

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang
Scribe: Iftikhar A Burhanuddin
burhanud@usc.edu
Class #3 - January 23, 2002

Administrivia: Scribe notes for class #2 are online at the course web-page: <http://www-rcf.usc.edu/~mdhuang/cs599>

Today's class:

1. Recap of class #2 - singularities,
2. Projective geometry
3. Counting points

Consider the real line, as you move away from the origin towards the right you approach $+\infty$ and towards the left of the origin you approach $-\infty$. If you took this line and made it compact topologically speaking, that is you folded it, you would get a circle with the two infinities becoming the point at infinity O . There is a 1 - 1 correspondence between the points on the line and the non-infinity points on the circle.

The points in the top half of the circle and left (right) of O get mapped to the left (right) part of line outside the circle and the points in the bottom left (right) half of the circle get mapped to the left (right) part of the line inside the circle as shown in Figure 1.

Similarly you can imagine compacting the affine plane into a sphere and you will be able to project the sphere onto an affine plane.

Projective Geometry:

We define the *projective 1-space* to be the set of 2-tuples (u, v) , with u, v not both zero such that $(u, v) \sim (u', v')$ iff there is some λ such that $(u, v) = \lambda(u', v')$.

Each point on the circle is uniquely determined by (u, v) and is a canonical representative of each equivalence class.

The equivalence relation \sim , partitions the affine plane $\mathbf{A}^2 - (0, 0)$ into equivalence classes and this gives us the projective 1-space.

$$\mathbf{A}^2 - (0, 0) / \sim = \mathbf{P}^1$$

More generally the *projective n-space* $\mathbf{P}^n = \mathbf{A}^{n+1} - 0 / \sim$

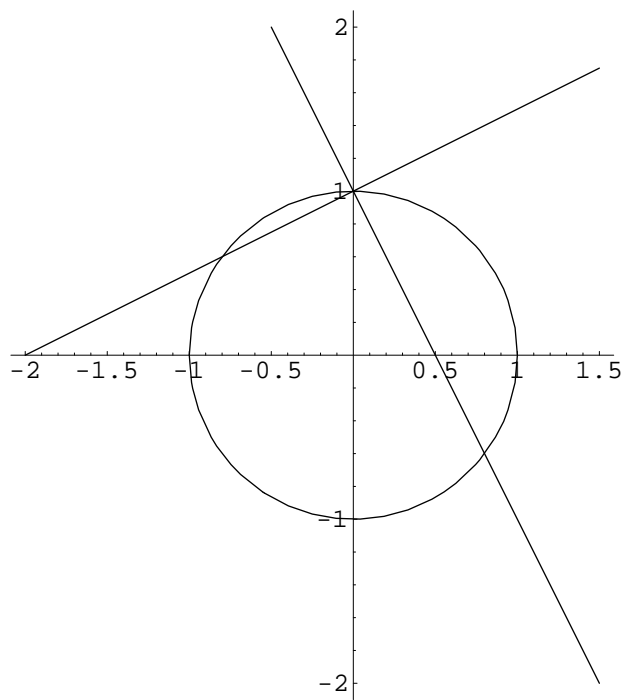


Figure 1: Projecting conic onto line

Homogenization:

A homogenous polynomial is one where the sum of the powers of variables in each term is the same. Hence homogenizing $y^2 = x^3 + ax + b$ gives us a homogenous polynomial of degree 3, $y^2z = x^3 + axz^2 + bz^3$.

In the projective plane $\mathbf{P}^2 = \mathbf{A}^3 - 0/ \sim$, $(0 : 1 : 0) \sim (0 : 2 : 0)$ and $(1 : 2 : 3) \sim (2 : 4 : 6)$

When the z -coordinate is not-zero, the class of points $(x : y : z)$ in the projective plane is equivalent to $(\frac{x}{z} : \frac{y}{z} : 1)$

In particular the set of points on the curve $E : y^2 = x^3 + ax + b$ in the projective plane is denoted by

$$\tilde{E} = \{(x : y : z) \mid y^2z = x^3 + axz^2 + bz^3\}$$

Note: Affine (projective) plane refers to affine (projective) 2-space.

If you have a point in the affine plane (u, v) then $(u, v, 1)$ satisfies $y^2z = x^3 + axz^2 + bz^3$. The map ψ embeds the affine plane into the projective plane:

$$\begin{aligned} \psi : \mathbf{A}^2 &\hookrightarrow \mathbf{P}^2 \\ (x, y) &\rightarrow (x : y : 1) \in \tilde{E} \end{aligned}$$

There are two types of points on $y^2z = x^3 + axz^2 + bz^3$

1. $z \neq 0$: The *affine* part $(x, y) \rightarrow (x : y : 1)$
2. $z = 0$: Plugging $z = 0$ in $y^2z = x^3 + axz^2 + bz^3 \Rightarrow x = 0$. But in the construction of $\mathbf{P}^2 [= \mathbf{A}^3 - (0, 0, 0)/ \sim]$ we exclude $(0, 0, 0) \Rightarrow y \neq 0$. Hence $(0 : y : 0) \sim (0 : 1 : 0) \in \tilde{E}$ is the missing point - the point at infinity

