Užití věty Pocklingtona a Lehmera

Věta. *Nechť N je přirozené číslo, $N > 1$. Nechť p je prvočíslo dělící $N - 1$. Předpokládejme dále, že existuje $a_p \in \mathbb{Z}$ tak, že*

$$a_p^{N-1} \equiv 1 \pmod{N} \quad a \quad \left(a_p^{\frac{N-1}{p}} - 1, N\right) = 1. \tag{1}$$

Nechť p^{α_p} je nejvyšší mocnina p dělící $N - 1$. Pak pro každý kladný dělitel d čísla N platí $d \equiv 1 \pmod{p^{\alpha_p}}$.

Důsledek. *Nechť $N \in \mathbb{N}$, $N > 1$. Předpokládejme, že můžeme psát $N - 1 = F \cdot U$, kde $(F, U) = 1$ a $F > \sqrt{N}$, přičemž známe rozklad čísla F na prvočinitele. Pak platí:*

- *jestliže pro každé prvočíslo $p \mid F$ můžeme najít $a_p \in \mathbb{Z}$ splňující (1) z předchozí věty, pak je N prvočíslo;*
- *je-li N prvočíslo, pak pro libovolné prvočíslo $p \mid N - 1$ existuje $a_p \in \mathbb{Z}$ splňující (1), například primitivní kořen modulo N;*
- *nalezneme-li $1 < a_p < N$ tak, že $a_p^{N-1} \not\equiv 1 \pmod{N}$, je N složené.*

Zesílení užití věty Pocklingtona a Lehmera

Důsledek. *Nechť $N \in \mathbb{N}$, $N > 1$. Předpokládejme, že můžeme psát $N - 1 = F \cdot U$, kde $(F, U) = 1$, přičemž známe rozklad čísla F na prvočinitele. Dále předpokládejme, že všechna prvočísla dělící U jsou větší než $B \in \mathbb{N}$ a že platí $B \cdot F \geq \sqrt{N}$.*
Pak platí: jestliže pro každé prvočíslo $p \mid F$ můžeme najít $a_p \in \mathbb{Z}$ splňující (1) z předchozí věty a jestliže navíc existuje $a_U \in \mathbb{Z}$ splňující

$$a_U^{N-1} \equiv 1 \pmod{N} \quad a \quad (a_U^F - 1, N) = 1,$$

pak je N prvočíslo.
Je-li naopak N prvočíslo, pak požadovaná $a_p, a_U \in \mathbb{Z}$ vždy existují.

Důkaz. Pro každé prvočíslo $d \mid N$ víme, že $d \equiv 1 \pmod{F}$. Protože $(a_U, N) = 1$, existuje $e = \min\{n \in \mathbb{N};\ a_U^n \equiv 1 \pmod{d}\}$. Odtud $e \mid d - 1$, $e \mid N - 1$ a $e \nmid F$. Kdyby $(e, U) = 1$, z $e \mid N - 1 = FU$ by plynulo $e \mid F$. Je tedy $(e, U) > 1$ a protože U je dělitelné pouze prvočísly většími než B, platí $(e, U) > B$. Protože $(F, U) = 1$, z $d \equiv 1 \pmod{e}$ a $d \equiv 1 \pmod{F}$ plyne $d \equiv 1 \pmod{F \cdot (e, U)}$ a tedy $d > F \cdot (e, U) > FB \geq \sqrt{N}$.

Příklad užití věty Pocklingtona a Lehmera – Pépinův test

Pro $k \in \mathbb{Z}$, $k > 0$, se $F_k = 2^{2^k} + 1$ nazývá k-té Fermatovo číslo.
Pépinův test: F_k je prvočíslo, právě když $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.

Důkaz. „$\Leftarrow$“ z důsledku věty Pocklingtona a Lehmera.
„$\Rightarrow$“ z kvadratického zákona reciprocity: $3^{(F_k-1)/2} \equiv \left(\frac{3}{F_k}\right) =$
$= \left(\frac{F_k}{3}\right) \cdot (-1)^{\frac{3-1}{2}\frac{F_k-1}{2}} = \left(\frac{F_k}{3}\right) = \left(\frac{2}{3}\right) = -1 \pmod{F_k}$.

- $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ jsou prvočísla.
- Rozklad čísla F_k na prvočinitele je znám jen pro $k \leq 11$.
- F_k jsou složená pro každé $k = 5, 6, \ldots, 32$ (ačkoli u F_{20} ani F_{24} není znám žádný prvočíselný dělitel).
- Největší F_k, pro které je znám prvočíselný dělitel, je $F_{2543548}$ dělitelné prvočíslem $9 \cdot 2^{2543551} + 1$ (objeveno 22. 6. 2011).
- Otevřené problémy: Existuje nekonečně mnoho složených Fermatových čísel? Existuje nekonečně mnoho Fermatových čísel, která jsou prvočísla?

