Introduction To Elliptic Curves

Franz Lemmermeyer

September 13, 2003

These are the notes for some lectures on the arithmetic of elliptic curves given in Seoul in August 2002.

Lecture 1	Aug. 08, 2002
Lecture 2	Aug. 09, 2002
Lecture 3	Aug. 12, 2002
Lecture 4	Aug. 13, 2002
Lecture 5	Aug. 14, 2002

Contents

Lecture 1.
The Rank of Elliptic Curves

1.1 Introduction

Let F be a field (most of the time we will consider the case where $F = \mathbb{Q}$ is the fild of rational numbers; other important examples are finite fields $\mathbb{F}_p$, the p-adic numbers $\mathbb{Q}_p$, as well as $\mathbb{R}$ and $\mathbb{C}$.

An elliptic curve E defined over a field F can be given by an equation in long Weierstrass form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

If F has characteristic $\neq 2$, one may transform this into

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{Q}, \tag{1.2}$$

where the polynomial on the right hand side is assumed not to have multiple roots; an equivalent condition is $\Delta(E) \neq 0$, where

$$\Delta(E) = 16(4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2).$$

An F-rational point on an elliptic curve (1.1) defined over a field F is a pair $(x, y) \in F \times F$ satisfying (1.1). In addition, we have to introduce a point $\mathcal{O}$ 'at infinity' that we think of being located infinitely far up the y-axis; this point $\mathcal{O}$ is also regared as being an F-rational point.

The set $E(F)$ of F-rational points on an elliptic curve can be made into an abelian group; two points $A, B \in E(F)$ are added by intersecting the line through A and B (the tangent to E at A if $B = A$) and reflecting the third point of intersection at the x-axis. Verifying the group axioms is easy except for associativity, which requires some effort.

Computing the addition formulas is essentially an exercise in highschool algebra:

Theorem 1.1. *Let E be an elliptic curve defined over some field F given in long Weierstrass form (1.1). Then the addition law is given by the following formulas:*

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

where

$$x_3 = -x_1 - x_2 - a_2 + a_1 m + m^2$$
$$y_3 = -y_1 - (x_3 - x_1)m - a_1 x_3 - a_3$$

and

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

1.2 Rational Points on Elliptic Curves

The structure of the abelian group $E(\mathbb{Q})$ is described by the following theorem:

Theorem 1.2 (Mordell-Weil). *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 $r \geq 0$ is a non-negative integer called the Mordell-Weil rank of E.

Theorem 1.2 was first proved by Mordell in the 1920s; as Weil has shown in 1928, it holds with $\mathbb{Q}$ replaced by any number field, and even with elliptic curves replaced by abelian varieties. Observe the analogy with number fields K: the units U_K of K form a finitely generated abelian group, and by Dirichlet's unit theorem we have

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

where $(U_K)_{\text{tors}}$ is the group of roots of unity in K, and where r is the unit rank, which can be computed in terms of the number of real and complex embeddings of K. For elliptic curves, determining r is a much more difficult problem.

The proof of the Mordell-Weil Theorem consists of two parts. The algebraic part is called the Weak Mordell-Weil Theorem:

Theorem 1.3. *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. The simplest proofs use $m = 2$.

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 $h(Q)$.

The torsion part of $E(\mathbb{Q})$ is rather easy to compute:

Theorem 1.4 (Nagell-Lutz). *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Z}$. If $P = (x, y) \in E(\mathbb{Q})$ is a torsion point, then*
i) $x, y \in \mathbb{Z}$;
ii) $y = 0$ or $y^2 \mid D = 4a^3 + 27b^2$.

As an example, consider the curve $E : y^2 = x^3 + 1$. Here $D = 27$, so if $(x, y) \in E(\mathbb{Q})_{\text{tors}}$, then $y = 0$ or $y^2 \mid 27$. By going through all these cases we find the following candidates of torsion points: $\mathcal{O}$, $(-1, 0)$, $(0, \pm 1)$, $(2, \pm 3)$. We claim that these are in fact torsion; for a proof it is sufficient to show that they are all killed by 6.

In fact, using the addition formulas we easily show that

$$\begin{aligned} 2 \cdot (2, 3) &= (0, 1), \\ 3 \cdot (2, 3) &= (0, 1) + (2, 3) = (-1, 0), \\ 4 \cdot (2, 3) &= 2 \cdot (0, 1) = (0, -1), \\ 5 \cdot (2, 3) &= (0, 1) + (-1, 0) = (2, -3), \\ 6 \cdot (2, 3) &= 2 \cdot (-1, 0) = \mathcal{O}. \end{aligned}$$

Thus $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/6\mathbb{Z}$.

For elliptic curves in short Weierstrass form (1.2), torsion points of order 2 can be described explicitly: if $x_1, x_2, x_3 \in \mathbb{C}$ denote the roots of the polynomial $x^3 + ax^2 + bx + c$, then

$$E(\overline{\mathbb{Q}})[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}.$$

Thus E has a rational point of order 2 if and only if $x^3 + ax^2 + bx + c$ has a rational root.

The torsion subgroup of elliptic curves defined over $\mathbb{Q}$ can be computed using `pari`. Elliptic curves are described by the long Weierstraß equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

(for memorizing, give x weight 2, y weight 3, and a_k weight k; then each term has weight 6), so our curve has $a_1 = a_2 = a_3 = a_4 = 0$, $a_6 = 1$, and we initialize

by typing `e = ellinit([0,0,0,0,1])`. Then `elltors(e)` produces the output `[6, [6], [[2,3]]]`: the first number is the cardinality of $E(\mathbb{Q})_{\rm tors}$, the second term [6] symbolizes the abstract structure $\mathbb{Z}/6\mathbb{Z}$ of $E(\mathbb{Q})_{\rm tors}$, and $[2,3]$ is a point generating the torsion subgroup.

The following deep result describes all possible torsion groups of elliptic curves over $\mathbb{Q}$:

Theorem 1.5 (Mazur). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\rm tors}$ is isomorphic to one of the following 15 groups:*

$$E(\mathbb{Q})_{\rm tors} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & \text{für } 1 \le m \le 4; \\ \mathbb{Z}/(2m-1)\mathbb{Z} & \text{für } 1 \le m \le 5; \\ \mathbb{Z}/2m\mathbb{Z} & \text{für } 1 \le m \le 6. \end{cases} \tag{1.3}$$

Loic Merel recently proved that the cardinality of $E(K)_{\rm tors}$ of elliptic curves over number fields K can be bounded in terms of the degree $(K:\mathbb{Q})$.

1.3 Simple 2-descent

In this section we are interested in studying rational points on cubic curves of the form

$$\mathrm{E}: y^2 = x^3 + ax^2 + bx + c, \tag{1.4}$$

where a, b, c are assumed to be integers. The rational points on (1.4) have a very special form:

Lemma 1.6. *Let $P = (x, y)$ be a rational point on (1.4); then there exist $m, n, e \in \mathbb{Z}$ such that $x = m/e^2$, $y = n/e^3$, and $(m, e) = (n, e) = 1$.*

Proof. Write $x = m/M$ und $y = n/N$ with $m, n \in \mathbb{Z}$, $M, N \in \mathbb{N}$ and $(m, M) = (n, N) = 1$. We want to show that $M^3 \mid N^2$ and $N^2 \mid M^3$, since this implies $M^3 = N^2$, that is, $M = e^2$ and $N = e^3$ for some $e \in \mathbb{N}$ (here we are using unique factorization: $N^2 = M^3$ implies that the exponent with which each prime factor appears is divisible by 2 and 3, hence by 6).

