Věty o eliptických křivkách nad konečnými tělesy

Projektivní rovina nad konečným tělesem má konečně mnoho bodů, proto eliptická křivka nad konečným tělesem je konečná grupa.

Věta. (Hasse)

1. *Nechť p je prvočíslo a $(\mathcal{E}, O)$ je eliptická křivka nad $\mathbb{F}_p$. Pak $|\mathcal{E}| = p + 1 - a_p$, kde celé číslo a_p splňuje $|a_p| < 2\sqrt{p}$.*
2. *Označme $\alpha_p \in \mathbb{C}$ kořen rovnice $x^2 - a_p x + p = 0$. Pro libovolné $n \in \mathbb{N}$ nechť $(\mathcal{E}_n, O)$ je eliptická křivka nad $\mathbb{F}_{p^n}$ určená stejnou Weierstrassovou rovnicí jako $(\mathcal{E}, O)$ (to má smysl, neboť $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$). Pak platí $|\mathcal{E}_n| = p^n + 1 - 2\Re(\alpha_p^n)$, kde $\Re$ značí reálnou část komplexního čísla.*

Věta. Nechť $(\mathcal{E}, O)$ je eliptická křivka nad konečným tělesem $\mathbb{F}_q$, kde q je mocnina prvočísla. Pak $(\mathcal{E}, +)$ je cyklická grupa nebo součin dvou cyklických grup. Navíc, ve druhém případě, je-li $(\mathcal{E}, +)$ izomorfní se součinem cyklických grup o d_1 a d_2 prvcích, přičemž $d_1 \mid d_2$, pak platí $d_1 \mid q - 1$.

Věty o eliptických křivkách nad $\mathbb{Q}$

Věta. (Mordell) Nechť $(\mathcal{E}, O)$ je eliptická křivka nad $\mathbb{Q}$. Pak $(\mathcal{E}, O)$ je konečně generovaná grupa. Jinými slovy: označme $(\mathcal{E}', +)$ podgrupu prvků konečného řádu v grupě $(\mathcal{E}, +)$ (tzv. torzní podgrupa); pak existuje (jednoznačně určené) nezáporné celé číslo r tak, že $(\mathcal{E}, +)$ je izomorfní se součinem $(\mathcal{E}', +) \times (\mathbb{Z}, +)^r$.

Věta. (Mazur) Nechť $(\mathcal{E}, O)$ je eliptická křivka nad $\mathbb{Q}$. Pak její torzní podgrupa je izomorfní s některou z následujících 15 grup:

$$(\mathbb{Z}/m\mathbb{Z}, +) \qquad \text{pro } 1 \leq m \leq 10 \text{ nebo } m = 12$$
$$(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2m\mathbb{Z}, +) \qquad \text{pro } 1 \leq m \leq 4$$

(a každá z uvedených grup je torzní grupa některé eliptické křivky nad $\mathbb{Q}$).

Proč si povídáme o eliptických křivkách?

Eliptické křivky se využívají v některých testech na prvočíselnost i v algoritmech hledání netriviálního dělitele.

Za tím účelem je třeba pracovat také s „eliptickými křivkami“ nad okruhem $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ zbytkových tříd modulo N i v případě, že přirozené číslo N není prvočíslo. Ovšem projektivní prostor je definován jen nad tělesem, což v tomto případě $\mathbb{Z}_N$ není (proto ty uvozovky).

Proto budeme definovat pojem projektivního prostoru i nad okruhem $\mathbb{Z}_N$ pro libovolné přirozené číslo N.

Projektivní prostor nad okruhem $\mathbb{Z}_N$

Definice. Nechť N je přirozené číslo (ne nutně prvočíslo). Pak n-rozměrným projektivním prostorem nad okruhem $\mathbb{Z}_N$ rozumíme rozklad na následující množině (n+1)-tic zbytkových tříd modulo N

$$M = \{([a_1]_N, \ldots, [a_{n+1}]_N);\ a_1, \ldots, a_{n+1} \in \mathbb{Z},\ (N, a_1, \ldots, a_{n+1}) = 1\}$$

příslušný ekvivalenci $\sim$, kterou definujeme takto: pro libovolné $(n+1)$-tice $([a_1]_N, \ldots, [a_{n+1}]_N)$, $([b_1]_N, \ldots, [b_{n+1}]_N) \in M$ položíme $([a_1]_N, \ldots, [a_{n+1}]_N) \sim ([b_1]_N, \ldots, [b_{n+1}]_N)$ právě tehdy, když existuje $\lambda \in \mathbb{Z}$, $(\lambda, N) = 1$, které pro každé $i \in \{1, \ldots, n+1\}$ splňuje podmínku $[a_i]_N = [\lambda b_i]_N$.
V tomto n-rozměrném projektivním prostoru $P^n(\mathbb{Z}_N)$ nad $\mathbb{Z}_N$ budeme třídu rozkladu (tj. bod projektivního prostoru) obsahující $(n+1)$-tici $([a_1]_N, \ldots, [a_{n+1}]_N)$ značit $[[a_1]_N, \ldots, [a_{n+1}]_N]$.

