения

$$ax_0+by_0=c \qquad d=(a,b)$$

Тогда

$$\begin{cases} x=x_0+k\cdot b/d \\ y=y_0-k\cdot a/d \end{cases} \quad k\in\mathbb{Z}$$

— это всё множество решений уравнения.

Д-во 1) Если есть еще решение $\bar{x},\bar{y}$, мы уже выяснили, что $\exists k\in\mathbb{Z}:$ $\bar{x}-x_0=k\cdot b/d$

$$\bar{y}-y_0=-k\cdot a/d$$

$$\Rightarrow \begin{cases} \bar{x}=x_0+k\,b/d \\ \bar{y}=y_0-k\,a/d \end{cases}$$

2) $\forall k$ полученные x и y — это решение

$$ax+by=a\left(x_0+k\frac{b}{d}\right)+b\left(y_0-k\,b/d\right)=\underbrace{ax_0+by_0}_{c}+\underbrace{ak\,b/d-bk\,a/d}_{0}$$

$$=c \Rightarrow x,y \text{ — корни уравнения} \quad \blacksquare$$

Пример: $6x+15y=9$

$x_0=9$
$y=-3$ проверим: $6\cdot 9+15(-3)=54-45=9$

Тогда все решения: $d=(6,15)=3$

$$\begin{cases} x = 9 + k\cdot 15/3 \\ y = -3 - k\cdot 6/3 \end{cases} \Leftrightarrow \begin{cases} x = 9+5k \\ y = -3-2k \end{cases}$$

Решения: ... $k=-2$: $x=-1$, $y=1$; $k=-1$: $x=4$, $y=-1$; $k=0$: $x=9$, $y=-3$ ✓; $k=1$: $x=14$, $y=-5$; $k=2$: $x=19$, $y=-7$ ...

Замечание. Это - то же все мн-во решений:

$$\begin{cases} x = -1 + 5\ell \\ y = 1 - 2\ell \end{cases} \quad \ell \in \mathbb{Z} \qquad (\ell = k-2)$$

Поиск частного решения

Th. $\exists$ уравнение $ax+by=c$ $\quad a,b,c \in \mathbb{Z}$

$d=(a,b)$ $\quad a \neq 0$ или $b \neq 0$

Тогда, если $c \,\vdots\, d$, то $\exists$ решение уравнения

если $c \not\vdots\, d$, то $\nexists$ решения ур-ия

Д-во. $\exists$ есть решение x_0 y_0:

$$\underbrace{\underset{\vdots\, d}{a x_0} + \underset{\vdots\, d}{b y_0}}_{\vdots\, d} = c \implies c \,\vdots\, d.$$

Итого, если $c \not\vdots\, d$, решений нет

Пример:

$\underbrace{2x+4y}_{\text{нет } \vdots 2} = \underset{\text{нечет}\ \not\vdots 2}{3}$

Если $c \,\vdots\, d$, то найдем решение, конструктивно.

Найдем линейное разложение НОД a, b.

$\exists \bar{x}\ \bar{y}$: $\quad a\bar{x} + b\bar{y} = d$ $\quad$ ($\bar{x}$ и $\bar{y}$ можно найти Расш. А Е.)

Тогда домножим обе части на $c/d \in \mathbb{Z}$

$$a\left(\bar{x}\ c/d\right) + b\left(\bar{y}\ c/d\right) = d\, c/d = c$$

Итого, $x_0 = \bar{x} \cdot c/d$ $y_0 = \bar{y} \cdot c/d$.

Модульная арифметика

Определение. $x \underset{m}{\equiv} y$ икс сравнимо с игрек по модулю эм

Иногда пишут $x \equiv y \pmod m$

Если 1) $x - y \vdots m$

2) $x \bmod m = y \bmod m$

Утв. Два определения эквивалентны

Д-во.

$\exists\ x = q_1 \cdot m + r_1$ ← деление с остатком

$y = q_2 m + r_2$

$x - y = (q_1 - q_2)m + (r_1 - r_2) \vdots m \iff r_1 - r_2 \vdots m \iff$

Но $0 \leq \begin{matrix} r_1 \\ r_2 \end{matrix} < m \Rightarrow -m < r_1 - r_2 < m$

$r_1 \geq 0$, $r_2 < m$, $r_1 - r_2 > 0 - m$ | $r_1 < m$, $r_2 \geq 0$, $r_1 - r_2 < m - 0$

$\iff r_1 - r_2 = 0 \iff r_1 = r_2$

Св-ва 1. $\underset{m}{\equiv}$ – отношение эквивалентности.
(похоже по св-вам на $=$)

1.1 $a \underset{m}{\equiv} a$

$a - a \vdots m$

1.2 $a \underset{m}{\equiv} b \iff b \underset{m}{\equiv} a$

$a - b \vdots m \iff b - a \vdots m$

1.3 $\left. \begin{matrix} a \underset{m}{\equiv} b \\ b \underset{m}{\equiv} c \end{matrix} \right| \Rightarrow a \underset{m}{\equiv} c$

$$+\ \frac{\begin{matrix} a - b \vdots m \\ b - c \vdots m \end{matrix}}{a - b + b - c \vdots m}$$