From $y^2 = x^3 + ax^2 + bx + c$ we get

$$M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3.$$

Since the right hand side is divisible by N^2, and since we know that $(n, N) = 1$, we conclude that $N^2 \mid M^3$. On the other hand we have $M \mid N^2m^3$ and $(m, M) = 1$, hence $M \mid N^2$. This implies $M^2 \mid N^2m^3$, that is, $M \mid N$, and running through this argument once more we find $M^3 \mid N^2$. □

From now on we consider curves (1.4) with $c = 0$:

$$y^2 = x(x^2 + ax + b), \quad a, b \in \mathbb{Z}, \quad b(a^2 - 4b) \neq 0. \tag{1.5}$$

These curves have the rational point $T = (0, 0)$; since $2T = \mathcal{O}$, this is a torsion point of order 2.

Now let us take such a rational point $P = (x, y)$ on such a curve (1.5) with $x = m/e^2$ and $y = n/e^3$ as in Lemma 1.6. Plugging this into equation (1.5) we get

$$n^2 = m(m^2 + ame^2 + be^4).$$

Thus we have two integers whose product is a square; if these integers were coprime we could conclude that each of them is a square since the integers form a UFD. Let us compute a bit: $\gcd(m, m^2+ame^2+be^4) = \gcd(m, be^4) = \gcd(m, b)$, since $(m, e) = 1$ by Lemma 1.6. If we write $b_1 = \gcd(m, b)$, then $b = b_1b_2$ and $m = b_1u$. This gives

$$n^2 = b_1u(b_1^2u^2 + ab_1ue^2 + b_1b_2e^4),$$

and with $n = b_1z$ we get

$$z^2 = u(b_1u^2 + aue^2 + b_2e^4).$$

Let us assume for now that $n \neq 0$. The two factors now *are* coprime (we just divided through by the greatest common divisor), and we see that u must be a square up to a unit factor. But by choosing the sign of b_1 appropriately we may assume that $u = M^2$ and $b_1u^2 + aue^2 + b_2e^4 = N^2$ for integers $M, N \in \mathbb{N}$ with $MN = z$. Replacing u by M^2 in the second equation we finally get

$$\mathcal{T}^{(\psi)}(b_1) : N^2 = b_1M^4 + aM^2e^2 + b_2e^4. \tag{1.6}$$

Thus every point $(x, y) \in \mathrm{E}(\mathbb{Q})$ gives rise to a point (N, M, e) on the curve $\mathcal{T}^{(\psi)}(b_1)$, where b_1 is given by $b_1 = \gcd(m, b)$ and $x = \frac{m}{e^2}$. Conversely, given (N, M, e) on $\mathcal{T}^{(\psi)}(b_1)$, we can get back our point (x, y) by reversing the construction. We know that $MN = z$ and $n = b_1z$; moreover $M^2 = u$ and $b_1u = m$. Thus $(x, y) = (b_1(M/e)^2, b_1NM/e^3)$. In particular, b_1 and x differ only by a square factor. This is a surprising result: if $(x, y) \in \mathrm{E}(\mathbb{Q})$, then even if $\mathrm{E}(\mathbb{Q})$ is infinite, there are only finitely many b_1 such that x/b_1 is a square.

Before we explore this further, let us address the case $n = 0$. If $m = 0$, then $(x, y) = (0, 0)$, hence $b_1 = \gcd(m, b) = b$, and in fact $N^2 = bM^4+aM^2e^2+e^4$ has the solution $(N, M, e) = (1, 0, 1)$ giving rise to the point $(0, 0) \in \mathrm{E}(\mathbb{Q})$. Assume now that $m \neq 0$. Then $(x, 0)$ must be a rational 2-torsion point different from $(0, 0)$; since torsion points have integral coordinates, we have $P = (c, 0)$ and $Q = (d, 0)$ for integers c, d; in particular we have $e = 1$. From $x^2 + ax + b = (x-c)(x-d)$ we read off $a = -c-d$ and $b = cd$, so for P we get $b_1 = \gcd(m, b) = \gcd(c, cd) = c$, and similarly $b_1 = d$ for Q. Thus in these cases, b_1 is given by the x-coordinate of the point.

We have shown that every rational point on (1.5) corresponds to a non-trivial[1] primitive[2] integral solution of one of the finitely many[3] curves (1.6);

[1] That is, we do not count the solution $N = M = e = 0$.
[2] This is our abbreviation for $(N, e) = (M, e) = 1$.
[3] There are only finitely many divisors b_1 of b.

these curves are called torsors of the elliptic curve (1.5) and will be denoted by $\mathcal{T}^{(\psi)}(b_1)$ in the following (the superscript (ψ) will be explained below). Torsors with a rational point are called trivial. By reversing our construction we already have seen that every integral point on (1.6) yields a rational point on (1.5): in fact, if (N,M,e) is a solution of (1.6), then $P=(x,y)$ is a rational point on (1.5), where $x=b_1M^2/e^2$ and $y=b_1MN/e^3$; solutions with $e=0$ correspond to the rational point $\mathcal{O}$ at infinity. Such a solution occurs if and only if $N^2=b_1M^4$, that is, if and only if b_1 is a square.

We also see that the solvability of (1.6) only depends on b_1 modulo squares: in fact, if (N,M,e) solves the torsor $\mathcal{T}^{(\psi)}(b_1)$, then (fN,M,fe) solves the torsor $\mathcal{T}^{(\psi)}(b_1f^2)$. Thus we only need to look at squarefree values of b_1:

Theorem 1.7. *The rational points on the elliptic curve (1.5) are in bijection with non-trivial primitive integral solutions on the torsors* (1.6)*, where b_1 runs through the squarefree divisors of $b=b_1b_2$.*

Given (N,M,e) on $\mathcal{T}^{(\psi)}(b_1)$, the point $(x,y)=(b_1M^2/e^2,b_1MN/e^3)$ is a rational point on $\mathrm{E}(\mathbb{Q})$*. Conversely, $P=(x,y)\in\mathrm{E}(\mathbb{Q})$ gives a primitive integral solution (N,M,e) on the torsor $\mathcal{T}^{(\psi)}(b_1)$, where b_1 is the squarefree number determined by $\alpha(P)=b_1\mathbb{Q}^{\times\,2}$, where $\alpha:\mathrm{E}(\mathbb{Q})\longrightarrow\mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ is the map given by*

$$\alpha(P)=\begin{cases}1\mathbb{Q}^{\times\,2} & \text{if } P=\mathcal{O};\\ b\mathbb{Q}^{\times\,2} & \text{if } P=(0,0);\\ x\mathbb{Q}^{\times\,2} & \text{if } P=(x,y)\in E(\mathbb{Q})\setminus\{\mathcal{O},(0,0)\}.\end{cases}\tag{1.7}$$

Observe that if (N,M,e) is a rational point on some torsor, and if d is the product of the denominators of N, M and e, then (d^2N,dM,de) is a point on the torsor with integral coordinates, and this point gives rise to the same point on $\widehat{\mathrm{E}}$ as (N,M,e).

Remark. Note that in our proof we have shown that $\gcd(N,M)=1$; we did, however, not assume that b_1 is squarefree. Thus we may assume that $\gcd(N,M)=1$ as long as b_1 runs through *all* divisors of b. If we restrict the values of b_1 to the squarefree divisors of b, then we have to allow common divisors of N and M. In any case we may assume that $(N,e)=(M,e)=1$: a common prime divisor of N and e divides M since b_1 is squarefree, and we may cancel the fourth power of the common divisor; similarly we can ensure that $(M,e)=1$.

