Algebraic Cryptography
Homework 6

Due Monday, 4 December 2017

Problem 1. Show that a linear change of variables can be used to transform the left side of the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

over a field $\mathbb{F}$ to the form:

(a) y^2 if $\mathrm{Char}(\mathbb{F}) \neq 2$;

(b) $y^2 + xy$ if $\mathrm{Char}(\mathbb{F}) = 2$ and the xy-term in equation (1) is nonzero (i.e., $a_1 \neq 0$).

Problem 2. If $\mathrm{Char}(\mathbb{F}) = 2$, show that there is no elliptic curve with equation (1) where $a_1 = a_3 = 0$.

Problem 3. In the case when $\mathrm{Char}(\mathbb{F}) \neq 2$, from the first problem we can write an equation for an elliptic curve in the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{2}$$

where the coefficients on the right are possibly different from the original ones, but this is not important. Show that this curve is smooth if and only if the cubic polynomial on the right has no multiple roots (in the algebraic closure $\overline{\mathbb{F}}$).

Problem 4. Each of the following points has finite order on the given elliptic curve over $\mathbb{Q}$. In each case, find the order of P.

(a) $P = (0, 16)$ on $y^2 = x^3 + 256$.

(b) $P = \left(\frac{1}{2}, \frac{1}{2}\right)$ on $y^2 = x^3 + \frac{1}{4}x$.

(c) $P = (3, 8)$ on $y^2 = x^3 - 43x + 166$.

Problem 5. (a) Describe in detail the Elliptic Curve Diffie–Hellman Key Exchange and ElGamal Message Transmission methods.

(b) Consider the Elliptic Curve Diffie–Hellman Problem (ECDHP), the ElGamal Problem (EGP) and the Elliptic Curve Discrete Log Problem (ECDLP). Prove that ECDHP and EGP are equivalent, and that both problems reduce to ECDLP.

(c) Explain why (we think) that ECDHP and EGP are secure schemes.

Problem 6. Let G be a group whose order is B-smooth. Prove that there is a polynomial time algorithm (the input size is B) to solve the Discrete Log Problem to base $g \in G$. More specifically, given $g, y \in G$, your algorithm should output an integer x less or equal to the order of g such that $g^x = y$; *or state that no such x exists.* (Note: for this problem you may assume without proof that the Chinese Remainder Theorem has an $O(\ln(N)^2)$ algorithm where N denotes the "big" modulus in the CRT, i.e., $N = n_1 \cdots n_k$ where $n_1, \ldots, n_k$ are relatively prime).