

## Основни елементи на теорията на числата. Делимост и сравнения

$$\text{GCD}(a, b) = (a, b) = d \quad d/a \text{ и } d/b \quad \nexists d_1 > d \quad \text{т.е. } d_1/a \text{ и } d_1/b$$

$$\text{LCM}(a, b) = [a, b] = A \quad a/A \text{ и } b/A \quad \nexists A < A \quad \text{т.е. } a/A_1 \text{ и } b/A_1$$

- Свойства:
- 1) ако  $b \neq 0$   $b/b$
  - 2) ако  $a/b$ , то  $|a| \leq |b|$
  - 3)  $a/b, b/a \Rightarrow |a|=|b|$
  - 4)  $a/b \Rightarrow \pm a/\pm b$
  - 5)  $b/a_1, \dots, b/a_k \Rightarrow b/(a_1 + \dots + a_k)$
  - 6)  $b/a_1+a_2 \text{ и } b/a_1 \Rightarrow b/a_2$
  - 7)  $b/a \Rightarrow b/d.a, d \in \mathbb{Z}$

Признаки за деление:

- 2, 4, 8, ..., 2<sup>n</sup> последните цифри образуват число, кое то се дели на 2<sup>n</sup>
- 3 цифрите имат сбор число, кое то се дели на 3
- 5 последната цифра е 5 и 0.

Зад. 1 Да се докаже, че  $\forall n \in \mathbb{N} \quad 6/n^3 + 11n$

Част 1 остатъци:

$$1) n=6k \quad n^3+11n = (6k)^3 + 11(6k) = 6 \cdot (6^2 k^3 + 11k) \quad \checkmark$$

$$(6k)^3 + 3(6k)^2 + 3(6k) + 1$$

$$2) n=6k+1 \quad n^3+11n = (6k+1)^3 + 11(6k+1) = 6A+1 + 6B+11 = 6A+6B+12 \quad \checkmark$$

$$3) n=6k+2 \quad n^3+11n = (6k+2)^3 + 11(6k+2) = 6A+8+6B+22 = 6A+6B+30 \quad \checkmark$$

$$4) n=6k+3$$

$$5) n=6k+4$$

$$6) n=6k+5$$

Част 2 разлагане:  $n^3+11n = n(n^2+11)$

$n$  и  $n^2+11$  са с различни четности  $\Rightarrow$  ние 1 от тях се дели на 2

деление на 3:  $3 \nmid n(n^2+2)$

$$1) n=3k \quad 3k((3k)^2+2) \quad \checkmark$$

$$2) n=3k+1 \quad (3k+1)^2+2 = 3A+1+2 = 3A+3$$

$$3/n^2+2 \Rightarrow 3/n(n^2+2) \quad \checkmark$$

$$3) n=3k+2 \quad (3k+2)^2+2 = 3A+4+2 = 3A+6$$

$$3/n^2+2 \Rightarrow 3/n(n^2+2) \quad \checkmark$$

и  $3/n, n^2$  дава остатък 1 при деление на 3

Зад. 2 Да се докаже, че  $\forall n \in \mathbb{N}$   $16/5^{n+1} - 4n - 5$

настъпва 3: индукция

Нека за произв.  $k$  е узл.  $5^{k+1} - 4k - 5 = 16M$

$$k+1: 5^{k+2} - 4(k+1) - 5 = 5 \cdot 5^{k+1} - 4k - 5 - 4 = \underbrace{5^{k+1} - 4k - 5 + 4 \cdot 5^{k+1} - 4}_{\text{гено } 16}$$

Доказваме  $16/4 \cdot 5^{k+1} - 4$

$$4 \cdot 5^{k+1} - 4 = 4 \cdot (5^{k+1} - 1) = 5^{k+1} \text{ дава остатък } 1 \text{ при деление на 4 т.е. } 5^{k+1} - 1 \text{ дава остатък } 0 \Rightarrow 4/5^{k+1} - 1 \\ = 4 \cdot 4 \cdot T = 16T \Rightarrow 16/4 \cdot 5^{k+1} - 4$$

II решение:

$$5^{n+1} - 4n - 5 = 5(5^n - 1) - 4n = 5(5-1)(5^{n-1} + 5^{n-2} + \dots + 1) - 4n = 4 \cdot (5(5^{n-1} + 5^{n-2} + \dots + 1) - n) = 4(5n - n) = 4 \cdot 4n = 16n$$

Алгоритъм на Евклид за търсене на HOD

$$(126, 54) \quad 126 = 2 \cdot 54 + 18 \\ 54 = 2 \cdot 18 + 0 = (126, 54) \\ 18 = 1 \cdot 18 + 0$$

