LECTURE 20, MONDAY 18.04.04

FRANZ LEMMERMEYER

1. Theorem of Mordell-Weil

Today we'll start discussing my favorite part of the introduction to the theory of elliptic curves: how to compute the rank of an elliptic curve defined over $\mathbb{Q}$ using various forms of descent, the technique that Fermat first used for showing that $X^4 + Y^4 = Z^2$ only has trivial solutions in integers.

Before we can compute the rank, we have to define it and prove it is finite; this is what the theorem of Mordell-Weil[1] does:

Theorem 1. *The group $E(\mathbb{Q})$ is finitely generated. In particular,*

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{\text{tors}}$ is a finite group, and where $r \ge 0$ is a non-negative integer called the Mordell-Weil rank of E.

The Theorem of Mordell-Weil can be interpreted as some kind of analog of Dirichlet's unit theorem:

Theorem 2. *The group $U(K)$ of units in the ring of integers of some algebraic number field is finitely generated. In particular,*

$$U(K) \simeq U(K)_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $U(K)_{\text{tors}}$ is the finite group of roots of unity contained in K, and where $r \ge 0$ is a non-negative integer called the unit rank of K.

The difference between these two theorems is that the unit rank of a number field can easily be determined by counting the number of real and complex embeddings of K; computing the Mordell-Weil rank is a lot more difficult.

When we proved Fermat's Last Theorem for the exponent 4, the first part was to find a new solution from a known one, and the second part was showing that the new solution was actually "smaller". Similalry, the proof of the Mordell-Weil Theorem consists of two parts: an algebraic part and one dealing with measuring how "small" a solution is. In the general situation, the algebraic part is called the Weak Mordell-Weil Theorem:

Theorem 3. *Given an elliptic curve E defined over $\mathbb{Q}$, there is an integer $m > 1$ such that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite.*

Actually, this is true for *any* integer $m > 1$, but one such m is sufficient for the proof of Mordell-Weil. The simplest proofs use $m = 2$, and in general this is also the easiest method for actually computing the rank.

[1] This version of the theorem, without the group theoretic language, was proved by Mordell. Weil generalized it from elliptic curves to abelian varieties and from $\mathbb{Q}$ to arbitrary number fields.

The fact that G is an abelian group and G/mG is finite for all $m \ge 1$ does not suffice to conclude that G is finitely generated. In fact, the group $G = \mathbb{Q}$ satisfies $G = mG$ (we say that $\mathbb{Q}$ is a divisible group: every element can be written as m times some other element) for any $m \ge 1$, yet $\mathbb{Q}$ is not finitely generated: not every rational number can be written as a finite $\mathbb{Z}$-linear combination of finitely many elements $r_1, \dots, r_n$; this is because the denominators of these linear combinations are bounded.

Thus for showing that $E(\mathbb{Q})$ is finitely generated we need a second ingredient: heights. These are machines that measure how complicated rational points are. We first define the height $H(x)$ of rational numbers $x \in \mathbb{Q}$ by writing $x = \frac{m}{n}$ with $\gcd(m,n) = 1$ and then putting $H(x) = \max\{|m|, |n|\}$. Note that $H(0) = H(\frac{0}{1}) = 1$. Observe that there are only finitely many rational numbers of height $< C$ for any fixed constant $C > 0$.

For a rational point $P \in E(\mathbb{Q})$ on an elliptic curve E we can now put

$$h(P) = \begin{cases} 1 & \text{if } P = \mathcal{O}, \\ \log H(x) & \text{if } P = (x,y). \end{cases}$$

Again it is easy to see that on a given elliptic curve E there are only finitely points of height bounded by some constant $C > 0$.

The second part of the proof of the Mordell-Weil theorem consists in checking that the height defined above is 'compatible' with the group law in the sense that one can bound $h(P+Q)$ in terms of $h(P)$ and $h(Q)$.

