Hledání netriviálního dělitele pomocí eliptických křivek

Mějme opět dáno složené přirozené číslo N, které chceme rozložit. Je přirozené předpokládat, že $(N, 6) = 1$. Zvolme a, $b \in \mathbb{Z}$ tak, aby $(4a^3 + 27b^2, N) = 1$. Pak rovnice

$$y^2 z = x^3 + axz^2 + bz^3$$

nám určuje „eliptickou křivku“ $(\mathcal{E}, O)$ nad $\mathbb{Z}_N$, přičemž $O = [0, 1, 0] \in P^2(\mathbb{Z}_N)$. Nechť p je nějaké (neznámé) prvočíslo dělící N. Předchozí rovnicí je zadána eliptická křivka $(\mathcal{E}_p, O_p)$, přičemž $O_p = [0, 1, 0] \in P^2(\mathbb{F}_p)$.

Připomeňme, že $(\mathcal{E}_p, +)$ je komutativní grupa a podle Hasseovy věty platí $|\mathcal{E}_p| = p + 1 - a_p$, kde celé číslo a_p splňuje $|a_p| < 2\sqrt{p}$.

Na množině $\mathcal{E}$ máme definovánu částečnou operaci $+$, přičemž kdykoli známe nějaké body $P = [\alpha_1, \beta_1, 1]$, $Q = [\alpha_2, \beta_2, 1] \in \mathcal{E}$ takové, že $P + Q$ není definováno, snadno najdeme netriviálního dělitele čísla N.

Navíc existuje částečný homomorfismus $f_p : \mathcal{E} \to \mathcal{E}_p$ takový, že jestliže je pro P, $Q \in \mathcal{E}$ definováno $P + Q$, pak platí $f_p(P + Q) = f_p(P) + f_p(Q)$.

Lenstrova metoda eliptických křivek

Představme si, že známe nějaký bod $P = [\alpha, \beta, 1] \in \mathcal{E}$ a že $|\mathcal{E}_p|$ je B-hladké pro nějaké nepříliš velké přirozené číslo B.
Označme L_B nejmenší společný násobek čísel $1, 2, \ldots, B$.
Pak ovšem $|\mathcal{E}_p| \mid L_B$ a platí tedy $L_B \cdot f_p(P) = O_p$.
Předpokládejme, že je definováno $L_B \cdot P$ (přitom si při provádění algoritmu budeme přát samozřejmě opak).
Pak musí pro $L_B \cdot P = [\alpha', \beta', \gamma']$ platit $p \mid \alpha'$, $p \mid \beta' - 1$, $p \mid \gamma'$.
Protože naše vzorce pro sčítání bodů ve třetí složce dávají vždy 0 nebo 1, musí platit $L_B \cdot P = O$. To ale znamená, že $L_B \cdot f_q(P) = O_q$ pro každé prvočíslo $q \mid N$.
Přitom budeme $L_B \cdot P$ počítat postupně „donásobováním“ jednotlivými prvočísly z rozkladu L_B, a tedy každý mezivýsledek musí mít ve třetí složce buď 0 nebo 1.
Protože donásobování prvočísly dělícími L_B provádíme podle velikosti od nejmenších k největším, pokud je $L_B \cdot P$ definováno, musí být největší prvočíslo dělící řád r_q bodu $f_q(P)$ v grupě $(\mathcal{E}_q, +)$ pro všechna prvočísla $q|N$ stejné.
To je ale značně nepravděpodobné.

Lenstrova metoda eliptických křivek - volba parametrů

Proto lze čekat, že pokud pro zvolené nepříliš velké přirozené číslo B platí, že $|\mathcal{E}_p|$ je B-hladké pro nějaké prvočíslo p dělící N, s velkou pravděpodobností najdeme zmíněným postupem netriviálního dělitele čísla N.

Problémem zůstává, že pro zvolené číslo B nemusí $|\mathcal{E}_p|$ být B-hladké pro žádné prvočíslo p dělící N, což objevíme až poté, co spočítáme $L_B \cdot P$. V tomto případě zvolíme jiná a, b a celý postup znovu zopakujeme.

