

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang  
Scribe: Iftikhar A Burhanuddin  
burhanud@usc.edu  
Class #2 - January 16, 2002

**Administrivia:** Scribe notes for class #1 and Koblitz's paper [1] is online at the course webpage: <http://www-rcf.usc.edu/~mdhuang/cs599>

Office hours: 1-2pm Th

**Today's class:** Walk thru' Elliptic Curves using [1]  
Elliptic curves can be defined over any field  $\mathbf{K}$ :

1. Fields with characteristic 0:  $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \dots$
2. Fields with non-zero char (prime)  $p$ :  $\mathbf{F}_p = \mathbf{Z}/n\mathbf{Z}, \mathbf{F}_{p^n}, \dots$

Curves over finite fields cannot be *easily* drawn on the board. We'll stick to  $\mathbf{EC}/\mathbf{R}$  for visualization purposes.

Elliptic curves over field  $\mathbf{k}$  (where  $\text{char } \mathbf{K} \neq 2, 3$ ):

$$E : y^2 = x^3 + ax + b$$

where  $a, b \in \mathbf{K}$  and the discriminant  $\Delta_E = 4a^3 + 27b^2 \neq 0$ , together with a special point  $\infty$  called the point at infinity. See [1] for the case where  $\text{Char } \mathbf{K}$  is 2 or 3.

In a *general* position if we pick two points on the curve and draw a straight line  $L : y = \lambda x + \mu$ , through them you expect a third point of intersection because there is a cubic on the right of  $E$ ,  $x^3 + ax + b$ , i.e., in general  $|L \cap E| = 3$ .

$E :=$  points on the curve plus "one point at  $\infty$ ".

In Figure 2 though the intersection of the x-axis and  $E : x^3 + x = 0$  has just one solution in  $\mathbf{R}$ , it has three solutions in  $\mathbf{C}$ .

On the other hand, in Figure 3 the intersection of the x-axis and  $E$ , i.e.,  $x^3 - x = 0$  has three solutions in  $\mathbf{R}$  itself, namely  $0, \pm 1$ .

**Addition on  $E$**  a.k.a Group Law:

$P_1, P_2 \in E$  with  $P_1 \neq P_2$  and drawing a line  $L$  thru  $P_1, P_2$ , we get a third point  $P_3$  i.e.  $L \cap E = \{P_1, P_2, P_3\}$ , we write