2. 2-Descent: Version I

The simplest version of 2-descent[2] applies to elliptic curves with three rational points of order 2:

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3), \tag{1}$$

where $e_1, e_2, e_3 \in \mathbb{Z}$ are pairwise distinct.

Now the left hand side of (1) is a square, hence the factors on the right hand side must be squares up to factors dividing their gcd. Let us therefore write

$$\begin{aligned} x - e_1 &= au^2, \\ x - e_2 &= bv^2, \\ x - e_3 &= cw^2, \end{aligned} \tag{2}$$

where a, b, c are squarefree integers and $u, v, w \in \mathbb{Q}$. Then $y^2 = abc(uvw)^2$, hence abc must be a square.

We will now prove the surprising fact that there are only finitely many possible values that a, b, c can take, even though the group of rational points on an elliptic curve can have infinitely many elements.

In fact, assume that $p \mid a$ and let p^k be the exact power of p dividing $x - e_1$. Since a is squarefree, k must be an odd integer. If $k < 0$, then p^k is also the exact power of p dividing $x - e_2$ and $x - e_3$ since e_2, e_3 are integers; thus the exact power of p dividing y^2 is p^{3k}, which is a contradiction since y^2 is a square and $3k$ is odd.

[2]Chowla, in his book *The Riemann Hypothesis and Hilbert's Tenth Problem*, said "The proof [...] is nothing beyond the capacity or ability of a ten year old."

Thus $k > 0$, and hence $x \equiv e_1 \bmod p$. Since p does not divide the denominator of x, the same is true for $bv^2 = x - e_2$ and $cw^2 = x - e_3$. Now $bv^2 = x - e_2 \equiv e_1 - e_2 \bmod p$ and $cw^2 = x - e_3 \equiv e_1 - e_3 \bmod p$. If $p \nmid (e_1 - e_2)(e_1 - e_3)$, then p^k is the exact power of p dividing y^2, which is nonsense because k is odd. Thus $p \mid (e_1 - e_2)(e_1 - e_3)$.

Similarly, we find $p \mid (e_2 - e_1)(e_2 - e_3)$ if $p \mid b$, and $p \mid (e_3 - e_1)(e_3 - e_2)$ if $p \mid c$. This means that every prime divisor of abc must also divide the product $(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$, and we have proved

Proposition 4. *There are only finitely many triples (a, b, c) of squarefree integers satisfying (2): any prime $p \mid abc$ must also divide $(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$.*

Let us now see what we have gained: starting from an elliptic curve (1) we have derived triples of equations (2) with the property that every rational point on E gives rise to a solution of one of the systems of equations. Instead of one equation we now have $3n$, where n is the number of triples (a, b, c) with the property that the integers a, b, c are squarefree and divisible only by a finite set of primes that we know. For $E : y^2 = x^3 - 4x$, for example, we have $e_1 = 0$, $e_2 = e_3 = 2$, hence there are 25 possible triples (a, b, c), because each of a, b has five possible values $0, \pm 1, \pm 2$, and c is determined by the fact that it is squarefree and abc is a square.

This does not look promising, but actually we will find that things are not as bad as they might look. What we have found is a map sending rational points $P \in E(\mathbb{Q})$ to some triple (a, b, c) of integers. In order to describe this map algebraically, we introduce the group $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. It consists of cosets $r\mathbb{Q}^{\times 2}$, where r is a nonzero rational integer defined up to squares. We can identify the triple (a, b, c) with the element $(a\mathbb{Q}^{\times 2}, b\mathbb{Q}^{\times 2}, c\mathbb{Q}^{\times 2}) \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \oplus \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \oplus \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ as long as $abc \neq 0$. Actually, since $a\mathbb{Q}^{\times 2} = (x - e_1)\mathbb{Q}^{\times 2}$, we can describe this map as follows:

$$(x, y) \longmapsto ((x - e_1)\mathbb{Q}^{\times 2}, (x - e_2)\mathbb{Q}^{\times 2}, (x - e_3)\mathbb{Q}^{\times 2}).$$

In order to simplify the notation, we will write the element on the right hand side as $(x - e_1, x - e_2, x - e_3)$.