Implementace algoritmu (tzv. $N-1$ test)

Vstupem je číslo N, které již prošlo testem Millera - Rabina, tedy číslo, o kterém s vysokou pravděpodobností platí, že je to prvočíslo. Je třeba to však dokázat.

V první části algoritmu rozkládáme číslo $N-1$ na součin $F \cdot U$ a to tak, že podrobíme $N-1$ algoritmu pokusného dělení, ukládáme získané dělitele a skončíme, až platí $BF \geq \sqrt{N}$, nebo až je B „dost velké“, abychom si byli jisti zastavením v „rozumném“ čase (zde B, F, U značí totéž, co v předchozí větě).

Pak náhodně volíme celá čísla a_p v intervalu $1 < a_p < N$ a počítáme $b_p = a_p^{\frac{N-1}{p}} \bmod N$ a $c_p = b_p^p \bmod N$ do té doby, než $c_p \equiv 1 \pmod N$ a $(b_p - 1, N) = 1$.

Je-li N opravdu prvočíslo, podmínku $(b_p - 1, N) = 1$ splňuje většina z čísel a_p, přesněji právě $\frac{p-1}{p}(N-1)$ čísel z $N-1$ čísel $1, 2, \ldots, N-1$. Můžeme tedy očekávat, že takové a_p brzy najdeme.

Pokud by však N bylo „velké“ Carmichaelovo číslo, algoritmus by se s velkou pravděpodobností nezastavil.

Časová náročnost algoritmu

Není-li N prvočíslo, algoritmus se nemusí zastavit.

Ani pro prvočísla nelze stanovit odhad: záleží na tom, jak snadno lze rozkládat číslo $N - 1$. Následné hledání čísel a_p je velmi rychlé (kontrola, zda zvolené a_p splňuje podmínku (1) je kvadratické časové náročnosti, navíc lze volit a_p „malá“).

Je možné nerozloženou část U podrobit testu Millera a Rabina a v případě, že test zjistí, že U je asi prvočíslo, dokázat nejprve prvočíselnost U (a tedy pracovat rekurzivně).

Zobecnění algoritmu

Je-li N prvočíslo, pak existuje těleso $\mathbb{F}_{N^2}$ o N^2 prvcích. Jeho multiplikativní grupa je cyklická řádu $N^2 - 1 = (N-1)(N+1)$. Existuje tedy $\alpha \in \mathbb{F}_{N^2}$ řádu $N+1$, tj. splňující $\alpha^{N+1} = 1$, avšak $\alpha^{\frac{N+1}{p}} \neq 1$ pro libovolné prvočíslo p dělící $N+1$.

Tuto myšlenku je možno využít pro tzv. $N+1$ test analogický $N-1$ testu. V něm vystupuje faktorizace čísla $N+1$ místo $N-1$.

Pro důkaz prvočíselnosti čísla N lze pak využít informace o dělitelích čísla N, získané z obou testů.

Podobně lze využít těleso $\mathbb{F}_{N^3}$ (a tedy faktorizovat $\frac{N^3-1}{N-1} = N^2 + N + 1$), těleso $\mathbb{F}_{N^4}$ (a faktorizovat $\frac{N^4-1}{N^2-1} = N^2 + 1$) nebo těleso $\mathbb{F}_{N^6}$ (a faktorizovat $\frac{N^6-1}{(N^3-1)(N+1)} = N^2 - N + 1$).

Vždy nám však už vycházejí čísla podstatně větší než N a tedy pravděpodobně obtížně rozložitelná.

Některé nezbytnosti z algebraické geometrie

Nechť K je těleso.

Definice. n-rozměrným afinním prostorem nad K rozumíme kartézskou mocninu K^n. Budeme jej značit $A^n(K)$, tj.

$$A^n(K) = \{(x_1, \ldots, x_n);\ x_1, \ldots, x_n \in K\}.$$

Definice. n-rozměrným projektivním prostorem nad K rozumíme rozklad na množině $K^{n+1} - \{(0, \ldots, 0)\}$ příslušný ekvivalenci $\sim$, kterou definujeme takto: pro libovolné $(n+1)$-tice $(x_1, \ldots, x_{n+1})$, $(y_1, \ldots, y_{n+1}) \in K^{n+1}$ položíme $(x_1, \ldots, x_{n+1}) \sim (y_1, \ldots, y_{n+1})$ právě tehdy, když existuje $\lambda \in K^\times$, které pro každé $i \in \{1, \ldots, n+1\}$ splňuje podmínku $x_i = \lambda y_i$. Tento n-rozměrný projektivní prostor nad K budeme značit $P^n(K)$, třídu rozkladu (tj. bod projektivního prostoru) obsahující $(n+1)$-tici $(x_1, \ldots, x_{n+1})$ budeme značit $[x_1, \ldots, x_{n+1}]$.

