Seriál – Teorie čísel I

Počínaje 17. ročníkem probíhá každý rok v PraSátku seriál na pokračování. Jde o výklad nějakého odvětví matematiky, se kterým se na střední škole s velkou pravděpodobností setkáš jen v omezené míře či vůbec ne, ale které je přesto možné vyložit tak, aby bylo středoškolákům přístupné. Cílem seriálu je tedy rozšířit Tvé matematické obzory o nějaký zajímavý kout matematiky. Letošní seriál na téma *Teorie čísel* pro Tebe píší Pepa Svoboda a Štěpán Šimsa. V prvních, druhých a třetích komentářích vyjde vždy jeden díl a k němu trojice úloh, k jejichž vyřešení by Ti měly stačit znalosti nabyté přečtením a plným pochopením doposud vydaných dílů. Na rozdíl od ostatních sérií se Ti z této do výsledného bodového hodnocení započítají všechny (tři) příklady.

Jak seriál číst?

Letošní téma je natolik zajímavé, obsáhlé a užitečné, že jsme se rozhodli udělat seriál vydatnější[1] než obvykle. Proto Tě v prvním díle seznámíme s důležitými základy, bez kterých bychom se v dalších dílech neobešli. Budeš-li mít pocit, že některou část seriálu máš v malíčku, můžeš ji s klidem přeskočit. Jestliže naopak nějakou část napoprvé nepochopíš, nezoufej a zkus to ještě jednou. Pokud to nepomůže, neboj se zeptat se na chatu nebo prostřednictvím e-mailu některého z autorů.[2]

Dohoda

Abychom se nezbláznili, budeme celá čísla (tj. -2, -1, 5, 0 apod.) označovat pouze jako „čísla“, protože s nimi budeme pracovat prakticky pořád. Pokud v seriálu použijeme neznámé a, b, c, d, myslíme tím vždy čísla (tedy celá!). Neznámé m, n máme vyhrazené pro čísla přirozená.

Úvod

Můžeš si blahopřát k výběru toho nejlepšího[3] tématu, kterým je Teorie čísel. Jde o obor zabývající se především vlastnostmi přirozených a celých čísel. Přestože mohou přirozená čísla působit jednoduše, opak je pravdou. Skrývají mnoho tajemství a nevyřešených problémů. Kde jinde se dají najít otevřené problémy s tak přístupným zadáním?

Příkladem mohou být takzvaná *dokonalá čísla*. Dokonalé je takové číslo, které je rovno součtu svých dělitelů s výjimkou sebe sama. Například číslo šest je dokonalé, protože $1 + 2 + 3 = 6$. Dalšími dokonalými čísly jsou 28, 496, 8 128, 33 660 336. Dohromady jich zatím známe jen 48, přičemž největší z nich má přes 17 miliónů cifer.

Cvičení. Dokaž, že součet převrácených hodnot dělitelů dokonalého čísla n je 2. (Například $\frac{1}{6} + \frac{1}{3} + \frac{1}{2} + 1 = 2$.)

Návod. Poděl definici číslem n.

[1] Občas se v poznámce pod čarou vyskytne vtip. Ten bude označen takto.[1]

[2] E-maily najdeš například na stránce *http://mks.mff.cuni.cz/organizatori.php*.

[3] My vlastně ani jiná témata ne(u)zná(vá)me.[1]

Velkou záhadou zůstává, jestli existuje i nějaké liché dokonalé číslo. Víme, že pokud by existovalo, tak by muselo splňovat mnoho podmínek. Například by bylo větší než 10^{300}, po dělení číslem 468 by dávalo zbytek 117, mělo by přes sto tisíc dělitelů a podobně.

Než si sami budeme moci dokázat něco pěkného o dokonalých číslech, musíme si vysvětlit základy, na kterých je celá teorie postavena. Ale neboj se, už v tomto díle se dozvíš spoustu zajímavých věcí, které Ti ve škole nejspíše neprozradí. Tak s chutí do toho!

Dělitelnost

Definice. Číslo b *je dělitelné* číslem $a \neq 0$, právě když existuje číslo c takové, že $ac = b$. Tento fakt zapisujeme $a \mid b$. Číslo a nazýváme *dělitelem* čísla b a b *násobkem* čísla a.[4]

Dělitelnost je základní pojem teorie čísel. Budeme se s ní setkávat na každém kroku, proto se s ní seznam v následujících cvičeních.

Cvičení. Dokaž si následující tvrzení.[5] Nechť platí $a, b \neq 0$.

(i) Platí $1 \mid a$ a $a \mid 0$.
(ii) Pokud $a \mid c$, tak i $a \mid cd$ a pokud $ab \mid c$, tak $a \mid c$.
(iii) Pokud $a \mid b$ a $b \mid c$, tak $a \mid c$. (Proto si můžeme dovolit zkrácený zápis $a \mid b \mid c$.)
(iv) Pokud $a \mid c$ a $b \mid d$, tak $ab \mid cd$.
(v) Pokud $a \mid c$, tak $c = 0$ nebo $|a| \leq |c|$.
(vi) Pokud $a \mid b$ a $b \mid a$, tak $|a| = |b|$.
(vii) Pokud $a \mid c$ a $a \mid d$, tak $a \mid c + d$.

Všimni si, že v posledním případě platí i $a \mid c - d$, ba dokonce $a \mid kc + ld$ pro libovolná čísla k, l.

Úloha. Urči všechna přirozená čísla m, n taková, že n dělí $2m - 1$ a m dělí $2n - 1$.
(MO 59–A–II–3)

Návod. Uvědom si, že pokud v části (v) je $c \neq 0$ a $|a| \neq |c|$, tak dokonce platí $2|a| \leq |c|$.

Cvičení. Rozmysli si, že obecně **neplatí**:

(i) Pokud $a \mid c$ a $b \mid d$, tak $a + b \mid c + d$.
(ii) Pokud $a \mid c$ a $b \mid c$, tak $ab \mid c$.
(iii) Pokud $a \mid cd$, tak $a \mid c$ nebo $a \mid d$.

Následuje jednoduché tvrzení, se kterým ses jistě již setkal a které často využíváme.

Tvrzení. (dělení se zbytkem) *Pro libovolná čísla a, b existuje jediná dvojice čísel q, r taková, že $a = bq + r$ a $0 \leq r < |b|$. Číslo q nazýváme* celočíselný podíl čísel a a b*; r nazýváme* zbytek po dělení čísla a číslem b.

NSD – největší společný dělitel

Nyní se seznámíme s největším společným dělitelem, vyzkoušíme si, jak se s ním pracuje, a ukážeme si snadný a rychlý způsob, jak jej vypočítat. Nejprve si ujasněme, co se pod tímto pojmem skrývá.

[4] Velmi často také říkáme, že a *dělí* b, ale pozor! To znamená, že a dělí b, a ne, že b dělí a.[1]

[5] $|x|$ je absolutní hodnota čísla x definovaná jako $|x| = x$ pro $x \geq 0$ a $|x| = -x$ pro $x < 0$.

Definice. *Největší společný dělitel* (NSD) čísel $a_1, a_2, \ldots, a_n$ (která nejsou všechna nulová) je největší přirozené číslo, které dělí všechna čísla $a_1, a_2, \ldots, a_n$. Budeme jej značit kulatými závorkami, tedy $(a_1, a_2, \ldots, a_n)$. Podobně *nejmenší společný násobek* (nsn)[6] je nejmenší přirozené číslo, které je násobkem všech čísel $a_1, a_2, \ldots, a_n$. Budeme jej značit hranatými závorkami $[a_1, a_2, \ldots, a_n]$.

Cvičení. Pro mírné seznámení si vypočítej hodnoty těchto NSD.

(i) $(-15, 24)$
(ii) $(n(n+1), 2)$

Řešení. Jediní dělitelé čísla -15 jsou čísla 1, 3, 5, 15 (a čísla jim opačná). Číslo 24 má kladné dělitele 1, 2, 3, 4, 6, 8, 12, 24. Společní dělitelé jsou jen -3, -1, 1, 3, z nichž největší je číslo 3. V části (ii) je určitě jedno z čísel n, $n+1$ sudé, tedy číslo $n(n+1)$ je dělitelné dvěma. To je ale největší dělitel čísla 2, takže i největší společný dělitel čísel $n(n+1)$ a 2.

Podívejme se nyní na NSD z jiného hlediska. K tomu bude potřeba začít něčím zdánlivě nesouvisejícím. Mějme daná čísla a, b, z nichž alespoň jedno je nenulové. Vezměme si množinu M všech čísel tvaru $ka + lb$, kde k, l jsou libovolná čísla (v množině jsou tedy například čísla a, $5a - 3b$, $-7b$ apod.). Všimněme si, že množina M má zajímavou vlastnost – kdykoliv do ní patří čísla i, j, tak do ní také patří jejich součet i rozdíl a také libovolný násobek jednoho z nich.

Nějaké číslo z množiny M musí být kladné (např. pro $k = a$ a $l = b$). Ze všech kladných čísel z M vyberme to nejmenší a označme ho r. Dokážeme, že všechna ostatní čísla v množině M (i ta záporná) jsou jeho násobkem. Pro spor předpokládejme, že nějaké číslo s není dělitelné číslem r. Nyní jej podělíme se zbytkem číslem r. Jinými slovy najdeme taková čísla u, v, pro která $s = ru + v$ a přitom $0 < v < r$ (v nemůže být nula, protože $r \nmid s$). Ale číslo r patří do naší množiny. Takže tam patří i číslo ru a dokonce i číslo $s - ru = v$. Tím jsme ale našli menší kladné číslo z množiny M, což je spor s předpokladem, že to nejmenší bylo r.

Jak to tedy ale všechno souvisí s NSD? Jak již možná tušíš, NSD čísel a, b není nic jiného než r. Víme totiž, že r patří do M, stejně jako čísla a, b. Takže $r \mid a$ a zároveň $r \mid b$. Ještě potřebujeme dokázat, že r je největší číslo s touto vlastností. Pro spor předpokládejme, že existuje takové větší číslo r'. Pak $r' \mid ka + lb$ pro všechna k, l, tedy dělí i r, protože $r = xa + yb$ pro nějaká x, y (patří do M). To je spor s tím, že je r' větší.

A dokázali jsme si hustou věc o NSD! Ale co víc – triviálně nám z tohoto důkazu plyne velice užitečná věta, jak v okamžení uvidíš.

Věta. (Bézoutova[7]) *Pro libovolná čísla a, b, z nichž alespoň jedno je nenulové, existují čísla k, l taková, že $ka + lb = (a, b)$.*

Důkaz. Jak víme z předchozích odstavců, tak (a, b) není nic jiného než r, které se dá zapsat jako $xa + yb$.

Když nastane případ $(a, b) = 1$, říkáme, že čísla a a b jsou *nesoudělná*. V opačném případě se jedná o čísla *soudělná*.

Příkladem použití Bézoutovy věty je důkaz následujícího tvrzení.

Tvrzení. *Nechť $a \neq 0$, b jsou nesoudělná čísla a platí $a \mid bc$. Potom také $a \mid c$.*

Důkaz. Z Bézoutovy věty plyne, že existují čísla k, l tak, že $ak + bl = (a, b) = 1$. Celou rovnici vynásobíme číslem c a dostaneme $ack + bcl = c$. Ale $a \mid ack$, dále $a \mid bc \mid bcl$, takže $a \mid ack + bcl = c$, což jsme chtěli dokázat.

