Modulární aritmetika

Vztah „a dělí b“ značíme $a \mid b$. Základní vlastnosti:

- $a \mid b$ a zároveň $a \mid c \implies a \mid (b + c)$,
- $a \mid b \implies a \mid bc$,
- 1 dělí cokoliv,
- cokoliv dělí 0,
- $a \mid bc$ a zároveň $\mathrm{NSD}(a, b) = 1 \implies a \mid c$,
- je-li p prvočíslo: $p \mid ab \implies p \mid a$ nebo $p \mid b$.

Definice

Řekneme, že a, b jsou *kongruentní modulo* m, pokud $m \mid a - b$. Značíme $a \equiv b \pmod{m}$.

Nechť $a \equiv c$ a zároveň $b \equiv d \pmod{m}$. To značí $m \mid (a - c)$ a zároveň $m \mid (b - d)$, takže pak i

- $a + b \equiv c + d \pmod{m}$, jelikož
  $m \mid (a - c) + (b - d) = (a + b) - (c + d)$.
- $ab \equiv cd \pmod{m}$, jelikož
  $m \mid a(b - d) + (a - c)d = ab - ad + ad - cd = ab - cd$.

Krácení $ac \equiv bc \pmod{m}$, tj. $m \mid c(a - b)$:

- Když $\mathrm{NSD}(m, c) = 1$, pak už $m \mid a - b$, tedy $a \equiv b \pmod{m}$.
- Když $c \mid m$, pak $\frac{m}{c} \mid a - b$, tedy $a \equiv b \pmod{\frac{m}{c}}$.

Obecně: $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{\frac{m}{\mathrm{NSD}(m,c)}}$.

Úloha 1

Ukažte, že $2^{60} + 7^{30}$ je násobek třinácti.

$$2^{60} + 7^{30} \equiv 16^{15} + 49^{15} \equiv 3^{15} + (-3)^{15} \equiv 3^{15} - 3^{15} \equiv 0 \pmod{13}$$

Úloha 2

Jaký zbytek po dělení sedmnácti dává 13^{2020}?

$$13^{2020} \equiv (-4)^{2020} \equiv 16^{1010} \equiv (-1)^{1010} \equiv 1^{505} \equiv 1 \pmod{17}$$

Úloha 3

Nechť $S(a)$ značí ciferný součet a v desítkové soustavě. Potom $S(a) \equiv a \pmod 9$.

Nechť $a = \overline{a_n a_{n-1} \dots a_1 a_0}$. Platí $10^i \equiv (1)^i \equiv 1 \pmod 9$, takže

$$\begin{aligned} a &= 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10 a_1 + a_0 \equiv \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 = S(a) \pmod 9. \end{aligned}$$

Úloha 4

Je dáno přirozené číslo n nesoudělné s 10. Dokažte, že nějaké číslo zapsané (v desítkové soustavě) samými jedničkami je násobkem n.

Nechť $J_k = \underbrace{11\ldots1}_{k\text{-krát}}$. Zbytků mod n je jen konečně mnoho, čísel J_k nekonečně mnoho. Pro jistá $a < b$ tak J_a a J_b dávají stejný zbytek.

$$\begin{aligned} 11\ldots11\ldots11 &= J_b \\ \underline{-\qquad\quad 1\ldots11} &= J_a \\ 11\ldots10\ldots00 &= J_{b-a}\cdot 10^a \end{aligned}$$

Platí $J_b \equiv J_a \pmod{n}$, tedy $n \mid J_a - J_b = 10^a \cdot J_{b-a}$.

Z nesoudělnosti n a 10 pak $n \mid J_{b-a}$.

Idea: některé výrazy nemusí dávat všechny zbytky mod n.

$x \pmod 7$	0	1	2	3	4	5	6
$x^2 \pmod 7$	0	1	4	2	2	4	1

Definice

Číslo a nazveme kvadratickým (ne)zbytkem mod n, pokud (ne)jde vyjádřit jako $a \equiv x^2 \pmod n$.

Pozorování: $x^2 \equiv (-x)^2$, takže kvadratických zbytků mod n je nanejvýš $\frac{n}{2} + 1$.

Příklady kvadratických zbytků:

- mod 4: 0, 1,
- mod 8: 0, 1, 4,
- mod 3: 0, 1,
- mod 9: 0, 1, 4, 7,
- mod 5: 0, 1, 4,
- mod 7: 0, 1, 2, 4.

Úloha 5

Najděte všechny dvojice přirozených čísel a, b, které splňují $a^2 = 1! + 2! + \cdots + b!$.

Zvolme n. Pro $b \geq n$ pak $b! \equiv 0 \pmod{n}$, takže

$$1! + 2! + \cdots + b! \equiv 1! + 2! + \cdots + (n-1)! \pmod{n}.$$

Zkusme najít n, pro které to bude kvadratický nezbytek:

- $n = 3$: $1! + 2! = 3 \equiv 0 \pmod{3} \longrightarrow$ kv. zbytek.
- $n = 4$: $1! + 2! + 3! = 9 \equiv 1 \pmod{4} \longrightarrow$ kv. zbytek.
- $n = 5$: $1! + 2! + 3! + 4! = 33 \equiv 3 \pmod{5} \longrightarrow$ kv. nezbytek.

