Uvod u aritmetiku eliptičkih krivulja

Konstrukcija i svojstva l-adskih brojeva - 21. lekcija

Definicija. Neka je l fiksiran prost broj i neka n prolazi skupom prirodnih brojeva. **Cijeli** l-adski broj je, prema definiciji, niz brojeva

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

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.

Ovo je jedna od konstrukcija cijelih l-adskih brojeva (inače uobičajeno je govoriti o p-adskim brojevima, ali u ovom kontekstu povijesno se pojavljuje oznaka l). Vrijedi sljedeće:
(i) Definicija jednakost cijelih l-adskih brojeva. Dva su cijela l-adska broja $a = (a_1, a_2, a_3, ...)$ i $b = (b_1, b_2, b_3, ...)$ jednaka ako je $a_n = b_n$ za sve n.

(ii) Skup svih cijelih l-adskih brojeva (oznaka $\mathbf{Z}_l$) je komutativni prsten s jedinicom uz neutralni element $0 := (0, 0, 0, ...)$, suprotni element $-a := (-a_1, -a_2, -a_3, ...)$, $1 := (1, 1, 1, ...)$, te uz pokomponentno zbrajanje i množenje, tj.
$a + b := (a_1 + b_1, a_2 + b_2, a_3 + b_3, ...)$; $ab := (a_1b_1, a_2b_2, a_3b_3, ...)$.
Lako se pokaže da je sve dobro definirano i da svojstva vrijede (tu je bitno da je prirodno preslikavanje s cijelih brojeva modulo l^{n+1} na cijele brojeve modulo l^n homomorfizam prstena - koji je ujedno i surjekcija). Na primjer, ako je $a_{n+1} = a_n$ modulo l^n i $b_{n+1} = b_n$ modulo l^n, onda je i $a_{n+1}b_{n+1} = a_nb_n$ modulo l^n.

(iii) Prsten cijelih brojeva $\mathbf{Z}$ prirodno se ulaže u prsten cijelih l-adskih brojeva preko $m \mapsto (m, m, m, ...)$. Od sad ćemo l-adski broj $(m, m, m, ...)$ jednostavno označavati kao m. Posebice, pisat čemo $m(a_1, a_2, a_3, ...)$ umjesto $(ma_1, ma_2, ma_3, ...)$.

(iv) Svaki se cijeli l-adski broj $(a_1, a_2, a_3, ...)$ različit od nule jednoznačno zapisuje kao $l^r(b_1, b_2, b_3, ...)$ gdje je r prirodan broj ili 0, a $(b_1, b_2, b_3, ...)$ je l-adski broj sa svojstvom $b_1 \neq 0$ modulo l.

za dokaz neka je $r+1$ prvi indeks n za koji je $a_n \neq 0$ modulo l^n. Dakle, $a_r = 0$ modulo l^r, pa je i $a_{r+1} = 0$ modulo l^r. Zato je $a_{r+1} = l^r b_1$ gdje je $b_1 \neq 0$ modulo l. Dalje $a_{r+2} = a_{r+1}$ modulo l^{r+1} pa je i a_{r+2} djeljiv s l^r. Slično je a_{r+2} djeljiv s l^r itd. Zato su dobro definirani brojevi $b_2, b_3, ...$ tako da bude

$$a = l^r(b_1, b_2, b_3, ...).$$

Kako je $l^r b_k = a_{r+k}$, za sve k, vrijedi $l^r b_{k+1} = l^r b_k$ modulo l^{r+k}, pa je $b_{k+1} = b_k$ modulo l^k, što znači da je sve dobro definirano.

(v) $\mathbf{Z}_l$ je prsten bez djelitelja nule. To proizlazi izravno iz (iv), jer ako su a, c različiti od nule, onda je
$a = l^r(b_1, b_2, b_3, ...)$ i $c = l^s(d_1, d_2, d_3, ...)$, gdje su $b_1, d_1 \neq o$ modulo l. Kako je $ad = l^{r+s}(b_1d_1, b_2d_2, b_3d_3, ...)$ i kako je $b_1d_1 \neq 0$ modulo l , zaključujemo da je $ab \neq 0$.