Zbývá vyjasnit několik věcí: jak volit a, b, jak najít $P \in \mathcal{E}$ a jak zvolit přirozené číslo B.

Nelze zvolit a, b náhodně a bod P najít jako nějaké řešení kongruence $y^2 \equiv x^3 + ax + b \pmod{N}$, tj. pro zvolené x nalézt y. Protože N není prvočíslo, řešit kvadratickou kongruenci modulo N je příliš obtížné (ze znalosti všech řešení takové kongruence bychom snadno spočítali netriviálního dělitele čísla N).

Proto zvolíme jiný postup: položíme $b = 1$, $P = [0, 1, 1]$ a volíme pouze a. Jistě potom $P \in \mathcal{E}$.

Lenstrova metoda eliptických křivek - volba parametrů

Otázkou zůstává jak volit B. Protože pro menší p je také menší $|\mathcal{E}_p|$, vzhledem k tomu, že menší čísla jsou s větší pravděpodobností B-hladká než velká, je metoda citlivá spíše na velikost p než na velikost N. Proto je nutno zvolit B tak velké, jak velká prvočísla jsme ještě ochotni hledat (nebo lépe, kolik času jsme ochotni hledání věnovat). Analýza pomocí odhadu pravděpodobnosti toho, že číslo jisté velikosti je B-hladké, ukazuje, že pro hledání prvočísel do velikosti v je vhodné volit B tak, aby $\ln B \doteq \sqrt{\frac{1}{2} \ln v \ln \ln v}$. Speciálně tedy, pro hledání prvočísel menších než 10^{20} je vhodnou hodnotou $B = 12\,000$ (přičemž očekáváme, že bude potřeba projít zhruba 12 000 eliptických křivek, než najdeme p).

Podobně jako u Pollardovy $p - 1$ metody je vhodné i zde doplnit druhé stadium spočívající v tom, že předpokládáme, že $|\mathcal{E}_p|$ je B_1-hladký násobek prvočísla menšího než B_2. Toto druhé stadium je zcela analogické jako u Pollardovy metody, proto si uvedeme algoritmus jen pro první stadium.

Algoritmus (Lenstrova metoda el. křivek, 1. stadium). *Dáno složené N nesoudělné s 6 a hranice B, hledáme netriviálního dělitele N. Máme tabulku $p[1], p[2], \ldots, p[k]$ všech prvočísel $\leq B$.*

1. *[Inicializace] Polož $a \leftarrow 0$.*
2. *[Inicializace křivky] Označme $(\mathcal{E}, O)$ křivku danou rovnicí $y^2z = x^3 + axz^2 + z^3$, kde $O = [0, 1, 0]$. Polož $P = [0, 1, 1]$, $i \leftarrow 0$.*
3. *[Další prvočíslo] Polož $i \leftarrow i + 1$. Je-li $i > k$, polož $a \leftarrow a + 1$ a jdi na 2. Jinak polož $q \leftarrow p[i]$, $r \leftarrow q$, $\ell \leftarrow [\frac{B}{q}]$, $R \leftarrow P$.*
4. *[Násob bod na křivce] Dokud $r \leq \ell$, opakuj $r \leftarrow q \cdot r$. Pak zkus spočítat $P \leftarrow r \cdot P$ na křivce $(\mathcal{E}, O)$. Pokud se to nepodařilo (tj. v průběhu výpočtu byl objeven nenulový prvek okruhu $\mathbb{Z}_N$, který není invertibilní), vytiskni získaného netriviálního dělitele N a skonči. Jinak (tj. P byl vypočten), je-li $P \neq O$, jdi na 3.*
5. *[Počítej znovu] Dokud nebude $R = O$, opakovaně zkoušej spočítat $R \leftarrow q \cdot R$ (pokud se to nepodaří, vytiskni získaného netriviálního dělitele N a skonči). Nakonec polož $a \leftarrow a + 1$ a jdi na 2.*

Dobré aproximace reálných čísel

Definice. Pro libovolné reálné číslo α nechť $\langle\alpha\rangle$ značí necelou část čísla α, to znamená $\alpha - \langle\alpha\rangle \in \mathbb{Z}$ a $0 \leq \langle\alpha\rangle < 1$.

