# 7 Teorie čísel

Nejběžnější asymetrické šifry a podpisy jsou založené na teorii čísel. V této kapitole si pro to připravíme půdu a potřebné části teorie čísel vybudujeme. Budeme předpokládat, že čtenář už zná základy obecné algebry (grupy, okruhy, tělesa). U tvrzení, jejichž důkaz je netriviální a podle našeho mínění není potřebný pro pochopení kryptografických souvislostí, je důkaz uveden v samostatném oddílu označeném hvězdičkou.

Nejprve připomeneme základní značení:

- Čísly budeme v této kapitole obvykle myslet čísla celá. Pokud nebude hrozit nedorozumění, budeme jim říkat prostě *čísla.*
- $p$ a $q$ budou typicky značit *prvočísla.*
- $x \setminus y$ značí, že číslo $x$ je *dělitelem* čísla $y$, tedy že existuje $d$ takové, že $y = xd$.
- $\gcd(x, y)$ je *největší společný dělitel* $x$ a $y$.[1] Případu $x = y = 0$ se chceme vyhnout, protože tam je každé číslo společným dělitelem.
- $x \perp y$ značí, že $x$ a $y$ jsou *nesoudělná,* tedy $\gcd(x, y) = 1$.
- $x \equiv_n y$ je *kongruence modulo* $n > 0$, která znamená, že $x$ a $y$ dávají stejný zbytek modulo $n$. To je totéž, jako že $n \setminus (x - y)$. Často se také píše

$$x \equiv y \pmod{n}.$$

  Pokud bude z kontextu jasné, modulo čím počítáme, budeme psát prostě $x \equiv y$.

## 7.1 Základní aritmetické algoritmy

Většinou nás bude zajímat nejen to, jak k danému výsledku dojít, ale také jak rychle to dokážeme. Zopakujme si proto složitost základních operací s čísly vzhledem k jejich délce $b$ v bitech:

- *Sčítání a odčítání* zvládneme v čase $\mathcal{O}(b)$ algoritmem „sčítání pod sebou“ ze základní školy.
- *Násobení* algoritmem ze základní školy trvá $\mathcal{O}(b^2)$, existují i efektivnější algoritmy – Karacubův-Ofmanův v čase $\mathcal{O}(b^{1.59})$, použitím FFT dokonce v $\mathcal{O}(b)$. Nám bude stačit $\mathcal{O}(b^2)$.

[1] Zkratka podle anglického *greatest common divisor.*

- *Dělení se zbytkem* buď algoritmem ze základní školy v čase $\mathcal{O}(b^2)$, nebo Newtonovou iterací – pokud násobíme v čase $\mathcal{O}(b^{1+\varepsilon})$, trvá dělení také $\mathcal{O}(b^{1+\varepsilon})$; pokud násobíme v lineárním čase, trvá dělení $\mathcal{O}(b \log b)$. Každopádně nám bude stačit $\mathcal{O}(b^2)$.
- *Modulární umocňování* $x^y \bmod n$ počítáme rekurzivním algoritmem: pro $y$ sudé počítáme $(x^{y/2})^2$, pro $y$ liché $(x^{(y-1)/2})^2 \cdot x$, vše modulo $n$. Kroků rekurze je $\log n \leq b$, každý nás stojí $\mathcal{O}(1)$ aritmetických operací v čase $\mathcal{O}(b^2)$. Celkem tedy $\mathcal{O}(b^3)$.

**Euklidův algoritmus**

K výpočtu $\gcd(x, y)$ můžeme používat Euklidův algoritmus. Jeho základní varianta opakovaně odečítá menší číslo od většího, než se vyrovnají. Vylepšená varianta místo opakovaného odčítání počítá zbytek po dělení.

Základní varianta je pomalá (představte si chování pro $x = 10^9$, $y = 1$). Vylepšená varianta doběhne v $\mathcal{O}(\log(\min(x, y))) \subseteq \mathcal{O}(b)$ krocích, důkaz najdete například v Průvodci labyrintem algoritmů. Jeden krok přitom trvá $\mathcal{O}(b^2)$, takže celý algoritmus $\mathcal{O}(b^3)$. Pečlivější analýzou, která bude brát v úvahu, jak se během výpočtu vyvíjí velikosti čísel, můžeme získat odhad $\mathcal{O}(b^2)$.

Často se nám bude hodit *rozšířený Euklidův algoritmus,* který získáme následovně.

**Lemma:** Všechny mezivýsledky v Euklidově algoritmu jsou lineární kombinace vstupů $x$ a $y$. Ke každému mezivýsledku můžeme během výpočtu udržovat i koeficienty příslušné lineární kombinace, aniž bychom algoritmus asymptoticky zpomalili.

*Důkaz:* Pro základní variantu algoritmu to snadno dokážeme indukcí podle počtu kroků. Označíme $x'$ a $y'$ pracovní proměnné algoritmu. Na začátku je $x' = 1 \cdot x + 0 \cdot y$ a $y' = 0 \cdot x + 1 \cdot y$. Kdykoliv odečteme od $x' = \alpha x + \beta y$ proměnnou $y' = \gamma x + \delta y$, získáme $x' - y' = (\alpha - \gamma)x + (\beta - \delta)y$.

Jeden krok vylepšené varianty je zkratkou za více kroků varianty základní. Počítáme-li $x' \bmod y'$ pro $x' = \alpha x + \beta y$ a $y' = \gamma x + \delta y$, provádíme vlastně $d = \lfloor x'/y' \rfloor$ odečtení $y'$ od $x'$. Výsledek tedy bude $(\alpha - d\gamma)x + (\beta - d\delta)y$. □

Finální výsledek $\gcd(x, y)$ je ovšem jedním z mezivýsledků, takže dostáváme:

**Důsledek:** Rozšířený Euklidův algoritmus v čase $\mathcal{O}(b^2)$ spočítá $\gcd(x, y)$ a čísla $\alpha$ a $\beta$ taková, že $\gcd(x, y) = \alpha x + \beta y$. Těmto číslům se říká *Bèzoutovy koeficienty.*

## 7.2 Algebraické minimum

V tomto oddílu připomeneme základní pojmy z obecné algebry.

**Definice:** *Algebra* je tvořena nosnou množinou spolu s nějakými *operacemi. k*-ární operací nazýváme funkci, která $k$-ticím prvků z nosné množiny přiřazuje opět prvky nosné množiny. Nulární operace jsou *konstanty.*

**Definice:** *Homomorfismus* mezi algebrami stejného typu (s odpovídajícími si operacemi) je zobrazení mezi jejich nosnými množinami, které je kompatibilní s operacemi. Tedy $f(a+b) = f(a)+f(b)$ apod. Pokud je zobrazení navíc bijektivní, mluvíme o *izomorfismu.*

**Grupy**

**Definice:**

- *Grupa* je algebra $(G, \cdot, \mathbf{1}, {}^{-1})$, kde $G$ je nosná množina, $\cdot$ binární operace nad $G$, $\mathbf{1}$ konstanta, ${}^{-1}$ unární operace nad $G$ a platí následující axiomy:
  1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(asociativita)*
  2. $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ *(prvek* $\mathbf{1}$ *je jednotkový)*
  3. $a \cdot (a^{-1}) = (a^1 \cdot a) = \mathbf{1}$ *(*$a^{-1}$ *je prvek inverzní k* $a$*)*
- V *komutativní grupě* navíc platí $a \cdot b = b \cdot a$ *(komutativita).*
- $(H, \cdot, \mathbf{1}, {}^{-1})$ je *podgrupou* grupy $(G, \cdot, \mathbf{1}, {}^{-1})$ právě tehdy, když $H \subseteq G$ a množina $H$ je uzavřená na všechny tři operace (tj. provedeme-li operaci s prvky z $H$, musí opět vyjít prvek z $H$). $(H, \cdot, \mathbf{1}, {}^{-1})$ je pak také grupou.
- *Řád grupy* říkáme počtu prvků její nosné množiny. Značíme ho $|G|$.
- Pro prvek $a$ a číslo $n \in \mathbb{Z}$ dále definujeme *mocninu* takto: $a^0 = \mathbf{1}$, $a^{n+1} = a^n \cdot a$, $a^{n-1} = a^n \cdot a^{-1}$. Platí obvyklé vlastnosti mocniny: $a^{m+n} = a^m \cdot a^n$, $a^{mn} = (a^m)^n$, $a^{-n} = (a^n)^{-1}$ apod.
- Prvku $g$ říkáme *generátor* grupy, jestliže se každý prvek nosné množiny dá vyjádřit jako nějaká mocnina $g$. Grupa je *cyklická,* pokud má generátor.
- Pro libovolný prvek $a$ je $\{a^n \mid n \in \mathbb{Z}\}$ cyklická podgrupa. *Řád prvku* $a$ definujeme jako řád této podgrupy.

