Torzijske točke i djelidbeni polinomi

Cilj ovog seminara je dokazati sljedeci teorem:

Teorem 1. *Neka je E eliptička krivulja nad poljem K i neka je n prirodan broj. Neka karackteristika od K ne dijeli n ili ako je 0, tada je*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n. \tag{1}$$

Ako K ima karakteristiku $p > 0$ i $p|n$, neka je $n = p^r n'$, gdje p ne dijeli n'. Tada je

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ ili } \mathbb{Z}_n \oplus \mathbb{Z}_{n'}. \tag{2}$$

Eliptička krivulja E nad poljem karakteristike p se naziva *obična* ako je $E[p] \simeq \mathbb{Z}_p$. E se nativa *supersingularna* a ako je $E[p] \simeq 0$.
Da bi proučavali torzijske podgrupe, trebamo opisati preslikavanje množenja s prirodnim brojem na eliptičkoj krivulji. To je endomorfizam elitičke krivulje i može se opisati racionalnim funnkcijama. Mi ćemo dati formule za te funkcije.
Počinjemo s varijablama A i B. Definiramo *djelidbeni polinom* $\psi_m \in \mathbb{Z}[x, y, A, B]$ s

$\psi_0 = 0$
$\psi_1 = 1$
$\psi_2 = 2y$
$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ za $m \geq 2$
$\psi_{2m} = (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi m + 1^2)$ za $m \geq 2$

Lema 2. *ψ_n je element prstana $\mathbb{Z}[x, y^2, A, B]$ kada je n neparan, a ψ_n je element od $2y\mathbb{Z}[x, y^2, A, B]$ kada je n paran.*

Dokaz:
Lema očito vrijedi $n \leq 4$. Pretpostavimo, indukcijom, da tvrdnja leme vrijedi za sve $n < 2m$. Možemo pretpostaviti da je $2m > 4$, tj. $m > 2$. Tada vrijedi $2m > m + 2$, tako da svi polinomi koji se pojavljuju u definciji od ψ_{2m} zadovoljavaju pretpostavku indukcije. Ako je m paran, tada su $\psi_m, \psi_{m+2}, \psi_{m-2}$ iz $2y\mathbb{Z}[x, y^2, A, B]$, iz čega slijedi da je i $\psi 2m$. Analogno ako je m neparan, tada su ψ_{m-1} i ψ_{m+1} iz $2y\mathbb{Z}[x, y^2, A, B]$, pa je i ψ_{2m}. Dakle lema vrijedi ako je $n = 2m$. Slučaj $n = 2m + 1$ je trivijalan. **Q.E.D.**

Definiramo polinome

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$$

$$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-1}\psi_{m+1}^2).$$

Lema 3. *$\phi_n \in \mathbb{Z}[x, y^2, A, B]$, $\forall n \in \mathbb{N}$. Ako je n neparan, tada je $\omega_n \in y\mathbb{Z}[x, y^2, A, B]$. Ako je n paran, tada je $\omega_n \in \frac{1}{2}\mathbb{Z}[x, y^2, A, B]$.*

Dokaz:
Ako je n neparan, tada su ψ_{n+1} i ψ_{n-1} iz $y\mathbb{Z}[x, y^2, A, B]$, pa je njihov umnožak iz $\mathbb{Z}[x, y^2, A, B]$. Slijedi da je $\phi_n \in \mathbb{Z}[x, y^2, A, B]$. Dokaz je analogan kada je n paran.
Neka je n neparan. Tada su po Lemi 2 ψ_{n-1}^2i ψ_{n+1}^2 iz $4y^2\mathbb{Z}[x, y^2, A, B]$ iz čega slijedi da je ω_n iz $y\mathbb{Z}[x, y^2, A, B]$.
Ako je n neparan, iz Leme 2 slijedi da je $\omega_n \in \frac{1}{2}\mathbb{Z}[x, y^2, A, B]$.**Q.E.D.**

