Seriál – Teorie čísel II

Po krátké přestávce se k Tobě dostává další díl seriálu! Jak sis možná všiml, první část seriálu byla poměrně hutná. Proto jsme se rozhodli udělat tento díl kratší, aby sis mohl dočíst z prvního dílu kapitoly, které jsi třeba předtím nestihl. Tak se do toho opři, bude to stát za to! Navíc jsme v textu odlišili náročnější pasáže, které nejsou potřeba k vyřešení seriálových úloh a k pochopení ostatní látky.

Tentokrát v seriálu najdeš návod, jak nakládat s umocňováním čísel. Nejdříve si zavedeme p-valuace, které jsou praktickým nástrojem při práci s dělitelností. Poté se seznámíme s primitivním prvkem, ukážeme si zajímavé vlastnosti kvadratických zbytků a probranou teorii využijeme v rozmanitých úlohách z olympiád.

Rozklady a p-valuace

Když pracujeme s dělitelností, vyplatí se rozkládat čísla na prvočísla. Pokud chceme například dokázat $60^{30} \mid 30^{60}$, tak stačí najít prvočíselný rozklad obou čísel. Vidíme $60^{30} = 2^{60} \cdot 3^{30} \cdot 5^{30}$ a $30^{60} = 2^{60} \cdot 3^{60} \cdot 5^{60}$. Jelikož exponenty u každého prvočísla jsou v prvním čísle menší než v tom druhém, tak dokazovaná dělitelnost skutečně platí. Když nepracujeme s konkrétními čísly, často se vyplatí podívat se pouze na nějaké obecné prvočíslo a na mocniny, v jakých dělí zadaná čísla. A k tomu si zavedeme pojem *p-valuace*.

Definice. Nechť n je přirozené číslo a p prvočíslo. Poté *p-valuací* čísla n myslíme největší číslo k takové, že $p^k \mid n$.[12] Značíme ji $v_p(n)$.

Jinými slovy, p-valuace jsou vlastně exponenty v prvočíselném rozkladu čísla n. Například pro $24 = 2^3 \cdot 3$ máme $v_2(24) = 3$, $v_3(24) = 1$ a $v_7(24) = 0$.

Cvičení. Uvědom si následující jednoduché vlastnosti p-valuací.

(i) $v_p(mn) = v_p(m) + v_p(n)$,
(ii) $v_p(m+n) \geq \min(v_p(m), v_p(n))$,
(iii) Pokud $v_p(m) \neq v_p(n)$, pak dokonce $v_p(m+n) = \min(v_p(m), v_p(n))$.

Tyto vlastnosti vyplývají z toho, že se jedná jen o exponenty jednotlivých prvočísel v rozkladu. A exponenty se při násobení přece sčítají. Povšimni si, že jako důsledek prvního cvičení platí například i $v_p(a^n) = n \cdot v_p(a)$.

Na následujících cvičeních si p-valuace trochu zažijeme.

Cvičení. Urči tyto hodnoty:

(i) $v_2(2^n + 4)$ (v závislosti na n).
(ii) $v_3(v_3(18^{18}))$.
(iii) $v_p((3p^3 + p^2)(p^3 + 2p^2 + 5p))$ (v závislosti na prvočíslu p).

[12] Tento fakt občas zapisujeme jako $p^k \parallel n$.

Cvičení. Máme tři čísla, z nichž žádné není dělitelné 8 ani 125. Kolika nejvíce nulami může končit jejich součin?

Základní použití p-valuací spočívá v této snadné úvaze. Představme si, že chceme dokázat $a \mid b$. Místo toho nám stačí ukázat, že když si vezmeme libovolné prvočíslo p, tak $v_p(a) \leq v_p(b)$. Ukažme si to na příkladu.

Příklad. Mějme čísla a, b, c, pro která platí $a \mid b^3$, $b \mid c^3$, $c \mid a^3$. Dokaž, že $abc \mid (a+b+c)^{13}$.

Řešení. Vezměme si libovolné prvočíslo p. Z toho, že platí $a \mid b^3$, můžeme odvodit $v_p(a) \leq v_p(b^3)$, takže $v_p(a) \leq 3v_p(b)$. Podobně víme $v_p(b) \leq 3v_p(c)$ a $v_p(c) \leq 3v_p(a)$. Nyní chceme dokazované tvrzení přeložit do řeči p-valuací. K tomu stačí využít výsledky (i) a (ii) z úvodního cvičení. BÚNO předpokládejme, že $v_p(a)$ je nejmenší z čísel $v_p(a)$, $v_p(b)$, $v_p(c)$. Pak

$$v_p\big((a+b+c)^{13}\big) \geq 13 \cdot \min(v_p(a), v_p(b), v_p(c)) = 13v_p(a),$$

ale

$$v_p(abc) = v_p(a) + v_p(b) + v_p(c) \leq v_p(a) + 4v_p(c) \leq 13v_p(a) \leq v_p\big((a+b+c)^{13}\big).$$

Jelikož tato nerovnost platí pro každé prvočíslo p, tak platí i pro všechna prvočísla v rozkladu abc, a tedy opravdu $abc \mid (a+b+c)^{13}$.

Podobné metody můžeme využít, když chceme dokázat, že se dvě čísla a, b rovnají (až na znaménko). Dokážeme jednoduše, že $v_p(a) = v_p(b)$ pro každé prvočíslo p. Než si tuto metodu předvedeme na příkladu, rozmyslíme si ještě, jaká je p-valuace NSD a nsn.[13]

Cvičení. Dokaž:

(i) $v_p((m,n)) = \min(v_p(m), v_p(n))$.
(ii) $v_p([m,n]) = \max(v_p(m), v_p(n))$.

