Torzijske grupe eliptičkih krivulja nad kvadratnim poljima

Antonela Trbović

Motivacija

Diofantske jednadžbe (tj. polinomijalne jednadžbe) nad Z, Q ili nekim drugim nama zanimljivim poljima (ili prstenima) proučavaju se još od stare Grčke. Zanimaju nas rješenja tih jednadžbi, odnosno postoje li uopće načini za određivanje postoje li rješenja takvih jednadžbi. Najpoznatiji takav problem je Fermatov zadnji teorem, koji nam govori kako ne postoje cijeli brojevi a, b, c strogo veći od 1 i n veći od 3 takvi da je $a^n + b^n = c^n$. Dokazao ga je Andrew Wiles 1994. godine, a ključnu ulogu u dokazu imale su eliptičke krivulje.

Za jednostavnije oblike diofantskih jednadžbi u dvije varijable, koje određuju krivulju genusa 0, problem određivanja rješenja je riješen. No, promatramo li kompliciraniji slučaj, tj. kubne diofantske jednadžbe u dvije varijable, one određuju krivulju genusa 1. To nas motivira da proučavamo eliptičke krivulje.

Imamo li eliptičku krivulju E definiranu nad poljem algebarskih brojeva K, znamo (prema Mordell-Weilovom teoremu) da ona ima oblik $E = T \times Z^r$, gdje je T podgrupa elemenata konačnog reda, torzijska podgrupa, a r neki cijeli broj veći od 0. Prirodno se postavlja pitanje koje su njene moguće torzijske podgrupe. Odgovor na to pitanje je za eliptičke krivulje definirane nad Q dao Mazur 1978. godine. Kasnije je dokazan sličan rezultat za eliptičke krivulje definirane nad kvadratnim poljima. No, taj rezultat nam ne govori ništa o tome koje torzijske grupe bismo mogli imati kada fiksiramo neko kvadratno polje. To je bila glavna motivacija za nastanak ovog rada.

Eliptičke krivulje

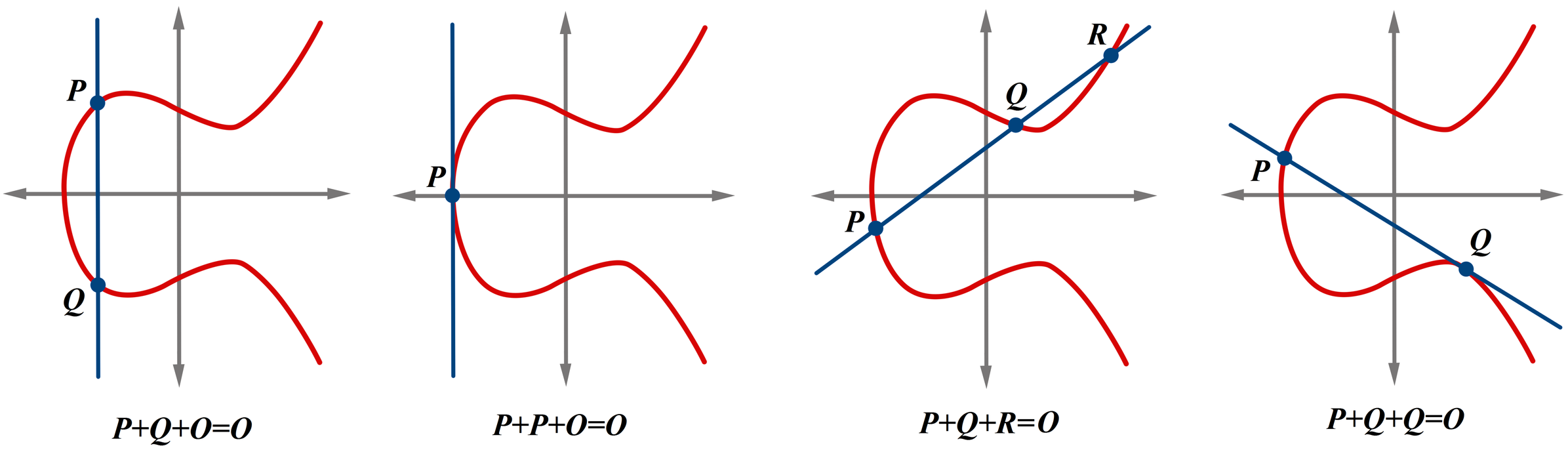
Neka je K polje. Eliptička krivulja nad K je nesingularna projektivna kubna krivulja nad K s barem jednom (K-racionalnom) točkom.