We shall call $\alpha:\mathrm{E}(\mathbb{Q})\longrightarrow\mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ the Weil map (it was introduced by André Weil in his proof of Mordell's theorem). We found the Weil map from the group of rational points on E to the group $\mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ by studying the rational points on elliptic curves (1.6). Later we shall prove that this map is actually a group homomorphism; here we stayed away from everything involving the group law on elliptic curves and only used 'classical' methods, namely nothing beyond unique factorization.

1.4 Tate's Method

In this section we want to describe Tate's method for computing the rank of (certain) elliptic curves $E : y^2 = x(x^2 + ax + b)$. The idea is to consider E simultaneously with the 2-isogenous curve $\widehat{\mathrm{E}} : y^2 = x(x^2 + \widehat{a}\,x + \widehat{b}\,)$, where $\widehat{a} = -2a$ and $\widehat{b} = a^2 - 4b$. Here's what to do:

1. List all torsors $\mathcal{T}^{(\psi)}(b_1) : N^2 = b_1M^4 + aM^2e^2 + b_2e^4$, where b_1 runs through the squarefree divisors of $b = b_1b_2$; the number of such torsors that have a rational point $\neq (0,0,0)$ is a power of 2, say 2^w.

2. List all torsors $\mathcal{T}^{(\phi)}(b_1) : N^2 = b_1M^4 + \widehat{a}\,M^2e^2 + b_2e^4$, where b_1 runs through the squarefree divisors of $\widehat{b} = b_1b_2$; the number of such torsors that have a rational point $\neq (0,0,0)$ is a power of 2, say $2^{\widehat{w}}$.

3. The rank of E (and of $\widehat{\mathrm{E}}$) is given by $r = w + \widehat{w} - 2$.

Example. 1. Consider $E : y^2 = x(x^2 + 1)$. There are only two squarefree divisors of $b = 1$, but only $\mathcal{T}^{(\psi)}(1)$ has a rational point:

b_1	$\mathcal{T}^{(\psi)}(b_1)$	(N, M, e)	P
1	$N^2 = M^4 + e^4$	$(1,1,0)$	$\mathcal{O}$
-1	$N^2 = -M^4 - 5e^4$		

Thus $w = 0$.

2. Consider $\widehat{\mathrm{E}} : y^2 = x(x^2 - 4)$. Here we find four torsors:

b_1	$\mathcal{T}^{(\phi)}(b_1)$	(N, M, e)	P
1	$N^2 = M^4 - 4e^4$	$(1,1,0)$	$\mathcal{O}$
-1	$N^2 = -4M^4 + e^4$	$(1,0,1)$	$(0,0)$
2	$N^2 = 2M^4 - 2e^4$	$(0,1,1)$	$(2,0)$
-2	$N^2 = -2M^4 + 2e^4$	$(0,1,1)$	$(-2,0)$

Thus $\widehat{w} = 2$.

3. Now Tate's formula gives $r = 0 + 2 - 2 = 0$, that is, $E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}}$ and $\widehat{\mathrm{E}}(\mathbb{Q}) = \widehat{\mathrm{E}}(\mathbb{Q})_{\mathrm{tors}}$. Determining these torsion groups using Nagell-Lutz is left as an exercise.

As we will see, the main problem with this method is that we do not have an algorithm for deciding which of the torsors $\mathcal{T}(b_1)$ have rational points and which don't.

Lecture 2.
Local Solvability

2.1 Example

In the first lecture we have seen that, for the computation of the rank of elliptic curves $y^2 = x(x^2 + ax + b)$, it is important to tell which of the curves

$$\mathcal{T}(b_1) : N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4, \tag{2.8}$$

where $b = b_1 b_2$ and b_1 runs through the squarefree divisors of b, have a nontrivial rational (and therefore integral) solution.

It is clear that if (N, M, e) is an integral solution of (2.8), then

$$N^2 \equiv b_1 M^4 + aM^2 e^2 + b_2 e^4 \bmod p^k$$

for all prime powers p^k. Thus a necessary condition for the rational solvability is solvability modulo all prime powers.

Example. Consider the curve $y^2 = x(x^2 - 5)$.

b_1	$\mathcal{T}^{(\psi)}(b_1)$	(N, M, e)	P
1	$N^2 = M^4 - 5e^4$	$(1, 1, 0)$	$\mathcal{O}$
-1	$N^2 = -M^4 + 5e^4$	$(2, 1, 1)$	$(-1, 2)$
5	$N^2 = 5M^4 - e^4$	$(2, 1, 1)$	$(5, 10)$
-5	$N^2 = -5M^4 + e^4$	$(1, 0, 1)$	$(0, 0)$

Now we do the same for $\widehat{\mathrm{E}} : y^2 = x(x^2 + 20)$. We do not have to consider negative values of b_1 since the corresponding torsors do not even have nontrivial real (let alone rational) solutions.

b_1	$\mathcal{T}^{(\phi)}(b_1)$	(N,M,e)	P
1	$N^2 = M^4 + 20e^4$	$(1,1,0)$	$\mathcal{O}$
2	$N^2 = 2M^4 + 10e^4$		
5	$N^2 = 5M^4 + 4e^4$	$(2,0,1)$	$(0,0)$
10	$N^2 = 10M^4 + 2e^4$		

What about $\mathcal{T}^{(\phi)}(2)$? Assume that (N,M,e) is an integral solution; Then clearly N is even, say $N=2n$, and we get $2n^2 = M^4 + 5e^4$. Reduction modulo 5 shows that $2n^2 \equiv M^4 \bmod 5$. But since 2 is a quadratic nonresidue, this implies $n \equiv M \equiv 0 \bmod 5$, which implies that $5 \mid e$ and therefore contradicts the assumption that $(N,e)=1$. Thus $\mathcal{T}^{(\phi)}(2)$ has no (nontrivial) solutions in $\mathbb{Z}$.

Similarly, it can be shown that $\mathcal{T}^{(\phi)}(10)$ has no (nontrivial) solutions in $\mathbb{Z}$. In particular, the elliptic curve $y^2 = x(x^2-5)$ has rank $r = 2+1-1 = 1$.

Given a torsor $\mathcal{T}(b_1)$, how can we find 'good' primes modulo which we can (possibly) get a contradiction? This is where a theorem of F.K. Schmidt comes in.

2.2 Quartics over $\mathbb{F}_p$

Consider the torsor $\mathcal{T}(b_1)$, with b_1 a squarefree integer, over the field $\mathbb{F}_p$. Our aim is to prove the following

Theorem 2.1. *The torsor (2.8) has an $\mathbb{F}_p$-rational point for every prime p such that $p \nmid 2(a^2-4b)$.*

Remark 1. The polynomial $f(X) = b_1X^4 + aX^2 + b_2$ has discriminant $\operatorname{disc} f = 16b(a^2-4b)^2 = 16b(\operatorname{disc} g)^2$, where $g(X) = b_1X^2 + aX + b_2$. Although $p \nmid 2\operatorname{disc} g$ suffices to guarantee solvability modulo p, for constructing solutions modulo p^k we need to apply Hensel's Lemma, and this applications forces us to assume that $p \nmid \operatorname{disc} f$. Thus a torsor $\mathcal{T}(b_1)$ has a solution in $\mathbb{Z}_p$ if $p \nmid 2b(a^2-4b)$; this is exactly the condition given in [5, Chap. X, Prop. 4.9].

