15. Prvočísla

V této kapitole se podíváme na některé důležité vlastnosti prvočísel (a taky na pár zajímavých). Připomeňme definici.

Definice.
Nechť $a \in \mathbb{N}$, $a \neq 1$.
Řekneme, že je to **prvočíslo** (**prime**), jestliže jediná přirozená čísla, která jej dělí, jsou 1 a a.
Řekneme, že a je **složené číslo** (**composite number**), jestliže to není prvočíslo.

Připomínáme také, že 1 stojí mimo tuto klasifikaci.

Všimneme si, že číslo $a \in \mathbb{N}$ je složené, jestliže existuje $k \in \mathbb{N}$ takové, že $k \,|\, a$ a $1 < k < a$. Ještě jinak: Číslo a je složené, jestliže existují čísla $x, y \in \mathbb{N}$ taková, že $a = xy$ a $x < a$, $y < a$.

Příklad 15.a: Prvočísla byla zkoumána už od nepaměti a každý určitě nějaká zná. Mezi první stovkou přirozených čísel jsou tato prvočísla (je jich 25):

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Další je pak 101.
△

Naším prvním velkým cílem je dokázat větu o prvočíselném rozkladu, na kterou si musíme připravit půdu. Nejprve dokážeme tvrzení již citované v kapitole 2 jako fakt 2b.1:

Fakt 15.1.
Nechť $n \in \mathbb{N}$, $n \neq 1$. Pak existuje prvočíslo p takové, že $p \,|\, n$.

Důkaz (poučný)**:** Dokážeme to silnou indukcí na n pro $n \geq 2$.
(0) $n = 2$: Ano, existuje prvočíslo $p = 2$, které dělí $n = 2$.
(1) Nechť $n \in \mathbb{N}$, $n \geq 2$. Předpokládejme, že tvrzení platí pro všechna čísla $2, 3, \ldots, n$. Uvažujme číslo $n + 1$. Pokud je to prvočíslo, tak dáme $p = n + 1$ a jsme hotovi.
Pokud to prvočíslo není, pak musí existovat $k \in \mathbb{N}$ takové, že $k \,|\, (n+1)$ a $1 < k < n+1$. Pak je ale k z množiny $2, 3, \ldots, n$, tudíž existuje prvočíslo p takové, že $p \,|\, k$. Spolu s $k \,|\, (n + 1)$ to díky větě 2a.2 (iii) dává $p \,|\, (n + 1)$ a jsme hotovi.
□

Dokážeme si také lemma 2b.23.

Lemma 15.2.
Nechť $a_1, \ldots, a_m \in \mathbb{N}$ a p je prvočíslo. Jestliže $p \,|\, (a_1 a_2 \cdots a_m)$, pak existuje i takové, že $p \,|\, a_i$.

Důkaz (poučný)**:** Dokážeme to indukcí na m.
(0) Jestliže $m = 1$, tak předpokládáme $p \,|\, a_1$, z čehož plyne $i = 1$ a je to.
(1) Předpokládejme, že pro nějaké $m \geq 1$ tvrzení Lemma platí pro libovolné $a_1, \ldots, a_m \in \mathbb{Z}$. Mějme teď $a_1, \ldots, a_m, a_{m+1} \in \mathbb{Z}$ takové, že $p \,|\, (a_1 \cdots a_m a_{m+1})$. Protože jediní dělitelé p jsou p a 1, tak je i $\gcd(p, a_{m+1})$ buď p nebo 1. V prvním případě je p dělitelem a_{m+1}, tedy $p \,|\, a_{m+1}$ a jsme hotovi.
V opačném případě $\gcd(p, a_{m+1}) = 1$. Označme $b = a_1 \cdots a_m$, máme tedy situaci, kdy $p \,|\, (a_{m+1} b)$ a také $\gcd(p, a_{m+1}) = 1$, tudíž Lemma 2b.22 říká, že $p \,|\, b$, tedy $p \,|\, (a_1 \cdots a_m)$. Pak ale podle indukčního předpokladu musí existovat $i \in \{1, 2, \ldots, m\}$ takové, že $p \,|\, a_i$.
□

Nyní jsme připraveni na to hlavní.

Věta 15.3. (Fundamentální věta aritmetiky) (Fundamental theorem of arithmetics)
Nechť $n \in \mathbb{N}$. Pak existují prvočísla $p_1, p_2, \ldots, p_m$ a exponenty $k_1, k_2, \ldots, k_m \in \mathbb{N}_0$ takové, že

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} = \prod_{i=1}^{m} p_i^{k_i}.$$

Jestliže pro $n \geq 2$ přidáme podmínky $p_1 < p_2 < \ldots < p_m$ a $k_i > 0$, tak je tato dekompozice jednoznačně určena.

