2. zadaća

1. zadatak. Neka je eliptička krivulja zadana jednadžbom $y^2 = x^3 + ax^2 + bx + c$, gdje su a, b, c cijeli brojevi. Pokažite da je svaka afina racionalna točka te krivulje oblika $(x, y) = (\frac{m}{e^2}, \frac{n}{e^3})$ za neke cijele brojeve m, e, n takve da je $e > 0$, i $(m, e) = 1$ ili $m = 0$, i $(n, e) = 1$ ili $n = 0$.
Mora li biti $(m, n) = 1$ ili $mn = 0$?.
Uputa. Pogledajte lekciju o Lutz-Nagellovu teoremu ili čitajte [S-T].

2. zadatak. (i) Odredite sve cjelobrojne točke krivulja $y^2 = x^3 \pm px$, za prost broj p.
(ii) Pokušajte odrediti moguće torzijske podgrupe za krivulje $y^2 = x^3 \pm p$. Što više primjera.

3. zadatak. Za rang r eliptičke krivulje $E_p : y^2 = x^3 + px$ pokažite (zad. 3.8. iz [S-T]):
(i) $r = 0, 1$ ili 2.
(ii) Ako je $p \equiv 7$ modulo 16, onda je $r = 0$.
(iii) Ako je $p \equiv 3$ modulo 16, onda je $r = 0$ ili $r = 1$.

4. zadatak. Odredite rang krivulje zadane jednadžbom (vidi [S-T, zad. 3.9.]):
(i) $y^2 = x^3 + 2x$
(ii) $y^2 = x^3 + 3x$
(iii) $y^2 = x^3 + 5x$
(iv) $y^2 = x^3 + 7x$
(v) $y^2 = x^3 + 73x$
(vi) $y^2 = x^3 - 82x$.

5. zadatak. Izaberite neku eliptičku krivulju $y^2 = x^3 + ax^2 + bx$ tako da bude $a \neq 0$ (i da se razlikuje od one iz lekcije) i odredite joj rang.

I.Gusić.