[6] V angličtině se používají zkratky gcd – greatest common divisor a lcm – least common multiple.

[7] Étienne Bézout (1730–1783) byl francouzský matematik.

Cvičení. V následujících cvičeních platí $(a, b) = 1$. Dokaž:

(i) Pokud $a \mid c, b \mid c$, pak $ab \mid c$.
(ii) $[a, b] = ab$.

Úloha. Nechť a, b jsou dvě kladná nesoudělná čísla, m a n přirozená čísla a součet

$$\frac{ma-1}{b} + \frac{nb-1}{a}$$

je celočíselný. Dokaž, že platí nerovnost

$$\frac{m}{b} + \frac{n}{a} > 1.$$

(zobecnění MO 61–A–I–4)

Řešení. Sečteme-li zlomky, vidíme, že musí platit $ab \mid a(ma-1) + b(nb-1)$.

Speciálně tedy $b \mid a(ma-1) + b(nb-1)$, a jelikož $b \mid b(nb-1)$, tak i $b \mid a(ma-1)$. Ale a, b jsou nesoudělná čísla, takže $b \mid ma - 1$. Analogicky $a \mid nb - 1$. Vynásobením dostáváme:

$$ab \mid (ma-1)(nb-1) = mnab - (ma + nb - 1),$$
$$ab \mid ma + nb - 1.$$

Z toho plyne buď $ma + nb - 1 = 0$ (což však neplatí, protože $m, a, n, b \geq 1$), nebo $ab \leq ma + nb - 1$. To už jen jednoduše upravíme

$$ab < ma + nb,$$
$$\frac{m}{b} + \frac{n}{a} > 1.$$

Přesně to jsme chtěli dokázat.

Abychom mohli využívat silných vlastností nesoudělnosti, můžeme často udělat jednoduchý, ale účinný trik. Označíme si (a, b) například d a řekneme $a = du$, $b = dv$. Potom jsou čísla u, v nesoudělná, čehož právě využijeme. Vyzkoušej si to na následujících cvičeních.

Cvičení.

(i) Nechť $a \mid c, b \mid c$. Dokaž $[a, b] \mid c$.
(ii) $(a, b)[a, b] = ab$.

Nyní si můžeš dokázat další užitečnou vlastnost NSD.[8]

Cvičení. Dokaž:

(i) Pokud $(a, b) = d$ a $d' \mid a$, $d' \mid b$, tak $d' \mid d$.
(ii) Pokud $[a, b] = q$ a $a \mid q'$, $b \mid q'$, tak $q \mid q'$.

Návod. Postupuj sporem. Kdyby $d' \nmid d$, uvažte číslo $[d', d]$. Podobně v (ii).

Cvičení. Dokaž:

(i) Pokud $(a, c) = 1$ a $(b, c) = 1$ tak $(ab, c) = 1$.
(ii) $(a, b) = 1$, právě když $(a^2, b) = 1$.
(iii) Pokud $(b, c) = 1$, tak $(a, bc) = (a, b)(a, c)$.
(iv) $(a, bc) \mid (a, b)(a, c)$.

[8] Ta se někdy používá přímo jako definice NSD.

Eukleidův[9] algoritmus

Jak jsme slíbili, ukážeme si praktický způsob, jak NSD vypočítat. K tomu se využívá tzv. *Eukleidův algoritmus*. Nejprve si ale dokažme jednoduché pomocné tvrzení, že $(a,b) = (a-b,b)$. Označme $d = (a,b)$ a $d' = (a-b,b)$. Pak $d \mid a$, $d \mid b$, proto $d \mid a-b$, takže i $d \mid (a-b,b) = d'$. Na druhou stranu $d' \mid a-b$, $d' \mid b$, proto $d' \mid (a-b)+b = a$, takže i $d' \mid (a,b) = d$. Vidíme, že $d \mid d' \mid d$, tedy $d = d'$. Tím je důkaz pomocného tvrzení hotov a můžeme si ukázat samotný Eukleidův algoritmus.

Když dostaneme zadaná dvě čísla a, b, odečteme menší od většího a dostaneme novou dvojici (která má stejný největší společný dělitel jako ta původní). Když takto budeme vždy odečítat menší číslo od většího, postupně se budou čísla zmenšovat, až jedno bude nula a druhé nějaké c. Pak ale zřejmě $(0,c) = c$, takže c je také NSD čísel a, b.

Tento výpočet se dá ještě urychlit, když čísla nebudeme odčítat, ale když je budeme dělit se zbytkem. Například $(72,21)$. Podělíme-li číslo 72 číslem 21, dostaneme 3 a zbytek 9. Tedy $(72,21) = (72-3\cdot 21,21) = (9,21)$. Takto můžeme pokračovat:

$$(72,21) = (9,21) = (9,21-2\cdot 9) = (9,3) = (9-3\cdot 3,3) = (0,3) = 3.$$

Cvičení. Rozmysli si, proč funguje i tento urychlený způsob.

Tohoto algoritmu můžeme vhodně využít i v případě, že neznáme konkrétní čísla. Například

$$(a,(a+1)(a+3)) = (a,a^2+4a+3) = (a,a^2+4a+3-(a+4)a) = (a,3).$$

Díky tomu víme, že hledaný největší společný dělitel je buď 3, nebo 1 (podle toho, jestli $3 \mid a$, nebo ne). Nyní si vyzkoušej následující cvičení, aby ses s NSD lépe seznámil a uměl ho rychle počítat.

Cvičení. Urči, čemu se mohou rovnat tyto NSD. Předpokládej $(a,b) = 1$.

(i) $(a+b, a-b)$
(ii) $(a+b, ab)$
(iii) $(a^2+ab, a+b)$
(iv) (a^2+a, a^2+3a+2)

Cvičení. (těžké) Nechť $m = ax+by$, $n = cx+dy$ a platí $ad-bc = \pm 1$. Ukaž, že $(m,n) = (x,y)$.

Celá část čísla

V tomto oddíle trošku odbočíme od celých čísel a seznámíme s dolní a horní celou částí. Co to tedy je?

Definice. *Dolní celá část* reálného čísla x je největší celé číslo, které není větší než x. Značíme ji $\lfloor x \rfloor$. *Horní celá část* reálného čísla x je nejmenší celé číslo, které není menší než x. Ta se značí $\lceil x \rceil$.

Jinak řečeno, dolní celá část zahazuje to, co je za desetinnou čárkou (ovšem pozor na záporná čísla). Takže například $\lfloor \frac{7}{3} \rfloor = 2$; $\lfloor 4 \rfloor = 4$; $\lfloor -5{,}352 \rfloor = -6$; $\lceil 5{,}8 \rceil = 6$. Ještě se hodí znát pojem *desetinná část* čísla, který vyjadřuje hodnotu $x - \lfloor x \rfloor$ a značí se $\{x\}$. Například $\{\frac{7}{3}\} = \frac{1}{3}$,

[9] Eukleides (nebo Eukleidés) byl řecký matematik, který působil v Egyptě v Alexandrii. Žil přibližně v letech 325 př. n. l. – 260 př. n. l. Napsal významné dílo Základy (první opravdovou učebnici s axiomy a důkazy, prý druhou nejvydávanější knihu po Bibli).

$\{-5{,}352\} = 0{,}648$. Všimni si, že pokud je x celé číslo, tak $\lfloor x \rfloor = \lceil x \rceil = x$ a $\{x\} = 0$, jinak $\lceil x \rceil = \lfloor x \rfloor + 1$ a $0 < \{x\} < 1$.

To, jak se s celou částí pracuje, si ukážeme na následujícím příkladě.

Příklad. Pro reálné číslo r platí

$$\left\lfloor r + \frac{19}{100} \right\rfloor + \left\lfloor r + \frac{20}{100} \right\rfloor + \cdots + \left\lfloor r + \frac{91}{100} \right\rfloor = 546.$$

Zjisti $\lfloor 100r \rfloor$. (AIME 1991)

Řešení. Na levé straně je $91 - 19 + 1 = 73$ členů. Všechny z nich mají hodnotu buď $\lfloor r \rfloor$, nebo $\lfloor r \rfloor + 1$. Jelikož $7 \cdot 73 < 546 < 8 \cdot 73$, tak $\lfloor r \rfloor = 7$. Navíc $546 = 7 \cdot 73 + 35$, takže prvních 38 členů má hodnotu 7 a zbylé členy mají hodnotu 8. Speciálně

$$\left\lfloor r + \frac{56}{100} \right\rfloor = 7, \quad \left\lfloor r + \frac{57}{100} \right\rfloor = 8.$$

Proto $r + \frac{56}{100} < 8$, $r + \frac{57}{100} \geq 8$ a z toho plyne $743 \leq 100r < 744$, takže $\lfloor 100r \rfloor = 743$.

Jako cvičení si zkus dokázat tyto vlastnosti celých částí:

Cvičení. Nechť jsou x, y reálná čísla a nechť je a celé.

(i) $\lfloor x + a \rfloor = \lfloor x \rfloor + a$ a $\lceil x + a \rceil = \lceil x \rceil + a$.
(ii) Dolní celá část je neklesající, tedy pro $x \leq y$ platí $\lfloor x \rfloor \leq \lfloor y \rfloor$.
(iii) $\lfloor x + \frac{1}{2} \rfloor$ zaokrouhluje x k nejbližšímu celému číslu.
(iv) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
(v) Počet kladných násobků čísla n nepřekračujících kladné x je roven $\lfloor \frac{x}{n} \rfloor$.
(vi) Dokaž si tvrzení o dělení se zbytkem.
(vii) $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \lfloor \frac{x}{n} \rfloor$.

Návod. V (iv) rozepiš $x = \lfloor x \rfloor + \{x\}$. Tato finta je velice často používaná. V (vi) uvaž číslo $\lfloor \frac{a}{b} \rfloor$.

Příklad. Dokaž, že

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \cdots = n.$$

(IMO 1968)

Řešení. Nejprve si uvědomíme, že pro $n = 1$ tvrzení platí (první člen je 1 a ostatní jsou nulové). Pro spor předpokládejme, že tvrzení pro nějaké n neplatí, a vezměme nejmenší takové n.[10] Vyřešme případ, kdy n je sudé, tedy $n = 2m$. Jelikož m je menší než n, tak pro něj tvrzení ze zadání platí.

$$\left\lfloor \frac{m+1}{2} \right\rfloor + \left\lfloor \frac{m+2}{4} \right\rfloor + \left\lfloor \frac{m+4}{8} \right\rfloor + \cdots = m.$$

Rozšíříme všechny zlomky na levé straně dvěma a dostaneme

$$\left\lfloor \frac{2m+2}{4} \right\rfloor + \left\lfloor \frac{2m+4}{8} \right\rfloor + \cdots = m.$$

Zbývá nám přičíst $\lfloor \frac{2m+1}{2} \rfloor = m$, čímž dostaneme po dosazení $n = 2m$ požadovaný spor.

Pro liché n je důkaz jen lehce těžší, zkus si jej dokončit sám.

[10] To, že takové n můžeme vybrat, je důležitá vlastnost přirozených čísel. Využíváme ji i při důkazu matematickou indukcí.