Promotrimo eliptičku krivulju

$$E: \ y^2 = x^3 + Ax + B, \ 4A^3 + 27B^2 \neq 0 \tag{3}$$

Ne specificiramo iz kojeg su prstena A i B, nego nastavljamo ih promatrati kao varijable. Možemo u navedenim polinomima zamijeniti y^2 s $x^3 + Ax + B$, pa nam svi polinomi koji us bili iz $Z[x, y^2, A, B]$ postaju polinomi iz $Z[x, A, B]$. Također primjetimo da ψ_n nije nužno polinom samo u varijabli x, dok ψ_n^2 je.

Lema 4. *Vodeći član od $\phi_n(x)$ je x^{n^2}, a od $\phi_n^2(x)$ je $n^2x^{n^2-1}$.*

Dokaz:
Tvrdimo da vrijedi

$$\psi_n = \begin{cases} y(nx^{n^2-4)/2} + \cdots) & \text{ako je } n \text{ paran} \\ nx^{n^2-1)/2} + \cdots & \text{ako je } n \text{ neparan.} \end{cases}$$

Ovo dokazujemo indukcijom po slučajevima. Iz gornje jednakosti odmah slijedi tvrdnja leme. Mi ćemo dokazati samo slučaj $n = 2m + 1$, kada je m paran, ostali slučajevi se dokazuju analogno. Vodeći član od $\psi_{m+2}\psi_m^3$ je

$$(m + 2)m^3y^4x^{\frac{(m+2)^2-4}{2}+\frac{3m^2-12}{2}}.$$

Mijenjajući y^4 u $(x^3 + Ax + B)^2$, dobivamo

$$(m + 2)m^3x^{\frac{(2m+1)^2-1}{2}}.$$

Na isti način dobivamo da je vodeći koeficijent od $\psi_{m-1}\psi_{m+1}^3$

$$(m - 1)(m + 1)^3x^{\frac{(2m+1)^2-1}{2}}.$$

Oduzimanjem druge vrijednosti od prve dobivamo da je vodeći koeficijent od ψ_{2m+1} jednak

$$(2m + 1)x^{\frac{(2m+1)^2-1}{2}},$$

što smo i htjeli pokazati.**Q.E.D.**
Iskažimo sada (bez dokaza) sljedeći bitan teorem.

Teorem 5. *Neka je $P = (x, y)$ točka na eliptičkoj krivulji $y^2 = x^3 + Ax + B$ (nad nekim poljem karakteristike različite od 2), te neka je n prirodan broj. Tada je*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3} \right) \tag{4}$$

Korolar 6. *Neka je E eliptička krivulja. Endomorfizam množenje s n je stupnja n je stupnja n^2 (tj. najveći stupanj koji se pojavljuje u brojniku ili nazivniku je n^2).*

Dokaz:
Iz Leme 4 se lako vidi da je najveći mogući stupanj n^2. Tvrdnja teorema je ekvivalentna tvrdnji da su $\phi_n(x)$ i $\psi_n^2(x)$ maksimalno skraćeni, tj. da nemaju zajedničkih korijena. Pokazat ćemo da ovo vrijedi. Pretpostavimo suprotno, te neka je n najmanji indeks za koji ova dva polinoma imaju zajednički korijen.
Pretpostavimo da je $n = 2m$. Prvo primjetimo da vrijede sljedeće jednakosti

$$\phi_2(x) = x^4 - 2Ax^2 - 8Bx + A^2,$$

$$\psi_2^2 = 4y^2 = 4(x^3 + Ax + B).$$

Sada želimo izračunati x-koordinatu od nP. Nju dobivamo prvo množenjem s m, pa zatim s 2. Ona će biti jednaka

$$\frac{\phi_{2m}}{\psi_{2m}}^2 = \frac{\phi_2(\phi_m/\psi_m^2)}{\psi_2^2(\phi_m/\psi_m^2)} = \frac{\phi_m^4 - 2A\phi_m^2\psi_m^4 - 8B\phi_m\psi_m^6 + A^2\psi_m^8}{(4\psi_m^2)(\phi_m^3 + A\phi_m\psi_m^4 + B\psi_m^6)}.$$

