LECTURE 17, WEDNESDAY 07.04.04

FRANZ LEMMERMEYER

1. Torsion Points

The main theorem about the group $E(\mathbb{Q})$ of rational points on an elliptic curve $E : y^2 = x^3 + ax + b$ defined over $\mathbb{Q}$ is the theorem of Mordell-Weil (due to Mordell), which says that $E(\mathbb{Q})$ is a finitely generated abelian group. This implies that $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$ for some integer $r \ge 0$, where $E(\mathbb{Q})_{\text{tors}}$ is the torsion group of $E(\mathbb{Q})$, i.e., the group of all elements of finite order. The torsion group of elliptic curves is well understood; the Mordell-Weil rank r remains mysterious to this day.

For a given integer $N \ge 1$, let $E[N]$ denote the group of points of order dividing N on the elliptic curve E; since the equation $N \cdot P = \mathcal{O}$ is equivalent to the z-coordinate of NP being 0, and since this z-coordinate is an polynomial in x_P, y_P, z_P and the coefficients a, b, the points in $E[N]$ are all algebraic numbers.

Points of Order 2. We know from the geometric definitionof the addition law that a point $P \in E(\overline{\mathbb{Q}})$ has order 2 if and only of it has y-coordinate 0: if $P = (x, y)$, then $P + P = \mathcal{O}$ is equivalent to $P = -P = (x, -y)$. Thus all points of order 2 must satisfy $0 = y^2 = x^3 + ax + b$, and this shows that

$$E[2] = \{\mathcal{O}, (\alpha, 0), (\alpha', 0), (\alpha'', 0)\},$$

where α, α', α'' are the three (distinct) roots of $f(x) = x^3 + ax + b$. It is clear that $E[2] \simeq V_4 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, the group $E(\mathbb{Q})[2]$ of rational points of order dividing 2 is isomorphic to a subgroup of V_4, and all possibilities occur according as $f(x)$ has no, one, or three rational roots:

- $f(x)$ is irreducible in $\mathbb{Q}[x]$; then it does not have a rational root, hence $E(\mathbb{Q})[2] = \{\mathcal{O}\}$.
- $f(x)$ is the product of a linear and an irreducible quadratic factor over $\mathbb{Q}$: then $E(\mathbb{Q})[2] = \{\mathcal{O}, (\alpha, 0)\} \simeq \mathbb{Z}/2\mathbb{Z}$, where α is the rational root of f.
- $f(x)$ has three rational roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$; then

$$E(\mathbb{Q})[2] = \{\mathcal{O}, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Points of Order 3. We can similarly determine $E[3]$. Observe that the duplication formula for $P = (x, y)$ gives

$$x_{2P} = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

Since $3P = \mathcal{O}$ is equivalent to $2P = -P = (x, -y)$, the x-coordinate of a point of order 3 must satisfy

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} = x,$$

which is equivalent to

$$f_3(x) = 3x^4 + 6ax^2 + 12bx - a^2 = 0.$$

Since disc $f_3 = -2^8 \cdot 3^3 \cdot (4a^3 + 27b^2)^2$, this polynomial has 4 distinct roots. Since the discriminant is negative, and since the discriminant has sign $(-1)^s$, where s is the number of pairs of nonreal roots, we deduce that f_3 has two real and a pair of complex roots. If $a \neq 0$, then exactly one of the real roots is positive and leads to two positive values of y; it is easily seen that the same is true in the case $a = 0$. Thus every elliptic curve defined over $\mathbb{Q}$ has exactly two real points of order 3.

Moreover, f_3 has four roots over $\mathbb{C}$, hence there are 8 points of order 3. Thus $E[3] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and $E(\mathbb{Q})[3] \simeq \mathbb{Z}/3\mathbb{Z}$ or $E(\mathbb{Q})[3] = \{cO\}$ according as the real points of order 3 have rational coordinates or not. This shows that there are at most 4 different x-coordinates of points of order 3, hence at most 9 points of order dividing 3 (including $\mathcal{O}$).

As a matter of fact, f_3 has at most 4 roots over any field F of characteristic not dividing 6Δ, so the same argument shows that there are at most 9 points of order dividing 3, which in turn shows that $E[F]$ is a subgroup of $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Points of Order N. The approach above can be generalized: the x-coordinate of a point of order dividing N is a root of a polynomial $\psi_N(X)$ of degree at most $\frac{N^2-1}{2}$ (exactly if the characteristic of the field does not divide N). The ψ_N are called division polynomials and satisfy a rather simple recursive relation which makes their calculation rather straightforward. Since ψ_N has at most $\frac{N^2-1}{2}$ pairwise distinct roots (exactly this many over algebraically closed fields of characteristic not dividing $2N\Delta$), the group $E(F)[N]$ of F-rational points has at most N^2 elements, hence must be isomorphic to a subgroup of $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.

