Další moderní metody hledání netriviálního dělitele

Nejúčinnější metody:

- Lenstrova metoda eliptických křivek,
- metoda kvadratického síta,
- metoda síta v číselném tělese.

Základní myšlenka kvadratického síta i síta v číselném tělese je stejná jako základní myšlenka metody řetězových zlomků, která je historicky první metodou subexponenciálního času a byla na konci 60-tých let a v 70-tých letech hlavní používanou metodou.

Nechť N je (velké) složené přirozené číslo, které není dělitelné žádnými „malými“ prvočísly (tj. prvočísly $\leq B$) a které není mocninou prvočísla. Hledáme netriviálního dělitele čísla N.

Budeme hledat x, $y \in \mathbb{Z}$, aby platilo

$$x^2 \equiv y^2 \pmod{N} \quad \text{a přitom} \quad x \not\equiv \pm y \pmod{N}.$$

Protože $x^2 - y^2 = (x - y)(x + y)$, je jasné, že pak největší společný dělitel $(x + y, N)$ bude netriviální dělitel čísla N.

Jak hledat $x,\ y \in \mathbb{Z},\ x^2 \equiv y^2 \pmod N,\ \ x \not\equiv \pm y \pmod N$

Hledáme kongruence tvaru

$$x_k^2 \equiv (-1)^{e_{0k}} p_1^{e_{1k}} p_2^{e_{2k}} \cdots p_m^{e_{mk}} \pmod N,$$

kde p_i jsou „malá“ prvočísla a $e_{ik} \in \{0,1\}$. Nalezneme-li dostatečně mnoho takových kongruencí (tj. alespoň $n \geq m+2$), můžeme Gaussovou eliminací nad $\mathbb{F}_2$ v $m+1$-rozměrném prostoru $\mathbb{F}_2^{m+1}$ najít lineární závislost mezi n vektory $(e_{0k}, e_{1k}, \ldots, e_{mk})$, (ztotožňujeme $\{0,1\}$ s $\mathbb{F}_2$), tj. najít $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{F}_2$, ne všechna nulová, pro která je $\sum_{k=1}^n \varepsilon_k (e_{0k}, e_{1k}, \ldots, e_{mk})$ nulový vektor. Budeme-li nyní $\varepsilon_1, \ldots, \varepsilon_n$ považovat za celá čísla, pak pro každé $i \in \{0, 1, \ldots, m\}$ je číslo $v_i = \frac{1}{2} \sum_{k=1}^n \varepsilon_k e_{ik} \in \mathbb{Z}$, protože $\sum_{k=1}^n \varepsilon_k e_{ik}$ leží v jádře homomorfismu okruhů $\mathbb{Z} \to \mathbb{F}_2$.
Pak pro $x = \prod_{k=1}^n x_k^{\varepsilon_k}$, $y = p_1^{v_1} p_2^{v_2} \cdots p_m^{v_m}$, platí

$$x^2 = \prod_{k=1}^n x_k^{2\varepsilon_k} \equiv \prod_{k=1}^n \left((-1)^{e_{0k}} p_1^{e_{1k}} p_2^{e_{2k}} \cdots p_m^{e_{mk}}\right)^{\varepsilon_k} = y^2 \pmod N,$$

což nám dá netriviálního dělitele čísla N, pokud $x \not\equiv y \pmod N$.

Jak hledat $x,\ y \in \mathbb{Z},\ x^2 \equiv y^2 \pmod N,\ \ x \not\equiv \pm y \pmod N$

V případě, že liché N je dělitelné právě r prvočísly, je pravděpodobnost, že nastane $x \equiv \pm y \pmod N$ za předpokladu, že platí $x^2 \equiv y^2 \pmod N$ a $(N, xy) = 1$, rovna 2^{1-r}. Proto je vhodné volit n o něco větší než $m + 2$, abychom Gaussovou eliminací našli více závislostí.

Množina $\{p_1, \ldots, p_m\}$ se nazývá báze faktorizace. Způsoby, jak ji zvolit optimálně a jak hledat potřebné kongruence

$$x_k^2 \equiv (-1)^{e_{0k}} p_1^{e_{1k}} p_2^{e_{2k}} \cdots p_m^{e_{mk}} \pmod N,$$

se u jednotlivých metod liší. Vždy však je mezi exponenty na pravé straně kongruence jen několik jedniček.

Matice takové soustavy má tedy v každém řádku jen několik jedniček a zbytek tvoří nuly. Uložit celou tuto obrovskou „řídkou“ matici do paměti se nám patrně nepodaří. Proto je třeba Gaussovu eliminaci provádět jinak, než u malých matic.