Označimo brojnik ovog razlomka s U, a nazivnik s V. Koristit ćemo sljedeću lemu

Lema 7. *Neka je $\Delta = 4A^3 + 27B^3$ i neka je*

$F(x,z) = x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4$
$G(x,z) = 4z(x^3 + Axz^2 + Bz^3)$
$f_1(x,z) = 12x^2z + 16Az^3$
$g_1(x,z) = 3x^3 - 5Axz^2 - 27Bz^3$
$f_2(x,z) = 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3$
$g_2(x,z) =$
$A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 - 3A^2(A^3 + 8B32)z^3.$

Tada vrijedi

$$Ff_1 - Gg_1 = 4\Delta z^7 \text{ i } Ff_2 + Gg_2 = 4\Delta x^7.$$

Dokaz:
Ovo se lako dokaže izravnim računom. Ove jednakosti dolaze iz činjenice da su $F(x,1)$ i $G(x,1)$ relativno prosti, tj. nemaju zajedničkih korijenova, pa su f_1 i g_1 funkcije dobivene Euklidovim algoritmom takve da vrijedi

$F(x,1)f_1(x) + G(x,1)g_1(x) = 1$. Zamjenom x s x/z, te množenjem s z^7 i 4Δ, dobivamo prvu jednakost. Zamjenom uloga od x i z, na isti način dobivamo drugu jednakost. **Q.E.D.**
Iz ove leme slijedi da je

$$U \cdot f_1(\phi_m, \psi_m^2) - V \cdot g_1(\phi_m, \psi_m^2) = 4\psi_m^{14}\Delta,$$

$$U \cdot f_2(\phi_m, \psi_m^2) + V \cdot g_2(\phi_m, \psi_m^2) = 4\phi_m^7\Delta.$$

Vidimo da ako V i U imaju zajednički korijen, tada imaju i ϕ_m i ψ_m^2. Pošto je $n = 2m$ prvi index za koji ovi polinomi imaju zajednički korijen, ovo je kontradikcija.
Još moramo pokazati da vrijedi $U = \phi_{2m}$ i $V = \psi_{2m}^2$. Pošto je $\frac{U}{V} = \frac{\phi_{2m}}{\psi_{2m}^2}$, te U i V nemaju zajednički korijen, slijedi da U dijeli ϕ_{2m} i V dijeli ψ_{2m}^2. Međutim, lako vidimo, koristeći Lemu 4 da je vodeći član od U jednak $4m^2$. Slijedi da je $U = \phi_{2m}$, te $V = \psi_{2m}^2$. Dakle ϕ_{2m} i ψ_{2m}^2 nemaju zajedničkih korijena.
Pretpostavimo sada da je najmanji indeks za koji ovi polinomi imaju zajednički korijen neparan, tj. $n = 2m + 1$. Neka je r korijen od ϕ_n i ψ_n^2. Iz

$$\phi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1},$$

te pošto je $\psi_{n-1}\psi_{n+1}$ polinom u x, slijedi da je $\psi_{n-1}\psi_{n+1}(r) = 0$, pa pošto su $\psi_{n\pm1}^2$ polinomi u x, r je također nultočka njihovog umnoška. Slijedi da je $\psi_{n+\delta}^2(r) = 0$, za $\delta = 1$ ili -1.
Pošto je n neparan, ψ_n i $\psi_{n+2\delta}$ su polinomi u x, te je r nultočka od $(\psi_n\psi_{n+2\delta})^2$, a time i od $\psi_n\psi_{n+2\delta}$. Iz

