

Arithmetická funkce  
 $f: \mathbb{N} \rightarrow \mathbb{N}$

multiplicativní:  $f(pq) = f(p)f(q)$   
 Sdělitel  $p, q$   $(p, q) = 1$

příklad:  $f(p) =$  počet dělitelů čísla  $p$

$p = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$   $\rightarrow$  rozděl na prvočte

dělitelé:  $p_1^1 \cdot p_1^2 \cdot \dots \cdot p_1^{\alpha_1}$   $0 \leq \lambda_i \leq \alpha_i$   
 je to multiplicativní

bře 5-14:03

12 má dělitele:  $1, 2, 3, 4, 6, 12$   
 $f(12) = 6$   $12 = 3 \cdot 4$   $(3, 4) = 1$   
 $f(3) = 2$   $f(4) = 3$   $12 = 2 \cdot 6$   
 $f(2) = 2$   $f(6) = 4$

9 prvočíslo  
 $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$

$\varphi$  .. Eulerova funkce  
 $p$  prvočíslo  $\Leftrightarrow \varphi(p) = p-1$

$\varphi(12)$ :  $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$   
 $\varphi(12) = 4$   $\varphi(3) = 2$ ,  $\varphi(4) = (2-1)2 = 2$

bře 5-14:11

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18$   
 $3^2 \Rightarrow$   $6^2$  není  $3^2$  dělitel

|   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |
|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 1 | 1 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 2  | 1  | 2  | 1  | 1  | 1  | 1  | 1  | 1  |

bře 5-14:21

$\varphi(p) = (p-1) = p(1 - \frac{1}{p})$   
 $= \frac{p}{p}(p-1) = p-1$

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

$\varphi(m) =$  # nevdělných čísel

$(x, a \cdot b) = 1 \Leftrightarrow (x, a) = 1 \wedge (x, b) = 1$   
 $(a, b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

bře 5-14:32

Eulerova věta:  $(a, m) = 1$   
 $\Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

Příklad:  
mod 7

|           |           |           |
|-----------|-----------|-----------|
| $a=3$     | $a=2$     | $a=4$     |
| $a^1 = 3$ | $a^1 = 2$ | $a^1 = 4$ |
| $a^2 = 2$ | $a^2 = 4$ | $a^2 = 2$ |
| $a^3 = 6$ | $a^3 = 1$ | $a^3 = 1$ |
| $a^4 = 4$ | $a^4 = 2$ | $a^4 = 4$ |
| $a^5 = 6$ | $a^5 = 4$ | $a^5 = 6$ |
| $a^6 = 1$ | $a^6 = 1$ | $a^6 = 1$ |

$\varphi(7) = 6$

$6^2 = 1$

bře 5-14:41

$7^{77} \pmod{100}$

$(7, 100) = 1$   $7^{\varphi(100)} = 1$  — Euler  
 $\varphi(100) = \varphi(4 \cdot 25) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$

$7^{77} = 7^{40} \cdot 7^{37} = 7^{-3} = (7^{-1})^3 \pmod{100}$   
 $7^{-1} = 43$   $\mathbb{Z}$  invertibilní

$7^2 = 49$   $49^2 \equiv (50-1)^2 \equiv 0 - 0 + 1 \checkmark$   
 $\Rightarrow$  mod 7 je 4  $\Rightarrow 7^7 = 4^6 + 6 = 4^6 + 1$   
 $\Rightarrow 7^{77} = 7 \pmod{100} = 7$

bře 5-14:49

$m=13$       $\varphi(13)=12$

$a=3$   
 $a^2 \equiv 9$      3 má řád 3 mod 13  
 $a^3 \equiv 1$

$b \equiv -4$   
 $b^2 = 16 \equiv 3$      -4 má též řád 3 mod 13  
 $b^3 \equiv +1$

bře 5-15:14

$a \in \mathbb{N}$   
 $a^{rs} = (a^r)^s$       $a^{r+s} = a^r \cdot a^s$

$\sim \mathbb{Z}_m$  je to před!

$a^t \equiv a^s \pmod{m}$   
 $\Downarrow$   
 $t \equiv s \pmod{\text{"řád } a"}$

bře 5-15:19

Pro jaké  $m$  je  $\varphi(m)=30$ ?

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$       $p$  je dle 7 u28

$\varphi(m) = (p_1-1)p_1^{\alpha_1-1} \cdot (p_2-1)p_2^{\alpha_2-1} \cdot \dots$

$\forall (p-1) | 30 \Rightarrow (p-1) \in \{1, 2, 3, 5, 6, 10, 15, 30\}$   
 $p \in \{2, 3, 7, 11, 31\}$   
 $\Rightarrow m = 2^{\alpha} \cdot 3^{\beta} \cdot 7^{\gamma} \cdot 11^{\delta} \cdot 31^{\epsilon}$

$\varphi(m) = 2^{\alpha-1} \cdot 2 \cdot 3^{\beta-1} \cdot 3 \cdot 7^{\gamma-1} \cdot 7 \cdot 11^{\delta-1} \cdot 11 \cdot 31^{\epsilon-1} \cdot 31 = 30$

( $\alpha=1$  atd) tedy  $\Rightarrow m = 31$  nebo  $m = 62$   
 (in  $\alpha=0, \delta=0, \dots$  k tomu)

bře 5-15:21