**Příklady:**

- $(\mathbb{Z}, +, 0, -)$ (celá čísla spolu s obvyklým sčítáním, nulou a změnou znaménka) tvoří cyklickou grupu (generátory jsou 1 a $-1$).
- $(2\mathbb{Z}, +, 0, -)$ (sudá celá čísla spolu s obvyklým sčítáním, nulou a změnou znaménka) tvoří podgrupu předchozí grupy, která je také cyklická (rozmyslete si, že každá podgrupa cyklické grupy je cyklická).

- $(\mathbb{Z}_n, +_{\bmod n}, 0, -)$ (čísla 0, 1, …, $n-1$ spolu se sčítáním modulo $n$, nulou a změnou znaménka) tvoří cyklickou grupu (generátorem je třeba 1; které jsou další?).
- $(\mathbb{Q}, \cdot, 1, ?)$ (racionální čísla s násobením) nemohou tvořit grupu, jelikož k nule neexistuje inverzní prvek.
- $(\mathbb{Q} - \{0\}, \cdot, 1, 1/x)$ (racionální čísla bez nuly s násobením a převrácenou hodnotou) grupu tvoří, není cyklická.
- $(\mathbb{Z}_n - \{0\}, \cdot_{\bmod n}, ?)$ (čísla $1 \ldots n-1$ s násobením modulo $n$) pro některá $n$ grupou je, pro jiná není, protože obecně nemusí existovat inverzní prvky. Za chvíli prozkoumáme, jak to přesně je.

**Pozorování:** Konečná cyklická grupa řádu $n$ je vždy izomorfní se $\mathbb{Z}_n$, nekonečná je izomorfní se $\mathbb{Z}$. Je-li $g$ generátor, funkce $x \mapsto g^x$ je izomorfismem.

**Věta (Lagrangeova):** Pokud má konečná grupa $G$ nějakou podgrupu $H$, platí $|H| \setminus |G|$.

*Důkaz:* Uvažme všechny množiny $xH = \{xh \mid h \in H\}$, kde $x \in G$. To jsou „posunuté kopie“ podgrupy $H$. Nejprve si všimneme, že každá kopie $xH$ ma stejný počet prvků jako $H$. Zobrazení $h \mapsto xh$ z $H$ do $xH$ je totiž invertibilní (má inverzi $t \mapsto x^{-1}t$), takže je to bijekce.

Pak nahlédneme, že každé dvě $xH$ a $yH$ jsou si buď rovny, nebo jsou disjunktní. Ukažeme, že pokud $xH$ a $yH$ nejsou disjunktní, pak $xH \subseteq yH$, a druhá inkluze se dá dokázat analogicky. Nechť existuje $a \in xH \cap yH$. To znamená, že $a = xh_x = yh_y$ pro nějaká $h_x \in H$ a $h_y \in H$. Z toho dostaneme $x = yh_yh_x^{-1}$. Chceme ukázat, že každý prvek $d \in xH$ leží také v $yH$. Takové $d$ lze napsat jako $xh$ pro $h \in H$. To je ovšem rovno $yh_yh_x^{-1}h$, což leží v $yH$, neboť $H$ je uzavřená na operace.

Navíc pro všechna $x \in G$ máme $x \in xH$ (neboť v $H$ je jednotkový prvek). Proto systém množin $\{xH \mid \mathbf{x} \in G\}$ tedy tvoří rozklad $G$ na disjunktní stejně velké množiny. Z toho přímo plyne tvrzení věty. □

### Okruhy a tělesa

**Definice:**

- *Okruh* je algebra $(R, +, \cdot, \mathbf{0}, \mathbf{1}, -)$, kde:
  - $R$ je nosná množina.
  - $+$ a $\cdot$ jsou binární operace, $\mathbf{0}$ a $\mathbf{1}$ konstanty, $-$ je unární operace.
  - $(R, +, \mathbf{0}, -)$ je komutativní grupa (aditivní grupa okruhu).
  - Operace $\cdot$ je komutativní a asociativní.
  - $a\mathbf{1} = \mathbf{1}a = a$ pro všechna $a$.

- $(a+b)\cdot c = a\cdot c + b\cdot c$ *(distributivita).*

  Algebraikové někdy připouští nekomutativní okruhy (s nekomutativní operací $\cdot$), naše okruhy budou vždy komutativní.

- Prvek $a \in R$ má *multiplikativní inverzi* $a^{-1}$, pokud platí $a \cdot a^{-1} = \mathbf{1}$. Pokud multiplikativní inverze existuje, je jednoznačně určena.

- *Těleso* je okruh, v němž má každý prvek $a \neq \mathbf{0}$ multiplikativní inverzi $a^{-1}$. Tedy $(R \setminus \{\mathbf{0}\}, \cdot, \mathbf{1}, {}^{-1})$ tvoří komutativní grupu. Přitom ${}^{-1}$ považujeme za další unární operaci algebry, kterou musí zachovávat morfismy (nenecháme se zmást tím, že pro $\mathbf{0}$ není definovaná; třeba ji pevně dodefinujeme jako $\mathbf{0}$).

**Příklady:**

- $(\mathbb{Z}, +, \cdot, 0, 1, -)$ (celá čísla spolu s obvyklými operacemi) tvoří okruh, který není tělesem (žádný prvek kromě $\pm 1$ není invertibilní).
- $(\mathbb{Q}, +, \cdot, 0, 1, -)$ (racionální čísla spolu s obvyklými operacemi) tvoří těleso.
- $(\mathbb{R}, +, \cdot, 0, 1, -)$ (reálná čísla spolu s obvyklými operacemi) tvoří těleso.
- $(\mathbb{Z}_n, +, \cdot, 0, 1, -)$ (čísla $\{0, \ldots, n-1\}$ se sčítáním, odčítáním a násobením modulo $n$) je také okruh, časem prozkoumáme, pro která $n$ tvoří těleso.
- $(\{0,1\}, \oplus, \wedge, 0, 1, id)$ (kde $\oplus$ je XOR) je okruh izomorfní se $\mathbb{Z}_2$, dokonce je to těleso.

## 7.3 Počítání modulo n

### Invertibilní prvky

Okruh $\mathbb{Z}_n$ není vždy těleso – často mu chybí inverzní prvky vzhledem k násobení.

**Definice:** *Multiplikativní inverze* čísla $x \in \mathbb{Z}_n$ je $x^{-1} \in \mathbb{Z}_n$ takové, že $xx^{-1} \equiv 1$. Číslo $x$ je *invertibilní,* pokud má multiplikativní inverzi.

**Příklad:** V okruhu $\mathbb{Z}_6$ jsou čísla 1 a $5 \equiv -1$ invertibilní, protože $1 \cdot 1 \equiv 1$ a $5 \cdot 5 \equiv 1$. Ostatní čísla invertibilní nejsou: například každý násobek 2 je sudý, což je modulo 6 stále sudé, takže to nemůže být 1. Naproti tomu v $\mathbb{Z}_5$ jsou všechna nenulová čísla invertibilní: $1 \cdot 1 \equiv 2 \cdot 3 \equiv 3 \cdot 2 \equiv 4 \cdot 4 \equiv 1$.

