Uvod u aritmetiku eliptičkih krivulja

l-adski brojevi - 20. lekcija

U elementarnoj teoriji brojeva (koja se bavi cijelim i racionalnim brojevima) postoje tri važne konstrukcije.
Prva je razmatranje ostataka modulo m, za neki cijeli broj m (različit od $0, -1, 1$). Taj je skup konačan prsten koji ima djelitelje nule, osim ako je m prost, kada je polje. Postoji prirodni surjektivni homomorfizam s prstena cijelih brojeva na prsten ostataka modulo m.
Druga je smještanje prstena cijelih brojeva u prsten cijelih algebarskih brojeva. Na primjer, izraz $a^2 + b^2$ ne može se rastaviti nad cijelim brojevima, dok na cijelim gaussovim brojevima vrijedi $a^2 + b^2 = (a + bi)(a - bi)$.
Treća je smještanje prstena cijelih brojeva u prsten $\mathbf{Z}_p$ cijelih p-adskih brojeva, za svaki prosti broj p. Pri tom se polje racionalnih brojeva smješta u polje p-adskih brojeva $\mathbf{Q}_p$. Sa staništa analize konstrukcija p-adskih brojeva analogna je konstrukciji realnih brojeva iz racionalnih (upotpunjenju), samo što se tu upotpunjenje vrši u tzv. p-adskoj apsolutnoj vrijednosti. S algebarskog stanovišta riječ je o razmatranju "uskladjenih" kongruencija modulo p^n za svaki prirodni broj n. Tu ćemo važnu konstrukciju opisati u sljedeće dvije lekcije, samo što ćemo umjesto oznake p za proste brojeve, koristiti oznaku l. Prije opisa te konstrukcije dat ćemo još jedan, čisto algebarski, dokaz komutativnosti Galoisove grupe $Gal(K_n/\mathbf{Q}(i))$ iz predhodne lekcije, u kojemu će se nazrijeti ta konstrukcija.

Eliptička krivulja $E : y^2 = x^3 + x$ ima kompleksno množenje s i, preciznije

$$\phi : E \to E;\ \phi(x, y) = (-x, iy)$$

je endomorfizam različit od svakog množenja $[m]$ s cijelim brojevima $P \mapsto mP$. Vidjeli smo da je ϕ i automorfizam od E.

Teorem 1. Neka je $E : y^2 = x^3 + x$ i n prirodan broj. Tada postoji baza od $E[n]$ nad $\mathbf{Z}/n\mathbf{Z}$) oblika $(P, \phi P)$.
Dokaz. Neka je (P, Q) bilo koja baza za ϕ i neka je u toj bazi automorfizmu ϕ pridružena (invertibilna) matrica

$$\rho_n(\phi) = A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Gl_2(\mathbf{Z}/n\mathbf{Z}).$$

To znači da je $\phi(P) = aP + cQ$ i $\phi(Q) = cP + dQ$, taj je prikaz jednoznačan za brojeve a, b, c, d modulo n. Sad dokaz provodimo u nekoliko koraka.
(I) Dovoljno je pokazati da postoji takva baza za koju je c invertibilan modulo n, tj. da je $(c, n) = 1$ (analogno za b). Naime, tada bi $(P, \phi P)$ bila dobra baza. Za to je dovoljno provjeriti da relacija $r\phi(P) = sP$ implicira $r = s = 0$ modulo n. Iz $\phi(P) = aP + cQ$ slijedi $r\phi(P) = arP + crQ$, a kad bi bilo $r\phi(P) = sP$ bilo bi $cr = s - ar = 0$, a kako je c invertibilan, bilo bi $r = 0$, a onda i $s = 0$.
(II) Ako je $n = l$, prost broj, tvrdnja teorema vrijedi. Možemo predpostaviti da je $l \neq 2$, jer za $l = 2$ imamo dobru bazu $((i, 0), (-i, 0))$ koja je oblika $(P, \phi(P))$.
Sad dokaz provodimo tako da predpostavimo da po volji odabrana baza (P, Q) ne zadovoljava (I), tj. da automorfizmu ϕ odgovara matrica

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$$

s koeficijentima iz polja ostataka modulo l. Zato bi u bazi $(P + Q, Q)$ automorfizam ϕ imao matricu

$$\begin{bmatrix} a & 0 \\ d-a & d \end{bmatrix}.$$

Ta matrica zadovoljava (I), što je nama dovoljno. Naime, u suprotnom bi bilo $d = a$, a odatle bi bilo $\phi(T) = T$ za sve T. Posebno bi bilo $\phi(P) = aP$ i $\phi(\bar{P}) = a\bar{P}$, za bazni element $P = (u, v)$. Odatle bismo dobili

$$\overline{\phi(\bar{P})} = aP$$

jer je kompleksno konjugiranje kao preslikavanje na $E[l]$ takodjer linearno prelikavanje (kao i svaki element Galoisove grupe). Sad je:
$aP = \overline{\phi(\bar{u}, \bar{v})} = \overline{(-\bar{u}, i\bar{v})} = (-u, -iv) = -(-u, iv) = -\phi(P)$.
Zaključujemo da je $-a = a$ pa je, zbog neparne karakteristike, $a = 0$, što je kontradikcija.
(III) Ako tvrdnja teorema vrijedi za n, ona vrijedi i za nl. Dokaz dijelimo u dva dijela, ovisno o tome je li n djeljiv s l ili nije.
(i) $l|n$.
Neka je (P, Q) dobra baza za $E[n]$, tj. neka u toj bazi preslikavanje ϕ ima matricu

