

4 Теорема за остатък

$a \neq 0$, $b \in \mathbb{Z}$

$a \mid b$, ако $\exists c \in \mathbb{Z} : b = a \cdot c$

$a \nmid b$, ако $\nexists c \in \mathbb{Z} : b = a \cdot c$

Ob-ba:

Теорема за generic остатък

$a, b \in \mathbb{Z}$ $\exists q, r \in \mathbb{Z} : a = bq + r$

q - частно $-$

r - остатък $0 \leq r < |b|$

Пример: $a = -17$, $b = -5$

$$-17 = 4 \cdot (-5) + 3$$

Зад. Да се $\forall n \in \mathbb{N} : a_n = 5^{n+1} - 4n - 5$
е generic на 16

Дбо: найдуващо no n

$$1) n=1 \quad 25 - 8 = 16 \quad \checkmark$$

$$2) \text{Нека } 16 \mid a_n$$

$$\begin{aligned}
 3) \quad a_{n+1} &= 5^{n+2} - 4(n+1) - 5 = \\
 &= 5^{n+2} - 4n + 4 - 5 = \\
 &= 5(5^{n+1} - 4n - 5) + 16n + 16 \\
 &\quad \underbrace{\qquad\qquad\qquad}_{16|a_n}
 \end{aligned}$$

$$\Rightarrow 16 | a_{n+1}$$

3e упражнение: $a_n = 2^3^n + 1$

Да се покаже $\forall n \in \mathbb{N}: 3^{n+1} | a_n$
ко $3^{n+2} \nmid a_n$

Заг. За $n \in \mathbb{Z}$ $n-3 | n^3 - 3$

$$D\text{-бо: } \frac{n^3 - 3}{n-3} \in \mathbb{Z}$$

$$n^3 - 3^3 = (n-3)(n^2 + 3n + 9)$$

$$\Rightarrow \frac{n^3 - 3^3}{n-3} + \frac{24}{n-3}, \text{ ко } \\
 \in \mathbb{Z}$$

$n-3 \mid 24$ како, чорато

$$n-3 = \pm \{1, 2, 3, 4, 6, 8, 12, 24\}$$

KOD: $\forall a, b \in \mathbb{Z} \ (\neq 0, 0) \ \exists! d \in \mathbb{N}:$

$$(a, b) = d - \text{KOD}$$

$$1) d \mid a \wedge d \mid b$$

$$2) \forall d_1 \in \mathbb{Z}: d_1 \mid a \wedge d_1 \mid b \Rightarrow d_1 \mid d$$

$$(a, b) = 1 - \text{безумно просто}$$

$$(a, 0) = |a|$$

Алгоритм на Евклида

$$a, b \in \mathbb{N}: a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

$$\text{делим } b \text{ на } r_1: b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$\star r_2 = 0 \Rightarrow (b, r_1) = r_1 = (a, b)$$

$$\star r_2 \neq 0 \Rightarrow r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$$\star r_3 = 0 \Rightarrow (r_1, r_2) = (b, r_1) = (a, b) = r_2$$

$$\star r_3 \neq 0 \dots \text{урах} \quad (r_1 > r_2 \dots > r_k)$$

$$\begin{aligned} r_{k-1} &= r_k q_{k+1} + 0 \\ \Rightarrow r_k &= (a, b) \end{aligned}$$

Тъждество на Безу

$$a, b \in \mathbb{Z} \quad (\neq 0, 0) \quad \exists u, v \in \mathbb{Z} \quad (u, v) = 1$$

$$au + bv = d = (a, b)$$

u, v не са единствени

Пример: $a = 3 \quad b = 5$

$$\begin{aligned} 2 \cdot 3 - 1 \cdot 5 &= 1 \\ -3 \cdot 3 + 2 \cdot 5 &= 1 \end{aligned}$$