Na eliptičkoj krivulji E možemo definirati zbrajanje na način da je P+Q+R=O ako točke P, Q, i R leže na istom pravcu, gdje je O točka u beskonačnosti. Na donjim slikama možemo vidjeti definiciju zbrajanja po slučajevima. Eliptička krivulja s tako definiranim zbrajanjem čini Abelovu grupu, a Mordell-Weilov teorem kaže da je ta grupa konačnogenerirana. Prema strukturnom teoremu o konačnogeneriranim Abelovim grupama, znamo da je E oblika $E = T \times Z^r$, gdje je T torzijska grupa. Sljedeći (Mazurov) teorem nam govori koje su moguće torzijske grupe eliptičkih krivulja nad Q:

Neka je E eliptička krivulja. Tada je njena torzijska grupa izomorfna jednoj od sljedećih 15 grupa:

$$Z/nZ, \quad n=1,2,...,10,12,$$
$$Z/2Z + Z/2nZ, \quad n=1,2,3,4.$$

Sličan rezultat imamo i za eliptičke krivulje nad kvadratnim poljima, u kojem imamo 26 mogućih torzijskih grupa kada prolazimo po svim eliptičkim krivuljama nad svim kvadratnim poljima. No, nas zanima što se događa ako fiksiramo jedno kvadratno polje.



Rezultati

Fiksirajmo kvadratno polje $\mathbb{K} = \mathbb{Q}(\sqrt{13})$.

Grupe

$$\mathbb{Z}/n\mathbb{Z}, \ n = 1,2,...,10,12$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \ n = 1,2,3,4$$

(iz Mazurovog teorema) se pojavljuju kao torzijske grupe nad svakim kvadratnim poljem, a grupe

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, \ n = 1,2,$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

nisu moguće torzijske grupe nad ovim poljem.

Od preostalih grupa prvo promatramo one grupe čije su pripadne modularne krivulje eliptičke krivulje, a zatim one čije su pripadne modularne krivulje hipereliptičke krivulje. Dajemo jedan primjer.

Propozicija. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/11\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je $Y_1(11)(\mathbb{Q}(\sqrt{13}))$ beskonačan skup, tj. da na modularnoj krivulji $X_1(11)(\mathbb{Q}(\sqrt{13}))$ osim kuspova ima još beskonačno mnogo točaka. Budući da znamo da kuspova ima samo konačno mnogo, nije ih potrebno računati, već će biti dovoljno vidjeti da je rang $rk(X_1(11)(\mathbb{Q}(\sqrt{13})))$ pozitivan.

Za modularnu krivulju

$$X_1(11): \ y^2 - y = x^3 - x^2$$

računamo rang nad $\mathbb{Q}(\sqrt{13})$,

$$rk(X_1(11)(\mathbb{Q}(\sqrt{13}))) = 1,$$

a jedan generator grupe $X_1(11)(\mathbb{Q}(\sqrt{13}))$ (modulo torzijska podgrupa), tj. točka beskonačnog reda je dana sa:

$$\left(\frac{1}{9}(-2\sqrt{13}+5), \frac{1}{27}(-2\sqrt{13}+32)\right).$$

Zaključujemo da se na toj modularnoj krivulji (i kada oduzmemo broj kuspova) nalazi još beskonačno mnogo točaka. Svaka od tih točaka je uređeni par jedne eliptičke krivulje (do na izomorfizam) nad $\mathbb{Q}(\sqrt{13})$ zajedno s točkom reda 11 na toj eliptičkoj krivulji. □

Na kraju, imamo sljedeći teorem:

Teorem. *Moguće torzijske grupe eliptičkih krivulja nad kvadratnim poljem* $\mathbb{Q}(\sqrt{13})$ *su:*

$$\mathbb{Z}/n\mathbb{Z}, \ n = 1,...,12,15,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \ n = 1,2,3,4,5,6.$$

Slične rezultate smo dokazali za još 3 najmanja realna kvadratna polja, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{7})$, i $\mathbb{Q}(\sqrt{11})$.

Prirodoslovno—matematički fakultet
Matematički odsjek
Zavod za algebru i osnove matematike

kontakt e-mail autora:
antonela.trbovic@gmail.com