Pro $b \geq 5$ tedy neexistuje řešení, vyzkoušením $b \in \{1, 2, 3, 4\}$ najdeme řešení $(a, b) = (1, 1)$ a $(a, b) = (3, 3)$.

Úloha 6

4042ciferné přirozené číslo n je zapsáno (v nějakém pořadí) 2021 nulami a 2021 jedničkami. Může n být druhou mocninou celého čísla?

Nemůže. Kdyby $n = a^2$, znamenalo by to

$$a^2 = n \equiv S(n) \equiv 2021 \equiv S(2021) \equiv 5 \pmod 9.$$

Ale 5 je kvadratický nezbytek modulo 9.

Úloha 7

Pro která n lze tabulku $n \times n$ vyplnit čísly 1 až n^2 tak, aby součet v každém sloupci i v každém řádku byl dělitelný sedmi?

Součet všech čísel v tabulce bude muset být $\frac{1}{2}n^2(n^2+1)$.

Takže $7 \mid n^2$ nebo $7 \mid n^2+1$. Ale -1 je kvadratický nezbytek mod 7, takže $7 \mid n$. Pro násobky sedmi tabulku snadno vyplníme:

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

Kdyby -1 byla kvadratický zbytek, našli bychom i další řešení. Např. pro $n = 3$ lze tabulku vyplnit tak, aby součty v řádcích i sloupcích byly násobky pěti:

5	1	4
2	6	7
3	8	9

Úloha 8

Najděte všechna celočíselná řešení rovnice $x^4 + y^4 = z^4 + 4$.

Modulo 8:
sudé $x \implies x^4 \equiv 0 \pmod 8$, liché $x \implies x^4 \equiv 1 \pmod 8$.

Pravá strana je potom 4 nebo 5, zatímco levá 0, 1 nebo 2.

Žádné řešení tedy neexistuje.

Věta (malá Fermatova)

Mějme prvočíslo p a číslo $a \not\equiv 0 \pmod{p}$. Pak $a^{p-1} \equiv 1 \pmod{p}$.

Důkaz.

Zapišme všechny navzájem různé nenulové zbytky mod p: $1, 2, \ldots, p-1$. Dále vše přenásobme a, dostaneme $a, 2a, \ldots, (p-1)a$. Opět navzájem různé zbytky: kdyby $ia \equiv ja \pmod{p}$, můžeme zkrátit a, což je nesoudělné s p, takže $i \equiv j$.

$(p-1)$-tice zbytků $(1, 2, \ldots, p-1)$, $(a, 2a, \ldots, (p-1)a)$ jsou stejné až na pořadí, takže

$$(p-1)! \equiv a \cdot 2a \cdots (p-1)a \equiv a^{p-1} \cdot (p-1)!,$$
$$1 \equiv a^{p-1} \pmod{p}.$$

□

Úloha 9

Jsou dána různá prvočísla p, q. Dokažte $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Označme $A = p^{q-1} + q^{p-1} - 1$, pak chceme $pq \mid A$. Platí

$$A = p^{q-1} + q^{p-1} - 1 \equiv 0^{q-1} + q^{p-1} - 1 \equiv 1 - 1 \equiv 0 \pmod{p},$$

tedy $p \mid A$. Obdobně $q \mid A$. Nesoudělností p, q pak $pq \mid A$.

Úloha 10

Modulo prvočíslo $p = 4k + 3$ je -1 kvadratický nezbytek.

Pro spor nechť $x^2 \equiv -1 \pmod{p}$. Potom určitě $x \neq 0 \pmod{p}$.

Umocněním obou stran na liché číslo $2k + 1$ tedy

$$-1 \equiv (-1)^{2k+1} \equiv \left(x^2\right)^{2k+1} \equiv x^{4k+2} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

To je spor, jelikož $p \nmid 2 = 1 - (-1)$.

Úloha 11

Je dáno prvočíslo p. Dokažte, že existuje nekonečně mnoho přirozených čísel n takových, že $p \mid 2^n - n$.

Pokud $p = 2$, vyhovuje každé sudé n. Nadále nechť je p liché.

Idea: odečítané n se chová modulo p, zatímco n v exponentu se chová modulo $p-1$. Přičtení $p-1$ k n pak výraz posune o 1:

$$2^{n+p-1} - (n+p-1) \equiv 2^n \cdot 2^{p-1} - n + 1 - p \equiv (2^n - n) + 1 \pmod{p}.$$

Pro $n = a(p-1)$ se zjednoduší $2^n - n \equiv 1 - a(p-1) \equiv 1 + a \pmod{p}$. Stačí tedy volit a o 1 menší než násobky p.

Zdroje:

1. Karolína Kuchyňová: *Kongruence*, `https://prase.cz/library/KongruenceKK/KongruenceKK.pdf`
2. Radovan Švarc: *Úvod do diofantických rovnic*, `https://prase.cz/library/DiofantickeRovniceRS/DiofantickeRovniceRS.pdf`
3. Filip Čermák: *Zbytky a mocnění*, `https://prase.cz/library/ZbytkyFC/ZbytkyFC.pdf`