Důkaz (poučný, drsný)**:** 1) K důkazu existence dekompozice použijeme silný princip indukce na $n \in \mathbb{N}$.

(0) Jestliže $n = 1$, tak zvolíme libovolné prvočíslo, třeba $p = 13$, a $k_1 = 0$, dostáváme $1 = p^0$.

(1) Předpokládejme, že rozklad existuje pro všechna čísla $1, 2, \dots, n$. Uvažujme nyní číslo $n+1$.

Jestliže je to prvočíslo, pak zvolíme $p_1 = n+1$ a $k_1 = 1$, hotovo.

Jinak je to číslo složené, tedy existují $a, b \in \mathbb{N}$ takové, že $n+1 = a \cdot b$ a $a, b < n+1$. Podle indukčního předpokladu máme $a = \prod_{i=1}^{M} q_i^{k_i}$ a $b = \prod_{i=1}^{N} r_i^{k_i}$ pro nějaká prvočísla q_i, r_j. Pak $n+1 = \prod_{i=1}^{M} q_i^{K_i} \prod_{i=1}^{N} r_i^{L_i}$, takže je to opravdu součin mocnin prvočísel. Aby to odpovídalo formálně, provedeme přejmenování: Označíme $m = M + N$, $p_i = q_i$ a $k_i = K_i$ pro $i = 1, \dots, M$, dále $p_i = r_{i-M}$ a $k_i = L_{i-M}$ pro $i = M+1, \dots, m$ a dostáváme $n+1 = \prod_{i=1}^{m} p_i^{k_i}$. Důkaz je hotov.

2) Jednoznačnost: Nechť $n \in \mathbb{N}$, $n \geq 2$, a předpokládejme, že $n = \prod_{i=1}^{m} p_i^{k_i}$ a $n = \prod_{i=1}^{M} q_i^{l_i}$, kde $p_1 < \cdots < p_m$, $q_1 < \cdots < q_M$ a $k_i, l_j > 0$.

a) Nejprve ukážeme, že jde o stejná prvočísla, tedy $M = m$ a $p_i = q_i$ pro každé i. Položme $P = \{p_1, p_2, \dots, p_m\}$ a $Q = \{q_1, q_2, \dots, q_M\}$.

Vezměme $i \in \{1, \dots, m\}$. Protože je p_i prvočíslo a dělí n, musí podle Lemma 2b.24 dělit i jedno z čísel q_j. Jenže q_j má jen dělitele 1 a q_j a p_i coby prvočíslo není 1, proto $p_i = q_j$ neboli $p_i \in Q$. Dokázali jsme, že $P \subseteq Q$.

Obdobně ukážeme, že každé q_j leží v P, tedy $P = Q$. Z toho hned vyplývá, že $m = M$.

Ještě potřebujeme ukázat, že jde nejen o rovnost množin, ale že jsou ta čísla dokonce stejně seřazena, tedy že $p_i = q_i$. To by platit mělo, protože v obou množinách řadíme dle velikosti. Formálně to jde například indukcí, pro zpestření ukážeme argument pomocí Principu dobrého uspořádání, který je, jak víme, s Principem indukce ekvivalentní (věta 5a.8).

Předpokládejme sporem, že pro některé indexy i neplatí $p_i = q_i$. Protože tvoří neprázdnou podmnožinu $\mathbb{N}$, lze najít nejmenší takový index, říkejme mu k. Protože $p_k \in P = Q$, musí existovat j takové, že $p_k = q_j$. Protože ovšem všechna q_i pro $i < k$ jsou už zabrána, $q_i = p_i$, tak nutně $j > k$. Protože jsou čísla uspořádána dle velikosti, máme $q_k < q_j = p_k$.

Ale také $q_k \in Q = P$, proto obdobně musí existovat $n > J$ takové, že $q_k = p_J$ a dostáváme $p_k < q_k$. Máme zároveň nerovnosti $q_k < p_k$ a $q_k > p_k$, což je nemožné a spor je hotov.

b) Teď již víme, že oba rozklady zahrnují stejná prvočísla, tedy máme $n = \prod_{i=1}^{m} p_i^{k_i}$ a $n = \prod_{i=1}^{m} p_i^{l_i}$. Potřebujeme ukázat, že $k_i = l_i$ pro všechna $i = 1, \dots, m$. Vezměme nějaké takové i a ze symetrie situace předpokládejme, že $k_i \leq l_i$. Vydělíme oba rozklady číslem $p_i^{k_i}$ a dostaneme dva rozklady pro číslo $\frac{n}{p_i^{k_i}}$. V tom prvním se p_i vůbec nevyskytuje, v tom druhém je s exponentem $l_i - k_i \geq 0$. Ale podle části a) aplikované na tyto dva vydělené rozklady musí mít oba stejná provočísla, což nastane jedině v případě, že $l_i - k_i = 0$, tedy $k_i = l_i$.