Invertibilní prvky můžeme snadno charakterizovat:

**Lemma:** $a \in \mathbb{Z}_n$ je invertibilní právě tehdy, když $a \perp n$.

*Důkaz:* Pro dané $a$ hledáme $x$ takové, že $ax \equiv 1$. Tedy $ax$ se liší od 1 o nějaký násobek $n$. To znamená, že existuje $y$ takové, že $ax + ny = 1$. Pokud $\gcd(a, n) = 1$, můžeme takové $x$ a $y$ snadno najít – jsou to totiž Bèzoutovy koeficienty. Je-li naopak $\gcd(a, n) = d > 1$, budou jak $ax$, tak $ny$ násobky $d$, takže bude násobkem $d$ i $ax + ny$, zatímco 1 nikdy není násobkem $d$. □

**Důsledek:** Rozšířeným Euklidovým algoritmem můžeme v čase $\mathcal{O}(b^2)$ rozhodnout, zda multiplikativní inverze existuje, a dokonce ji i najít.

**Definice:** $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \perp n\}$ je množina všech invertibilních prvků ze $\mathbb{Z}_n$. Spolu s násobením modulo $n$ a jednotkovým prvkem 1 tvoří *multiplikativní grupu modulo n*. Její řád (počet prvků) udává *Eulerova funkce* $\varphi(n) = |\mathbb{Z}_n^*|$.

Ověřme, že se opravdu jedná o grupu. Musíme ukázat, že množina $\mathbb{Z}_n^*$ je uzavřená na všechny grupové operace:

(1) Pro $x$ a $y$ invertibilní je $xy$ též invertibilní. Jelikož $(xy)(y^{-1}x^{-1}) \equiv x1x^{-1} \equiv 1$, máme $(xy)^{-1} = y^{-1}x^{-1}$.
(2) $x^{-1}$ je invertibilní, jeho inverzí je zpět $x$.
(3) Prvek 1 je invertibilní, neboť $1 \cdot 1 \equiv 1$.

**Důsledek:** Počítáme-li modulo prvočíslo $p$, pak všechna nenulová $x \in \mathbb{Z}_p$ jsou nesoudělná s $p$, a tedy invertibilní. Proto $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ a $\varphi(p) = p - 1$. Z toho plyne, že $\mathbb{Z}_p$ je nejen okruh, ale dokonce těleso. Sčítání, odčítání, násobení i dělení v tomto tělese můžeme počítat v čase $\mathcal{O}(b^2)$.

### Malá Fermatova a Eulerova věta

**Věta (malá Fermatova):** Pro každé prvočíslo $p$ a číslo $x \perp p$ platí $x^{p-1} \equiv_p 1$.

**Důsledek:** $x^{p-2} \bmod p$ je multiplikativní inverze $x$ modulo $p$, neboť $x \cdot x^{p-2} \equiv x^{p-1} \equiv 1$.

Malou Fermatovu větu nebudeme dokazovat přímo, plyne totiž z následující obecnější věty díky tomu, že pro prvočísla platí $\varphi(p) = p - 1$.

**Věta (Eulerova):** Pro každé $n > 1$ a $x \perp p$ platí $x^{\varphi(n)} \equiv_n 1$.

*Důkaz:* Uvažme množinu $H = \{x^0, x^1, x^2, \ldots\}$ (umocňujeme modulo $n$). Jelikož $x$ je invertibilní prvek a ty jsou uzavřené na násobení, je $H$ podmnožinou $\mathbb{Z}_n^*$. Dokážeme, že je dokonce podgrupou $\mathbb{Z}_n^*$.

Jelikož $x^i$ mohou nabývat jen konečně mnoha hodnot, musí se nějaká hodnota zopakovat. Uvažme první takové opakování, tedy nejmenší $j$ takové, že $x^j$ je rovno nějakému $x^i$ pro $i < j$. Všimneme si, že prvek, který se zopakoval, musí být $x^0 = 1$. Kdyby tomu tak

nebylo, pak je $x^{j-i} = 1$, takže 1 se zopakovala dřív. Máme tedy $x^j = 1$, mocniny $x^0$ až $x^{j-1}$ jsou navzájem různé, a proto $|H| = j$.

Nyní si všimneme, že množina $H$ je uzavřená na násobení: $x^a \cdot x^b \equiv x^{a+b}$. Je-li $a+b < j$, pak $x^{a+b}$ leží v $H$. Jinak je $x^{a+b} \equiv x^j \cdot x^{a+b-j}$, jenže $x^j \equiv 1$ a $a+b-j < j$, takže $x^{a+b}$ opět leží v $H$. Podobně nahlédneme, že $H$ je uzavřená na inverzní prvky: inverzním prvkem k $x^a$ je $x^{j-a}$.

Teď už víme, že $H$ je podgrupou $\mathbb{Z}_n^*$, a můžeme použít Lagrangeovu větu. Podle ní platí $|H| \setminus |\mathbb{Z}_n^*|$, tedy $j \setminus \varphi(n)$. Tím pádem je $\varphi(n) = jk$ pro nějaké $k$, takže můžeme psát $x^{\varphi(n)} \equiv x^{jk} \equiv (x^j)^k \equiv 1^k \equiv 1$. □

### Čínská věta o zbytcích

Nyní se zamysleme nad tím, jak najít číslo $x$, které dává modulo $n_1$ zadaný zbytek $a_1$ a modulo $n_2$ zbytek $a_2$. Řešíme tedy soustavu kongruencí:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

Především si můžeme všimnout, že najdeme-li nějaké řešení, přičtením libovolného násobku čísla $n = n_1 n_2$ získáme další řešení. Stačí se tedy omezit na $x \in \mathbb{Z}_n$.

Také si všimneme, že jsou-li $n_1$ a $n_2$ soudělná, nemusí řešení vůbec existovat – například v soustavě

$$\begin{aligned} x &\equiv 2 \pmod{6} \\ x &\equiv 3 \pmod{8} \end{aligned}$$

první kongruence vynucuje, aby $x$ bylo sudé, zatímco druhá, aby bylo liché. Za chvíli uvidíme, že soudělnost je jediná překážka.

**Pozorování:** Nechť $n_1 \perp n_2$. Uvažme funkci $f : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ definovanou takto:

$$f(x) = (x \bmod n_1, x \bmod n_2).$$

Zamysleme se nad jejími vlastnostmi:

1. Nejprve si všimneme, že $f$ je prostá. Pokud $f(x) = f(y)$, pak $x \bmod n_1 = y \bmod n_1$, tedy $n_1 \setminus (x-y)$. Podobně dostaneme $n_2 \setminus (x-y)$. Jelikož $n_1 \perp n_2$, plyne z toho také $n \setminus (x-y)$. To je ovšem pro $x, y \in \mathbb{Z}_n$ možné jen tehdy, když $x = y$.
2. Každá prostá funkce mezi dvěma stejně velkými množinami musí být bijekce. To znamená, že naše soustava kongruencí má pro každé $a_1$ a $a_2$ právě jedno řešení $f^{-1}(a_1, a_2)$.

3. Naše funkce $f$ je dokonce izomorfismus okruhů $Z_n$ a $Z_{n_1} \times \mathbb{Z}_{n_2}$. (Součinem okruhů $R_1$ a $R_2$ se myslí okruh, jehož nosná množina je kartézský součin nosných množin $R_1 \times R_2$ a operace se aplikují po složkách.) Platí totiž $f(0) = (0,0)$, $f(1) = (1,1)$, $f(x+y) = f(x) + f(y)$ a $f(xy) = f(x) \cdot f(y)$.

Tím jsme dokázali speciální případ takzvané Čínské věty o zbytcích.[⟨2⟩] Ukážeme si její dvě verze:

**Věta (Čínská o zbytcích neboli CRT):** Nechť $n_1, \ldots, n_k$ jsou navzájem nesoudělná kladná čísla, $n = n_1 \cdot \ldots \cdot n_k$ a $a_i \in \mathbb{Z}_{n_i}$ pro $i = 1, \ldots, k$. Pak existuje právě jedno $x \in \mathbb{Z}_n$ takové, že $x \bmod n_i = a_i$ pro všechna $i$.

**Věta (Algebraická formulace CRT):** Nechť $n_1, \ldots, n_k$ jsou navzájem nesoudělná kladná čísla a $n = n_1 \cdot \ldots \cdot n_k$. Pak funkce $f : \mathbb{Z}_n \to Z_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ definovaná jako $f(x) = (x \bmod n_1, \ldots, x \bmod n_k)$ je izomorfismus okruhů $Z_n$ a $Z_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$.

