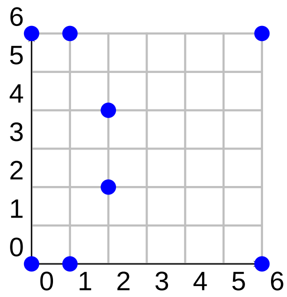
Freshman Seminar 21n: Elliptic Curves

William Stein

March 18, 2003



$y^2 + y = x^3 - x$ over $\mathbb{F}_7$

1 Remarks

This week is about **elliptic curves over finite fields**. These yield encryption algorithms with small key sizes, are of central importance in the best known factorization algorithms, and are crucial to understanding elliptic curves over $\mathbb{Q}$.

If $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$, then MAGMA can easily compute the group associated to the elliptic curve defined by $y^2 = x^3 + ax + b$. Here's an example:

```
> AbelianGroup(EllipticCurve([GF(7)|1,3]));
Abelian Group isomorphic to Z/6 Defined on 1 generator
Relations: 6*$.1 = 0
```

2 Reading Assignment

Read pages **121–138** of Silverman-Tate and Chapter 11 of my book (which I will give to you). Please carefully write up the solutions to your problems and give them to Grigor around April 1, 2003.

3 Problems

1. (Jenna) Let $N = pq$ be a product of distinct odd primes and let $a, b \in \mathbb{Z}/N$ be such that $\gcd(4a^3 + 27b^2, N) = 1$. Let E be the elliptic curve defined by $y^2 = x^3 + ax + b$. Prove that reduction modulo p and modulo q induces an isomorphism
$$E(\mathbb{Z}/N) \to E(\mathbb{Z}/p) \times E(\mathbb{Z}/q).$$

2. (Jeff) Let m be a positive integer. Prove that any subgroup of $\mathbb{Z}/m \times \mathbb{Z}/m$ can be generated by two elements. (Hint: Count ℓ-torsion for each prime ℓ.)

3. (Alex) Let $p \equiv 3 \pmod 4$ be a prime, and let $b \in \mathbb{F}_p^*$.

   (a) Show that the equation $v^2 = u^4 - 4b$ has $p-1$ solutions (u, v) with $u, v \in \mathbb{F}_p$.

   (b) Show that if (u, v) is a solution of the equation in (a), then

   $$\phi(u,v) = \left(\frac{1}{2}(u^2+v),\ \frac{1}{2}u(u^2+v)\right)$$

   is a point on the elliptic curve

   $$C:\ y^2 = x^3 + bx.$$

   (c) Prove that the curve C defined in (b) satisfies $\#C(\mathbb{F}_p) = p + 1$.

4. (Jennifer) Let C be a cubic curve given by a Weierstrass equation

   $$y^2 = x^3 + ax^2 + bx + c$$

   with integer coefficients. Let $p \geq 3$ be a prime not dividing the discriminant, so when we reduce C modulo p we get a nonsingular cubic curve $\tilde{C}$ with coefficients in $\mathbb{F}_p$. We define a general *reduction modulo p map* from $C(\mathbb{Q})$ to $\tilde{C}(\mathbb{F}_p)$ as follows: Let

   $$P = (x,y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in C(\mathbb{Q}).$$

   If p does not divide d, we choose an integer e such that $de \equiv 1 \pmod p$ and set

   $$\tilde{P} = (\tilde{a}\tilde{e}^2,\ \tilde{b}\tilde{e}^3) \in \tilde{C}(\mathbb{F}_p).$$

   If p does divide d, we set $\tilde{P} = \tilde{\mathcal{O}}$. Show that this map is a homomorphism from $C(\mathbb{Q})$ to $\tilde{C}(\mathbb{F}_p)$, and that its kernel is the subgroup $C(p)$ from II.4,5 of Silverman-Tate. Thus, there is a one-to-one homomorphism

   $$\frac{C(\mathbb{Q})}{C(p)} \longrightarrow \tilde{C}(\mathbb{F}_p).$$

   Since $C(p)$ has no torsion, this implies the reduction theorem.

5. (Mauro) Let E be the elliptic curve $y^2 + y = x^3 + x$. You may assume that $E(\mathbb{Q})$ is generated by $P = (0,0)$. Use the result of Exercise 4 (and a computer) to compute $C(p)$ for $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

6. (Jeff) 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 $kP \pmod n$ to find a nontrivial factor of n.

7. (Jenna) Suppose $n > 1$ is an integer. Make a conjecture about whether or not $\mathbb{Z}/n$ must be isomorphic to a group $E(\mathbb{F}_p)$ for some elliptic curve E over some finite field $\mathbb{F}_p$. Support your conjecture with evidence.