Edoardo Persichetti Lecture 4: Elliptic Curves 11/03/2014

Definition 1 (Algebraic Curve) Let $\mathbb{K}$ be a field. An algebraic curve of order n is given by an equation $f(x, y) = 0$ for a polynomial $f \in \mathbb{K}[x, y]$ of degree n.

e.g. quadratic, cubic, quartic etc. In our case interested in $n = 3$.

Field can be for example $\mathbb{C}, \mathbb{R}, \mathbb{Q}$, algebraic extensions of $\mathbb{Q}$, or a finite field.

Definition 2 (Singular point) A point P such that both partial derivatives are 0 in P.

"Nasty" things can happen: cusps, knots etc. See extra sheet 1.

Definition 3 (Genus) The genus g of a curve is the difference between the maximum number M of singular points the curve can have, and the number of points the curve has.

Lemma 1 $M = \binom{n-1}{2} = \frac{(n-1)(n-2)}{2}$.

If a curve has genus 0 is *rational* (Example $x^3 + x^2 - y^2$, intersect with $y = mx$ and find $x = m^2 - 1, y = m^3 - m$). Note that for $n = 3$ we have $M = 1$ so g is either 0 or 1.

Definition 4 (Elliptic curve) A cubic curve of genus 1.

For $g \geq 2$ ($n > 3$) the curve is hyperelliptic.

Definition 5 (Weierstrass Equation) $y^2 = x^3 + Ax + B$.

Examples $y^2 = x^3 - x$ and $y^2 = x^3 + x$ over $\mathbb{R}$. Projective space $\mathbb{P}$ over $\mathbb{K}$ is space of equivalence classes (multiples) $(x : y : z) \sim (x/z : y/z : 1)$ if $z \neq 0$. If $z = 0$ points at infinity $(x : y : 0)$. Homogeneous form with z ($F(x, y, z) = z^n f(x/z, y/z)$ so we're sure all solutions are in the eq. classes). Example with lines. In elliptic curve, homogeneous form and solve implies $(0 : 1 : 0)$. Set of points $E(\mathbb{L}) = \{\infty\} \cup \{(x, y) \in \mathbb{L}^2 | y^2 = x^3 + Ax + B\}$ for $\mathbb{K} \subseteq \mathbb{L}$.

Definition 6 (Resultant) For two polynomials f and g of degrees n and m, the resultant is the determinant of the square $(n + m)$ matrix (...)

Theorem 1 *f and g have common roots iff resultant is equal to 0.*

Since f has multiple roots iff has common roots with f' we can use the theorem to obtain that f has multiple roots iff resultant of f and f' is equal to 0. In this case the resultant is called *discriminant*. For elliptic curves want no repeated roots, so $\Delta \neq 0$ in our case $\Delta = -(4A^3 + 27B^2)$ (for characteristic $\neq 2, 3$).

Definition 7 (Generalized Weierstrass Equation) $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

This is equivalent to the other form when $\neq 2, 3$.

Addition of Points and Group Structure: Every line intersects in three points. For $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ define $P_1 + P_2 = P_3$ as in drawing. How to find coordinates? Intersect curve with line through two points $y = m(x - x_1) + y_1$, with $m = \frac{y_2 - y_1}{x_2 - x_1}$ get $0 = x^3 - m^2x^2 + \dots$. Since cubic is $(x - \alpha)(x - \beta)(x - \gamma) = expand$ we obtain $x_1 + x_2 + x_3 = 0$ and $-x_1x_2x_3 = B$ so we can find x_3 and then $y_3 = m(x_3 - x_1) + y_1$ and reflect. If the line is vertical $P_1 + P_2 = \infty$. If $P_1 = P_2$ it's simply the tangent, so implicit diff. $2ydy/dx = 3x^2 + A$ and $m = \frac{3x_1^2 + A}{2y_1}$. Concise formulas:

- if $x_1 \neq x_2$ then $x_3 = m^2 - x_1 - x_2$ and $y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$
- if $x_1 = x_2$ then $P_1 + P_2 = \infty$
- if $P_1 = P_2$ and $y_1 = y_2 \neq 0$ then $x_3 = m^2 - 2x_1$ and $y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{3x_1^2 + A}{2y_1}$
- if $P_1 = P_2$ and $y_1 = y_2 = 0$ then $P_1 + P_2 = \infty$

So set of points is additive group with ∞ as the 0, and it's abelian. There exist inverse $-P = (x, -y)$. Need to verify associativity (...)
For generalized Weierstrass we have $-P = (x, -a_1x - a_3 - y)$.