*Důkaz:* Pro $k = 1$ jsou obě věty triviální, pro $k = 2$ jsme je už dokázali. Dále pokračujeme indukcí podle $k$, přičemž případ pro $k = 2$ použijeme jako indukční krok. □

Nám se ovšem bude hodit i konstruktivní důkaz, který nám umožní hledané $x$ efektivně najít.

**Věta (Efektivní CRT):** $f^{-1}(a_1, \ldots, a_k)$ lze spočítat v čase $\mathcal{O}(kb^2)$.

*Důkaz:* Větu opět stačí dokázat pro $k = 2$ a pak použít indukci.

Inspirujeme se Lagrangeovou interpolací z oddílu **??**. Pokud bychom znali čísla $u_1$ a $u_2$ taková, že $f(u_1) = (1,0)$ a $f(u_2) = (0,1)$, řešením je jejich lineární kombinace $x = (a_1 u_1 + a_2 u_2) \bmod n$. Jelikož $f$ je homomorfismus, je lineární. Proto platí: $f(x) = a_1 f(u_1) + a_2 f(u_2) = a_1(1,0) + a_2(0,1) = (a_1, a_2)$.

Zbývá si pořídit $u_1$ ($u_2$ najdeme obdobně) Nejprve si všimneme, že $f(n_2) = (v_1, 0)$ pro nějaké $v_1$. Pokud je $v_1 = 1$, položíme $u_1 = n_2$ a jsme hotovi. Jinak najdeme multiplikativní inverzi $w_1$ čísla $v_1$ modulo $n_1$ a položíme $u_1 = w_1 n_2$. Bude platit $f(u_1) = f(w_1 n_2) = w_1 f(n_2) = w_1(v_1, 0) = (w_1 v_1 \bmod n_1, 0) = (1,0)$. □

### Eulerova funkce

Už jsme zavedli funkci $\varphi(n)$, která udává, kolik prvků ze $\mathbb{Z}_n$ je nesoudělných s $n$, tedy invertibilních. Nyní se podívejme, jak tuto funkci počítat.

**Lemma:** Pro Eulerovu funkci $\varphi$ platí:

[⟨2⟩] Čínská se jí říká proto, že byla známa už ve starověké Číně. Zkracuje se jako CRT – Chinese Remainder Theorem.

1. $\varphi(p) = p - 1$.
2. $\varphi(p^k) = (p-1)p^{k-1}$.
3. $\varphi(mn) = \varphi(m)\varphi(n)$, kdykoliv $m \perp n$.

*Důkaz:*

1. S prvočíslem $p$ jsou nesoudělná všechna čísla od 1 do $p-1$.
2. S mocninou $p^k$ jsou soudělná čísla dělitelná $p$, a těch je jedna $p$-tina všech. Zbývá tedy $(1-(1/p))p^k$ nesoudělných, což je rovno uvedenému výrazu.
3. Využijme bijekci $x \mapsto (a \bmod m, a \bmod n)$ z CRT. Číslo $x$ je nesoudělné s $mn$ právě tehdy, když je nesoudělné s $m$ a současně s $n$. To je totéž jako že ve dvojici zbytků $(a, b)$ je $a$ nesoudělné s $m$ a současně $b$ nesoudělné s $n$. Takových dvojic je $\varphi(m) \cdot \varphi(n)$ a každá odpovídá právě jednomu nesoudělnému $x$. □

Z tohoto lemmatu plyne, že kdykoliv umíme číslo $n$ faktorizovat (rozložit na součin mocnin různých prvočísel), umíme efektivně spočítat $\varphi(n)$. Žádný efektivní způsob, který nepotřebuje faktorizaci, není znám.

## 7.4 Faktorizace versus prvočíselnost

Mezi základní algoritmické problémy teorie čísel patří *faktorizace* celých čísel (rozklad na součin prvočísel) a testování, zda dané číslo je prvočíslem. Jakkoliv podobně tyto problémy vypadají, jejich obtížnost je zásadně různá.

Faktorizace:

- Známe triviální exponenciální algoritmus (zkoušení všech dělitelů až do odmocniny trvá $\mathcal{O}(2^{b/2}b^2)$).
- Neznáme žádný polynomiální algoritmus.
- Známe subexponenciální algoritmy, zatím nejlepší je general number field sieve se složitostí $\exp(1.923 \cdot (\log n)^{1/3}(\log\log n)^{2/3})$. Paralelní verze tohoto algoritmu běžící na stovkách počítačů dokázala v roce 2020 faktorizovat 829-bitové číslo.
- Rozhodovací verze (je dáno $x$ a interval $[a, b]$, existuje dělitel čísla $x$ ležící v intervalu?) leží v průniku NP a co-NP, považuje se za nepravděpodobné, že by byla NP-úplná.
- Známe polynomiální kvantový algoritmus (Shorův z roku 1994).

Prvočíselnost:

- Známe rychlé pravděpodobnostní testy s malou pravděpodobností chyby.

- Známe deterministické polynomiální algoritmy, zatím nejlepší je od Lenstry a Pomerance se složitostí $\mathcal{O}(b^6 \log^c b)$. V praxi jsou mnohem pomalejší než ty pravděpodobnostní.

**Triviální testy**

Jak navrhnout pravděpodobnostní test prvočíselnosti? Testujeme-li číslo $n$, můžeme vygenerovat rovnoměrně náhodné $a \in \{2, \ldots, n-1\}$ a otestovat, zda $a$ je dělitelem $n$. Pokud je, odpovíme, že $n$ je složené. Jinak odpovíme, že $n$ je prvočíslo.

Jak dobrý tento test je? Doběhne vždy v čase $\mathcal{O}(b^2)$. Pokud odpoví SLOŽENÉ, je to vždy pravda. Pokud odpoví PRVOČÍSLO, může se mýlit. Pro prvočíslo tedy vždy odpoví PRVOČÍSLO, ale pro složené číslo může odpovědět špatně. Chtěli bychom tedy dokázat, že test složené číslo „usvědčí“ s dost velkou pravděpodobností. To bohužel neplatí: je-li $n = pq$ pro dvě různá prvočísla $p$ a $q$, test odpoví SLOŽENÉ pouze pro $a = p$ a $a = q$. Pravděpodobnost usvědčení je tedy pouze $2/(n-2)$.

Druhý pokus: opět vygenerujeme náhodné $a$ a tentokrát spočítáme $\gcd(a, n)$. Pokud je to více než 1, našli jsme netriviálního dělitele a odpovíme SLOŽENÉ (takovému $a$ se říká *Euklidův svědek* složenosti). Pokud vyjde 1, odpovíme PRVOČÍSLO. Pro prvočísla tedy vždy odpovídáme správně, zatímco u složeného čísla se můžeme mýlit. Jaká je pravděpodobnost, že složené číslo usvědčíme? Pro $n = pq$ bohužel stále dost malá. Jelikož $\varphi(pq) = (p-1)(q-1)$, Euklidových svědků existuje jenom $pq - 1 - (p-1)(q-1) = p + q$. Je-li $p \approx q$, je počet svědků řádově $\sqrt{n}$, takže pravděpodobnost, že se do nějakého strefíme, je pouze $\sqrt{n}/n = 1/\sqrt{n}$.

**Fermatův test**

Zajímavější test získáme z malé Fermatovy věty. Ta říká, že pro prvočíslo $n$ a libovolné $a \perp n$ platí $a^{n-1} \bmod n = 1$. Pokud tedy pro dané $n$ najdeme $a \perp n$, pro které $a^{n-1} \bmod n \neq 1$, víme, že $n$ není prvočíslo. Takovému $a$ se říká *Fermatův svědek* složenosti. Celý test bude vypadat následovně:

**Algoritmus** FERMATŮVTEST
*Vstup:* číslo $n > 1$

1. Zvolíme rovnoměrně náhodně $a \in \{2, \ldots, n-1\}$.
2. Pokud $\gcd(a, n) \neq 1$, odpovíme SLOŽENÉ. ◁ *a je Euklidův svědek*
3. Pokud $a^{n-1} \bmod n \neq 1$, odpovíme SLOŽENÉ. ◁ *a je Fermatův svědek*
4. Odpovíme PRVOČÍSLO.