Návod. Ukaž, že $p^{\min(v_p(m), v_p(n))}$ dělí m i n, zatímco větší mocnina p už jedno z nich nedělí.

Příklad. Nechť $a_1, a_2, \ldots, a_k$, $b_1, b_2, \ldots, b_k$ jsou přirozená čísla, která splňují $(a_i, b_i) = 1$ pro každé $i \in \{1, 2, \ldots, k\}$. Dále buď $m = [b_1, b_2, \ldots, b_k]$. Ukaž, že platí

$$\left(\frac{a_1 m}{b_1}, \frac{a_2 m}{b_2}, \ldots, \frac{a_k m}{b_k}\right) = (a_1, a_2, \ldots, a_k).$$

(IMO shortlist 1974)

Řešení. Vezměme si libovolné prvočíslo p. Stačí nám dokázat, že p-valuace levé (L) a pravé (P) strany je stejná. A to podle předchozího cvičení znamená, že

$$v_p(L) = \min\left(v_p\left(\frac{a_1 m}{b_1}\right), v_p\left(\frac{a_2 m}{b_2}\right), \ldots, v_p\left(\frac{a_k m}{b_k}\right)\right),$$
$$v_p(P) = \min(v_p(a_1), v_p(a_2), \ldots, v_p(a_k)).$$

Ale zároveň platí $v_p(a_i m/b_i) = v_p(a_i) + v_p(m) - v_p(b_i)$ a $v_p(m) = \max(v_p(b_1), \ldots, v_p(b_k))$. Nyní rozebereme dvě možnosti.

Pokud $v_p(b_i) = 0$ pro všechna i, tak i $v_p(m) = 0$. Poté zřejmě $v_p(a_i) + v_p(m) - v_p(b_i) = v_p(a_i)$ pro každé i. Pak je ale $v_p(a_i m/b_i) = v_p(a_i)$, a to znamená, že také $v_p(L) = v_p(P)$.

Nechť pro nějaké b_i platí $v_p(b_i) \neq 0$. Vezměme i takové, že $v_p(b_i)$ je největší, takže $v_p(m) = v_p(b_i)$. Pak $v_p(a_i) + v_p(m) - v_p(b_i) = v_p(a_i)$. Jelikož ale $p \mid b_i$ a protože $(a_i, b_i) = 1$, tak $p \nmid a_i$.

[13] Připomeneme, že NSD čísel a, b značíme (a,b), zatímco nsn značíme $[a,b]$. Totéž značení používáme i pro více jak dvě čísla.

To znamená, že $v_p(a_i) = 0$. Proto $v_p(a_i m/b_i) = 0$ a levá strana není dělitelná prvočíslem p, stejně jako pravá (protože $p \nmid a_i$).

Úloha. Přirozená čísla a, b, c, d splňují $ab = cd$. Ukaž, že platí

$$(a, c) \cdot (a, d) = a \cdot (a, b, c, d).$$

(Polská MO, Mecz 2009)

Návod. Označ si p-valuace čísel a, b, c, d, rozepiš obě rovnosti do řeči p-valuací a rozeber několik případů.

Úloha. Víme, že pro přirozená čísla m, n platí $m \mid n^2$, $n^3 \mid m^4$, $m^5 \mid n^6$, ... Dokaž $m = n$.

Návod. Kdyby pro nějaké prvočíslo neplatilo $v_p(m) = v_p(n)$, tak si zvol dostatečně velké k a dojdi ke sporu s tím, že $m^{4k+1} \mid n^{4k+2}$, nebo s tím, že $n^{4k+3} \mid m^{4k+4}$.

Díky p-valuacím získáváme ještě nový pohled[14] na to, co je to největší společný dělitel, případně nejmenší společný násobek. Napišme si prvočíselný rozklad čísel m, n.

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$
$$n = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

kde $p_1 < p_2 < \dots < p_k$ jsou prvočísla a α_i, β_i pro $i \in \{1, \dots, k\}$ jsou nezáporná čísla (do obvyklého prvočíselného rozkladu můžeme přidat jakékoli prvočíslo umocněné na nultou, což je jedna, a zajistit si tak v obou rozkladech stejná prvočísla). Už víme, že $v_{p_i}((m, n)) = \min(v_{p_i}(m), v_{p_i}(n))$ a $v_{p_i}([m, n]) = \max(v_{p_i}(m), v_{p_i}(n))$. Z toho pak můžeme vyvodit

$$(m, n) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)},$$
$$[m, n] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}.$$

S p-valuacemi je nyní snadné dokázat rovnosti, jako je tato:

Příklad. Dokaž, že

$$\frac{[a, b, c]^2}{[a, b] \cdot [b, c] \cdot [c, a]} = \frac{(a, b, c)^2}{(a, b) \cdot (b, c) \cdot (c, a)}.$$

(USAMO 1972)

Řešení. Abychom měli jistotu, že pracujeme s celými čísly, tak si nejdříve rovnost upravíme do tvaru

$$[a, b, c]^2 \cdot (a, b) \cdot (b, c) \cdot (c, a) = (a, b, c)^2 \cdot [a, b] \cdot [b, c] \cdot [c, a].$$

Vezměme si libovolné prvočíslo p a označme $x = v_p(a), y = v_p(b), z = v_p(c)$. Můžeme BÚNO předpokládat $x \geq y \geq z$. Označme L a P levou a pravou stranu rovnosti. Spočítáme jejich p-valuace

$$v_p(L) = 2 \cdot \max(x, y, z) + \min(x, y) + \min(y, z) + \min(z, x) = 2x + y + 2z,$$
$$v_p(P) = 2 \cdot \min(x, y, z) + \max(x, y) + \max(y, z) + \max(z, x) = 2x + y + 2z.$$

[14] Jde vlastně o obvyklý pohled, který se učí ve škole. Většinou je ale naprosto nevhodný pro výpočet NSD (zkus se například zeptat své učitelky, jak by počítala NSD čísel $2^{42} + 3^{42}$ a 2^{42}), na rozdíl od Euklidova algoritmu, který je rychlý i pro velká čísla. Velká čísla totiž neumíme rychle rozkládat na prvočísla.