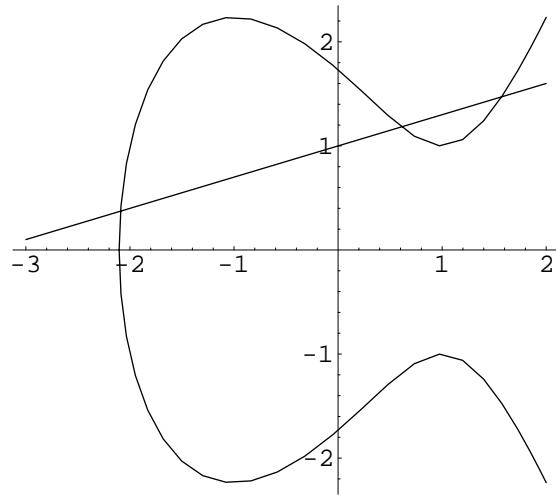


Figure 1:  $E: y^2 = x^3 - 3x + 3, \Delta = 135$

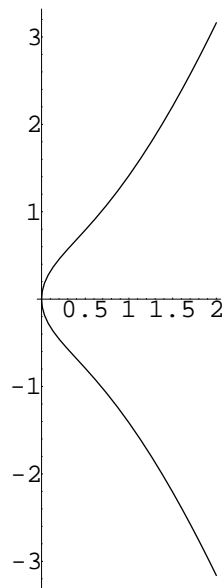


Figure 2:  $E: y^2 = x^3 + x, \Delta = 4$

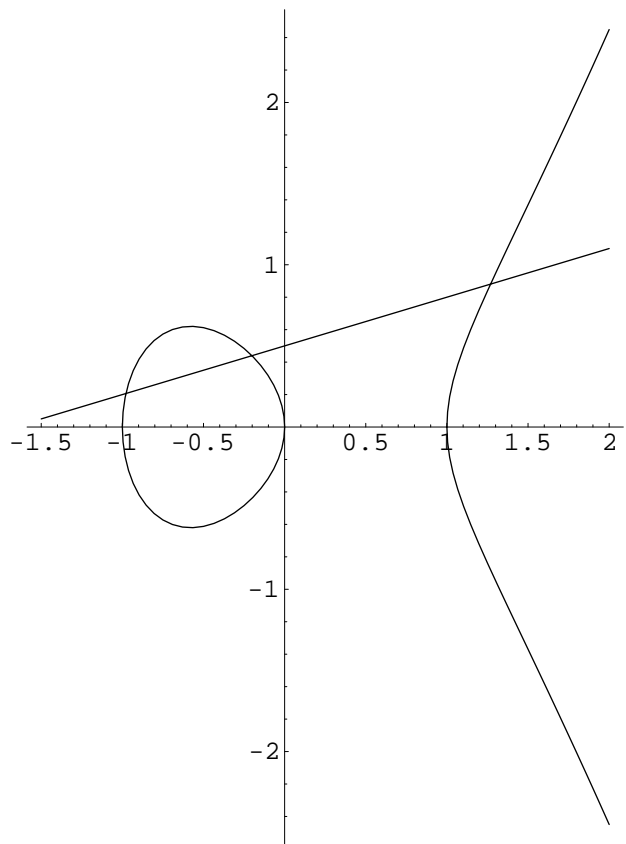


Figure 3: E:  $y^2 = x^3 - x, \Delta = -4$

$$P_1 \oplus P_2 \oplus P_3 = O$$

i.e.,  $P_1 \oplus P_2 = -P_3$ , where we define the additive inverse of a point as follows: if  $P = (x, y) \in E$ , then  $-P = (x, -y) \in E$ .

Where is the identity? It is the point of infinity  $O$  and it is unique!

$P \in E, P \oplus O = P$ , i.e.,  $P \oplus (-P) \oplus O = O$

When we talk about the group law we are forced to think of “the” point at infinity.

**Plane curves:**

Let  $F(x, y) = 0$  be a polynomial in two variables that represents a plane curve. For example  $F : y^2 - (x^3 + ax + b)$

Say  $P = (x_0, y_0) \in F$ , i.e.,  $F(x_0, y_0) = 0$ . WLOG,  $P=(0,0)$  by using coordinate transformation

$$\begin{aligned} F(x, y) = & Ax + By \text{ linear terms} \\ & + F_2(x, y) \text{ homogenous deg 2 terms - } x^2, xy, y^2 \\ & + F_3(x, y) \text{ homogenous deg 3 terms} \\ & + \dots \text{ higher degree terms} \end{aligned}$$

$F$  can be viewed as a real-valued function in 2 variables. Using the Taylor series expansion of the value of  $F$  near the origin:

$$\begin{aligned} F(x, y) &= \frac{\partial F}{\partial x}(0, 0)x + \frac{\partial F}{\partial y}(0, 0)y + \dots \\ &= (Ax + By) + \dots \end{aligned}$$

If  $A \neq 0$  or  $B \neq 0$ , then near  $(0, 0)$  the higher degree terms are insignificant and behave like error terms, hence the linear terms are a good approximation. In terms of the curve defined by  $F$ , in this case  $(0, 0)$  is called a *simple point* and  $Ax + By = 0$  the *tangent line* to  $F$  at  $(0, 0)$ .

In  $E : y^2 = x^3 - x$ ,  $F = y^2 - (x^3 - x)$  the linear term is  $x$ , and  $x = 0$  is the tangent at  $(0, 0)$ .

If the partial derivative is zero, then we don't have a linear term and the terms  $F_m$  with smallest degree are ones with  $\text{deg } m > 1$ . In this case,  $(0, 0)$  is a multiple point. In this case, the tangents are not unique. More precisely,  $F_m = \prod L_i^{r_i}$  where  $L_i$  is a tangent line of multiplicity  $r_i$ . For elliptic curves this gives us the degenerate cases.

*Example 1 -*

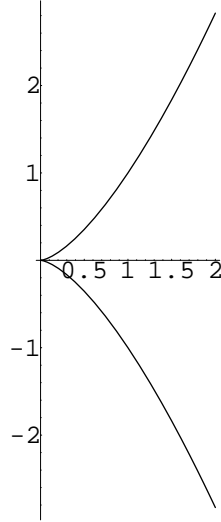


Figure 4:  $E : y^2 = x^3, F = y^2 - x^3, \Delta = 0$

In Figure 4 the point  $(0,0)$  is a double intersection of  $y = 0$  with the curve. So we have one tangent direction of order 2, such a singularity is called a *cusp*.