Test pracuje v čase $\mathcal{O}(b^3)$. Krok 2 bychom dokonce mohli vynechat, protože pokud $d = \gcd(a, n) > 1$, je $a^{n-1}$ dělitelné $d$, a tím pádem i $a^{n-1} \bmod n$ dělitelné $d$, a proto by číslo

prohlásil za složené i samotný krok 3. Přítomnost druhého kroku nám nicméně zjednoduší uvažování o testu.

Pokud test odpoví SLOŽENÉ, nemýlí se. Pro prvočísla tedy vždy odpovídá správně. Potřebujeme ukázat, že složená čísla mají dostatek svědků, takže se s nezanedbatelnou pravděpodobností do nějakého strefíme.

To bohužel není pravda: existují *Carmichaelova čísla,* což jsou složená čísla bez Fermatových svědků, takže je lze usvědčit pouze Euklidovými svědky, kterých je obecně málo. Nejmenší Carmichaelovo číslo je 561 a dnes už se ví, že existuje nekonečně mnoho dalších, takže nestačí do algoritmu zabudovat tabulku výjimek. Dobrá zpráva ovšem je, že pro ostatní čísla test funguje dobře.

**Lemma:** Je-li $n$ složené číslo, které není Carmichaelovo, Fermatův test ho usvědčí s pravděpodobností aspoň $1/2$.

*Důkaz:* Spusťme algoritmus s daným $n$. Pokud narazíme na Euklidova svědka, rovnou odpovíme správně. Stačí tedy lemma dokázat pro $a$ rovnoměrně náhodně vybrané z $\mathbb{Z}_n^*$. Uvažme podmnožinu $H \subseteq \mathbb{Z}_n^*$ čísel, která nejsou Fermatovými svědky. Tedy:

$$H = \{a \in \mathbb{Z}_n^* \mid a^{n-1} \bmod n = 1\}.$$

Dokážeme, že $H$ je podgrupu $\mathbb{Z}_n^*$. Jistě platí $1 \in H$. Pokud $a, b \in H$, máme $(ab)^{n-1} \equiv a^{n-1}b^{n-1} \equiv 1 \cdot 1 \equiv 1$, takže $ab \in H$. Podobně ověříme, že pro $a \in H$ je $a^{-1} \in H$.

Nyní použijeme Lagrangeovu větu a získáme $|H| \setminus |\mathbb{Z}_n^*|$. Jenže $n$ není Carmichaelovo, takže $H \neq \mathbb{Z}_n^*$, a tím pádem musí být $|H| \leq |\mathbb{Z}_n^*|/2$. Pravděpodobnost, že najdeme Fermatova svědka, je tedy alespoň $1/2$. □

Může se zdát, že pravděpodobnost usvědčení $1/2$ není nic moc. Ovšem pravděpodobnostní test můžeme iterovat: spustíme ho $t$-krát s nezávisle náhodnými $a$ a odpovíme PRVOČÍSLO pouze tehdy, když se na tom všechna spuštění shodla. Pravděpodobnost chyby je pak nejvýše $1/2^t$. Časovou složitost jsme přitom zhoršili jen na $\mathcal{O}(tb^3)$.

### Rabinův-Millerův test

V praxi se používá důmyslnější test, který se nenechá zmást ani Carmichaelovými čísly. Funguje následovně:

**Algoritmus** RabinůvMillerůvTest
*Vstup:* číslo $n > 1$

1. Zvolíme rovnoměrně náhodně $a \in \{2, \ldots, n-1\}$.
2. Pokud $\gcd(a, n) \neq 1$, odpovíme SLOŽENÉ. ◁ *a je Euklidův svědek*

3. Najdeme $t$ a liché $m$ taková, že $n-1 = 2^t \cdot m$.
4. Spočteme $b_0 \leftarrow a^m \bmod n$.
5. Spočteme $b_1, \ldots, b_t$: $b_{i+1} = a_i^2 \bmod n$ (tudíž $b_t \equiv x^{n-1}$).
6. Pokud je $b_t \neq 1$, odpovíme SLOŽENÉ. ◁ *a je Fermatův svědek*
7. Pokud jsou všechna $b_0, \ldots, b_t = 1$, odpovíme PRVOČÍSLO.
8. Jinak vezmeme nejvyšší $i$, pro něž $b_i \neq 1$:
9. Pokud je $b_i \equiv -1$, odpovíme PRVOČÍSLO.
10. Jinak odpovíme SLOŽENÉ. ◁ *a je Riemannův svědek*

Krok 2 můžeme stejně jako u Fermatova testu vypustit, ale jeho přítomnost nám usnadní analýzu algoritmu.

Na algoritmus se můžeme dívat i jinak: nejdříve spočteme $a^{n-1}$ (vše mod $n$). Pokud nevyjde jednička, je $n$ složené podle Fermatova testu. Pokud vyjde a $n-1$ je sudé, musí být $a^{(n-1)/2}$ odmocninou z jedničky. Tyto odmocniny mohou existovat jenom dvě: 1 a $-1$ (kvadratický polynom má nejvýš dva kořeny v každém tělese). Pokud tedy vyjde něco jiného, $n$ jistě není prvočíslo. Pokud vyjde opět jednička, pokračujeme v odmocňování a počítáme $a^{(n-1)/4}$, $a^{(n-1)/8}$, atd. Zastavíme se, když narazíme na $-1$ (tehdy odpovíme PRVOČÍSLO), nebo na něco jiného než $\pm 1$ (SLOŽENÉ), nebo když exponent přestane být celočíselný (PRVOČÍSLO). Z této úvahy plyne, že kdykoliv odpovíme SLOŽENÉ, je to pravda.

Důležité ovšem je, že pro všechna složená čísla existuje dostatek svědků:

**Věta:** Rabinův-Millerův test testuje prvočíselnost v polynomiálním čase, na prvočísla odpovídá správně a složená čísla prohlašuje za prvočísla s pravděpodobností nejvýše 1/4.

Důkaz je poměrně náročný, naleznete ho například v knize Computational Number Theory od Victora Shoupa. Zjednodušenou verzi (pro konstantu 1/2 namísto 1/4) uvádíme v oddílu 7.7.

**Poznámka:** Za zmínku ještě stojí, že původní Millerův test byl deterministický a pan Miller o něm dokázal, že pokud platí rozšířená Riemannova hypotéza, má každé složené číslo svědka (Fermatova či Riemannova), který je jen logaritmicky velký. Zda hypotéza platí, se dosud neví, nicméně pan Rabin později nahlédl, že svědků vždy existuje alespoň $3/4 \cdot n$, a randomizovaný algoritmus byl na světě.

### Hledání prvočísel

Často potřebujeme opatřit si nějaké velké ($b$-bitové) prvočíslo. Nabízí se generovat náhodná $b$-bitová čísla (začínající na 1), testovat, zda to jsou prvočísla, a opakovat, dokud nedostaneme prvočíslo.

Jak efektivní tento přístup bude? Je známo, že hustota prvočísel okolo $n$ je přibližně $1/\ln n$. Tudíž pravděpodobnost, že náhodné $b$-bitové číslo bude prvočíslem, je $\Theta(1/b)$.

Podle lemmatu o chození se džbánem pro vodu tedy na prvočíslo narazíme po průměrně $\Theta(b)$ pokusech.

## 7.5 Diskrétní logaritmy

Důležitou vlastností těles modulo prvočíslo je, že se v nich dá logaritmovat. Začneme následující větou (důkaz zájemce najde v závěru tohoto oddílu).

**Věta:** Pro každé prvočíslo $p$ je multiplikativní grupa $\mathbb{Z}_p^*$ cyklická. Existuje tedy alespoň jedno $g$ (generátor) takové, že $\mathbb{Z}_p^* = \{g^0, \ldots, g^{p-2}\}$.

Grupa $\mathbb{Z}_p^*$ je tedy izomorfní s grupou $\mathbb{Z}_{p-1}$. Izomorfismus v jednom směru je funkce $e : x \mapsto g^x \bmod p$, v druhém směru její inverze, které se říká *diskrétní logaritmus.* Zatímco mocniny modulo $p$ dokážeme počítat efektivně (v čase $\mathcal{O}(b^3)$), diskrétní logaritmus nikoliv. Podobně jako u faktorizace neznáme žádný polynomiální algoritmus, ale známe zajímavé subexponenciální algoritmy a polynomiální kvantový algoritmus.