What if $abc = 0$? Clearly, $a = 0$ happens if and only if $x = e_1$, that is, if and only if $P = (e_1, 0)$ is a point of order 2. Thus our map is defined for all elements of order not dividing 2. How should we define it at the torsion points? In order to get an answer, write $\alpha_i(P) = (x - e_i)\mathbb{Q}^{\times 2}$ for all $P = (x, y) \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, and put $\alpha = (\alpha_1, \alpha_2, \alpha_3)$. In this case, $y \neq 0$, and Equation (1) shows that

$$\alpha_1(P)\alpha_2(P)\alpha_3(P) = y^2 \cdot \mathbb{Q}^{\times 2} = 1 \cdot \mathbb{Q}^{\times 2}.$$

Now we use this relation to define $\alpha(P)$ for $P \in E[2]$:

$$\begin{aligned} \alpha_1(e_1, 0) &= \alpha_2(e_1, 0)\alpha_3(e_1, 0) = (e_1 - e_2)(e_1 - e_3)\mathbb{Q}^{\times 2}, \\ \alpha_2(e_2, 0) &= \alpha_1(e_2, 0)\alpha_3(e_2, 0) = (e_2 - e_1)(e_2 - e_3)\mathbb{Q}^{\times 2}, \\ \alpha_3(e_3, 0) &= \alpha_1(e_3, 0)\alpha_2(e_3, 0) = (e_3 - e_2)(e_3 - e_1)\mathbb{Q}^{\times 2}. \end{aligned} \tag{3}$$

Finally, we put $\alpha(\mathcal{O}) = (1, 1, 1)$. With these conventions we have

$$\alpha_1(P)\alpha_2(P)\alpha_3(P) = (1, 1, 1,),$$

or, since $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ has exponent 2, $\alpha_1(P)\alpha_2(P) = \alpha_3(P)$ for all $P \in E(\mathbb{Q})$. Now we claim

Proposition 5. *Let $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$ be an elliptic curve with $e_1, e_2, e_3 \in \mathbb{Z}$. The map*

$$\alpha = (\alpha_1, \alpha_2, \alpha_3) : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2} \oplus \mathbb{Q}^\times/\mathbb{Q}^{\times\,2} \oplus \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$$

defined above is a group homomorphism.

This is a surprising result containing a wealth of information. To see why let us denote the set of equations (2) by $C_{a,b,c}$; we will later see that $C_{a,b,c}$ is a curve, in fact a smooth curve of genus 1. Proposition 5 implies that if $C_{a,b,c}$ and $C_{a',b',c'}$ have a rational point, then so does the curve $C_{aa',bb',cc'}$. In fact, the equations for (a,b,c) are solvable in the rationals if and only if $(a,b,c) \in \operatorname{im}\alpha$ (where we declare that $C_{1,1,1}$ always has a rational solution, namely the point at infinity; we will make this precise later), and the claim now follows from the fact that $W(E) := \operatorname{im}\alpha$ is a group.

We also remark that our proof does not use the fact that we are working over $\mathbb{Q}$: Proposition 5 holds in any field containing $E[2]$. In particular, the triples (a,b,c) corresponding to curves $C_{a,b,c}$ with $\mathbb{Q}_p$-rational points also form a group $W_p(E)$ for each prime p, and it is clear that $W(E) \subseteq W_p(E)$. This implies that $W(E)$ is a subgroup of the 2-Selmer group $\mathrm{Sel}^{(2)}(E) := \bigcap W_p(E)$, whose elements (a,b,c) correspond to curves having p-adic points for every prime p (including $p=\infty$, i.e. the equations have solutions in $\mathbb{R}$).

