LECTURE 7, WEDNESDAY 25.02.04

FRANZ LEMMERMEYER

1. Singular Weierstrass Curves

Consider cubic curves in Weierstraß form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where the coefficients a_i lie in some field K; we say that E is defined over K and occasionally denote this by E/K.

Note that (1) is irreducible; this is clear if $a_1 = a_3 = 0$, since $Y^2 = f(X)$ can only be reducible if $\deg f$ is even, and can be proved with a little bit more effort in the general case.

We next observe that the point $\mathcal{O} = [0 : 1 : 0]$ at infinity is always smooth since $F_Z(\mathcal{O}) = 1$. It thus remains to study affine points.

Before we do that, we will show how to transform long into short Weierstrass forms over fields of characteristic $\neq 2, 3$.

If K is a field of characteristic $\neq 2$, we can put $\eta = y + (a_1x + a_3)/2$ (we are completing the square) and find

$$\eta^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \tag{2}$$

with $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, and $b_6 = a_3^2 + 4a_6$.

If, moreover, $\operatorname{char} K \neq 3$, then we can put $\xi = x + b_2/12$ and find the short Weierstraß normal form

$$\eta^2 = \xi^3 - \frac{c_4}{48}\xi - \frac{c_6}{864}, \tag{3}$$

where

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

We also introduce

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$$

and define the *discriminant* Δ of E by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

We will see below that $\Delta \neq 0$ for elliptic (i.e., nonsingular) cubics, hence we can define the j-invariant of E by $j = c_4^3/\Delta$.

We have collected all these definitions in table 1.

Recall that the discriminant of a cubic polynomial

$$f(x) = x^3 + ax^2 + bx + c = (x - \alpha)(x - \alpha')(x - \alpha'')$$

is defined to be

$$\operatorname{disc} f = [(\alpha - \alpha')(\alpha' - \alpha'')(\alpha'' - \alpha)]^2.$$

TABLE 1

$$
\begin{array}{lcl}
b_2 & = & a_1^2 + 4a_2\,, \\
b_4 & = & a_1a_3 + 2a_4\,, \\
b_6 & = & a_3^2 + 4a_6, \\
b_8 & = & a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2\,, \\
c_4 & = & b_2^2 - 24b_4\,, \\
c_6 & = & -b_2^3 + 36b_2b_4 - 216b_6\,, \\
\Delta & = & -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\,, \\
4b_8 & = & b_2b_6 - b_4^2\,, \\
1728\Delta & = & c_4^3 - c_6^2\,, \\
j & = & c_4^3/\Delta \;=\; 1728 + c_6^2/\Delta\,.
\end{array}
$$

Thus disc $f = 0$ if and only if f has multiple roots. Moreover, for the polynomial $f(x) = x^3 + \frac14 b_2x^2 + \frac12 b_4x + \frac14 b_6$ on the right hand side of (2) we have $16\,\mathrm{disc}\, f = \Delta$.

When should we consider two elliptic curves to be essentially the same? Consider the transformation

$$x \longmapsto x' + r, \quad y \longmapsto y' + sx' + t \tag{4}$$

for coefficients $r, s, t, u \in K$. Substituting these equations into (1) gives a new equation $E' : y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'$, where (with a little help from `pari`)

$$
\begin{aligned}
a_1' &= a_1 + 2s, \\
a_2' &= a_2 - a_1s + 3r - s^2, \\
a_3' &= a_3 + a_1r + 2t, \\
a_4' &= a_4 - a_3s + 2ra_2 - a_1(rs + t) - 2st + 3r^2, \\
a_6' &= a_6 + a_4r - a_3t + a_2r^2 - a_1rt - t^2 + r^3, \quad \text{hence} \\
b_2' &= b_2 + 12r, \\
b_4' &= b_4 + rb_2 + 6r^2, \\
b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3, \\
c_4' &= c_4, \quad c_6' = c_6, \quad \Delta' = \Delta.
\end{aligned}
$$

Thus changing the coordinate system via (4) does not change c_4, c_6, and the discriminant. These transformations allow us to move any affine point P into the origin. Note that the point at infinity as well as the line at infinity are fixed by (4).