Note that since the coordinates x, y of points $P = (x, y) \in E[N]$, where $E[N]$ denotes the n-torsion points in the algebraic closure of $\mathbb{Q}$, are roots of polynomials with rational coefficients, the extension $\mathbb{Q}(P) := \mathbb{Q}(x, y)$ is an algebraic extension of $\mathbb{Q}$. Since automorphisms must map torsion points of order N to other torsion points of order N, the extension $\mathbb{Q}[N] = \mathbb{Q}(E(\mathbb{C})[N])$ is a Galois extension of $\mathbb{Q}$. Studying these extensions is a central task in the theory of elliptic curves.

If E has complex multiplication (every elliptic curve admits trivial endomorphisms $E \longrightarrow E$, namely multiplication by n; if E has other endomorphisms, then we say it has complex multiplication, since these additional endomorphisms correspond to "multiplication" by certain elements in the maximal order of some complex quadratic number field K), then it has been known for a long time that $\mathrm{Gal}\,(\mathbb{Q}[N]/K)$ is abelian: thus elliptic curves with complex multiplication can be used to construct abelian extensions of certain complex quadratic fields (this is part of class field theory). In some sense, these fields are the analogs of cyclotomic extensions of $\mathbb{Q}$: these are generated by division values $\exp(\frac{2\pi i}{N})$.

If E does not have complex multiplication, then there is an important theorem due to Serre which says that the Galois group of $\mathbb{Q}[N]/\mathbb{Q}$ is, in some sense, "as large as possible" in general. In order to explain what this means, we need more background.

2. Elliptic Curves over $\mathbb{C}$

Cyclotomic Extensions. Recall that the exponential function is periodic with period $2\pi i$; defining $e(x) = \exp(ix)$ we find that the function e is a complex-valued

function defined on $\mathbb{R}$ with period 2π; this means that e is actually defined on the 1-dimensional lattice $\Lambda = \mathbb{R}/2\pi\mathbb{Z}$.

The function e maps this lattice onto the complex unit circle: $e(x) = \cos 2\pi x + i \sin 2\pi x \in S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Actually, it is a group isomorphism: the functional equation for exp gives $e(x+y) = e(x)e(y)$. The neutral element of the lattice Λ is of course 0, and the neutral element of S^1 is $1 = e(0)$.

The group of elements of order dividing n on S^1 is therefore the image of the group of elements of order dividing n in Λ; but this group conists of the elements $0, \frac{1}{n}, \frac{2}{n}, \dots \frac{n-1}{n}$ and is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Its image consists of the n-th roots of unity $e(0) = 1, e(\frac{1}{n}) = \exp(\frac{2\pi i}{n}), \dots, e(\frac{n-1}{n}) = \exp(\frac{2\pi i(n-1)}{n})$. Via the identification $x + iy \longmapsto (x, y)$, the complex unit circle becomes the unit circle $\mathcal{C} : x^2 + y^2 = 1$ in the reals, and the roots of unity become torsion points on $\mathcal{C}$. However, only the points corresponding to $0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ have rational coordinates.

Going back to S^1, we see that the division values of e generate the extensions $\mathbb{Q}[n] = \mathbb{Q}(\zeta_n)$, that is, the cyclotomic fields of n-th roots of unity. These are Galois extensions of $\mathbb{Q}$, and its auomorphisms are given by $\sigma_a : \zeta_n \longrightarrow \zeta_n^a$ for all integers $0 < a < n$ with $(a, n) = 1$; in other words: $\mathrm{Gal}\,(\mathbb{Q}[n]/\mathbb{Q}) \simeq \mathrm{GL}_1(\mathbb{Z}/n\mathbb{Z})$.

2.1. **Elliptic Curves and Lattices.** Now suppose you have a lattice Λ in $\mathbb{C}$; think of it as the set of points $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ for some nonzero complex numbers ω_1, ω_2 with $\tau = \omega_1/\omega_2 \in \mathbb{C} \setminus \mathbb{R}$; actually, replacing ω_2 by $-\omega_2$ if necessary we can make sure that $\tau \in \mathcal{H}$, the upper half plane. The Weierstrass $\wp$-function associated to such a lattice is defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \Big(\frac{1}{(z-w)^2} - \frac{1}{w^2} \Big).$$

The Weierstrass $\wp$-function is periodic with period lattice Λ.

