

Legendreův symbol

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

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

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

Zřejmě platí

$$a, b \in \mathbb{Z}, a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Proto můžeme definici ekvivalentně přepsat také takto:

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

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

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

Důkaz. Příklad $p \mid a$ 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 $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Důkaz. Podle lemma 1 je $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. 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 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

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

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

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

Důkaz. Víme, že $\{b_1, \dots, b_{(p-1)/2}\} \subseteq \{1, \dots, \frac{p-1}{2}\}$. 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 $a^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^e \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$. Protože $p \nmid \left(\frac{p-1}{2}\right)!$, plyne odtud $a^{(p-1)/2} \equiv (-1)^e \pmod{p}$ a lemma 1 dává $\left(\frac{a}{p}\right) \equiv (-1)^e \pmod{p}$. Na obou stranách je ± 1 , proto rovnost.

Lemma 3. Necht p je liché prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$. Pak

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} \left[\frac{2ai}{p}\right]}$$

Důkaz. Platí $\frac{ai}{p} = \left[\frac{ai}{p}\right] + \left\langle \frac{ai}{p} \right\rangle$, a tedy $a \cdot i \equiv p \cdot \left\langle \frac{ai}{p} \right\rangle \pmod{p}$.

V lemma 2 je tedy $e_i = 0$, právě když $\left\langle \frac{ai}{p} \right\rangle < \frac{1}{2}$. Odtud $e_i = \left[2\left\langle \frac{ai}{p} \right\rangle\right]$.

Platí $\left[\frac{2ai}{p}\right] = \left[2\left[\frac{ai}{p}\right] + 2\left\langle \frac{ai}{p} \right\rangle\right] = 2\left[\frac{ai}{p}\right] + \left[2\left\langle \frac{ai}{p} \right\rangle\right] = 2\left[\frac{ai}{p}\right] + e_i$. Proto

$(-1)^{\left[\frac{2ai}{p}\right]} = (-1)^{e_i}$. 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 $\left[\frac{4i}{p}\right] \in \{0, 1\}$.

Přitom $\left[\frac{4i}{p}\right] = 1 \Leftrightarrow \frac{4i}{p} \geq 1 \Leftrightarrow i \geq \frac{p}{4} \Leftrightarrow i > \left[\frac{p}{4}\right]$. Proto

$$\sum_{i=1}^{(p-1)/2} \left[\frac{4i}{p}\right] = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

Nechť $p = 4k \pm 1$ pro $k \in \mathbb{N}$. Pak $\frac{p-1}{2} = 2k + \frac{\pm 1 - 1}{2}$,

$\left[\frac{p}{4}\right] = k + \left[\frac{\pm 1}{4}\right]$, a tedy $\frac{p-1}{2} - \left[\frac{p}{4}\right] = k$.

Současně platí $\frac{p^2-1}{8} = \frac{16k^2 \pm 8k}{8} = 2k^2 \pm k$.

Užitím lemma 3 dostáváme $\left(\frac{2}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} \left[\frac{4i}{p}\right]} = (-1)^{(p^2-1)/8}$.

Lemma 4. Nechť p je liché prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$, $2 \nmid a$. Pak

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} \left[\frac{ai}{p}\right]}.$$

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 $(-1)^{\sum_{i=1}^{(p-1)/2} \left[\frac{ai}{p}\right]} = (-1)^{\sum_{i=1}^{(p-1)/2} \left[\frac{(a+p)i}{p}\right] - i} = \left(\frac{a+p}{p}\right) \cdot \left(\frac{2}{p}\right) = \left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.

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 $i \in \{1, \dots, \frac{p-1}{2}\}$ je uvnitř „dolního“ trojúhelníku právě $\left[\frac{qi}{p}\right]$ mřížových bodů s x -ovou souřadnicí i . Proto je

uvnitř „dolního“ trojúhelníku právě $\sum_{i=1}^{(p-1)/2} \left[\frac{qi}{p}\right]$ mřížových bodů.

Ze symetrie je uvnitř „horního“ trojúhelníku právě $\sum_{i=1}^{(q-1)/2} \left[\frac{pi}{q}\right]$ mřížových bodů.

Dostali jsme $\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{i=1}^{(p-1)/2} \left[\frac{qi}{p}\right] + \sum_{i=1}^{(q-1)/2} \left[\frac{pi}{q}\right]$.

Věta nyní plyne z lemma 4.

Jacobiho symbol

Pro usnadnění počítání Legendreova symbolu $\left(\frac{a}{p}\right)$ 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 $\left(\frac{a}{b}\right) = 1$. Je-li $b > 1$, rozložíme b na součin prvočísel $b = p_1 \cdot p_2 \cdot \dots \cdot p_s$. Jacobiho symbol $\left(\frac{a}{b}\right)$ pak definujeme rovností

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \dots \cdot \left(\frac{a}{p_s}\right).$$

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

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 $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$.

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

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 $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$.

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

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

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

Zjednodušení vzorců

Větu 2 lze formulovat také jako rovnost

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

kteřá 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:

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

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 $\left(\frac{a}{b}\right)$.

1. [Inicializace] Je-li $a > 0$, polož $k \leftarrow 1$. Je-li $a < 0$, polož $k \leftarrow \left(\frac{-1}{b}\right)$, $a \leftarrow -a$.
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 $k \leftarrow k \cdot \left(\frac{2}{b}\right)$.
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 $k \cdot \left(\frac{a}{b}\right)$ 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

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

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.