ALGORITMI ZA ELIPTIČKE KRIVULJE

1. zadaća

12. 12. 2008.

1. Pokažite da je krivulja
$$y^2 = x^3 - 2x^2 + x$$
singularna. Odredite joj singularnu točku, te nađite jednu njezinu racionalnu parametrizaciju.

2. Otvoreni tekst na hrvatskom jeziku šifriran je pomoću ElGamalovog kriptosustava, čiji su parametri $p = 31847$, $\alpha = 5$, $a = 7899$, $\beta = 18074$, na sljedeći način. Najprije su slovima pridružene odgovarajuće brojevne vrijednosti: A = 0, B = 1, C = 2, Č = 3, ... , Z = 28, Ž = 29. Potom su tri po tri susjedna slova otvorenog teksta "kodirana" kao elementi od $\mathbb{Z}_n$, kao što pokazuju ovi primjeri:
$$DAN = 5 \cdot 30^2 + 0 \cdot 30 + 18 = 4518, \quad PUT = 21 \cdot 30^2 + 26 \cdot 30 + 25 = 19705.$$
Konačno su ovako dobiveni elementi od $\mathbb{Z}_n$ šifrirani pomoću ElGamalovog kriptosustava s gore navedenim parametrima. Dešifrirajte šifrat
$$(6841, 10449), \quad (8006, 21703),$$
tj. odredite polazni otvoreni tekst na hrvatskom jeziku.

3. Zadana je eliptička krivulja
$$E : \ y^2 = x^3 + 33750x + 2953125.$$
Odredite njezin minimalni Weierstarssov model. Kakvu redukciju (dobru ili lošu; aditivnu ili mutiplikativnu; rascjepivu ili nerascjepivu) ima ta krivulja za $p = 3$?

4. Neka je E eliptička krivulja s jednadžbom
$$y^2 = x^3 + ax + b.$$
Neka je $P = (x_1, y_1)$ točka na E, te neka je $2P = (x_2, y_2)$. Dokažite da vrijedi
$$y_1^2(4x_2(3x_1^2 + 4a) - 3x_1^3 + 5ax_1 + 27b) = 4a^3 + 27b^2.$$

5. Pokažite primjerom da eliptička krivulja s jednadžbom
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
gdje su $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, može imati točku konačnog reda čije koordinate nisu cjelobrojne.

6. Nađite sve točke konačnog reda, te odredite strukturu torzijske grupe za sljedeće eliptičke krivulje:
   a) $y^2 = x^3 + 3x + 7$
   b) $y^2 = x^3 - 19x + 30$
   c) $y^2 = x^3 - 219x + 1654$
   d) $y^2 = x^3 - 12987x - 263466$
   e) $y^2 = x^3 - 1386747x + 368636886$

   Pokažite da u svakom od ovih primjera postoje prosti brojevi p_1, p_2, takvi da $p_i \nmid 2\Delta$, za koje vrijedi
$$|E(\mathbb{Q})_{\text{tors}}| = \text{nzd}(|E(\mathbb{F}_{p_1})|, |E(\mathbb{F}_{p_2})|).$$

Rok za predaju zadaće je 21.1.2009.

Andrej Dujella