Gaussova eliminace „řídké“ matice

Nemáme uloženou celou matici, ale pro každý řádek máme uloženy jen informace o poloze jedniček v tomto řádku.
Při provádění eliminace se rozlišuje mezi „řídkými“ a „hustými“ sloupci: hodnoty v „hustých“ sloupcích se neuchovávají, místo nich se uchovává pro každý řádek informace o tom, jak byl odvozen z původní matice (tj. kterých řádků původní matice je součtem).
Eliminace se provádí tak, že hledáme řádek, který má pouze jednu jedničku v „řídkých“ sloupcích. Ten pak přičteme ke všem řádkům, které v tomto sloupci mají jedničku. Poté už tento řádek nebudeme potřebovat. V případě, že žádný řádek, který by měl pouze jednu jedničku v „řídkých“ sloupcích, neexistuje, vybereme ten, který má jedniček co nejméně. Vybereme v něm jednu jedničku a sloupce, ve kterých jsou ostatní jedničky tohoto řádku, prohlásíme za husté. Skončíme v okamžiku, kdy už nemáme žádný řídký sloupec. Pomocí informací o odvozování řádků nyní sestavíme mnohem menší „hustou“ matici, v níž se provede Gaussova eliminace obvyklým způsobem.

Metoda řetězových zlomků

Potřebujeme hledat kongruence tvaru

$$x_k^2 \equiv (-1)^{e_{0k}} p_1^{e_{1k}} p_2^{e_{2k}} \cdots p_m^{e_{mk}} \pmod{N},$$

kde p_i jsou pevně zvolená prvočísla a $e_{ik} \in \{0, 1\}$.

Budeme vycházet z toho, že pokud zvolíme do naší báze faktorizace všechna prvočísla $p_1, \ldots, p_m$ menší než nějaká hranice a najdeme-li kongruenci $x^2 \equiv t \pmod{N}$ s „malým“ $|t|$, je reálná šance, že v rozkladu čísla $|t|$ se nevyskytují jiná prvočísla než $p_1, \ldots, p_m$ a tedy že získáme kongruenci požadovaného tvaru.

Metoda řetězových zlomků - základní myšlenka

Nechť $\frac{p}{q}$ je dobrá aproximace čísla $\sqrt{kN}$, kde k je nějaké nepříliš velké přirozené číslo nedělitelné druhou mocninou prvočísla. Pak

$$\left|\sqrt{kN} - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Označme $t = p^2 - kNq^2$. Pak $p^2 \equiv t \pmod{N}$. Nalezněme odhad pro $|t|$. Pak

$$-\frac{1}{q} < \sqrt{p^2 - t} - p < \frac{1}{q}.$$

Přičtením p, umocněním a odečtením p^2 dostaneme

$$-\frac{2p}{q} + \frac{1}{q^2} < -t < \frac{2p}{q} + \frac{1}{q^2},$$

odkud vzhledem k $\sqrt{kN} > \frac{p}{q} - \frac{1}{q^2}$ plyne

$$|t| < \frac{2p}{q} + \frac{1}{q^2} < 2\sqrt{kN} + \frac{3}{q^2}.$$

Číslo $|t|$ tedy opravdu není „velké“ a šance na získání užitečné kongruence hledaného tvaru je.

Metoda řetězových zlomků - postup

Metoda řetězových zlomků tedy dává následující algoritmus: postupně za k volíme přirozená čísla nedělitelná druhou mocninou prvočísla a pro každé takové k počítáme jistý počet dobrých aproximací $\frac{p}{q}$. Pro každou dobrou aproximaci zkoušíme rozložit číslo $|t| = |p^2 - kNq^2|$ pomocí prvočísel z báze faktorizace. Jestliže se to podaří, získáme kongruenci požadovaného tvaru.

Pokud $|t|$ není možné rozložit pomocí prvočísel z báze faktorizace, avšak platí $|t| = F \cdot U$, kde F se pomocí prvočísel z báze faktorizace rozkládá a U je (asi) prvočíslo podle testu Millera a Rabina, je vhodné uložit i trojici (p, t, U). Získáme-li totiž později ještě jinou trojici (p', t', U) se stejným U, pak z $p^2 \equiv t \pmod{N}$ a $(p')^2 \equiv t' \pmod{N}$ získáme kongruenci požadovaného tvaru $x^2 \equiv \frac{tt'}{U^2} \pmod{N}$, kde x je řešení kongruence $Ux \equiv pp' \pmod{N}$.

Lepší metoda: metoda kvadratického síta

Jiným způsobem budeme opět hledat kongruence tvaru

$$x_k^2 \equiv (-1)^{e_{0k}} p_1^{e_{1k}} p_2^{e_{2k}} \cdots p_m^{e_{mk}} \pmod{N},$$

kde p_i jsou pevně zvolená prvočísla a $e_{ik} \in \{0, 1\}$.
Označme $d = [\sqrt{N}]$ a uvažme kvadratický polynom

$$Q(x) = (x + d)^2 - N.$$

Je jasné, že $Q(a) \equiv (a + d)^2 \pmod{N}$ a že $|Q(a)|$ nebude „velké“ pro celá čísla a s „malou“ absolutní hodnotou. Ačkoli je to jednodušší metoda generování „malých“ kvadrátů modulo N než metoda řetězových zlomků, zatím není příliš zajímavá. Rozhodující důvod, proč je tato metoda rychlejší než metoda řetězových zlomků, je tento: není nutné rozkládat „malé“ kvadráty modulo N. Vzhledem k tomu, že většinu z nich rozložit nad zvolenou bází faktorizace nelze, znamená toto marné rozkládání plýtvání časem.