Vidíme, že každým prvočíslem je levá i pravá strana dělitelná ve stejné mocnině, takže se obě strany rovnají.

Další využití p-valuací najdeme, pokud se v úloze na dělitelnost setkáme s faktoriály.[15] Uvedeme si základní tvrzení, které se v takových úlohách používá.

Tvrzení. (Legendreova formule)

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

Důkaz. Nejprve si uvědomme, že součet je vlastně jen konečný, protože od jistého členu bude $n < p^k$, a tak budou všechny následující členy už jen nulové. A proč vzoreček funguje? Vezmeme všechna čísla menší nebo rovná n. Nejprve započítáme jedničku za všechna čísla dělitelná p, kterých je $\lfloor n/p \rfloor$. Ale některá čísla jsou dělitelná dokonce p^2, za každé z nich tedy připočítáme další jedničku v dalším členu $\lfloor n/p^2 \rfloor$. Poté připočítáme další jedničku za čísla dělitelná p^3, atd.

Cvičení.

(i) Rozlož 15! na prvočísla.
(ii) Urči, kolika nulami končí 100!.
(iii) Dokaž, že číslo $N = 46! \cdot 47! \cdot 48! \cdot 49!$ není druhou mocninou celého čísla, a najdi jeho největší dělitel, který druhou mocninou celého čísla je.

Návod.

(i) Stačí spočítat p-valuace pro prvočísla menší než 15.
(ii) Stačí spočítat $v_5(100!)$.
(iii) Zde je výhodnější nepočítat p-valuace všech prvočísel v součinu, ale jen se zamyslet, jestli je p-valuace sudá.

Úloha. (těžká) Dokaž, že číslo $M_n = (2n)!/(n!)^2$ je celé a že pro každé prvočíslo p platí $p^{v_p(M_n)} \leq 2n$.

Návod. Spočti si p-valuaci čitatele a jmenovatele, odečti je od sebe a dokaž, že

$$0 \leq \left\lfloor \frac{2n}{x} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{x} \right\rfloor \leq 1.$$

Uvědom si, že $v_p(M_n)$ je maximálně takové k, že $p^k \leq 2n < p^{k+1}$.

Náročnější pasáž

Díky tomuto zdánlivě samoúčelnému cvičení dostaneme velmi dobrý odhad počtu prvočísel. Zatím víme jen to, že jich je nekonečně mnoho, ale nemáme žádnou představu o tom, jak „hustě“ se mezi přirozenými čísly vyskytují. Označme tedy $\pi(x)$ počet prvočísel menších než x a zkusme tuto funkci nějak odhadnout.

Dá se poměrně snadno indukcí dokázat, že pro M_n z předchozí úlohy platí $M_n \geq 2^n$. Spolu s tím, že každé prvočíslo splňuje $p^{v_p(M_n)} \leq 2n$, dostaneme, že pro počet prvočísel $\pi(2n)$, která jsou menší než $2n$ (žádné větší prvočíslo nedělí M_n), platí $(2n)^{\pi(2n)} \geq M_n \geq 2^n$. Pokud označíme $x = 2n$, můžeme předchozí vztah upravit do tvaru

$$\pi(x) \geq \frac{1}{2} \cdot \frac{x}{\log_2 x}.$$

[15] Připomeňme si, že číslo $n!$ je rovno $1 \cdot 2 \cdot \ldots \cdot n$ a čte se [n faktoriál].

To jsme tedy dokázali pro sudá x. Pro x lichá máme

$$\pi(x) \geq \pi(x-1) \geq \frac{1}{2} \cdot \frac{x-1}{\log_2(x-1)}.$$

Návrat do reality

Pokud nevíš, co je funkce $\log_2 x$ nebo jak přesně jsme k výše uvedenému výsledku dospěli, nezoufej. Nebudeš to dále v seriálu potřebovat a jen věz, že jsme si ukázali, že je prvočísel opravdu hodně.

Eulerova věta

Nejprve si zavedeme dva užitečné pojmy.

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 $\mathbb{Z}_n^*$.

Například pro $n = 10$ je redukovaná sada zbytků $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$. Pro prvočíslo p je $\mathbb{Z}_p^*$ množina $\{1, 2, \ldots, p-1\}$, tedy $\mathbb{Z}_p$ bez nuly.

Cvičení. Rozmysli si, že součin dvou prvků ze $\mathbb{Z}_n^*$ je opět v $\mathbb{Z}_n^*$. Jak je to s jejich součtem?

Cvičení. Uvědom si, jak se pojmy, které známe, dají převést do řeči sad zbytků. Například, že $a \equiv b \pmod{n}$ říká totéž, co $a = b$ v $\mathbb{Z}_n$, nebo že Eulerova funkce[16] není nic jiného než počet prvků $\mathbb{Z}_n^*$. Tvrzení z minulého dílu, že „zbytky lze dělit“ zase říká, že každý prvek ze $\mathbb{Z}_n^*$ má v $\mathbb{Z}_n^*$ inverzi.[17]

S těmito pojmy jsme již vlastně pracovali, jejich pořádné zavedení nám ale usnadní mnoho úvah.

V minulém díle jsme se seznámili s Malou Fermatovou větou. Nyní si ukážeme její zobecnění pro libovolné přirozené modulo m, které se připisuje Eulerovi.

Věta. (Eulerova) *Nechť* $(a, m) = 1$. *Pak* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Důkaz se dá provést stejně jako důkaz MFV v prvním díle, uvedeme si však ještě jiný (a překvapivě kratší) důkaz.