Зад. $a = 975 \quad b = 308 \quad ? u, v$

$$(975, 308) = (51, 308) = (51, 2) = (1, 2) = 1$$

$$975 = 3 \cdot 308 + 51$$

$$308 = 6 \cdot 51 + 2$$

$$51 = 25 \cdot 2 + 1$$

$$\Rightarrow \text{WOD}(a, b) = 1$$

$\hookrightarrow u, v$

$$\begin{aligned}
 1 &= 51 - 2 \cdot 25 = 51 - 25(308 - 6 \cdot 51) = \\
 &= 51 - 25 \cdot 308 + 150 \cdot 51 = \\
 &\equiv 151 \cdot 51 - 25 \cdot 308 = \\
 &= 151(975 - 3 \cdot 308) - 25 \cdot 308 \\
 &= 151 \cdot 975 - 478 \cdot 308 \\
 \Rightarrow u &= 151, v = -478
 \end{aligned}$$

За упражнение: $a = 315$, $b = 22$
 кот $\underline{\underline{?}}$, $u, v = ?$

Втори метод за налигане на кот
 u, v

Метод на Бланкини

$$\begin{array}{c}
 \left(\begin{array}{ccc} a & 1 & 1 \\ b & 0 & 1 \end{array} \right) \sim \cdots \left(\begin{array}{ccc} 0 & * & * \\ d & u & v \end{array} \right) \\
 \left(\begin{array}{ccc} 975 & 1 & 0 \\ 308 & 0 & 1 \end{array} \right) \xrightarrow{(-3)} \left(\begin{array}{ccc} 91 & 1 & -3 \\ 308 & 0 & 1 \end{array} \right) \xrightarrow{(-6)} \left(\begin{array}{ccc} 51 & 1 & -3 \\ 2 & -6 & 19 \end{array} \right) \xrightarrow{(-25)} \left(\begin{array}{ccc} 1 & 151 & -478 \\ 2 & -6 & 19 \end{array} \right) \sim
 \end{array}$$

$$\sim \begin{pmatrix} 0 & * & * \\ 1 & 151 & -478 \end{pmatrix} \quad u = 151, \quad v = -478$$

\downarrow

$$\text{HOD}(a, b) = 1$$

KOK (наи-малко общо уравнение)

$\forall a, b \in \mathbb{Z} (\neq 0, 0) \exists! c \in \mathbb{N} : [a, b] = c$ - KOK

$$1) a | c \wedge b | c$$

$$2) \forall c_1 \in \mathbb{N} : a | c_1 \wedge b | c_1 \Rightarrow c | c_1$$

Возможна несигу KOK и HOD: $[a, b] = \frac{a \cdot b}{(a, b)}$

(б-бо: Ако $a | b \Rightarrow a | bc$

Теорема рацио $p > 1$ е просто \Leftrightarrow

$\forall a, b \in \mathbb{Z} : p | ab \Rightarrow p | a$ или $p | b$

Зад. Да се намерят всички прости числа, за които $p+4$ и $p+14$ са прости

Реш: 1) $p=2$ - не

2) $p=3$: $p+4=7$, $p+14=17 \checkmark$

3) $p=3k+1$ - представяне на простите числа
като умножение по $(mod 3)$
Ето е, че всичко число можем да
представим като $s=3k$ или $s=3k+1$ или
 $s=3k+2$

$$p+4=3k+5$$

$$p+14=3k+15 \Rightarrow 3 \mid p+14 \quad \text{у}$$

4) $p=3k+2$

$$p+4=3k+6 \quad \text{у} \quad 3 \mid p+4$$

Зато че разглеждаме $p=3k$?

Знам, че 3 е единственото просто
число, за което условието е във
съвпадение.

За упражнение: Да се намерят всички
прости числа p , за които
 $4p^2+1$, $6p^2+1$ са прости

Нин: $p = 2 - \kappa e \sim p = 5 - g_a$, $p > 5$?