Metoda kvadratického síta - postup prosívání

Předpokládejme, že pro nějaké $n \in \mathbb{N}$ víme, že $n \mid Q(a)$. Pak ovšem pro každé $k \in \mathbb{Z}$ platí $n \mid Q(a + kn)$. Hledat takové a znamená řešit kongruenci $x^2 \equiv N \pmod{n}$ a vzít $a = x - d$. Přitom řešení této kongruence pro malé n není tak obtížné (pro prvočíslo n existuje Shanksův algoritmus časové náročnosti $O(\ln^4 n)$).

Jak budeme čísla prosívat: pro každé celé číslo a z velmi dlouhého intervalu uložíme do vektoru indexovaného a přibližnou hodnotu $\log_2 |Q(a)|$ (stačí $\frac{1}{2}$ plus řád první jedničky binárního zápisu, pak je chyba menší než $\frac{1}{2}$).

Pak pro všechny mocniny prvočísel $p^k \leq B$ pro zvolené B odečteme $\log_2 p$ od všech prvků v našem vektoru, jejichž index a je kongruentní modulo p^k s předem vypočteným řešením kongruence $Q(a) \equiv 0 \pmod{p^k}$, tj. $(a + d)^2 \equiv N \pmod{p^k}$. Protože předpokládáme, že $p \nmid N$, má pro lichá p tato kongruence dvě řešení, je-li N kvadratický zbytek modulo p, a žádné, jestliže je N kvadratický nezbytek modulo p – do báze faktorizace tedy dáváme kromě 2 jen ta prvočísla, pro která je N kvadratický zbytek.

Metoda kvadratického síta - vyhodnocení prosívání

Po ukončení prosívání zjistíme, pro která a není $Q(a)$ dělitelné mocninou prvočísla větší než B. Pro tato a je totiž prvek ve vektoru indexovaný a malý (kdyby logaritmy byly přesné, byla by to nula). V opačném případě zde musí být číslo větší než $\log_2 B$ (odhlédneme-li od nepřesnosti logaritmů).

Odhadněme potřebnou přesnost ε výpočtu $\log_2 p$. Označme k největší číslo ve vektoru před započetím prosívání. Pak každé číslo $|Q(a)|$ má nejvýše k činitelů. Je-li $Q(a)$ rozložitelné pomocí naší báze faktorizace, je po provedení odčítání logaritmů ve vektoru s indexem a číslo menší než $\frac{1}{2} + k\varepsilon$. Naproti tomu pro nerozložitelné $Q(a)$ dostaneme číslo větší než $(\log_2 B) - \frac{1}{2} - (k + \frac{1}{2} - \log_2 B)\varepsilon$. Stačí tedy $\varepsilon < \frac{-1+\log_2 B}{2k+\frac{1}{2}-\log_2 B}$.

Pak pro všechna a, pro které jsme dostali ve vektoru číslo menší než $\frac{1}{2} + k\varepsilon$, spočítáme znovu $Q(a)$ a rozložíme, čímž získáme kongruenci požadovaného tvaru. Máme-li dost místa v paměti, ukládáme v průběhu prosívání u každé položky a několik největších prvočísel, jejichž logaritmy odčítáme, což pak urychlí rozkládání.

Metoda kvadratického síta - možnosti vylepšení

Podobně jako u metody řetězových zlomků i v tomto případě můžeme hledat kongruence $x^2 \equiv F \cdot U \pmod{N}$, kde F se pomocí prvočísel z báze faktorizace rozkládá a U je „nepříliš velké“ číslo. V tom případě rozkládáme $Q(a)$ pro všechna a, pro které po prosívání zůstalo ve vektoru číslo menší než nějaká předem daná mez a nerozložitelný faktor spolu s a uchováváme pro případ, že by se týž faktor objevil ještě jednou.

Nevýhodou je, že na dlouhém intervalu prosívání hodnoty polynomu $Q(x)$ značně rostou a s tím i klesají naše šance na úspěšné rozložení. Mohli bychom proto vzít ještě další polynom a prosívat i jeho hodnoty, například $Q(x) = (x + [\sqrt{\ell N}])^2 - \ell N$ pro nějaké přirozené číslo ℓ nedělitelné druhou mocninou prvočísla. V tom případě bychom však museli doplnit naši bázi faktorizace: máme v ní pouze ta prvočísla p, pro která je N kvadratický zbytek modulo p, kdežto nyní potřebujeme ta, pro která je ℓN kvadratický zbytek modulo p. Ovšem zvětšení báze faktorizace znamená potřebu více kongruencí a také Gaussovu eliminaci větší matice.

