Eulerova-Fermatova věta

Pozorování: 1.) $\overline{8}_{14} = \{\dots 8, 22, 36, 50, \dots\}$

$2 = \gcd(8,14) = \gcd(22,14) = \gcd(36,14) = \gcd(50,14)$

2.) $\overline{5}_{15} = \{\dots 5, 20, 35, 50, \dots\}$

$5 = \gcd(5,15) = \gcd(20,15) = \gcd(35,15) = \gcd(50,15)$

Věta: Nechť $\gcd(a,m) = d$ a $a \equiv b \pmod m$. Potom $\gcd(b,m) = d$.

Důkaz: Označme $d_a = \gcd(a,m)$; $d_b = \gcd(b,m)$ a předpokládejme, že $a \equiv b \pmod m$.
Dokážeme, že $d_a = d_b$.
$a \equiv b \pmod m \Rightarrow \exists k \in \mathbb{Z} : a - b = k.m$

α) $a = b + k.m \quad / \, b = d_b k_1, \; m = d_b m_1$
$a = d_b(k_1 + k m_1) \Rightarrow (d_b | a \wedge d_b | m) \Rightarrow \boxed{d_b \,|\, \gcd(a,m) = d_a}$

β) $b = a - km \quad / \, a = d_a \cdot a_2, \; m = d_a m_2$
$b = d_a(a_2 - k m_2) \Rightarrow (d_a | b \wedge d_a | m) \Rightarrow \boxed{d_a \,|\, \gcd(b,m) = d_b}$

$(d_a | d_b \wedge d_b | d_a) \Rightarrow |d_a| = |d_b|$. Protože $d_a, d_b \geq 0 \Rightarrow d_a = d_b$.

Důsledek: Nechť $\gcd(a,m) = 1$ a $a \equiv b \pmod m$. Potom $\gcd(b,m) = 1$.

Poznámka: Znamená to, že když je a nesoudělné s m, pak také každý prvek ze zbytkové třídy $\overline{a}_m$ je nesoudělný s m.

Př: $\overline{3}_5 = \{\dots, 3, 8, 13, 18, \dots\}$ a $\gcd(3,5) = \gcd(8,5) = \gcd(13,5) = \gcd(18,5) = \dots = 1$

Ještě jinak: To znamená, že $\gcd(a,m)$ nezávisí na výběru reprezentanta $\overline{a}_m$!

Eulerova-Fermatova věta

Pozorování: $\gcd(3,5)=1$ a uvažujme prvky ze zbytkové třídy $\bar{3}_5$:

$\bar{3}_5 = \{\ldots, 3, 8, 13, 18, 23, \ldots\}$ platí, že

$\gcd(8,5) = \gcd(13,5) = \gcd(23,5) = 1$

Zdá se, že všechny prvky zbytkové třídy $\bar{3}_5$ jsou nesoudělné s 5.

Věta: Nechť $a \equiv b \pmod{n}$. Jestliže $\gcd(a,n)=1$, pak také $\gcd(b,n)=1$

Důkaz: Předpokládejme, že $\gcd(a,n)=1$ a označme $d=\gcd(b,n)$.

$$a \equiv b \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z}: a-b = k \cdot n \quad \Rightarrow$$

$$a = b + k \cdot n$$

$$d=\gcd(b,n) \Rightarrow b = d b_0, \ n = d \cdot n_0 \Rightarrow d \mid n, \text{ kde } b_0, n_0 \in \mathbb{Z} \quad \Rightarrow$$

$$a = d(b_0 + k n_0)$$

$\Rightarrow d \mid a$. Číslo d je tedy společným dělitelem čísel a, n.

Číslo d proto musí dělit i $\gcd(a,n)=1 \quad \Rightarrow \quad d=1$.

Poznámka: Dokázali jsme, že když jeden prvek zbytkové třídy $\bar{a}_n$ je nesoudělný s n, pak také všechny ostatní.