Důkaz pro $n \geq 2$ je hotov.

□

Jednoznačnost vlastně platí i pro $n = 1$, ale je to trikem, proto jsme to do věty nezahrnuli. Jak se vůbec vyjádří 1 pomocí prvočísel, když máme podmínku $k_1 > 0$? Zvolíme $m = 0$ (prvočísla žádná nevybíráme), pak se v součinu $\prod_{i=1}^{0}$ násobí přes prázdnou množinu, což je podle definice právě 1. Jiná možnost není.

Vyjádření čísla n jako ve větě říkáme **prvočíselný rozklad**. V mnoha situacích máme rádi jednoznačnost z části b), ale někdy je pro změnu výhodné si dovolit přidat do rozkladu prvočísla s mocninou 0 (třeba $13 = 13 \cdot 3^0 = 13 \cdot 23^0 \cdot 33^0$), což například umožní sjednotit použitá prvočísla pro více čísel. Dobrým příkladem je následující aplikace prvočíselného rozkladu na dělitelnost.

Lemma 15.4.
Nechť $a \in \mathbb{N}$ je číslo s prvočíselným rozkladem $\prod_{i=1}^{m} p_i^{k_i}$, nechť $d \in \mathbb{N}$. Číslo d dělí a právě tehdy, když existují čísla $K_i \in \mathbb{N}_0$ splňující pro všechna i podmínku $0 \leq K_i \leq k_i$ taková, že $d = \prod_{i=1}^{m} p_i^{K_i}$.

Přeloženo do lidštiny, aby číslo d dělilo číslo a, nemůže mít v rozkladu prvočísla jiná, než jsou v a, a prvočíslo, které v d je, tam nemůže být vicekrát, než je v a.

Důkaz je variací na důkaz předchozí Věty. Pokud d dělí a, tak se pro každé p z rozkladu d ukáže, že musí být v rozkladu a, načež se vydělením p^k ukáže, že v čísle a musí být exponent alespoň tak velký jako u d. Pokud naopak nějaké prvočíslo p z rozkladu a chybí v daném rozkladu d, tak jej tam prostě přidáme s mocninou 0.

Odtud hned dostaneme následující tvrzení, které matematicky potvrdí oblíbený způsob hledání gcd a lcm pro menší čísla. Obě čísla napíšeme pomocí prvočíselného rozkladu, gcd se pak získá pomocí nejmenších mocnin a lcm pomocí největších mocnin u prvočísel (pokud nějaké prvočíslo z jednoho rozkladu chybí v druhém, dodáme jej tam s mocninou 0). Formálně řečeno:

Fakt 15.5.
Nechť $a, b \in \mathbb{N}$. Předpokládejme, že máme prvočísla $p_1 < \cdots < p_m$ a čísla $k_i, l_i \in \mathbb{N}_0$ taková, že $a = \prod_{i=1}^{m} p_i^{k_i}$ a $b = \prod_{i=1}^{m} p_i^{l_i}$. Pak $\gcd(a,b) = \prod_{i=1}^{m} p_i^{\min(k_i,l_i)}$ a $\operatorname{lcm}(a,b) = \prod_{i=1}^{m} p_i^{\max(k_i,l_i)}$.

Důkaz (z povinnosti)**:** 1) Označme $n = \prod_{i=1}^{m} p_i^{\min(k_i,l_i)}$. Protože má n ve svém rozkladu stejná prvočísla jako a i b a jejich exponenty splňují $\min(k_i,l_i) \le k_i$ a $\min(k_i,l_i) \le l_i$, podle předchozího Lemmatu $n \mid a$ a $n \mid b$. Je to tedy společný dělitel. Zbývá ukázat, že je největší.

Nechť d je nějaký společný dělitel a, b. Pak podle předchozího Lemmatu musí existovat čísla K_i taková, že $d = \prod_{i=1}^{m} p_i^{K_i}$ a přitom $K_i \le k_i$ a $K_i \le l_i$ pro všechna i. To pak ale znamená, že $K_i \le \min(k_i,l_i)$ pro všechna i, tudíž zase podle Lemmatu $d \mid n$. Takže n je opravdu největší společný dělitel a, b.

2) Důkaz vzorce pro $\operatorname{lcm}(a,b)$ je obdobný.

