Řády a mocniny

David Hruška

Abstrakt. Olympiádní teorie čísel se často zabývá úlohami o zbytcích a mocninách. K této oblasti existuje poměrně bohatá teorie, která nám jednak dává dobrou představu, jak zbytky fungují, a jednak se hodí v matematických soutěžích. Příspěvek obsahuje shrnutí jejích přístupnějších partií a přes dvacet různě obtížných úloh k procvičení.

V rámci úloh z teorie čísel můžeme často místo s danými čísly pracovat jen s jejich zbytky po dělení vhodným n (říká se také „modulo n“). Podíváme se podrobně na to, co se děje se zbytky modulo pevné n, když je násobíme a mocníme.

Zbytky, zejména ty nesoudělné s n

Definice. *Úplnou sadou zbytků* myslíme množinu $\{0, 1, 2, \ldots, n-1\}$ zbytků modulo n. Značíme ji $\mathbb{Z}_n$. Když v ní sčítáme nebo násobíme, tak myslíme automaticky sčítání a násobení modulo n. *Redukovaná sada zbytků* je podmnožina $\mathbb{Z}_n$ obsahující všechna čísla nesoudělná s n. Značíme ji $\mathbb{Z}_n^*$ a má $\phi(n)$ prvků, kde ϕ nazýváme *Eulerova funkce*.

Věta. *Pokud $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, kde p_i jsou po dvou různá prvočísla, pak platí*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Kvadratické zbytky

Definice. Číslo $a \in \mathbb{Z}_n^*$ je *kvadratický zbytek*, pokud $x^2 \equiv a \pmod{n}$ pro nějaké $x \in \mathbb{Z}_n$. Pokud takové x neexistuje, říkáme, že a je *kvadratický nezbytek*.

Tvrzení. *Pro liché prvočíslo p je kvadratických zbytků $\frac{p-1}{2}$.*

Definice. Nechť p je liché prvočíslo a $a \in \mathbb{Z}$, pak definujeme *Legendreův symbol* $\left(\frac{a}{p}\right)$ následovně:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{pro } p \mid a \\ 1 & \text{pokud } a \text{ je kvadratickým zbytkem a } p \nmid a \\ -1 & \text{pokud } a \text{ není kvadratickym zbytkem} \end{cases}$$

Úloha 1. Dokaž, že liché číslo, které se dá zapsat jako součet dvou čtverců, je nutně ve tvaru $4k+1$.

Úloha 2. Dokaž, že pokud $7 \mid a^2+b^2$, pak $7 \mid a$ a $7 \mid b$. Dokaž, že obdobné tvrzení pro pětku neplatí.

Úloha 3. Bětka si myslí třísetciferné číslo, které se skládá ze sta nul, sta jediček a sta dvojek, přičemž první cifra není nula. Může být Bětčino číslo čtverec?

(MKS 29–2–4)

Řády a mocnění

Definice. Pro každé číslo $a \in \mathbb{Z}_n^*$ existuje právě jedna *inverze* modulo n, tj. prvek $a' \in \mathbb{Z}_n^*$ takový, že $aa' \equiv 1 \pmod{n}$. Obvykle inverzi značíme a^{-1}.

Definice. Pro $a \in \mathbb{Z}_n^*$ nazveme *řád prvku a modulo n* nejmenší $k \in \mathbb{N}$ takové, že $a^k \equiv 1 \pmod{n}$. Značíme ho $\mathrm{ord}_n(a)$.

Tvrzení. *Pro $a \in \mathbb{Z}_n^*, x, y \in \mathbb{N}_0$ platí*

$$a^x \equiv a^y \pmod{n} \iff x \equiv y \pmod{ord_n(a)}.$$

Důsledek. *Nechť $a \in \mathbb{Z}_n^*, x \in \mathbb{N}_0$. Pak $a^x \equiv 1 \pmod{n}$ právě, když $ord_n(a) \mid x$.*

Důsledek. *Pokud $a^x \equiv 1 \pmod{p}$ a zároveň $a^y \equiv 1 \pmod{p}$, pak též $a^{(x,y)} \equiv 1 \pmod{p}$.*

