Definice kongruence

Kongruence modulo p (kde $p \in \mathbb{N}$) je relace $\equiv$ definovaná na $\mathbb{Z}$:
$x \equiv y \text{ (mod p)} \Leftrightarrow p \mid (x - y)$
$p \mid (x - y) \Leftrightarrow x - y = k \cdot p,\ k \in \mathbb{Z}$

Sčítání, odčítání, násobení kongruencí

Kongruence lze sčítat, odčítat a násobit.
$\forall n \in \mathbb{N}, x \equiv a \pmod{p}, y \equiv b \pmod{p} :$
$x \pm y \equiv a \pm b \pmod{p}$
$xy \equiv ab \pmod{p}$

Příklad 1

$(15 \cdot 19 + 17)^3 \mod 5 =$

Řešení

Nejprve upravíme výrazy modulo 5:

$$15 \mod 5 = 0, \qquad 19 \mod 5 = 4, \qquad 17 \mod 5 = 2$$

Dosadíme do výrazu:

$$(15 \cdot 19 + 17)^3 \equiv (0 \cdot 4 + 2)^3 \pmod{5}$$

Zjednodušíme:

$$(0 \cdot 4 + 2)^3 \equiv 2^3 \pmod{5}$$

Vypočítáme mocninu:

$$2^3 = 8 \quad \Rightarrow \quad 8 \mod 5 = 3$$

Konečný výsledek:

$$(15 \cdot 19 + 17)^3 \mod 5 = 3$$

Umocňování kongruencí

Obě strany kongruence lze umocnit na totéž číslo.
$\forall n \in \mathbb{N}, \forall k \in \mathbb{N}, x \equiv a \pmod{p} :$
$x^k \equiv a^k \pmod{p}$

Příklad 2

$7^5 \mod 6 =$

Řešení

Nejprve využijeme vlastnosti kongruence:

$$7 \equiv 1 \pmod 6$$

Poté umocníme obě strany:

$$7^5 \equiv 1^5 \pmod 6$$

Proto:

$$7^5 \mod 6 = 1$$

Malá Fermatova věta

Malá Fermatova věta je základní tvrzení v teorii čísel:
$a^p \equiv a \pmod p$,
kde p je prvočíslo a a je libovolné celé číslo.
Pokud a a p jsou nesoudělná čísla, platí zjednodušený tvar:
$a^{p-1} \equiv 1 \pmod p$.

Příklad 3

$17^{100} \mod 5 =$

Řešení

Podle Malé Fermatovy věty:

$$a^{p-1} \equiv 1 \pmod p, \quad \text{kde } a = 17,\ p = 5.$$

Protože $p - 1 = 4$, víme:

$$17^4 \equiv 1 \pmod 5.$$

Rozložíme exponent:

$$17^{100} = (17^4)^{25}.$$

Dosadíme za $17^4 \mod 5$:

$$(17^4)^{25} \equiv 1^{25} \equiv 1 \pmod 5.$$

Konečný výsledek: $17^{100} \mod 5 = 1$

Příklad 4

Dokažte, že pro všechna přirozená čísla n platí: $2 \mid (n^2 - n)$

Řešení

1. Důkaz pomocí algebraického rozkladu
Nejprve rozložíme výraz $n^2 - n = n(n-1)$.
Tento součin je součinem dvou po sobě jdoucích čísel n a $n-1$. Nyní je třeba ukázat, že tento součin je vždy dělitelný 2:
a) Pokud je n sudé, tj. $n = 2k$, pak $n - 1 = 2k - 1$ je liché. Součin $n(n-1) = 2k(2k-1)$ obsahuje činitel $2k$, který je sudý, a tedy celý součin je sudý.
b) Pokud je n liché, tj. $n = 2k + 1$, pak $n - 1 = 2k$ je sudé. Součin $n(n-1) = (2k+1)2k$ obsahuje činitel 2, který je sudý, a tedy celý součin je sudý. Tedy pro všechna n platí $2 \mid (n^2 - n)$.