□

Z toho hned dostaneme zajímavý důkaz věty 2b.10. Pro všechna $k, l \in \mathbb{N}_0$ platí $\max(k,l) + \min(k,l) = k + l$ (zkuste si to rozmyslet, stačí rozebrat varianty podle toho, které z těchto čísel je větší), což dává

$$\begin{aligned}\gcd(a,b)\cdot\operatorname{lcm}(a,b) &= \prod_{i=1}^{m} p_i^{\min(k_i,l_i)} \cdot \prod_{i=1}^{m} p_i^{\max(k_i,l_i)} = \prod_{i=1}^{m} p_i^{\min(k_i,l_i)+\max(k_i,l_i)} \\ &= \prod_{i=1}^{m} p_i^{k_i+l_i} = \prod_{i=1}^{m} p_i^{k_i} \cdot \prod_{i=1}^{m} p_i^{l_i} = a \cdot b.\end{aligned}$$

Pro úplnost ukážeme několik příkladů na hledání gcd a lcm pomocí rozkladu.

Příklad 15.b: Uvažujme čísla 24 a 60. Jejich prvočíselné rozklady jsou $24 = 2^3 \cdot 3$ a $60 = 2^2 \cdot 3 \cdot 5$, takže máme $\gcd(24,60) = \gcd(2^3 \cdot 3 \cdot 5^0, 2^2 \cdot 3 \cdot 5) = 2^2 \cdot 3 = 12$ a $\operatorname{lcm}(24,60) = 2^3 \cdot 3 \cdot 5 = 120$.

Podobně $\gcd(2 \cdot 3^2 \cdot 5 \cdot 7^2, 3 \cdot 7^4 \cdot 13) = 3 \cdot 7^2$ a $\operatorname{lcm}(2 \cdot 3^2 \cdot 5 \cdot 7^2, 3 \cdot 7^4 \cdot 13) = 2 \cdot 3^2 \cdot 5 \cdot 7^4 \cdot 13$.

△

Tento postup je ovšem jako obecný přístup neperspektivní, protože prvočíselný rozklad daného čísla je jedním z nejnáročnějších výpočetních problémů.

15.6 Rozklad na prvočísla.

Hlavním krokem je umět najít k danému číslu n nějaké prvočíslo p, které jej dělí. Pokud toto umíme, tak aplikací téhož postupu na číslo n/p atd. získáme nakonec rozklad. Budeme se tedy soustředit na problém nalezení prvočíselného dělitele.

Jako první metoda se nabízí prostě zkoušet dělit rozkládané číslo n čísly $2, 3, 4, \ldots$. To asi čtenář zná. Vezme 45, zkusí vydělit dvojkou, nic, zkusí trojkou, zásah, máme $45 \div 3 = 15$. Pokračujeme s patnáctkou, zkusíme zase trojku, bingo, $15 \div 3 = 5$, rozklad hotov, $45 = 3^2 \cdot 5$.

U malých čísel toto může fungovat efektivně, zejména když si vzpomeneme na rozličná kritéria dělitelnosti, viz například cvičení 2a.10 a 3a.13.

Pro větší čísla je tento přístup totální katastrofa. Dobrá zpráva je, že nemusíme zkoušet dělit všemi čísly $1, 2, \ldots, n$.

Fakt 15.7.
Jestliže je n složené číslo, pak existuje jeho prvočíselný dělitel menší či roven číslu $\sqrt{n}$.

Důkaz: Předpokládejme, že $n = ab$ a $a, b > 1$. Tvrdíme, že buď $a \le \sqrt{n}$ nebo $b \le \sqrt{n}$. V opačném případě bychom totiž měli $ab > \sqrt{n} \cdot \sqrt{n} = n$.

Takže předpokládejme, že třeba $a \le \sqrt{n}$. Vezměme libovolné prvočíslo p z prvočíselného rozkladu a, to pak splňuje $p \le a \le \sqrt{n}$ a dělí n.

□

To znamená, že pokud dané číslo n nedělí nic až po $\sqrt{n}$, tak už víme, že je to prvočíslo. Podobně lze ukázat, že pokud nějaké číslo n vzniklo jako součin tří prvočísel, pak to nejmenší z nich nesmí být větší než $\sqrt[3]{n}$, a tak dále.

Náročnost našeho naivního algoritmu (kterému se také říká „direct search algorithm“ či „trial division“) je tedy $\sqrt{n}$ kroků, když do toho započítáme náročnost dělení, budeme na tom ještě hůř. V praxi se často velikost čísla soudí podle počtu cifer (ve dvojkové soustavě) $m = \log_2(n)$, pak $n = 2^m$ a lze říci, že v nejhorším případě potřebujeme pro m-ciferné číslo použít $2^{m/2}$ testů, což je hodně.

