

$m=7$   
 $9 \equiv 30 \pmod{7}$  (ANO)  
 $9 = \cancel{14} + 2$      $30 = \cancel{21} + 9$

$30 - 9 \equiv 2 - 2 \equiv 0$   
 $9 - 30 \equiv -21 \equiv 0$

$11 \equiv -3$   
 $9 + 11 \equiv 30 - 3$   
 $20 \equiv 27$

$a = b + t_1 m$   
 $b = c + t_2 m$   
 $\Downarrow$   
 $a = c + (t_1 + t_2) m$

úno 26-13:59

$7 \equiv 2 \pmod{5}$   
 $9 \equiv -1$   
 $7 \cdot 9 \equiv -2$

$16 \equiv 1$      $a = b + t_1 m$   
 $a' = b' + t_2 m$   
 $a \cdot a' = b \cdot b' + m(b t_2 + t_1 b' + t_1 t_2 m)$

$50 \equiv 70 \pmod{5}$  ?  
 $5 \neq 7$  nelze dělit  
 $25 \equiv 35 \pmod{5}$  lze dělit

úno 26-14:22

$5^{20} \pmod{26}$  (?)  
 $5^2 \equiv 26 \equiv -1$   
 $5^{20} = (5^2)^{10} = (-1)^{10} = 1$

$5^{20} \pmod{27}$   
 $5^2 \equiv -2$   
 $5^{20} \equiv (-2)^{10} \equiv (-5)^2 \equiv -2$

úno 26-14:30

$p$  prvočíslo  $\Rightarrow a^p + b^p \equiv (a+b)^p \pmod{p}$

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

$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!}$  ←  $p$  dělí čísl.  $k!$   
 není dělitelný 2, 3, ...,  $k$  pro  $1 < k < p$

$\Rightarrow \binom{p}{k} \equiv 0 \pmod{p}$

úno 26-14:35

$168 = 2 \cdot 84 = 2 \cdot 2 \cdot 42 = 2 \cdot 2 \cdot 2 \cdot 21$   
 $= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 = 2^3 \cdot 3 \cdot 7$

Resty modulo  $m$ :  $\{0, 1, \dots, m-1\}$

$m=7$ :  $\{0, 1, 2, 3, 4, 5, 6\}$   
 $\{-3, -2, -1, 0, 1, 2, 3\}$

$m=3$ :  $\{0, 1, 2\}$

$m=4$ :  $\{0, 1, 2, 3\}$   
 $2 \cdot 2 \equiv 0$

úno 26-15:01

Pravidla pro dělitelnost:  
 $1 \leq n \leq 13$

- $a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0 \equiv a_0$
- $a_n 10^n + \dots + a_1 10 + a_0 \equiv a_0 + a_1 + \dots + a_n$
- test
- $100 \equiv 0$
- $10 \equiv 0$
- zároveň 3, 2
- $10 \equiv 3, 100 \equiv 2, 1000 \equiv -1$   
 $a \cdot 1000 + b \equiv b - a$   
 $2019 \cdot 19 \equiv 19 - 2019 \equiv -2$

poslední dvojčíslí  
 $a_n 10^n + \dots + a_2 10^2 + a_1 10 + a_0 \equiv a_1 + a_2 + \dots + a_n$   
 $2019 \equiv 6$      $2019019 \equiv 2$   
 $(13)$      $2019 \equiv 19 - 2 \equiv -5$   
 $2019 \cdot 19 \equiv 19 - 2019 \equiv -2$   
 $\equiv 3$

úno 26-15:18

$$\begin{aligned}
 n &= p_1^{m_1} \cdot p_2^{m_2} \cdots p_t^{m_t} \\
 m &= q_1^{m_1} \cdot q_2^{m_2} \cdots q_e^{m_e} \\
 &[2 \cdot 2 \cdot 7 \cdot 3 \cdot 3 \cdot 5, 2 \cdot 2 \cdot 3]
 \end{aligned}$$

úno 26-15:37

$$(p-1)(p^n + p^{n-1} + \dots + p^0) = p^{n+1} - 1$$

úno 26-15:42