Pro celou část $[\alpha]$ reálného čísla α tedy platí $[\alpha] = \alpha - \langle\alpha\rangle$.

Definice. Pro libovolné reálné číslo α nechť $\|\alpha\|$ je vzdálenost α od nejbližšího celého čísla, tj.

$$\|\alpha\| = \min\{|\alpha - n|;\ n \in \mathbb{Z}\}.$$

Definice. Nechť $\theta \in \mathbb{R}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$, přičemž $(p, q) = 1$.
Racionální číslo $\frac{p}{q}$ se nazývá dobrá aproximace čísla θ, jestliže $\|q\theta\| = |q\theta - p|$ a pro všechna $q' \in \mathbb{N}$, $q' < q$ platí $\|q'\theta\| > \|q\theta\|$.

Příklad. Platí $\|\pi\| \doteq 0.141593$, $\|2\pi\| \doteq 0.283185$,
$\|3\pi\| \doteq 0.424778$, $\|4\pi\| \doteq 0.433629$, $\|5\pi\| \doteq 0.292037$,
$\|6\pi\| \doteq 0.150444$, $\|7\pi\| \doteq 0.008851$, $\|8\pi\| \doteq 0.132741$,
$\|9\pi\| \doteq 0.274334$. Proto jsou 3 a $\frac{22}{7}$ dobré aproximace čísla π.
Další dobrá aproximace $\frac{333}{106}$ pochází z $\|106\pi\| \doteq 0.008821$.

Věta 1. *Nechť $\theta \in \mathbb{R}$, $Q \in \mathbb{R}$, $Q > 1$. Pak existuje $q \in \mathbb{N}$, $q < Q$ s vlastností $\|q\theta\| \leq \frac{1}{Q}$. Jestliže navíc $\theta \notin \mathbb{Q}$ anebo $Q \notin \mathbb{N}$, existuje $q \in \mathbb{N}$ tak, že $q < Q$, $\|q\theta\| < \frac{1}{Q}$.*

Důkaz. Nejprve budeme předpokládat $Q \in \mathbb{N}$. Uvažme $Q+1$ čísel 0, 1, $\langle\theta\rangle$, $\langle 2\theta\rangle$, $\ldots$, $\langle(Q-1)\theta\rangle$ a rozdělme je do Q intervalů $[0, \frac{1}{Q})$, $[\frac{1}{Q}, \frac{2}{Q})$, $\ldots$, $[\frac{Q-1}{Q}, 1]$. Z Dirichletova principu plyne, že alespoň jeden interval obsahuje aspoň dvě čísla, tedy existují $r_1, r_2, s_1, s_2 \in \mathbb{Z}$ taková, že $0 \leq r_1 < r_2 < Q$ s vlastností $|(r_1\theta - s_1) - (r_2\theta - s_2)| \leq \frac{1}{Q}$. Položme $q = r_2 - r_1$, pak $\|q\theta\| \leq \frac{1}{Q}$. Jestliže $Q \notin \mathbb{N}$, plyne věta z platnosti věty pro $[Q]+1$.

Poznámka. Ukážeme si, že z předchozí věty plyne, že pro libovolné $\theta \in \mathbb{R} - \mathbb{Q}$ existuje nekonečně mnoho $q \in \mathbb{N}$ splňujících

$$q \cdot \|q\theta\| < 1. \tag{1}$$

Ve skutečnosti je možné dokonce dokázat více: číslo 1 na pravé straně může být nahrazeno číslem $\frac{1}{\sqrt{5}}$. Toto silnější tvrzení však nebudeme dokazovat.

Konstrukce posloupnosti dobrých aproximací čísla θ

Zvolme pevně $\theta \in \mathbb{R} - \mathbb{Q}$. Sestrojme indukcí posloupnost všech dobrých aproximací čísla θ. Jistě $q_1 = 1$ dává dobrou aproximaci $\frac{p_1}{q_1}$ čísla θ spolu s nějakým $p_1 \in \mathbb{Z}$ a platí $|q_1\theta - p_1| = \|\theta\| < \frac{1}{2}$. Protože $2\theta \notin \mathbb{Z}$, je touto rovností p_1 určeno jednoznačně. Zřejmě $(q_1, p_1) = 1$.