2. Důkaz pomocí Malé Fermatovy věty
MFV: $a^p \equiv a \pmod{p}$, kde p je prvočíslo a a je libovolné celé číslo.
a) $n = 2k, k \in \mathbb{N} : n^2 - n = 4k^2 - 4k + 1 - 2k + 1 = 2(2k^2 - 3k + 1)$
b) $n \neq 2k, k \in \mathbb{N} : n^2 \equiv n \pmod{2}$ - MFV neboli $2 \mid (n^2 - n)$ - definice kongruence

3. Důkaz pomocí matematické indukce
Chceme dokázat, že pro všechna přirozená čísla n platí $2 \mid (n^2 - n)$.
Krok 1: Pro $n = 1$ máme $n^2 - n = 1^2 - 1 = 0$, 0 je dělitelná dvěma.
Krok 2: Předpokládejme, že tvrzení platí pro nějaké $n = k$, tj. $2 \mid (k^2 - k)$, což znamená, že $k^2 - k = 2m$ pro nějaké celé číslo m.
Dokážeme, že tvrzení platí i pro $n = k + 1$, tedy že $2 \mid ((k+1)^2 - (k+1))$:
$(k+1)^2 - (k+1) = k^2 + 2k + 1 - k - 1 = k^2 + k = (k^2 - k) + 2k$
Z indukčního předpokladu: $k^2 - k = 2m$, takže: $k^2 + k = 2m + 2k = 2(m+k)$.
Tento výraz je dělitelný dvěma.

4. Důkaz pomocí zbytkových tříd
Pro dělitelnost dvěma použijeme zbytkové třídy po dělení dvěma.
a) $n = 2k, k \in \mathbb{N} : n^2 - n = 4k^2 - 2k = 2k(2k-1)$... je dělitelné dvěma
b) $n = 2k - 1, k \in \mathbb{N} : n^2 - n = 4k^2 - 4k + 1 - 2k + 1 = 2(2k^2 - 3k + 1)$... je dělitelné dvěma

Příklady k procvičení

bez kalkulaček:

1. $123 \pmod 7 =$
2. Ověřte, zda platí: $212 \equiv 17 \pmod 3$
3. $(12 \cdot 19 - 8^4) \pmod 5 =$
4. $18^{501} \pmod{17} =$
5. $2^{120} \pmod 7 =$
6. $2^{501} \pmod{17} =$
7. $17^{341} \pmod 5 =$
8. $345^{123} \pmod 7 =$

9. Co jsou zbytkové třídy modulo 3 (na celých číslech)?
10. Dokažte, že pro všechna přirozená čísla n platí: $3 \mid (n^3 - n)$
11. Dokažte, že pro všechna přirozená čísla n platí: $5 \mid (n^5 - n)$

Řešení

1. $123 \pmod 7 \equiv 53 \pmod 7 = 4$

2. Ověřte, zda platí: $212 \equiv 17 \pmod 3$
   $212 \pmod 3 \equiv 2 \pmod 3 = 2$
   $53 \pmod 3 \equiv 2 \pmod 3 = 2$
   Čísla 212 a 53 dávají stejný zbytek po dělení třemi (zbytek 2), jsou ve stejné zbytkové třídě. Platí tedy, že $212 \equiv 17 \pmod 3$.

3. $(12 \cdot 19 - 8^4) \pmod 5 \equiv (2 \cdot 4 - 3^4) \pmod 5 \equiv (2 \cdot 4 - 9^2) \pmod 5 \equiv$ $(2 \cdot 4 - 4^2) \pmod 5 \equiv 3$ - $1 = 2$

4. $18^{501} \pmod{17} \equiv 1^{501} = 1$

5. $2^{120} \pmod 7 \equiv \left(2^3\right)^{40} = 1$

6. $2^{501} \pmod{17} \equiv \left(2^4\right)^{124} \cdot (2^4) \cdot 2 \pmod{17} \equiv (-1)^{124} \cdot (-2) \pmod{17} \equiv$ $-2 \pmod{17} = 15$

7. $17^{341} \pmod 5 \equiv (17^2)^{170} \cdot 17 \pmod 5 \equiv \left(-1\right)^{170} \cdot 2 \pmod 5 = 2$

8. $345^{123} \pmod 7 \equiv (65^3)^{41} \pmod 7 = 1$