It is known that quadratic equations $ax^2+by^2=c$ have a rational solution if and only if they have solutions in every completion $\mathbb{Q}_p$. The analogue for the equations corresponding to (a,b,c) is false: there exist examples where $W(E)$ is a proper subgroup of $\mathrm{Sel}^{(2)}(E)$. This suggests to look at the quotient group $\mathbf{Ш}(E)[2] := \mathrm{Sel}^{(2)}(E)/W(E)$, which is called the 2-part of the Tate-Shafarevich group of E. It is defined by the exact sequence

$$0 \longrightarrow W(E) \longrightarrow \mathrm{Sel}^{(2)}(E) \longrightarrow \mathbf{Ш}(E)[2] \longrightarrow 0$$

The group $\mathbf{Ш}(E)[2]$ is the subgroup of a bigger group $\mathbf{Ш}(E)$, the full Tate-Shafarevich group of E; it can be defined using Galois cohomology (we'll see how later), and is conjectured to be finite.

The next thing to do is work out the kernel:

Proposition 6. *We have* $\ker\alpha = 2E(\mathbb{Q})$.

These two propositions immediately imply the weak theorem of Mordell-Weil: we have $E(\mathbb{Q})/2E(\mathbb{Q}) = E(\mathbb{Q})/\ker\alpha \simeq \operatorname{im}\alpha$, and the image of α consists of triples (a,b,c) of squarefree integers whose prime factors divide the number $(e_1-e_2)(e_2-e_3)(e_3-e_1)$. This shows that the image of α is finite.

Once we know that $E(\mathbb{Q})$ is finitely generated, this even gives us a formula for the rank:

Corollary 7. *The rank r of the elliptic curve E is given by $2^{r+2} = \#\operatorname{im}\alpha$.*

In fact, if $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$, and $E(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2m$ for some $m \ge 1$, then $2E(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/m$, hence $E(\mathbb{Q})_{\mathrm{tors}}/2E(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2$, hence $E(\mathbb{Q})/2E(\mathbb{Q}) \simeq (\mathbb{Z}/2)^{r+2}$, and this implies the claim.

Before we complete the proof of Mordell-Weil, let us see how this works in the example $E : y^2 = x^3 - 4x$ coming up in the proof of Fermat's Last Theorem for the exponent 4. Nagell-Lutz shows that $E(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}, (-2,0), (0,0), (2,0)\}$. We

already know that these points correspond to the trivial solutions of $z^4 + 1 = w^2$ (namely $(w, z) = (\pm 1, 0)$ and two points at infinity), so Fermat's Last Theorem for the exponent 4 is equivalent to $r = 0$.

Now consider $x = au^2, x - 2 = bv^2, x + 2 = cw^2$. Since $a, b, c \in \{\pm 1, \pm 2\}$, the image of α has at most 16 elements. From $y^2 = x(x-2)(x+2)$ we deduce that $x \geq -2$, hence $c \geq 0$ and therefore $c > 0$. This implies $\#\operatorname{im} \alpha \mid 8$ (and therefore $r \leq 1$).

Now consider the triple $(a, b, c) = (1, 2, 2)$; here

$$x = u^2, \quad x - 2 = 2v^2, \quad x + 2 = 2w^2.$$

Writing $u = n/e$ for coprime integers n, e gives

$$n^2 - 2e^2 = 2r^2, \quad n^2 + 2e^2 = 2s^2$$

for integers $r = ev$, $s = ew$. This shows $n = 2N$, hence

$$2N^2 - e^2 = r^2, \quad 2N^2 + e^2 = s^2.$$

From $(n, e) = 1$ we deduce that e must be odd; but then r and s are odd. If N is odd, then the second equation shows that $1 \equiv s^2 = 2N^2 + e^2 \equiv 3 \bmod 8$. If N is even, then the first equation gives $1 \equiv r^2 = 2N^2 - e^2 \equiv -1 \bmod 4$. These contradictions show that $(1, 2, 2)$ is not in the image of α, hence $\#\operatorname{im} \alpha \mid 4$, and therefore $r = 0$ as claimed.