Často potřebujeme nějaký generátor najít. K tomu se hodí otestovat, zda dané číslo $g$ je generátorem.

**Věta:** $g \in \mathbb{Z}_p^*$ je generátorem $\mathbb{Z}_p^*$ právě tehdy, když pro všechny prvočíselné dělitele $d$ čísla $p-1$ platí $g^{(p-1)/d} \not\equiv 1$.

*Důkaz:* Pokud pro některého z dělitelů vyjde $g^{(p-1)/d} \equiv 1$, znamená to, že $g$ není generátorem celé grupy, nýbrž jen nějaké menší podgrupy.

Pro opačnou implikaci uvažme $g$, které generuje jen nějakou podgrupu $H = \{g^0, \ldots, g^{t-1}\} \subset \mathbb{Z}_p$, přičemž $g^t \equiv 1$. Podle Lagrangeovy věty platí $t = |H| \setminus |\mathbb{Z}_p| = \varphi(p) = p - 1$.

Pro $d = (p-1)/t$ by tedy bylo $g^{(p-1)/d} \equiv 1$. Jenže $d$ nemusí být prvočíslo (a testovat všechny neprvočíselné dělitele by trvalo příliš dlouho). V takovém případě uvážíme rozklad $d = d'e$, kde $d'$ je prvočíslo a $e > 1$. Potom $g^{(p-1)/d'} \equiv g^{((p-1)/d)e} \equiv \left(g^{(p-1)/d}\right)^e \equiv 1^e \equiv 1$. Takže $g$ z negenerování usvědčíme volbou prvočíselného dělitele $d'$. □

**Důsledek:** Známe-li faktorizaci čísla $p-1$, umíme otestovat, zda $g$ je generátor, v čase $\mathcal{O}(b^4)$. Prvočíselných dělitelů totiž musí být $\mathcal{O}(b)$.

#### Hledání generátoru

Pro hledání generátoru se nabízí podobně jako u prvočísel náhodně vybírat prvky $\mathbb{Z}_p^*$, dokud nenarazíme na generátor. Aby to bylo efektivní, potřebujeme, aby generátory byly v $\mathbb{Z}_p^*$ dostatečně časté.

**Lemma:** Nechť $g$ je nějaký generátor $\mathbb{Z}_p^*$. Pak $g^i$ je generátor právě tehdy, když $i \perp p-1$.

*Důkaz:* Zajímá nás, zda mocniny $(g^i)^j = g^{ij}$ pro $j = 0, \ldots, p-2$ projdou celou multiplikativní grupu. Prvek $g^k$ navštívíme právě tehdy, když pro nějaké $j$ platí $k \equiv_{p-1} ij$. Pro $k = 1$ je takové $j$ multiplikativní inverzí $i$ modulo $p-1$ a ta existuje právě tehdy, když $i \perp p-1$. Ovšem najdeme-li takové $j$, dostaneme libovolné $g^k$ jako $g^{ijk} \equiv (g^i)^{jk}$. □

**Důsledek:** Grupa $\mathbb{Z}_p^*$ má $\varphi(p-1)$ generátorů.

Generátory budeme často potřebovat v případech, kdy $p = 2q+1$ a $q$ je také prvočíslo. Tehdy $\varphi(p-1) = \varphi(2q) = \varphi(2)\varphi(q) = 1 \cdot (q-1) = q-1 \approx p/2$. Generátory tedy tvoří přibližně polovinu prvků $\mathbb{Z}_p^*$, takže po průměrně dvou pokusech nějaký najdeme.

### Důkaz věty o cykličnosti multiplikativní grupy*

Nejprve definujme $N_p(d)$ jako počet prvků $\mathbb{Z}_p^*$, které mají řád $d$. Řády prvků musí dělit řád celé grupy, což je $p-1$, takže $N_p(d)$ může být nenulové jen pro $d \setminus (p-1)$.

Generátor celé grupy je prvek řádu $p-1$, takže tvrzení věty je ekvivalentní s $N_p(p-1) > 0$.

**Lemma:** Nechť $d \setminus (p-1)$ a $N_p(d) > 0$. Potom $N_p(d) = \varphi(d)$.

*Důkaz:* Nechť $N_p(d) > 0$ a $a \in \mathbb{Z}_p^*$ je nějaký prvek řádu $d$. Uvažujme rovnici $x^d \equiv 1$ v $\mathbb{Z}_p$. To je polynomiální rovnice řádu $d$ v tělese, takže má nejvýše $d$ kořenů. Všechny mocniny $a^0$ až $a_{d-1}$ patří mezi kořeny (platí $(a^i)^d \equiv a^{id} \equiv (a^d)^i \equiv 1^i \equiv 1$), tím pádem žádné další kořeny neexistují.

Každý prvek řádu $d$ ovšem musí být kořenem této rovnice, takže ho jde zapsat jako $a^i$ pro nějaké $i$. Z úvahy o počítání generátorů plyne, že $a^i$ generuje právě tehdy, když $i \perp d$. Takových $i$ je $\varphi(d)$. □

**Důsledek:** Pro každé $d \setminus (p-1)$ platí $N_p(d) \leq \varphi(d)$.

Každý prvek $\mathbb{Z}_p^*$ má nějaký řád. Proto sečteme-li $N_p(d)$ přes všechna $d$, musíme dostat $p-1$. Zkombinováním s předchozím důsledkem dostaneme:

$$p - 1 = \sum_{d \setminus (p-1)} N_p(d) \leq \sum_{d \setminus (p-1)} \varphi(d). \qquad (*)$$

Platí ovšem i opačná nerovnost:

**Lemma:** Pro každé $n > 0$ platí $\sum_{d \setminus n} \varphi(n) = n$.

*Důkaz:* Budeme počítat zlomky

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots \frac{n-1}{n}, \frac{n}{n}.$$

rozdělené do skupin podle jmenovatele po zkrácení. Pokud se zlomek $i/n$ zkrátí na $j/d$, musí být $j \perp d$ a $d \setminus n$. Navíc $1 \leq i \leq n$ je ekvivalentní s $1 \leq j \leq d$. Pro dané $d$ tedy připadají v úvahu všechna $j$ od 1 do $d$, která jsou nesoudělná s $d$. Těch je $\varphi(d)$. Sečtením přes všechna $d$ získáme rovnost z tvrzení lemmatu. □

Spojením lemmatu s nerovností $(*)$ dostaneme

$$\sum_{d \setminus (p-1)} N_p(d) = \sum_{d \setminus (p-1)} \varphi(d).$$

Žádná z nerovností $N_p(d) \leq \varphi(d)$ tedy nemůže být ostrá. Proto je $N_p(p-1) = \varphi(p-1)$, což je nenulové číslo. Tím je věta dokázaná.

## 7.6 Kvadratické zbytky

Prozkoumejme, jak se v $\mathbb{Z}_p$ chovají druhé odmocniny (v tomto oddílu budeme říkat prostě odmocniny). Ptáme se tedy na řešení kongruence $x^2 \equiv_p a$ pro dané $a$.

**Příklad:** V $\mathbb{Z}_5$ je $0^2 \equiv 0$, $1^2 \equiv 4^2 = 1$ a $2^2 \equiv 3^2 \equiv 4$. Prvky 1 a 4 tedy mají dvě různé odmocniny, 0 má jednu a 2 ani 3 žádnou.

Tohle není náhoda:

**Věta:** V každém tělese $\mathbb{Z}_p$ má prvek 0 právě jednu odmocninu, $(p-1)/2$ prvků má dvě odmocniny (těmto prvkům se říká *kvadratické zbytky, QR*) a zbylých $(p-1)/2$ prvků nemá žádnou (*kvadratické nezbytky*[3]). Zvolíme-li libovolný generátor $\mathbb{Z}_p$, kvadratické zbytky jsou ty prvky, jejichž diskrétní logaritmy jsou sudé.

*Důkaz:* Je-li $x^2 \equiv a$, je také $(-x)^2 \equiv a$. Odmocniny se tedy vyskytují v párech. Přitom $x \equiv -x$ pouze pro $x = 0$, takže každý nenulový prvek má sudý počet odmocnin. 0 má jen jednu (součinem nenulových prvků není nikdy 0).