The Weierstrass $\wp$-function and its derivative satisfy the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

where

$$g_2 = 60 \sum_{w \in \Lambda \setminus \{0\}} w^{-4}$$
$$g_3 = 140 \sum_{w \in \Lambda \setminus \{0\}} w^{-6}.$$

Thus the Weierstrass elliptic function and its derivative parametrize elliptic curves $E : y^2 = 4x^3 - g_2x - g_3$. The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ defined by $z + \Lambda \longmapsto (\wp(z), \wp'(z))$ (with elements in Λ going to the point at infinity on E) is a group isomorphism.

The torsion points of order dividing N in the abelian group $\mathbb{C}/\Lambda$ consist of the points $\frac{a}{N}\omega_1\mathbb{Z} \oplus \frac{b}{N}\omega_2\mathbb{Z}$ for $0 \le a, b < N$, and they form a group isomorphic to $\mathbb{Z}/N \oplus \mathbb{Z}/N$. The image of this group under the isomorphism $\mathbb{C}/\Lambda E(\mathbb{C})$ is then a group isomorphic to $\mathbb{Z}/N \oplus \mathbb{Z}/N$.

In general, of course, the coefficients g_2, g_3 of E will not be rational numbers. If you start with an elliptic curve defined over $\mathbb{Q}$ and construct the corresponding lattice Λ (this is not difficult: if $y^2 = f(x)$, consider $F(z) = f(x)^{-1/2}$; this defines a Riemann surface of genus 1, i.e., a torus; integrating F over two independent paths generating the fundamental group of the torus gives the complex numbers ω_1 and

ω_2), then the image of $\mathbb{C}/\Lambda[N]$ will give you $E[N]$, and there is no guararantee that any of these torsion points except $\mathcal{O}$ will have rational coordinates. Note, however, that the points $P_j = (\wp(\frac{1}{N}\omega_j), \wp'(\frac{1}{N}\omega_j))$ $(j = 1, 2)$ generate $E[N]$, and that these points can be computed with high accuracy; if P_1, P_2 and $P_1 + P_2$ are not close to a rational integer, the elliptic curve will not have a rational point of order N; if they are close to an integer, just check whether this integral point P is torsion or not by computing NP.

Now recall that the points in $E[N]$ have algebraic coordinates (if E is defined over $\mathbb{Q}$, which we still assume). This allows us to construct the extensions $\mathbb{Q}[N] = \mathbb{Q}(E[N])$ by adjoining the coordinates of all N-torsion points to $\mathbb{Q}$. This is a Galois extension, since automorphisms of $\mathbb{C}/\mathbb{Q}$ will map points of order N to points of order N. We can make this explicit by using the points P_1 and P_2 introduced above: any $\sigma \in \mathrm{Gal}\,(\mathbb{Q}[N]/\mathbb{Q})$ will send P_1 to some torsion point, which can be written as $aP_1 + bP_2$ with a, b defined uniquely modulo N; similarly, σ will send P_2 to some $cP_1 + dP_2$. Thus every σ determines a matrix $S_\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N)$. The map $\sigma \longmapsto S_\sigma$ defines an injective group homomorphism $\mathrm{Gal}\,(\mathbb{Q}[N]/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N)$.

Remark. These maps are called Galois representations, in particular if N is prime. In the general terminology, a group representation is a homomorphism from a group G into the automorphism group if a vector space; observe that $\mathrm{GL}_2(\mathbb{F}_p)$ is the automorphism group of $\mathbb{F}_p^2$. It can be shown that $\mathrm{GL}_2(\mathbb{F}_p)$ has $(p-1)^2p(p+1)$ elements; we have $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ and $\mathrm{GL}_2(\mathbb{F}_3) = \widetilde{S}_4$, a quadratic extension of S_4. Galois representations constructed by elliptic curves play a huge role in the proof of Fermat's Last Theorem.

Now we can ask how large the image is. Before we can answer this question, we have to talk about complex multiplication. Take an elliptic curve E defined over $\mathbb{Q}$, and let Λ denote the associated lattice. Then $n\Lambda \subseteq \Lambda$ for every integer n. If there is any complex number $\lambda \in \mathbb{C} \setminus \mathbb{Z}$ with $\lambda\Lambda \subseteq \Lambda$, then E is said to have complex multiplication. In fact it is easy to verify that if E has complex multiplication, then λ is an algebraic integer in some complex quadratic number field K; in addition, E has CM if and only if $\tau = \omega_1/\omega_2$ is an element of this field K. As an example, consider the lattice $\Lambda = \mathbb{Z} \oplus i\mathbb{Z}$ (which corresponds to an elliptic curve defined over $\mathbb{Q}$ only after rescaling): since $i\Lambda = \Lambda$, the associated elliptic curve has complex multiplication.