Remark 2. There is a general theorem due to F.K. Schmidt (also proved by Châtelet) saying that any smooth curve of genus 1 has a point over any finite field. Note that the torsors $\mathcal{T}(b_1)$ are singular at infinity, so one has to be careful when applying this result.

Remark 3. The simple proof of Theorem 2.1 given here is due to Wayne Aitken (San Marcos) and myself.

Proof. If $e = 0$ gives rise to a solution (N, M, e), then $N^2 \equiv b_1 M^4 \bmod p$, and this implies that b_1 is a square modulo p (possibly 0). Conversely, if b_1 is a square modulo p, then there exists an $\mathbb{F}_p$-rational point $(N, M, e) \in \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ with $e = 0$ (and $M \neq 0$).

Thus Theorem 2.1 is proved if b_1 is a square modulo p, so from now on we will assume that $(b_1/p) = -1$. In this case we can't have solutions with $e = 0$, so we might as well divide through by e^4, put $y = N/e^2$ and $X = M/e$, and get

$$y^2 = b_1 X^4 + aX^2 + b_2. \tag{2.9}$$

Now the substitution $X^2 = x$ transforms (2.9) into the conic

$$C : y^2 = b_1 x^2 + ax + b_2. \tag{2.10}$$

The condition $p \nmid 2(a^2 - 4b_1 b_2)$ ensures that C is nonsingular. Our aim is to find an $\mathbb{F}_p$-rational point (x, y) on C such that $x = X^2$ is a square.

The proof proceeds in several steps: we start by assuming that p is an odd prime not dividing $a^2 - 4b$.

1. The conic C has an $\mathbb{F}_p$-rational point. Assume not; then the right hand side of (2.10) is a nonsquare for every $x \in \mathbb{F}_p$. Thus, by Euler's criterion, $f(X) = (b_1 X^2 + aX + b_2)^{(p-1)/2} + 1$ is a polynomial of degree $p - 1$ with $f(x) = 0$ for all $x \in \mathbb{F}_p$: this is a contradiction because nonzero polynomials f over fields have at most $\deg f$ roots. Observe that f is nonzero: its degree is $\geq \frac{p-1}{2}$ unless $p \mid b_1$ and $p \mid a$; but then $p \mid (a^2 - 4b)$, contradicting our assumption.

2. Parametrize the conic C. Starting with the $\mathbb{F}_p$-rational point $P = (x_0, y_0)$ we can parametrize the conic C: consider all lines L_t through P with 'slope' $t \in \mathbb{F}_p$; L_t intersects the conic in P and in a second point with coordinates (x, y), where

$$x = \frac{t^2 x_0 - 2ty_0 + b_1 x_0 + a}{t^2 - b_1}, \tag{2.11}$$

$$y = t(x - x_0) + y_0 = \frac{-t^2 y_0 + t(2b_1 x_0 + a) - b_1 y_0}{t^2 - b_1}. \tag{2.12}$$

Since we assumed that b_1 is a nonsquare modulo p, every $t \in \mathbb{F}_p$ gives rise to a point on C over $\mathbb{F}_p$. If $x_0 = 0$, then x_0 is a square and we are done. If $x_0 \neq 0$, then we can multiply the numerator and denominator in (2.11) by x_0 and get

$$x = \frac{(x_0 t - y_0)^2 - b_2}{x_0(t^2 - b_1)}. \tag{2.13}$$

Assume that there is no point $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ on C with x a square in $\mathbb{F}_p$; then we must have $(x/p) = -1$ for all x, in particular $(x_0/p) = -1$ and therefore $\left(\frac{(x_0 t - y_0)^2 - b_2}{p}\right) = \left(\frac{t^2 - b_1}{p}\right)$ for all $t \in \mathbb{F}_p$.

3. By Corollary 2.4 below we have $y_0 = 0$ and $b_2 = x_0^2 b_1$. This gives $0 = y_0^2 = b_1 x_0^2 + a x_0 + b_2 = b_1 x_0^2 + a x_0 + b_1 x_0^2$, hence $a = -2b_1 x_0$. But then $a^2 - 4b = a^2 - 4b_1 b_2 = 4b_1^2 x_0^2 - 4b_1(b_1 x_0^2) = 0$ contradicting the assumption that $p \nmid (a^2 - 4b)$.

This concludes the proof. □

It remains to prove Corollary 2.4. We start with

Lemma 2.2. *Let $f, g \in \mathbb{F}_p[X]$ be quadratic polynomials over $\mathbb{F}_p$. If $f(t)^n = g(t)^n$ for all $t \in \mathbb{F}_p$ and some integer $n \le \frac{p-1}{2}$, then there exists a constant $c \in \mathbb{F}_p$ such that $f = c \cdot g$.*

Proof. Clearly $\deg f^n = n \deg f \le p-1$, hence the polynomial $f^n - g^n$ has degree $\le p-1$ and at least p roots $0, 1, \ldots, p-1$. Since $\mathbb{F}_p$ is a field, polynomials of degree m have at most m roots; hence we conclude that $f^n = g^n$.

Now factor f and g into linear factors over some finite extension of $\mathbb{F}_p$; then every root α with multiplicity m is a root of multiplicity mn of f^n, thus of g^n, hence a root of multiplicity m of g. Thus f and g have the same roots (with multiplicity) over some extension of $\mathbb{F}_p$, hence they are equal up to some constant c (which necessarily is an element of the base field $\mathbb{F}_p$ since the coefficients of f and g are). □

Proposition 2.3. *Assume that $f, g \in \mathbb{F}_p[X]$ are quadratic polynomials over $\mathbb{F}_p$ such that $(\frac{f(t)}{p}) = (\frac{g(t)}{p})$ for all $t \in \mathbb{F}_p$. Then there exists a constant $c \in \mathbb{F}_p$ such that $f = c \cdot g$.*

Proof. By Euler's criterion we know that $(\frac{f(t)}{p}) \equiv f(t)^n \pmod p$ with $n = \frac{p-1}{2}$; thus the assumptions imply that $f(t)^n \equiv g(t)^n \pmod p$ for all $t \in \mathbb{F}_p$, so the claim follows from Lemma 2.2. □

Remark. It would be interesting to know whether the condition that $(\frac{f(t)}{p}) = (\frac{g(t)}{p})$ for all $t \in \mathbb{F}_p$ can be weakened.

Corollary 2.4. *If $\left(\frac{(x_0 t - y_0)^2 - b_2}{p}\right) = \left(\frac{t^2 - b_1}{p}\right)$ for $t = 0, 1, \ldots, p-1$, then $y_0 = 0$ and $b_2 = b_1 x_0^2$.*

Proof. The converse of the claim is trivially true. On the other hand, applying Prop. 2.3 to the assumption shows that $f(X) = (x_0 X - y_0)^2 - b_2$ and $g(X) = X^2 - b_1$ differ by a constant factor c; comparing the coefficients of the leading term shows that $c = x_0^2$ whereas comparing linear terms gives $y_0 = 0$. Finally, comparing constant terms shows that $b_2 = b_1 x_0^2$. □

2.3 Reichardt's Counterexample to the Hasse Principle

Let us now try to compute the rank of the elliptic curve $E : y^2 = x(x^2 + 17)$. We find

b_1	$\mathcal{T}^{(\psi)}(b_1)$	(N, M, e)	P
1	$N^2 = M^4 + 17e^4$	$(1, 1, 0)$	$\mathcal{O}$
17	$N^2 = 17M^4 + e^4$	$(1, 0, 1)$	$(0, 0)$