Při postupném dělení čísly $2, 3, 4, \ldots$ by pomohlo, kdybychom měli tabulku prvočísel, protože pak bychom nemuseli dělit n všemi čísly až po $\sqrt{n}$, stačilo by brát jen prvočísla. Těch je relativně málo, například jsme viděli, že je jen 25 prvočísel menších než 100. To znamená, že kdybychom chtěli udělat rozklad čísla 10003, tak bychom nemuseli zkoušet dělit všemi čísly až po $\sqrt{10001} \sim 100$, ale jen oněmi 25 prvočísly.

Takovou tabulku naštěstí nemusíme tvořit postupným testováním čísel, existuje metoda, která to zvládá relativně efektivně.

Příklad 15.c: Pokud potřebujeme identifikovat všechna prvočísla v rozmezí 1 až n, pak můžeme s úspěchem použít metodu zvanou **Eratosthenovo síto** (sieve of Eratosthenes). Funguje to následovně.

Nejprve si všechna čísla od 2 do n napíšeme na papír, třeba do tabulky nebo za sebe, to je jedno:

$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, \ldots$

Začneme s $a = 2$. Je to prvočíslo, tak jej označíme a pak ze seznamu vyškrtneme všechny jeho násobky:

$\boxed{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{64}, 17, \cancel{18}, \ldots$

Podíváme se do seznamu a najdeme první další nevyškrtnuté a neoznačené číslo, je to $a = 3$. Musí to být prvočíslo, tak jej označíme a pak ze seznamu vyškrtneme všechny jeho násobky, které tam ještě zbyly:

$\boxed{2}, \boxed{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{64}, 17, \cancel{18}, \ldots$

Podíváme se do seznamu a najdeme první další neoznačené číslo, tedy $a = 5$. Označíme jej coby prvočíslo a pak ze seznamu vyškrtneme atd.: $\boxed{2}, \boxed{3}, \cancel{4}, \boxed{5}, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{64}, 17, \cancel{18}, \ldots$

Takto pokračujeme, dokud nedojdeme k $\sqrt{n}$. Všimněte si, že při vyškrtávní čísel nemusíme dělit, jen sčítáme (3, $3+3$, $6+3$, $9+3$, …), což je mnohem lepší, a ještě hezčí je, že k vyřazení každého neprvočísla jsme potřebovali jen jednu operaci. Je to tedy velmi efektivní metoda.

△

Metoda je to sice pěkná, ale my většinou potřebujeme faktorizovat či testovat na prvočíselnost čísla řádu třeba 10^{200} a vyrábět si kvůli tomu tak velké monstrózní síto by bylo pořád nepředstavitelně drahé. Tak či onak, pokud zkoušíme najít rozklad n-ciferného (n-bitového) čísla pomocí podobných přímočarých metod, tak se v zásadě díváme na náročnost okolo $e^{n/2}$ operací. Nic lepšího zatím nebylo vymyšleno, takže jak jsme viděli v kapitole kapitole 3a (příklad 3a.l), nejpoužívanější veřejné šifrování na Internetu je založeno na tom, že faktorizovat velké číslo by i dnešním superpočítačům zabralo desítky až stovky let.

Když s faktorizací nepomohla matematika, zkouší se na to jít přes hardware, jmenovitě zrovna lámání šifer skrz faktorizaci je velmi silnou motivací pro rozvoj kvantových počítačů.

U testování prvočíselnosti je situace přece jen o něco lepší a existují existují metody na urychlení. Což je dobře, protože moderní aplikace potřebují velká prvočísla. Věnujeme tomu samostatnou poznámku.

15.8 Poznámka o testování prvočíselnosti: Cílem je najít nějaké velké prvočíslo, třeba o 200 cifrách. Neumíme to přímo, postupuje se tedy metodou pokus-omyl, kdy se generují čísla a testují. Bohužel, potvrzení prvočíselnosti je opět docela náročný problém, ale většina čísel, která zkusíme, prvočísla nebudou, takže je dobře, že na vyřazování nevhodných kandidátů existují docela efektivní metody.

Ukážeme si jednu, která vychází z nám známé malé Fermatovy věty. Její obměna zní takto:

• Jestliže jsou čísla $a \in \mathbb{Z}$ a n nesoudělná a neplatí $a^{n-1} \equiv 1 \pmod{n}$, pak už n nemůže být prvočíslo.

Toto může sloužit jako test prvočíselnosti. Vezměme libovolné liché $n > 2$, chceme vědět, zda je to prvočíslo. Použijeme $a = 2$, protože pro liché číslo určitě $\gcd(2, n) = 1$. Jestliže $2^{n-1} \not\equiv 1 \pmod{n}$, pak podle malé Fermatovy věty n určitě není prvočíslo. Tento výpočet lze provést vcelku rychle, je to tedy efektivní „vylučovač“.

