Uvod u aritmetiku eliptičkih krivulja

1. domaća zadaća

Napomena. Zadatci se odnose samo na lekcije $5, 6i7$.

1. zadatak. (i) Dokažite izravno da je uvjet nesingularnosti krivulje zadane afinom jednadžbom $y^2 = x^3 + Ax + B$ upravo $4A^3 + 27B^2 \neq 0$.
Uputa. Pogledajte petu lekciju. Pokažite da sustav $x^3 + Ax + B = 0,\ 3x^2 + A = 0$ ima rješenje akko $4A^3 + 27B^2 = 0$.
(ii) Primijenite (i) za dobivanje analognog uvjeta za krivulje zadane s $y^2 = x^3 + ax^2 + bx + c$.
Uputa. Iskoristite činjenicu da se polinom $x^3 + ax^2 + bx + c$, zgodnom zamjenom može svesti na oblik $x^3 + Ax + B$. Pogledajte knjigu [Silverman-Tate, poglavlje The discriminant na str. 47.].
2. zadatak. Neka je $E : y^2 = x^3 + ax^2 + bx$; $\bar{E} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Definirajmo $\phi : E \to \bar{E}$ lokalno formulom $\phi(x, y) = (\frac{y^2}{x^2}, y\frac{x^2-b}{x^2})$, za $P \neq T := (0, 0)$ i $P \neq O$. Pokažite da je ϕ dobro definirano i da je definirano za svaki P i da vrijedi $\phi(T) = \phi(O) = O$.
Uputa. Pogledajte 7. lekciju, naročito Primjer 2.
3. zadatak (zadatak 1.18. a),b) i c) u [Silverman-Tate]). Provjerite da eliptička krivulja $y^2 = x^3 + 17$ ima racionalne točke
$P_1(-2, 3),\ P_2(-1, 4),\ P_3(2, 5),\ P_4(4, 9),\ P_5(8, 23)$.
(a) Pokažite da se svaka od P_2, P_4, P_5 može predočiti kao $mP_1 \oplus nP_2$ za neke cijele m, n.
(b) Odredite točke $P_6 := -P_1 \oplus 2P_3$ i $P_7 := 3P_1 \oplus (-P_3)$.
(c) Pronadjite još jednu točku s cjelobrojnim koordinatama različitu od gore spomenutih.
4. zadatak (zadatak 1.20. u [Silverman-Tate]). Pokažite da je $P(3, 8)$ točka eliptičke krivulje $y^2 = x^3 - 43x + 166$. Odredite $P, 2P, 3P, 4P$ i $8P$. Koji zaključak izvodite usporedbom točaka P i $8P$?
5. Neka je eliptička krivulja zadana jednadžbom $y^2 = x^3 + x^2 + x + 1$. Riješite jednadžbu $2P = Q$, ako je $Q(1, 2)$. Što općenito možete reći o jednadžbi $2P = Q$ na eliptičkoj krivulji?