Legendreův symbol

Nechť p je liché prvočíslo, $a \in \mathbb{Z}$. Legendreův symbol $(\frac{a}{p})$ (čti a vzhledem k p) definujeme takto:

$$(\tfrac{a}{p}) = \begin{cases} 0 & \text{jestliže } p \mid a, \\ 1 & \text{jestliže } p \nmid a \text{ a kongruence } x^2 \equiv a \pmod{p} \text{ má řešení}, \\ -1 & \text{jestliže } p \nmid a \text{ a kongruence } x^2 \equiv a \pmod{p} \text{ nemá řešení}. \end{cases}$$

Jestliže $(\frac{a}{p}) = 1$, nazývá se a kvadratický zbytek modulo p, jestliže $(\frac{a}{p}) = -1$, nazývá se a kvadratický nezbytek modulo p.

Zřejmě platí

$$a, b \in \mathbb{Z},\ a \equiv b \pmod{p} \quad \Rightarrow \quad (\tfrac{a}{p}) = (\tfrac{b}{p}).$$

Proto můžeme definici ekvivalentně přepsat také takto:

$$(\tfrac{a}{p}) = \begin{cases} 0 & \text{jestliže } [a]_p = [0]_p, \\ 1 & \text{jestliže } [a]_p \in \mathbb{Z}_p^\times \text{ je druhou mocninou v této grupě}, \\ -1 & \text{jestliže } [a]_p \in \mathbb{Z}_p^\times \text{ není druhou mocninou v této grupě}. \end{cases}$$

Lemma 1. *Nechť p je liché prvočíslo, $a \in \mathbb{Z}$. Pak*

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

Důkaz. Případ $p \mid a$ je zřejmý. Dále předpokládejme $p \nmid a$.

Protože grupa $\mathbb{Z}_p^\times$ je cyklická sudého řádu $p-1$, jsou druhými mocninami prvků právě mocniny generátoru se sudým exponentem. Je zde tedy $\frac{p-1}{2}$ prvků, které jsou druhé mocniny, a $\frac{p-1}{2}$ prvků, které nejsou druhé mocniny.
Každý prvek grupy $\mathbb{Z}_p^\times$ je kořenem polynomu $x^{p-1}-1$ v tělese $\mathbb{Z}_p$. Protože $x^{p-1}-1 = (x^{(p-1)/2}-1)(x^{(p-1)/2}+1)$, je každý z prvků $\mathbb{Z}_p^\times$ kořenem alespoň jednoho z obou polynomů stupně $\frac{p-1}{2}$. Protože polynom nad tělesem nemůže mít víc kořenů, než je jeho stupeň, má každý z obou polynomů $x^{(p-1)/2}-1$, $x^{(p-1)/2}+1$ právě $\frac{p-1}{2}$ kořenů.
Zřejmě každá sudá mocnina generátoru je kořenem polynomu $x^{(p-1)/2}-1$. Množina jeho kořenů se tedy skládá právě ze sudých mocnin generátoru, zatímco liché tvoří množinu kořenů polynomu $x^{(p-1)/2}+1$. Odtud plyne dokazovaná kongruence.

Důsledek 1. *Pro každé liché prvočíslo p platí* $(\frac{-1}{p}) = (-1)^{(p-1)/2}$.

Důkaz. Podle lemma 1 je $(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \pmod{p}$. Na obou stranách kongruence je ± 1, jejich rozdíl je tedy -2, 0, nebo 2. Ovšem $p \nmid 2$.

Důsledek 2. *Pro každé liché prvočíslo p a každé $a, b \in \mathbb{Z}$ platí* $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

Důkaz. Podle lemma 1 je
$(\frac{ab}{p}) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv (\frac{a}{p})(\frac{b}{p}) \pmod{p}$.
Na obou stranách kongruence je opět ± 1, proto rovnost.

Poznámka. Každé celé číslo je kongruentní modulo p s právě jedním z čísel 0, ± 1, ± 2, …, $\pm \frac{p-1}{2}$.

Lemma 2. *Nechť p je liché prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$. Pro každé $i = 1, \ldots, \frac{p-1}{2}$ nechť $a \cdot i \equiv (-1)^{e_i} \cdot b_i \pmod p$, kde $e_i \in \{0, 1\}$, $b_i \in \{1, \ldots, \frac{p-1}{2}\}$. Pak $(\frac{a}{p}) = (-1)^e$, kde $e = \sum_{i=1}^{(p-1)/2} e_i$.*

Důkaz. Víme, že $\{b_1, \ldots, b_{(p-1)/2}\} \subseteq \{1, \ldots, \frac{p-1}{2}\}$. Ukažme sporem, že zde platí rovnost. Jestliže zde není rovnost, existují $1 \leq i < j \leq \frac{p-1}{2}$ tak, že $b_i = b_j$. Pak $a \cdot i \equiv \pm a \cdot j \pmod p$, což vzhledem k $p \nmid a$ dává $i \equiv \pm j \pmod p$, a to je spor. Vynásobením kongruencí $a^{(p-1)/2} \cdot (\frac{p-1}{2})! \equiv (-1)^e \cdot (\frac{p-1}{2})! \pmod p$. Protože $p \nmid (\frac{p-1}{2})!$, plyne odtud $a^{(p-1)/2} \equiv (-1)^e \pmod p$ a lemma 1 dává $(\frac{a}{p}) \equiv (-1)^e \pmod p$. Na obou stranách je ± 1, proto rovnost.