Bohužel, malá Fermatova věta je jen implikace. Takže pokud by platilo $2^{n-1} \equiv 1 \pmod{n}$, pak n prvočíslo být může, ale nemusí. Jsou zvláštní čísla, která $2^{n-1} \equiv 1 \pmod{n}$ splňují, ale jsou složená, říkáme jim **pseudoprvočísla**. Dobrá zpráva je, že pseudoprvočísel je velice málo, například mezi prvními 10^{10} přirozenými čísly je cca 450,000,000 prvočísel, ale jen cca 15,000 pseudoprvočísel. To znamená, že tento test je vysoce účinný při vyřazování čísel, která prvočísly nejsou, a pokud už nějaké n tímto testem projde, tak je vysoká pravděpodobnost, že jsme opravdu ulovili prvočíslo, a vyplatí se investovat další námahu na skutečné potvrzení této skutečnosti.

Tato myšlenka se dá samozřejmě rozvést dále. Řekneme, že n je pseudoprvočíslo vzhledem k základu a, jestliže $a^{n-1} \equiv 1 \pmod{n}$. Takže pokud nějaké pseudoprvočíslo přežije první test, zvolíme nějaké nesoudělné a, například další prvočíslo $a = 3$, a zkusíme, zda neplatí $a^{n-1} \equiv 1 \pmod{n}$. To při troše štěstí zase vyřadí neprvočíslo.

Řekneme, že n je Carmichaelovské číslo, jestliže $a^{n-1} \equiv 1 \pmod{n}$ pro všechna $a \in \mathbb{N}$ s $\gcd(a,n) = 1$. Např. 561 je takové číslo. Carmichaelovských čísel je sice nekonečně mnoho, ale zase hrozně málo, čili když začneme s n a protestujeme jej pro hodně a, tak v případě úspěchu už je skoro jisté, že n je prvočíslo.

Je to dobrá strategie pro hledání velkých prvočísel, například pro kódování RSA. Dělá se to tak, že si prostě zvolíme nějaké vhodně dlouhé číslo (liché a nekončící pětkou, samozřejmě). Testovat přímo dělením, zda je to prvočíslo, by trvalo strašně dlouho (mluvíme zde o desítkách let na těch nejvýkonnějších počítačích). Místo toho jej rychle proženeme testy popsanými výše a ono asi vypadne jako složené číslo. Tak zkusíme jiné velké číslo (třeba přičteme 2 k tomu neúspěšnému) a jedeme znovu. Nakonec nějaké číslo těmi testy projde, pak je téměř jisté, že je to prvočíslo. Tak prostě z takového čísla zkusíme RSA kódování udělat, zkusmo něco zakódujeme a rozkódujeme a pokud to vyjde, tak jsme našli, co jsme potřebovali.

△

V poznámce jste jistě zaznamenali zajímavé postřehy o četnosti prvočísel a další zajímavé nápady, které pocházejí z teorie čísel. Několik si jich pro zajímavost představíme a začneme jednoduchou odpovědí na otázku, kolik je prvočísel.

Věta 15.9.
Pročísel je nekonečně mnoho.

Důkaz (poučný)**:** Ukážeme si klasický Euklidův důkaz, takže jdeme až ke starým Řekům, cca 300 př.n.l. Dělá se sporem, předpokládáme, že existuje jen konečně mnoho prvočísel $p_1, p_2, \ldots, p_m$.

Vezměme číslo $a = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$. Podle Faktu 2b.1 existuje prvočíslo p takové, že dělí a. Podle předpokladu to ale musí být jedno z těch p_i, proto také p dělí ten součin $p_1 \cdot p_2 \cdot \ldots \cdot p_m$. Máme $p \mid a$, $p \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_m)$, proto nutně p dělí jejich rozdíl, viz Fakt 2a.4. Takže $p \mid 1$ a to je spor, neboť $p \geq 2$.

□

Zajímavé je, že ve skutečnosti jsou čísla typu $a = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$ docela často prvočísla, třeba $2 \cdot 3 + 1 = 7$, $2 \cdot 3 \cdot 5 + 1 = 31$ nebo $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. Známá čísla tohoto typu se používají pro testování kvality nových superpočítačů.

Víme, že prvočísel je nekonečně mnoho, což samozřejmě už po staletí nedá lidem spát a snaží se najít co největší. Je to věc prestiže, výsledky jsou kombinací brutální výpočetní síly a vysoce sofistikovaných matematických metod (viz třeba příklad 3a.m). Má to ale i praktické důsledky, třeba pro bezpečnost šifrování. Posledních 300 let byla největší nalezená prvočísla ve tvaru $2^p - 1$ pro prvočíslo p. Samozřejmě ne každé takové číslo je prvočíslem, to by bylo moc snadné, například $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ jsou prvočísla, ale $2^{11} - 1 = 2047 = 23 \cdot 89$. Prvočíslům ve tvaru $2^p - 1$ se říká Mersennova prvočísla a jsou populární díky tomu, že výrazy typu $2^p - 1$ se relativně dobře testují na prvočíselnost.