Каноничен запис: $n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$
 $d_i \geq 1$, $p_i \neq p_j$ (несту)

Диофантово уравнение

Деф) Диофантово уравнение користимо
уравнение от буга

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b, \quad b, a_i, x_i \in \mathbb{Z}$$

Ме разрешимо уравнение от буга

$$ax + by = c$$

Уравнението има решение, иначе

$$(a, b) = d, \quad d \mid c$$

$$a = a_1d \quad b = b_1d$$

Всички решения изразяват се с
формулата

$$x = x_0 + k \cdot b_1$$

$k \in \mathbb{Z}$ (x_0, y_0) — едно
решение на уравнението

$$y = y_0 - k \cdot a_1$$

$$\text{Задача. } 32x + 14y = 3$$

$(32, 14) = 2 \times 3 \Rightarrow$ неко решение

$$\text{Задача. } 32x + 14y = 4$$

$(32, 14) = 2 \mid 4 \Rightarrow$ одна решение

$$32 = a_1 \cdot 2 = 16 \cdot 2 \rightarrow a_1 = 16$$

$$14 = b_1 \cdot 2 = 7 \cdot 2 \rightarrow b_1 = 7$$

$$\left(\begin{array}{ccc} 32 & 1 & 0 \\ 14 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{ccc} 4 & 1 & -2 \\ 14 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{ccc} 4 & 1 & -2 \\ 2 & -3 & 7 \end{array} \right)$$

$$\sim \left(\begin{array}{ccc} 0 & * & * \\ 2 & -3 & 7 \end{array} \right) \quad 2 = -3 \cdot 32 + 7 \cdot 14$$

$\begin{matrix} \nearrow & \nearrow & \nearrow \\ d & 4 & \checkmark \end{matrix}$

$$4 = \underline{-6} \cdot 32 + \underline{14} \cdot 14$$

$\begin{matrix} \searrow & \searrow & \searrow \\ x_0 & y_0 & \end{matrix}$

$$\left| \begin{array}{l} x = -6 + u \cdot 7 \\ y = 14 - u \cdot 16 \end{array}, u \in \mathbb{Z} \right.$$

Алгоритм: 1) находим НОД

2. a_1, b_1

3. $\frac{b_1}{\text{Безы}} \rightarrow (x_0, y_0)$

4. Замечание в вида формула

$$\text{Зад. } 1001x + 3059y = 77$$

$$\begin{pmatrix} 1001 & 1 & 0 \\ 3059 & 0 & 1 \end{pmatrix} \xrightarrow{(-3)} \sim \begin{pmatrix} 1001 & 1 & 0 \\ 56 & -3 & 1 \end{pmatrix} \xrightarrow{(-17)} \sim$$

$$\begin{pmatrix} 49 & 51 & -17 \\ 56 & -3 & 1 \end{pmatrix} \xrightarrow{(-1)} \sim \begin{pmatrix} 49 & 51 & 0 \\ 7 & -54 & 18 \end{pmatrix} \sim \begin{pmatrix} 0 & * & * \\ 7 & -54 & 18 \end{pmatrix}$$

$$\Rightarrow \text{НОД}(1001, 3059) = 7 \mid 77 \quad \checkmark$$

$$1001 = 143 \cdot 7 \quad d_1 = 143$$

$$3059 = 437 \cdot 7 \quad b_1 = 437$$

$$7 = -55 \cdot 1001 + 18 \cdot 3059 \quad | : 11$$

$$7 = -\frac{605}{x_0} \cdot 1001 + \frac{198}{y_0} \cdot 3059$$

$$\begin{cases} x = -605 + u \cdot 437 \\ y = 198 - k \cdot 143 \end{cases}, u \in \mathbb{Z}$$

Задание: $533x + 195y = 26$

Модульное сведение

Для $a, b \in \mathbb{Z}$. Возьмем, что $a \neq b$ и a и b не
сравнимы по модулю n , то есть $n \nmid a - b$
 $a \equiv b \pmod{n} \Rightarrow n \mid a - b$

" a и b имеют одинаковый остаток при
делении на n "

Пример: $7 \equiv 3 \pmod{4}$
 $-1 \equiv 3 \pmod{4}$

$$-1 \equiv 3 \equiv 7 \equiv 11 \equiv \dots \pmod{4}$$

$$1 \equiv 5 \pmod{4}$$
$$0 \equiv 4 \equiv 16 \pmod{4}$$

\equiv "равны по модулю" - это эквивалентность

(б-б):