Lemma 3. *Nechť p je liché prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$. Pak $(\frac{a}{p}) = (-1)^{\sum_{i=1}^{(p-1)/2} [\frac{2ai}{p}]}$.*

Důkaz. Platí $\frac{ai}{p} = [\frac{ai}{p}] + \langle \frac{ai}{p} \rangle$, a tedy $a \cdot i \equiv p \cdot \langle \frac{ai}{p} \rangle \pmod p$. V lemma 2 je tedy $e_i = 0$, právě když $\langle \frac{ai}{p} \rangle < \frac{1}{2}$. Odtud $e_i = [2\langle \frac{ai}{p} \rangle]$. Platí $[\frac{2ai}{p}] = [2[\frac{ai}{p}] + 2\langle \frac{ai}{p} \rangle] = 2[\frac{ai}{p}] + [2\langle \frac{ai}{p} \rangle] = 2[\frac{ai}{p}] + e_i$. Proto $(-1)^{[\frac{2ai}{p}]} = (-1)^{e_i}$. Lemma 2 dává dokazované.

Důsledek 3. *Pro každé liché prvočíslo p platí* $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Důkaz. Pro $1 \leq i \leq \frac{p-1}{2}$ platí $0 < \frac{4i}{p} < 2$, a tedy $[\frac{4i}{p}] \in \{0, 1\}$.
Přitom $[\frac{4i}{p}] = 1 \Leftrightarrow \frac{4i}{p} \geq 1 \Leftrightarrow i \geq \frac{p}{4} \Leftrightarrow i > [\frac{p}{4}]$. Proto
$\sum_{i=1}^{(p-1)/2} [\frac{4i}{p}] = \frac{p-1}{2} - [\frac{p}{4}]$.
Nechť $p = 4k \pm 1$ pro $k \in \mathbb{N}$. Pak $\frac{p-1}{2} = 2k + \frac{\pm 1 - 1}{2}$,
$[\frac{p}{4}] = k + [\frac{\pm 1}{4}]$, a tedy $\frac{p-1}{2} - [\frac{p}{4}] = k$.
Současně platí $\frac{p^2-1}{8} = \frac{16k^2 \pm 8k}{8} = 2k^2 \pm k$.
Užitím lemma 3 dostáváme $\left(\frac{2}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} [\frac{4i}{p}]} = (-1)^{(p^2-1)/8}$.

Lemma 4. *Nechť p je liché prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$, $2 \nmid a$. Pak*
$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} [\frac{ai}{p}]}$.

Důkaz. Platí $\sum_{i=1}^{(p-1)/2} i = \frac{p^2-1}{8}$. Protože je a liché, je $\frac{a+p}{2} \in \mathbb{Z}$.
Užitím lemma 3 a důsledků 3 a 2 dostáváme $(-1)^{\sum_{i=1}^{(p-1)/2} [\frac{ai}{p}]} =$
$= (-1)^{\sum_{i=1}^{(p-1)/2} [\frac{(a+p)i}{p}] - i} = \left(\frac{\frac{a+p}{2}}{p}\right) \cdot \left(\frac{2}{p}\right) = \left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.

Kvadratický zákon reciprocity

Věta 1. *Pro lichá prvočísla $p \neq q$ platí* $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Důkaz. V kartézské soustavě souřadnic si představme obdélník, jehož strany leží na osách a na přímkách $x = \frac{p}{2}$, $y = \frac{q}{2}$. Uvnitř tohoto obdélníku leží právě $\frac{p-1}{2} \cdot \frac{q-1}{2}$ mřížových bodů (tedy bodů, jejichž obě souřadnice jsou celá čísla).
Jeho úhlopříčka leží na přímce $y = \frac{q}{p}x$, žádný z mřížových bodů uvnitř obdélníku neobsahuje a rozděluje obdélník na dva trojúhelníky.
Pro pevně zvolené $i \in \{1, \ldots, \frac{p-1}{2}\}$ je uvnitř „dolního“ trojúhelníku právě $[\frac{qi}{p}]$ mřížových bodů s x-ovou souřadnicí i. Proto je uvnitř „dolního“ trojúhelníku právě $\sum_{i=1}^{(p-1)/2}[\frac{qi}{p}]$ mřížových bodů.
Ze symetrie je uvnitř „horního“ trojúhelníku právě $\sum_{i=1}^{(q-1)/2}[\frac{pi}{q}]$ mřížových bodů.
Dostali jsme $\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{i=1}^{(p-1)/2}[\frac{qi}{p}] + \sum_{i=1}^{(q-1)/2}[\frac{pi}{q}]$.
Věta nyní plyne z lemma 4.

