a je dělitelné $m \iff a \equiv 0 \pmod m$

$m = 3$

zb. 0 $\quad -3 \equiv 0 \equiv 3 \equiv 6$

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

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

---

v každém řádku navzájem se liší o násobek m

Minule:

a dává zb. 1
b dává zb. 1
$\Rightarrow$ $a \cdot b$ dává zb 1

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

$a \equiv 2$

$b \equiv 2$

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

$a \equiv b \;,\; c \equiv d \quad \overset{?}{\Longrightarrow} \quad a+c \equiv b+d \pmod{m}$

$b - a = k \cdot m \qquad d - c = l \cdot m$

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

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

$= k \cdot m + l \cdot m$

$= (k+l) \cdot m$

---

spec. $\quad m \equiv 0, \quad 0 \equiv m$

$a \equiv b \;,\; c \equiv d \quad \overset{?}{\Longrightarrow} \quad a \cdot c \equiv b \cdot d$

$b = a + km \;,\; d = c + l \cdot m$

$b \cdot d \overset{?}{=} a \cdot c + x \cdot m$

$(a + km)(c + lm) = ac + alm + kmc + kl m^2$

$= ac + (\underbrace{al + kc + kl m}_{x}) \cdot m$

---

spec $a = b, \quad a \equiv b \Rightarrow a^c = b^c$

$a^2 = b^2, \quad a = b \not\Rightarrow a^3 \equiv b^3$

---

dělení: ~~$ab \equiv ac \pmod{m}$~~

$3 \equiv 24 \pmod 7$ ⇓

$1 \equiv 8 \pmod 7$

$3 \equiv 24 \pmod 3$ ⇓

$1 \equiv 8 \pmod 3$ neplatí

3 nesoudělné s 7

▽
0

Chceme $26 \mid 5^{20}$ $\qquad 25 \equiv -1 \pmod{26}$

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

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

$\Rightarrow$ není dělitelné, dává zbytek 1

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

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

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

$$(a+b)^p = a^p + \underbrace{\binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-2} a^2 b^{p-2} + \binom{p}{p-1} a b^{p-1}}_{\text{chceme ukázat, že prostřední členy jsou dělitelné } p} + b^p$$

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

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$

dělitelné p — není dělitelný p

Počítejme $(47, 39) = 1 = 47 \cdot k + 39 \cdot l$

a uvažme modulo 47

$$1 \equiv \underbrace{47 \cdot k}_{\equiv 0} + 39 \cdot l \quad (47)$$

$$1 \equiv 39 \cdot l \quad (47)$$

Konkrétně:

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

$5 \cdot 47 - 6 \cdot 39 = 1$

$-6 \cdot 39 \equiv 1 \quad (47)$

$x \equiv 41$ nebo $x \equiv -6$

Jinak (cca 2/3 práce): vše modulo 47

$$47 \cdot x \equiv 0$$
$$39 \cdot x \equiv 1$$
$$8x \equiv -1$$
$$7x \equiv 5$$
$$x \equiv -6$$

$121 \mid$ [illegible] 240

$\| \qquad \|$

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

$2 \leq 4$

$1 \leq 1$

$0 \leq 1$

Kolik je dělitelů 240?

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

$0 \leq a \leq 4$ 5 možností

$0 \leq b \leq 1$ 2 možnosti

$0 \leq c \leq 1$ 2 možnosti

Dělitelů je $5 \cdot 2 \cdot 2 = 20$