(vi) $a = l^r(b_1, b_2, b_3, ...)$ je invertibilan ako i samo ako je $r = 0$ i $b_1 \neq 0$ modulo l. Drugim riječima $a = (a_1, a_2, a_3, ...)$ je invertibilan ako i samo ako je $a_1 \neq 0$.
Jedan je smjer očit: ako je a invertibilan, mora tako biti. Za obrat, ako je $r = 0$, onda $a = (b_1, b_2, b_3, ...)$, a kako je $b_1 \neq 0$, postoji cijeli c_1 takav da je $b_1c_1 = 1$ modulo l. Posebno $c_1 \neq 0$ modulo l. Kako je $b_2 = b_1$ modulo l, vidimo da je b_2 invertibilan modulo l^2. Zato postoji cijeli broj c_2 sa svojstvom $b_2c_2 = 1$ modulo l^2. Slično konstruiramo brojeve c_3, c_4 itd. tako da vrijedi $b_nc_n = 1$ modulo l^n za sve n. Tada je $c := (c_1, c_2, ...)$ inverz od a. Da to dokažemo dovoljno je vidjeti da je c zaista cijeli l-adski broj. Treba vidjeti da je $c_2 = c_1$ modulo l, zatim da je $c_3 = c_2$ modulo l^2 itd. Zaista:
$c_2 - c_1 = \frac{1}{a_2} - \frac{1}{a_1} = \frac{a_1 - a_2}{a_1 a_2} = 0$ modulo l. Slično:
$c_3 - c_2 = \frac{1}{a_3} - \frac{1}{a_2} = \frac{a_2 - a_3}{a_2 a_3} = 0$ modulo l^2 itd.
Uočite da smo usput dokazali i to da je $a := (a_1, a_2, ...)$ invertibilan ako i samo ako su svi a_n invertibilni.

(vii) Prsten $\mathbf{Z}_l$ ima jedinstveni prosti ideal (koji je onda ujedno i maksimalan). To je glavni ideal generiran s l, tj. $\mathcal{P}_l := l\mathbf{Z}_l = \{a \in \mathbf{Z}_l : a_1 = 0\}$ modulo l.
Lako se dokazuje da $\mathbf{Z}_l/\mathcal{P}_l \equiv \mathbf{Z}/l\mathbf{Z}$.

(viii) Prema (v) dobro je definirano polje razlomaka $\mathbf{Q}_l$ od $\mathbf{Z}_l$. Vidimo

da se svaki element od $\mathbf{Q}_l$ jednoznačno zapisuje kao

$$l^r u$$

gdje je r cijeli broj, a u je invertibilan element od $\mathbf{Z}_l$.

Primjer. Znamo da jednadžba $x^2 = 2$ nema rješenja u polju racionalnih brojeva $\mathbf{Q}$.
(A) Ta jednadžba nema rješenja u $\mathbf{Q}_3$. Dovoljno je pokazati da ona nema rješenja u $\mathbf{Z}_3$. Naime, kad bi $a := (a_1, a_2, ...)$ bilo rješenje te jednadžbe, bilo bi $a_1^2 = 2$ modulo 3, a to je nemoguče.
(B) Ta jednadžba ima rješenja u $\mathbf{Z}_7$. Naime, kako je $2 = 3^2$ modulo 7, možemo staviti $a_1 = 3$. Za a_2 možemo staviti 10 jer je $10 = 3$ modulo 7 i $10^2 = 2$ modulo 7^2 itd.
Da pokažemo da to uvijek možemo sprovesti, predpostavimo da smo konstruirali dobre $a_1, a_2, ..., a_n$. Dakle, vrijedi $a_n^2 = 2 + m7^n$ za neki cijeli m. Tada stavimo

$$a_{n+1} = a_n + k7^n$$

pri čemu ćemo k izabrati tako da bude $a_{n+1}^2 = 2$ modulo 7^{n+1}. Dakle, treba biti
$a_n^2 + 2a_n k7^n + k^2 7^{2n} = 2$ modulo 7^{n+1}, a za to je dovoljno da bude $m + 2a_n k = 0$ modulo 7,
tj. $k = m$ modulo 7.
Napomenimo da smo ovako pokazali da se polje $\mathbf{Q}(\sqrt{2})$ ne može smjestiti u $\mathbf{Q}_3$, ali da se to polje može smjestiti u $\mathbf{Q}_7$. Govoreći malo neprecizno $\sqrt{2} \notin \mathbf{Q}_3$, ali $\sqrt{2} \in \mathbf{Q}_5$.

U sljedečoj lekciji ova če nam konstrukcija poslužiti za opis tzv. l-adske reprezentacije Galoisove grupe u grupu regularnih matrica s koeficijentima u $\mathbf{Z}_l$.