Аритметички својства на елиптични криви

Никола Велов

Шести семинар „Математика и примени“, 17 март 2023
Институт за математика, Природно-математички факултет,
Универзитет „Св. Кирил и Методиј“, Скопје

- Елиптични криви се кубни криви со природна структура на група.
- Во оваа група множењето е дефинирано геометриски. Елиптични криви се специјален случај на Абелови вариетети.
- Елиптични криви не се исто што и елипси. Името го добиле заради историски контекст а и фактот дека слични алгебарски изрази се појавуваат кај елиптичните интеграли.
- Елиптични криви се релевантни во разни области на математиката, како што се теорија на броеви, комплексна анализа, алгебарска геометрија, а имаат и важни примени во криптографија.

Равенка на елиптична крива

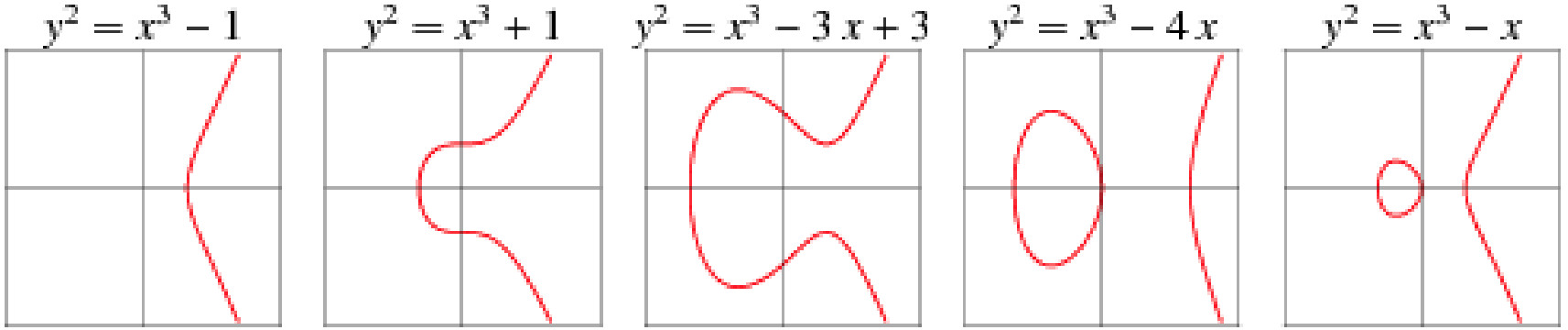
Нека K е произволно поле со карактеристика различна од 2 и 3. Елиптична крива е кубна крива дефинирана со следната равенка чии коефициенти припаѓаат во K:

$$y^2 = x^3 + ax + b$$

при што полиномот на десната страна од равенството има само прости корени.

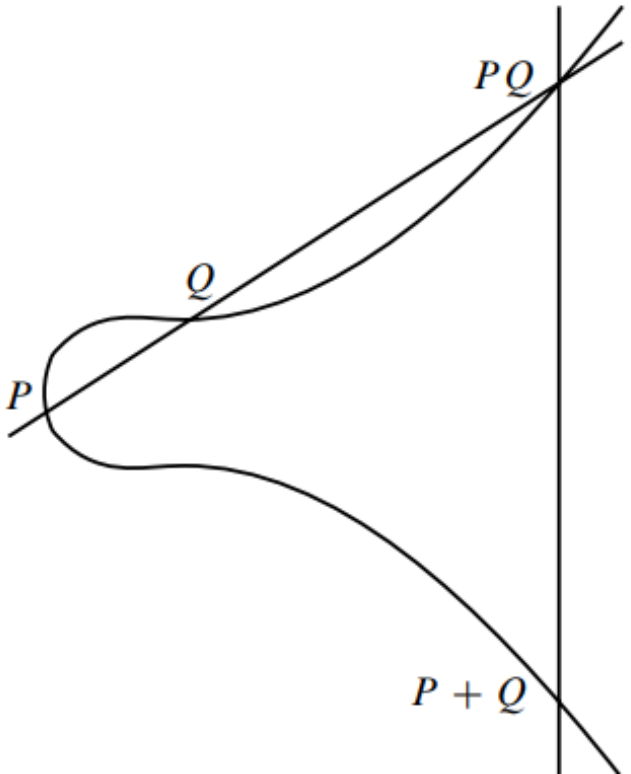
- Најчесто работиме со полиња како што се $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ и $\mathbb{F}_p$ за прост број $p > 3$.
- Еден пример на елиптична крива во $\mathbb{Q}$ е кривата дадена со равенката $y^2 = x^3 - x$, затоа што сите комплексни корени на полиномот $x^3 - x = x(x-1)(x+1)$ се различни.

- Условот дека десната страна има само прости корени гарантира дека елиптичната крива е глатка (нема сингуларитети).



- На секоја елиптична крива ѝ доделуваме бесконечна точка означена со $\mathcal{O}$.