Důkaz. Vezměme redukovanou sadu zbytků $\mathbb{Z}_m^*$. Nechť a je pevně dané číslo nesoudělné s m. Pokud jím každý prvek ze $\mathbb{Z}_m^*$ vynásobíme, dostaneme opět celou $\mathbb{Z}_m^*$, jen v jiném pořadí. Kdyby se totiž nějaké dva prvky ak a al rovnaly ($k \neq l$), tedy

$$ak \equiv al \pmod{m},$$

tak díky tomu, že $(a, m) = 1$, to znamená i $k \equiv l \pmod{m}$, což je požadovaný spor.

Například pro $m = 10$ a $a = 3$ (víme, že 3 je v $\mathbb{Z}_{10}^*$) máme

$$\{3 \cdot 1, 3 \cdot 3, 3 \cdot 7, 3 \cdot 9\} = \{3, 9, 1, 7\} = \{1, 3, 7, 9\}.$$

[16] Připomeneme, že Eulerova funkce $\varphi(n)$ přiřazuje číslu n počet přirozených čísel menších nebo rovných n a nesoudělných s n.

[17] Inverzí čísla a ze $\mathbb{Z}_n^*$ myslíme takové číslo a^{-1}, že $a \cdot a^{-1} \equiv 1 \pmod{n}$.

Nyní udělejme součin všech prvků ze $\mathbb{Z}_m^*$, čímž dostaneme nějaké číslo K nesoudělné s m. To je však stejné číslo, jako když vynásobíme všechny zbytky v jiném pořadí, takže platí

$$a^{\varphi(m)} \cdot K \equiv K \pmod{m}.$$

Protože číslo K je nesoudělné s m, můžeme jím obě strany vydělit a dostáváme požadovanou kongruenci. Pro náš případ $n = 10$, $a = 3$ to znamená

$$3^4 \cdot 1 \cdot 3 \cdot 7 \cdot 9 = (3 \cdot 1) \cdot (3 \cdot 3) \cdot (3 \cdot 7) \cdot (3 \cdot 9) \equiv 3 \cdot 9 \cdot 1 \cdot 7 = 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10},$$

takže $3^{\varphi(10)} = 3^4 \equiv 1 \pmod{10}$.

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

Řešení. Jak jsme si ukázali v minulém díle,[18] $\varphi(p^k) = p^k - p^{k-1}$, tedy speciálně $\varphi(p^2) = p^2 - p$. Z Eulerovy věty tedy víme $b^{p^2-p} \equiv 1 \pmod{p^2}$. Proto

$$b^{p-1} \equiv 1 \pmod{p^2}, \quad \text{právě když} \quad b^{p^2-p} \cdot b^{p-1} \equiv 1 \pmod{p^2},$$

což je ale po úpravě přesně $b^{p^2-1} \equiv 1 \pmod{p^2}$.

Primitivní prvek

Připomeňme si, že řád $\mathrm{ord}_m(a)$ čísla a modulo m je nejmenší přirozené číslo r takové, že $a^r \equiv 1 \pmod{m}$. Budeme se nyní zabývat otázkou, pro která m existuje a, jehož řád je maximální možný, tj. $\mathrm{ord}_m(a) = \varphi(m)$. Z Eulerovy věty totiž víme, že řád libovolného prvku je maximálně $\varphi(m)$, neboť $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Definice. Pokud $\mathrm{ord}_m(a) = \varphi(m)$, nazveme *a primitivním prvkem* modulo m.

Cvičení. Primitivní prvek je tedy číslo, které „generuje“ celou $\mathbb{Z}_m^*$, neboli každé číslo ze $\mathbb{Z}_m^*$ se dá zapsat jako jeho mocnina.

Návod. Co by se stalo, kdyby se dvě mocniny primitivního prvku rovnaly? Kolik je tedy různých mocnin primitivního prvku?

Příklad. Najdi primitivní prvek modulo 5 a dokaž, že neexistuje primitivní prvek modulo 8.

Řešení. Modulo 5 je primitivní prvek například číslo 2, protože čísla 2^1, 2^2, 2^3, 2^4 dávají zbytky po dělení pěti postupně 2, 4, 3, 1, takže opravdu $\mathrm{ord}_5(2) = 4$ (resp. číslo 2 skutečně generuje celou $\mathbb{Z}_5^*$).

Primitivní prvek modulo 8 nemůže být sudý, protože pak bychom nemohli dostat jako jeho mocninu žádné liché číslo. Na druhou stranu $1^1 \equiv 1$, $3^2 \equiv 1$, $5^2 \equiv 1$, $7^2 \equiv 1 \pmod{8}$, takže řád žádného lichého čísla není roven $\varphi(8) = 4$.

Cvičení. Najdi primitivní prvek modulo 13.

Náročnější pasáž

K důkazu existence primitivního prvku modulo každé prvočíslo se ještě potřebujeme lehce seznámit s chováním polynomů[19] modulo p. Jak jsi asi slyšel, polynom stupně n s reálnými koeficienty

[18] Nebo jak si snadno rozmyslíš.

