Malá Fermatova veta

Ján Mazák, verzia 1.87

Vezmime si postupnosť čísel $2, 2^2, 2^3, 2^4, \dots, 2^k, \dots$ a všímajme si jej zvyšky po delení 7. Vieme objaviť nejakú pravidelnosť či zákonitosť? Postupnosť týchto zvyškov je $2, 4, 1, 2, 4, 1, 2, 4, 1, \dots$ a vyzerá to tak, že je periodická s periódou 3. Je ľahké to dokázať: po zvyšku 1 nasleduje zvyšok 2, po zvyšku 2 zvyšok 4 a po zvyšku 4 zvyšok 1 (rozpíšte si to, po čísle tvaru $7k + 4$ nasleduje $2 \cdot (7k + 4) = 14k + 8 = 7(2k + 1) + 1$).

Podobný záver vieme sformulovať pre všetky prvočísla p a ani na tej dvojke nie je nič špeciálne. Majme prirodzené číslo a nesúdeliteľné s p, potom postupnosť zvyškov čísel $a, a^2, a^3, \dots, a^k, \dots$ po delení p je periodická. Zrejme možných zvyškov v tejto postupnosti je $p - 1$ (zvyšok 0 sa tam nevyskytuje), preto keď vezmeme p za sebou idúcich členov, nejaký sa tam zopakuje dvakrát. Jeho dva najbližšie výskyty určujú periódu postupnosti.

Ďalšie zaujímavé výsledky sú sformulované v nasledujúcich vetách a úlohách. Ešte predtým si však zavedieme užitočné označenie: budeme písať $a \equiv b \pmod n$ (a hovoriť a je kongruentné s b modulo n), ak $n \mid a - b$. Inak povedané, čísla a a b dávajú rovnaký zvyšok po delení n, čiže sú v istom zmysle rovnaké. Môžeme si to predstaviť trebárs ako hodiny s n číslami od 0 do $n - 1$, ktoré reprezentujú zvyšky; $(n + 1)$-vá hodina je vlastne totožná s prvou atď.

Veta (malá Fermatova). *Nech p je prvočíslo a nech a je prirodzené číslo nesúdeliteľné s číslom p. Potom číslo $a^{p-1} - 1$ je deliteľné číslom p.*

Dôkaz. (Euler) Vezmime si čísla $a, 2a, \dots, (p - 1)a$. Ani jedno z týchto čísel nie je deliteľné číslom p. Tieto čísla dávajú navzájom rôzne zvyšky po delení číslom p, toto dokážeme sporom. Ak by čísla ia a ja dávali rovnaké zvyšky, tak ich rozdiel $(i - j)a$ je deliteľný číslom p. Ale p je prvočíslo, preto $p \mid a$ alebo $p \mid (i - j)$. Ani jedna z týchto možností nemôže nastať, pretože čísla a a p sú nesúdeliteľné a $1 \le i - j \le p - 2$). Preto spomínané čísla dávajú (v nejakom poradí) zvyšky $1, 2, \dots, p - 1$ a platí

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p \qquad \text{a}$$
$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod p\,.$$

Keďže čísla p a $(p - 1)!$ sú nesúdeliteľné, dostávame

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

Iný dôkaz. Pointou tohto dôkazu je, že nakoľko nevieme zatiaľ pracovať s premennou v exponente, tak ju binomickou vetou prehodíme do nejakého súčtu, kde už v exponente vystupovať nebude. Dobre to vidno pre $a = 2$, to je najmenšie a, pre ktoré tvrdenie neplatí triviálne. Zrejme $2^p = (1 + 1)^p$ a rozvinutím tohto dostaneme súčet, s ktorým si už vieme poradiť.

Matematickou indukciou podľa čísla a dokážeme, že $a^p \equiv a \pmod p$. Pre $a = 1$ tvrdenie zrejme platí. Nech tvrdenie platí pre nejaké a, ukážeme, že platí aj pre $a + 1$. Umocnime použitím binomickej vety číslo $a + 1$:

$$(a+1)^p = a^p + pa^{p-1} + \binom{p}{2}a^{p-2} + \dots + pa + 1 \equiv a^p + 1 \equiv a + 1 \pmod p\,.$$

Najprv sme využili, že $p \mid \binom{p}{k}$ pre prvočíslo p a všetky celé čísla k spĺňajúce $1 \le k \le p - 1$ a potom indukčný predpoklad. Z práve dokázaného tvrdenia a nesúdeliteľnosti a a p vyplýva tvrdenie vety.