*Example 2 -*

In curve in Figure 5 has no linear term and in this case we have two tangent directions  $y^2 - x^2 : (y - x)$  and  $(y + x)$  at  $(0,0)$ . Such a singularity is called a *node*.

*Example 2' -*

This example also gives rise to a node, but  $F$  is not an elliptic curve. The curve in Figure 6 has two tangent directions at  $(0,0)$ , namely  $(y - x)$  and  $(y + x)$ .

**The classification of singularities:**

Say  $F(0,0)=0$ . A plane curve can be thought as the summation of homogenous degree  $i$  terms  $F_i$

$$F = F_m + F_{m+1} + F_{m+2} + \dots$$

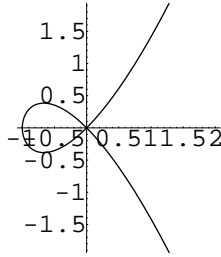


Figure 5:  $E : y^2 = x^2(x + 1), F = y^2 - x^2(x + 1) = (y^2 - x^2) - x^3$

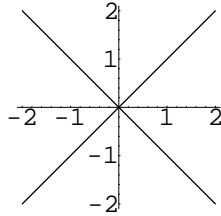


Figure 6:  $F = y^2 - x^2 = (y^2 - x^2)$

where  $F_m \neq 0$  is the minimum degree non-zero term.

If  $m = 1$ , then the point  $(0, 0)$  is a non-singular or smooth point.

If  $m > 1$ , then  $(0, 0)$  is a singularity. If the tangents at the point are distinct, we have an ordinary singularity. An ordinary singularity of multiplicity 2 is called a node.

For a curve  $y^2 = x^3 + ax + b$ , an ordinary singular point is a node, otherwise we have a cusp. For further details on classes please refer to the standard references.

**Theorem:**  $\Delta_E \neq 0 \Leftrightarrow E$  has no singularity.

*Proof:*  $E : y^2 = x^3 + ax + b, F = y^2 - (x^3 + ax + b), \text{char} \neq 2, 3$

$$\frac{\partial F}{\partial x} = 0 \Rightarrow 3x^2 + a = 0$$

$$\frac{\partial F}{\partial y} = 0 \Rightarrow 2y = 0$$

A cluster/loci of singularities on  $E$  are the set of points satisfying:

$$F(x, y) = 0, 3x^2 + a = 0, y = 0$$

Note: The same proof doesn't hold for char 2, 3

$$\Rightarrow x^3 + ax + b = 0, 3x^2 + a = 0$$

$\Rightarrow$  the polynomial and its first derivative are simultaneously zero

$\Rightarrow x^3 + ax + b = 0$  has multiple roots

Using the second condition  $3x^2 + a = 0 \Rightarrow x^2 = -\frac{a}{3} \Rightarrow x^3 = -\frac{ax}{3}$ .

Substituting  $x^3 = -\frac{ax}{3}$  into the first condition  $x^3 + ax + b = 0$ ,

$\Rightarrow -\frac{ax}{3} + ax + b = 0 \Rightarrow x = -\frac{3b}{2a}$

Substituting  $x = -\frac{3b}{2a}$  into the second condition  $3x^2 + a = 0$ ,

$\Rightarrow 3x^2 = -a = \frac{9b^2}{4a^2}$

Substituting values of  $x$  and  $a$  into the second condition  $3x^2 + a = 0$ ,

$\Rightarrow \frac{4a^3 + 27b^2}{4a^2} = 0$ .

So for  $a \neq 0, 4a^3 + 27b^2 \neq 0 \Rightarrow$  no singularities.

Hence we can take the non-zeroness of the discriminant of the polynomial as an indicator of the smoothness of the Elliptic curve.

Denoting  $2P = P \oplus P, 2P + Q = O$

If you have a node, you have two tangents at a point and are in a fix on what the double of point  $P$  is. By removing the singular points, the remaining points together with the point at infinity are closed under addition and form a group.

Consider  $E : y^2 = x^3 + 1/\mathbf{Q}$ .

$(1, \sqrt[3]{2}) \notin E(\mathbf{Q})$  but  $\in E(\mathbf{R})$ , that is there is no rational point on the curve with  $x = 1$ .