Thus $w = 1$. Next consider $\widehat{\mathrm{E}} : y^2 = x(x^2 - 4 \cdot 17)$. We find

b_1	$\mathcal{T}^{(\psi)}(b_1)$	(N, M, e)	P
1	$N^2 = M^4 - 68e^4$	$(1, 1, 0)$	$\mathcal{O}$
-1	$N^2 = -M^4 + 68e^4$		
2	$N^2 = 2M^4 - 34e^4$		
-2	$N^2 = -2M^4 + 34e^4$		
17	$N^2 = 17M^4 - 4e^4$		
-17	$N^2 = -17M^4 + 4e^4$	$(1, 0, 1)$	$(0, 0)$
34	$N^2 = 34M^4 - e^4$		
-34	$N^2 = -34M^4 + 2e^4$		

At this point we only know that $1 \leq \widehat{w} \leq 3$, giving $0 \leq r \leq 2$. Thus consider the torsor $N^2 = -M^4 + 68e^4$; reduction modulo 17 gives $N^2 \equiv -M^4 \bmod 17$, but this does not help us since $-1 \equiv 4^2 \bmod 17$. Note, however, that M is odd (otherwise 2 would divide both M and N); reduction modulo 4 shows that $N^2 \equiv -M^4 \equiv -1 \bmod 4$, which is impossible. Similarly, reduction modulo 4 shows that $\mathcal{T}^{(\psi)}(17)$ does not have a rational point.

This improves our estimates to $1 \leq \widehat{w} \leq 2$ and $0 \leq r \leq 1$.

Now consider the torsor

$$N^2 = 2X^4 - 34Y^4. \tag{2.14}$$

In 1942, Reichardt proved that this curve has solutions modulo every $m > 1$, but that it doesn't have any rational points different from $(0, 0, 0)$. The argument he used for showing the nonexistence of rational points was ingenious but more complicated than the simple proof below.

Local Solutions

By Theorem 2.1 there are solutions to this congruence modulo every odd prime $p \neq 17$, and Hensel's Lemma guarantees that we can lift these solutions to prime powers p^k.

For $p = 17$, we find a 17-adic solution of (2.14) by letting $n = X = \sqrt{2}$ and $Y = 0$. For $p = 2$, we can find an $x \in \mathbb{Z}_2$ such that $x^4 = 17$ and then put $n = 0$, $X = x$, and $Y = 1$.

Thus (2.14) has $\mathbb{Q}_p$-rational points for every p, and clearly has solutions in $\mathbb{R} = \mathbb{Q}_\infty$, hence has local solutions everywhere.

Global Solutions

Using the quadratic reciprocity law it can be shown that (2.14) does not have any nontrivial rational point. In fact, assume that $p \equiv 1 \bmod 8$ is a prime, and that $N^2 = 2M^4 - 2pe^4$ for some triple of nonzero integers (N, M, e) with $(N, e) = (M, e) = 1$. Write $N = 2n$; then $2n^2 = M^4 - pe^4$. Clearly $p \nmid M$ since otherwise p would divide both M and N. Reducing modulo p gives $2n^2 \equiv M^4 \bmod p$, and raising this to the $\frac{p-1}{4}$-th power we get $(n/p) = (2/p)_4$, where $(a/p)_4 \equiv a^{(p-1)/4} \bmod p$ is the fourth power residue symbol. Note that $(2/p)_4 = \pm 1$ since $(2/p) = +1$ from $p \equiv 1 \bmod 8$.

On the other hand, we can compute (n/p) in a different way: write $n = 2^j t$ for some odd integer t; then $(n/p) = (t/p)$ since $(2/p) = +1$. Next, $(t/p) = (p/t)$ by quadratic reciprocity. On the other hand, reducing $2n^2 = M^4 - pe^4$ modulo any prime q dividing t, we get $M^4 \equiv pe^4 \bmod q$, that is, $(p/q) = +1$. Thus $(p/t) = +1$, and we have proved

Proposition 2.5. *Let $p \equiv 1 \bmod 8$ be a prime. If $N^2 = 2M^4 - 2pe^4$ has a nontrivial integral solution, then $(2/p)_4 = +1$.*

Thus in particular, $N^2 = 2M^4 - 34e^4$ does not have nontrivial solutions since $(2/17)_4 = -1$.

Lecture 3.
Conics

Elliptic curves are nonsingular cubic curves with a rational point and have genus 1; conics are quadratic curves and have genus 0. In this lecture we will present a theory of conics that is closely analogous to that of elliptic curves. First, however, we will talk about parametrization, a technique that only works for curves of genus 0.

3.1 Parametrization

Parametrization of conics is a technique that allows to find all rational points on a conic if at least one such point is known. Note that there are conics without any rational point such as $x^2 + y^2 = 3$.

It will be sufficient to present an example: the unit circle $C : x^2 + y^2 = 1$. We start with the known point $P = (-1, 0)$ and consider all lines through P with slope t: $y = t(x + 1)$. Next we compute the points of intersection of the line and C: we find

$$0 = x^2 + t^2(x + 1)^2 - 1 = (x + 1)(x - 1 + t^2(x + 1)).$$

The solution to $x+1 = 0$ corresponds to P; the solution to $x-1+t^2(x+1) = 0$, namely $x = \frac{1-t^2}{1+t^2}$, corresponds to the second point of intersection, and we find $y = t(x + 1) = \frac{2t}{1+t^2}$.

Now if t is rational, then these formulas will give a rational point on C. Conversely, if $Q = (x, y)$ is any rational point on C different from $P = (-1, 0)$, then the line through P and Q will have a rational slope $t = \frac{y}{x+1}$ and will therefore be given by the formulas above.

3.2 The Group Law

We can study plane algebraic curves both over the affine plane and over the projective plane. If we want to give elliptic curves a group law, we have to use the projective plane; similarly, we can give conics a group law as long as we stick to the affine plane.

For the unit circle $C : x^2 + y^2 = 1$ over the real numbers we can define a group law simply by 'adding angles': fix a rational point N on C, say $N = (1, 0)$, and define $A + B$ to be the point P such that $\angle NOA + \angle NOB = \angle NOP$.

The group law on non-degenerate conics C defined over a field F is quite simple: fix any rational point N on C; for computing the sum of two rational points $A, B \in C(F)$, draw the line through N parallel to AB, and denote its second point of intersection with C by $A+B$. It is a simple geometric exercise to show that, in the case of the unit circle in the Euclidean plane, both definitions agree.

It is straight forward to write down formulas for the addition of points on a conic, but it takes some effort to simplify these formulas to the one given in the next proposition:

Proposition 3.1. *Consider the conic $\mathcal{C} : X^2 - dY^2 = c$ over a field K with odd characteristic, and assume that $cd \neq 0$. Let $N = (x, y)$ be a K-rational point on $\mathcal{C}$. Then the group law on $\mathcal{C}$ with neutral element N is given by*

$$(r, s) + (t, u) = \Big(\frac{x(rt + dsu) - dy(ru + st)}{c}, \frac{x(ru + st) - y(rt + dsu)}{c}\Big).$$

Proof. For adding the points $P = (r, s)$ and $Q = (t, u)$, we have to draw a parallel to the line PQ through N and compute its second point of intersection with $\mathcal{C}$.