Předpokládejme, že pro nějaké $n \in \mathbb{N}$ máme dobrou aproximaci $\frac{p_n}{q_n}$ čísla θ. Protože $\theta \notin \mathbb{Q}$, je $\|q_n\theta\| \neq 0$ a věta 1 s $Q = \|q_n\theta\|^{-1}$ zaručuje existenci $q \in \mathbb{N}$, které splňuje $\|q\theta\| < \|q_n\theta\|$. Nechť q_{n+1} je nejmenší q s touto vlastností a $p_{n+1} \in \mathbb{Z}$ je určeno podmínkou $\|q_{n+1}\theta\| = |q_{n+1}\theta - p_{n+1}|$. Je tedy $\|q_{n+1}\theta\| < \|q_n\theta\|$ a pro všechna pro všechna $q \in \mathbb{N}$, $q < q_{n+1}$ platí $\|q\theta\| \geq \|q_n\theta\|$; je tedy $\frac{p_{n+1}}{q_{n+1}}$ dobrá aproximace čísla θ. Protože $\frac{p_n}{q_n}$ je také dobrá aproximace čísla θ, platí $q_{n+1} > q_n$. Kdyby $t = (q_{n+1}, p_{n+1}) > 1$, pak by $p' = \frac{p_{n+1}}{t} \in \mathbb{Z}$, $q' = \frac{q_{n+1}}{t} \in \mathbb{N}$, $q' < q_{n+1}$, přitom
$\|q_{n+1}\theta\| = |q_{n+1}\theta - p_{n+1}| = t|q'\theta - p'| \geq t\|q'\theta\| > \|q'\theta\|$,
což by byl spor s definicí q_{n+1}. Je tedy $(q_{n+1}, p_{n+1}) = 1$.

Vlastnosti posloupnosti dobrých aproximací čísla θ

Dostali jsme posloupnost přirozených čísel

$$1 = q_1 < q_2 < q_3 < \dots \tag{2}$$

a celých čísel $p_1,\ p_2,\ p_3,\ \dots$ splňujících $(p_n, q_n) = 1$ a

$$\|q_n\theta\| = |q_n\theta - p_n|, \tag{3}$$

$$\|q_{n+1}\theta\| < \|q_n\theta\|, \tag{4}$$

$$\|q\theta\| \geq \|q_n\theta\| \quad \text{pro všechna } q \in \mathbb{N},\ q < q_{n+1}. \tag{5}$$

Z věty 1 pro $Q = q_{n+1}$ dostaneme existenci $q \in \mathbb{N}$, $q < q_{n+1}$, takového, že $\|q\theta\| \leq \frac{1}{q_{n+1}}$. Podle (5) platí

$$q_n\|q_n\theta\| < q_{n+1}\|q_n\theta\| \leq 1. \tag{6}$$

Kdyby čísla $q_{n+1}\theta - p_{n+1}$ a $q_n\theta - p_n$ měla stejná znaménka, pro $p' = p_{n+1} - p_n$, $0 < q' = q_{n+1} - q_n < q_{n+1}$, bychom dostali $|q'\theta - p'| < |q_n\theta - p_n| = \|q_n\theta\|$, což by byl spor s (5). Proto

$$(q_n\theta - p_n)(q_{n+1}\theta - p_{n+1}) < 0. \tag{7}$$

Lemma 1. $\{\frac{p_n}{q_n};\, n \in \mathbb{N}\}$ *je množina všech dobrých aproximací a platí* $\lim_{n\to\infty} \frac{p_n}{q_n} = \theta$.

Důkaz. První část plyne z konstrukce, druhá z (6), neboť $|\theta - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$.

Lemma 2. $q_{n+1}p_n - q_n p_{n+1} = \pm 1$.