Тъждество на базу на  $\mathbb{Z}$   $\exists u, v \in \mathbb{Z}$  т.е.  $ua + vb = (a, b)$

Пример  $(38, 35)$

$$\begin{aligned} 38 &= 1 \cdot 35 + 3 & 1 = 3 - 1 \cdot 2 = (38 - 1 \cdot 35) - (35 - 1 \cdot 3) = \\ 35 &= 11 \cdot 3 + 2 & = (38 - 1 \cdot 35) - (35 - 11(38 - 1 \cdot 35)) = \\ 3 &= 1 \cdot 2 + 1 & = 38 - 1 \cdot 35 - 35 + 11(38 - 1 \cdot 35) = \\ 2 &= 2 \cdot 1 + 0 & = 38 - 2 \cdot 35 + 11 \cdot 38 - 11 \cdot 35 = \\ && = 12 \cdot 38 - 13 \cdot 35 \end{aligned}$$

Теорема: Съществуват безброй много прости числа.

Д-бо: Допускаме противното т.е., че има краен брой прости числа  $p_1, \dots, p_k$ .

$$A = p_1 \cdots p_k / -1$$

$$A - 1 = p_1 \cdots p_k - 1$$

има поне 1 просто число  $p_m$ , което дели  $A - 1$ , което дели и  $p_1 \cdots p_k - 1$ , но  $p_m \neq p_1, \dots, p_k$

$\Rightarrow$  съществува просто число извън  $p_1, \dots, p_k$

def. Нека  $m \in \mathbb{N}$ ,  $a, b \in \mathbb{Z}$ . Казваме, че  $a$  е „сравнимо“ с  $b$  по модул  $m$  и пишем  $a \equiv b \pmod m$ , ако

$m | a - b$ . Еквивалентно,  $a \equiv b \pmod m$ , ако  $a$  и  $b$  имат равни остатъци при деление с  $m$

Пример:  $1 \equiv 13 \pmod 4$   $15 \equiv -1 \pmod {16}$

## Свойства:

- 1)  $a \equiv a \pmod{m}$  рефлексивност
  - 2)  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$  симетричност
  - 3)  $a \equiv b \pmod{m} \text{ и } b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$  транзитивност
  - 4)  $a_1 \equiv b_1 \pmod{m} \text{ и } a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$
  - 5)  $a \cdot n \equiv b \cdot n \pmod{m} /:n \Rightarrow a \equiv b \pmod{\frac{m}{(n,m)}}$  Ако  $(n,m)=1 \Rightarrow a \equiv b \pmod{m}$
- "≡" е релация на еквивалентност

Задача 2 Да се намерят последните 2 цифри на

$$A) 12^3 = (10+2)^3 = \underbrace{10^3}_{\equiv 0(100)} + \underbrace{3 \cdot 10^2 \cdot 2}_{\equiv 0(100)} + 3 \cdot 10 \cdot 2^2 + 2^3$$

$$12^3 \equiv 3 \cdot 10 \cdot 2^2 + 2^3 \equiv 120 + 8 \equiv 128 \equiv 28 \pmod{100}$$

$$B) 33^4 = (3 \cdot 11)^4 = 3^4 \cdot 11^4 = \underbrace{9^2}_{(10-1)} \cdot \underbrace{11^4}_{(10+1)} = (10-1)^2 \cdot (10+1)^4 = [(10-1)(10+1)]^2 \cdot (10+1)^2 = (100-1)^2 \cdot (10+1)^2 \equiv 1 \pmod{100} \equiv 2 \cdot 10 + 1 \pmod{100}$$

$$33^4 \equiv 21 \pmod{100}$$

Функцията Ойлер  $\varphi(n)$  - бројт на всички ест. числа  $< n$ , които са взаимнопрости с  $n$ .