I) $a_1 \equiv b_1 \pmod{n}$ $a_2 \equiv b_2 \pmod{n}$, то

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$$

$$a_1 a_2 \equiv b_1 b_2 \pmod{n}$$

II) ано $a + b \equiv c \pmod{n}$, то $a \equiv c - b \pmod{n}$

$$3 + 5 \equiv 2 \pmod{6}$$

$$3 \equiv -3 \pmod{6}$$

$$5 \equiv -1 \pmod{6}$$

III) also $a \equiv b \pmod{n}$, then $a+c \equiv b+c \pmod{n}$

IV) also $u \cdot a \equiv u \cdot b \pmod{n}$, then
 $a \equiv b \pmod{\frac{n}{(u, n)}} \rightarrow$ rop

Def [Модулни съвместни]

Def от това $aX \equiv b \pmod{n}$

Така е гажко мод. сп. $aX \equiv b \pmod{n}$

и $d = (a, n)$. Такава, also:

1) $d = 1$, сп. има единствено реш.

2) $d > 1$, $d \mid b$, сп. има реш.

3) $d > 1$, $d \nmid b$, сп. има d на споси

реш: $X_k = X_0 + k \cdot \frac{m}{d} \quad k=0, 1, \dots, d-1$

Зад. Да се реши съвокупето

a) $28x \equiv 12 \pmod{45}$

$$\xrightarrow{\text{a}} \begin{pmatrix} 28 & 1 & 0 \\ 45 & 0 & 1 \end{pmatrix} \xrightarrow{\text{b}} \begin{pmatrix} 28 & 1 & 0 \\ 17 & -1 & 1 \end{pmatrix} \xrightarrow{\text{c}} \begin{pmatrix} 11 & 2 & -1 \\ 17 & -1 & 1 \end{pmatrix} \sim$$

$$\xrightarrow{\text{d}} \begin{pmatrix} 11 & 2 & -1 \\ 6 & -3 & 2 \end{pmatrix} \xrightarrow{\text{e}} \begin{pmatrix} 5 & 5 & -3 \\ 6 & -3 & 2 \end{pmatrix} \xrightarrow{\text{f}} \begin{pmatrix} 5 & 5 & -3 \\ 1 & -8 & 5 \end{pmatrix}$$

$$\sim \begin{pmatrix} 0 & * & * \\ 1 & -8 & 5 \end{pmatrix} \Rightarrow 1 = -8 \cdot 28 + 5 \cdot 45 \pmod{45}$$

$$-8 \cdot 28 + 5 \cdot 45 \equiv 1 \pmod{45} \quad \begin{matrix} \swarrow \\ \begin{matrix} y \equiv 0 \pmod{2} \\ x = y \\ x = y^{(n)} \end{matrix} \end{matrix}$$

$$1 \equiv -8 \cdot 28 \pmod{45}$$

$\Rightarrow -8$ е обратен елемент на 28
но модул 45

$$-8 \cdot 28 \equiv 1 \pmod{45}$$

$$-8 \equiv 37 \pmod{45}$$

$$28x \equiv 12 \pmod{45} \quad | \cdot (-8)$$

$$-8 \cdot 28x \equiv 1 \cdot x \equiv -8 \cdot 12 \equiv -96 \equiv -6 \equiv 39 \pmod{45}$$

$$x \equiv 39 \pmod{45}$$

$$x = 39 + k \cdot 45 \quad k \in \mathbb{Z}$$

$$\text{d) } 15x \equiv 7 \pmod{31} \quad (15, 31) = 1 \xrightarrow{\text{! prem.}}$$

$$\begin{pmatrix} 15 & 1 & 0 \\ 31 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 15 & 1 & 0 \\ 1 & -2 & 1 \end{pmatrix} \xrightarrow{(-15)} \begin{pmatrix} 0 & 31 & -15 \\ 1 & -2 & 1 \end{pmatrix}$$

$$1 = -2 \cdot 15 + 1 \cdot 31$$

$$1 \equiv -2 \cdot 15 + \underbrace{31}_{\sim} \pmod{31}$$

$$1 \equiv -2 \cdot 15 \pmod{31}$$

$$15x \equiv 7 \pmod{31} \quad | \cdot -2$$

$$\underbrace{-2 \cdot 15}_{} x \equiv 1 \cdot x \equiv -2 \cdot 7 = -14 \pmod{31}$$