Jacobiho symbol

Pro usnadnění počítání Legendreova symbolu $(\frac{a}{p})$ pro konkrétní hodnoty a, p tento symbol nyní zobecníme.

Nechť $b \in \mathbb{N}$ je liché číslo, $a \in \mathbb{Z}$. Je-li $b = 1$, klademe $(\frac{a}{b}) = 1$. Je-li $b > 1$, rozložíme b na součin prvočísel $b = p_1 \cdot p_2 \dots p_s$. Jacobiho symbol $(\frac{a}{b})$ pak definujeme rovností

$$(\tfrac{a}{b}) = (\tfrac{a}{p_1}) \cdot (\tfrac{a}{p_2}) \dots (\tfrac{a}{p_s}).$$

Lemma 5. *Jsou-li $b, d \in \mathbb{N}$ lichá čísla, $a, c \in \mathbb{Z}$, pak* $(\frac{ac}{bd}) = (\frac{a}{b})(\frac{c}{b})(\frac{a}{d})(\frac{c}{d})$.

Důkaz. Plyne z definice a důsledku 2.

Lemma 6. *Jsou-li $a, b \in \mathbb{N}$ lichá čísla, pak* $(-1)^{(a-1)/2}(-1)^{(b-1)/2} = (-1)^{(ab-1)/2}$.

Důkaz. Máme dokázat $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2$. Ekvivalentně $(a-1) + (b-1) \equiv ab - 1 \pmod 4$, neboli $4 \mid (a-1)(b-1)$. To však zřejmě platí.

Důsledek 4. *Pro každé liché číslo* $b \in \mathbb{N}$ *platí* $(\frac{-1}{b}) = (-1)^{(b-1)/2}$.

Důkaz. Plyne z definice, lemma 6 a důsledku 1 indukcí.

Lemma 7. *Jsou-li* $a, b \in \mathbb{N}$ *lichá čísla, pak* $(-1)^{(a^2-1)/8}(-1)^{(b^2-1)/8} = (-1)^{(a^2b^2-1)/8}$.

Důkaz. Máme dokázat $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} \pmod 2$.
Ekvivalentně $(a^2-1) + (b^2-1) \equiv a^2b^2 - 1 \pmod{16}$, neboli $16 \mid (a^2-1)(b^2-1)$. Platí dokonce $64 \mid (a^2-1)(b^2-1)$.

Důsledek 5. *Pro každé liché číslo* $b \in \mathbb{N}$ *platí* $(\frac{2}{b}) = (-1)^{(b^2-1)/8}$.

Důkaz. Plyne z definice, lemma 7 a důsledku 3 indukcí.

Věta 2. *Pro lichá nesoudělná* $a, b \in \mathbb{N}$ *platí* $(\frac{b}{a}) \cdot (\frac{a}{b}) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$.

Důkaz. Rozložme na součin prvočísel $a = p_1 \cdot p_2 \dots p_s$, $b = q_1 \cdot q_2 \dots q_t$. Z lemma 5 a věty 1 plyne užitím lemma 6

$$(\tfrac{b}{a}) \cdot (\tfrac{a}{b}) = \prod_{i=1}^{s} \prod_{j=1}^{t} (\tfrac{p_i}{q_j}) \cdot (\tfrac{q_j}{p_i}) = \prod_{i=1}^{s} \prod_{j=1}^{t} (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} =$$

$$= \prod_{j=1}^{t} \Big(\prod_{i=1}^{s} (-1)^{\frac{p_i-1}{2}} \Big)^{\frac{q_j-1}{2}} = \prod_{j=1}^{t} \Big((-1)^{\frac{a-1}{2}} \Big)^{\frac{q_j-1}{2}} =$$

$$= \Big(\prod_{j=1}^{t} (-1)^{\frac{q_j-1}{2}} \Big)^{\frac{a-1}{2}} = \Big((-1)^{\frac{b-1}{2}} \Big)^{\frac{a-1}{2}} = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}.$$

Zjednodušení vzorců

Větu 2 lze formulovat také jako rovnost

$$\left(\tfrac{a}{b}\right) = \begin{cases} \left(\tfrac{b}{a}\right) & \text{pro } a \equiv 1 \pmod 4 \text{ nebo } b \equiv 1 \pmod 4, \\ -\left(\tfrac{b}{a}\right) & \text{pro } a \equiv b \equiv 3 \pmod 4, \end{cases}$$

která platí pro každá lichá čísla $a, b \in \mathbb{N}$ (i pro soudělná, kdy je na obou stranách 0). Důsledky 4 a 5 lze formulovat takto:

$$\left(\tfrac{-1}{b}\right) = \begin{cases} 1 & \text{pro } b \equiv 1 \pmod 4, \\ -1 & \text{pro } b \equiv 3 \pmod 4, \end{cases} \qquad \left(\tfrac{2}{b}\right) = \begin{cases} 1 & \text{pro } b \equiv \pm 1 \pmod 8, \\ -1 & \text{pro } b \equiv \pm 3 \pmod 8. \end{cases}$$