$\begin{matrix} a \bmod m = b \bmod m \\ b \bmod m = c \bmod m \end{matrix} \Rightarrow a \bmod m = c \bmod m$

2. Арифметические св-ва

$a \underset{m}{\equiv} b$, $c \underset{m}{\equiv} d$ Тогда:

2.1 $a+c \underset{m}{\equiv} b+d$ 2.2 $a-c \underset{m}{\equiv} b-d$

2.3 $a\cdot c \underset{m}{\equiv} b\cdot d$ 2.4 $a^n \underset{m}{\equiv} b^n$ $(n\geq 0)$

Д-во 2.1

$$a-b \,\vdots\, m,\quad c-d \,\vdots\, m \Rightarrow a+c-b-d \,\vdots\, m$$
$$\Rightarrow (a+c)-(b+d) \,\vdots\, m \Rightarrow a+c \underset{m}{\equiv} b+d$$

2.2 аналогично

2.3.
$$a-b \,\vdots\, m \Rightarrow (a-b)c \,\vdots\, m \Rightarrow ac-\cancel{bc} \,\vdots\, m$$
$$c-d \,\vdots\, m \Rightarrow (c-d)\cdot b \,\vdots\, m \Rightarrow \cancel{bc}-bd \,\vdots\, m$$
$+$ $ac-bd \,\vdots\, m$

2.4. следствие 2.3

$$\left.\begin{matrix} a \underset{m}{\equiv} b \\ a \underset{m}{\equiv} b \end{matrix}\right\} n \text{ шт, умножаем}$$
$$a^n \underset{m}{\equiv} b^n$$

Примеры и пояснения

$1 \underset{3}{\equiv} 4$ т.к $4-1 \,\vdots\, 3$ $4 \underset{3}{\equiv} 7$

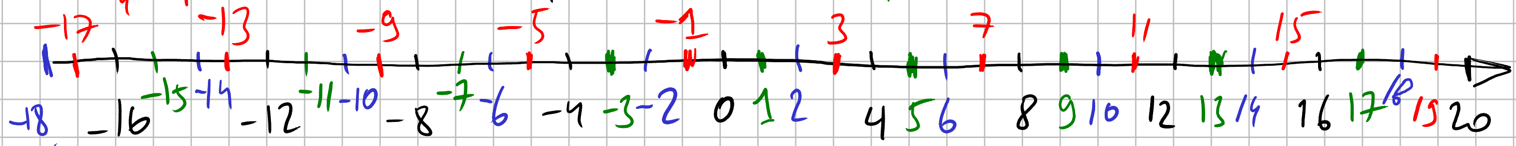
$1 \underset{3}{\equiv} -2$ т.к. $1-(-2) \,\vdots\, 3$

$10 \underset{5}{\equiv} 30$ т.к. $30-10 \,\vdots\, 5$

$1 \underset{4}{\equiv} 1, 5, 9, 13$ $1 \underset{4}{\equiv} 1+4k,\ k\in\mathbb{Z}$ т.к. $1+4k-1=4k \,\vdots\, 4$

$1 \underset{4}{\equiv} -3, -7, \ldots$

$3 \underset{4}{\equiv}$ красный $0 \underset{4}{\equiv}$ черные $1 \underset{4}{\equiv}$ зеленые $2 \underset{4}{\equiv}$ синие



Св-ва про деление

3.1 $ac \underset{m}{\equiv} bc \Rightarrow a \underset{m}{\equiv} b$ $\boxed{\text{если } (m,c)=1}$

$0\cdot 2 \underset{4}{\equiv} 2\cdot 2 \not\Rightarrow 0 \underset{4}{\equiv} 2$

$(2,4)=2\neq 1$

3.2 $ac \underset{m}{\equiv} bc \Rightarrow a \underset{m/(m,c)}{\equiv} b$ $\quad 0\cdot 2 \underset{4}{\equiv} 2\cdot 2 \Rightarrow 0 \underset{\frac{4}{(4,2)}=2}{\equiv} 2$

Д-во 3.1 $ac - bc \vdots m \Rightarrow (a-b)c \vdots m$, но $(c,m)=1$

$\Rightarrow a-b \vdots m \Rightarrow a \underset{m}{\equiv} b$ ∎

3.2. $ac-bc \vdots m \Rightarrow (a-b)c \vdots m \Rightarrow \underset{\exists k}{(a-b)\cdot c = km}$

$\Rightarrow$ сократим на $(m,c)=d$ $\quad (a-b)\,c/d = k\,m/d$

$\Rightarrow (a-b)\,c/d \vdots m/d$, но $(c/d, m/d)=1$.

см прошлую лекцию

$\Rightarrow a-b \vdots m/d \Rightarrow a \underset{m/d}{\equiv} b$ ∎