Afinní část projektivního prostoru

Nechť $x_1, \ldots, x_{n+1}$ jsou z tělesa K, přičemž alespoň jedno z nich je různé od nuly.

Jestliže $x_{n+1} \neq 0$, pak platí $[x_1, \ldots, x_{n+1}] = [\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}, 1]$, čímž je pevně dán bod $(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}) \in A^n(K)$.

Jestliže naopak $x_{n+1} = 0$, určuje $[x_1, \ldots, x_{n+1}]$ jednoznačně bod $[x_1, \ldots, x_n] \in P^{n-1}(K)$.

Lze tedy n-rozměrný projektivní prostor „rozdělit“ na n-rozměrný afinní prostor, který považujeme za množinu „vlastních bodů“ a na množinu „nevlastních bodů“, která tvoří $(n-1)$-rozměrný projektivní prostor.

Můžeme si představovat, že nevlastní body „leží v nekonečnu.“ Toto rozdělení však *není* kanonické – lze to provést mnoha způsoby. Tedy to, zda je bod vlastní nebo ne, je věc naší volby.

Nadplochy projektivního prostoru

Máme-li homogenní polynom $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ o $n+1$ proměnných nad K stupně k a bod $[x_1, \ldots, x_{n+1}] \in P^n(K)$, má smysl se ptát, zda $F(x_1, \ldots, x_{n+1}) = 0$. Je-li totiž $[x_1, \ldots, x_{n+1}] = [y_1, \ldots, y_{n+1}]$, pak existuje $\lambda \in K^\times$, které pro každé $i \in \{1, \ldots, n+1\}$ splňuje podmínku $x_i = \lambda y_i$. Pak ovšem $F(x_1, \ldots, x_{n+1}) = F(\lambda y_1, \ldots, \lambda y_{n+1}) = \lambda^k \cdot F(y_1, \ldots, y_{n+1})$, a tedy $F(x_1, \ldots, x_{n+1}) = 0$, právě když $F(y_1, \ldots, y_{n+1}) = 0$.

Definice. Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k. Množina

$$\mathcal{C} = \{[x_1, \ldots, x_{n+1}] \in P^n(K);\ F(x_1, \ldots, x_{n+1}) = 0\}$$

se nazývá nadplocha stupně k v $P^n(K)$. Je-li $n = 2$, hovoříme také o křivce stupně k v projektivní rovině $P^2(K)$.

Singulární bod nadplochy projektivního prostoru

Parciální derivací homogenního mnohočlenu je opět homogenní mnohočlen. Má proto smysl následující definice.

Definice. Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k a

$$\mathcal{C} = \{[x_1, \ldots, x_{n+1}] \in P^n(K);\ F(x_1, \ldots, x_{n+1}) = 0\}$$

příslušná nadplocha. Bod $[x_1, \ldots, x_{n+1}] \in \mathcal{C}$ se nazývá singulární, jestliže pro každé $i \in \{1, \ldots, n+1\}$ platí

$$\frac{\partial F}{\partial x_i}(x_1, \ldots, x_{n+1}) = 0.$$

Nadplocha $\mathcal{C}$ se nazývá singulární, existuje-li alespoň jeden její singulární bod.

Příklad

Uvažme reálnou projektivní rovinu $P^2(\mathbb{R})$.
Abychom se vyhnuli indexům, budeme psát x, y, z místo t_1, t_2, t_3.

Kubický mnohočlen $F_1(x, y, z) = x^3 + x^2z - y^2z$ nám definuje kubickou křivku $\mathcal{C}_1$ (tj. křivku stupně 3)

$$\mathcal{C}_1 = \{[x, y, z] \in P^2(\mathbb{R});\ F_1(x, y, z) = 0\}.$$

Jistě $[0, 0, 1] \in \mathcal{C}_1$. Tento bod je singulární, neboť

$$\frac{\partial F_1}{\partial x} = 3x^2 + 2xz, \quad \frac{\partial F_1}{\partial y} = -2yz, \quad \frac{\partial F_1}{\partial z} = x^2 - y^2.$$

Je tedy $\mathcal{C}_1$ singulární křivka.

Další příklad

Opět pracujme s reálnou projektivní rovinu $P^2(\mathbb{R})$.

Uvažme nyní mnohočlen $F_2(x, y, z) = x^3 + xz^2 - y^2z$ a příslušnou kubickou křivku

$$\mathcal{C}_2 = \{[x, y, z] \in P^2(\mathbb{R});\ F_2(x, y, z) = 0\}.$$

Hledejme singulární body na $\mathcal{C}_2$. Platí

$$\frac{\partial F_2}{\partial x} = 3x^2 + z^2, \quad \frac{\partial F_2}{\partial y} = -2yz, \quad \frac{\partial F_2}{\partial z} = 2xz - y^2.$$

Z $\frac{\partial F_2}{\partial x} = 0$ plyne $x = 0$ a $z = 0$, pak ale z $\frac{\partial F_2}{\partial z} = 0$ plyne i $y = 0$.