Důkaz. Levá strana je celé číslo a platí

$$q_{n+1}p_n - q_n p_{n+1} = q_n(q_{n+1}\theta - p_{n+1}) - q_{n+1}(q_n\theta - p_n), \qquad (8)$$

odkud spolu s (3), (4), (6) a (7) plyne

$$0 < q_n\|q_{n+1}\theta\| + q_{n+1}\|q_n\theta\| = |q_{n+1}p_n - q_n p_{n+1}| < 2q_{n+1}\|q_n\theta\| \le 2.$$

Důsledek. *Číslo* $q_{n+1}p_n - q_n p_{n+1}$ *má opačné znaménko než* $q_n\theta - p_n$ *a platí* $q_{n+1}p_n - q_n p_{n+1} = -(q_n p_{n-1} - q_{n-1}p_n)$.

Důkaz. Plyne z (8) s přihlédnutím k (3), (4) a $q_{n+1} > q_n$, druhá část z (7) a lemmatu 2.

Lemma 3. *Pro libovolné $n \geq 2$ existuje $a_n \in \mathbb{N}$ tak, že*

$$q_{n+1} = a_n q_n + q_{n-1}, \tag{9}$$

$$p_{n+1} = a_n p_n + p_{n-1}, \tag{10}$$

$$|q_{n-1}\theta - p_{n-1}| = a_n |q_n\theta - p_n| + |q_{n+1}\theta - p_{n+1}|. \tag{11}$$

Důkaz. Z důsledku dostáváme $p_n(q_{n+1} - q_{n-1}) = q_n(p_{n+1} - p_{n-1})$. Protože $(q_n, p_n) = 1$, plyne odtud existence celého čísla a_n s vlastností $q_{n+1} - q_{n-1} = a_n q_n$, $p_{n+1} - p_{n-1} = a_n p_n$. Protože $q_{n+1} > q_{n-1}$, je $a_n > 0$. Konečně, (11) plyne z (9) a (10) díky (7).

Poznámka. Z (11) pro každé $n \geq 2$ plyne

$$a_n = \left[\frac{|q_{n-1}\theta - p_{n-1}|}{|q_n\theta - p_n|}\right] = \left[\frac{\|q_{n-1}\theta\|}{\|q_n\theta\|}\right]. \tag{12}$$

Známe-li tedy p_1, p_2, q_1, q_2 a θ, můžeme pomocí (12), (9) a (10) dopočítat všechny dobré aproximace iracionálního čísla θ.
Pro $\theta \in \mathbb{Q}$, $2\theta \notin \mathbb{Z}$, probíhá celý proces stejně až do okamžiku, kdy $\|q_n\theta\| = 0$, tj. $\frac{p_n}{q_n} = \theta$, kdy se proces konstrukce dobrých aproximací zastaví. Pro $\theta \in \mathbb{Q} - \frac{1}{2}\mathbb{Z}$ tedy dostáváme konečně mnoho dobrých aproximací, z nichž poslední je rovna θ.

Věta. *Nechť $\theta \in \mathbb{R}$, $2\theta \notin \mathbb{Z}$. Generujme rekurentně celá čísla p_n, q_n, a_n; nejprve položme*

$$p_0 = 1, \qquad q_0 = 0,$$
$$p_1 = [\theta], \qquad q_1 = 1.$$

Pro každé $n \in \mathbb{N}$ takové, že $q_n\theta \neq p_n$, pokračujme

$$\begin{aligned} a_n &= \left[\frac{|q_{n-1}\theta - p_{n-1}|}{|q_n\theta - p_n|}\right] \\ p_{n+1} &= a_n p_n + p_{n-1}, \\ q_{n+1} &= a_n q_n + q_{n-1}. \end{aligned}$$

Pak všechny dobré aproximace čísla θ jsou právě získaná čísla $\frac{p_n}{q_n}$ pro $n \geq 1$, je-li $a_1 > 1$, resp. pro $n \geq 2$, je-li $a_1 = 1$. Navíc platí

$$(-1)^n(q_n\theta - p_n) \leq 0, \tag{13}$$
$$q_{n+1}p_n - q_n p_{n+1} = (-1)^n. \tag{14}$$

Ve studijním textu je uveden *důkaz této věty* i její použití pro *důkaz Lehmannovy věty*.