

a je delitelne' $m \Leftrightarrow a \equiv 0 \pmod{m}$

$m = 3$

zb. 0

$-3 \equiv 0 \equiv 3 \equiv 6$

zb. 1

$-2 \equiv 1 \equiv 4 \equiv 7$

zb. 2

$-1 \equiv 2 \equiv 5 \equiv 8$

v ka'ede'm r'adku
narzajem se list
0 usrobet m

Minule: a ddva' zb. 1 $\Rightarrow a \cdot b$ ddva' zb. 1
 b ddva' zb. 1

$a \equiv 1 \pmod{m} \Rightarrow a \cdot b \equiv 1 \pmod{m}$
 $b \equiv 1 \pmod{m}$

$$a \equiv 2$$

$$b \equiv 2$$

$$\Rightarrow a \cdot b \equiv 4$$

$$a \equiv b, \quad c \equiv d \quad \stackrel{?}{\Rightarrow}$$

$$b - a = \xi \cdot m \quad d - c = \ell \cdot m$$

$$a + c \equiv b + d \quad (\text{mod } m)$$

$$(b + d) - (a + c)$$
$$= (b - a) + (d - c)$$

$$= \xi \cdot m + \ell \cdot m$$

$$= (\xi + \ell) \cdot m$$

spec.

$$m \equiv 0, \quad 0 \equiv m$$

$$a \equiv b, \quad c \equiv d \quad \stackrel{?}{\Rightarrow} \quad a \cdot c \equiv b \cdot d$$

$$b = a + \xi m, \quad d = c + \ell m$$

$$b \cdot d = a \cdot c + x \cdot m$$

$$(a + \ell m)(c + l m) = ac + a l m + \ell m c + \ell l m^2 \\ = ac + \underbrace{(a l + \ell c + \ell l m)}_{x} \cdot m$$

spec

$$a \equiv b, a \equiv b \Rightarrow a^x \equiv b^x \\ a^2 \equiv b^2, a \equiv b \Rightarrow a^3 \equiv b^3$$

delem:

$$a \equiv b \pmod{m}$$

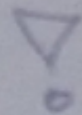
$$3 \equiv 24 \pmod{7}$$

$$\Downarrow 1 \equiv 8 \pmod{7}$$

$$3 \equiv 24 \pmod{3}$$

$$\Downarrow 1 \equiv 8 \pmod{3} \text{ neplati}$$

3 nesodelno s 7



Chceme $26 \mid 5^{20}$

$$25 \equiv -1 \pmod{26}$$

$$\Leftrightarrow 5^{20} \equiv 0 \pmod{26}$$

$$5^{20} \equiv \left((5^2)^2 \right)^5 \equiv (25^2)^5 \equiv \left((-1)^2 \right)^5 \equiv 1^5 \equiv 1$$

\Rightarrow není dělitelné, dáva zbytek 1

$$(a+b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2 \pmod{2}$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \equiv a^3 + b^3 \pmod{3}$$

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \\ \equiv a^5 + b^5 \pmod{5}$$

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots +$$

$$+ \binom{p}{p-2} a^2 b^{p-2} + \binom{p}{p-1} a b^{p-1} + b^p$$

↳ chceme ukázat, že
prostorům členy jsou
dělitelné p

Jinak: $\binom{p}{k} \stackrel{?}{\equiv} 0 \pmod{p}$ pro $0 < k < p$

$$\frac{p(p-1) \dots (p-k+1)}{k(k-1) \dots 1}$$

dělitelné p není dělitelný p

Počítáme $(47, 39) = 1 = \underline{47 \cdot k + 39 \cdot l}$

a uvažeme modulo 47

$$1 \equiv \frac{47 \cdot k}{\equiv 0} + 39 \cdot l \pmod{47}$$

$$1 \equiv 39 \cdot l \pmod{47}$$

Konkrétně:

47	39	
1	0	47
0	1	39
1	-1	8
-4	5	7
5	-6	1

$$5 \cdot 47 - 6 \cdot 39 = 1$$
$$-6 \cdot 39 \equiv 1 \pmod{47}$$

$$x \equiv 41 \text{ nebo}$$
$$x \equiv -6$$

Jinak (cca 2/3 práce): vše modulo 47

$$47 \cdot x \equiv 0$$

$$39 \cdot x \equiv 1$$

$$8 \cdot x \equiv -1$$

$$7 \cdot x \equiv 5$$

$$x \equiv -6$$

12 | ~~240~~ 240

||

||

$$2^2 \cdot 3$$

$$2^4 \cdot 3 \cdot 5$$

$$2 \leq 4$$

$$1 \leq 1$$

$$0 \leq 1$$

Kolik je dělitelů 240?

$$2^a \cdot 3^b \cdot 5^c$$

$$0 \leq a \leq 4 \quad 5 \text{ možností}$$

$$0 \leq b \leq 1 \quad 2 \text{ možnosti}$$

$$0 \leq c \leq 1 \quad 2 \text{ možnosti}$$

$$\text{Dělitelů je } 5 \cdot 2 \cdot 2 = 20$$