Prvočísla

Nyní se dostáváme k asi nejdůležitějšímu pojmu teorie čísel. *Prvočíslo.* Pravděpodobně víš ze školy, že prvočísla jsou taková čísla, která mají právě dva kladné dělitele – jedničku a sama sebe (takzvaní triviální dělitelé). Ostatní přirozená čísla nazýváme *složená* (pouze jedničku nepovažujeme ani za prvočíslo, ani za číslo složené[11]). Začneme klíčovým tvrzením o prvočíslech, které se také často používá jako definice.[12]

Tvrzení. (klíčové) *Přirozené číslo p je prvočíslo právě tehdy, když pro každá a, b platí, že pokud $p \mid a \cdot b$, tak $p \mid a$ nebo $p \mid b$.*

Důkaz. Nejprve předpokládejme, že p není prvočíslo. Pak podle naší definice existuje dělitel $1 < a < p$, tudíž $\frac{p}{a}$ je celé číslo. Platí $p \mid a \cdot \frac{p}{a}$, ale přitom $p \nmid a$ a $p \nmid \frac{p}{a}$, protože $p > a$ a $p > \frac{p}{a}$.

Druhou (obtížnější) implikaci dokážeme sporem. Mějme tedy prvočíslo p a nechť platí $p \mid ab$, ale přitom $p \nmid a$, $p \nmid b$. Z $p \mid ab$ plyne $(p, ab) = p$. Ze cvičení (iv) na straně 4 víme, že $(p, ab) \mid (p, a)(p, b)$. Ale (p, a) může být jen 1 nebo p (protože p nemá jiné dělitele). Jelikož ale $p \nmid a$, tak musí být $(p, a) = 1$. Analogicky dostaneme $(p, b) = 1$. Pak ale $p \mid 1 \cdot 1$, což je požadovaný spor.

Cvičení. Nechť k, l, m jsou přirozená čísla.

(i) Dokaž, že pokud $k + l + m \mid klm$, tak je $k + l + m$ složené.
(ii) Mějme prvočíslo $p = 2k + 3$. Dokaž $p \nmid 2k^3 + 7k^2 + 3k$.

Návod. Rozlož na součin a využijte definici prvočísla.

Nyní jsme připravení vrhnout se na důkaz zásadního tvrzení, které nám říká, že veškerá informace o přirozeném čísle se ukrývá v prvočíslech, která jej dělí.

Tvrzení. (Základní věta aritmetiky) *Každé přirozené číslo $n > 1$ lze jednoznačně (až na pořadí) zapsat jako součin $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kde $p_1, p_2, \dots, p_k$ jsou po dvou různá prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k$ jsou přirozená čísla.*

Důkaz. Pro spor si vezměme nejmenší přirozené n, které nemá prvočíselný rozklad. Nemůže to být prvočíslo, protože to by zřejmě rozklad mělo. Jelikož je n složené, tak $n = ab$ pro nějaká a, $b < n$. Čísla a, b mají rozklad na prvočinitele (n je první číslo, které ho nemá), takže má prvočíselný rozklad i jejich součin, tj. n. Ještě ale nevíme, jestli je tento rozklad jednoznačný.

Nyní si pro spor vezměme nejmenší n, jehož prvočíselný rozklad není jednoznačný, tedy $n = p_1 p_2 \dots p_k = s_1 s_2 \dots s_l$, kde $p_1 \le p_2 \le \dots \le p_k$ ($s_1 \le s_2 \le \dots \le s_l$) jsou ne nutně různá prvočísla. Kdyby $p_1 \neq s_1$, tak můžeme BÚNO[13] předpokládat $p_1 < s_1$. Jelikož je p_1 prvočíslo, tak musí dělit alespoň jedno z čísel $s_1, \dots, s_l$, to jsou ale všechno prvočísla větší než p_1, což je spor. Proto $p_1 = s_1$, a tedy číslo $\frac{n}{p_1} < n$ nemá jednoznačný rozklad, protože můžeme psát

$$\frac{n}{p_1} = p_2 p_3 \dots p_k = s_2 s_3 \dots s_l.$$

Dospěli jsme ke sporu s tím, že n je nejmenší číslo, které má nejednoznačný rozklad.

Nabízí se otázka, kolik je vůbec prvočísel. Ukážeme si snadný, leč trikový důkaz, že jich je nekonečně mnoho.

Tvrzení. *Existuje nekonečně mnoho prvočísel.*

Důkaz. Předpokládejme, že prvočísel je jen konečně mnoho, a označme si je $p_1, p_2, \dots, p_k$. Uvažme číslo $n = p_1 p_2 \dots p_k + 1$. Díky existenci rozkladu na prvočísla musí být toto číslo

[11] Zlé jazyky ovšem tvrdí, že jednička je jediné složené prvočíslo.[1]

[12] K tomu matematici mají hlubší důvody, které jsou ovšem nad rámec tohoto seriálu.

[13] BÚNO je oblíbená matematická zkratka znamenající „bez újmy na obecnosti“.

dělitelné nějakým prvočíslem p_i, kde $i \in \{1, 2, \ldots, k\}$. Pak ale $p_i \mid n$ a současně $p_i \mid n-1$, takže i $p_i \mid n-(n-1) = 1$, což je spor.

Cvičení. (těžké) Ukaž, že existuje nekonečně mnoho prvočísel ve tvaru $4k+3$.

Kongruence

Nyní se naučíme jeden velice užitečný zápis. Budeme ho používat, když nebudeme potřebovat pracovat s čísly jako takovými, ale pouze s jejich zbytky po dělení nějakým číslem.

Definice. Skutečnost $m \mid (b-a)$ zapisujeme $a \equiv b \pmod{m}$ a čteme „*a je kongruentní s b modulo m*“.

Uvedenému výrazu se pak říká *kongruence*. Rozmysli si, že dvě čísla jsou kongruentní, právě když dávají stejný zbytek po dělení číslem m. Proto například $5 \equiv 17 \pmod{6}$ nebo $-2 \equiv 13 \pmod{5}$. Kongruence jsou velice přirozené díky své podobnosti s obyčejnými rovnicemi. Počítá se s nimi skoro stejně, což ukazuje následující tvrzení.

Tvrzení. *Pokud $a \equiv b \pmod{m}$ a k je libovolné číslo, tak platí:*

(i) $a + k \equiv b + k \pmod{m}$.
(ii) $a \cdot k \equiv b \cdot k \pmod{m}$.

Jinými slovy, k oběma stranám kongruence můžeme přičíst celé číslo a můžeme je také celým číslem vynásobit.

Tvrzení. *Pokud $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, tak platí:*

(iii) $a + c \equiv b + d \pmod{m}$.
(iv) $ac \equiv bd \pmod{m}$.

Důkaz. (iv) Víme, že $m \mid b-a$ a $m \mid d-c$. Proto $b = a + km$ a $d = c + lm$. Takže $bd = ac + m(kc + la + klm)$. Jinými slovy $bd - ac = m(kc + la + klm)$, což znamená $m \mid bd - ac$.

Cvičení. Jako cvičení si dokaž (i), (ii), (iii).

Vidíme, že kongruence můžeme navzájem sčítat (odčítat) a násobit. Nabízí se tedy otázka, jestli v nich lze – podobně jako v rovnicích – i dělit celým číslem. Odpověď je, že jen částečně.

Tvrzení. *Pokud $a \cdot c \equiv b \cdot c \pmod{m}$ a $(m, c) = 1$, tak $a \equiv b \pmod{m}$.*

Důkaz. Víme, že $m \mid c(b-a)$. Jelikož $(m, c) = 1$, platí i $m \mid (b-a)$.

V důkazu pěkně vidíme, proč je nesoudělnost potřeba. Opravdu, pokud například $8 \equiv 2 \pmod{6}$, tak z toho neplyne $4 \equiv 1 \pmod{6}$.

Viděli jsme, že jsme s kongruencemi proti obyčejným rovnicím v něčem trochu omezeni (byť jen zdánlivě, protože dělit soudělným číslem je podobné jako dělit nulou). Ale ještě nám zbývá zmínit vlastnosti, které zase mohou závidět rovnice.

Tvrzení. *Předpokládáme $a \equiv b \pmod{m}$, m' je přirozené číslo. Pak platí:*

(i) $a + k \cdot m \equiv b \pmod{m}$.
(ii) $m' \mid m$, *pak* $a \equiv b \pmod{m'}$.
(iii) (vylepšené dělení) *Pokud* $ca \equiv cb \pmod{m}$, *tak* $a \equiv b \pmod{\frac{m}{(m,c)}}$.

Cvičení. Zmíněná tvrzení si dokaž.

Návod. V (iii) polož $(m, c) = d$ a $m = du$, $c = dv$.

Úloha. Dokaž, že neexistuje přirozené číslo n takové, že $89^2 \mid n^2+n-22$. (MKS 30–2–6)

Řešení. Pro spor předpokládejme, že jsme našli n, pro které je podmínka splněna. Pak ale musí platit, že

$$\begin{aligned} n^2+n-22 &\equiv 0 \pmod{89^2},\\ 4(n^2+n-22) &\equiv 0 \pmod{89^2},\\ (2n+1)^2 &\equiv 89 \pmod{89^2}. \end{aligned}$$

Nyní můžeme přejít k modulu $89 \mid 89^2$ a zjistíme

$$\begin{aligned} (2n+1)^2 &\equiv 89 \pmod{89},\\ (2n+1)^2 &\equiv 0 \pmod{89}. \end{aligned}$$

Proto $89 \mid (2n+1)^2$, a jelikož je 89 prvočíslo, tak i $89 \mid 2n+1$. Pak ale $89^2 \mid (2n+1)^2$, takže

$$0 \equiv (2n+1)^2 \equiv 89 \pmod{89^2},$$

což je spor.

Uvedené vlastnosti kongruencí můžeme dobře shrnout. Pokud máme nějaký výraz, kde se jen násobí a sčítá, můžeme do něj dosadit dvě kongruentní čísla a výsledky budou také kongruentní. To je formálněji vyjádřeno v následujícím cvičení.

Cvičení. Mějme $a \equiv b \pmod{m}$.

(i) Pak $a^n \equiv b^n \pmod{m}$.

(ii) Nechť P je polynom[14] s celočíselnými koeficienty. Pak platí $P(a) \equiv P(b) \pmod{m}$. Jinými slovy – posloupnost zbytků, které dávají hodnoty polynomu v celých číslech, je periodická.

Návod. Polynom si rozepiš podle definice a pro každou mocninu použij (i).

Kvadratické zbytky

Zajímavou partií teorie kongruencí jsou kvadratické zbytky.

Definice. Číslo a nesoudělné s m je *kvadratický zbytek* modulo m, pokud existuje číslo x takové, že $x^2 \equiv a \pmod{m}$. Pokud takové x neexistuje, říkáme, že číslo je *nezbytek* modulo m.

Přestože jsme si kvadratické zbytky zavedli pro libovolné přirozené modulo m, nejzajímavější a nejužitečnější případ nastává, když je m prvočíslo. Tomuto případu se proto budeme věnovat více.

Pro prvočíselné modulo p můžeme kvadratické zbytky dobře popisovat tzv. *Legendreovým*[15] *symbolem*. Ten značíme $\left(\frac{a}{p}\right)$. Definujeme ho následujícím způsobem:

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

[14] Polynom neboli mnohočlen je funkce tvaru $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, kde $a_n \neq 0$. Čísla $a_n, a_{n-1}, \ldots, a_0$ nazýváme koeficienty polynomu. Je to přesně ten výraz, kde se pouze sčítá a násobí.

[15] Adrien-Marie Legendre [ležándr] byl francouzský matematik žijící v letech 1752–1833.