Just for fun, let us compute $\mathrm{Sel}^{(2)}$ and $W(E)$ exactly. We claim that

$$W(E) = \mathrm{Sel}^{(2)} = \{(1, 1, 1), (-1, -2, 2), (2, 1, 1), (2, -1, -2)\}.$$

The fact that all other triples are not solvable in $\mathbb{R}$ or in $\mathbb{Q}_2$ is a tedious but elementary exercise. It remains to show that the curves $C_{a,b,c}$ for the remaining triples have rational points.

(a, b, c)	x	u	v	w
$(-1, -2, 2)$	0	0	1	1
$(2, 2, 1)$	2	1	0	2
$(-2, -1, 2)$	-2	1	2	0

Note that these solutions come from the torsion points $(0, 0)$, $(2, 0)$ and $(-2, 0)$. Finally, $(1, 1, 1) = \alpha(\mathcal{O})$.

Proposition 8. *We have* $E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}, (-2, 0), (0, 0), (2, 0)\}$ *for* $E : y^2 = x^3 - 4x$.

Observe that the proof of Fermat's Last Theorem for the exponent 4 has been reduced to a couple of computations of signs and residue classes modulo 8 that can in principle be done by a computer.

Proof of Prop. 5. We have to show that $\alpha(P+Q) = \alpha(P)\alpha(Q)$ for all $P, Q \in E(\mathbb{Q})$.

Assume first that the points $P_i = (x_i, y_i)$, $i = 1, 2, 3$, are not in $E[2]$, and assume that they are collinear, i.e. that $P_1 + P_2 + P_3 = \mathcal{O}$. Letting $y = ax + b$ denote the line through the P_i, we find that the x-coordinates of the points of intersection of the line and the elliptic curve are roots of the monic cubic equation

$$(x - e_1)(x - e_2)(x - e_3) - (ax + b)^2.$$

Thus

$$(x - e_1)(x - e_2)(x - e_3) - (ax + b)^2 = (x - x_1)(x - x_2)(x - x_3). \tag{4}$$

Evaluation at $x = e_i$ yields

$$(x_1 - e_1)(x_2 - e_2)(x_3 - e_3) = (ae_i + b)^2 \in \mathbb{Q}^{\times 2}, \tag{5}$$

ans this shows that

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1 \cdot \mathbb{Q}^{\times 2}.$$

But now $\alpha(-P_3) = \alpha(P_3)$ since both points have the same x-coordinate and therefore the same image under α. Thus finally

$$\alpha(P_1)\alpha(P_2) = \alpha(-P_3) = \alpha(P_1 + P_2).$$

It remains to discuss the special cases where one of the points involved is in $E[2]$.

If $P = \mathcal{O}$, then $\alpha(P+Q) = \alpha(Q) = \alpha(P)\alpha(Q)$ since $\alpha(P) = (1,1,1)$ is the neutral element of the target group. If $P + Q = \mathcal{O}$, then $x_P = x_Q$, hence $\alpha(P) = \alpha(Q)$ amd therefore $\alpha(P + Q) = (1,1,1)$ since the target group has exponent 2.

If P is a point of order 2, then $\alpha(P + P) = \alpha(\mathcal{O}) = (1,1,1) = \alpha(P)^2$. If P and Q are distinct points order 2, say $P = (e_1, 0)$ and $Q = (e_2, 0)$, then $\alpha(P + Q) = \alpha((e_3, 0)) = \alpha(P)\alpha(Q)$ by direct inspection.