Iný dôkaz. Majme a farieb a z každej farby p guľôčok. Koľko existuje náhrdelníkov zložených z p guľôčok aspoň dvoch rôznych farieb, ak dva náhrdelníky sú rovnaké, ak vieme jeden dostať pootočním druhého? Rozviňme si náhrdelník do radu. Počet radov, ktoré obsahujú guľôčky aspoň dvoch farieb, je $a^p - a$. Pre každý náhrdelník spĺňajúci požadované podmienky máme p

možností, ako ho rozvinúť do radu. Tieto rozvinutia sú navzájom rôzne. (Ak by nejaké dve boli rovnaké, tak pre nejaké r dostaneme pootočením náhrdelníka o $1 \leq r < p$ guľôčok rovnaký náhrdelník. Keďže p a r sú nesúdeliteľné, zvyšky čísel $r, 2r, \ldots, pr$ po delení číslom p sú rôzne a preto pootočenia o tieto čísla sú vždy rôzne. Všímajme si konkrétnu pozíciu. Na tejto pozícii sa pri týchto pootočeniach vystriedajú všetky guľôčky a preto sú všetky rovnaké, čo je spor.) Preto hľadaný počet náhrdelníkov (to je celé číslo) je $(a^p - a)/p$. Platí $p \mid a(a^{p-1} - 1)$ a keďže čísla a a p sú nesúdeliteľné, platí $p \mid (a^{p-1} - 1)$.

Nasledujúca veta je zovšeobecnením malej Fermatovej vety. Skôr, ako si ju uvedieme, potrebujeme istú funkciu, pomerne dôležitú pri práci v oblasti teórie čísel. Volá sa Eulerova funkcia a zvyčajne sa označuje φ. Jej hodnotou v prirodzenom čísle n je počet čísel z množiny $\{1, 2, \ldots, n\}$, ktoré sú nesúdeliteľné s n. V prípade, že poznáme prvočíselný rozklad čísla $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, môžeme vypočítať hodnotu $\varphi(n)$ podľa vzorca

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} \cdot (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

Vzorec si môžete dokázať napr. použitím princípu zapojenia a vypojenia.

Veta (Eulerova). Nech a je prirodzené číslo nesúdeliteľné s n. Potom $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dôkaz tejto vety ponechávame na čitateľa, skúste upraviť niektorý z uvedených dôkazov malej Fermatovej vety. V nasledujúcej vete sformulujeme vlastnosť prvočísel tvaru $4k + 3$, ktorá je občas užitočná pri riešení úloh.

Veta (bez mena). Nech p je prvočíslo tvaru $4k+3$ a nech a, b sú ľubovoľné celé čísla. Potom ak $p \mid a^2 + b^2$, tak $p \mid a$ a súčasne $p \mid b$.

Dôkaz. Ak p delí a, tak potom p delí b^2 a teda aj b. Zostáva nám prípad, keď a je nesúdeliteľné s p. Zrejme v tomto prípade aj p a b sú nesúdeliteľné. Vynásobme kongruenciu $a^2 \equiv -b^2 \pmod{p}$ číslom b^{p-3}. Podľa malej Fermatovej vety potom platí

$$a^2 b^{p-3} \equiv -b^2 \cdot b^{p-3} = -b^{p-1} \equiv -1 \pmod{p}.$$

Číslo $p-3$ je párne, preto číslo $c = a \cdot b^{\frac{p-3}{2}}$ je celé a nesúdeliteľné s p. Preto $c^2 = a^2 b^{p-3} \equiv -1 \pmod{p}$. Ak túto kongruenciu umocníme na nepárne číslo $(p-1)/2$, dostaneme

$$c^{p-1} \equiv (-1)^{p-1} \equiv -1 \pmod{p}.$$

Ale podľa malej Fermatovej vety je $c^{p-1} \equiv 1 \pmod{p}$, takže $-1 \equiv 1 \pmod{p}$ a dostávame spor.

Úlohy

V úlohách sa vám môžu hodiť doteraz uvedené vety, metódy ich dôkazov alebo tvrdenia či metódy z predchádzajúcich úloh. Keď niektorú úlohu neviete vyriešiť, vráťte sa k nej neskôr, prípadne mi napíšte (`mazo@kms.sk`).