Sice jsme odpověděli na otázku, kolik je prvočísel, ale to byla snadná odpověď. Lepší otázka je, kolik jich je relativně, třeba takto: Označme pro $n \in \mathbb{N}$ jako $\pi(n)$ počet prvočísel p splňujících $p \leq n$ (seznámek $2, 3, 5, 7$ ukazuje, že $\pi(10) = 4$, už třeba víme, že $\pi(100) = 25$). Jak rychle tato funkce roste? Hluboké výsledky říkají, že pro velká n je $\pi(n)$ přibližně rovno $\frac{n}{\ln(n)}$. (Má to dost komplikované důkazy, jako hypotéza se to objevilo v 19. století, první důkaz 1896.) Znamená to tedy, že relativní hustota prvočísel mezi prvními n čísly je přibližně $\frac{1}{\ln(n)}$, takže se zvětšujícím se n klesá, tedy prvočísel je čím dál relativně méně.

Tento výsledek se dá interpretovat různými způsoby, třeba takto: Jestliže si mezi čísly 1 až n zvolíte náhodně jedno, tak je pravděpodobnost $\frac{1}{\ln(n)}$, že to bude prvočíslo. Ještě jinak: Tato pravděpodobnost je nepřímo úměrná počtu cifer čísla n (čím víc cifer, tím menší pravděpodobnost). Dá se také říct, že průměrná vzdálenost mezi prvočísly okolo čísla n je zhruba $\ln(n)$.

Přesto je prvočísel v jistém smyslu dost. Připomeňme si známou divergentní harmonickou řadu $\sum_{k=1}^{\infty} \frac{1}{k} = \infty$. Když z té řady vynecháme relativně dost členů (neboli necháme si jich relativně málo), tak začne konvergovat. Pokud například označíme jako M množinu všech druhých mocnin přirozených čísel, tak již $\sum_{k \in M} \frac{1}{k}$ konverguje. Když si ale vezmeme množinu P všech prvočísel, pak $\sum_{p \in P} \frac{1}{p} = \infty$ (Eulerův výsledek). Takže jich zase tak málo není.

Víme, že prvočísla nám dají všechna přirozená čísla prostřednictvím násobení. Zajímavá otázka je, jestli je jich dost na to, aby nám dala přirozená čísla prostřednictvím sčítání. K tomu se váže Goldbachova hypotéza (1742), která říká: Každé liché $n \in \mathbb{N}$ větší než 5 je součtem tří prvočísel. Tato hypotéza má i ekvivalentní vyjádření: Každé sudé $n \in \mathbb{N}$ větší než 2 je součtem dvou prvočísel. Neví se, zda toto platí, zatím je dokázáno, že každé sudé $n \in \mathbb{N}$ větší než 2 je součtem nejvýše 6 prvočísel, což je od cíle dost daleko.

Hodně úsilí šlo do odhalování různých pravidelností ve výskytu prvočísel. Hned na začátku je třeba říct, že celkově v jejich výskytu žádná pravidelnost není. Mohou se ale vyskytovat zajímavé pravidelnosti dočasné, lokální. Několik výsledků:

• Kdykoliv zvolíme a, b nesoudělné, pak v aritmetické posloupnosti $\{an+b\}$ najdeme nekonečně mnoho prvočísel (Dirichletova věta).

• V opačném směru je tu hypotéza: Pro libovolné m existuje $a, d \in \mathbb{N}$ takové, že $a, a+d, a+2d, \dots, a+md$ jsou prvočísla. Krátce řečeno, lze vytvořit konečné aritmetické posloupnosti libovolných délek, které se skládají z prvočísel. Zdá se, že je to pravda, v roce 2004 byl prezentován důkaz, ale byl tak hrozný, že ještě v době psaní tohoto skripta nebyl pořádně prověřen.

Určitě ale víme, že nejde najít nekonečnou aritmetickou posloupnost z prvočísel. Kdyby totiž existovala posloupnost ve tvaru $a_k = dk + b$ generující prvočísla, pak by pro velká n bylo poměrné zastoupení prvočísel v $\mathbb{N}$ přinejmenším $\frac{1}{d}$ neboli platilo by $\pi(n) \geq \frac{1}{d}n$, což je ale ve sporu s $\pi(n) \sim \frac{n}{\pi(n)}$.