If $P = Q$, then the slope m can be computed by taking the derivative of the curve equation and solving for Y'; we find $Y' = \frac{x}{dy}$, hence $m = \frac{r}{ds}$ in $P = (r, s)$. A simple calculation yields

$$X = \frac{x(r^2 + ds^2) - 2rsdy}{r^2 - ds^2} = \frac{x(r^2 + ds^2) - 2rsdy}{c}.$$

Now assume that $P \neq Q$; if $r = t$, then $(r, s) = P = -Q = (t, -u)$ and $P + Q = N = (x, y)$, which agrees with the claimed formula. Thus we may assume that $r \neq t$; the line through PQ has slope $m = \frac{s-u}{r-t}$, hence the parallel through N is given by the equation $Y - y = m(X - x)$. Intersecting this line with $\mathcal{C}$ leads to

$$(X - x)\big[X + x - dm^2(X - x) - 2mdy\big] = 0;$$

since $X = x$ gives the point N, the X-coordinate of the second point of intersection is given by

$$X = \frac{2mdy - (1 + dm^2)x}{1 - dm^2}.$$

Plugging in $m = \frac{s-u}{r-t}$, we find

$$X = \frac{2(s - u)(r - t)dy - [(r - t)^2 + d(s - u)^2]x}{(r - t)^2 - d(s - u)^2}.$$

We now take a closer look at the denominator. We find

$$(r - t)^2 - d(s - u)^2 \;=\; r^2 - ds^2 + t^2 - du^2 - 2rt + 2dsu \;=\; 2(c - rt + dsu).$$

Next

$$(c - rt + dsu)(ru + st) = c(r - t)(u - s).$$

This shows that

$$\frac{2y(s-u)(r-t)}{(r-t)^2 - d(s-u)^2} \;=\; -\frac{y(ru+st)}{c};$$

and that the X-coordinates of both sides agree if $x = 0$.

I haven't seen yet how to transform the term involving x. □

Algebraically, the group law on a conic $X^2 - aY^2 = c$ with neutral element $N = (x, y)$ can be described as follows: identify points (r, s) on the conic with the algebraic number $r + s\sqrt{d}$ of norm c; then

$$(r + s\sqrt{d}\,) * (t + u\sqrt{d}\,) = \frac{(r + s\sqrt{d}\,)(t + u\sqrt{d}\,)}{x + y\sqrt{d}}$$

corresponds to the point $(r, s) + (t, u)$ on the conic.

Proposition 3.1 implies that the group law on conics $Y^2 - aX^2 = 1$ is defined over $\mathbb{Z}$, hence over any ring! In general, the group law of $Y^2 - aX^2 = c$ is defined over the ring $\mathbb{Z}[\frac{1}{c}]$.

What about associativity? It is easy to see that associativity of the group law on conics is equivalent to a special case of Pascal's theorem:

Proposition 3.2. *Let $ABCPNQ$ be a hexagon inscribed into a conic. Then the points of intersection of the lines AB and PN, BC and NQ, CP and QA are collinear.*

The special case we need is when the line containing these points of intersection is the line at infinity, that is, when the lines in question are parallel in the affine plane.

For checking that $(A+B)+C = A+(B+C)$, put $P = A+B$ and $Q = B+C$. Associativity is equivalent to $P + C = A + Q$, which in turn holds if and only if $QA \parallel CP$. But since $AB \parallel PN$ and $BC \parallel NQ$ by construction and the definition of the group law, this follows immediately from Pascal's theorem.

Exercise. Show that the addition on a parabola $\mathcal{P} : y = x^2$ with neutral element $\mathcal{O} = (0, 0)$ is given by $(a, a^2) + (b, b^2) = (c, c^2)$ with $c = a + b$; in other words: $\mathcal{P}(R) \simeq (R, +)$ is the additive group of the ring over which we work.

Exercise. Show that the addition on a hyperbola $\mathcal{H} : xy = 1$ with neutral element $\mathcal{O} = (1, 1)$ is given by $(a, 1/a) + (b, 1/b) = (c, 1/c)$ with $c = ab$; in other words: $\mathcal{H}(R) \simeq R^\times$ is the group of units of the ring over which we work.

3.3 The Group Structure

For conics, we have the following nice result (our rings have an identity preserved by ring homomorphisms):

Proposition 3.3. *If C is a conic defined over $\mathbb{Z}$, and if $f : R \longrightarrow S$ is a ring homomorphism, then $f^*(x,y) = (f(x), f(y))$ induces a group homomorphism $f^* : C(R) \longrightarrow C(S)$. If f is injective (bijective), then so is f^*.*

Proof. A simple exercise. Note that surjectivity of f does not imply surjectivity of f^*. □

In particular, the Chinese Remainder Theorem applies to conics in the sense that

$$C(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_i C(\mathbb{Z}/p^{a_i}\mathbb{Z})$$

whenever $N = \prod_i p^{a_i}$, that is, if

$$\mathbb{Z}/N\mathbb{Z} \simeq \prod_i \mathbb{Z}/p^{a_i}\mathbb{Z}.$$

The structure of $C(\mathbb{F}_p)$ for odd primes p and conics $C : x^2 - ny^2 = 1$ can be determined easily: we have

$$C(\mathbb{F}_p) \simeq \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } (n/p) = +1 \\ \mathbb{Z}/(p+1)\mathbb{Z} & \text{if } (n/p) = -1. \end{cases}$$

In particular, we have $\#C(\mathbb{F}_p) = p - (n/p)$ for all primes $p \nmid 2n$.

Primality tests

Proposition 3.4. *Let $\mathcal{C} : x^2 - dy^2 = 1$ be a conic, pick $N = (1,0)$ as the neutral element, and assume that $q \equiv 7 \bmod 8$ is an integer such that $(\frac{d}{q}) = -1$. Then q is prime if and only if there exists a point $P \in \mathcal{C}(\mathbb{Z}/q\mathbb{Z})$ such that*

i) $(q+1)P = (1,0)$;

ii) $\frac{q+1}{r} P \neq (1,0)$ *for any prime r dividing $(q+1)$.*

In the special case of Mersenne numbers $q = 2^p - 1$ (note that $q \equiv 7 \bmod 12$ for $p \geq 3$), we have $\frac{q+1}{2} = 2^{p-1}$, and if we choose $\mathcal{C} : x^2 - 3y^2 = 1$ and $P = (2,1)$, then the test above is nothing but the Lucas-Lehmer test.

Factorization Methods

The factorization method based on elliptic curves is very well known. Can we replace the elliptic curve by conics? Yes we can, and what we get is the $p-1$-factorization method for integers N if $\#C(\mathbb{Z}/p\mathbb{Z}) = p - 1$ for all primes $p \mid N$ (for example if we work with the conic $\mathcal{H} : xy = 1$), the $p+1$-factorization method if $\#C(\mathbb{Z}/p\mathbb{Z}) = p + 1$ for all $p \mid N$, and some hybrid method otherwise.

The only exposition of primality tests and factoring using conics in the mathematical literature seems to be [9].

3.4 Computing the Rank

Now let us compare the structure of the groups of rational points: for elliptic curves, we have the famous theorem of Mordell-Weil that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, where $E(\mathbb{Q})_{\text{tors}}$ is the finite group of points of finite order, and r is the Mordell-Weil rank. For conics, on the other hand, we have two possibilities: either $C(\mathbb{Q}) = \varnothing$ (for example if $C : x^2 + y^2 = 3$) or $C(\mathbb{Q})$ is infinite, and in fact not finitely generated (see Tan [8]). The analogy can be saved, however, by looking at integers instead of rational numbers: Shastri [4] has shown that for the unit circle $C : x^2 + y^2 = 1$ over number fields K we have $C(\mathcal{O}_K) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^r$, where $r = s - 1$ if K contains a square root of -1, and $r = s$ otherwise; here s is the number of complex primes of K. More generally, we consider rings $\mathcal{O}_S$ of S-integers for finite sets S of primes; an element of K is an S-integer if its denominator is divisible at most by primes in S. Then we find

$$C(\mathcal{O}_K) \simeq C(\mathcal{O}_K)_{\text{tors}} \oplus \mathbb{Z}^r \qquad\qquad E(K) \simeq E(K)_{\text{tors}} \oplus \mathbb{Z}^r$$

where $r \geq 0$ is an integer that – in the case of conics $x^2 - dy^2 = 1$ – can be determined in terms of the number of complex primes in K.