1. Zistite zvyšky čísel $2^{10}, 2^{100}, 2^{1000}$ po delení siedmimi a čísel 2^{1000}, $2^{2^{1000}}$ po delení 41.

2. Nech k je prirodzené číslo. Aký zvyšok môže dávať číslo 2^{10^k} po delení číslami 7, 8, 9?

3. Dokážte, že pre ľubovoľné dve rôzne prvočísla p, q platí $pq \mid p^{q-1} + q^{p-1} - 1$.

4. Ak p a q sú dve navzájom rôzne prvočísla, tak $p^q + q^p \equiv p + q \pmod{pq}$. Dokážte.

5. Dokážte, že $2730 \mid a^{13} - a$. Dokážte, že $341 \mid 2^{341} - 2$. Zistite, či platí aj $341 \mid 3^{341} - 3$.

6. Aké zvyšky môžu dávať sté mocniny prirodzených čísel po delení 125?

7. Dokážte, že pre ľubovoľné prvočíslo p, prirodzené číslo n a celé číslo a platí $p \mid a^{n(p-1)+1} - a$.

8. Dokážte, že pre ľubovoľné celé čísla a, b také, že $(a, 65) = (b, 65)$ [1], je číslo $a^{12} - b^{12}$ násobkom 65.

9. Nech p je prvočíslo a a prirodzené číslo. Pre ktoré prirodzené čísla n platí $a^{p^n} \equiv a \pmod{p}$?

10. Nájdite všetky prvočísla p, pre ktoré $p \mid 5^{p^2} + 1$.

11. Nájdite všetky riešenia rovnice $2^m - 3^n = 1$ v obore prirodzených čísel.

12. Nech p je prvočíslo a a prirodzené číslo nesúdeliteľné s p. Nech k je najmenšie prirodzené číslo také, že $p \mid a^k - 1$. Dokážte, že potom $k \mid p - 1$.

13. Nech p je prvočíslo a n kladné celé číslo. Ak $n \equiv 1 \pmod{p^\alpha}$, tak $n^p \equiv 1 \pmod{p^{\alpha+1}}$. Dokážte.

14. Rozhodnite, či $7^3 \mid 2^{147} - 1$.

15. Nájdite najväčší spoločný deliteľ čísel z množiny $\{n^{13} - n \mid n \in \mathbb{Z}\}$.

16. Nájdite nekonečne veľa prirodzených čísel n takých, že $2^{2^n} + 3$ je zložené číslo.

17. Dokážte, že pre ľubovoľné prvočíslo p existuje nekonečne veľa násobkov p tvaru $2^n - n$ $(n \in \mathbb{N})$.

18. Nájdite všetky dvojice celých čísel x, y, pre ktoré platí $x^2 + y^2 = 2001(x - y)$.

19. Nájdite všetky trojice prvočísel p, q, r, pre ktoré platí $p^2 + q^2 + r^2 = 4422$.

20. a) Aký zvyšok môže dávať desiata mocnina prirodzeného čísla po delení 11?
b) Vyriešte rovnicu $x_1^{10} + x_2^{10} + \cdots + x_7^{10} = 2009^{2009}$.
c) Vyriešte rovnicu $x_1^{12} + x_2^{12} + \cdots + x_7^{12} = 2009^{2009}$.
d) Vyriešte rovnicu $x_1^4 + x_2^4 + \cdots + x_7^4 = 2009^{2009}$.

21. Dokážte, že ak n je nesúdeliteľné s 10, tak existuje násobok n, ktorého zápis v desiatkovej sústave pozostáva zo samých deviatok.

22. Dôkaz „vety bez mena“ je dosť umelý. Prirodzenejší dôkaz sa dá spraviť tak, že si uvedomíme, že ak prvočíslo p nedelí b, musí existovať číslo d také, že $bd \equiv 1 \pmod{p}$ (dokážte). V kongruencii $a^2 \equiv -b^2$ potom vieme dostať iba jedno písmenko miesto dvoch, stačí ju prenásobiť číslom d^2 a spraviť vhodnú substitúciu. Skúste dokončiť dôkaz.

23. Dokážte, že čísla $2^{2^{4n+1}} + 7$, $2^{2^{6n+2}} + 13$, $2^{2^{10n+1}} + 19$, $(2^{2 \cdot 3^{6n+3}+4} + 1)^2 + 2^2$ sú zložené pre všetky prirodzené čísla n.

24. Nech $P(n)$ je ľubovoľný polynóm s celočíselnými koeficientmi. Dokážte, že postupnosť čísel

$$P(1)^1, P(2)^2, \ldots, P(n)^n, \ldots$$

je periodická.

25. Dokážte, že medzi číslami tvaru $10^n + 3$ $(n \in \mathbb{N})$ je nekonečne mnoho zložených.

---

[1] (x, y) je najväčší spoločný deliteľ čísel x, y

26. Nájdite všetky prirodzené čísla n, pre ktoré číslo $n^{n^3} - n^n$ nie je násobkom piatich.

27. Nech a je prirodzené číslo. Ak číslo n spĺňa vzťah $a^n \equiv a \pmod{n}$, nazývame ho *pseudoprvočíslom pri báze a*. Dokážte, že ak n je nepárne pseudoprvočíslo pri báze 2, tak aj číslo $2^n - 1$ je pseudoprvočíslo pri báze 2. Overte, že číslo 561 je pseudoprvočíslo pri ľubovoľnej báze.

28. Nájdite všetky kladné celé čísla nesúdeliteľné s každým členom postupnosti $(a_n)_{n=1}^{\infty}$,

$$a_n = 2^n + 3^n + 6^n - 1.$$

29. a) Ukážte, že pre nesúdeliteľné prirodzené čísla a a b platí $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.
(Funkciám s touto vlastnosťou sa hovorí *multiplikatívne*.)
b) Dokážte, že pre každé prirodzené číslo n platí $\sum_{d|n} \varphi(d) = n$.