Která čísla jsou tedy kvadratickými zbytky? Všechna, nebo jen některá? Zkusíme-li to na malých případech, snadno zjistíme, že všechna to nebudou. Už pro modulo $m = 3$ dávají čísla 0^2, 1^2, 2^2 zbytky 0, 1, 1 (z nich je kvadratický zbytek pouze číslo 1, protože 0 není nesoudělná s m). Můžeme tedy dostat zbytek 2? Odpověď je, podle očekávání, ne. Kdybychom za x dosadili něco jiného, nepomohlo by nám to, protože

$$(x + 3a)^2 = x^2 + 6a + 9a^2 = x^2 + 3(2a + 3a^2) \equiv x^2 \pmod 3.$$

Všechna další x^2 už tedy budou dávat stejný zbytek jako jedno z čísel 0^2, 1^2, 2^2, tj. pouze 0 nebo 1 (všimni si, že jsme jen dosadili dvě kongruentní čísla, museli jsme tedy dostat stejný zbytek).

To už nám dává návod, jak zjistit, která čísla jsou kvadratické zbytky modulo nějaké m. Stačí si postupně spočítat zbytky po dělení čísel $0^2, 1^2, \ldots, (m-1)^2$. Takto například zjistíme, že modulo 4 je kvadratický zbytek pouze 1 a modulo 7 pak 1, 2, 4.

Příklad. Dokaž, že liché číslo, které se dá napsat jako součet dvou čtverců[16], je nutně tvaru $4k + 1$ pro číslo k.

Důkaz. Nechť $c = a^2 + b^2$. Na tuto rovnici se můžeme podívat modulo 4. Víme, že x^2 modulo 4 může dávat pouze zbytky 0 a 1, takže součet $a^2 + b^2$ může nabývat pouze zbytků 0, 1, 2. Jelikož se ale má jednat o liché číslo, tak musí jít o zbytek 1, tedy $c = 4k + 1$.

Cvičení. Urči hodnoty těchto Legendreových symbolů za předpokladu, že p je prvočíslo:

$$\left(\frac{1}{p}\right), \quad \left(\frac{4-p^2}{p}\right), \quad \left(\frac{3}{5}\right), \quad \left(\frac{p}{2}\right).$$

Cvičení. Předpokládej, že $\left(\frac{-1}{p}\right) = -1$ pro prvočíslo p. Dokaž $\left(\frac{-4}{p}\right) = -1$.

Návod. Vezmi si $x^2 \equiv -4$ a zaměř se na číslo $\frac{x}{2}$, případně $\frac{x+p}{2}$.

Mohlo by nás zajímat, kolik vlastně je kvadratických zbytků (mezi čísly $1, \ldots, p-1$). Pokud si to vyzkoušíme na malých případech,[17] lehko tipneme, že odpověď je $\frac{p-1}{2}$ pro prvočíselné modulo p. Nejdříve si uvědomíme, že více jich nebude. Druhá mocnina má totiž užitečnou vlastnost $x^2 = (-x)^2$. Toho můžeme využít i zde, neboť

$$x^2 = (-x)^2 \equiv (p - x)^2 \pmod p.$$

To znamená, že čísla 1, $p - 1$, dále 2, $p - 2$, atd. dávají po umocnění na druhou stejný zbytek. Kvadratických zbytků bude tedy nejvýše $\frac{p-1}{2}$.

Zbývá dokázat, že jich bude alespoň tolik. To je ekvivalentní s tím, že čísla $1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ dávají po dvou různé zbytky. Stačí nám tedy dokázat, že pro celá čísla $a \neq b$, která splňují $0 < a, b \leq \frac{p-1}{2}$, neplatí $a^2 \equiv b^2 \pmod p$. Pro spor předpokládejme, že by to platilo. Pak

$$\begin{aligned} a^2 &\equiv b^2 \pmod p, \\ a^2 - b^2 &\equiv 0 \pmod p, \\ (a-b)(a+b) &\equiv 0 \pmod p. \end{aligned}$$

Má tedy platit $p \mid (a-b)(a+b)$. Ale p je prvočíslo, takže $p \mid (a-b)$ nebo $p \mid (a+b)$. Víme, že $a \neq b$, takže $a - b \neq 0$. Navíc $-\frac{p-1}{2} < a - b < \frac{p-1}{2}$, takže určitě $p \nmid (a-b)$. (To plyne z toho,

[16] Čtvercem myslíme druhou mocninu celého čísla.

[17] Do olympiády doporučujeme si zapamatovat kvadratické zbytky pro malá čísla.

že mezi $-\frac{p-1}{2}$ a $\frac{p-1}{2}$ je jen číslo 0 dělitelné p.) Ale $0 < a + b \leq (p-1)$, takže i $p \nmid (a+b)$. To je požadovaný spor.

Malá Fermatova[18] věta

V tomto odstavci se více podíváme na to, jak se zbytky násobí a mocní. Vezměme libovolné číslo a nesoudělné s m, umocňujme ho a počítejme zbytky mod m. Protože zbytků je jen konečně mnoho, najdeme dvě čísla $k > l$ tak, že $a^k \equiv a^l \pmod{m}$. To znamená, že $a^{(k-l)} \equiv 1 \pmod{m}$, neboť kongruenci můžeme vydělit číslem a^l nesoudělným s m. Našli jsme tedy přirozené číslo $r = k - l$ takové, že $a^r \equiv 1 \pmod{m}$. Nejmenší přirozené číslo s touto vlastností nazýváme *řád* prvku a modulo m a značíme jej $\mathrm{ord}_m(a)$. (Nebo pouze r, pokud to je z kontextu jasné.) Pokud číslo a je soudělné s m, řád neexistuje: pokud umocňujeme třeba 2 (mod 4), dostáváme $2, 0, 0, 0, \ldots$ a nikde žádná jednička.

Cvičení. Proč čísla soudělná s modulem nemají řád?

Návod. Pokud $a^r \equiv 1 \pmod{m}$, pak také $a^r \equiv 1 \pmod{(a,m)}$.

Cvičení. Jaký je řád 2 mod 5?

Tvrzení. („zbytky lze dělit“) *Pro každé číslo a nesoudělné s m existuje právě jedna inverze modulo m, tj. prvek a' takový, že $aa' \equiv 1 \pmod{m}$. Obvykle inverzi značíme $\frac{1}{a}$ nebo a^{-1}.*

Důkaz. Nejprve si dokážeme, že takové číslo existuje alespoň jedno. Stačí si zvolit $a' = a^{r-1}$. Pak $a \cdot a' \equiv a \cdot a^{r-1} \equiv a^r \equiv 1 \pmod{n}$, tedy toto a' vyhovuje zadané podmínce.

Nyní si dokážeme, že je takové číslo (modulo m) jen jedno. Kdyby existovaly dvě různé inverze a' a a'' modulo n, tak $a \cdot a' \equiv 1 \equiv a \cdot a'' \pmod{m}$, a jelikož čísla a a m jsou nesoudělná, tak můžeme kongruenci $a \cdot a' \equiv a \cdot a'' \pmod{m}$ podělit číslem a. Tím dostaneme $a' \equiv a'' \pmod{m}$, což je spor s tím, že a' bylo různé od a''.

Cvičení. Dokažte předchozí tvrzení pomocí Bézoutovy věty.

To pro nás znamená, že v kongruencích můžeme používat i zlomky. Zlomkem $\frac{a}{b}$ jednoduše myslíme $a \cdot b^{-1}$. V kongruencích se tedy klidně může vyskytnout něco jako $\frac{1}{3} + \frac{1}{4} \equiv 0 \pmod{7}$. To proto, že inverze k číslu 3 modulo 7 je 5 (platí $3 \cdot 5 \equiv 1 \pmod{7}$) a inverze k číslu 4 je číslo 2. Takže $\frac{1}{3} + \frac{1}{4} \equiv 5 + 2 \equiv 0 \pmod{7}$. Naopak nemá v kongruencích modulo 6 smysl výraz $\frac{1}{2}$, protože čísla 2 a 6 jsou soudělná, a tedy číslo 2 nemá inverzi modulo 6.

Cvičení. Dokaž, že čísla, která jsou soudělná s m, inverzi modulo m nemají.

Cvičení. Dokaž, že zlomky můžeme v kongruencích upravovat podobně jako v obyčejných rovnicích. Tedy, že pro b, d nesoudělná s m platí:

(i) $\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \pmod{m}$.
(ii) $\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \pmod{m}$.

Nyní si ukážeme, k čemu se inverze například hodí, na důkazu Wilsonovy[19] věty.

Věta. (Wilsonova) *Nechť p je prvočíslo. Pak $(p-1)! \equiv -1 \pmod{p}$.*[20]

Důkaz. Podívejme se na číslo a mezi 1 a $p-1$. To je nesoudělné s p, takže má inverzi a^{-1}. Pokud $a \equiv a^{-1} \pmod{p}$, tak platí $a^2 \equiv 1 \pmod{p}$, neboli $(a+1)(a-1) \equiv 0 \pmod{p}$. Takže

[18] Pierre de Fermat (1601–1665) byl francouzský matematik amatér, povoláním právník.

[19] Wilsonova věta byla prý poprvé uvedena Ibn al-Haythamem (cca 1000 n. l.) a potom Waringem, jehož žákem byl Wilson. Ani jeden ze jmenovaných ji nedokázal, to udělal až Lagrange.

[20] Znakem $n!$ [n faktoriál] myslíme číslo $n \cdot (n-1) \cdots 1$.

$p \mid a+1$ nebo $p \mid a-1$. To ale znamená, že a je $p-1$ nebo 1. V ostatních případech tudíž platí $a \not\equiv a^{-1} \pmod{p}$. Ale pokud a má inverzi a^{-1}, tak zřejmě a^{-1} má inverzi a. Pokud tedy vynásobíme všechny zbytky od 2 do $p-2$, tak se každý zbytek popáruje se svojí inverzí a jejich součin bude 1. Proto

$$(p-1)! = (p-1) \cdot 1 \cdot (2 \cdot 3 \cdots (p-2)) \equiv (-1) \cdot 1 \cdot 1 \equiv -1 \pmod{p}.$$

Cvičení. Dokaž si ještě opačnou implikaci. Tedy pokud $(p-1)! \equiv -1 \pmod{p}$, tak p je prvočíslo.

Následující tvrzení popisuje důležitou vlastnost řádu.

Tvrzení. *Nechť a, n jsou nesoudělná čísla. Pak $a^n \equiv 1 \pmod{p}$ právě tehdy, když $r \mid n$.*

Návod. U jedné implikace stačí kongruenci umocnit. U druhé podělte n číslem r se zbytkem a ukažte, že r není řád, čímž dostanete spor.

Věta. (Malá Fermatova) *Nechť p je prvočíslo a a je číslo s ním nesoudělné. Potom $a^{p-1} \equiv 1 \pmod{p}$.*

Důkaz. Postupovat můžeme mnoha způsoby, například indukcí. My však předvedeme trochu jiný, poučný důkaz.

Vezměme r jako řád čísla a modulo p. Pro každé b od 1 do $p-1$ uvažujme množinu A_b obsahující zbytky čísel $b, ba, ba^2, \ldots, ba^{r-1}$ po dělení p. Dokažme si, že takováto množina má r prvků. Opravdu, kdyby $ba^k \equiv ba^l \pmod{p}$, kde $k > l$, dostali bychom $a^{k-l} \equiv 1 \pmod{p}$. Ale $k-l$ je menší než r, což je spor s tím, že r je řád, tedy nejmenší přirozené číslo, pro které platí $a^r \equiv 1 \pmod{p}$.