$(x, y) \in E \quad \rightarrow \quad E : y^2 = x^3 + ax + b \subseteq \mathbf{A}^2$
$(x : y : 1) \in \tilde{E} \quad \rightarrow \quad \tilde{E} : y^2z = x^3 + axz^2 + bz^3 \subseteq \mathbf{P}^2$

The view at infinity:

We dehomogenize the equation $E' : y^2z = x^3 + axz^2 + bz^3$ by setting $\hat{x} = \frac{x}{y}$ and $\hat{z} = \frac{z}{y}$. The equation is transformed into $\hat{E} : \hat{z} = \hat{x}^3 + a\hat{x}\hat{z}^2 + b\hat{z}^3$. The point $(x : y : z) \in E'$ with $y \neq 0$ is equivalent to $(\frac{x}{y} : 1 : \frac{z}{y})$ and is mapped to $(\hat{x}, \hat{z}) \in \hat{E}$

\hat{E} can be transformed to it's equivalent Weierstrass form. The point $(0, 0)$ corresponds to the point of infinity in E and the tangent at this point in \hat{E}

is $\hat{z} = 0$. \hat{E} gives us a view about what happens at infinity. The point at infinity is a non-singular (smooth) point.

2-torsion points:

A 2-torsion point P is one which is killed by 2, i.e., $2P = O \Leftrightarrow P = -P$. Since $-(x, y) = (x, -y)$ the 2-torsion points are those whose y -coordinates equal 0. Figure 2 shows 3 such points, $(-1, 0)$, $(0, 0)$ and $(1, 0)$. The fourth 2-torsion point is the point at infinity O . These four points form an abelian subgroup.

Say K is the smallest field containing some roots of $x^3 + ax + b = 0$ and $E(K) = \{(x, y) \mid y^2 = x^3 + ax + b, x, y \in K\} \cup \{O\}$. If $\#E(K)$ is finite, then $\#E(K)$ is even. In general over a field K , if $\#E(K)$ is finite then $E(K)$ contains some non-zero 2-torsion points $\Leftrightarrow \#E(K)$ is even.

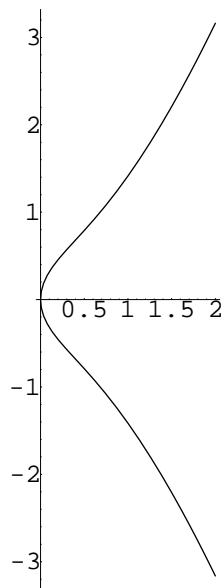


Figure 2: $E : y^2 = x^3 - x$

Rational points over finite fields:

Say $q = p^m$, where p is a prime and $m \geq 1$, $\text{char } \mathbf{F}_q = p \neq 2, 3$

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

If $x^3 + ax + b$ is a quadratic residue (square-root) in \mathbf{F}_q then there are two points on the curve otherwise it doesn't contribute any points to $E(\mathbf{F}_q)$. So if $x^3 + ax + b$ is *random* enough half the time we expect to get a quadratic residue and half the time we expect to hit a quadratic non-residue.

$$\text{Hence } \#E(\mathbf{F}_q) = \frac{1}{2}2(q-1) + 1 \sim q$$

We can come up with a formula to count points on Elliptic curves over prime fields by computing the Legendre symbol of $x^3 + ax + b$ over p :

$$\#E(\mathbf{F}_p) = 1 + \sum_{x \in \mathbf{F}_p} \left[\left(\frac{x^3 + ax + b}{p} \right) + 1 \right]$$

Hasse [2] in 1933 gave us an upper and lower bound for the number of rational points over \mathbf{F}_q :

$$\begin{aligned} q + 1 - 2\sqrt{q} &\leq \#E(\mathbf{F}_q) \leq q + 1 + 2\sqrt{q} \\ \#E(\mathbf{F}_q) &= q + 1 - t \\ |t| &\leq 2\sqrt{q} \end{aligned}$$

where t is called the trace of the curve

Note: $E(\mathbf{F}_q)$ is called the group of rational points i.e., points that are *rational* over the ground field \mathbf{F}_q). Not to be confused with $E(Q)$!

The knowledge of the rational points on the curve is essential to cryptosystems because we often desire curves E with a large prime dividing $\#E(\mathbf{F}_q)$. So we can either construct curves with the right properties (like $\#E(\mathbf{F}_q)$ containing a large prime) or generate curves randomly and check if they have the desired properties. Hence efficient computation of $\#E(\mathbf{F}_q)$ is an important question. Both approaches are useful depending on the application. For example EC factoring algorithms search for curves where the number to be factored, decomposes smoothly.

Bibliography:

1. Neal Koblitz, Alfred Menezes and Scott Vanstone, The State of Elliptic Curve Cryptography, Designs, Codes and Cryptography, 19, 173-193, 2000.
2. H. Hasse, Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzetafunktionen in gewissen elliptischen Fällen, Vorläufige Mitteilung, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen I, 42: 253-262, 1933.