$$\phi_{n+\delta} = x\psi_{n+\delta}^2 + \psi_n\psi_{n+2\delta},$$

slijedi da je $\phi_{n+\delta}(r) = 0$.
Pošto je $n + \delta$ paran, te pošto smo već pokazali da ako ϕ_{2m} i ψ_{2m}^2 imaju zajedničku nultočku, tada imaju i ϕ_m i ψ_m^2. Pošto smo pretpostavili da je n najmanji takav indeks, mora vrijediti da je $n \leq m = \frac{n+\delta}{2}$. Jedina mogućnost da ova nejednakost vrijedi je $n = \delta = 1$. Međutim, $\phi_1 = x$, a $psi_1^2 = 1$, te očito nemaju zajedničkih korijenova. Dakle, dokazali smo korolar. **Q.E.D.**
Poznato je da ako je $\alpha(x,y) = (R(x), yS(x))$ endomorfizam eliptičke krivulje, tada je *alpha* separabilno preslikavanje ako je $R'(x) \neq 0$. Pošto iz Teorema 5 znamo da je za množenje s n

$$R(x) = \frac{x^{n^2} + \cdots}{n^2 x^{n^2-1} + \cdots},$$

lako se vidi da ako karakteristika p ne dijeli n, tada je brojnik od $R'(x) = n^2x^{2n^2-2} + \cdots \neq 0$. Slijedi da je množenje s n separabilno, pa pošto je, po Korolaru 6, stupanj tog preslikavanja n^2, slijedi da jezgra ima n^2 korijena.

Po teoremu o konačno generiranim Abelovim grupama, slijedi da je $E[n]$ izomorfan s $\mathbb{Z}_{n_1} \oplus \cdots \mathbb{Z}_{n_k}$, gdje je $n_i | n_{i+1}$ za sve i-ove.
Neka je q prost broj koji dijeli n_1. Slijedi da q dijeli n_i za svaki i. Tada $E[q] \leq E[n]$ reda q^k. Međutim, dokazali smo da je $E[q]$ reda q^2, tj. $k = 2$. Slijedi da je $E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$. Međutim, pošto je svaki elemsnt maksimalno reda n, slijedi da $n_2 | n$. Slijedi da je $n_1 = n_2 = n$, tj.

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

kada karakteristika p ne dijeli n.

Ostaje nam za promotriti slučaj kada je $p|n$. Iz svojstava endomorfizma znamo da $E[p]$ je reda manjeg od p^2. Dakle, moguć nosti su da je $|E[p]|$jednak ili 1 ili p. Ako je $E[p]$ trivijalna grupa, slijedi da je $E[p^k]$ trivijalna za sve k-ove.
Pretpostavimo da je $E[p] \simeq \mathbb{Z}_p$. Tvrdimo da je $E[p^k] \simeq \mathbb{Z}_{p^k}$. To ćemo dokazati tako da pokažemo da postoji element reda p^k. Neka je P element reda p^j. Pošto je množenje s p surjekcija, postoji točka Q takva da je $pQ = P$. Pošto vrijedi

$$p^j Q = p^{j-1} P \neq O \text{ i } p^{j+1} Q = p^j P = O,$$

slijedi da je Q reda p^{j+1}. Dakle postoji točka reda p^k za svaki k. Slijedi, zbog $E[p] \simeq \mathbb{Z}_p$, da je $E[p^k] \simeq \mathbb{Z}_{p^k}$.
Neka je sada $n = p^r n'$, gdje p ne dijele n' i $r \geq 0$. Lako se vidi da je

$$E[n] \simeq E[n'] \oplus E[p^r]$$

Pošto karakteristika p ne dijeli n' znamo da je $E[n'] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$. Pošto je $\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} \simeq \mathbb{Z}_n$, zaključujemo da je

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'} \text{ ili } \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}.$$

Time je dokazan Teorem 1. **Q.E.D.**