Pokud dvě z těchto množin A_b a A_c mají společný prvek $ba^k \equiv ca^l \pmod{p}$, potom pro libovolné i platí $ba^i \equiv ca^{(l-k)i} \equiv ca^x \pmod{p}$, kde x je zbytek čísla $(l-k)i$ po dělení r. Ale ca^x leží v A_c, tedy ba^i leží v A_c pro každé i od 0 do $p-1$. Jinak řečeno, každý prvek A_b je také prvkem A_c. Obdobně dostaneme i to, že prvky A_c jsou v množině A_b. To znamená, že $A_b = A_c$. Každé dvě množiny jsou tedy buď disjunktní (nemají žádný společný prvek), nebo se sobě rovnají.

Pokud označíme počet různých množin A_b (pro b od 1 do $p-1$) jako s, dostáváme, že $rs = p-1$, neboť sjednocením všech množin A_b dostaneme celou množinu zbytků (až na 0), tedy $p-1$ čísel. Z toho plyne, že $r \mid p-1$, takže $a^{p-1} \equiv 1 \pmod{p}$ podle předchozího tvrzení.

Díky MFV[21] se můžeme dozvědět více o kvadratických zbytcích.

Příklad. Nechť p je liché prvočíslo. Ukaž, že pokud je -1 kvadratický zbytek modulo p, potom je p tvaru $4k+1$ pro nějaké číslo k.

Řešení. Pro spor předpokládejme, že $p = 4k+3$. Protože $x^2 \equiv -1 \pmod{p}$ pro nějaké x, máme $x^{p-1} \equiv x^{4k+2} \equiv (x^2)^{2k+1} \equiv -1 \pmod{p}$, což je spor s MFV.

Nyní si ukážeme užitečný způsob, jak zjistit, jestli je číslo zbytek, nebo nezbytek.

Tvrzení. (Eulerovo[22] kritérium) *Nechť p je liché prvočíslo a a je číslo nesoudělné s p, potom $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Důkaz. Předpokládejme, že a není kvadratický zbytek modulo p. Chceme dokázat, že potom $a^{\frac{p-1}{2}}$ dává zbytek -1 po dělení p. Pro spor předpokládejme, že to neplatí. Mějme číslo b mezi 1 a $p-1$. Pak má kongruence $bx \equiv a \pmod{p}$ právě jedno řešení v x modulo p, a to $b' = ab^{-1}$. Kdyby $b' = b$, tak by platilo $b^2 \equiv a \pmod{p}$, tedy a by byl kvadratický zbytek modulo p, což

[21] Takto budeme označovat Malou Fermatovu větu.

[22] Leonhard Euler (1707–1783) byl švýcarský matematik působící (hlavně) v Petrohradu.

je spor. Musí tudíž platit $b' \neq b$. Pak se čísla 1 až $p-1$ po vynásobení popárují do dvojic se zbytkem a, a tedy bude platit

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

Z Wilsonovy věty plyne, že $(p-1)!$ dává zbytek -1 po dělení p, takže $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Sám si jako cvičení dokaž opačnou implikaci.

Pomocí Eulerova kritéria si můžeš dokázat, že v předešlém příkladu platí i opačná implikace:

Cvičení. Ukaž, že pokud je prvočíslo p tvaru $4k+1$, tak -1 je kvadratický zbytek modulo p.

Cvičení. (těžké) Dokaž, že prvočísel tvaru $4k+1$ je nekonečně mnoho.

Návod. Uvaž číslo $(n!)^2+1$ a ukaž, že má prvočíselného dělitele p tak, že -1 je kvadratický zbytek modulo p.

Nyní se seznámíme s důležitou funkcí, se kterou se budeme setkávat během celého seriálu.

Definice. *Eulerova funkce* $\varphi(n)$ je počet přirozených čísel nesoudělných s n a menších či rovných n.

Podívejme se, jak se funkce chová na prvočíslech. Mějme prvočíslo p. Potom každé přirozené číslo menší než p je s p nesoudělné. Proto $\varphi(p) = p-1$.

Pro mocniny prvočísel je situace podobně jednoduchá. Pokud máme číslo p^k, kde p je prvočíslo, tak nesoudělná čísla jsou právě ta, která nejsou dělitelná p. Ale čísel dělitelných p od 1 do p^k je $\frac{p^k}{p} = p^{k-1}$. Proto je nesoudělných čísel $p^k - p^{k-1}$.

Abychom mohli funkci spočítat pro libovolné n, musíme ještě dokázat zásadní vlastnost Eulerovy funkce, kterou nazýváme *multiplikativita*.

Tvrzení. *Eulerova funkce je multiplikativní, tedy pro nesoudělná čísla a, b platí $\varphi(ab) = \varphi(a)\varphi(b)$.*

Důkaz. Napišme si všechna čísla $0, 1, \ldots, ab-1$ do tabulky – jednoduše po řádcích zleva doprava.

0	1	2	...	$a-1$
a	$a+1$	$a+2$	...	$2a-1$
...	...	...	...	...
$a(b-1)$	$a(b-1)+1$	$a(b-1)+2$	...	$ab-1$

Koukněme se na číslo v řádku i a sloupci j, přičemž řádky a sloupce značíme od nuly. Pak je na tomto místě napsané číslo $ia+j$. Zajímá nás, zda je soudělné s ab. Jelikož jsou ale čísla a a b nesoudělná, tak stačí zjistit, jestli je $ia+j$ nesoudělné jak s a, tak s b. Aby bylo číslo nesoudělné s a, tak musí být $(ia+j, a) = 1$, tedy $(j, a) = 1$. To ale znamená, že čísla nesoudělná s ab mohou být jen ve sloupcích označených čísly, která jsou nesoudělná s a. Těchto sloupců je $\varphi(a)$.

Podívejme se na čísla v jednom z těchto sloupců. Jsou to čísla $j, a+j, 2a+j, \ldots, (b-1)a+j$. Tato čísla dávají navzájem různé zbytky modulo b. (Rozmysli si, že to platí – předpokládej, že by dvě čísla byla navzájem kongruentní modulo b, a dojdi ke sporu.)

Čísla tedy dávají v nějakém pořadí zbytky $0, 1, \ldots, b-1$ modulo b. Právě $\varphi(b)$ z nich je nesoudělných s b, a tedy i s ab. V každém z uvažovaných $\varphi(a)$ sloupců máme $\varphi(b)$ čísel nesoudělných s ab, dohromady je tedy čísel nesoudělných s ab přesně $\varphi(a)\varphi(b)$, což jsme chtěli dokázat.

Díky multiplikativitě dostáváme pro $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ vztah

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

Cvičení. Uprav vzoreček do tvaru

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right).$$

Seriál zakončíme kouzelnou formulí.

Tvrzení. *Platí*

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

Pokud Tě zaráží symbol $\sum$, rádi Ti ho vysvětlíme. Říká se mu *suma* a značí součet několika členů. Například $\sum_{k=1}^{n} a_k$ znamená $a_1 + a_2 + \dots + a_n$ (tj. sečti a_k pro k od 1 do n). Když pod sumou píšeme $d \mid n$, tak tím myslíme součet přes všechny kladné dělitele d čísla n. Například $\sum_{d\mid 6}\varphi(d) = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(6) = 1+1+2+2 = 6$.

Naše formule tedy říká, že pokud sečteme $\varphi(d)$ přes všechny dělitele d čísla n, tak dostaneme přesně n. Ale ještě si to musíme dokázat! Držte si klobouky.

Důkaz. Budeme potřebovat rozklad čísla n na prvočísla $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Nejprve si musíme uvědomit, že součet všech dělitelů se dá zapsat takto:

$$\sum_{d\mid n} d = \big(1+p_1+p_1^2+\dots+p_1^{\alpha_1}\big)\big(1+p_2+p_2^2+\dots+p_2^{\alpha_2}\big)\dots\big(1+p_k+p_k^2+\dots+p_k^{\alpha_k}\big).$$

Pokud totiž roznásobíme všechny závorky na pravé straně, dostaneme každého dělitele čísla n právě jednou. Ale s využitím toho, že funkce φ je multiplikativní, můžeme psát i toto:

$$\sum_{d\mid n}\varphi(d) = \big(\varphi(1)+\varphi(p_1)+\dots+\varphi(p_1^{\alpha_1})\big)\dots\big(\varphi(1)+\varphi(p_k)+\dots+\varphi(p_k^{\alpha_k})\big).$$

My ale víme, že $\varphi(p^k) = p^k - p^{k-1}$, takže

$$\varphi(1)+\varphi(p_i)+\dots+\varphi(p_i^{\alpha_i}) = 1+(p_i-1)+(p_i^2-p_i)+\dots+(p_i^{\alpha_i}-p_i^{\alpha_i-1}) = p_i^{\alpha_i}.$$

To nám dohromady dává

$$\sum_{d\mid n}\varphi(d) = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k} = n.$$

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 $p^k \mid n$.[23] 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).

[23] 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.[24]

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 $p \nmid a_i$.

[24] 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[25] 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

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

[25] 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.[26] 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

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

[26] 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[27] 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.[28]

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

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

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

[28] 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,[29] $\varphi(p^k) = p^k - p^{k-1}$, 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[30] modulo p. Jak jsi asi slyšel, polynom stupně n s reálnými koeficienty

[29] Nebo jak si snadno rozmyslíš.

[30] 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[31]) *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[32]

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

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.

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

[32] 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.[33] 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[34] a dostaneme[35]

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

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[36] 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“).

---

[33] Jak v PraSeti, tak v olympiádě.

[34] 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 $k \cdot \frac{q^n - 1}{q-1}$.

[35] 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.

[36] (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[37] čísel. Připomeňme, že Mersennovo číslo je číslo ve tvaru $2^n - 1$.

[37] 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[38]

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

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 $2^n - 1$.[39]

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

[38] Jak si poctivá čtenářka snadno roznásobí.

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

[40] 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.

Seriál – Teorie čísel III

A je tu třetí, závěrečný, opět o něco kratší díl seriálu! K jeho přečtení nebudeš příliš potřebovat látku předchozích dílů, spíš bude nutné nebát se a pořádně se zamýšlet. Odměnou Ti bude kus krásné matematiky, který sice tolik nevyužiješ v olympiádě, ale pro který stojí za to žít.

Na co se tedy můžeš těšit? Nejprve se naučíš zkrotit hrůzostrašně vyhlížející sumy. Poté se seznámíš s všelijakými aritmetickými funkcemi, naučíš se je chytře násobit a vše využiješ k jednoduchým a extrémně elegantním důkazům překvapivých identit.

Práce se sumami

V tomto díle budeme často používat složitější úpravy výrazů se sumami. Jedná se sice o techničtější část matematiky, ale zjistíš, že se v ní ukrývají i pěkné triky. Práci se sumami navíc mnohokrát zúročíš i v dalších oborech. Nejprve si zopakujeme sumární zápis a poté si ukážeme základní úpravy, které nám později ulehčí život.

Symbol $\sum$ značí součet několika členů, a to v různých kontextech, jak se nejlépe ukáže na příkladech. Mějme nějakou funkci f.