The last case to consider is where P_1 is a point of order 2, say $P_1 = (e_1, 0)$, and $P_2 = (x_1, y_1) \in E(\mathbb{Q}) \setminus E[2]$. The proof above was completely general up to (4); but now we have $y_1 = 0$, and evaluation at $x = e_1$ will not help us. Evaluation at e_2 and e_3 works just fine, however, and (5) shows that

$$\alpha_i(P_1 + P_2) = \alpha_i(P_1)\alpha_i(P_2), \quad i = 2, 3.$$

Note that $y_3 \neq 0$ since otherwise $P_2 = -P_1 - P_3$ would have order 1 or 2.

Now since $\alpha_2(P)\alpha_3(P) = \alpha_1(P)$,

$$\begin{aligned}\alpha_1(P_1 + P_2) &= \alpha_2(P_1 + P_2)\alpha_3(P_1 + P_2)\\ &= \alpha_2(P_1)\alpha_2(P_2)\alpha_3(P_1)\alpha_3(P_2)\\ &= \alpha_1(P_1)\alpha_1(P_2),\end{aligned}$$

which is what we wanted to prove. □

And now let us compute the kernel. This calculation is essentially equivalent to the following result:

Lemma 9. *Let $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$ be an elliptic curve with $e_1, e_2, e_3 \in \mathbb{Z}$. Then $P = (x, y) \in E(\mathbb{Q})$ can be written as $P = 2Q$ for some $Q \in E(\mathbb{Q})$ if and only if $x - e_i = r_i^2$ for rational numbers r_1, r_2, r_3. If this condition is satisfied, then $Q = (X, Y)$, where*

$$X = x + r_1r_2 + r_2r_3 + r_3r_1, \quad Y = (r_1 + r_2 + r_3)(X - x) - y,$$

and where the signs of the r_i have been chosen in such a way that $r_1r_2r_3 = y$.

Note that the different choices of the signs of the r_i give 4 solutions, namely Q and $Q + (e_i, 0)$.

Proof. Assume first that $P = 2Q$. Fix $i \in \{1, 2, 3\}$; the transformation $\xi = x - e_i$ transforms the equation of the elliptic curve into $y^2 = \xi(\xi^2 + a\xi + b)$ for integers a, b. The duplication formula for curves of that form is

$$2(x, y) = \Big(\Big(\frac{x^2 - b}{2y}\Big)^2, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3}\Big).$$

Thus if $(\xi, y) = 2(X, Y)$, then $\xi = x - e_i$ is a square.

A simpler proof proceeds as follows: the map $\alpha : E(\mathbb{Q}) \longrightarrow (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^3$ is a homomorphism into a group of exponent 2. Thus the image of $2E(\mathbb{Q})$ must be trivial, and this means exactly that the $x - e_i$ are rational squares.

The converse is just some calculation, which we will do by hand later once we have a few more tools. For now, let us use `pari`. Write $E : y^2 = x(x^2 + ax_b)$; then $e_1 = 0$, $a = -e_2 - e_3$ and $b = e_2e_3$. We know that $x - e_i = r_i^2$ for some rational numbers r_i. Choose the signs in such a way that $r_1r_2r_3 = y$. Then we claim that $Q = (X, Y)$, where

$$X = x + r_1r_2 + r_2r_3 + r_3r_1, \quad Y = (r_1 + r_2 + r_3)(X - x) - y.$$

Here's what `pari` says:

```
e2=r1^2-r2^2: e3=r1^2-r3^2
a=-e2-e3: b=e2*e3
x=r1^2: y=r1*r2*r3
X=x+r1*r2+r2*r3+r3*r1
Y=(r1+r2+r3)*(X-x)-y
ellpow(e,[X,Y],2)
```

The output is

```
[r1^2, r3*r2*r1]
```

which is exactly what we want in light of $x = r_1^2$ and $y = r_1r_2r_3$. □

The proof of Proposition 6 is now trivial: the condition $P = (x, y) \in \ker \alpha$ means that $\alpha(P) = (1, 1, 1)$, i.e., that $x - e_i = r_i^2$ for rational numbers r_1, r_2, r_3. The lemma above then implies that $P = 2Q$.