Proposition 3.5. *Let C be the conic defined by $x^2 - dy^2 = 1$. Let K be a number field, S a finite set of prime ideals in K, $\mathcal{O}_S$ the ring of S-integers in K. Then*

$$C(\mathcal{O}_S) = C(\mathcal{O}_S)_{\text{tors}} \oplus \mathbb{Z}^k$$

for some integer $k \geq 0$ and a finite group $C(\mathcal{O}_S)_{\text{tors}}$.

In the special case $S = \varnothing$, let r and $2s$ denote the number of real and complex embeddings of K. Then $\mathcal{O}_S = \mathcal{O}_K$, and

$$C(\mathcal{O}_K) = C(\mathcal{O}_K)_{\text{tors}} \oplus \mathbb{Z}^k,$$

where

$$k = \begin{cases} r + s - 1 & \text{if } \sqrt{d} \in K; \\ r + s & \text{if } \sqrt{d} \notin K \text{ and } d > 0, \\ s & \text{if } \sqrt{d} \notin K \text{ and } d < 0. \end{cases}$$

Moreover,

$$C(\mathcal{O}_K) \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } d = 1, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } d \neq 1. \end{cases}$$

The proof given in Shastri [4] works with only minor modifications. Observe that by choosing conics $C : x^2 - dy^2 = c$ such that the set S of primes dividing c is large, we can make the rank of the group $C(\mathbb{Z}_S)$ of S-integral points on C arbitrarily large.

Exercise. Let (t, u) be a solution of $t^2 - u^2 m = 1$; show that $(t, u\sqrt{-m})$ is a solution of $x^2 + y^2 = 1$ over $\mathbb{Q}(\sqrt{-m})$.

There is very close analogy between elliptic curves and conics $x^2 - ny^2 = 1$:

object	conics	elliptic curves
group structure in	affine plane	projective plane
defined over	rings	fields
group elements	integral points	rational points
group structure	$C(\mathcal{O}_S)_{\text{tors}} \oplus \mathbb{Z}^r$	$E(K)_{\text{tors}} \oplus \mathbb{Z}^r$
associativity	Pascal's theorem	Bezout's theorem

Consider $x^2 - dy^2 = 1$ over $\mathbb{Z}_S = \mathbb{Z}[\frac{1}{s}]$, where $S = \{p : p \mid s\}$. Then $dy^2 = (x-1)(x+1)$; write

$$\delta = \gcd(x-1, x+1) = \begin{cases} 1 & \text{if } 2 \mid x, \\ 2 & \text{if } 2 \nmid x. \end{cases}$$

Observe that $\delta = 1$ implies $d \equiv 3 \bmod 4$.

Assume $\delta = 2$. Then $x + 1 = 2ar^2$, $x - 1 = 2bs^2$, with $ab = d$ and $2rs = y$. Thus $1 = ar^2 - bs^2$.

If $d \equiv 3 \bmod 4$ and $\delta = 1$, then $x + 1 = ar^2$, $x - 1 = bs^2$, where $ab = d$ and $rs = y$. Thus $2 = ar^2 - bs^2$.

Consider the map $\alpha : C(\mathbb{Z}_S) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ defined by

$$(x, y) \longmapsto \begin{cases} 2(x+1)\mathbb{Q}^{\times\,2} & \text{if } x \ne -1, \\ -d\mathbb{Q}^{\times\,2} & \text{if } x = -1. \end{cases}$$

Note that $2(x+1)\mathbb{Q}^{\times\,2} = a\mathbb{Q}^{\times\,2}$ if $\delta = 2$ and $2(x+1)\mathbb{Q}^{\times\,2} = 2a\mathbb{Q}^{\times\,2}$ if $\delta = 1$.

Claim. α is a group homomorphism.

Thus given points $P = (r, s), Q = (t, u) \in C(\mathbb{Z}_S)$ we have to show that $\alpha(P)\alpha(Q) = \alpha(P+Q)$. The left hand side is $2(r+1)\cdot 2(t+1)\mathbb{Q}^{\times\,2} = (r+1)(t+1)\mathbb{Q}^{\times\,2}$; the right hand side equals $2(rt + dsu + 1)\mathbb{Q}^{\times\,2}$, and the problem is to show that $(r+1)(t+1)$ and $2(rt + dsu + 1)$ differ at most by a square factor.

Proposition 3.6. *The image of α consists of all square classes $\delta a\mathbb{Q}^{\times\,2}$ such that $ar^2 - bs^2 = 2/\delta$ has an S-integral solution.*

Proof. If $\delta a\mathbb{Q}^{\times\,2} \in \operatorname{im}\alpha$, then there is a $P = (x, y) \in C(\mathbb{Z}_S)$ such that $\alpha(P) = \delta a\mathbb{Q}^{\times\,2}$, and by our construction above the point P comes from an integral point on $ar^2 - bs^2 = 2/\delta$. The converse is also true. □

The kernel of α is easy to compute:

Proposition 3.7. *We have* $\ker\alpha = 2C(\mathbb{Z}_S)$.

This implies that we have an exact sequence

$$0 \longrightarrow 2C(\mathbb{Z}_S) \longrightarrow C(\mathbb{Z}_S) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

Thus we have $C(\mathbb{Z}_S)/2C(\mathbb{Z}_S) \simeq \operatorname{im}\alpha$; in particular, $C(\mathbb{Z}_S)/2C(\mathbb{Z}_S)$ is finite since $\#\operatorname{im}\alpha \mid 2^{s+2}$. In fact, using the theory of heights (or by generalizing Shastri's proof) we can show that $C(\mathbb{Z}_S)$ is finitely generated, hence $C(\mathbb{Z}_S) \simeq C(\mathbb{Z}_S) \oplus \mathbb{Z}^r$ for some integer $r \geq 0$; since $C(\mathbb{Z}_S)$ is a subgroup of $\mathbb{Z}/4\mathbb{Z}$ and therefore cyclic, we have $C(\mathbb{Z}_S)/2C(\mathbb{Z}_S) \simeq (\mathbb{Z}/2\mathbb{Z})^{r+1}$.

Example 1.

Consider $C(\mathbb{Z})$ for $C : x^2 - 2y^2 = 1$. The associated curves are

$$\begin{aligned} r^2 - 2s^2 &= 1 && (r,s) = (1,0) \\ 2r^2 - s^2 &= 1 && (r,s) = (1,1) \\ -r^2 + 2s^2 &= 1 && (r,s) = (1,1) \\ -2r^2 + s^2 &= 1 && (r,s) = (1,0) \end{aligned}$$

Thus $C(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

Example 2.