In addition to these translations we can also rescale the equation by substituting

$$x = u^{-2}x', \quad y = u^{-3}y' \tag{5}$$

for some $u \in K^\times$. After getting rid of denominators we find

$$E' : y'^2 + a_1ux'y' + a_3u^3y' = x'^3 + a_2u^2x'^2 + a_4u^4x' + a_6u^6.$$

Thus each a_i gets multiplied by u^i, and the same thing happens to the b's and the c's. In particular $c_4' = u^4 c_4$ and $\Delta' = u^{12}\Delta$, hence $j' = {c_4'}^3/\Delta' = j$ remains the same: the j-invariant is invariant under both types of transformations (whence the name).

Weierstrass curves that can be transformed into each other using (4) or (5) are called isomorphic. Isomorphic elliptic curves have the same j-invariant. It can be proved (quite easily) that elliptic curves with the same j-invariant are isomorphic over the algebraic closure of K (that is, the transformations (4) and (5) might involve coefficients from some extension of K).

Now we are ready for

Theorem 1. *The cubic E in (1) defined over some field K is singular if and only if $\Delta = 0$ in K. In this case there exists a unique singular point P which is determined as follows:*

- *If* char $K = 2$ *and E in given by (1), then*
$$P = \begin{cases} (\sqrt{a_4}, \sqrt{a_2 a_4 + a_6}\,) & \text{if } c_4 = 0 \ (\iff a_1 = 0) \\ (a_3/a_1, (a_3^2 + a_1^2 a_4)/a_1^3) & \text{if } c_4 \neq 0 \ (\iff a_1 \neq 0) \end{cases}$$
- *If* char $K = 3$ *and E is given by (2), then*
$$P = \begin{cases} (-\sqrt[3]{b_6}, 0) & \text{if } c_4 = 0 \ (\iff b_2 = 0) \\ (-b_4/b_2, 0) & \text{if } c_4 \neq 0 \ (\iff b_2 \neq 0) \end{cases}$$
- *Finally, if* char $K \neq 2, 3$ *and E is given by (3), then*
$$P = \begin{cases} (0,0) & \text{if } c_4 = 0 \\ (-c_6/12c_4, 0) & \text{if } c_4 \neq 0. \end{cases}$$

In particular, the unique singularity of E/K is always K-rational if K has characteristic 0 *or is a finite field.*

Proof. Let us first consider the case where char $K \neq 2, 3$. Then we may assume that E is given in short Weierstrass form. Here we use the fact that *invertible* affine transformations $x' = ax + by + c$, $y' = dx + ey + f$ map singular points to singular points, since the derivatives of $g(x', y') = f(x, y)$ with respect to x' and y' are linear combinations of f_1 and f_2 and therefore vanish; we also use that translations $x' = x + c$, $y' = y + c$ do not change the discriminant Δ.

The derivatives we have to look at are $f_x = -3x^2 + c_4/48$ and $f_y = 2y$. The first equation gives $x = \pm\sqrt{c_4}/12$, the second $y = 0$; plugging this into (3) we get $c_6 = \mp\sqrt{c_4}^3$ (in particular we have $\sqrt{c_4} \in K$). This implies that $\Delta = 0$.

If $c_4 = 0$, then $x = 0$ and $y = 0$; if $c_4 \neq 0$, then $x = \pm\sqrt{c_4}/12 = -c_6/12c_4$. Thus we have seen: if there is a singular point, then it is the one given above, and we have $\Delta = 0$. Conversely, if $\Delta = 0$, then the derivatives f_x and f_y vanish in the given point, and the equation $\Delta = 0$ guarantees that the point lies on E.

Now assume that char $K = 2$. Then $b_2 = a_1^2$, $b_4 = a_1 a_3$, $c_4 = a_1^4$, hence $c_4 = 0 \iff a_1 = 0$.

The coordinates of a singular point in the affine plane satisfy the three equations
$$\begin{aligned} f &= y^2 + a_1 xy + a_3 y + x^3 + a_2 x^2 + a_4 x + a_6, \\ f_x &= a_1 y + x^2 + a_4, \\ f_y &= a_1 x + a_3. \end{aligned}$$

Note that signs are irrelevant in light of $-1 = +1$. If $a_1 = 0$, then $f_y = 0$ is equivalent to $a_3 = 0$, and in this case we have $\Delta = 0$ as well as $x_0 = \sqrt{a_4}$ and $y_0 = \sqrt{a_2a_4 + a_6}$.

If $a_1 \neq 0$, then $x = a_3/a_1$ (since $f_y = 0$) and $y = (a_3^2 + a_1^2a_4)/a_1^3$ (since $f_x = 0$). The condition $f = 0$ now yields $\Delta = 0$: on the one hand we have (observe that $2 = 0$ and $-1 = 1$)

$$\begin{aligned}\Delta &= b_2^2b_8 + b_6^2 + b_2b_4b_6\\ &= a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_3^4 + a_1^3a_3^3,\end{aligned}$$

on the other hand we find

$$\begin{aligned}a_1^6f(x,y) &= a_1^6(y^2 + a_1xy + a_3y + x^3 + a_2x^2 + a_4x + a_6)\\ &= a_3^4 + a_1^4a_4^2 + a_1^3a_3^3 + a_1^3a_3^3 + a_1^5a_3a_4 + a_1^3a_3^3 + a_1^4a_2a_3^2 + a_6a_1^6,\end{aligned}$$

and since $3a_1^3a_3^3 = a_1^3a_3^3$, we see that $\Delta = 0$ is in fact equivalent to $f(x,y) = 0$.

The case char $K = 3$ is left as an exercise.

Finally some remarks on the question whether the singular point is defined over K (i.e. has coordinates from K): if K is a finite field of characteristic 2, then $x \longmapsto x^2$ is an automorphism, hence every element of K is a square. □

Corollary 2. *Cubic curves in Weierstrass form are irreducible.*

Proof. Reducible cubic curves consist of three lines or a conic and a line; every point of intersection of components is singular, hence reducible cubics have at least two singular points. □

If a Weierstrass curve E defined over a field K has a singular point P, then $E_{\rm ns} = E(K) \setminus \{P\}$ is called the nonsingular part of E.

2. Addition Formulas

Let E be an elliptic curve in long Weierstrass form (1) defined over some field K. For $P \in E(K)$ we define $-P$ as the third point of intersection of the line through P and $\mathcal{O} = [0:1:0]$ with E. If $P = [x_1 : y_1 : 1]$, the line $P\mathcal{O}$ is given by $x = x_1$; intersection gives

$$y^2 + (a_1x_1 + a_3)y - (x_1^3 + a_2x_1^2 + a_4x_1 + a_6) = 0,$$

that is, the sum of the two roots of this quadratic equation is $-(a_1x_1 + a_3)$; note that this equation describes the affine points only. Since one root is given by $y = y_1$, the other one must be $-(a_1x_1 + a_3) - y_1$.