Výhoda výše uvedených rovností oproti původním je v tom, že je vidět, že není nutné počítat hodnoty zlomků $\frac{a-1}{2}$, $\frac{b-1}{2}$ a $\frac{b^2-1}{8}$.

Výpočet hodnoty Jacobiho, a tedy i Legendreova symbolu

Algoritmus (Jacobiho symbol). *Pro daná* $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $2 \nmid b$, $(a, b) = 1$, *algoritmus najde hodnotu Jacobiho symbolu* $(\frac{a}{b})$.

1. *[Inicializace] Je-li* $a > 0$, *polož* $k \leftarrow 1$. *Je-li* $a < 0$, *polož* $k \leftarrow (\frac{-1}{b})$, $a \leftarrow -a$.
2. *[Jsi hotov?] Je-li* $b = 1$, *pak vytiskni* k *jako odpověď a skonči.*
3. *[Euklidovský krok] Polož* $r \leftarrow a \bmod b$, $u \leftarrow 0$. *Dokud je* r *sudé, opakuj* $r \leftarrow \frac{r}{2}$, $u \leftarrow u + 1$. *Je-li* u *liché, polož* $k \leftarrow k \cdot (\frac{2}{b})$.
4. *[Zde je již* r *liché] Polož* $a \leftarrow b$, $b \leftarrow r$. *Jestliže platí* $a \equiv b \equiv 3 \pmod 4$, *polož* $k \leftarrow -k$. *Jdi na 2.*

Vzhledem k podobnosti s Euklidovým algoritmem víme, že se tento algoritmus vždy zastaví a že je kvadratické časové náročnosti (avšak s jinou O-konstantou než Euklidův algoritmus). Zbývá dokázat, že dává správný výsledek. Ukažme, že vždy na začátku kroku 3 je $k \cdot (\frac{a}{b})$ rovno hledané hodnotě Jacobiho symbolu. To zřejmě platí, když jsme na začátku kroku 3 poprvé.

Důkaz správnosti algoritmu

Algoritmus (Jacobiho symbol). *Pro daná $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $2 \nmid b$, $(a, b) = 1$, algoritmus najde hodnotu Jacobiho symbolu $(\frac{a}{b})$.*

1. *[Inicializace] Je-li $a > 0$, polož $k \leftarrow 1$. Je-li $a < 0$, polož $k \leftarrow (\frac{-1}{b})$, $a \leftarrow -a$.*
2. *[Jsi hotov?] Je-li $b = 1$, pak vytiskni k jako odpověď a skonči.*
3. *[Euklidovský krok] Polož $r \leftarrow a \bmod b$, $u \leftarrow 0$. Dokud je r sudé, opakuj $r \leftarrow \frac{r}{2}$, $u \leftarrow u + 1$. Je-li u liché, polož $k \leftarrow k \cdot (\frac{2}{b})$.*
4. *[Zde je již r liché] Polož $a \leftarrow b$, $b \leftarrow r$. Jestliže platí $a \equiv b \equiv 3 \pmod 4$, polož $k \leftarrow -k$. Jdi na 2.*

Po provedení kroku 3 je nová hodnota $r' \equiv a \pmod b$, poté je spočítáno $r'' = r' \cdot 2^{-u}$, $k' = k \cdot (\frac{2}{b})^u$.

V kroku 4 je $a' = b$, $b' = r''$, $k'' = k' \cdot (-1)^{\frac{a'-1}{2} \cdot \frac{b'-1}{2}}$. Pak platí $k'' \cdot (\frac{a'}{b'}) = k' \cdot (-1)^{\frac{a'-1}{2} \cdot \frac{b'-1}{2}} \cdot (\frac{a'}{b'}) = k' \cdot (-1)^{\frac{b-1}{2} \cdot \frac{r''-1}{2}} \cdot (\frac{b}{r''}) = k' \cdot (\frac{r''}{b}) =$ $= k \cdot (\frac{2}{b})^u \cdot (\frac{r''}{b}) = k \cdot (\frac{2^u r''}{b}) = k \cdot (\frac{r'}{b}) = k \cdot (\frac{a}{b})$. Hodnota $k \cdot (\frac{a}{b})$ je tedy na začátku kroku 3 skutečně stejná, jako byla minule.