Poznámka. Pro libovolné $d \mid N$ homomorfismus okruhů $\mathbb{Z}_N \to \mathbb{Z}_d$ určený předpisem $[a]_N \mapsto [a]_d$ pro každé $a \in \mathbb{Z}$ indukuje zobrazení n-rozměrných projektivních prostorů $P^n(\mathbb{Z}_N) \to P^n(\mathbb{Z}_d)$.

Test na prvočíselnost

Dáno přirozené číslo $N > 1$, o kterém jsme testem Millera a Rabina zjistili, že N je asi prvočíslo. Můžeme také předpokládat, že víme, že N není dělitelné malými prvočísly. Test na prvočíselnost má dokázat, že N skutečně prvočíslem je, anebo to vyvrátit.

Známe už $N - 1$ test Pocklingtona a Lehmera. Ten pracuje dobře, pokud jsme schopni dostatečně rozložit číslo $N - 1$. Pokud však neexistuje dost velký dělitel $F|N - 1$, který jsme schopni rozložit na prvočinitele, tato metoda neuspěje. Pak můžeme ještě zkusit $N + 1$ test, ten však vyžaduje rozložit dost velkého dělitele čísla $N + 1$, což se však často také nemusí podařit a skončíme nezdarem.

Řešení nabízí teorie eliptických křivek: je-li N skutečně prvočíslo, máme spoustu eliptických křivek nad $\mathbb{Z}_N$. Jejich řády jsou rovny přirozeným číslům v intervalu $(N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N})$. Je pravděpodobné, že nezanedbatelnou část z těchto čísel budeme schopni rozložit na prvočinitele.

Síla metody eliptických křivek je v jejich počtu: pokud nevyhovuje několik konkrétních křivek, nevadí, vezmeme další.

Opakování $N-1$ testu Pocklingtona a Lehmera

Předpokládáme, že známe prvočíslo p dělící $N-1$, přitom p^{α_p} je nejvyšší mocnina p dělící $N-1$.
Dále označme d libovolné neznámé prvočíslo dělící N.
Máme homomorfismus okruhů $f : \mathbb{Z}_N \to \mathbb{Z}_d$, kde $f([a]_N) = [a]_d$ pro každé $a \in \mathbb{Z}$. Homomorfismus f je dobře definován, neboť $d \mid N$. Protože je d prvočíslo, je druhý okruh těleso $\mathbb{F}_d = \mathbb{Z}_d$.
Předpokládáme existenci $a_p \in \mathbb{Z}$, které splňuje

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

Označme $b = f([a_p]_N) \in \mathbb{F}_d$. Pak $b^{N-1} = 1$, $b^{\frac{N-1}{p}} \neq 1$, a tedy řád prvku b je dělitelný p^{α_p}, odkud $p^{\alpha_p} \mid |\mathbb{F}_d^\times| = d-1$, tedy $d \equiv 1 \pmod{p^{\alpha_p}}$. Získali jsme tím informaci o neznámém d.

Klíčem k úspěchu zde byl homomorfismus $f : \mathbb{Z}_N \to \mathbb{Z}_d$.
Přestože jsme neznali d, a tedy nebyli schopni v $\mathbb{Z}_d$ pracovat, počítali jsme ve známém okruhu $\mathbb{Z}_N$ a výsledky výpočtů jsme do $\mathbb{Z}_d$ zobrazili homomorfismem f.