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ modulo } n.$$

Neka je par (P', Q') bilo koji sa svojstvom $lP' = P$ i $lQ' = Q$ (takvi parovi zaista postoje). Tvrdimo da je (P', Q') baza za $E[nl]$, a za to je dovoljno pokazati da iz $rP' = sQ'$ slijedi $r = s = 0$ modulo nl. Množenjem relacije $rP' = sQ'$ s l dobijemo $rP = sQ$, odakle slijedi $r = s = o$ modulo n. Sad samo treba pokazati da je $r = s = n$ modulo nl nemoguće. Zaista, kad bi tako bilo, bilo bi;
$r = \alpha n$ i $s = \beta n$ za neke $\alpha, \beta = 0, 1, ..., l - 1$.
Sad bismo iz $\alpha n P' = \beta n Q'$ dobili $(\alpha \frac{n}{l})P = (\beta \frac{n}{l})Q$, a odatle $\alpha = \beta = 0$, što je kontradikcija.
Dakle (P', Q') je baza na $E[nl]$ pa neka ϕ u toj bazi ima matricu

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ modulo } nl.$$

Odatle je $\phi(P') = aP' + cQ'$ pa je $\phi(P) = \phi(lP') = laP' + lcQ' = aP + bQ$, a kako je $\phi(P) = Q$, zaključujemo da je $c = 1$ modulo n, posebice c je invertibilan modulo n, pa prema (I) zaključujemo da ima dobra baza za $E[nl]$.
(ii) l ne dijeli n.
Neka je (P, Q) dobra baza za $E[n]$ i neka je (P_l, Q_l) dobra baza za $E[l]$.
Neka su, dalje, P_1, Q_1 jedinstvene točke iz $E[n]$ za koje je $lP_1 = P$ i $lQ_1 = Q$ (one postoje jer l ne dijeli n, a zato su i jedinstvene).
Sad definiramo

$$(P', Q') := (P_1 + P_l, Q_1 + Q_l).$$

Tvrdimo da je (P', Q') baza za $E[nl]$. Za dokaz, kao i prije, predpostavimo da je $rP' = sQ'$ i dokažimo da je $r = s = 0$ smodulo nl.
;Množenjem gornje jednakosti s l dobijemo $rP = sQ$, pa je $r = s = 0$ modulo n.
Množenjem, pak, s n dobijemo $rnP_l = snQ_l$ pa je, jer l ne dijeli n, $rP_l = sQ_l$, odnosno $r = s = 0$ modulo l.
Sve skupa daje $r = s = 0$ modulo nl.
Sad kad znamo da je (P', Q') baza za $E[nl]$, neka preslikavanju ϕ u toj bazi odgovara matrica

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ modulo } nl.$$

Odatle, slično kao u (i) dobijemo

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ modulo } n.$$

Jednako tako dobijemo

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ modulo } l.$$

Te dvije relacije za posljedicu imaju da je c relativno prost s nl, pa prema (I) postoji dobra baza za $E[nl]$.
Dokaz završavamo primjedbom da je (II) baza indukcije, a (III) korak indukcije s obzirom na broj prostih faktora od n.

Pojava l-adskih brojeva. Pri dokazu teorema, dio (III), pojavila se konstrukcija baze za $E[nl]$ iz baze za $E[n]$ tako da ako je preslikavanju ϕ na $E[nl]$ bila pridružena matrica $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ modulo nl, odnosno matrica $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ modulo n na $E[n]$, onda je vrijedilo

$$\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ modulo } n.,$$

što znači da je $a' = a$ modulo n, $b' = b$ modulo n, itd. Tu treba uočiti i to da je a' zadan modulo nl, a a modulo n, itd.
Posebno, ako gledamo samo (III) (i), kad $l|n$, onda možemo startati s $n = l$, pa nastaviti s $l^2, l^3, ...$, tj. gledati module točaka konačnog reda
$E[l], E[l^2], E[l^3], ..., E[l^n], E[l^{n+1}], ...$,
onda na njima tako možemo izabrati baze da pripadne matrice za ϕ ali i za bilo koje drugo linearno preslikavanje budu redom
$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ modulo l, $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ modulo l^2, $\begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$ modulo $l^3, ...$
i da bude $a_2 = a_1$ modulo l, $a_3 = a_2$ modulo l^2, itd. (a isto i za $b_1, b_2, b_3, ...$ itd.).
Dakle, pojavio se niz brojeva

$$(a_1, a_2, a_3, ...)$$

takav da je n-ta koordinata zadana modulo l^n i da za svaki prirodni n bude $a_{n+1} = a_n$ modulo l^n. Takvi se nizovi zovu l-adski brojevi i o njima govorimo u sljedećoj lekciji.