Metoda kvadratického síta s více polynomy

Pro obecný kvadratický polynom $Q(x) = Ax^2 + 2Bx + C$ takový, že $A \in \mathbb{N}$, $B, C \in \mathbb{Z}$, platí $AQ(x) = (Ax + B)^2 - (B^2 - AC)$. Pokud bude splněno $N \mid B^2 - AC$, pro každé $a \in \mathbb{Z}$ dostaneme kongruenci tvaru $AQ(a) \equiv (Aa + B)^2 \pmod{N}$.

Zvolíme délku $2M$ intervalu; protože chceme, aby maximum funkce $|Q(x)|$ na intervalu prosívání bylo co nejmenší, zvolíme interval $I = (-\frac{B}{A} - M, -\frac{B}{A} + M)$ a chceme $Q(-\frac{B}{A} + M) \doteq -Q(-\frac{B}{A})$, tj. $A^2M^2 \doteq 2(B^2 - AC)$, tedy $A \doteq \frac{\sqrt{2(B^2-AC)}}{M}$. Potom platí

$$\max_{x \in I} |Q(x)| \doteq |Q(-\tfrac{B}{A})| = \tfrac{B^2-AC}{A} \doteq M\sqrt{\tfrac{B^2-AC}{2}}.$$

Protože toto číslo potřebujeme mít co nejmenší, ale současně má být $B^2 - AC$ dělitelné číslem N, je vhodné volit A, B, C tak, aby $B^2 - AC = N$, kdy maximum $|Q(x)|$ na I bude zhruba $M\sqrt{\frac{N}{2}}$.

Volba koeficientů polynomu $Q(x) = Ax^2 + 2Bx + C$

Nejdříve zvolíme délku prosívání M. Pak zvolíme A blízko $\frac{\sqrt{2N}}{M}$ tak, aby A bylo prvočíslo a N byl kvadratický zbytek modulo A.

Pak nalezneme B tak, aby $B^2 \equiv N \pmod{A}$.

Nakonec položíme $C = \frac{B^2 - N}{A}$. Pak tedy skutečně $N = B^2 - AC$.

Dále pokračujeme stejně jako v metodě kvadratického síta – pro každou mocninu p^k prvočísla p menší než nějaká předem daná hranice určíme kořen a_{p^k} kongruence $x^2 \equiv N \pmod{p^k}$, má-li tato kongruence řešení (pro lichá p to znamená, že N je kvadratický zbytek modulo p), ostatní prvočísla ignorujeme. Čísla a_{p^k} spočítáme pro všechny polynomy jen jednou a uschováme.

Protože $AQ(x) = (Ax + B)^2 - N$, pak kořeny polynomu $Q(x)$ modulo p^k vyhovují kongruenci $Ax \equiv -B \pm a_{p^k} \pmod{p^k}$.

V bázi faktorizace pak máme -1, 2, všechna lichá prvočísla p až do zvolené hranice taková, že N je kvadratický zbytek modulo p, a konečně pro každý použitý polynom $Q(x)$ jeho koeficient A.

Vlastní algoritmus

Postupně prosíváme hodnoty jednoho polynomu $Q(x)$ po druhém, dokud nezískáme dostatek kongruencí pro Gaussovu eliminaci.

Protože malá prvočísla dělí hodně hodnot $Q(x)$, trvá prosívání malými prvočísly nejdéle, přičemž jejich logaritmus je malý. Proto se v některých implementacích prosívání malými prvočísly (řekněme menšími než 100) vynechává, jen je nutné zvýšit hranici, používanou po skončení prosívání pro rozhodování, zda dotyčnou hodnotu polynomu $Q(x)$ budeme rozkládat nebo ne. Přitom strategie je taková: raději zkusit rozkládat nerozložitelné $Q(x)$, než ztratit některé rozložitelné, a tedy nějakou užitečnou kongruenci.

Vzhledem k tomu, že získané kongruence je snadné kontrolovat, je možné do generování kongruencí zapojit více lidí tak, že pomocí e-mailu je jim distribuován program s daty, který nechají běžet ve volném čase na svém počítači, a získané výsledky opět vracejí e-mailem.

Příklad použití metody distribuovaného počítání

Metoda distribuovaného počítání e-maily s následnou kontrolou vrácených výsledků byla s úspěchem použita při rozkládání devátého Fermatova čísla $N = 2^{2^9} + 1$ v roce 1990 (toto N má 155 dekadických cifer).

A. K. Lenstra, H. W. Lenstra, M. S. Manasse a J. M. Pollard tímto způsobem získali matici o 226 688 řádcích a 199 203 sloupcích. Po „zahuštění“ této matice získali matici o 72 413 řádcích a 72 213 sloupcích. Gaussovou eliminací této matice pak získali kongruenci, která jim určila netriviálního dělitele čísla N.

Nepoužili metodu kvadratického síta s více polynomy, ale metodu síta v číselném tělese. Tato metoda je založena na výsledcích algebraické teorie čísel, je tedy z námi studovaných metod teoreticky nejnáročnější, a proto se jí budeme věnovat až do konce semestru.