Uvod u aritmetiku eliptičkih krivulja - Zadatci 3.

1. Pokažite da je $E : y^2 = x^3 + x + 1$ eliptička krivulja nad konačnim poljem $\mathbf{F}_p$ za proste brojeve $p = 3, 7, 11, 13$ i odredite grupe $E(\mathbf{F}_p)$ (skup rješenja i strukturu grupe).

2. Za eliptičku krivulju $E : y^2 = x^3 + x$ odredite $E[4]$ i zbrajanje u toj grupi. Izaberite bazu u $E[4]$ i u njoj odredite $\rho_4(G)$, gdje je $G := Gal(\mathbf{Q}(E[4])/\mathbf{Q})$.
Uputa: Pogledajte stranicu 192. u [S-T].

3. Odredite $Gal(\mathbf{Q}(E[2])/\mathbf{Q})$ i $\rho_2(G)$ (uz neki izbor baze od $E[2]$) ako je E zadana jednadžbom
a) $y^2 = x^3 + x - 2$.
b) $y^2 = x^3 - x - 2$.
a) $y^2 = x^3 - 3x + 1$.

4. Dokažite da su $E_1 : y^2 = x^3 + Ax$ i $E_2 : y^2 = x^3 + B$ eliptičke krivulje s kompleksnim množenjem za sve cijele brojeve $A, B \neq 0$.
Odredite $E_1[2]$ i $Gal(\mathbf{Q}(E_1[2])/\mathbf{Q})$ u ovisnosti o A, te $E_2[2]$ i $Gal(\mathbf{Q}(E_2[2])/\mathbf{Q})$ u ovisnosti o B.

5. Neka je $E : y^2 = x^3 + x$ eliptička krivulja, neka je $K_n := \mathbf{Q}(E[n])$ za $n \geq 2$, i neka je $G := Gal(K_n)/\mathbf{Q})$ i $H := Gal(K_n)/\mathbf{Q}(i))$.
Neka τ označava kompleksno konjugiranje. Dokažite:
(i) $\tau \in G$ i $\tau \notin H$.
(ii) Svaki element σ iz G ili je iz H ili se jednoznačno predočuje u obliku $\sigma = s\tau$, za neki $s \in H$.
(iii) Za svaki $s \in H$ vrijedi $s\tau = \tau s^{-1}$.
(iv) G je abelova ako i samo ako je $s^2 = id$ za sve $s \in H$ (tu id označava identitetu).
Uputa. Vidi [S-T, zad. 6.17] i lekciju 19.