[19] Polynom s koeficienty ze $\mathbb{Z}_p$ je funkce $\mathbb{Z}_p \to \mathbb{Z}_p$ taková, že $P(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, kde $a_i \in \mathbb{Z}_p$ a $n \in \mathbb{N}$. Je-li $a_n \neq 0$, pak říkáme, že polynom má stupeň n. Polynom nazýváme nulový, pokud jsou všechny jeho koeficienty nulové.

má maximálně n kořenů v reálných číslech, a dokonce přesně n kořenů v oboru komplexních čísel. Pro sady zbytků máme tuto analogii:

Věta. (Lagrangeova[20]) *Nechť P je nenulový polynom stupně n s koeficienty ze $\mathbb{Z}_p$. Pak má rovnice $P(x) \equiv 0 \pmod p$ maximálně n kořenů modulo p.*

Důkaz. Postupujme indukcí podle n. Pro $n = 0$ to platí triviálně. Předpokládejme, že tvrzení platí pro nějaké n, a dokažme, že platí i pro $n+1$. Nechť je $P(x) = \sum_{i=0}^{n+1} a_i x^i$ polynom stupně $n+1$. Pokud má 0 kořenů, jsme hotovi, protože 0 je menší než $n+1$. Jinak má nějaký kořen r, a protože pro každé i platí $x - r \mid x^i - r^i$, tak můžeme upravit $P(x) = P(x) - P(r) = \sum_{i=0}^{n+1} a_i(x^i - r^i) = (x-r)Q(x)$, kde Q je nějaký polynom stupně n a má tedy z indukčního předpokladu maximálně n kořenů.

Dosud jsme nijak nevyužili, že pracujeme modulo prvočíslo. Víme, že když p je prvočíslo, pak z $ab \equiv 0 \pmod p$ plyne $a \equiv 0 \pmod p$ nebo $b \equiv 0 \pmod p$. To znamená, že pokud x je kořen polynomu $F(x)G(x)$ modulo p, pak musí být také kořenem jednoho z polynomů F nebo G. V našem případě víme, že $F(x) = x - r$ má jeden kořen a $G(x) = Q(x)$ má maximálně n kořenů, takže $P(x) = F(x)G(x)$ má maximálně $n+1$ kořenů. Tím je indukční krok hotov.

Uvědom si, že věta neplatí pro složená modula! Například polynom $x^2 - 1$ má 4 kořeny modulo 8, přestože je jeho stupeň jen 2.

Nyní jsme dostatečně vyzbrojeni pro důkaz existence primitivního prvku.

Věta. *Pro každé prvočíslo p existuje primitivní prvek modulo p.*

Důkaz. Využijeme Lagrangeovu větu a především poslední tvrzení z předchozího dílu, které říká, že

$$\sum_{d \mid n} \varphi(d) = n.$$

Označme $\psi(d)$ počet zbytků ze $\mathbb{Z}_p^*$, které mají řád d. Již víme, že pokud existuje prvek řádu d, tak $d \mid p-1$. Protože každý prvek má nějaký řád a žádný prvek nemá dva různé řády, dostáváme, že[21]

$$\sum_{d \mid p-1} \psi(d) = |\mathbb{Z}_p^*| = p - 1,$$

takže také

$$\sum_{d \mid p-1} \psi(d) = p - 1 = \sum_{d \mid p-1} \varphi(d). \qquad (\heartsuit)$$

Mějme nějaké $d \mid p-1$. Ukážeme, že $\psi(d) \le \varphi(d)$. Pokud neexistuje žádné a, které má řád d, tak je zřejmě $0 = \psi(d) \le \varphi(d)$. V opačném případě si takové a vezměme. Pak jsou všechna čísla $a^0, a^1, \ldots, a^{d-1}$ různá (rozmysli si). Ale přitom pro $i \in \{0, \ldots, d-1\}$ platí $(a^i)^d - 1 \equiv 0 \pmod p$. Navíc podle Lagrangeovy věty má polynom $x^d - 1$ maximálně d kořenů, takže už jsme našli všechny. Vezměme si $i \in \{0, 1, \ldots, d-1\}$, které je soudělné s d. Nechť $(i, d) = k$ a $i = mk$, $d = nk$. Potom

$$(a^i)^n \equiv (a^m)^d \equiv 1 \pmod p,$$

takže a^i nemá řád d, nýbrž n. To znamená, že čísla, která mají řád d, jsou ta čísla a^i, která mají i nesoudělné s d, a je jich tedy maximálně $\varphi(d)$. Tudíž $\psi(d) \le \varphi(d)$.

Kdyby nyní pro nějaké $d \mid p-1$ platilo $\psi(d) < \varphi(d)$, tak by neplatila rovnost ($\heartsuit$), protože levá strana by byla menší než pravá. Takže speciálně $\psi(p-1) = \varphi(p-1) > 0$. Mimo jiné jsme tedy zjistili, kolik má prvočíslo primitivních prvků.

[20] Joseph-Louis Lagrange byl významný italsko-francouzský matematik a astronom (1736–1813).

[21] Symbol $|\mathbb{Z}_p^*|$ značí počet prvků množiny $\mathbb{Z}_p^*$.

Návrat do reality

V předchozí části jsme si dokázali existenci primitivního prvku modulo každé prvočíslo. Přestože je důkaz poměrně náročný, k samotnému řešení úloh ho znát nepotřebuješ. Existenci primitivního prvku můžeš využívat bez důkazu.[22] Tento fakt nyní zkusíme zužitkovat v úlohách:

Příklad. Nechť p je liché prvočíslo. Najdi všechna taková k, že $1^k + 2^k + \cdots + (p-1)^k$ je dělitelné p. (Hungary-Israel Math Competition 2009)

Řešení. Každé číslo a z množiny $\mathbb{Z}_p^*$ se dá zapsat jako q^{i_a}, kde q je primitivní prvek. Čísla i_a jsou navzájem různá. Proto

$$\begin{aligned} 1^k + 2^k + \cdots + (p-1)^k &\equiv (q^{i_1})^k + (q^{i_2})^k + \cdots + (q^{i_{p-1}})^k \\ &\equiv (q^k)^{i_1} + (q^k)^{i_2} + \cdots + (q^k)^{i_{p-1}} \\ &= (q^k)^1 + (q^k)^2 + \cdots + (q^k)^{p-1} \pmod p, \end{aligned}$$

neboť čísla $i_1, i_2, \ldots, i_{p-1}$ jsou čísla $1, 2, \ldots, p-1$, jen v jiném pořadí.