(i) Definujeme $\sum_{k=1}^{n} f(k) = f(1) + f(2) + \cdots + f(n)$. Suma tedy vyjadřuje následující: Nejprve za k dosaďme 1, potom 2, 3, ... a nakonec n. Všechny tyto členy sečtěme. Například

$$\sum_{k=1}^{n} 1 = n, \quad \sum_{m=2}^{4} (m^2+1) = 32 = 1 + \sum_{n=0}^{4} 2^n.$$

(ii) Výraz $\sum_{d|n} f(d)$ vyjadřuje součet $f(d)$ přes všechny kladné dělitele d čísla n. Tedy

$$\sum_{d|18} d^2 - 1 = (1^2-1) + (2^2-1) + (3^2-1) + (6^2-1) + (9^2-1) + (18^2-1).$$

(iii) Obecně $\sum_{i \in I} f(i)$ znamená součet přes všechny prvky množiny I. Třeba

$$\sum_{i \in \{1,\,3,\,-6,\,8\}} f(i) = f(1) + f(3) + f(-6) + f(8).$$

(iv) Také se nám může stát, že potřebujeme sčítat přes dvě proměnné. Například

$$\sum_{2 \le a,b \le 3} f(a) \cdot f(b) = f(2)^2 + f(2)f(3) + f(3)f(2) + f(3)^2,$$

$$\sum_{\substack{2 \le i \le 4 \\ d \mid i}} \frac{f(i)}{f(d)} = \frac{f(2)}{f(1)} + \frac{f(2)}{f(2)} + \frac{f(3)}{f(1)} + \frac{f(3)}{f(3)} + \frac{f(4)}{f(1)} + \frac{f(4)}{f(2)} + \frac{f(4)}{f(4)}.$$

Proměnnou k (resp. d, m, n, i, a, b), přes kterou jsme v sumě sčítali, nazýváme index a automaticky ji považujeme za celé číslo. Ukažme ještě jeden konkrétní příklad s vnořenými sumami:

$$\sum_{d|4}\sum_{a=1}^{d} 2a = (2) + (2+4) + (2+4+6+8) = 28.$$

Vytknutí čísla před sumu

První často používanou úpravou je vytknutí čísla před sumu. Když máme uvnitř sumy součin a jeden z činitelů je nezávislý na sčítacím indexu, můžeme tento činitel vytknout před sumu. Jedná se o běžné vytknutí, jak ho známe, jen u sum může působit nezvykle. Například

$$\begin{aligned}\sum_{i=1}^{n} n\cdot(n+i-1) &= n\cdot n + n\cdot(n+1) + \cdots + n\cdot(2n-1)\\ &= n\cdot\big(n + (n+1) + \cdots + (2n-1)\big)\\ &= n\cdot\sum_{i=1}^{n}(n+i-1).\end{aligned}$$

Prohazování sum

Často se nám stane, že máme dvě sumy vedle sebe. Pak je můžeme prohodit. Například

$$\sum_{i=1}^{n}\sum_{j=1}^{m} f(i)\cdot g(j) = \sum_{j=1}^{m}\sum_{i=1}^{n} f(i)\cdot g(j).$$

Uvědomme si, že se opravdu nic nezměnilo. Když si totiž představíme čísla $f(i)\cdot g(j)$ v tabulce s m řádky a n sloupci, tak levá strana vyjadřuje, že jsme udělali součty v každém ze sloupců a výsledky jsme pak sečetli. Naproti tomu na pravé straně jsme sečetli součty řádků. Zřejmě jsme tedy dostali v obou případech stejné číslo – součet všech čísel v tabulce. Na ten se taky můžeme dívat jako na sumu

$$\sum_{\substack{1\le i\le n\\ 1\le j\le m}} f(i)\cdot g(j).$$

Prohazování sum se dá vhodně kombinovat s vytýkáním:

$$\sum_{i=1}^{n}\Big(f(i)\sum_{j=1}^{m} g(j)\Big) = \sum_{i=1}^{n}\sum_{j=1}^{m} f(i)\cdot g(j) = \sum_{j=1}^{m}\sum_{i=1}^{n} f(i)\cdot g(j) = \sum_{j=1}^{m}\Big(g(j)\sum_{i=1}^{n} f(i)\Big).$$

To se může hodit například, pokud neumíme vyjádřit součet $\sum_{i=1}^{m} g(i)$, ale součet $\sum_{i=1}^{n} f(i)$ ano. První, resp. poslední výraz v předchozí rovnosti se dá taky upravit dalším vytknutím na součin dvou sum, tedy na

$$\Big(\sum_{i=1}^{n} f(i)\Big)\cdot\Big(\sum_{j=1}^{m} g(j)\Big).$$

Prohození sum je ještě o trochu komplikovanější, když prvky, přes které sčítáme ve vnitřní sumě, jsou závislé na indexu vnější sumy. Například $\sum_{d|n}\sum_{e|d} f(e)$. Chtěli bychom na první místo dostat sumu přes e. K tomu si stačí uvědomit, že e je dělitel čísla n. Tedy vnější suma

bude $\sum_{e|n}$. A jaké nyní klást podmínky na d? Musí platit, že d je násobek e a přitom $d \mid n$. Vnitřní suma proto bude $\sum_{\substack{d=e\cdot x \\ d|n}}$. Výraz tak upravíme do podoby

$$\sum_{d|n}\sum_{e|d} f(e) = \sum_{e|n}\sum_{\substack{d=e\cdot x \\ d|n}} f(e) = \sum_{e|n}\Big(f(e)\sum_{\substack{d=e\cdot x \\ d|n}} 1\Big).$$

Rozmysli si, že jsme opravdu žádný člen nevypustili a žádný nezapočítali vícekrát.

Cvičení. Opravdu si to rozmysli.

Nyní uvidíme, proč se prohození sum vyplatilo. Vnitřní sumu totiž umíme dál pěkně upravit. Sčítáme několikrát jedničku, stačí jen zjistit kolikrát. Jinak řečeno, vnitřní suma se rovná počtu takových čísel d, že $d = ex$ a zároveň $d \mid n$. Tedy $ex \mid n$, a jelikož $e \mid n$, tak $x \mid \frac{n}{e}$. Počet vyhovujících čísel d je proto stejný jako počet x takových, že $x \mid \frac{n}{e}$. Odpovědí je tedy počet dělitelů čísla $\frac{n}{e}$. Pokud označíme $\tau(n)$ počet dělitelů čísla n, tak jsme původní výraz upravili na

$$\sum_{d|n}\sum_{e|d} f(e) = \sum_{e|n} f(e)\cdot\tau\Big(\frac{n}{e}\Big). \qquad (\heartsuit)$$

Aritmetické funkce

V této kapitole se dostáváme k hlavnímu programu našeho seriálu – aritmetickým funkcím. Budeme je zkoumat, sčítat, násobit (a možná jinak, než bys čekal(a)), a díky tomu si odvodíme mnoho zajímavých výsledků teorie čísel. Co to tedy je?

Definice. *Aritmetická funkce* je funkce z přirozených čísel do reálných čísel.[41]

Příkladem aritmetických funkcí jsou funkce $f(n) = n^3$, $f(n) = \log(n)$ nebo Eulerova funkce $\varphi(n)$.

Zajímavé aritmetické funkce dostaneme, když vezmeme všelijaké vlastnosti čísla n týkající se dělitelnosti.

Definice. Aritmetickou funkcí $\tau(n)$ myslíme počet všech kladných dělitelů čísla n.[42] Součet všech kladných dělitelů čísla n označujeme jako $\sigma(n)$.

S těmito aritmetickými funkcemi jsme se vlastně již setkali – zmiňovali jsme totiž dokonalá čísla, což jsou přesně ta čísla n, pro která platí $\sigma(n) = 2n$.

Počet dělitelů $\tau(n)$ můžeme snadno vyjádřit, pokud známe rozklad čísla n na prvočísla.

Tvrzení. *Nechť $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ je rozklad čísla n na prvočísla. Pak platí*

$$\tau(n) = (\alpha_1+1)\cdots(\alpha_r+1).$$

Důkaz. Stačí si uvědomit, že každý dělitel obsahuje ve svém rozkladu pouze prvočísla $p_1,\ldots,p_r$, přičemž prvočíslo p_i v mocnině 0 až α_i. To je tedy (α_i+1) možností pro prvočíslo p_i. Jelikož můžeme exponenty u různých prvočísel volit nezávisle na sobě, zjistíme počet všech dělitelů jako součin těchto výrazů.

[41] Nebo dokonce komplexních. Aritmetické funkce jsou vlastně jen jiný pohled na posloupnosti.

[42] Mluvíme o ní krátce jako o *počtu dělitelů*.

Podobný vzorec závislý na rozkladu na prvočísla existuje i pro součet dělitelů. K němu přirozeně dospějeme v kapitole o multiplikativních funkcích, zatím si jen uvědomíme, že platí následující.

Tvrzení. *Pro součet dělitelů mocniny prvočísla platí* $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$.

Důkaz. Jedná se pouze o známý[43] vztah pro součet geometrické řady $1 + p + \cdots + p^k$. Se znalostí tohoto vzorečku už snadno požadovaný výsledek dokážeš.

Seznámíme se nyní s další aritmetickou funkcí – Möbiovou funkcí μ, která hraje v následující teorii klíčovou roli.

Definice. *Möbiova*[44] *funkce* μ je

$$\mu(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0, & \text{je-li } n \text{ čtvercové, tedy existuje-li } a > 1 \text{ takové, že } a^2 \mid n, \\ (-1)^r, & \text{je-li } n = p_1 p_2 \cdots p_r, \text{ kde } p_i \text{ jsou navzájem různá prvočísla.} \end{cases}$$

Například $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$. Jednu z pěkných vlastností Möbiovy funkce ukazuje následující důležité tvrzení.

Tvrzení. *Platí:*

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n > 1. \end{cases} \qquad (\clubsuit)$$

Důkaz. Všimněme si, že pokud jsou a, b nesoudělná, platí $\mu(a)\mu(b) = \mu(ab)$. Pro $n = 1$ je triviálně součet roven jedné. Máme-li $n > 1$, můžeme ho rozložit na prvočísla, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Jediní dělitelé čísla n, kteří do sumy přispějí, jsou ti bezčtvercoví. Proto můžeme psát (vyzkoušej si, že po roznásobení prostředního výrazu opravdu dostaneme každé nenulové číslo ze součtu nalevo právě jednou)

$$\sum_{d|n} \mu(d) = (1 + \mu(p_1))(1 + \mu(p_2)) \ldots (1 + \mu(p_r)) = 0 \cdot 0 \cdots 0 = 0,$$

což jsme chtěli dokázat.

Dirichletova konvoluce

Nyní již umíme sčítat sumy a můžeme se vrhnout na tento příklad (dobře si ho promysli).

Příklad. Ukaž, že pro $n \geq 1$ platí

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}.$$

Řešení. Nejprve si uvědomíme, že výraz $\lfloor 1/(a,b) \rfloor$ je roven jedné, právě když jsou čísla a, b nesoudělná, jinak je to nula. Proto se $\varphi(n)$ dá vyjádřit jako tato suma:

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor.$$

[43] A snadno vygooglitelný.

[44] August Ferdinand Möbius (1790–1868) byl německý matematik a teoretický astronom. Kromě toho, že se věnoval teorii čísel, byl také jedním ze zakladatelů topologie. Pravděpodobně jsi už slyšel(a) o Möbiově pásce.

