Uvod u aritmetiku eliptičkih krivulja

Dokaz Lutz-Nagell-ova teorema - 9.lekcija

Vidjeli smo da se Lutz-Nagell-ov teorem sastoji od dva dijela. Pokazuje se da je teži onaj dio koji govori da su torzijske točke na cjelobrojnom W. modelu nužno cjelobrojne. To je upravo tvrdnja (II) iz predhodne lekcije. Da pokažemo kako iz tog dijela teorema slijedi drugi dio potrebna je samo jedna dobro poznata činjenica o diskriminanti D polinoma

$$f(x) := x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3),$$

naime da postoje polinomi h_1, h_2 s cjelobrojnim koeficijentima tako da bude

$$h_1(x)f(x) + h_2(x)g(x) = D, \tag{1}$$

gdje je g brojnik u duplikacijskoj formuli (iz 6. lekcije - tamo je $x = x(P)$ i $y = y(P)$)

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + (b^2 - 4ac)}{4y^2}. \tag{2}$$

Pokušajte sami naći h_1, h_2 uz napomenu da je h_1 drugog, a h_2 trećeg stupnja.

Dokaz kriterija iz L-N teorema, modulo tvrdnja (II).
Neka je P točka konačnog reda za koju je $y(P) \neq 0$. Tada je $2P \neq O$ i $2P$ je takodjer torzijska, pa su, prema tvrdnji (II), brojevi $x(P), y(P), x(2P), y(2P)$ cijeli. Prema formuli (2) vrijedi $y(P)^2 | g(x(P))$, a kako je $y(P)^2 = f(x(P))$, iz (1) slijedi $y(P)^2 | D$, kako smo i htjeli.

Priprema za dokaz tvrdnje II.
Sad vidimo da je za dokaz Lutz-Nagell-ova teorema dovoljno pokazati da su torzijske točke na cjelobrojnom W. modelu cjelobrojne. Za dokaz se podsjetimo diskretne valuacije u prostom broju p. Ako se racionalni broj q različit od nule napiše kao $q = p^r \frac{m}{n}$ gdje su m, n, p medjusobno relativno prosti, onda definiramo $v_p(q) := r$.
Sad se dokaz provodi tako da se pokaže, da za svaku racionalnu torzijsku točku $P(x, y)$, uz $y \neq 0$, eliptičke krivulje $E : y^2 = x^3 + ax^2 + bx + c$ uz cjelobrojne a, b, c, i svaki prosti broj p vrijedi $v_p(x) \geq 0$ i $v_p(y) \geq 0$.
Dokaz se provodi kontradikcijom, pa razmotrimo što znači da je $v_p(x) < 0$ ili

$v_p(y) < 0$ za neki p. Iz jednadžbe eliptičke krivulje evidentno je da vrijedi: $v_p(x) < 0$ akko $v_p(y) < 0$, i tada je $3v_p(x) = 2v_p(y)$, tj. $v_p(x) = -2k,\ i\ v_p(y) = -3k$, za $k \in \mathbf{N}$ (*).
Da lakše provedemo razmatranje uvodimo sljedeće oznake:

$$E(p^k) := \{(x, y) \in E(\mathbf{Q}) : v_p(x) \leq -2k\} \cup \{O\},\ \ k = 1, 2, 3, ...$$

Napominjemo da je prema (*) gornji uvjet ekvivalentan s $v_p(y) \leq -3k$ (jer točke očito nisu reda 2). Takodjer napominjemo da smo dodali O da bi $E(p^k)$ bila grupa, što je za dokaz vrlo važno i što ćemo dokazati poslije.
Vidi se da vrijedi: $E(\mathbf{Q}) \supset E(p) \supset E(p^2) \supset ....$
Vidi se takodjer da je naš cilj pokazati da torzijska točka ne može biti niti u jednom $E(p)$. Pokazuje se da je za provodjenje dokaza vrlo korisno iz afinih x, y koordinata na krivulji prijeći na t, s koordinate oko O, gdje je:

$$s := \frac{1}{y},\ \ t := \frac{x}{y}$$

koje smo već upoznali (uz druge oznake: u, v).
Odmah se vidi da su $E(p^k)$ jednostavno zadani, naime:

$$E(p^k) := \{(t, s) \in E(\mathbf{Q}) : v_p(t) \geq k\} \cup \{O\},\ \ k = 1, 2, 3, ...$$

(naravno, gornji je uvjet ekvivalentan s $v_p(s) \geq 3k$).
Uvedimo sad još jednu korisnu oznaku (relaciju): za racionalne brojeve pišemo $q_1 \equiv q_2 \pmod{p^k}$ ako $v_p(q_2 - q_1) \geq k$.

Dokaz tvrdnje II uz jednu predpostavku.

