LECTURE 18, MONDAY 12.04.04

FRANZ LEMMERMEYER

1. Tate's Elliptic Curves

Assume that E is an elliptic curve defined over $\mathbb{Q}$ with a rational point P of order $N \ge 4$. By changing coordinates we may move P to $(0,0)$ and make sure that $y = 0$ is the tangent to E at P. Then E has the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

If we had $a_2 = 0$, then P would be a flex, contradicting the fact that it has order ≥ 4. Thus $a_2 \ne 0$, and the admissible transformation $x \longmapsto u^2x$, $y \longmapsto u^3y$ with $u = a_3/a_2$ brings E into the form

$$E : y^2 + \alpha xy + \beta y = x^3 + \beta x^2.$$

`pari` shows that

$$\text{disc } E = -\beta^3(\alpha^4 - \alpha^3 + 8\beta\alpha^2 - 36\beta\alpha + (16\beta^2 + 27\beta));$$

in particular, E is singular if $\beta = 0$.

The group law (`pari` will help) now gives

$$\begin{aligned} 2P &= (-\beta, \beta(\alpha - 1)), \\ 3P &= (1 - \alpha, \alpha - \beta - 1), \\ 4P &= \Big(\frac{\beta(1 - \alpha + \beta)}{(1-\alpha)^2}, \frac{\beta^2(\alpha^2 - 3\alpha + \beta + 2)}{(1-\alpha)^3}\Big). \end{aligned}$$

Thus P will have order 4 if and only if $\alpha = 1$:

Proposition 1. *The point $(0,0)$ on the elliptic curve*

$$E : y^2 + xy + \beta y = x^3 + \beta x^2$$

with discriminant $-16\beta^4(\beta + 1)$ has order 4 for all $\beta \ne -1, 0$.

Moreover, P will have order 5 if and only if $2P = -3P$, which happens if and only if $\alpha = 1 + \beta$.

Proposition 2. *The point $(0,0)$ on the elliptic curve*

$$E : y^2 + (1 + \beta)xy + \beta y = x^3 + \beta x^2$$

with discriminant $-\beta^5(\beta^2 - 11\beta + 1)$ has order 5 for all $\beta \in \mathbb{Q}^\times$.

The equation $2P = -4P$ leads to $\beta = -(\alpha - 1)(\alpha - 2)$, and we get

Proposition 3. *The point $(0,0)$ on the elliptic curve*

$$E : y^2 + \alpha xy + \beta y = x^3 + \beta x^2$$

with $\beta = -(\alpha - 1)(\alpha - 2)$ has discriminant $(\alpha - 1)^6(\alpha - 2)^3(9\alpha - 10)$ has order 6 for all $\alpha \in \mathbb{Q} \setminus \{1, 2, \frac{10}{9}\}$.

Finally, $3P = -4P$ leads to $(1-\alpha)^3 = \beta(1-\alpha+\beta)$. Substituting x and y for $1-\alpha$ and β we find that this equation describes a cubic curve $x^3 = y(x+y)$, which is a singular cubic curve. Such curves can be parametrized, and putting $y = tx$ we get $x = t + t^2$ and $y = t^2 + t^3$; this gives $\alpha = 1 - t - t^2$ and $\beta = t^2 + t^3$:

Proposition 4. *The point* $(0,0)$ *on the elliptic curve*

$$E : y^2 + (1 - t - t^2)xy + (t^2 + t^3)y = x^3 + (t^2 + t^3)x^2$$

with discriminant $\operatorname{disc} E = -t^7(1+t)^7(t^3 + 8t^2 + 5t - 1)$ *has order* 7 *for all* $t \in \mathbb{Q} \setminus \{0, -1\}$.

Thus the condition for P to have order 7 led to a singular cubic curve with a rational point (and therefore infinitely many). It turns out that conditions for order 8 and higher also lead to curves; we will see below that not all of the resulting curves do have (nontrivial) rational points, however.

In order to go further, we need to simplify our equations. Let us put $a = 1 - \alpha$ and $b = -\beta$, and introduce $c = \frac{b}{a}$ and $d = \frac{a}{c-1}$. Tate's elliptic curve now has the equation

$$y^2 + (1-a)xy - by = x^3 - bx^2, \tag{1}$$

and we find

$$\begin{aligned}
P &= (0,0) & -P &= (0,b)\\
2P &= (b,ab) & -2P &= (b,0)\\
3P &= (a,b-a) & -3P &= (a,a^2)\\
4P &= (c(c-1), c^2(a-c+1)) & -4P &= (c(c-1), c(c-1)^2)\\
5P &= (cd(d-1), cd^2(c-d)) & -5P &= (cd(d-1), c^2d(d-1)^2)
\end{aligned}$$

Now $8P = \mathcal{O}$ is equivalent to $4P = -4P$, which leads to $c^2(a-c+1) = c(c-1)^2$. Since $c \neq 0$, this implies $c(a-c+1) = (c-1)^2$, and we get $a = \frac{(2c-1)(c-1)}{c}$, hence $b = ac = (2c-1)(c-1)$ and finally $a^2b = (2b-a)(b-a)$. This is again a singular cubic; putting $b = ta$ gives $a = \frac{(2t-1)(t-1)}{t}$ and $b = (2t-1)(t-1)$.

Proposition 5. *The cubic* $E : y^2 + (1-a)xy + by = x^3 + bx^2$ *with* $a = \frac{(2t-1)(t-1)}{t}$ *and* $b = -(2t-1)(t-1)$ *has discriminant* $\operatorname{disc} E = t^{-4}(t-1)^4(2t-1)^4(8t^2-8t+1)$ *and hence is an elliptic curve for all* $t \in \mathbb{Q}$ *with* $t \neq 0, \frac{1}{2}, 1$. *Its point* $(0,0)$ *has order* 8.

On to torsion points of order 9. Here find that $5P = -4P$ is equivalent to $c - 1 = d(d-1)$ and $(c-1)^2 = d^2(c-d)$. Squaring the first one and subtracting it from the second gives $c = d^2 - d + 1$; plugging this into the equations shows that both hold identically. Now we get

$$\begin{aligned}
a &= cd - d = d^3 - d^2,\\
b &= ac = (d^3 - d^2)(d^2 - d + 1) = d^5 - 2d^4 + 2d^3 - d^2.
\end{aligned}$$

This is a rational parametrization of the quintic you get by plugging $d = \frac{a}{c-1} = \frac{a^2}{b-a}$ into $a = d^3 - d^2$ and factoring out a, namely

$$a^5 + a^3(a-b) + (a-b)^3 = 0.$$

Putting $x = a$ and $y = a - b$ we find the quintic curve $x^5 + x^3y + y^3 = 0$; it has $(0,0)$ as its only singular point, and the curve has multiplicity 3 there, which means that parametrization with lines would not work. However, the quadratic map $x = u$, $u = uv$ transforms this into the conic $u^2 + uv + v^2 = 0$ with rational point $(0,0)$.

Proposition 6. *The cubic (1) with $a = d^3 - d^2$ and $b = d^5 - 2d^4 + 2d^3 - d^2$ has discriminant* $\operatorname{disc} E = d^9(d-1)^9(d^2-d+1)^3(d^3-6d^2+3d+1)$ *and thus defines an elliptic curve defined over $\mathbb{Q}$ for all $d \in \mathbb{Q} \setminus \{0,1\}$. The point $(0,0)$ has order 9 in $E(\mathbb{Q})$.*

Next P has order 10 if $5P = -5P$, which gives $d(c-d) = c(d-1)^2$, that is, $c = -\frac{d^2}{d^2-3d+1}$. This shows

$$a = cd - d = -\frac{d(2d^2-3d+1)}{d^2-3d+1}, \quad b = ac = \frac{d^3(2d^2-3d+1)}{(d^2-3d+1)^2}. \tag{2}$$

This is a parametrization of the quintic

$$a^5 + ba^4 + 3ba^3 - 3b^2a^2 + ba^2 - 2b^2a + b^3 = 0,$$

whose blow up at $(0,0)$ is a singular cubic.

Proposition 7. *The cubic (1) with a and b as in (2) has discriminant* $\operatorname{disc} E = d^{10}(d-1)^{10}(2d-1)^5(d^2-3d+1)^{-10}(4d^2-2d-1)$*, and thus defines an elliptic curve defined over $\mathbb{Q}$ for all $d \in \mathbb{Q} \setminus \{0, \frac{1}{2}, 1\}$. The point $(0,0)$ has order 10 in $E(\mathbb{Q})$.*

And now, finally, the case $N = 11$. In order to avoid having to compute the coordinates of $6P$, observe that $11P = \mathcal{O}$ is equivalent to $2P$, $4P$ and $5P$ being collinear. This happens if and only if

$$\begin{vmatrix} 1 & 1 & 1 \\ b & c(c-1) & cd(d-1) \\ ab & c^2(a-c+1) & cd^2(c-d) \end{vmatrix} = 0$$

Plugging in $a = (c-1)d$ and $b = ac$ gives $c^2d(c-1)(-c^2 + (d^3 - 3d^2 + 4d)c - d) = 0$. Factoring out c^2d and substituting $c = x + 1$, $d = y + 1$ yields the quartic curve

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

which is singular at $(0,0)$. Using the quadratic transformation $y = u$, $x = uv$ finally gives the cubic $vu^2 + u + (-v^2 + v) = 0$. It has a flex at $(u,v) = (0,1)$, and moving this flex and its tangent there to infinity and the line at infinity gives us the Weierstrass equation $y^2 + y = x(x+1)^2$; replacing $x + 1$ by x and y by $-y$, this gives

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

This is an elliptic curve with discriminant -11; transforming it into short Weierstrass form its torsion group is easily computed as

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (1,0), (0,1), (1,1)\} \simeq \mathbb{Z}/5\mathbb{Z}.$$

Going all the way back to our points, we find that each of these gives a solution where $5P$ coincides with one of $\pm P$, $\pm 4P$. If we can show that $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}}$, then we will have shown that there does not exist an elliptic curve defined over $\mathbb{Q}$ with a rational torsion point of order 11. We might do this once we have discussed the theorem of Mordell-Weil.

2. Levi's Idea

Let us now show how to construct elliptic curves with given torsion, and how to prove that certain torsion groups do not occur. The idea going back to Beppo Levi and used by Billing & Mahler, Ogg, and essentially everyone up to Mazur is the following: consider an elliptic curve defined over $\mathbb{Q}$ with a rational torsion point P of order ≥ 7. Then no three of the four points $\mathcal{O}$, P, $2P$, $3P$ can be collinear, so by the fundamental theorem of projective geometry there is a unique projective transformation sending P, $2P$, $3P$, and $\mathcal{O}$ to $[1:0:0]$, $[0:1:0]$, $[0:0:1]$, and $[1:1:1]$, respectively. The point $4P$ will then have coordinates $[a:b:c]$. It is now a matter of brute force calculations to compute the coordinates of the following points (for computing e.g. $-P$ we use the fact that P, $\mathcal{O}$ and $-P$ are collinear):

$$\begin{aligned} P &= [1:0:0] & -P &= [a-b+c:c:c],\\ 2P &= [0:1:0] & -2P &= [a-b+c:c:a-b+c],\\ 3P &= [0:0:1] & -3P &= [1:1:0],\\ 4P &= [a:b:c] & -4P &= [a-b:0:c-b]. \end{aligned}$$

Note that P cannot have order dividing 6, since this would imply $3P = -3P$, which is nonsense. Similarly it cannot have order 7 since this would give $a = b$, $c = 0$ and then $-P = [0:0:0]$. Thus these curves can only be used to study torsion groups of order 8 or higher.

Lemma 8. *If E is a nondegenerate cubic passing through the points kP for $-4 \le k \le 4$, then $[1:1:1]$ is a flex point.*

Proof. Write $P_k = kP$ and consider the degenerate cubics C_1 and C_2, where C_1 consists of the three lines $\mathcal{O}P$, $\mathcal{O}P_3$ and $\mathcal{O}P_4$, and C_2 of P_1P_3, $P_{-1}P_{-3}$ and the tangent at $\mathcal{O}$. The cubic C_1 intersects E in the six points kP with $k = \pm1, \pm3, \pm4$ and three times in $\mathcal{O}$. The cubic C_2 intersects E in the same six points, and at least twice in $\mathcal{O}$. If $\mathcal{O}$ were a double point, consider the line $\mathcal{O}P_4$ intersecting E in $\pm4P$ and $\mathcal{O}$: this can only happen if $P_4 = \mathcal{O}$ or $-P_4 = \mathcal{O}$, which leads to contradictions. Thus $\mathcal{O}$ is a simple point. Now C_2 is a cubic sharing eight points of intersection of C_1 and E, hence it must also pass through the ninth: thus the tangent at $\mathcal{O}$ must intersect E with multiplicity 3 there, hence $\mathcal{O}$ is a flex point. □

We now compute the coordinates of more points:

$$\begin{aligned} 5P &= [ab+ac-b^2 : ac : b(a-b+c)],\\ -5P &= [0:b:c],\\ 6P &= [(a-b+c)(a^2b-ab^2-ac^2+b^2c) :\\ &\qquad c(b-c)(ab+ac-b^2) : ac(b-c)(a-b+c)],\\ -6P &= [ab(a-b+c) : ac^2 : bc(a-b+c)], \end{aligned}$$

From $11P = \mathcal{O}$ we see that $6P = -5P$. If we had $a-b+c = 0$, then $-2P = [0:1:0] = 2P$, hence $4P = \mathcal{O}$ and $P = \mathcal{O}$, contradicting the assumption that P has order 11. Thus we must have

$$a^2b - ab^2 - ac^2 + b^2c = 0.$$

This is a smooth cubic projective curve with a rational flex point $[1:1:1]$, hence it can be transformed into Weierstrass form:

$$E_{11} : y^2 = x^3 - 432x + 8208. \tag{3}$$

Now given a rational point on this elliptic curve, we can work backwards and find the possible coordinates for $4P = [a:b:c]$. Applying Nagell-Lutz shows that E_{11} has a torsion group of order 5 given by

$$E_{11}(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-12, 108), (-12, -108), (24, 108)(24, -108)\}.$$

These points correspond to $[a:b:c] = [1:1:1]$, $[1:0:0]$, $[0:1:0]$, $[0:0:1]$ and $[1:1:0]$, none of which leads to a curve with rational 11-torsion. Now it can be shown (but this is not easy) that E_{11} has rank 0, hence the only rational points on E_{11} are the five torsion points given above. But this means that there is no rational elliptic curve with a rational point of order 11.

Note that the discriminant of (3) is $-2^{12} \cdot 3^{12} \cdot 11$, and that standard transformations give us the simpler equation

$$y^2 - y = x^3 - x^2$$

with discriminant $\Delta = -11$. It was this equation that was used by Levi as well as by Billing & Mahler.

For your entertainment, here's the table computed by Billing & Mahler giving conditions for the existence of a point of order N on E (we have put $c = 1$ here):

N	curve	genus
8	$b = 0$	0
9	$a = 0$	0
10	$ab + a - b^2 = 0$	0
11	$a^2 - ab^2 - a + b^2 = 0$	1
12	$b^2 - a = 0$	0
13	$a^2b^2 - ab^3 - ab + a + a^3 - b^2 = 0$	2
14	$a^3b - a^2b^2 - a^2b - a^2 - a + ab + b^4 - b^3 = 0$	1
15	$a^2b^2 + a^2b + a^2 - ab^3 - ab^2 - ab + b^3 = 0$	1