Eliptická křivka daná Weierstrassovou rovnicí

Nechť K je těleso charakteristiky různé od 2 a 3, $a, b \in K$, $4a^3 + 27b^2 \neq 0$. Pak Weierstrassova rovnice

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

spolu s význačným bodem $O = [0, 1, 0]$ zadává v projektivní rovině $P^2(K)$ eliptickou křivku $\mathcal{E}$.

Tento význačný bod O je jediným bodem na nevlastní přímce $z = 0$. Platí dokonce, že nevlastní přímka $z = 0$ má s eliptickou křivkou $\mathcal{E}$ trojnásobný bod dotyku O, neboť dosazením $z = 0$ do rovnice křivky dostaneme $x^3 = 0$.

Ostatní body eliptické křivky jsou vlastní a jsou v afinní rovině $A^2(K) = K^2$ určeny rovnicí $y^2 = x^3 + ax + b$.

Je-li $A = [\alpha, \beta, 1] \in \mathcal{E}$, pak i $B = [\alpha, -\beta, 1] \in \mathcal{E}$. Přímka AB má v $P^2(K)$ rovnici $x = \alpha z$ a obsahuje ještě třetí bod na $\mathcal{E}$, totiž O.

Eliptická křivka $\mathcal{E}: \; y^2z = x^3 + axz^2 + bz^3$, $O = [0,1,0]$

Jsou-li $A = [\alpha, \beta, 1] \in \mathcal{E}$, $B = [\gamma, \delta, 1] \in \mathcal{E}$, přičemž $\alpha \neq \gamma$, přímka AB má v $P^2(K)$ rovnici $y = \beta z + (x - \alpha z)k$, kde $k = \frac{\delta - \beta}{\gamma - \alpha}$. Hledejme průsečíky přímky AB s eliptickou křivkou $\mathcal{E}$.

Dosazením této rovnice za y do rovnice $y^2z = x^3 + axz^2 + bz^3$ a vydělením z^3 dostaneme kubickou rovnici pro $\frac{x}{z}$ s koeficienty z K:

$$\left(\tfrac{x}{z}\right)^3 + a\tfrac{x}{z} + b - \left(\beta + (\tfrac{x}{z} - \alpha)k\right)^2 = 0.$$

Jde o normovaný kubický polynom v $\frac{x}{z}$, jehož dva kořeny α a γ už známe. Proto má ještě třetí kořen $\sigma \in K$ a z Viétových vztahů zjistíme, že platí $\alpha + \gamma + \sigma = k^2$.

Přímka AB a eliptická křivka $\mathcal{E}$ mají tedy ještě třetí průsečík $C = [\sigma, \tau, 1]$, kde $\sigma = k^2 - \alpha - \gamma$, $\tau = \beta + k(\sigma - \alpha)$.

Někdy může bod C splynout s některým z bodů A, B, v tom případě mluvíme o dvojnásobném průsečíku.

Eliptická křivka $\mathcal{E}: \; y^2z = x^3 + axz^2 + bz^3,\; O = [0,1,0]$

Podobně se odvodí, že pokud sestrojíme křivce $\mathcal{E}$ v jejím bodě A tečnu, protne tato tečna křivku $\mathcal{E}$ ještě v jednom bodě. Máme tedy operaci: pro libovolnou dvojici bodů $A, B \in \mathcal{E}$ je jejím výsledkem třetí průsečík, který nazveme $A \star B$. Tato operace však není „pěkná“: nemá neutrální prvek, není asociativní.

Proto operaci ještě trochu pozměníme pomocí pevně zvoleného bodu O. Definujeme součet bodů $A, B \in \mathcal{E}$ předpisem

$$A + B = (A \star B) \star O.$$

Tato operace sčítání bodů je zřejmě komutativní, $(\mathcal{E}, +)$ má neutrální prvek O a libovolný bod $A = [\alpha, \beta, 1] \in \mathcal{E}$ má opačná bod $-A = [\alpha, -\beta, 1] \in \mathcal{E}$. Je možné dokázat, že operace sčítání bodů je také asociativní, je tedy $(\mathcal{E}, +)$ komutativní grupa. Důkaz asociativity je mimo možnosti této přednášky.

Explicitní popis operace sčítání bodů

Věta. *Nechť K je těleso charakteristiky různé od 2 a 3, $a, b \in K$, $4a^3 + 27b^2 \neq 0$. Nechť $\mathcal{E}$ je eliptická křivka daná Weierstrassovou rovnicí $y^2z = x^3 + axz^2 + bz^3$ s význačným bodem $O = [0, 1, 0]$. Operaci $+$ na $\mathcal{E}$ je možné popsat takto:*

1. *Pro libovolné $A \in \mathcal{E}$ klademe $A + O = O + A = A$.*
2. *Pro libovolné $A = [\alpha, \beta, 1] \in \mathcal{E}$ je také $B = [\alpha, -\beta, 1] \in \mathcal{E}$ a klademe $A + B = O$. (Tento bod B pak označujeme $-A$.)*
3. *Pro libovolné $A = [\alpha, \beta, 1] \in \mathcal{E}$, $B = [\gamma, \delta, 1] \in \mathcal{E}$ takové, že $B \neq -A$, položme*

$$k = \begin{cases} \frac{\beta-\delta}{\alpha-\gamma} & \text{je-li } A \neq B, \\ \frac{3\alpha^2+a}{2\beta} & \text{je-li } A = B, \end{cases}$$
$$\sigma = k^2 - \alpha - \gamma,$$
$$\tau = -\beta + k(\alpha - \sigma),$$

pak platí $[\sigma, \tau, 1] \in \mathcal{E}$ a klademe $A + B = [\sigma, \tau, 1] \in \mathcal{E}$.