Následně využijeme vztahu (♣) pro každý ze sčítanců sumy a dostaneme

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor = \sum_{k=1}^{n} \sum_{d \mid (n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d \mid n \\ d \mid k}} \mu(d).$$

Nyní přichází čas na prohození sum, které je opět poměrně náročné, pročež si jej dobře rozmysli.

$$\sum_{k=1}^{n} \sum_{\substack{d \mid n \\ d \mid k}} \mu(d) = \sum_{d \mid n} \sum_{\substack{k = dx \\ k \leq n}} \mu(d) = \sum_{d \mid n} \Big(\mu(d) \sum_{\substack{k = dx \\ k \leq n}} 1 \Big).$$

Zbývá si uvědomit, že poslední vnitřní suma vyjadřuje jen počet násobků čísla d menších nebo rovných n. A jelikož $d \mid n$, je jich přesně $\frac{n}{d}$. Tím jsme dostali požadovaný vztah, který si připomeneme pro případ, že už jsi zapomněl(a), co vlastně dokazujeme:

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

Poznámka. Součet v minulém příkladu je speciálním případem výrazu

$$\sum_{d \mid n} f(d) \cdot g\Big(\frac{n}{d}\Big),$$

kde f a g jsou aritmetické funkce. Takovéto součty se v teorii čísel často objevují a my se nyní budeme zabývat jejich obecnými vlastnostmi.

Předtím si zavedeme ještě dvě jednoduché, ale užitečné aritmetické funkce:

Definice. *Jednotka* je aritmetická funkce u, která všem číslům přiřadí jedničku (tedy $u(n) = 1$ pro každé n.)[45]

Definice. Aritmetická funkce N je definovaná vztahem $N(n) = n$ pro každé n.[46]

Definice. *Dirichletova konvoluce*[47] aritmetických funkcí f a g je aritmetická funkce

$$h(n) = \sum_{d \mid n} f(d) \cdot g\Big(\frac{n}{d}\Big).$$

Konvoluci funkcí f a g značíme $f * g$.

Konvoluce je tedy operace, která vezme dvě aritmetické funkce a vyrobí z nich třetí. Na příkladu jsme viděli, že když zvolíme za f Möbiovu funkci μ a za g funkci N, dostaneme φ, jinými slovy $\varphi = \mu * N$.

Jiným zajímavým příkladem jsme zakončili první díl seriálu, když jsme si ukázali, že platí

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

Tento vztah neříká nic jiného, než že $N = \varphi * u$. V takovémto případě, kdy je jedna z funkcí v konvoluci u, zavádíme nový pojem.

[45] Značení vychází z anglického slova *unit*.

[46] Značení vychází z českého slova *nuda*.

[47] Můžeš se také setkat s pojmem Dirichletův součin. My budeme v seriálu říkat jednoduše konvoluce.

Definice. Nechť f je aritmetická funkce. Pak aritmetickou funkci $g = f * u$, tedy $g(n) = \sum_{d|n} f(d)$, nazveme *sumární funkcí* funkce f.

Cvičení. Najdi sumární funkci k N.

Tvrzení. (Obecné vlastnosti konvoluce) *Nechť f, g, h jsou libovolné aritmetické funkce. Pak platí:*

(i) $f * g = g * f$, *(komutativita)*
(ii) $(f * g) * h = f * (g * h)$. *(asociativita)*

Říkáme, že je konvoluce komutativní a asociativní, což jinými slovy znamená, že nezáleží na tom, v jakém pořadí konvoluci provádíme, ani jak uzávorkujeme výrazy typu $f * g * h * i * j * k$.

Důkaz.

(i) K důkazu komutativity je třeba si uvědomit, že

$$\sum_{d|n} f(d)\, g\Big(\frac{n}{d}\Big) = \sum_{a\cdot b=n} f(a)\, g(b) = \sum_{b\cdot a=n} f(b)\, g(a) = \sum_{d|n} f\Big(\frac{n}{d}\Big)\, g(d),$$

kde prostřední sumy probíhají přes všechny dvojice čísel (a, b), pro které platí $ab = n$.

(ii) Označme $A = g * h$ a upravme $f * A = f * (g * h)$. Máme

$$\begin{aligned}(f * A)(n) &= \sum_{a\cdot d=n} f(a)\, A(d) = \sum_{a\cdot d=n} f(a) \sum_{b\cdot c=d} g(b)\, h(c) \\ &= \sum_{a\cdot b\cdot c=n} f(a)\, g(b)\, h(c).\end{aligned}$$

Je vidět, že pokud analogicky upravujeme výraz $((f*g)*h)(n)$, dospějeme ke stejnému výsledku.

Ještě se seznámíme s funkcí, která „nechává jiné funkce na pokoji“.[48]

Definice. *Identita* je aritmetická funkce I definovaná jako

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n > 1. \end{cases}$$

Tvrzení. *Nechť f je aritmetická funkce. Pak platí $f * I = I * f = f$.*

Důkaz. Viz cvičení.

Cvičení. Tvrzení si dokaž.

Cvičení. Najdi sumární funkci k I.

Poznámka. V sekci o Möbiově funkci μ jsme si dokázali, že

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = I.$$

Pokud tento vztah přeložíme do řeči konvoluce, dostaneme, že $I = \mu * u$. Tento vztah částečně vysvětluje, proč je zrovna Möbiova funkce tak zajímavá. Je to totiž přesně ta funkce, jejíž sumární funkcí je I.

[48] Dokonce nechává na pokoji i sama sebe.

Nyní si můžeme ukázat, jaká síla se ukrývá v základních vlastnostech konvoluce.

Příklad. Dokážeme si novým a jednodušším způsobem, že

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d},$$

neboli $\varphi = \mu * N$.

Důkaz. Z prvního dílu víme, že $N = \varphi * u$. To znamená, že také $N * \mu = (\varphi * u) * \mu$. Pravá strana se díky asociativitě(!) rovná $\varphi * (u * \mu)$. Navíc víme, že $u * \mu = I$, takže $N * \mu = \varphi * I = \varphi$. Jak snadné (a bez sum).

Poznámka. Vzpomeňme si nyní, kolik jsme museli udělat úprav, než jsme dostali vztah (♡) v kapitole o sumách:

$$\sum_{d|n} \sum_{e|d} f(e) = \sum_{e|n} f(e)\, \tau\left(\frac{n}{e}\right).$$

Přitom si stačí uvědomit, že výraz na levé straně je sumární funkce ze sumární funkce z f. Tedy $(f * u) * u$. S využitím asociativity víme, že se to rovná $f * (u * u)$, ale $u * u$ není nic jiného než $\sum_{d|n} 1$, tedy počet dělitelů $\tau(n)$ čísla n. Tedy $(f * u) * u = f * \tau$, což je výraz na pravé straně.

Řešení druhé čokoládové úlohy – náročnější pasáž

Jako příklad využití nabytých znalostí si ukážeme, jak se řešila druhá čokoládová úloha k minulé sérii, jejíž řešení nám bohužel nikdo neposlal.

Úloha. V závislosti na prvočísle p urči v $\mathbb{Z}_p$ součet všech primitivních prvků modulo p.

Řešení. Vezměme si nějaký primitivní prvek g modulo p (z minulého dílu víme, že existuje). Hledaný součet pak je

$$\sum_{\substack{1 \le k \le p-1 \\ (k,p-1)=1}} g^k,$$

což vyplývá z tvrzení zmíněného ve druhém díle, že g^k je primitivní prvek, právě když čísla k a $p-1$ jsou nesoudělná. V kapitole o aritmetických funkcích jsme si dokázali tvrzení

$$\sum_{d|n} \mu(d) = I(n).$$

Díky tomu lze naši sumu takto upravit:

$$\sum_{\substack{1 \le k \le p-1 \\ (k,p-1)=1}} g^k = \sum_{k=1}^{p-1} g^k \cdot I((k,p-1)) = \sum_{k=1}^{p-1} g^k \sum_{d|(k,p-1)} \mu(d) = \sum_{k=1}^{p-1} g^k \sum_{\substack{d|k \\ d|p-1}} \mu(d).$$

Podařilo se nám získat vnořené sumy, které můžeme prohodit, tak hurá do toho. Ve vnější sumě budeme tedy sčítat přes $d \mid p-1$ a ve vnitřní přes taková k, která jsou násobkem d a pro která platí $k \le p-1$. Pokud napíšeme $k = dr$, můžeme místo přes k sčítat přes r od 1 do $\frac{p-1}{d}$.

$$\sum_{k=1}^{p-1} g^k \sum_{\substack{d|k \\ d|p-1}} \mu(d) = \sum_{k=1}^{p-1} \sum_{\substack{d|k \\ d|p-1}} g^k \cdot \mu(d) = \sum_{d|p-1} \sum_{r=1}^{(p-1)/d} g^{rd} \cdot \mu(d) = \sum_{d|p-1} \mu(d) \sum_{r=1}^{(p-1)/d} g^{rd}.$$

Nyní stačí zjistit, čemu se rovná vnitřní suma. Pro $d = p-1$ je kongruentní s 1 modulo p. Pro $d \mid p-1$, $d < p-1$ stačí jen sumu sečíst jako geometrickou řadu, čímž dostaneme

$$\sum_{r=1}^{(p-1)/d} g^{rd} = g^d \frac{(g^d)^{(p-1)/d} - 1}{g^d - 1}.$$

Z Malé Fermatovy věty plyne $p \mid g^{p-1} - 1 = (g^d)^{(p-1)/d} - 1$, ale přitom $p \nmid g^d - 1$ (protože g je primitivní prvek a $d < p-1$). Tyto členy nám tudíž modulo p vypadnou a zůstane jen $\mu(p-1)$, což je řešení úlohy.

Multiplikativita funkcí

Většina aritmetických funkcí, se kterými jsme se dosud v seriálu setkali a se kterými se zde ještě setkáme, má významnou[49] vlastnost, které se říká multiplikativita.

Definice. O aritmetické funkci f řekneme, že je *multiplikativní*, pokud pro každou dvojici a, b přirozených navzájem nesoudělných čísel platí $f(ab) = f(a)f(b)$. Funkce je *úplně multiplikativní*, pokud $f(ab) = f(a)f(b)$ platí pro každou dvojici přirozených čísel.

Proč je multiplikativita aritmetických funkcí z několika důvodů velmi příjemná? Z několika důvodů. Jedním z nich je to, že je funkce jednoznačně určená svými hodnotami v mocninách prvočísel. Pomocí matematické indukce totiž snadno dostaneme intuitivní vzoreček

$$f(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = f(p_1^{\alpha_1}) \cdots f(p_r^{\alpha_r}).$$

Když tedy potřebujeme spočítat hodnotu v čísle n, stačí jej rozložit na prvočísla, zjistit hodnoty v mocninách prvočísel a využít tohoto vzorečku. Obdobně, když chceme ukázat rovnost dvou multiplikativních funkcí, stačí dokázat, že se rovnají ve všech mocninách prvočísel.

Pro úplně multiplikativní funkce je situace podobná. Pro výpočet hodnoty n stačí znát hodnoty v jednotlivých prvočíslech z rozkladu (úplně multiplikativní funkce je totiž multiplikativní a navíc platí $f(p^k) = f(p)^k$). Aby se dvě úplně multiplikativní funkce rovnaly, stačí, aby měly stejné hodnoty v prvočíslech.

Cvičení. Uvědom si, že funkce I, u, N a μ jsou multiplikativní. Které z nich jsou multiplikativní úplně?