Tímto jsme se zbavili nepříjemného součtu a nahradili ho známou geometrickou posloupností, kterou už není problém sečíst. Musíme ale ještě rozebrat dva případy.

(i) $q^k \equiv 1 \pmod p$, což je ekvivalentní s $(p-1) = \mathrm{ord}_p(q) \mid k$, protože q je primitivní prvek. Potom $(q^k)^1 + (q^k)^2 + \cdots + (q^k)^{p-1} \equiv 1 + 1 + \cdots + 1 = p - 1 \pmod p$, takže tato k nevyhovují.

(ii) $q^k \not\equiv 1 \pmod p$. Poté můžeme sečíst geometrickou posloupnost pomocí známého vzorečku[23] a dostaneme[24]

$$q^k \cdot \frac{(q^k)^{p-1} - 1}{q^k - 1} \equiv q^k \cdot \frac{1-1}{q^k - 1} = 0 \pmod p.$$

Vyhovují tedy všechna k, která nejsou dělitelná $p-1$.

Cvičení. (těžké) Ukaž, že 2 je primitivní prvek mod 3^n.

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

Primitivní prvek neexistuje jen pro prvočíselné moduly. Známý výsledek shrnuje následující věta, která popisuje všechna modula, pro která primitivní prvek existuje. Důkaz už není tak těžký jako pro případ, kdy n je prvočíslo, ale ani tolik zajímavý, takže ho zde neuvádíme.

Věta. *Primitivní prvek modulo n existuje právě tehdy, když $n = 1, 2, 4, p^k$ nebo $2p^k$, kde p je liché prvočíslo a k je přirozené číslo.*

Zmíníme ještě slavnou Dirichletovu[25] větu. Důkaz této věty je bohužel nad rámec našeho seriálu. Někdy se však hodí i v olympiádě (typicky ji vzorové řešení nevyužívá, ale Dirichletova věta je opravdu „silná“).

[22] Jak v PraSeti, tak v olympiádě.

[23] Pokud ses s geometrickou posloupností ještě nesetkal, tak věz, že to je posloupnost tvaru $a_n = k \cdot q^{n-1}$, kde $k \neq 0$ a $q \neq 1$ jsou kladná reálná čísla. Dá se snadno odvodit, že součet prvních n členů je $k \cdot \frac{q^n - 1}{q-1}$.

[24] To, že máme zlomek v kongruenci, je v pořádku. Zlomek $\frac{a}{b}$ se totiž v kongruenci dá chápat jako $a \cdot b^{-1}$, tedy a vynásobeno inverzním prvkem k b.

[25] (Johann Peter Gustav) Lejeune Dirichlet (1805–1859) byl německý matematik. Proslavil se hlavně výsledky v teorii čísel, matematické analýze a statistice. Vzal si nejmladší sestru slavného hudebního skladatele Mendelssohna-Bartholdyho, Rebeccu.

Věta. (Dirichletova) *Pro každá dvě nesoudělná přirozená čísla a, b existuje nekonečně mnoho prvočísel tvaru $ak + b$.*

V následující úloze ukážeme, jak se dá vhodně zkombinovat s úvahami o primitivním prvku.

Příklad. Ukaž, že existuje nekonečně mnoho přirozených n takových, že číslo $n^4 + 1$ má prvočíselného dělitele většího než $2n$. (MKS 30–2–8)

Řešení. Nechť p je prvočíslo tvaru $8k + 1$ a q primitivní prvek modulo p. Potom z MFV víme, že

$$1 \equiv q^{p-1} \equiv q^{8k} \equiv (q^{4k})^2 \pmod{p},$$

což se dá přepsat do tvaru

$$(q^{4k} + 1)(q^{4k} - 1) \equiv 0 \pmod{p}.$$

Protože p je prvočíslo, dělí alespoň jednu ze závorek. Ale q je primitivní prvek, takže $p \nmid q^{4k} - 1$. Proto kongruence $n^4 + 1 \equiv 0 \pmod{p}$ má vždy řešení pro prvočíslo tvaru $8k + 1$ (a to $n = q^k$). Můžeme si vzít takové n, že $1 \leq n \leq p - 1$ (protože $p \nmid n$ a $(n + kp)^4 + 1 \equiv n^4 + 1 \pmod{p}$). Ale zřejmě platí $n^4 + 1 \equiv (p - n)^4 + 1$, takže si můžeme vzít to z čísel n, $p - n$ které je menší. Tím dostaneme nové n, pro které platí $n < p/2$.

Zbývá dokázat, že takovýchto n existuje nekonečno. Budeme postupovat sporem. Nechť je takových n jen konečně a n_1 je největší z nich. Podle Dirichletovy věty existuje nekonečně mnoho prvočísel tvaru $8k + 1$, takže najdeme i takové, že $p > n_1^4 + 1$. Z předchozího odstavce plyne, že existuje n_2 takové, že $p \mid n_2^4 + 1$ a $p > 2n_2$. Navíc $n_2^4 + 1 \geq p > n_1^4 + 1$. Takže jsme našli vyhovující n větší než n_1, což je požadovaný spor.

Úloha. Urči počet všech posloupností reálných čísel $\{a_n\}_{n=1}^{\infty}$ takových, že pro všechna přirozená čísla m, n platí $a_m \cdot a_n = a_{m \cdot n}$ a zároveň $a_n = a_{n+2011}$. (MKS 30–6–8)

Řády

V této kapitole si důkladně procvičíme práci s řády. Opravdu se totiž hodí mít je v malíčku.

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

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

(IMO 2005)

Řešení. Číslo 1 to triviálně splňuje. Všechna další čísla tvaru $2^k \cdot 3^l$ pro $k, l \geq 0$ nevyhovují, protože jsou soudělná s $a_2 = 48 = 2 \cdot 3 \cdot 8$. Dokážeme, že ani žádné jiné přirozené číslo s výjimkou jedničky zadání nesplní. Vezmeme si prvočíslo $p > 3$ a najdeme v posloupnosti člen, který je tímto prvočíslem dělitelný. Vzpomeneme si na malou Fermatovu větu, která nám pomáhá zbavovat se mocnin v kongruencích. Po chvilce zkoušení zjistíme, že viník je člen a_{p-2}.

$$\begin{aligned} 6 \cdot a_{p-2} &= 6 \cdot (2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \\ &\equiv 3 + 2 + 1 - 6 = 0 \pmod{p}, \end{aligned}$$

a jelikož $p > 3$, tak nutně $p \mid a_{p-2}$.

Podívejme se, co nám řeknou řády o dělitelích Mersennových[26] čísel. Připomeňme, že Mersennovo číslo je číslo ve tvaru $2^n - 1$.

[26] Marin Mersenne (1588–1648) byl francouzský matematik, filozof, teolog a hudební teoretik.

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

Návod. Řád prvku 2 modulo q dělí všechna čísla k, pro která platí $2^k \equiv 1 \pmod{q}$. Díky MFV je mezi nimi i $q - 1$.

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

Návod. Úlohu zabijeme podobnou myšlenkou jako minule. Zde je však třeba ještě použít trik „umocnění kongruence na druhou“, abychom si vyrobili z -1 jedničku.

Příklad. Dokaž, že pro $n > 1$ nemůže nastat $n \mid 2^{n-1} + 1$.

Řešení. Řešení je velmi trikové, ale pěkné. Budeme postupovat sporem, tedy předpokládejme, že takové n existuje. Zřejmě n nemůže být sudé. Rozložme si n na prvočísla:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Vezměme si takové i, že $v_2(p_i - 1)$ je nejmenší. Napišme $p_i = 1 + m \cdot 2^r$, kde m je nějaké liché číslo. Z výběru i víme, že pro každé prvočíslo p_j z rozkladu čísla n platí $p_j^{\alpha_j} \equiv 1 \pmod{2^r}$. Když tyto kongruence vynásobíme pro $i = 1, \ldots, k$, tak dostaneme $n \equiv 1 \pmod{2^r}$, takže $n - 1 = t \cdot 2^r$. Z podmínky ze zadání víme $2^{t \cdot 2^r} \equiv -1 \pmod{p_i}$, takže po umocnění na liché číslo m dostáváme, že

$$-1 = (-1)^m \equiv \left(2^{t \cdot 2^r}\right)^m \equiv 2^{t \cdot m \cdot 2^r} \equiv 2^{(p_i - 1) \cdot t} \equiv 1^t = 1 \pmod{p_i}.$$

Přitom poslední kongruence plyne z MFV. Ale potom $p_i \mid 2$, což je spor.

Kvadratické zbytky a reciprocita

V minulém díle jsme se seznámili s kvadratickými zbytky. To jsou ta čísla k ze $\mathbb{Z}_p^*$, pro která existuje x takové, že platí $x^2 \equiv k \pmod{p}$. Ukážeme si další užitečná tvrzení o zbytcích. Představíme si také standardní metody, jak kvadratické zbytky využívat v úlohách. Připomeneme ještě, že Legendreovým symbolem $\left(\frac{a}{p}\right)$ myslíme

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{pokud } p \mid a, \\ 1, & \text{pokud } a \text{ je kvadratický zbytek modulo } p, \\ -1, & \text{pokud } a \text{ je kvadratický nezbytek modulo } p. \end{cases}$$

Zabývejme se tedy vlastnostmi Legendreova symbolu. Je dobré si uvědomit, že Legendreův symbol není jen hezké značení vlastnosti „být kvadratickým zbytkem“. Je to chytře zvolená funkce z množiny zbytků do množiny $\{-1, 0, 1\}$, která má mnoho pěkných vlastností. Díky nim se nám například značně zjednoduší rozhodování, zda je daný zbytek kvadratický.

Tvrzení. (Základní vlastnosti Legendreova symbolu) *Nechť p je liché prvočíslo, a, b, k jsou celá čísla, pak platí:*

(i) *Pokud* $a \equiv b \pmod{p}$, *pak* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, *neboli* $\left(\frac{a}{p}\right) = \left(\frac{a + kp}{p}\right)$,

(ii) (Eulerovo kritérium) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Návod.

(i) Pokud existuje číslo x takové, že $x^2 \equiv a \pmod p$, pak také platí $x^2 \equiv b \pmod p$. Pokud takové číslo neexistuje, nemůže existovat ani pro b.
(ii) Viz minulý díl.
(iii) Aplikuj Eulerovo kritérium.

Už pomocí těchto jednoduchých vlastností můžeme odvodit zajímavé výsledky. V následujícím tvrzení ještě o kvadratické zbytky nejde.

Tvrzení. *Mersennovo číslo $2^n - 1$ je složené, pokud je n složené.*

Důkaz. Pokud $n = ab$, můžeme $2^n - 1$ upravit pomocí známého vzorce[27]

$$2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)\big((2^a)^{b-1} + (2^a)^{b-2} + \cdots + (2^a)^1 + (2^a)^0\big),$$

přičemž oba členy v součinu napravo jsou větší než jedna. Číslo $2^{ab} - 1$ má tedy dva netriviální dělitele, takže je složené.

S pomocí kvadratických zbytků se dá sestrojit případ, kdy podmínka prvočíselnosti n nestačí k prvočíselnosti čísla $2^n - 1$.[28]

Úloha. Nechť čísla $4n + 3$ a $8n + 7$ jsou prvočísla. Pak číslo $M_{4n+3} = 2^{4n+3} - 1$ je složené.

Návod. Například $23 \mid M_{11}$, $47 \mid M_{23}$ nebo $503 \mid M_{251}$.

Dostáváme se k hlavnímu výsledku teorie kvadratických zbytků – kvadratické reciprocitě. Ta nám říká, že pokud víme, zda je prvočíslo p kvadratický zbytek modulo jiné prvočíslo q, můžeme kongruenci „obrátit“ a dozvíme se, zda je q kvadratický zbytek modulo p. Všechno, co jsme dosud dělali, se (s trochou nadsázky) dá považovat za intuitivní. To však není případ kvadratické reciprocity – důvody, proč tato věta platí, rozhodně elementární nejsou.

Věta. (Kvadratická reciprocita) *Nechť p, q jsou lichá prvočísla. Pak platí*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)\cdot(q-1)}{4}}.$$

Bohužel si neuvedeme důkaz této věty, protože je obtížný a v seriálu nám na něj nezbývá místo. Pokud Tě to zajímá, jistě najdeš rozmanité důkazy v pokročilejších učebnicích teorie čísel nebo na internetu (sám Gauss[29] byl prý kvadratickou reciprocitou natolik nadšen, že ji nazýval „zlatou větou“ a objevil několik různých důkazů).

Ještě si všimni, že kvadratická reciprocita nám říká, že existuje nějaké řešení x kongruencí typu $x^2 \equiv p \pmod q$, ale nedává nám žádný nástroj, jak toto řešení najít. Ještě než si ukážeme příklad na využití reciprocity, přidáme dodatek, kterým počítáme kvadratické zbytky v případech, které reciprocita nezahrnuje, tedy pro -1 a 2.

Tvrzení. (Dodatek ke kvadratické reciprocitě) *Pro liché prvočíslo p platí*

(i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

(ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

[27] Jak si poctivá čtenářka snadno roznásobí.

[28] Neboli neplatí Mersennova hypotéza, která tvrdí opak.

[29] Carl Friedrich Gauss (1777–1855) byl slavný německý matematik a fyzik, který ovlivnil mnoho matematických disciplín včetně teorie čísel. Jeho mozek prý vážil 1492 gramů.

První tvrzení plyne jednoduše z Eulerova kritéria. Druhé tvrzení je opět těžké, jeho důkaz si tedy dovolíme zamlčet. Spolu s dodatkem se kvadratická reciprocita stává ultimátní zbraní, jak rozhodnout, jestli je něco kvadratický zbytek.

Cvičení. (uvědomovací) Mějme lichá prvočísla p, q. Uvědom si, že $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)$ je -1, právě když jsou obě prvočísla tvaru $4k+3$.

Ukažme si tedy, jak se reciprocita používá.

Příklad. Zjisti, zda je 179 kvadratický zbytek modulo 463.

Řešení. Všimneme si, že příklad je zadán tak pěkně, že 179 a 463 jsou prvočísla. Počítejme tedy s využitím tvrzení (i) a (iii) z úvodu kapitoly a s pomocí kvadratické reciprocity:

$$\begin{aligned}\left(\frac{179}{463}\right) &= -\left(\frac{463}{179}\right) = -\left(\frac{105}{179}\right) = -\left(\frac{3\cdot 5\cdot 7}{179}\right) = -\left(\frac{3}{179}\right)\cdot\left(\frac{5}{179}\right)\cdot\left(\frac{7}{179}\right)\\ &= -\left(-\left(\frac{179}{3}\right)\right)\cdot\left(\frac{179}{5}\right)\cdot\left(-\left(\frac{179}{7}\right)\right) = -\left(\frac{2}{3}\right)\cdot\left(\frac{4}{5}\right)\cdot\left(\frac{4}{7}\right) = 1.\end{aligned}$$

Takto jsme dostali, že 179 je kvadratický zbytek modulo 463 (aniž bychom museli najít konkrétní řešení kongruence $x^2 \equiv 179 \pmod{463}$).

Cvičení. Je 365 kvadratický zbytek modulo 1847?

A co na to primitivní prvek?

Ukážeme si důležitou souvislost mezi kvadratickými zbytky a primitivním prvkem. Jak víme, primitivní prvek je takový, že jeho umocňováním dostaneme všechny různé zbytky. Které z nich jsou kvadratické? Odpověď je jednoduchá – jsou to ty, které vzniknou umocněním primitivního prvku q na sudou mocninu. Každá sudá mocnina q je totiž zřejmě kvadratický zbytek. Žádné další číslo už kvadratický zbytek nebude. Počet sudých mocnin mezi zbytky je totiž $(p-1)/2$, což je přesně počet kvadratických zbytků!

Cvičení. Dokaž, že kvadratický zbytek nemůže být (pro lichá prvočísla) primitivním prvkem.

Cvičení. Urči prvočísla p, pro která je q primitivní prvek, právě když je $-q$ primitivní prvek.

Úloha. Mějme prvočíslo p. Ukaž, že p je Fermatovo prvočíslo (tedy tvaru $2^{2^n}+1$) právě tehdy, když je každý kvadratický nezbytek zároveň primitivním prvkem modulo p.

Návod. Uvědom si, kolik je nezbytků a kolik je primitivních prvků modulo p. Tím dokážeš, že Fermatovo prvočíslo podmínku splňuje a že p je tvaru 2^m+1. Kdyby nějaké liché číslo dělilo m, využij vzorečku

$$a^{2k+1}+b^{2k+1} = (a+b)\big(a^{2k}-a^{2k-1}b+a^{2k-2}b^2-\cdots-ab^{2k-1}+b^{2k}\big)$$

a dostaneš spor s prvočíselností p. Proto je m tvaru 2^n.