Пример:  $\varphi(6) = 1, \cancel{2}, \cancel{3}, \cancel{4}, 5 \quad \varphi(1) = 1$

Th. на Ойлер-Ферма  $a^{\varphi(n)} \equiv 1 \pmod{n} \quad \forall a, n \in \mathbb{N}$ . Ако  $n$  е прост:  $a^{n-1} \equiv 1 \pmod{n}$

$\phi$ -а на Ойлер свойства:

1) Ако  $n$  е просто  $\varphi(n) = n-1$

4)  $(a,n)=1 \quad a^{\varphi(n)} \equiv 1 \pmod{n}$

2) Ако  $n = p^s$ ,  $p$ -просто  $\Rightarrow \varphi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1)$

3) Ако  $n = n_1 \cdot n_2$   $(n_1, n_2) = 1 \Rightarrow \varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$

Задача 3. Да се намери остатъка на  $(4^{100} + 7^{100})^{100}$  при делителя 13

$$4^{12} \equiv 1 \pmod{13} \quad 7^8 \pmod{13} \quad 7^{12} \equiv 1 \pmod{13} \quad 7^8 \pmod{13}$$

$$\begin{aligned} & \times (4^{96} \equiv 1 \pmod{13}) \\ & 4^4 \equiv 16^2 \equiv 3^2 \equiv 9 \pmod{13} \\ & 4^{100} \equiv 9 \pmod{13} \end{aligned}$$

$$\begin{aligned} & \times (7^{96} \equiv 1 \pmod{13}) \\ & 7^4 \equiv 49^2 \equiv 10^2 \equiv 100 \equiv 9 \pmod{13} \\ & 7^{100} \equiv 9 \pmod{13} \end{aligned}$$

$$18^{100} \equiv ? \pmod{13} \quad 18^{12} \equiv 1 \pmod{13}$$

$$18^{96} \equiv 1 \pmod{13}$$

$$18^4 = 5^4 \equiv 25^2 \equiv (-1)^2 \equiv 1 \pmod{13}$$

$$\Rightarrow 18^{100} \equiv 1 \pmod{13}$$

задача 4 Да се намери остатъкът на  $(4^{100} + 7^{100})^{100}$  при деление на 17

задача 5 Да се намерят всички чести числа, за които  $a_n = \frac{4n^2 - 4n + 25}{dn-1} \in \mathbb{Z}$  (e член)

$$4n^2 - 4n + 25 = (2n-1)^2 + 24$$

$a_n = dn-1 + \frac{24}{dn-1} \in \mathbb{Z} \Rightarrow \frac{24}{dn-1} \in \mathbb{Z} \Rightarrow$  търсим такива  $n$ , че  $dn-1 | 24$

Делителите на 24 са  $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$

$$6) \frac{4n^2 - 4n + 25}{dn-1} = dn-1 \cdot \frac{dn+24}{dn-1} = dn + \frac{24}{dn-1} \Rightarrow dn-1 = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$$

задача 6 да се докаже, че съществува безброй много прости числа от вида  $4k+3$

Доказателство: Допускаме противното: има крайен брой прости числа от вида  $4k+3$

Задачи прости числа имат вида  $4k+1$  или  $4k+3$ .

$$\text{Нека } A = (4k_1+3)(4k_2+3) \dots (4k_m+3) / 4, -1$$

$$4A-1 = 4(4k_1+3)(4k_2+3) \dots (4k_m+3) - 1$$

$$4A-1 \equiv -1 \equiv 3 \pmod{4}$$

$4A-1$  е число от вида  $4k+3$

Допускаме, че  $4A-1$  има само прости делители от вида  $4k+1$  т.е.

$$4A-1 = (4k'_1+1)(4k'_2+1) \dots (4k'^n+1) \equiv \underbrace{1 \dots 1}_{t \text{ четни}} = 1 \pmod{4}$$

Но  $4A-1 \equiv 3 \pmod{4} \Rightarrow 4A-1$  има някои 1 делители от вида  $4k+3$

Но  $4t+3 \neq 4k_i+3 \quad i=1, \dots, n$

задача 6 За кои прости числа  $p$  е изпълнено  $3^{\frac{p-1}{2}} \equiv 12 \pmod{p}$   $\otimes$

Доказателство: 1)  $p=3 \quad 3^1 \equiv 12 \equiv 0 \pmod{3}$

2)  $p \neq 3 \quad 3^{p-1} \equiv 1 \pmod{p} \quad 3^{p-1} \equiv 144 \pmod{p} \Rightarrow 1 \equiv 144 \pmod{p} \Rightarrow p / 144-1 = 143 \quad 143=11 \cdot 13$

Проверка дали  $p=11$  и  $p=13$  изпълняват  $\otimes$

$$3^5 \stackrel{?}{=} 12 \pmod{11} \quad 3^2 \equiv 9 \pmod{11}$$

$$3^4 \equiv 1 \pmod{11} \quad 3^5 \equiv 12 \pmod{11}$$

$$3^6 \equiv 12 \pmod{11} \quad 3^3 \equiv 1 \pmod{13} \quad 3^5 \equiv 1 \pmod{5} \quad 1 \not\equiv 12 \pmod{13}$$