Predpostavimo da znademo da su skupovi $E(p^k)$ grupe i da za svake dvije točke $P_1, P_2 \in E(p^k)$ vrijedi

$$t(P_1 \oplus P_2) \equiv t(P_1) + t(P_2)\ (mod\ p^{3k}), \tag{3}$$

gdje su $t(P), s(P)$ oznake za t, s koordinate točke P. Neka je sad P torzijska točka reda m koja je u $E(p)$ (podsjetimo da iz te predpostavke treba izvesti kontradikciju). Tada postoji k tako da je $P \in E(p^k)$, ali $P \notin E(p^{k+1})$. Iz (3) zaključujemo da mora biti (sjetite se da je $O(0, 0)$ u t, s koordinatama)

$$0 = t(O) = t(mP) \equiv mt(P)\ (mod\ p^{3k}).$$

Sad smo gotovi ako p ne dijeli m, jer bi to značilo da $t(P) \equiv 0 \ (mod\ p^{3k})$, što bi značilo da je $p \in E(p^{3k})$, što je u kontradikciji s $P \notin E(p^{k+1})$.
Slučaj $p|m$ samo je tehnički nešto složeniji. Naime, tada je $m = pn$ i točka $P' = nP$ ima red p. Sad ponavljamo gornji postupak, ali s točkom P'. Najprije treba napomenuti da je $P' \in E(p)$ (jer je $P \in E(p)$ i $P' = nP$ i $E(p)$ je grupa), pa postoji $l \in \mathbf{N}$ tako da je $P' \in E(p^l)$, ali $P' \notin E(p^{l+1})$. Sad provodimo prijašnji postupak, ali uz P' umjesto P, uz p umjesto m i uz l umjesto k. Dobijemo

$$0 = t(O) = t(pP') \equiv pt(P') \ (mod\ p^{3l}),$$

odakle zaključujemo da je $P' \in E(p^{3l-1})$, što je u kontradikciji s $3l-1 \geq l+1$.

Dokaz da su svi $E(p^k)$ grupe i da vrijedi (3) - skica - detalji u [S-T, str. 49-56]

Priprema dokaza.

Pažljivijom analizom vidimo da je dovoljno pokazati da su skupovi $E(p^k)$ zatvoreni na zbrajanje, medjutim oni su zatvoreni i na promjenu predznaka. Pokazuje se da je puno pogodnije razmatranje provoditi u t, s koordinatama. Opet podsjetimo da u t, s koordinatama E ima jednadžbu

$$s = t^3 + at^2s + bts^2 + cs^3 \tag{4}$$

i da je $O(0,0)$. Uočite da u ovom afinom modelu od E nema točaka $(e_i, 0)$, $i = 1,2,3$ (u x, y koordinatama), medjutim ako neke od njih i jesu racionalne, tj. ako je neki od e_i racionalan, onda su i cjelobrojne, pa nisu u $E(p)$ niti za jedan p.

Transformacije prijelaza iz x, y u t, s koordinate su projektivne, pa pravci prelaze u pravce, pa se grupni zakon provjerava kao i prije (naravno vidi se i izravno da jednadžba $y = \lambda x + \mu$ prelazi u $s = -\frac{\lambda}{\mu}t + \frac{1}{\mu}$)

Ako (4) presječemo s pravcem $s = \alpha t + \beta$, dobijemo, kao i prije, kubnu jednadžbu, i ako su $P_i(t_i, s_i)$, $i = 1,2,3$ tri točke presjeka (vidi sl.2.7 u [S-T] i detalje), onda je

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3} \tag{5}$$

Ako, kako je i prije bilo, predpostavimo da P_1, P_2 imamo, a tražimo P_3, onda je (nakon lakog računa)

$$\alpha = \frac{t_2^2 + t_1t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1s_2 + s_1^2)} \tag{6}$$

(to je za $P_1 \neq P_2$), a ako je $P_1 = P_2$, onda je

$$\alpha = \frac{3t_1^2 + 2at_1s_1 + bs_1^2}{1 - at_1^2 - 2bt_1s_1 - 3cs_1^2} \tag{7}$$

a uvijek je $\beta = s_1 - \alpha t_1$.
Uočite takodjer da ako je (t_0, s_0) na krivulji, onda je $(-t_0, -s_0)$ na krivulji i spojnica kroz te dvije točke prolazi ishodištem $(0,0)$. Zato je (u t, s koordinatama) $-(t,s) = (-t,-s)$.
Dokaz.
Prtedpostavimo da su P_1, P_2 iz $E(p^k)$, tj. $v_p(t_i) \geq k$ i $v_p(s_i) \geq 3k$ za $i = 1, 2$. Tada zahvaljujući jedinici u nazivniku od (6), odnosno (7), dobijemo da je

$$v_p(\alpha) \geq 2k, \ \textit{a onda} \ \ v_p(\beta) \geq 3k.$$

Sad, opet zahvaljujući jedinici u nazivniku od (5) dobijemo

$$v_p(t_1 + t_2 + t_3) \geq 3k$$

što dokazuje relaciju (3), a i grupoidnost. Naime iz te relacije slijedi $v_p(-t_3) = v_p(t_3) \geq k$, a za s koordinatu dobije se slično.