Test na prvočíselnost pomocí eliptických křivek

Přejděme k eliptickým křivkám, opět d značí libovolné neznámé prvočíslo dělící dané N, $(N, 6) = 1$. Zvolme libovolně $a, b \in \mathbb{Z}$ taková, že $(4a^3 + 27b^2, N) = 1$. Rovnice $y^2z = x^3 + axz^2 + bz^3$ nám dává „eliptickou křivku“ $\mathcal{E}_N$, na níž máme definovánu částečnou operaci, a eliptickou křivku $\mathcal{E}_d$, což je komutativní grupa. Z Hasseho věty víme, že $||\mathcal{E}_d| - d - 1| < 2\sqrt{d}$.
Přestože v $\mathcal{E}_d$ nejsme schopni počítat (vždyť neznáme d), máme částečný homomorfismus $f : \mathcal{E}_N \to \mathcal{E}_d$, kterým můžeme výpočet provedený v $\mathcal{E}_N$ zobrazit do $\mathcal{E}_d$. Víme, že $f([[0]_N, [1]_N, [0]_N]) = O$ a že pro libovolný $P = [[u]_N, [v]_N, [1]_N] \in \mathcal{E}_N$ platí $f(P) \neq O$.
Je-li q prvočíslo a bod $P = [[u]_N, [v]_N, [1]_N] \in \mathcal{E}_N$ takový, že máme definované $q \cdot P = P + P + \cdots + P = [[0]_N, [1]_N, [0]_N]$, pak řád bodu $f(P)$ v grupě $\mathcal{E}_d$ je q, a tedy $(\sqrt{d} + 1)^2 > |\mathcal{E}_d| \geq q$.
Najdeme-li takový bod P pro prvočíslo $q > (\sqrt[4]{N} + 1)^2$, plyne odtud $d > \sqrt{N}$, a tedy N je prvočíslo.

Problém je, jak volit čísla a, b a jak najít prvočíslo q a bod $P \in \mathcal{E}_N$ s potřebnými vlastnostmi...

Goldwasser - Kilian, 1986

Řešení navržené Goldwasserem a Kilianem má spíše teoretický význam; je možné dokázat, že platí-li jistá hypotéza o rozložení prvočísel v krátkých intervalech, pak očekávaný čas výpočtu je $O(\ln^{12} N)$, tedy polynomiální.

Existuje algoritmus Schoofa, který pro prvočíslo p počítá řád (tj. počet bodů) dané eliptické křivky nad $\mathbb{F}_p$ v čase $O(\ln^8 p)$.

Zvolíme náhodně a, $b \in \mathbb{Z}$ tak, aby $(4a^3 + 27b^2, N) = 1$. Pomocí Schoofova algoritmu určíme pro křivku $(\mathcal{E}, O)$ určenou rovnicí $y^2 = x^3 + ax + b$ a pro $p = N$ její řád m (jestliže N není prvočíslo, nemá m žádný význam). Získané m zkoušíme dělit malými prvočísly s nadějí, že poté, co odstraníme malé faktory, zůstane nám $q > (\sqrt[4]{N} + 1)^2$, $q < \frac{N}{2}$, o kterém test Millera a Rabina zjistí, že q je asi prvočíslo. Pokud se nám to nepodaří, začneme znovu s jinými a, $b \in \mathbb{Z}$.

Existuje algoritmus, který pro prvočíslo p a celé číslo e hledá v čase $O(\ln^4 p)$ řešení kongruence $x^2 \equiv e \pmod p$ a to, že takové řešení neexistuje, zjistí dokonce v čase $O(\ln^2 p)$.

Goldwasser - Kilian, 1986, pokračování

Najdeme bod P na křivce: náhodně zvolíme $c \in \mathbb{Z}_N$ a hledáme $d \in \mathbb{Z}_N$ tak, aby $d^2 = c^3 + ac + b$ (jde o kongruenci modulo N; d hledáme jako by bylo N prvočíslo, pak uděláme zkoušku, pokud nevyjde, nebylo N prvočíslo a jsme zcela hotovi). Neexistuje-li takové d, zkusíme jiné c. Pak za P zvolíme $\frac{m}{q}$-násobek bodu $[c, d, 1]$ v $(\mathcal{E}, +)$. Je-li $P = [0, 1, 0]$, zvolíme jiné c atd. Je-li $P \neq [0, 1, 0]$, pak platí $P = [x, y, 1]$ pro nějaké x, $y \in \mathbb{Z}_N$. Spočítáme q-násobek bodu P v $(\mathcal{E}, +)$. Není-li definován, našli jsme netriviálního dělitele čísla N. Jestliže nedostaneme $[0, 1, 0]$, není m řád křivky $(\mathcal{E}, O)$, Schoofův algoritmus tedy nedal správný výsledek a proto N není prvočíslo. Jestliže q-násobek bodu P je $[0, 1, 0]$, pak je N prvočíslo, pokud q je prvočíslo. To zjistíme rekurzívně ($N_0 = N$, N_1 je q pro N_0, N_2 je q pro N_1, ...). S rekurzí skončíme v okamžiku, kdy N_i je dost malé na to, abychom ověřili jeho prvočíselnost pokusným dělením (to nastane v $O(\ln N)$ krocích vzhledem k $N_{i+1} < \frac{1}{2} N_i$). Je třeba si uvědomit, že není-li N_i prvočíslo, skončíme jen v případě $i = 0$, pro $i < 0$ je třeba se vrátit k $i - 1$ a najít nové N_i.