

Math 497A Homework 12
Fall 2008
Due: Friday, December 5

- (1) Let E be a curve over K with equation $y^2 = x^2(x+a)$. Let $E_{ns}(K)$ be the nonsingular points on E with coordinates in K . Let $\alpha^2 = a$. Consider the map

$$\psi : (x, y) \mapsto \frac{y + \alpha x}{y - \alpha x}, \infty \mapsto 1.$$

- (a) Show that if $\alpha \in K$, then ψ gives an isomorphism from $E_{ns}(K)$ to K^* .
(b) Show that if $\alpha \notin K$, then ψ gives an isomorphism

$$E_{ns}(K) \cong \{u + \alpha v : u, v \in K, u^2 - \alpha v^2 = 1\},$$

where the right-hand side is a group under multiplication.

(For this problem, just show that the above map is a bijection. Proving that ψ is a homomorphism will give extra credit.)

- (2) In this exercise we describe a version of the $p + 1$ factoring method. In the next exercise we will relate this to the elliptic curve factorization method applied to a singular curve $y^2 = x^2(x + a)$.

Let p be an odd prime factor of the integer n that we want to factor. Let $t_0 = 2$ and choose a random integer $t_1 \pmod{n}$. Define t_m by the recurrence relation

$$t_{m+2} = t_1 t_{m+1} - t_m$$

for $m \geq 0$. Let β, γ be the two roots of $f(X) = X^2 - t_1 X + 1$ in \mathbb{F}_{p^2} . Assume that $\beta, \gamma \notin \mathbb{F}_p$. Let $s_m = \beta^m + \gamma^m$ for $m \geq 0$.

- (a) Show that $\beta^{m+2} = t_1 \beta^{m+1} - \beta^m$ for $m \geq 0$, and similarly for γ .
(b) Show that $s_{m+2} = t_1 s_{m+1} - s_m$ for all $m \geq 0$.
(c) Show that $t_m \equiv s_m \pmod{p}$ for all $m \geq 0$.
(d) Show that β^p is a root of $f(X) \pmod{p}$, and that $\beta^p \neq \beta$. Conclude that $\gamma = \beta^p$.
(e) Show that $\beta^{p+1} = 1$, and that $\gamma^{p+1} = 1$.
(f) Show that $t_{p+1} - 2 \equiv 0 \pmod{p}$.
(g) Show that if $p + 1 \mid B!$ for some bound B then $\gcd(t_{B!} - 2, n)$ is a multiple of p . Since there are ways to compute $t_{B!} \pmod{n}$ quickly, this gives a factorization method.

- (3) Consider a curve E given by $y^2 = x^2(x + a) \pmod{n}$ where a is not a square mod p . (Again, p will be a divisor of n .) Choose a random point P on E . To factor n by the elliptic curve method we compute $(B!) \cdot P$. By Problem 1, $P \pmod{p}$ corresponds to an element $\beta = u + v\sqrt{a} \in \mathbb{F}_{p^2}$ with $u^2 - v^2 a = 1$.

- (a) Show that β is a root of $X^2 - 2uX + 1$.
(b) Show that $B!P = \mathcal{O} \pmod{p}$ if and only if $\beta^{B!} = 1$ in \mathbb{F}_{p^2} .
(c) Let $t_1 = 2u$ and define the sequence t_m as in Problem 2.

Show that $B!P = \mathcal{O} \pmod{p}$ if and only if p divides $\gcd(t_{B!} - 2, n)$. Therefore the elliptic curve method factors n exactly when the $p + 1$ method factors n .

- (4) Let $n = 199843247$. Using the elliptic curve $E : y^2 = x^3 + 59x - 59$, the point $P = (1, 1)$, and the integer $k = 16296$, compute $kP \pmod{n}$ as in Lenstra's algorithm to find a non-trivial factor of n .