- Нека $E : y^2 = x^3 + ax + b$ е елиптична крива и нека k е поле. Да го означиме со $E(k)$ множеството на сите точки што се на E и имаат координати во k.
- Ако P и Q се две точки од $E(k)$, правата PQ ја сече кривата во некоја трета точка (заради теоремата на Безу). Точката $P + Q$ се добива со рефлексија на оваа точка во однос на x-оската.



- Кога $P = Q$, наместо правата PQ се користи тангентата во точката P. Тангентата е добро дефинирана затоа што кривата е глатка.
- Доколку правата PQ (односно тангентата во случајот $P = Q$) е паралелна со y-оската, тогаш $P + Q = \mathcal{O}$ е бесконечна точка.

Структура на Абелова група

Собирање на точки во елиптични криви ги поседува следните особини:

1. $P + \mathcal{O} = \mathcal{O} + P = P$ за сите $P \in E(k)$.
2. $P + (-P) = \mathcal{O}$ за сите $P \in E(k)$.
3. $P + (Q + R) = (P + Q) + R$ за сите $P, Q, R \in E(k)$.
4. $P + Q = Q + P$ за сите $P, Q \in E(k)$.

Mordell, 1922

Нека E е елиптична крива дадена со равенката $E : y^2 = x^3 + ax + b$ каде што $x, y \in \mathbb{Q}$. Тогаш $E(\mathbb{Q})$ е **конечно генерирана** Абелова група, што значи дека постојат $P_1, ..., P_t \in E(\mathbb{Q})$ така што секоја точка $P \in E(\mathbb{Q})$ има облик

$$P = n_1 P_1 + n_2 P_2 + ... + n_t P_t$$

за некои цели броеви $n_1, ..., n_t$.

- Со други зборови, постои изоморфизам

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r,$$

каде што $E(\mathbb{Q})_{tors}$ е конечна група што се нарекува **торзиона група** од $E(\mathbb{Q})$, додека бројот r се нарекува **ранг** од $E(\mathbb{Q})$.

- Елиптичните криви имаат значајна примена во теорија на броеви. Единствениот зачуван доказ од Ферма е дека бројот 1 не е конгруентен и тоа е првиот пример каде е употребен методот на бесконечно спуштање.

Конгруенти броеви

За природен број n се вели дека е **конгруентен** ако постои правоаголен триаголник со рационални страни и плоштина еднаква на n.

- Проблемот на определување кои броеви се конгруентни се сведува на изучување на елиптичната крива $E : y^2 = x^3 - n^2x$.

- Прстенот $\mathbb{Z}$ не е поле, што значи дека во општ случај $E(\mathbb{Z})$ не е група.
- Меѓутоа, множеството од сите точки на елиптична крива со целобројни координати е конечно.

Siegel, 1928

Нека E е елиптична крива дефинирана со равенката $E : y^2 = x^3 + ax + b$, каде што $a, b \in \mathbb{Z}$. Тогаш множеството $E(\mathbb{Z})$ е конечно.

- На пример, Диофантовата равенка $y^2 = x^3 - x$ има само конечно целобројни решенија.

- Елиптични криви се користат во доказот на познатата Голема теорема на Ферма.

Голема теорема на Ферма

Нека $n > 2$ е природен број. Тогаш не постојат природни броеви a, b, c кои што ја задоволуваат равенката $a^n + b^n = c^n$.

- Во доказот се користи дека ако постои непарен прост број p и цели броеви $abc \neq 0$ такви што $a^p + b^p = c^p$, тогаш елиптичната крива $y^2 = x(x - a^p)(x + b^p)$ не може да биде модуларна.

- Можеме да рабтиме и со елиптични криви над конечни полиња како што е $\mathbb{F}_p$.
- Ако кривата е дефинирана со $y^2 = x^3 + ax + b$, веднаш се гледа дека $E(\mathbb{F}_p)$ нема повеќе од $2p + 1$ точки. Постои уште попрецизна проценка.

Hasse, 1922

Нека E е елиптичната крива дадена со равенката $y^2 = x^3 + ax + b$, каде што $a, b \in \mathbb{F}_p$. Тогаш важи неравенството:

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}.$$

- Елиптични криви сè повеќе се користат и во криптографија.
- Причината зошто е поефикасно податоците да се шифруваат со елиптични криви е затоа што е многу потешко да се реши проблемот на дискретен логаритам во однос на нивната група на рационални точки.

- Да претпоставиме дека A и B сакаат да ја осигураат нивната комуникација. Треба прво да фиксираат елиптична крива, како и некоја точка P од ред n.
- A тогаш треба да замисли број d_A и јавно да ја сподели точката $Q_A = d_A \cdot P$, додека B треба да замисли број d_B и јавно да ја сподели точката $Q_B = d_B \cdot P$.
- На овој начин на A и B им е познато колку е $d_A \cdot Q_B = d_B \cdot Q_A$, додека некој трет мора да го реши проблемот на дискретен логаритам за да ја добие оваа информација.