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 (?) 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.*

[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“.

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

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

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 $\sum_{d|6}\varphi(d) = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(6) = 1+1+2+2 = 6$.

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:

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

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:

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

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

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