ALGORITHMIC ASPECTS OF ELLIPTIC CURVES

22. 5. 2007.

1. Let x_1, x_2, x_3 be the zeros of the polynomial $f(x) = x^3 + ax + b$. Prove that
$$(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = -4a^3 - 27b^2.$$

2. Find the order of the point $P = (3, 8)$ on the elliptic curve $y^2 = x^3 - 43x + 166$ over $\mathbb{Q}$.

3. Find all points of finite order and describe the structure of the torsion group for the following curves over $\mathbb{Q}$:

   a) $y^2 = x^3 - x$, b) $y^2 = x^3 + 4$, c) $y^2 = x^3 + x + 2$, d) $y^2 = x^3 - 43x + 166$.

4. For the polynomial
$$p(x) = (x-18)(x-16)(x-15)(x-13)(x-12)(x-11)(x-10)(x-9)(x+15)(x+16)(x+17)(x+18),$$
find polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $p(x) = q^2(x) - r(x)$ and $\deg r \leq 4$.

5. For each $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$, find an elliptic curve E_n over $\mathbb{F}_5$ such that $\#E_n(\mathbb{F}_5) = n$.

6. For the point $P = (0, 376)$ on the elliptic curve $y^2 = x^3 - x + 188$ over $\mathbb{F}_{751}$, compute $[100]P$.

7. The elliptic curve E over $\mathbb{F}_{151}$ is given by the equation $y^2 = x^3 + x + 4$. Compute $\#E(\mathbb{F}_{151})$ by Shanks-Mestre method, using the point $P = (0, 2)$.

8. The elliptic curve E over $\mathbb{F}_{11}$ is given by the equation $y^2 = x^3 + x + 6$.

   a) Prove that $\alpha = (2, 7)$ is a generator of the group $E(\mathbb{F}_{11})$.

   b) Using Menezes-Vanstone cryptosystem with public keys E, α and $\beta = (7, 2)$, encrypt the plaintext $(x_1, x_2) = (9, 1)$, using $k = 6$.

Andrej Dujella