Def. (Redukovaný zbytkový systém): Redukovaným zbytkovým systémem modulo n nazveme množinu:

$$\mathbb{Z}_n^* = \{ \overline{a}_n \in \mathbb{Z}_n \mid \gcd(a,n)=1 \}$$

Př.: a) $\mathbb{Z}_6 = \{ \overline{0}_6, \overline{1}_6, \overline{2}_6, \overline{3}_6, \overline{4}_6, \overline{5}_6 \}$, $\mathbb{Z}_6^* = \{ \overline{1}_6, \overline{5}_6 \}$

Zaveďme násobení zbytkových tříd předpisem:

$$\overline{a}_n \cdot \overline{b}_n = \overline{a \cdot b}_n$$

násobení zbytkových tříd

násobení celých čísel

$\cdot$	$\overline{1}_6$	$\overline{5}_6$
$\overline{1}_6$	$\overline{1}_6$	$\overline{5}_6$
$\overline{5}_6$	$\overline{5}_6$	$\overline{1}_6$

$\Rightarrow$ Vynásobíme-li dvě zbytkové třídy ze $\mathbb{Z}_6^*$, výsledkem je zbytková třída ze $\mathbb{Z}_6^*$.

Platí to obecně pro libovolné $\mathbb{Z}_n^*$?

Ano! Vynásobíme-li a a b, kde $\gcd(a,n) = \gcd(b,n) = 1$, pak $a \cdot b$ je jistě také nesoudělné s n!

Věta: Redukovaný zbytkový systém $\mathbb{Z}_n^*$, kde $n \in \mathbb{N}$ je uzavřený vzhledem k násobení. Tzn.:

$$\forall \bar{a}_n, \bar{b}_n \in \mathbb{Z}_n^* : \quad \bar{a}_n \cdot \bar{b}_n \in \mathbb{Z}_n^*$$

Důkaz: Stačí dokázat, že $\forall n \in \mathbb{N}$:

$$(\gcd(a,n)=1 \wedge \gcd(b,n)=1) \Rightarrow \gcd(ab,n)=1$$

$$\left.\begin{array}{l} \gcd(a,n)=1 \Rightarrow \exists x_1, y_1 \in \mathbb{Z}: \quad ax_1 + ny_1 = 1 \\ \gcd(b,n)=1 \Rightarrow \exists x_2, y_2 \in \mathbb{Z}: \quad bx_2 + ny_2 = 1 \end{array}\right\} \Rightarrow$$

$$(ax_1 + ny_1)(bx_2 + ny_2) = 1$$

$$ab\underbrace{x_1x_2}_{x_0} + n\underbrace{(y_1bx_2 + y_1ny_2 + ax_1y_2)}_{y_0} = 1$$

$$abx_0 + ny_0 = 1 \qquad (*)$$

Jestliže $d = \gcd(ab, n)$, pak $ab = d \cdot k_1$, $n = d \cdot k_2$, kde $k_1, k_2 \in \mathbb{Z} \Rightarrow$
$\Rightarrow$ dosadíme-li do $(*)$:

$$d(k_1x_0 + k_2y_0) = 1$$

$$d \mid 1 \qquad \Rightarrow \qquad d = \gcd(ab, n) = 1.$$

Def. (Eulerova funkce): Eulerovou funkcí nazveme funkci $\varphi: \mathbb{N} \to \mathbb{N}$, která je dána předpisem:

$$\varphi(n) = \sum_{\substack{1 \leq a \leq n \\ \gcd(a,n)=1}} 1$$

Tzn. $\varphi(n)$ je počet přirozených čísel z množiny $\{1, 2, \dots, n\}$ nesoudělných s n. Je zřejmé, že platí:

$$|\mathbb{Z}_n^*| = \varphi(n)$$

To jest, počet prvků redukovaného zbytkového systému modulo n je roven $\varphi(n)$.

Př.: a) $\varphi(1) = 1$

b) $\varphi(2) = 1$

c) $\varphi(3) = 2$

d) $\varphi(4) = 2$

e) $\varphi(5) = 4$

f) $\varphi(6) = 2$

g) Jestliže p je prvočíslo, pak $\varphi(p) = p - 1$.

Věta (Eulerova-Fermatova): Nechť $\gcd(a,n)=1$. Potom

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Důkaz: Snažíme se dokázat, že $\overline{a^{\varphi(n)}} = (\bar{a})^{\varphi(n)} = \bar{1}$.