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 $|\mathcal{E}_n| = p^n + 1 - 2\,\mathrm{Re}(\alpha_p^n)$, 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 $\mathbb{Z}_N$ 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

$$M = \{([u_1]_N, \ldots, [u_{n+1}]_N);\ u_1, \ldots, u_{n+1} \in \mathbb{Z},\ (N, u_1, \ldots, u_{n+1}) = 1\}$$

příslušný ekvivalenci $\sim$, kterou definujeme takto: pro libovolné $(n+1)$-tice $([u_1]_N, \ldots, [u_{n+1}]_N)$, $([v_1]_N, \ldots, [v_{n+1}]_N) \in M$ položíme $([u_1]_N, \ldots, [u_{n+1}]_N) \sim ([v_1]_N, \ldots, [v_{n+1}]_N)$ právě tehdy, když existuje $\lambda \in \mathbb{Z}$, $(\lambda, N) = 1$, které pro každé $i \in \{1, \ldots, n+1\}$ splňuje podmínku $[u_i]_N = [\lambda v_i]_N$.
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 $([u_1]_N, \ldots, [u_{n+1}]_N)$ značit $[[u_1]_N, \ldots, [u_{n+1}]_N]$.

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

„Eliptická křivka“ nad okruhem $\mathbb{Z}_N$

Definice. Mějme dána celá čísla a, b a zvolme přirozené číslo N tak, že $(4a^3 + 27b^2, N) = 1$. Pak

$$\mathcal{E}_N = \left\{ \left[[x]_N, [y]_N, [z]_N \right] \in P^2(\mathbb{Z}_N);\ y^2 z \equiv x^3 + axz^2 + bz^3 (\mathrm{mod}\, N) \right\}$$

spolu s význačným bodem $O = \left[[0]_N, [1]_N, [0]_N \right]$ je „eliptická křivka“ nad okruhem $\mathbb{Z}_N$.

Poznámka. Jestliže $\left[[x_1]_N, [y_1]_N, [z_1]_N \right] = \left[[x_2]_N, [y_2]_N, [z_2]_N \right]$, pak

$$y_1^2 z_1 \equiv x_1^3 + a x_1 z_1^2 + b z_1^3 (\mathrm{mod}\, N) \ \Leftrightarrow\ y_2^2 z_2 \equiv x_2^3 + a x_2 z_2^2 + b z_2^3 (\mathrm{mod}\, N).$$

Definice je tedy korektní.

Věta. Jestliže $d \mid N$, pak zobrazení $f : P^2(\mathbb{Z}_N) \to P^2(\mathbb{Z}_d)$, určené předpisem $f\left(\left[[x]_N, [y]_N, [z]_N \right] \right) = \left[[x]_d, [y]_d, [z]_d \right]$, lze zúžit na zobrazení $f : \mathcal{E}_N \to \mathcal{E}_d$.

Částečná operace na „eliptické křivce“ nad okruhem $\mathbb{Z}_N$

Pro $a, b \in \mathbb{Z}$ a $N \in \mathbb{N}$ splňující $(4a^3 + 27b^2, N) = 1$ definujme na „eliptické křivce“ $\mathcal{E}_N$ částečnou operaci $+$ pomocí vzorců odvozených pro eliptické křivky nad tělesy, pokud se tyto vzorce dají použít. Jediné místo, kdy mohou nastat potíže, je v situaci, kdy chceme dělit, abychom našli směrnici k tečny nebo přímky spojující dva body „eliptické křivky“. Konkrétněji je to tehdy, když chceme dělit zbytkovou třídou $[u]_N \neq [0]_N$ takovou, že $[u]_N \notin \mathbb{Z}_N^\times$. V tom případě je (u, N) netriviální dělitel čísla N.

Avšak naším cílem bude rozhodnout o prvočíselnosti čísla N, popřípadě najít jeho netriviálního dělitele. Pokud se tedy dostaneme do situace, že neumíme na $\mathcal{E}_N$ sečíst dva body, budeme hotovi. Proto nám nevadí, že operace $+$ je jen částečná.

Pro libovolné $d \mid N$ je dříve zmíněné zobrazení $f : \mathcal{E}_N \to \mathcal{E}_d$, určené předpisem $f\big([[x]_N, [y]_N, [z]_N]\big) = \big[[x]_d, [y]_d, [z]_d\big]$, částečný homomorfismus: pro libovolné $A, B \in \mathcal{E}_N$ takové, že máme definován součet $A + B$, platí $f(A + B) = f(A) + f(B)$.