• Pro libovolné $n \in \mathbb{N}$ existuje mezi prvočísly někde mezera délky alespoň n. Ekvivalentně, existuje n po sobě jdoucích čísel takových, že jsou složená. Toto je vlastně snadné, začne se číslem $(n+1)! + 2$ a skončíme $(n+1)! + (n+1)$. Pro každé $2 \leq k \leq n+1$ totiž platí, že k dělí $(n+1)!$, proto jsou pak čísla $(n+1)! + k$ dělitelná k a tedy složená.

• Hodně by pomohlo najít funkci takovou, aby $f(n)$ bylo prvočíslo pro všechna $n \in \mathbb{N}$. Umožnilo by to snadné generování libovolně velkých prvočísel. Zatím ji nikdo nenašel, i když se zajímavé věci našly, například funkce $f(n) = n^2 - n + 41$, která dává prvočísla pro $n = 1, \dots, 40$, ale pak už ne, $f(41) = 41^2$. Jenže takovéto polynomy jsou stejně slepá ulička, pro každý polynom p s celočíselnými koeficienty existuje $y \in \mathbb{N}$ takové, že $p(y)$ je složené.

I to je vlastně snadné. Nechť $p(x) = a_n x^n + \cdots + a_0$. Jestliže $a_0 \neq 0$, pak $f(|a_0|) = a_0(\pm a_n a_0^{n-1} \pm \cdots \pm 1)$ a máme číslo složené, v případě $a_0 = 0$ pak $p(x) = x(a_n x^{n-1} + \cdots + 1)$ a stačí dosadit jakékoliv $a \in \mathbb{N}$.

• Není známo, zda existuje nekonečně mnoho prvočísel typu $n^2 + 1$. Zatím je známo, že pro nekonečně mnoho n je $n^2 + 1$ prvočíslo nebo součin dvou prvočísel.

• Není známo, zda existuje nekonečně mnoho dvojic p, $p+2$, kde obě jsou prvočísla (známe třeba dvojice 3 a 5, 11 a 13, 17 a 19 atd).

Takto by se dalo pokračovat ještě dlouho, ale jako nahlédnutí do teorie čísel to stačí.

Cvičení

Cvičení 15.1 (rutinní)**:** Najděte faktorizaci následujících čísel: (i) 156; (ii) 165; (iii) 504.

Cvičení 15.2: Dokažte/vyvraťte: Existují tři po sobě jdoucí lichá čísla, která jsou prvočísla, tj. p, $p+2$, $p+4$.

Cvičení 15.3 (drsné)**:** Najděte nějaký předpis používající prvočísla a prvočíselné rozklady pro následující posloupnosti:
(i) $0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, \dots$
(ii) $1, 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, \dots$
(iii) $1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 5, \dots$
(iv) $1, 2, 3, 3, 5, 5, 7, 7, 7, 7, 11, 11, 13, 13, \dots$
(v) $1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870, \dots$

Cvičení 15.4 (poučné)**:** Nechť $a_1, a_2, \dots, a_n \in \mathbb{N}$. Dokažte, že když jsou a_i po dvou nesoudělná, pak $\operatorname{lcm}(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdots a_n$.

Řešení:
15.1: (i): $156 = 2^2 \cdot 3 \cdot 13$;
(ii): $165 = 3 \cdot 5 \cdot 11$;
(iii): $504 = 2^3 \cdot 3^2 \cdot 7$.
15.2: $3, 5, 7$.
15.3: Předpisy pro a_n: (i): n prvočíslo ano/ne; (ii): a_n je nejmenší prvočíselný dělitel n; (iii): počet kladných dělitelů; (iv): a_n je největší prvočíslo $\leq n$; (v): součin prvních $n-1$ prvočísel.
15.4: Označme $a = a_1 \cdot a_2 \cdots a_n$. Protože $a_i \,|\, a$, pak také $\operatorname{lcm}(a_1, a_2, \dots, a_n) \,|\, a$. Potřebujeme opačný směr.
Nechť $a = \prod_j p_j^{k_j}$ je prvočíselný rozklad. Zvolme nějaké j. Pak podle Lemma 2b.24 musí existovat i takové, že $p_j \mid a_i$. Protože jsou všechna a_k po dvou nesoudělná, tak už žádné jiné a_k nemůže mít p_j jako dělitele, tudíž dokonce $p_j^{k_j} \mid a_i$, tedy i $p_j^{k_j} \mid \operatorname{lcm}(a_1, a_2, \dots, a_n)$. Ukázali jsme, že všechny prvočíslé faktory $p_j^{k_j}$ z rozkladu a dělí $\operatorname{lcm}(a_1, a_2, \dots, a_n)$, tedy a dělí $\operatorname{lcm}(a_1, a_2, \dots, a_n)$.