$$x \equiv -14 \equiv \underbrace{17}_{\sim} \pmod{31}$$

$$x = 17 + 31k \quad k \in \mathbb{Z}$$

$$b) \underline{21}x \equiv \underline{35} \pmod{\underline{56}}$$

$$\begin{array}{l} (-2) \\ b) \left(\begin{array}{ccc} 21 & 1 & 0 \\ 56 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{ccc} 21 & 1 & 0 \\ 14 & -2 & 1 \end{array} \right) \xrightarrow[-1]{} \left(\begin{array}{ccc} 7 & 3 & -1 \\ 14 & 0 & 1 \end{array} \right) \xrightarrow[-2]{} \\ \sim \left(\begin{array}{ccc} 7 & 3 & -1 \\ 0 & 2 & 3 \end{array} \right) \sim \left(\begin{array}{ccc} 0 & 2^* & 3^* \\ 7 & 3 & -1 \end{array} \right) \end{array}$$

$$\Rightarrow (21, 56) = 7$$

? $7 \mid 35 - g$ \Rightarrow имеем 7 решений
(такие, которых в КОР)

$$3x \equiv 5 \pmod{8} \quad | \cdot 3 \quad (\text{результат от})$$

$$\underbrace{g}_7 x \equiv \underbrace{15}_{\sim} \pmod{8} \quad 21x \equiv \underline{35} \pmod{\underline{56}}$$

$$8x + x \equiv 7 \pmod{8}$$

$$x \equiv 7 \pmod{8} \rightarrow \text{результат}$$

$$x = \underline{7 + s \cdot 8}, \quad s = \underline{0, 1, \dots, 6}$$

$$x \equiv \overbrace{7}^{x_1}, \overbrace{15}^{x_2}, 23, 31, 39, 47, 55 \pmod{56}$$

$$x = \underline{x_i + 56k} \quad k \in \mathbb{Z} \quad i=1, \dots, 7$$

об-е на Опер. Т-ма на Опер-
Форма.

Def_o [$n \in \mathbb{N}$, $\varphi(n)$ - об-е на Опер.

$\varphi(n)$ - броят змезд, бъзачкото проста
с n , но- максим $\begin{cases} \text{или равна} \\ \text{от} \end{cases}$ n
 $(\in \mathbb{N})$

Ob-бq:

$$1) 1 \leq \varphi(n) \leq n-1$$

$$2) \text{ако } p \text{ е просто, то } \varphi(p) = p-1$$

$$3) \text{ако } p \text{ е просто, и } a \in \mathbb{N}$$

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$$

$$4) \text{множителност. Ако } a, b \in \mathbb{N},$$

$$(a, b) = 1, \text{то } \varphi(ab) = \varphi(a) \cdot \varphi(b)$$

Зад. $\varphi(1024) = \varphi(2^{10}) = 2^{10} - 2^9 = 2^9(2-1)$

$1024 = 2^{10}$ $= 512$

$$\begin{aligned}\varphi(100) &= \varphi(2^2 \cdot 5^2) = \varphi(2^2) \varphi(5^2) = \\100 &= 2^2 \cdot 5^2 \quad = (2^2 - 2^1)(5^2 - 5^1) = 2 \cdot 20 \\&\quad = 40\end{aligned}$$

$$\varphi(100) = 40$$

$$144 = 12^2 = (4 \cdot 3)^2 = (2^2 \cdot 3^2)^2 = \underline{\underline{3^2 \cdot 2^4}}$$

$\xrightarrow{\text{натуральное представление}}$

$$\begin{aligned}\varphi(144) &= \varphi(3^2 \cdot 2^4) = \varphi(3^2) \cdot \varphi(2^4) = \\&= (3^2 - 3) \cdot (2^4 - 2^3) = (9 - 3)(16 - 8) \\&= 6 \cdot 8 = 48\end{aligned}$$