Another point on the curve is  $(1, \sqrt[3]{2}\zeta_3) \notin E(\mathbf{Q})$  but  $\in E(\mathbf{C})$ , where  $\zeta_3 = e^{\frac{2\pi i}{3}}$  is the 3th root of unity.

Note: the point at infinity is considered a rational point.

The set of  $\mathbf{F}_p$ -points on the curve are:

$$E(\mathbf{F}_p) = \{(x, y) \mid y^2 = x^3 + ax + b, x, y \in \mathbf{F}_p\} \cup \{\infty\}$$

Let  $K$  be any field, the set of  $K$ -points on the curve are:

$$E(\mathbf{K}) = \{(x, y) \mid y^2 = x^3 + ax + b, x, y \in \mathbf{K}\} \cup \{\infty\}$$

*Theorem:* If  $\mathbf{K}$  is finite then  $\#E(\mathbf{K})$  is also finite.

Let  $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbf{K})$ , then  $P_1 \oplus P_2 = (x_3, y_3)$ , where  $x_3 = \lambda^2 - x_1 - x_2$  and  $y_3 = \lambda(x_1 - x_3) - y_1$  and if  $P_1 \neq P_2, \lambda = \frac{y_2 - y_1}{x_2 - x_1}$

Given that  $y_2 - y_1 \in \mathbf{K}$  and  $x_2 - x_1 \in \mathbf{K} \Rightarrow \lambda \in \mathbf{K}$ .

Important fact: Add two  $\mathbf{K}$ -points and you get another  $\mathbf{K}$ -point, that is  $E(\mathbf{K})$  is closed under the group law.

$$P_1 \in E(\mathbf{K}), P_2 \in E(\mathbf{K}) \Rightarrow P_1 \oplus P_2 \in E(\mathbf{K})$$

Elliptic curves are not only geometric but also arithmetic.

The set of (algebraic) points on  $E$  is  $E(\overline{\mathbf{K}})$ , where  $\overline{\mathbf{K}} :=$  algebraic closure of  $\mathbf{K}$ , and it contains the roots of polynomials  $\in \mathbf{K}[x]$ . For example,  $(\pi, \sqrt{\pi^3 + 1})$  is not an algebraic point of  $y^2 = x^3 + 1$ .

Note:  $E(\overline{\mathbf{Q}}) \subset E(\mathbf{C})$ , strict containment where  $\overline{\mathbf{Q}}$  is the algebraic closure of  $\mathbf{Q}$ .

$$\begin{aligned} \text{Let } \mathbf{F}_{p^n} &= \mathbf{F}_p[x]/(f) = \mathbf{F}_p(\alpha) \\ &= \{a_0\alpha + a_1\alpha^2 + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbf{F}_p\}, \end{aligned}$$

where  $f$  is an irreducible polynomial of degree  $n$  and  $f(\alpha) = 0$ , that is  $\alpha$  is a root of  $f$ .

$$\text{Theorem: } \mathbf{F}_{p^n} \subseteq \mathbf{F}_{p^m} \Leftrightarrow n \mid m$$

$$\overline{\mathbf{F}}_p = \mathbf{F}_p \cup \mathbf{F}_{p^2} \cup \mathbf{F}_{p^3} \dots$$

$$\text{Example: } E : y^2 = x^3 + 1 / \mathbf{F}_5$$

|       |   |   |   |   |   |
|-------|---|---|---|---|---|
| $z$   | 0 | 1 | 2 | 3 | 4 |
| $z^2$ | 0 | 1 | 4 | 4 | 1 |

|     |         |   |         |   |   |
|-----|---------|---|---------|---|---|
| $x$ | 1       | 2 | 3       | 4 | 5 |
| $y$ | $\pm 1$ | ? | $\pm 2$ | ? | 0 |

$$E(\mathbf{F}_5) = \{\infty, (0, \pm 1), (2, \pm 2), (4, 0)\}. \text{ Hence } \#E(\mathbf{F}_5) = 6.$$

Similarly we can compute  $\#E(\mathbf{F}_{5^2}), \#E(\mathbf{F}_{5^3}), \dots$ . Also note that  $E(\mathbf{F}_5) \subset E(\mathbf{F}_{5^2})$ , that is strict containment.

$$E(\mathbf{K}) \text{ is abelian, i.e., } P \oplus Q = Q \oplus P.$$

### Bibliography:

1. Neal Koblitz, Alfred Menezes and Scott Vanstone, The State of Elliptic Curve Cryptography, Designs, Codes and Cryptography, 19, 173-193, 2000.