KONGRUENCIE

Nech $a, b, m \in \mathbb{Z}$, $m \geq 0$. Hovoríme, že a je *kongruentné* s b *modulo* m, a píšeme

$$a \equiv b \pmod{m},$$

ak m delí $a - b$.

Pri $m \neq 0$ je to ekvivalentné s podmienkou, že čísla a a b dávajú pri delení m rovnaký zvyšok.

Kongruencia modulo m je pre každé m reláciou ekvivalencie, čo znamená, že je

a) reflexívna: $a \equiv a \pmod{m}$ pre každé $a \in \mathbb{Z}$;

b) symetrická: ak $a \equiv b \pmod{m}$, tak $b \equiv a \pmod{m}$;

c) tranzitívna: ak $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$, tak $a \equiv c \pmod{m}$.

Kongruencie modulo 0 a 1 sú podľa definície prípustné, ale nie veľmi zaujímavé: $a \equiv b \pmod{1}$ platí vždy (všetky čísla sú v 1 skupine), zatiaľ čo $a \equiv b \pmod{0}$ platí len pre $a = b$ (každé číslo je v inej "skupine").

Samozrejme, $a \equiv 0 \pmod{m}$ práve vtedy, keď $m|a$.

Pravidlá pre počítanie s kongruenciami sú zhrnuté v nasledujúcom tvrdení.

Veta 1. *Pre každé* $a, b, c, d, n, m \in \mathbb{Z}$, $m, n \geq 0$ *platí:*

(i) *ak* $a \equiv b \pmod m$ *a* $c \equiv d \pmod m$, *tak* $a + c \equiv b + d \pmod m$;

(ii) *ak* $a \equiv b \pmod m$, *tak* $a + c \equiv b + c \pmod m$;

(iii) $a \equiv b \pmod m$ *a* $c \equiv d \pmod m$, *tak* $ac \equiv bd \pmod m$;

(iv) *ak* $a \equiv b \pmod m$, *tak* $ac \equiv bc \pmod m$;

(v) *ak* $a \equiv b \pmod m$, *tak* $a^n \equiv b^n \pmod m$.

Uvedené pravidlá možno využit napríklad na tzv. *modulárne umocňovanie.*

Príklad Vypočítame zvyšok po delení čísla 5^{222} číslom 11. Použijeme kongruenciu modulo 11 a dostávame

$$5^{222} = (5^2)^{111} = 25^{111} \equiv 3^{111} = (3^3)^{37} = 27^{37} \equiv 5^{37} =$$

$$= 25^{18} \cdot 5 \equiv 3^{18} \cdot 5 = 27^6 \cdot 5 \equiv 5^6 \cdot 5 = 25^3 \cdot 5 \equiv 3^3 \cdot 5 =$$

$$= 27 \cdot 5 \equiv 5 \cdot 5 = 25 \equiv 3,$$

takže hľadaný zvyšok je 3.

Teraz uvedieme pravidlá pre krátenie kongruencií.

Veta 2 *Nech* $a, b, c, m \in \mathbb{Z}$, $c \neq 0$, $m \geq 0$.

(i) *Ak* $ac \equiv bc \pmod{mc}$, *tak* $a \equiv b \pmod{m}$.

(ii) *Ak* $ac \equiv bc \pmod{m}$ *a* $(m, c) = 1$, *tak* $a \equiv b \pmod{m}$.

Nasledujúce tvrdenie je známe ako *Malá veta Fermatova* (MVF).

Veta 3. *Pre každé prvočíslo* p *a každé* $n \in \mathbb{Z}$ *platí*

$$n^p \equiv n \pmod{p}.$$

Naviac, keď $(p, n) = 1$, *tak*

$$n^{p-1} \equiv 1 \pmod{n}.$$

Spolu s technikou modulárneho umocňovania poskytuje Malá veta Fermatova možnosť efektívneho testovania prvočíselnosti. Pre veľké čísla p (povedzme rádu 10^{100}) priame testovanie prvočíselnosti (delením) presahuje možnosti aj najrýchlejších počítačov. Efektívne však vieme zistiť, či pre zvolené n platí $n^p \equiv n \pmod p$. Ak taká kongruencia neplatí, máme istotu, že p je zložené. (Ale nezistíme tým jeho rozklad!) Ak kongruencia platí, máme aspoň 50% pravdepodobnosť, že p je prvočíslo. (Pre niektoré p tento odhad celkom neplatí a treba použiť trochu zložitejšie metódy.). Opakovaním tohoto testu sa môže istota prvočíselnosti priblížiť ľubovoľne blízko k 100%.

Z druhej strany, ak *vieme*, že modul je prvočíslo, Malá veta Fermatova urýchli modulárne umocňovanie. Zopakujme výpočet 5^{222} modulo 11. Pre $p = 11$, $n = 5$ nám MVF dáva

$$5^{10} \equiv 1 \pmod{11}.$$

Po umocnení na 22 dostávame

$$5^{220} \equiv 1^{20} = 1 \pmod{11},$$

takže

$$5^{222} = 5^{220} \cdot 5^2 \equiv 1 \cdot 25 = 25 \equiv 3,$$

čím sme dospeli k rovnakému výsledku ako predtým.

Kontrolný test

Začiatok testu (6 bodov) :

1. Počet čísel, ktoré sú kongruentné s a modulo $m > 0$ je

- [ ] 1
- [ ] 2
- [ ] m
- [ ] nekonečne veľa

2. Množina čísel, z ktorých žiadne 2 nie sú kongruentné modulo $m > 0$ môže mať

- [ ] najviac 1 prvok
- [ ] najviac 2 prvky
- [ ] najviac $m - 1$ prvkov

- [ ] najviac m prvkov
- [ ] nekonečne veľa prvkov

3. Ak $a \equiv b \pmod{m}$, $m > 0$, tak

- [ ] $a \equiv b \pmod{n}$ pre každé $n|m$
- [ ] $a \equiv b \pmod{n}$ pre každé $n < m$
- [ ] $a \equiv b \pmod{n}$ pre každé $m|n$

4. Ak $a \equiv b \pmod{m}$, $m > 0$, tak

- [ ] $n^a \equiv n^b \pmod{m}$ pre každé n
- [ ] $a^n \equiv b^n \pmod{m}$ pre každé n
- [ ] $\sqrt[n]{a} \equiv \sqrt[n]{b} \pmod{m}$ vždy keď $\sqrt[n]{a}$ a $\sqrt[n]{b}$ sú celé čísla

5. Z Malej vety Fermatovej vyplýva, že

- ☐ $7^{40} \equiv 7 \pmod{40}$
- ☐ $7^{41} \equiv 7 \pmod{41}$
- ☐ $7^{40} \equiv 1 \pmod{40}$
- ☐ $7^{41} \equiv 1 \pmod{40}$
- ☐ $7^{40} \equiv 1 \pmod{41}$
- ☐ $7^{41} \equiv 1 \pmod{41}$

6. Modulárne umocňovanie sa dá využiť na

- ☐ výpočet NSD;
- ☐ hľadanie prvočíselného rozkladu
- ☐ testovanie prvočíselnosti
- ☐ testovanie nesúdeliteľnosti

Koniec testu

Správne odpovede

Získané body:

Úspešnosť: