	úplná soustava zbytků		
-4	0	4	$\dots$
-3	$\boxed{1}$	5	$\dots$
-2	2	6	$\dots$
-1	$\boxed{3}$	7	$\dots$

redukovaná soustava zbytků

Zbytkové třídy mod 4

$(a,4)=1$ závisí pouze na třídě a mod 4

$$\dots = (1,4) = (5,4) = (9,4) = \dots$$
$$(1,4) = 1$$

vidíme $\varphi(4) = 2$

Př. $\varphi(p) = p-1$, protože mezi $1,\dots,p$ je pouze p soudělné s p

Př. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, protože mezi $1,\dots,p^\alpha$ jsou pouze $p, 2p, 3p, \dots, p^{\alpha-1}\cdot p$ soudělná s p

f multiplikativní

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

$$f(a) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$$

– f je určena hodnotami na mocninách prvočísel

kladných

Př. $\tau(a)$ ... počet dělitelů čísla a

$$\tau(a) = (\alpha_1+1) \cdots (\alpha_k+1)$$

je multiplikativní ... $f(p^\alpha) = \alpha+1$

Uvidíme, že φ je multiplikativní, takže

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

$$\varphi(a) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) = (p^{\alpha_1} - p^{\alpha_1 - 1}) \cdots (p^{\alpha_k} - p^{\alpha_k - 1})$$

Př. $\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3)\,\varphi(3^2)$

$$= (2^3 - 2^2)(3^2 - 3^1) = (8-4)(9-3) = 24$$

Alternativně: $p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$

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

$$\varphi(a) = \underline{p_1^{\alpha_1}} \left(1 - \frac{1}{p_1}\right) \cdots \underline{p_k^{\alpha_k}} \left(1 - \frac{1}{p_k}\right)$$

$$= \underline{a} \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Pr. $n = 12$

$$\underline{\tfrac{1}{12}},\ \tfrac{1}{6},\ \tfrac{1}{4},\ \tfrac{1}{3},\ \underline{\tfrac{5}{12}},\ \tfrac{1}{2},\ \underline{\tfrac{7}{12}},\ \tfrac{2}{3},\ \tfrac{3}{4},\ \tfrac{5}{6},\ \underline{\tfrac{11}{12}},\ \tfrac{1}{1}$$

$\frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}$ ... $\varphi(12) = 4$

$\frac{1}{6}, \frac{5}{6}$ ... $\varphi(6) = 2$

$\frac{1}{4}, \frac{3}{4}$ ... $\varphi(4) = 2$

$\frac{1}{3}, \frac{2}{3}$ ... $\varphi(3) = 2$

$\frac{1}{2}$ ... $\varphi(2) = 1$

$\frac{1}{1}$ ... $\varphi(1) = 1$

$$\varphi(12) + \varphi(6) + \varphi(4) + \varphi(3) + \varphi(2) + \varphi(1) = 12$$

$$\varphi(12) = 12 - \varphi(6) - \varphi(4) - \varphi(3) - \varphi(2) - \varphi(1)$$

$$= 12 - (6 - \varphi(3) - \varphi(2) - \varphi(1))$$

$$- (4 - \varphi(2) - \varphi(1))$$

$$- (2 - \varphi(1))$$

$$- 1$$

$$= \dots = 12 - \frac{12}{2} - \frac{12}{3} + \frac{12}{2\cdot 3}$$

$$= 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$$

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

spec. případ: $m = p$ prvočíslo $\Rightarrow \varphi(p) = p-1$

Fermatova věta: $(a,p) = 1 \rightarrow a^{p-1} \equiv 1 \pmod{p}$

! Pokud $(a,p) \neq 1$, tj $p | a \Leftrightarrow a \equiv 0 \pmod{p}$ ⑥

$a^{p-1} \not\equiv 1 \pmod{p}$

$m = 11, \quad a = 2$

$a^0 \equiv 1 \quad a^1 \equiv 2 \quad a^2 \equiv 4 \quad a^3 \equiv 8 \quad a^4 \equiv 5$

$a^5 \equiv -1 \quad a^6 \equiv -2 \quad a^7 \equiv -4 \quad a^8 \equiv -8 \quad a^9 \equiv -5$

$a^{10} \equiv 1$ řád 2 modulo 11 je $10 = \varphi(11)$

$\rightarrow$ 2 je primitivní kořen mod 11

$m = 11, \quad a = 3$

$a^0 \equiv 1 \quad a^1 \equiv 3 \quad a^2 \equiv 9 \quad a^3 \equiv 5 \quad a^4 \equiv 4$

$a^5 \equiv 1$ řád 3 modulo 11 je 5

$a \equiv b \pmod{m}$ nesoudělná s m

$r \equiv s \pmod{\underline{\varphi(m)}}$!

$\Longrightarrow a^r \equiv b^s \pmod{m}$

$$a^s \equiv a^t \pmod m \iff s \equiv t \pmod r$$

$$a^{\varphi(m)} \equiv 1 \equiv a^0 \pmod m \Rightarrow \varphi(m) \equiv 0 \pmod r$$

$$\iff r \mid \varphi(m).$$

$$ax \equiv b \pmod m \qquad (\text{zadme pro } b = 1)$$

Pokud $(a, m) = 1$, podle Eulerovy věty

$$a^{\varphi(m)} \equiv 1 \quad \ldots \quad a \cdot \underbrace{a^{\varphi(m)-1}}_{\text{inverze k } a \text{ modulo } m} \equiv 1$$

$/ \cdot a^{\varphi(m)-1}$

$$\underbrace{a \cdot a^{\varphi(m)-1}}_{\equiv 1} x \equiv b\, a^{\varphi(m)-1}$$

$$x \equiv b \cdot a^{\varphi(m)-1}$$

Prakticky:

$$39x \equiv 41 \quad (47)$$

podobně jako počítání inverze:

$$47x \equiv 0 \quad (47) \qquad \text{(platí vždy)}$$

$$39x \equiv 41$$

$$8x \equiv 6$$

$$7x \equiv 17$$

$$x \equiv -11 \equiv 36 \quad (47)$$

Toto bylo za předpokladu $(a,m)=1$.

Co když ne?

$78x \equiv 82 \quad (94)$

$(78, 94) = 2$ .... modulo 2 je $LHS \equiv 0 \quad (2)$

$\Rightarrow$ RHS musí být $\equiv 0 \quad (2)$ jinak nemá řešení

$78x \equiv 82 \quad (2)$

$0 \quad 0$ platí... vydělíme celou kongruenci 2

původní kongruence je ekvivalentní

$39x \equiv 41 \quad (47)$ ... vše vydělené 2

teď nesoudělné, vyřešíme jako předtím

OBECNĚ

$a \equiv b \pmod m$

$\Updownarrow$

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