Constant Multiplication of Points: Want to calculate $kP = P + \dots + P$ k times. Just sum, but quickly through doubling and summing.

It is possible to obtain elliptic curve starting from other types of equations: e.g. cubic, quartic etc. Example $x^3 + y^3 + z^3 = 0$.

The j-invariant: Change of coordinates call $\tilde{x} = \mu^2 x$ and $\tilde{y} = \mu^3 y$ for $\mu \in \bar{\mathbb{K}}^*$. Then we obtain $\tilde{y}^2 = \tilde{x}^3 + \tilde{A}\tilde{x} + \tilde{B}$, with $\tilde{A} = \mu^4 A$ and $\tilde{B} = \mu^6 B$.

Definition 8 (j-invariant) $j = j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}$.

Denominator is nonzero by assumption (opposite of determinant). Invariant under change of coordinates.

Theorem 2 *Let $\tilde{E}$ and $\hat{E}$ be given by $\tilde{y}^2 = \tilde{x}^3 + \tilde{A}\tilde{x} + \tilde{B}$ and $\hat{y}^2 = \hat{x}^3 + \hat{A}\hat{x} + \hat{B}$ and having j-invariants $\tilde{j}$ and $\hat{j}$. if = then exists μ s.t. $\hat{A} = \mu^4\tilde{A}$ and $\hat{B} = \mu^6\tilde{B}$.*

The transformation $\hat{x} = \mu^2\tilde{x}$ and $\hat{y} = \mu^3\tilde{y}$ changes one equation into the other.
For $j = 0$ equation $y^2 = x^3 + B$, for $j = 1728$ equation $y^2 = x^3 + Ax$. In addition to trivial automorphism $(x, y) \to (x, -y)$ valid for all ell. curves, these have respectively $(x, y) \to (\zeta x, -y)$ (for ζ non-trivial cube root of 1) and $(x, y) \to (-x, iy)$ (for usual $i^2 = -1$). If working over algebraically closed field, then j-invariant tells us isomorphism (*twists*). Example $y^2 = x^3 - 25x$ $y^2 = x^3 - 4x$ both $j = 1728$ then first infinitely many points in $\mathbb{Q}$ (integer multiples of $(-4, 6)$) while second $\infty, (2, 0), (-2, 0), (0, 0)$ so no twist in $\mathbb{Q}$ but only in $\mathbb{Q}(\sqrt{10})$ with $\mu = \sqrt{10}/2$.

Singular Curves: What happens if there are multiple roots? For example if reduced. First case triple root $\Rightarrow y^2 = x^3$ (see figure). Then $(0, 0)$ only singular point, we exclude it.

Theorem 3 *The other points $E_{ns}(\mathbb{K})$ form a group isomorphic to additive $\mathbb{K}$ through $(x, y) \to \frac{x}{y}$ and $\infty \to 0$.*

Second case: double root. We can translate the curve and assume root is at 0 so $y^2 = x^2(x + a)$. Again $(0, 0)$ only singularity. Rearrange divide by x^2: near 0 approx. a. So $y/x = \pm\alpha$ and tangents $y = \alpha x$ and $y = -\alpha x$.

Theorem 4 *The other points $E_{ns}(\mathbb{K})$ form a group isomorphic to multiplicative $\mathbb{K}^*$ through $(x, y) \to \frac{y+\alpha x}{y-\alpha x}$ and $\infty \to 1$, for $\alpha^2 = a$ (two cases).*

Example $y^2 = x(x+35)(x-55)$. Possibilities: additive, split multiplicative, non-split multiplicative, good reduction ($p \geq 13$).