MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #12

Problems for all

Problem 1. Let E be the elliptic curve given by the equation $y^2 = x^3 + x^2 + 1$ over $\mathbb{F}_3$.

(a) Determine all points of $E(\mathbb{F}_3)$.
(b) Make an addition table for $E(\mathbb{F}_3)$.

Problem 2.

(a) Factor $n = 35$ by the elliptic curve method by using the elliptic curve $y^2 = x^3 + 26$ and calculating 3 times the point $P = (10, 9)$.
(b) Suppose you want to factor a composite integer n by using the elliptic curve method. You start with the curve $y^2 = x^3 - 4x$ and the point $(2, 0)$. Why will this not yield the factorization of n?

Problem 3. Alice and Bob use a Diffie-Hellman exchange with the elliptic curve $E : y^2 = x^3 + 383$ over $\mathbb{F}_{2003}$ with $\#E(\mathbb{F}_{2003}) = 2004$ and the point $G = (977, 314)$. Alice sends Bob the point $(930, 937)$ and Bob sends Alice the point $(425, 1182)$. What is their common secret key? *[Hint: Use baby-step giant-step to solve an elliptic curve discrete logarithm problem.]*

Additional problems for 395A

Problem 4. The theorem of Hasse (second version) is the following.

Theorem (Hasse)**.** *For every elliptic curve E over the finite field $\mathbb{F}_q$, there exists $\pi \in \mathbb{C}$ with $|\pi| = \sqrt{q}$ such that for all $n \geq 1$, one has*

$$E(\mathbb{F}_{q^n}) = (\pi^n - 1)(\overline{\pi}^n - 1).$$

(a) Assuming this theorem, prove that $|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$.
(b) Define $t_0, t_1, t_2, \ldots$ by $t_0 = 2$, $t_1 = q + 1 - \#E(\mathbb{F}_q)$, and

$$t_n = t_1 \cdot t_{n-1} - qt_{n-2},$$

for $n \geq 2$. Using Hasse's theorem, prove that for all n one has

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - t_n.$$

The integers t_i are called the *traces of Frobenius*.
(c) Let E be the elliptic curve given by $y^2 = x^3 - x + 1$ over $\mathbb{F}_3$. Determine $\#E(\mathbb{F}_3)$, prove that $E(\mathbb{F}_3) = E(\mathbb{F}_9)$, and compute $\#E(\mathbb{F}_{27})$ and $\#E(\mathbb{F}_{81})$.

Date: Due Wednesday, 10 December 2008.