Odmocniny prvku $a$ jsou kořeny kvadratického polynomu $x^2 - a$ a ty mohou v libovolném tělese existovat nejvýš 2. To v kombinaci s předchozím odstavcem dává, že každý nenulový prvek má 0 nebo 2 odmocniny.

Každý nenulový prvek $\mathbb{Z}_p$ leží v $\mathbb{Z}_p^*$, takže ho můžeme napsat jako mocninu nějakého generátoru $g$. Polovinu $\mathbb{Z}_p^*$ tvoří sudé mocniny $g^{2k}$ a ty jistě mají druhou odmocninu $g^k$, a tím pádem i $g^{-k}$. Těchto $(p-1)/2$ čísel patří mezi kvadratické zbytky.

[3] Za tento termín se omlouváme. Smysl moc nedává, ale je tradiční.

Každé z nich ovšem spotřebovalo 2 prvky $\mathbb{Z}_p^*$ na své odmocniny, takže na zbylých $(p-1)/2$ prvků žádné odmocniny nezbyly. Zbylé prvky tedy kvadratickými zbytky nejsou. □

**Lemma:** Pro libovolný generátor $g$ platí $g^{(p-1)/2} \equiv -1$.

*Důkaz:* $g^{(p-1)/2}$ je odmocnina z $g^{(p-1)} \equiv 1$. Odmocniny z jedničky existují dvě: 1 a $-1$. Ovšem 1 to být nemůže, protože by se mocniny generátoru začaly opakovat dřív, než by vygenerovaly celou $\mathbb{Z}_p^*$. □

Jelikož diskrétní logaritmy je těžké počítat, bude se hodit efektivnější test na kvadratické zbytky:

**Věta (Eulerovo kriterium):** Pro $x \in \mathbb{Z}_p^*$ je $x^{(p-1)/2}$ rovno 1, pokud $x$ je kvadratický zbytek, a jinak rovno $-1$.

*Důkaz:* Opět uvažujme $x$ jako mocninu nějakého generátoru $g$. Pokud $x \equiv g^{2k}$ (a tedy $x$ je kvadratický zbytek), dostaneme

$$\left(g^{2k}\right)^{\frac{p-1}{2}} \equiv g^{\frac{2k(p-1)}{2}} \equiv g^{k(p-1)} \equiv (g^{p-1})^k \equiv 1^k \equiv 1.$$

Pro $x \equiv g^{2k+1}$ (není kvadratický zbytek), vyjde

$$\left(g^{2k+1}\right)^{\frac{p-1}{2}} \equiv g^{\frac{2k(p-1)}{2}} \cdot g^{\frac{p-1}{2}} \equiv 1 \cdot (-1) \equiv -1.$$

□

**Důsledek:** Množina všech kvadratických zbytků tvoří podgrupu $\mathbb{Z}_p^*$.

**Důsledek:** Testovat, zda číslo je kvadratickým zbytkem, lze v čase $\mathcal{O}(b^3)$.

### Výpočet diskrétních odmocnin

Prvočísla existují ve dvou „příchutích“: $p = 4\ell + 1$ a $p = 4\ell + 3$. Je překvapivě, jak různě se v mnoha situacích tyto dva druhy prvočísel chovají.

Pokud $p = 4\ell+3$, je výpočet diskrétní odmocniny snadný. Pro každý kvadratický zbytek $a$ totiž platí

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} \cdot a \equiv 1 \cdot a,$$

přičemž poslední rovnost získáme z Eulerova kriteria. To znamená, že $a^{(p+1)/4}$ je odmocninou z $a$.

Pro $p = 4\ell + 1$ není známý žádný deterministický algoritmus pro výpočet odmocnin. Existuje Tonelliho-Shanksův randomizovaný algoritmus, který pracuje v průměrně polynomiálním čase. Detaily nebudeme potřebovat.

**Odmocniny modulo složené číslo**

V $\mathbb{Z}_n$ pro složené $n$ je situace mnohem složitější. Prozkoumejme nejdřív případ, $n = pq$ pro dvě různá prvočísla $p$ a $q$. Aby $x^2$ bylo kongruentní s nějakým $a$ modulo $n$, musí s ním být kongruentní i modulo $p$ a modulo $q$. Hledáme tedy dvojici $(x_1, x_2)$ takovou, že $x_1^2 \equiv_p a_1$ a $x_2^2 \equiv_q a_2$, kde $a_1 = a \bmod p$ a $a_2 = a \bmod q$. Podle Čínské věty o zbytcích odpovídá každá taková dvojice právě jedné odmocnině $x \in \mathbb{Z}_n$.

Každé $a_i$ je buďto 0 (pak existuje právě jedno $x_i$) nebo kvadratický zbytek (dvě $x_i$), případně kvadratický nezbytek (žádné $x_i$). V závislosti na tom existují 0, 2, nebo 4 dvojice $(x_1, x_2)$, a tedy stejný počet odmocnin $x$.

Toto lze zobecnit pro libovolné složené $n$ a převést tak odmocňování modulo $n$ na odmocňování modulo prvočíselné faktory $n$, pokud umíme $n$ faktorizovat. Žádný efektivní způsob počítání diskrétních odmocnin bez faktorizace $n$ není znám. (Možnost, že $n$ může mít násobné faktory, s dovolením nebudeme zkoumat.)

# 7.7* Rozbor Rabinova-Millerova testu

O Rabinově-Millerově testu již víme, že prvočíslo vždy prohlásí za prvočíslo a že složené číslo, které není Carmichaelovo, usvědčí s pravděpodobností alespoň 1/2. Nyní dokážeme, že je to pravda i pro Carmichaelova čísla. Nejprve si připravíme půdu jedním drobným lemmatem:

**Lemma:** Žádné Carmichaelovo číslo není mocninou prvočísla (druhou nebo větší).

*Důkaz:* Uvažujme libovolné $n = p^e$, kde $p$ je prvočíslo a $e > 1$. Zvolíme $a = 1 + p^{e-1}$, což je jistě nesoudělné s $n$. Podle binomické věty spočteme $a^p$ (vše počítáme v $\mathbb{Z}_n$, kde je $a$ invertibilní):

$$a^p \equiv (1+p^{e-1})^p \equiv \binom{p}{0} \cdot 1 \cdot 1 + \binom{p}{1} \cdot 1 \cdot p^{e-1} + \binom{p}{2} \cdot 1 \cdot p^{2(e-1)} + \ldots + \binom{p}{p} \cdot 1 \cdot p^{p(e-1)} \equiv 1$$

(všechny členy mimo nultého jsou totiž dělitelné $p^e$ – prvnímu pomůže kombinační číslo, u ostatních stačí vyšší mocnina $p^{e-1}$). Proto také $a^n \equiv (a^p)^e \equiv 1$. Tedy $a^{n-1} \equiv a^{-1} \not\equiv 1$, takže $n$ není Carmichaelovo. □

Teď uvažujme, kdy může Rabinův-Millerův test odpovědět, že číslo je prvočíslem. Stane se tak buď v kroku 7 (všechna $b_0, \ldots, b_t$ jsou jedničky, což nastane, kdykoliv $b_0 \equiv 1$) nebo v kroku 9 (nějaké $b_i \equiv -1$ a $b_{i+1} \equiv \ldots \equiv b_t \equiv 1$). Rozebereme postupně oba případy.

**Lemma:** Buď $n$ Carmichaelovo a $n - 1 = 2^t \cdot m$ jako v algoritmu. Poté existuje alespoň $|\mathbb{Z}_n^*|/2$ čísel $a \in \mathbb{Z}_n^*$, pro něž $b_0 := a^m \not\equiv 1$.

*Důkaz:* Podobnou úvahou založenou na Lagrangeově větě, jako jsme použili u Fermatova testu. Množina $B = \{b \in \mathbb{Z}_n^* \mid b^m \equiv 1\}$ tvoří podgrupu $\mathbb{Z}_n^*$, takže zbývá ukázat, že alespoň jeden prvek $a \in \mathbb{Z}_n^*$ neleží v $B$.