Věta. (Wilsonova) *Platí, že p je prvočíslo právě tehdy, když $(p-1)! \equiv -1 \pmod{p}$.*

Věta. (Eulerova) *Pro $a \in \mathbb{Z}_n^*$ platí $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Speciálnímu případu této věty, kdy n je prvočíslo (a tedy $\phi(n) = n-1$), se říká *malá Fermatova věta.*

Tvrzení. (Eulerovo kritérium) *Nechť p je liché prvočíslo a a je číslo nesoudělné s p, potom* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Tvrzení. *Buď p liché prvočíslo a a, b celá čísla. Pak* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Úloha 4. Ukaž, že kdykoliv je p prvočíslo a a, b přirozená čísla, pak $p \mid ab^p - ba^p$.

Úloha 5. Ukaž, že pro různá prvočísla p, q platí

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Úloha 6. Nechť p je prvočíslo a b je celé číslo. Dokažte, že $b^{p^2-1} \equiv 1 \pmod{p^2}$, právě když $b^{p-1} \equiv 1 \pmod{p^2}$. (MKS 28–9–4)

Úloha 7. Ukaž, že -1 je kvadratický zbytek modulo p, právě když p je ve tvaru $4k+1$.

Úloha 8. Nechť p je prvočíslo a q je prvočíslo, které dělí $2^p - 1$. Dokaž, že pak $p \mid q - 1$.

Úloha 9. Pokud prvočíslo p dělí n-té Fermatovo číslo $2^{2^n} + 1$, pak $2^{n+1} \mid p - 1$.

Úloha 10. Najdi všechna kladná celá čísla nesoudělná se všemi členy nekonečné posloupnosti

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

(IMO 2005, 4)

Úloha 11. Buď p prvočíslo ve tvaru $3k + 2$. Platí, že $p \mid a^2 + ab + b^2$, kde $a, b \in \mathbb{N}$. Ukaž, že pak i $p \mid a$, $p \mid b$.

Úloha 12. Nechť $p \geq 5$ je prvočíslo a $n = \frac{2^{2p}-1}{3}$. Ukaž, že $n \mid 2^n - 2$.

(iKS 1, N4)

Úloha 13. Dokaž, že pro $n > 1$ nemůže nastat $n \mid 2^{n-1} + 1$. (Schinzel)

Úloha 14. Nalezni všechny trojice prvočísel p, q, r splňující soustavu dělitelností

$$p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q + 1.$$

(USA TST 2003)

Úloha 15. Najdi všechna $n > 1$, pro která existuje právě jedno $0 < a \leq n!$ takové, že $a^n + 1$ je dělitelné $n!$. (ISLS 2005, N4)

Úloha 16. Nechť $p \geq 5$ je prvočíslo. Dokaž, že existuje $1 \leq a \leq p - 2$ takové, že ani $a^{p-1} - 1$, ani $(a + 1)^{p-1} - 1$ není dělitelné p^2. (ISLS 2001, N4)

Úloha 17. Nechť p je prvočíslo. Dokaž, že existuje prvočíslo q takové, že pro žádné přirozené číslo n není $n^p - p$ dělitelné q. (IMO 2003, 6)

Primitivní prvek

Asi nejzajímavější tvrzení o zbytcích modulo p je existence primitivního prvku. Nebudeme ji dokazovat, ale krátce si ukážeme, jak funguje.

Definice. Číslo $a \in \mathbb{Z}_n^*$ nazveme *primitivní prvek*, pokud $\mathrm{ord}_n(a) = \phi(n)$.

Poznámka. Primitivní prvek g je tedy číslo, které „generuje“ celou $\mathbb{Z}_n^*$, neboli

$$\{g^0 \pmod n, g^1 \pmod n, g^2 \pmod n, \dots\} = \mathbb{Z}_n^*.$$

Věta. *Primitivní prvek existuje právě pro modula ve tvaru* $2, 4, p^k, 2p^k$, *kde* p *je liché prvočíslo a* $k \in \mathbb{N}$.