Given two points $P_1 = (x_1, y_1)$ and $P_1 = (x_2, y_2)$ in $E(K)$ with $x_1 \neq x_2$, let $-P_1 - P_2 = P_3 = (x_3, y_3)$ be the third point of intersection of the line P_1P_2 with E. The line P_1P_2 has the equation $y = y_1 + m(x - x_1)$ with $m = (y_2 - y_1)/(x_2 - x_1)$; plugging this into (1) yields a cubic equation in x with the roots x_1, x_2 and x_3. The sum of these roots is the coefficient of x^2 (observe that the coefficient of x^3 is -1), hence $x_3 = -x_1 - x_2 - a_2 + m(a_1 + m)$. Plugging this into the line equation we find the y-coordinate of P_3, hence

$$x_3 = -x_1 - x_2 + m(a_1 + m), \quad y_3 = -[y_1 + m(x_3 - x_1) + a_1x_3 + a_3].$$

If $x_1 = x_2$, then $y_1 = \pm y_2$. If $y_1 = -y_2$, then we put $P_1 + P_2 = \mathcal{O}$; if $y_1 = y_2$, that is, $P_1 = P_2$, then we let $-2P_1$ be the third point of intersection of the tangent to E in P_1 with E; a simple calculation then gives

Theorem 3. *Let E/K be an elliptic curve given in long Weierstrass form (1). The chord-tangent method defines an addition on the set $E(K)$ of K-rational points on E; the addition formulas are given by*

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3),$$

where

$$\begin{aligned} x_3 &= -x_1 - x_2 - a_2 + a_1 m + m^2 \\ y_3 &= -y_1 - (x_3 - x_1)m - a_1 x_3 - a_3 \end{aligned}$$

and

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} & \text{if } x_1 = x_2 \end{cases}$$

In particular, for $P = (x, y)$ the x-coordinate of $2P$ is given by

$$x_{2P} = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6}. \tag{6}$$

Specializing this to curves in short Weierstrass form, we get

$$x_3 = -x_1 - x_2 + m^2, \; y_3 = -y_1 - m(x_3 - x_1),$$

where

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_2 \neq x_1, \\ \frac{3x^2 + a}{2y} & \text{if } x_2 = x_1, y \neq 0. \end{cases}$$

The cases not covered by these formulas are

a) $x_1 = x_2$ and $y_1 = -y_2$: here $P_1 = -P_2$, hence $P_1 + P_2 = \mathcal{O}$;
b) $2(x, y)$ with $y = 0$: here $(x, 0)$ is a point of order 2, that is, $2(x, y) = \mathcal{O}$.

In order to see these formulas in action take the curve $E : y^2 + xy = x^3 - 18x + 27$. Here $a_1 = 1$, $a_2 = a_3 = 0$, $a_4 = -18$ and $a_6 = 27$. We find $b_2 = 1$, $b_4 = -36$, $b_6 = 108$, $b_8 = -324$, hence $c_4 = 865$, $c_6 = -24625$ and $\Delta = 23625 = 3^3 \cdot 5^3 \cdot 7$. Thus E is an elliptic curve over $\mathbb{F}_p$ for all $p \neq 3, 5, 7$. The point $P = (1, 1)$ is in $E(\mathbb{F}_2) : y^2 + xy = x^3 + 1$; let us compute a few multiples of P.

Bu the addition law we have

$$m = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} = \frac{x_1^2 - y_1}{x_1} = 0,$$

hence $x_{2P} = -2x_P + m + m^2 = 0$ and $y_{2P} = -y_P - (x_{2P} - x_P)m - x_{2P} = 1$, i.e., $2P = (0, 1)$.

We get $3P$ by adding P and $2P$; here $m = (y_2 - y_1)/(x_2 - x_1) = 0$, hence $x_{3P} = -x_P - x_{2P} = 1$, as well as $y_{3P} = -y_P - x_{3P} = 0$, hence $3P = (1, 0)$.

Finally $4P = P + 3P$, but here m is not defined because $x_P = x_{3P}$. This implies (since $P \neq 3P$) that $4P = \mathcal{O}$. In fact we have seen that $-(x, y) = (x, -a_1 x - a_3 - y)$, so in our case we have $-(x, y) = (x, -x - y)$, in particular $-(1, 1) = (1, 0)$.

Thus P generates a group of order 4. Listing all points in $E(\mathbb{F}_2)$ we find that these are all, and we have proved that $E(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$.