Buď $p$ nějaký prvočíselný dělitel čísla $n$. Zvolme $a \in \mathbb{Z}_p^*$, které není modulo $p$ odmocnitelné. Už víme, že takových čísel existuje $(p-1)/2$ a že splňují následující vlastnosti:

$$a^{p-1} \equiv 1 \pmod{p},$$
$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Uvažujme podgrupu $H \subseteq \mathbb{Z}_p$ generovanou prvkem $a$ (tedy množinu $\{a^0, a^1, a^2, \ldots\}$). Z předchozích dvou rovností vyplývá, že řád této podgrupy dělí $p-1$, ale nedělí $(p-1)/2$, takže řád musí být sudé číslo. Pro liché $m$ tedy nemůže platit $a^m \equiv_p 1$, takže ani $a^m \equiv_n 1$. □

Nyní se přesuneme ke kroku 9. Z předchozího lemmatu víme, že pro některé volby čísla $a$ v algoritmu je $b_0 \not\equiv 1$, ale pro všechna $a \in \mathbb{Z}_n^*$ je $b_t \equiv 1$. Můžeme proto zvolit $i$ $(0 \leq i < t)$ takové, že $b_{i+1} \equiv a^{2^{i+1}m} \equiv 1$ pro všechna možná $a \in \mathbb{Z}_n^*$, ale $b_i \equiv a^{2^i m} \not\equiv 1$ pro alespoň jedno takové $a$. Jakmile dokážeme, že $b_i \not\equiv \pm 1$ pro alespoň polovinu z možných $a$, máme vyhráno.

**Lemma:** Pro $n$ Carmichaelovo, $n - 1 = 2^t \cdot m$ a $i$ definované podle předchozího odstavce existuje alespoň $|\mathbb{Z}_n^*|/2$ čísel $a \in \mathbb{Z}_n^*$ takových, že $a^{2^i m} \not\equiv_n \pm 1$.

*Důkaz:* Ještě jednou stejný trik s podgrupou. Tentokrát zvolíme $G = \{x \in \mathbb{Z}_n^* \mid a^{2^i m} \equiv \pm 1\}$, což je evidentně podgrupa $\mathbb{Z}_n^*$, a opět chceme dokázat, že alespoň jeden prvek leží mimo ni.

Z volby $i$ víme, že existuje $c$, pro něž $c^{2^i m} \not\equiv 1$. Pokud $c^{2^i m} \not\equiv -1$, máme vyhráno, neboť takové $c$ neleží v $G$. V opačném případě zvolíme nějaký člen $p^e$ z prvočíselného rozkladu čísla $n$. Jelikož $c^{2^i m} \equiv_n -1$, musí tato kongruence platit i modulo $p^e$. Nyní pomocí Čínské věty o zbytcích najdeme $d$ tak, aby splňovalo současně $d \equiv_{p^e} c$ a $d \equiv_{n/p^e} 1$ (zde jsme potřebovali, že $n$ není mocnina prvočísla). Spočítáme-li $(2^i m)$-tou mocninu čísla $d$ modulo jak $p^e$, tak $n/p^e$, dostaneme $d^{2^i m} \equiv_{p^e} c^{2^i m} \equiv_{p^e} -1$ a $d^{2^i m} \equiv_{n/p^e} 1$. Proto $d^{2^i m}$ nemůže být modulo $n$ ani 1, ani $-1$, takže $d \notin G$. □

# 7.8* Ještě jeden test prvočíselnosti

Nakonec předvedeme ještě jeden algoritmus pro pravděpodobnostní testování prvočísel, jehož korektnost je snadné dokázat. Daní za jednoduchost důkazu ovšem bude to, že náš

test může udělat chybu na obě strany: jak prohlásit složené číslo za prvočíslo, tak prvočíslo za složené. Bude fungovat následovně:

**Algoritmus** OdmocninovýTest
*Vstup:* $n > 1$ je testované číslo, $t \geq 1$ počet iterací

1. Pokud je $n$ netriviální mocninou nějakého přirozeného čísla, odpovíme SLOŽENÉ.
2. Vygenerujeme náhodná $a_1, \ldots, a_t \in \mathbb{Z}_n \setminus \{0\}$.
3. Pokud pro nějaké $i$ je $\gcd(a_i, n) \neq 1$, odpovíme SLOŽENÉ.
4. Spočítáme $r_i \leftarrow a_i^{(n-1)/2} \bmod n$ pro všechna $i$.
5. Pokud pro nějaké $i$ je $r_i \not\equiv \pm 1$, odpovíme SLOŽENÉ.
6. Pokud pro všechna $i$ je $r_i = 1$, odpovíme SLOŽENÉ.
7. Jinak odpovíme PRVOČÍSLO.

Nejprve si všimneme, že algoritmus běží v polynomiálním čase. Největší společné dělitele a mocniny modulo $n$ už polynomiálně umíme počítat, jediný problematický krok je ten první. V něm ale stačí zkoušet všechny možné exponenty (těch je $\mathcal{O}(\log n) = \mathcal{O}(b)$, jelikož základ je alespoň 2) a pro každý exponent binárně vyhledávat odmocninu (opět $\mathcal{O}(b)$ kroků).

Nyní nahlédněme, jak algoritmus probíhá pro prvočísla. První ani třetí krok prvočíslo neodmítnou, pátý také ne, jediný problém může nastat v šestém kroku. Podle Eulerova kriteria je $r_i = 1$ právě tehdy, má-li $a_i$ druhou odmocninu, a to nastane s pravděpodobností $1/2$. Šestý krok tedy odpoví SLOŽENÉ jen tehdy, když jsou všechna $a_i$ odmocnitelná, pravděpodobnost čehož je $1/2^t$.

Složené číslo naopak prohlásíme za prvočíslo jen tehdy, pokud jsou všechna $a_i \in \mathbb{Z}_n^*$, nalezneme alespoň jedno $r_i \equiv -1$ a všechna ostatní $r_j$ jsou buďto 1 nebo $-1$. K odhadu pravděpodobnosti tohoto nám poslouží následující lemma:

**Lemma:** Buď $n$ složené číslo, které není mocninou prvočísla. Nechť pro nějaké $a \in \mathbb{Z}_n^*$ je $a^{(n-1)/2} \equiv_n -1$. Pak množina $S_n = \{x \in \mathbb{Z}_n^* \mid x^{(n-1)/2} \equiv_n \pm 1\}$ obsahuje nejvýše $|\mathbb{Z}_n^*|/2$ prvků.

*Důkaz:* Podobně jako u Fermatova testu: Všimneme si, že $S_n$ je podgrupa $\mathbb{Z}_n^*$, takže zbývá dokázat, že je to podgrupa netriviální, a použít Lagrangeovu větu. Najdeme číslo $c$, které nebude ležet v $S_n$.

Nechť $n$ má prvočíselný rozklad $p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$. Již víme, že $s \geq 2$. Označme $q = p_1^{k_1}$ a $m = n/q$. Jelikož $q \setminus n$ i $m \setminus n$, musí být pro každý prvek $x \in S_n$ jak $x^{(n-1)/2} \equiv_q \pm 1$, tak $x^{(n-1)/2} \equiv_m \pm 1$ a znaménka obou zbytků jsou stejná.

Kýžené číslo $c$ zvolíme tak, aby pro něj platilo $c \equiv_q a$ a současně $c \equiv_m 1$ (Čínská věta o zbytcích nám jeho existenci zaručuje, jelikož $q \perp m$). Snadno ověříme, že platí:

$$c^{(n-1)/2} \equiv_q a^{(n-1)/2} \equiv_q -1,$$
$$c^{(n-1)/2} \equiv_m 1.$$

Takové $c$ ovšem neleží v $S_n$, protože jak už jsme pozorovali, pro každý prvek z $S_n$ jsou zbytky po dělení $q$ a $m$ stejné, zatímco jsme si $c$ zvolili tak, aby zbytky byly různé. □

Náš algoritmus tudíž selže jedině tehdy, když $a_2, \ldots, a_t$ padnou všechna do $S_n$, a to nastane s pravděpodobností nejvýše $1/2^{t-1}$. Sečteno a podtrženo, dokázali jsme následující větu:

**Věta:** Prvočíselný test z tohoto oddílu má při $t$ iteracích pravděpodobnost chyby nejvýše $1/2^{t-1}$.