Заг. Док, че ако $d \mid n$, то $\varphi(d) \mid \varphi(n)$

Реш: $d = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$

$n = p_1^{b_1} \dots p_k^{b_k} q_1^{r_1} \dots q_s^{r_s}$

$d_i \leq b_i$

Тогда

$$\begin{aligned}\varphi(d) &= \varphi(p_1^{d_1}) \dots \varphi(p_k^{d_k}) = \\ &= p_1^{d_1}(p_1 - 1) p_2^{d_2}(p_2 - 1) \dots p_k^{d_k}(p_k - 1)\end{aligned}$$

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{b_1}) \dots \varphi(p_k^{b_k}) \varphi(q_1^{r_1}) \dots \varphi(q_s^{r_s}) \\ &= p_1^{b_1}(p_1 - 1) \dots p_k^{b_k}(p_k - 1) q_1^{r_1}(q_1 - 1) \dots q_s^{r_s}(q_s - 1)\end{aligned}$$

$$\Rightarrow \varphi(d) \mid \varphi(n)$$

Т.к. $\varphi(n)$ ділиться на $\varphi(d)$

Існує $a \in \mathbb{Z}$ та $n \in \mathbb{N}$ $(a, n) = 1$

Тогда $a^{\varphi(n)} \equiv 1 \pmod{n}$

В заг. 2 на 2д) $\underbrace{x}_{\varphi(n)} \equiv 1 \pmod{n}$

Зад. Какуюите остатки генератора
 $(2013^{87} + 17^{74})^{37} \pmod{13}$

Реш: $2013 \equiv ? \pmod{13}$

$$(2013, 13) = 1 \text{ б. н. о.} \Rightarrow 0 \cdot 00.$$

$$2013^{4(13)} \equiv 1 \pmod{13}$$

$$2013^{12} \equiv 1 \pmod{13}$$

$$(2013^{12})^8 = 18 \pmod{13}$$

$$\Rightarrow 2013^{96} \equiv 1 \pmod{13}$$

$$2013^{97} \equiv 2013 \pmod{13}$$
$$\equiv 11$$

$$a \equiv b \pmod{n}$$
$$a^k \equiv b^k \pmod{n} \quad k \in \mathbb{N}$$

$$(17, 13) = 1 \Rightarrow 0 \cdot 00. \quad 74$$

$$17^{12} \equiv 1 \pmod{13}$$

$$(17^{12})^6 \equiv 1^6 \equiv 1 = 17^{72} \pmod{13}$$

$$17^{74} \equiv 17^2 \equiv 289 \equiv 3 \pmod{13}$$

$$37 \mid 2013^{97} + 17^{74} \equiv 11 + 3 \equiv 14 \equiv 1 \pmod{13}$$

$$(2013^{87} + 17^{74})^{37} \equiv 1 \pmod{13}$$

Зад. Какитеите ночи ще имат на засчет
33⁴⁰²

Реш: $33^{402} \equiv ? \pmod{100}$

$(33, 100) = 1 \rightarrow 0\text{-го.}$

$$33^{4(100)} \equiv 33^4 \equiv 1 \pmod{100}$$

$$33^{400} \equiv 1 \pmod{100}$$

$$33^{402} = 33^2 \equiv 1089 \equiv 89 \pmod{100}$$

Зад. ? Понесите 2 цифри на 7²¹³

Реш: $(7, 100) = 1$

$$7^{4(100)} \equiv 1 \pmod{100}$$

$$7^{40} \equiv 1 \pmod{100}$$

$$\Rightarrow 7^{40 \cdot 5} \equiv 1^5 \equiv 1 \pmod{100}$$

Значи трети $7^{40 \cdot 5 + 13} \equiv 7^{13} \equiv 1 \pmod{100}$

$$7^4 \equiv 2401 \equiv 1 \pmod{100}$$

$$\Rightarrow 7^{12} \equiv 1 \pmod{100} \Rightarrow 7^{13} \equiv 7^{213} \equiv 7 \pmod{100}$$

\Rightarrow понесите 2 цифри са 0 и 7

Задача Упражнение:

Да се решат $2^{70} + 3^{70}$ за модул 13

Задача. Да се намерят поснедружите 2
членови на

$$7^{\overbrace{7}^{\cdot \cdot \cdot}} \quad n \text{ члену}$$

Решение: $7 \equiv 1 \pmod{100}$

$$7^7 \equiv 7^4 \cdot 7^3 \equiv 1 \cdot 7^3 \equiv 1 \cdot 43 \equiv 43 \pmod{100}$$

$$7^{\overbrace{7}^{\cdot \cdot \cdot}} \equiv 43^7 \equiv (7^3)^7 \equiv 7^{21} \equiv 7 \pmod{100}$$

Заделенуване, се се повторат

$$\Rightarrow 7^{\overbrace{7}^{\cdot \cdot \cdot}} \quad n \text{ члену} = \begin{cases} 07, & n=0 \pmod{2} \\ 43, & n \neq 0 \pmod{2} \end{cases}$$

Задача? Постнедружите 2 членови на 2^{2032}

Решение: $(2, 100) \neq 1 \therefore$, от овие го има бугар

$$x \equiv 2^2 \cdot t \pmod{100}, \text{ t.u. } (2^{2032}, 100) = 2^2$$

Znaczu $2^2 \cdot t \equiv 2^{2032} \pmod{100}$, podzielna przez
 $t \equiv 2^{2030} \pmod{25}$

$$(2, 25) = 1 \Rightarrow 2^{\varphi(25)} \equiv 2^{20} \equiv 1 \pmod{25}$$

$$\Rightarrow \text{reszta z dzielenia} \quad t \equiv 2^{10} \pmod{25}$$

$$2^7 \equiv 3 \pmod{25} \Rightarrow 2^{10} \equiv 3 \cdot 2^3 \equiv 24 \pmod{25}$$

$$\Rightarrow t \equiv 24 + k \cdot 25, \quad k \in \mathbb{Z}$$

$$\Rightarrow x \equiv 4(24 + k \cdot 25) = 96 + 100 \cdot k$$

\Rightarrow no ch. 2 wydruk na 96

Zad. ? $x, y \in \mathbb{Z}$ | 56 | 4x92y6

Rew: $4 \cdot 10^5 + x \cdot 10^4 + 9 \cdot 10^3 + 2 \cdot 10^2 + y \cdot 10 + 6 \cdot 1$
 $\equiv 0 \pmod{2^3}$
 $\equiv 0 \pmod{7}$

$$y \cdot 10 + 6 \equiv 0 \pmod{2^3} \quad 2y \equiv 2 \pmod{8} \Rightarrow y \equiv 1 \pmod{4}$$
$$y = 1 + 4k \Rightarrow y \in \{1, 5, 9\}$$

$$4 \cdot 3^5 + x \cdot 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 + y \cdot 3 - 1 \equiv 0 \pmod{7}$$

$$(3^2 \equiv 2 \pmod{7}), \quad 3^3 \equiv -1 \pmod{7}$$

$$4 \cdot 2 + x \cdot 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 + y \cdot 3 - 1 \equiv 0 \pmod{7}$$

$$3y \equiv 3x \pmod{7}$$

$$y \equiv x \pmod{7} \Rightarrow x = y + 7s$$

$$\Rightarrow y = 1 \Rightarrow x \in \{1, 8\}$$

$$y = 5 \Rightarrow x = 5$$

$$y = 9 \Rightarrow x = 9, x = 2$$

Задачи за упражнение

1 а) $7x \equiv 12 \pmod{45}$

б) $25x + 105 \equiv 0 \pmod{265}$

в) $8x + 20 \equiv 0 \pmod{20}$

г) $24x \equiv 60 \pmod{84}$

д) $15x + 60 \equiv 0 \pmod{93}$

2. а) $122x + 284y = 100$

б) $7x + 75y = 6$

3. За кои $n \in \mathbb{Z}$ $n-3 | n+4$?

4. НОД, безъ ка:

а) 232, 108

б) 157, 143

5. ? $x, y \in \mathbb{Z}$ $\overline{25xy^5}$ се делува на 3

6. ? $x, y \in \mathbb{Z}$ $\overline{13xy}$ габа остатък $\frac{u}{7}$

3 при деление на 13, а $\overline{x^3y^3}$ габа остатък 8 при деление на 11