Ale trojice nul nedává žádný bod projektivní roviny. Singulární bod na $\mathcal{C}_2$ tedy neexistuje a proto $\mathcal{C}_2$ není singulární křivka.

Eliptické křivky

Definice. Eliptická křivka nad tělesem K je uspořádaná dvojice $(\mathcal{E}, O)$, kde $\mathcal{E}$ je nesingulární kubická křivka v $P^2(K)$ a $O \in \mathcal{E}$.

Poznámka. Je možné zavést pojem biracionální ekvivalence dvou křivek, spočívající v tom, že existují transformace prostoru převádějící jednu křivku na druhou a obráceně, přičemž tyto transformace jsou „pěkné“ v tom smyslu, že transformační rovnice jsou dány homogenními polynomy téhož stupně nad K.

Věta. *Libovolná eliptická křivka nad K je biracionálně ekvivalentní s nějakou eliptickou křivkou $(\mathcal{E}, O)$ následujícího tvaru (přičemž transformace převádějí vyznačený bod jedné křivky na vyznačený bod druhé křivky)*

$$\mathcal{E} = \{[x, y, z] \in P^2(K);\ F(x, y, z) = 0\},$$

kde

$$F(x, y, z) = y^2z + a_1xyz + a_2yz^2 - x^3 - a_3x^2z - a_4xz^2 - a_5z^3,$$

$a_1, \ldots, a_5 \in K$ *a* $O = [0, 1, 0]$.

Eliptické křivky dané Weierstrassovou rovnicí

V projektivní rovině zvolme za afinní část množinu těch bodů, které mají nenulovou třetí souřadnici, tedy bodů $[x, y, 1]$.

Každá eliptická křivka ve tvaru z předchozí věty má jeden nevlastní bod (totiž $O = [0, 1, 0]$) a v afinní části je dána rovnicí

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5.$$

Tato rovnice se nazývá **Weierstrassova rovnice**.

V dalším textu budeme předpokládat, že charakteristika tělesa K není ani 2 ani 3, tj. že 2 i 3 jsou invertibilní prvky v K.

Důvodem je to, že pro naše účely eliptické křivky nad tělesy charakteristiky 2 a 3 nejsou zapotřebí a že tento předpoklad dále zjednodušuje Weierstrassovu rovnici.

Můžeme pak totiž předpokládat, že $a_1 = a_2 = a_3 = 0$, a tedy Weierstrassova rovnice je tvaru $y^2 = x^3 + a_4x + a_5$.

Kdy Weierstrassova rovnice zadává eliptickou křivku?

Věta. *Nechť K je těleso charakteristiky různé od 2 a 3, $a, b \in K$. Rovnice $y^2 = x^3 + ax + b$ je Weierstrassovou rovnicí nějaké eliptické křivky, právě když platí $4a^3 + 27b^2 \neq 0$.*

Důkaz. Položme $F(x, y, z) = y^2z - x^3 - axz^2 - bz^3$. Platí

$$\frac{\partial F}{\partial x} = -3x^2 - az^2, \quad \frac{\partial F}{\partial y} = 2yz, \quad \frac{\partial F}{\partial z} = y^2 - 2axz - 3bz^2.$$

Předpokládejme, že $[x, y, z]$ je singulární bod. Pak $z = 0$ implikuje $x = y = 0$, spor. Je tedy $z \neq 0$. Proto $y = 0$ a pro $\gamma = \frac{x}{z}$ platí $3\gamma^2 = -a$, $2a\gamma = -3b$. Jestliže $a = 0$, pak také $b = 0$. Naopak pro $a = b = 0$ je bod $[0, 0, 1]$ singulární. Zabývejme se dále případem $a \neq 0$. Platí $\gamma = -\frac{3b}{2a}$, $\gamma^2 = -\frac{a}{3} = \frac{9b^2}{4a^2}$, tj. $4a^3 + 27b^2 = 0$. Naopak, je-li $4a^3 + 27b^2 = 0$, $a \neq 0$, ověřme, že pro $\gamma = -\frac{3b}{2a}$ je $[\gamma, 0, 1]$ singulární bod, což je snadné, například $\gamma^2 = \frac{9b^2}{4a^2} = -\frac{a}{3}$, dále

$$\gamma^3 + a\gamma + b = \left(-\tfrac{3b}{2a}\right)\left(-\tfrac{a}{3}\right) + a\left(-\tfrac{3b}{2a}\right) + b = \tfrac{b}{2} - \tfrac{3b}{2} + b = 0.$$