Víme, že $|\mathbb{Z}_n^*| = \varphi(n) \Rightarrow \mathbb{Z}_n^* = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\varphi(n)}\}$

$$\gcd(a,n)=1 \Rightarrow \underbrace{\bar{a}\cdot\bar{a}_1, \bar{a}\cdot\bar{a}_2, \dots, \bar{a}\cdot\bar{a}_{\varphi(n)}}_{\text{ukážeme, že jsou to navzájem různé zbytkové třídy:}} \in \mathbb{Z}_n^*$$

Předpokládejme, že $\underbrace{a a_i \equiv a a_j}_{\gcd(a,n)=1 \Rightarrow \text{můžeme krátit } a} \pmod{n} \Rightarrow$

$$\Downarrow$$

$$a_i \equiv a_j \pmod{n}$$

$$\Downarrow$$

$$i = j$$

$\Rightarrow$ Pro $i \neq j$ jsou $\bar{a}\bar{a}_i$ a $\bar{a}\bar{a}_j$ různé zbytkové třídy $\in \mathbb{Z}_n^*$ a je jich celkem $\varphi(n) \Rightarrow$

$$\mathbb{Z}_n^* = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\varphi(n)}\} = \{\bar{a}\bar{a}_1, \bar{a}\bar{a}_2, \dots, \bar{a}\,\bar{a}_{\varphi(n)}\} \Rightarrow$$

$$\overline{a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)}} = \overline{a a_1 \cdot a a_2 \cdot \ldots \cdot a a_{\varphi(n)}}$$

$$\underbrace{a_1 a_2 \dots a_{\varphi(n)}} \equiv a^{\varphi(n)} \cdot \underbrace{a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(n)}} \pmod{n}$$

číslo nesoudělné s n $\Rightarrow$ můžeme krátit $\Rightarrow$

$$1 \equiv a^{\varphi(n)} \pmod{n}$$

Př: Vyřešte lineární kongruenci $3X \equiv 1 \pmod{10}$

Označme $a = 3$, $n = 10$ $\Rightarrow$ $\gcd(3,10) = 1$ $\Rightarrow$

Podle Eulerovy-Fermatovy věty můžeme psát:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10

$$3^{\overbrace{\varphi(10)}^{=4}} \equiv 1 \pmod{10}$$

$$3 \cdot 3^3 \equiv 1 \pmod{10}$$

"hledané X"

$\Rightarrow$ $X \equiv 3^3 \equiv 27 \equiv 7 \pmod{10}$ a opravdu $3 \cdot 7 = 21 \equiv 1 \pmod{10}$.

Př: Nalezněte $\overline{3}_7^{-1}$.

Tzn. hledáme zbytkovou třídu $\overline{X}_7$ tak, aby platilo:

$$\overline{X}_7 \cdot \overline{3}_7 = \overline{1}_7$$

Zapsáno pomocí kongruencí, hledáme $x \in \mathbb{Z}$ splňující:

$$X \cdot 3 \equiv 1 \pmod 7$$

$\gcd(3,7) = 1$ $\Rightarrow$ $3^{\varphi(7)} = 3^6 \equiv 1 \pmod 7$

$$\Rightarrow X \equiv 3^5 \pmod 7$$

$$X \equiv 9 \cdot 9 \cdot 3 \pmod 7$$

$$X \equiv 2 \cdot 2 \cdot 3 \pmod 7$$

$$X \equiv 12 \pmod 7$$

$$X \equiv 5 \pmod 7 \Rightarrow \underline{\underline{\overline{3}_7^{-1} = \overline{5}_7}}$$

A opravdu: $\overline{5}_7 \cdot \overline{3}_7 = \overline{15}_7 = \overline{1}_7$.

Ve speciálním případě, kdy $n = p$ = prvočíslo, z Eulerovy-Fermatovy věty plyne:

Věta (Malá Fermatova): Nechť p je prvočíslo, $a \in \mathbb{Z}$, $\gcd(a, p) = 1$. Potom platí:

$$a^{p-1} \equiv 1 \pmod{p}$$

Důkaz: Stačí si uvědomit, že $\varphi(p) = p - 1$

$\square$

Tvrzení Malé Fermatovy věty lze přeformulovat pro libovolné $a \in \mathbb{Z}$:

Věta (Malá Fermatova): Nechť $a \in \mathbb{Z}$ a p je prvočíslo. Potom

$$a^{p} \equiv a \pmod{p}$$

Důkaz: Jsou dvě možnosti:

a) $\gcd(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{p} \equiv a \pmod{p}$

b) $\gcd(a, p) \neq 1 \Rightarrow a$ je násobkem $p \Rightarrow a \equiv 0 \pmod{p} \Rightarrow$

$$\underset{0}{\underset{\parallel\!\!\!|}{a^{p}}} \equiv \underset{0}{\underset{\parallel\!\!\!|}{a}} \pmod{p} \checkmark$$

$\square$