U dvou důležitých funkcí už jsme si multiplikativitu nenápadně dokázali – u Eulerovy funkce φ (již v prvním díle) a Legendreova symbolu L_p (ve druhém díle).

Cvičení. Dokaž, že pokud je f multiplikativní funkce, tak $f(1) = 1$.

Asi nikoho nepřekvapí, že jsou-li f a g multiplikativní funkce a h je definovaná jako $h(n) = f(n) \cdot g(n)$, tak je i h multiplikativní. Ale opravdové kouzlo a sílu multiplikativity poodkrývá následující tvrzení.

Tvrzení. (Konvoluce zachovává multiplikativitu) *Pokud jsou f a g multiplikativní, pak je multiplikativní i $f * g$.*

Důkaz. Nechť $h = f * g$ a m, n jsou dvě nesoudělná čísla. Pak

$$h(mn) = \sum_{d \mid mn} f(d)\, g\Big(\frac{mn}{d}\Big).$$

[49] Extrémně významnou.

Každý dělitel d čísla mn se dá napsat ve tvaru $d = ab$, kde $a \mid m$, $b \mid n$. Navíc platí $(a, b) = 1$, $(\frac{m}{a}, \frac{n}{b}) = 1$. Naopak každá taková dvojice a, b odpovídá právě jednomu děliteli d. Proto se rovnají sumy

$$\sum_{d \mid mn} f(d)\, g\Big(\frac{mn}{d}\Big) = \sum_{\substack{a \mid m \\ b \mid n}} f(ab)\, g\Big(\frac{mn}{ab}\Big).$$

Na pravé straně jsme získali dvojitou sumu, ze které vyrobíme součin sum, podobně jako jsme si to ukazovali v úvodní kapitole.

$$\begin{aligned} h(mn) &= \sum_{\substack{a \mid m \\ b \mid n}} f(ab)\, g\Big(\frac{mn}{ab}\Big) \\ &= \sum_{b \mid n} \sum_{a \mid m} \Big(f(a)\, f(b)\, g\Big(\frac{m}{a}\Big)\, g\Big(\frac{n}{b}\Big)\Big) \\ &= \sum_{b \mid n} \Big(f(b)\, g\Big(\frac{n}{b}\Big) \cdot \Big(\sum_{a \mid m} f(a)\, g\Big(\frac{m}{a}\Big)\Big)\Big) \\ &= \Big(\sum_{a \mid m} f(a)\, g\Big(\frac{m}{a}\Big)\Big)\Big(\sum_{b \mid n} f(b)\, g\Big(\frac{n}{b}\Big)\Big) \\ &= h(m)\, h(n). \end{aligned}$$

Získali jsme novou zbraň, jak o funkcích ukazovat, že jsou multiplikativní.

Tvrzení. *Funkce τ (počet dělitelů) a σ (součet dělitelů) jsou multiplikativní.*[50]

Důkaz. Tvrzení se samozřejmě dá dokázat z definice multiplikativity, ale vyžaduje to netriviální množství počítání a úprav. S tím, co jsme si dokázali o konvoluci, se tvrzení vzdá.

Stačí si uvědomit, že $\tau(n) = \sum_{d \mid n} 1$ je sumární funkce jednotky u, tedy $\tau = u * u$. Podobně $\sigma(n) = \sum_{d \mid n} d$ je sumární funkce „nudy“ N, tedy $\sigma = N * u$. Funkce u a N jsou multiplikativní a díky tomu, že konvoluce zachovává multiplikativitu, jsou i funkce τ a σ multiplikativní.

Poznámka. Nyní již snadno dokážeme, že pro $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ platí

$$\sigma(n) = \frac{p_1^{\alpha_1+1}}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1}}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1}}{p_r - 1}.$$

Cvičení. Dokaž si, že součet dělitelů závisí na počtu dělitelů takto:

$$\sigma(n) = \sum_{d \mid n} \tau(d)\, \varphi\Big(\frac{n}{d}\Big).$$

Cvičení. Uvědom si, že konvoluce nezachovává úplnou multiplikativitu.

Návod. $\tau = u * u$.

Z toho důvodu je multiplikativita důležitější a zajímavější než úplná multiplikativita.[51] To, že je funkce multiplikativní úplně, už je jen taková třešnička na dortu.[52] Na druhou stranu se tato vlastnost občas chová nadstandardně pěkně. Tak je tomu například u Dirichletových inverzí.

[50] Platí dokonce zobecněná věta: součet k-tých mocnin dělitelů čísla n, neboli $\sigma_k(n) = \sum_{d \mid n} d^k$, je multiplikativní.

[51] Přestože definice úplné multiplikativity se zdá být přirozenější.

[52] Nebo hřebíček do rakve.

Definice. Nechť f je aritmetická funkce taková, že $f(1) \neq 0$. Potom funkci g nazveme *Dirichletovou inverzí* k f, pokud $f * g = g * f = I$. Obvykle ji značíme f^{-1}.

Dá se ukázat, že pro každou funkci existuje právě jedna Dirichletova inverze, my to ale dělat nebudeme. Také se dá odvodit ne úplně pěkný rekurentní vztah pro hodnoty funkce f^{-1} v závislosti na funkci f. My díky Dirichletovým inverzím dostaneme zajímavou charakterizaci úplně multiplikativních funkcí. Drž si klobouk!

Tvrzení. *Nechť f je multiplikativní. Pak f je úplně multiplikativní, právě když*

$$f^{-1}(n) = \mu(n) f(n) \quad \text{pro každé přirozené } n.$$

Cvičení. (těžké) Zkus si tvrzení dokázat.

Návod. Pro jednu implikaci využij tvrzení $\sum_{d|n} \mu(d) = I(d)$. V druhé implikaci si uvědom, jak vypadá $\mu(p^k)$, a dokaž $f(p^\alpha) = f(p)^\alpha$.

Bonusy na závěr

Jednoduchou aplikací Dirichletovy konvoluce je následující překvapivé tvrzení, které říká, jak obrátit vztah „f je sumární funkce g“.

Tvrzení. (Möbiova inverzní formule) *Rovnosti*

$$f(n) = \sum_{d|n} g(d)$$

a

$$g(n) = \sum_{d|n} f(d)\, \mu\Big(\frac{n}{d}\Big)$$

jsou ekvivalentní.

Důkaz. Víme, že první rovnost znamená $f = g * u$. Vynásobením funkcí μ dostáváme $f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$, což je druhá rovnost. Když naopak tuto rovnost vynásobíme funkcí u, dostaneme opět první rovnost.

Vše, čím jsme se dosud v seriálu zabývali, bylo konečné (a tedy do jisté míry omezené). Pojďme se tedy na chvilku odpoutat od nudné reality a vrhněme se do nekonečného vesmíru plného nekonečných řad.

S nějakou nekonečnou řadou ses již pravděpodobně setkal(a). Například s krotkou řadou

$$1 + \frac{1}{2} + \cdots + \frac{1}{2^k} + \cdots = \sum_{k=0}^{\infty} 2^{-k},$$

která má konečný součet 2. Naproti tomu řada

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots$$

má součet nekonečno.[53]

[53] Vyšetřování, zda má nekonečná řada konečný součet, není snadné a my se jím nebudeme zabývat.

Obrovské využití v teorii čísel ale mají poněkud divočejší řady, kupříkladu řady tvaru

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{pro pevné } s > 1.$$

Dá se ukázat, že pro $s > 1$ má tato řada konečný součet, který označujeme $\zeta(s)$.[54] Platí například známý vztah

$$\zeta(2) = \frac{\pi^2}{6}.$$

Pořád je Ti to málo? Nám také. Pojďme si tyto řady ještě zobecnit.

Definice. Nechť a je aritmetická funkce. Pak

$$D(a, s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s},$$

nazveme *Dirichletovou řadou* funkce a.

Příkladem jsou tyto řady:

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)},$$
$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \zeta(s)^2,$$
$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s) \cdot \zeta(s-1).$$

Tvrzení. *Platí*

$$D(a * b, s) = D(a, s) \cdot D(b, s).$$

Náznak důkazu. Představ si, jak se postupně roznásobuje pravá strana. Pokud dáš k sobě členy, které mají ve jmenovateli n^s pro nějaké n, tak zjistíš, že v čitateli bude přesně

$$\sum_{d|n} a(d) \cdot b\Big(\frac{n}{d}\Big).$$

Tato úvaha opravdu funguje i pro nekonečné řady, jen je potřeba ještě trocha teorie a formalit, což překračuje rámec seriálu.

Cvičení. S pomocí tvrzení si dokaž tři předchozí identity.

Cvičení. (těžké) Nahlédni, že asi platí

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}},$$

kde v součinu násobíme přes všechna prvočísla.

Návod. Rozepiš si $\frac{1}{1-1/p^s}$ jako geometrickou řadu

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots.$$

[54] Jedná se o známou Riemannovu zeta funkci, o které hovoří nejslavnější nevyřešený matematický problém – Riemannova hypotéza.

Jak dostaneš na pravé straně $1/n^s$? Zkus si n rozložit na prvočísla.

Cvičení. (těžké) Dokaž, že

$$\frac{6}{\pi^2} < \frac{\varphi(n) \cdot \sigma(n)}{n^2} < 1.$$

Návod. Napiš si vzorečky pro $\varphi(n)$ a $\sigma(n)$, z obou vytkni n a využij předchozí cvičení.

Závěr

Pokud ses dočetl(a) až sem, chtěli bychom Ti pogratulovat a poděkovat za to, že jsi našemu seriálu udržel(a) přízeň. Pokud Tě téma zaujalo, v příštích komentářích najdeš seznam další literatury, mimo jiné zdroje, ze kterých jsme při psaní seriálu čerpali.

Dále bychom rádi poděkovali našemu jazykovému korektorovi Kubovi a TEXaři Olinovi za to, že po nás celý text důkladně pročítali, a za trpělivost, kterou s námi měli. Rovněž děkujeme i ostatním organizátorům, kteří pomohli výsledný text doladit.

Stručný dovětek k seriálu

Rádi bychom poděkovali řešitelům, kteří trpělivě pročetli všechny tři díly letošního seriálu. Snažili jsme se pokrýt témata, která nám přišla zajímavá, ale kvůli omezenému rozsahu jsme jich spoustu nestihli zahrnout. Pro ty, které tato témata zaujala, uvádíme zdroje, ze kterých jsme čerpali. Jde v nich najít inspiraci pro další studium teorie čísel a pro přípravu na olympiádu.

(1) Titu Andreescu, *104 Number Theory Problems* (povinná četba každého olympionika obsahující 104 příkladů s řešeními)
(2) Titu Andreescu, *Number Theory*
(3) Tom Apostol, *Introduction to Analytic Number Theory* (zde najdeš vše z třetího dílu seriálu a mnoho dalších zajímavých věcí)
(4) Hua Loo Keng, *Introduction to Number Theory* (všechno, co jsi chtěl vědět o teorii čísel, ale bál ses zeptat)
(5) PraSečí seriál z let 2008/2009, *http://mks.mff.cuni.cz/archive/archive.php* (zde najdeš Diofantické rovnice a RSA, témata, kterým jsme se vyhnuli)
(6) Třetí díl PraSečího seriálu o komplexních číslech z let 2010/2011 (Gaussova a Eisensteinova čísla)

Přejeme Ti hodně zdaru při dalším studiu.

Pepa Svoboda a Štěpán Šimsa