Úloha 18. Nechť p je liché prvočíslo. Najdi všechna taková k, že

$$p \mid 1^k + 2^k + \cdots + (p - 1)^k.$$

(Hungary-Israel Math Competition 2009)

Úloha 19. Pro prvočíslo p urči, jaký je součet všech kvadratických zbytků modulo p. Jak je to s kvadratickými nezbytky?

Úloha 20. Dokaž, že součin všech primitivních prvků modulo p je kongruentní 1 mod p.

Úloha 21. Ukaž, že 2 je primitivní prvek mod 3^n.

Úloha 22. Dokaž, že pokud je p Fermatovo prvočíslo (tedy je ve tvaru $2^{2^k}+1$ pro nějaké $k \in \mathbb{N}$), pak je každý kvadratický nezbytek modulo p současně primitivním prvkem.

Návody

1. Modulo 4.

2. Rozeberte možnosti na zbytky modulo 7.

3. Modulo 9.

4. Rozeber zvlášť případ, kdy je jedno z čísel dělitelné p, pak využij malou Fermatovu větu.

5. Podívej se na kongruenci zvlášť modulo p a q, použij malou Fermatovu větu.

6. Využij Eulerovu větu.

7. První implikaci sporem s malou Fermatovou větou. Druhou implikaci Eulerovým kritériem.

8. $\mathrm{ord}_q(2) = p$.

9. Umocni kongruenci na druhou, abys dostal řád prvku 2 modulo p.

10. Pro prvočísla $p > 3$ uvaž člen a_{p-2} a využij malou Fermatovu větu.

11. Platí také $a^3 \equiv b^3 \pmod p$. Umocni na vhodnou mocninu, aby šla využít malá Fermatova věta.

12. Dokaž $2p \mid n-1$.

13. Vyluč sudá čísla, rozlož na součin a uvaž takové prvočíslo p v rozkladu, že $p-1$ je dělitelné nejmenší mocninou r čísla 2. Dokaž $n \equiv 1 \pmod{2^r}$.

14. BÚNO p je nejmenší. Pokud je p liché, dokaž $p \mid q-1$ nebo $p \mid q+1$ a vyluč první možnost a následně dokaž $q \mid r+1$ a $r \mid p+1$.

15. Platí pro prvočísla. Pro lichá složená uvaž $a = \frac{n!}{d} - 1$, kde $d \mid n$. Pro lichá prvočísla dokaž, že $\frac{a^n+1}{a+1}$ je nesoudělné s $(n-1)!$.

16. Označ C množinu těch a, pro které $a^{p-1} \equiv 1 \pmod{p^2}$. Dokaž $|C| \leq \frac{p-1}{2}$. Dále sporem dostaň $1, 3, \ldots, p-2 \in C$ a spor vyvoď z $p-4, p-2 \in C$.

17. Vezmi libovolné prvočíslo $q \mid \frac{p^p-1}{p-1}$. Dokaž $q \equiv 1 \pmod p$ a $q \mid p^k - 1$, kde $q = kp + 1$. Potom dokaž $p \mid k$ a $q \equiv 1 \pmod{p^2}$. To nemůže nastat pro všechny prvočíselné dělitele $\frac{p^p-1}{p-1}$.

18. Zapiš čísla $1, \ldots, p-1$ pomocí jednoho primitivního prvku a využij vzoreček pro součet geometrické řady.

19. Kvadratické zbytky jsou přesně ty prvky $\mathbb{Z}_p^*$, u kterých má primitivní prvek sudý exponent.

20. Inverzní prvek k primitivnímu prvku je opět primitivní.

21. Indukcí podle n. Musí platit $\phi(3^n) = \mathrm{ord}_{3^n}(2) \mid \mathrm{ord}_{3^{n+1}}(2) \mid \phi(3^{n+1})$. Další indukcí vyluč případ $\mathrm{ord}_{3^{n+1}} = 2 \cdot 3^{n-1}$.

22. Kvadratické zbytky nemohou být primitivními prvky. Kolik má p primitivních prvků?

Literatura a zdroje

Tento příspěvek je téměř podmnožinou příspěvku *Štěpána Šimsy* z pátého soustředění *i*KS s názvem *Řády a primitivní prvek*, kterému tímto děkuji.