Elliptic curves with CM have lots of special properties because they have more symmetries than the average elliptic curve. One of the main results about them that has been known for a long time is the following

Theorem 1. *If an elliptic curve E defined over $\mathbb{Q}$ has complex multiplication by elements in some complex quadratic field K, then the group of $K[N]/K$ (where $K[N] = K\mathbb{Q}[N] = K(E[N])$) is abelian.*

This implies that the Galois group of $\mathbb{Q}[N]/\mathbb{Q}$ for elliptic curves with CM is almost abelian in the sense that it has an abelian subgroup of index at most 2, namely the Galois group of $(\mathbb{Q}[N] \cap K)/\mathbb{Q}$.

On the other hand, the Galois group of $\mathbb{Q}[N]/\mathbb{Q}$ for elliptic curves without CM is as large as possible in general; this is the result of a theorem due to Serre:

Theorem 2. *If E is an elliptic curve without CM, then for almost all primes ℓ we have* $\mathrm{Gal}\,(\mathbb{Q}[N]/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$.

I will not even try to sketch the proof (it is not too deep, though), but instead will give a few ingredients. Essentially Serre uses ℓ-adic numbers, some (topological) group theory, and algebraic number theory, in particular inertia and ramification groups.

3. Exceptional Points

Already at the beginning of the 20th century, elliptic curves with given small torsion groups were constructed (the group law was not yet known; these results were stated in the form that there exist certain "exceptional" points for which the chord-tangent method produces only finitely many other points. Beppo Levi, in particular, showed that each of the following groups occurs infintely often:

$$E_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & \text{für } 1 \leq m \leq 4; \\ \mathbb{Z}/(2m-1)\mathbb{Z} & \text{für } 1 \leq m \leq 5; \\ \mathbb{Z}/2m\mathbb{Z} & \text{für } 1 \leq m \leq 6. \end{cases} \tag{1}$$

Levi could also prove that the groups $\mathbb{Z}/m\mathbb{Z}$ forr $m = 14, 16, 20$, and the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ forr $m = 5, 6$ do not occur as torsion groups of elliptic curves. In a lecture at the International Congress of Mathematicians in Rome (1908) he mentioned the conjecture that the list above (with the possible exception of $\mathbb{Z}/24\mathbb{Z}$, which he forgot or chose not to mention) is complete. Fourty years later Nagell rediscovered the same conjecture, and another 20 years later Ogg called it a "folklore conjecture" (from then on it was known as Ogg's conjecture).

Levi tried to prove that there are not rational torsion points of order 11, but did not succeed. He could show that the existence of such an elliptic curve implies that the elliptic curve $y^2 - y = x^3 - x^2$ with discriminant $\Delta = -11$ has a rational point different from the five torsion points $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ and $\mathfrak{O}$. Disproving the existence of such a point was beyond his means: this was done later by Billing and Mahler, based on the methods of Billing's 165-page thesis. Over the years, more and more cases were excluded, and finally Mazur managed to prove

Theorem 3. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tors}}$ is one of the following groups: $\mathbb{Z}/m\mathbb{Z}$ for $1 \leq m \leq 10$ or $m = 12$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 4$. In particular, $\#E(\mathbb{Q})_{\text{tors}} \leq 16$.*

The following table, taken from Knapp's book, shows that all these cases occur:

E	$E(\mathbb{Q})_{\rm tors}$	Δ
$y^2 = x^3 + 2$	0	$-2^6 3^3$
$y^2 = x^3 + x$	$\mathbb{Z}/2\mathbb{Z}$	-2^6
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$-2^8 3^3$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	-2^{12}
$y^2 + y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	-11
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$-2^4 3^3$
$y^2 - xy + 2y = x^3 + 2x^2$	$\mathbb{Z}/7\mathbb{Z}$	$-2^7 13$
$y^2 + 7xy - 6y = x^3 - 6x^2$	$\mathbb{Z}/8\mathbb{Z}$	$2^8 3^4 17$
$y^2 + 3xy + 6y = x^3 + 6x^2$	$\mathbb{Z}/9\mathbb{Z}$	$-2^9 3^5$
$y^2 - 7xy - 36y = x^3 - 18x^2$	$\mathbb{Z}/10\mathbb{Z}$	$-2^5 3^{10} 11^2$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$2^{12} 3^6 5^3 7^4 13$
$y^2 = x^3 - x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	2^6
$y^2 = x^3 + 5x^2 + 4x$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$2^8 3^2$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$2^2 3^6 5^2$
$y^2 = x^3 + 337x^2 + 20736x$	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$2^{20} 3^8 5^4 7^2$