Consider $C(\mathbb{Z})$ for $C : x^2 - 6y^2 = 1$. The associated curves are

$$\begin{aligned} r^2 - 6s^2 &= 1 && (r,s) = (1,0) \\ 2r^2 - 3s^2 &= 1 \\ 3r^2 - 2s^2 &= 1 && (r,s) = (1,1) \\ 6r^2 - s^2 &= 1 \\ -r^2 + 6s^2 &= 1 \\ -2r^2 + 3s^2 &= 1 && (r,s) = (1,1) \\ -3r^2 + 2s^2 &= 1 \\ -6r^2 + s^2 &= 1 && (r,s) = (0,1) \end{aligned}$$

Thus $C(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

Selmer and Tate-Shafarevich Group

The subset of curves $ar^2 - bs^2 = 2/\delta$ with a rational point corresponds to a subgroup $\mathrm{Sel}_2(C)$ of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ called the 2-Selmer group of C. The Tate-Shafarevich group $\mathbf{Ш}_2(C)$ is then defined by the exact sequence

$$1 \longrightarrow \operatorname{im}\alpha \longrightarrow \mathrm{Sel}_2(C) \longrightarrow \mathbf{Ш}_2(C) \longrightarrow 1.$$

In Example 2, the Selmer group is given by $\mathrm{Sel}_2(C) = \langle -2\mathbb{Q}^{\times 2}, 3\mathbb{Q}^{\times 2}\rangle$; since $\operatorname{im}\alpha = \mathrm{Sel}_2(C)$, we have $\mathbf{Ш}_2(C) = 0$. These calculations are valid in $\mathbb{Z}_S$ for all finite sets S.

Example 3.

Consider $C(\mathbb{Z})$ for $C : x^2 - 3y^2 = 1$. The associated curves are

$$\begin{aligned}
r^2 - 3s^2 &= 1 && (r,s) = (1,0)\\
3r^2 - s^2 &= 1\\
-r^2 + 3s^2 &= 1\\
-3r^2 + s^2 &= 1 && (r,s) = (0,1)\\
r^2 - 3s^2 &= 2\\
3r^2 - s^2 &= 2 && (r,s) = (1,1)\\
-r^2 + 3s^2 &= 2 && (r,s) = (1,1)\\
-3r^2 + s^2 &= 2
\end{aligned}$$

Thus $C(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

Example 3.

Consider $C(\mathbb{Z})$ for $C : x^2 - dy^2 = 1$; the necessary calculations for producing the table below are left as an exercise.

d	$C(\mathbb{Z})$	$\mathrm{Sel}_2(\mathbb{Z})$	$\mathbf{Ш}_2(\mathbb{Z})$
7	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2$	0
34	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$	$(\mathbb{Z}/2)^3$	$\mathbb{Z}/2\mathbb{Z}$
-1	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	0
-3	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	0
-5	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	0
-6	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	0
-17	$\mathbb{Z}/2\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$

Here are some details for $d = 34$: the associated curves are

$$\begin{aligned}
r^2 - 34s^2 &= 1 && (r,s) = (1,0)\\
2r^2 - 17s^2 &= 1 && (r,s) = (3,1)\\
17r^2 - 2s^2 &= 1 && (r,s) = (\tfrac{1}{3},\tfrac{2}{3})\\
34r^2 - s^2 &= 1 && (r,s) = (\tfrac{1}{3},\tfrac{5}{3})\\
-r^2 + 34s^2 &= 1 && (r,s) = (\tfrac{5}{3},\tfrac{1}{3})\\
-2r^2 + 17s^2 &= 1 && (r,s) = (\tfrac{2}{3},\tfrac{1}{3})\\
-17r^2 + 2s^2 &= 1 && (r,s) = (1,3)\\
-34r^2 + s^2 &= 1 && (r,s) = (0,1)
\end{aligned}$$

Consider $17r^2 - 2s^2 = 1$; since it has a rational point, it represents an element in the Selmer group $\mathrm{Sel}_2(C)$. We claim that it does not have a nontrivial integral

point. Assume it does; then $\gcd(r,s) = 1$, hence $(-2/17)_4(s/17) = +1$. Now $(-1/17)_4 = 1$; writing $s = 2^j t$ we find $(s/17) = (t/17) = (17/t) = +1$, hence the existence of an integral point implies $(2/17)_4 = 1$, which is not true.

Thus $\mathrm{Sel}(C) \simeq (\mathbb{Z}/2)^3$, $C(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$, and $\mathbf{Ш}_2(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$; moreover, $C(\mathbb{Z}_3) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2$ and $\mathbf{Ш}_2(\mathbb{Z}_3) = 1$.

Theorem 3.8. *For squarefree integers d, then the conic $C : x^2 - dy^2 = 1$ has Tate-Shafarevich group $\mathbf{Ш}_2(\mathbb{Z}) \simeq \mathrm{Cl}^+(k)^2/\mathrm{Cl}^+(k)^4$.*

Corollary 3.9. *For conics $C : x^2 - dy^2 = 1$, the Tate-Shafarevich group $\mathbf{Ш}_2(\mathbb{Z})$ can have arbitrarily large 2-rank as d varies.*

Corollary 3.10. *For conics $C : x^2 - dy^2 = 1$, the rank of $C(\mathbb{Z}_S)$ can become arbitrarily large as d and S vary.*

By defining $\mathbf{Ш}(\mathbb{Z})$ for $C : x^2 - dy^2 = 1$ using Galois cohomology it should be possible to show that $\mathbf{Ш}(\mathbb{Z}) \simeq \mathrm{Cl}^+(k)^2$ for $k = \mathbb{Q}(\sqrt{d}\,)$.

Lecture 4.
2-Descent (Proofs)

4.1 2-Isogenies

We have already explained that for computing the rank of an elliptic curve $E : y^2 = x(x^2 + ax + b)$ one has to study the torsors of E as well as those for $\widehat{\mathrm{E}} : y^2 = x(x^2 + \widehat{a}\,x + \widehat{b}\,)$ with $\widehat{a} = -2a$ and $\widehat{b} = a^2 - 4b$. Now we will explain where this curve comes from.

To this end let us look at the torsor

$$\mathcal{T}^{(\psi)}(1) : n^2 = m^4 + am^2 + b. \tag{4.15}$$

Multiplying through by 4 and rearranging terms, we find

$$a^2 - 4b = (2m^2 + a)^2 - 4n^2 = (2m^2 + a + 2n)(2m^2 + a - 2n).$$

Let us put $t = 2m^2 + a + 2n$; then $(t - a)^2 = t(t - 2a) + a^2$, and since $a^2 = t(t - 4n) + 4b$, this gives

$$(t - a)^2 - 4b = t(t - 2a + t - 4n) = 4m^2 t.$$

But now $(t - a)^2 - 4b = t^2 + \widehat{a}\,t + \widehat{b}\,$, where $\widehat{a} = -2a$ and $\widehat{b} = a^2 - 4b$. Thus $t(t^2 + \widehat{a}\,t + \widehat{b}\,) = 4m^2t^2$, in other words: the point $(\widehat{x}\,, \widehat{y}\,) = (t, 2mt)$ is a rational point on the curve

$$\widehat{\mathrm{E}} : \widehat{y}^{\,2} = \widehat{x}\,(\widehat{x}^{\,2} + \widehat{a}\;\widehat{x}\; + \widehat{b}\,). \tag{4.16}$$

Conversely, assume that $(\widehat{x}\,, \widehat{y}\,) \in \widehat{\mathrm{E}}(\mathbb{Q})$. If $\widehat{x} \neq 0$, then $m = \widehat{y}\,/2\widehat{x}$ gives us back m, and then $n = \frac{1}{2}(\widehat{x} - a) - m^2 = \frac{1}{4}(2\widehat{x} - \widehat{a}\,) - m^2$; this way we get a map $\widehat{\mathrm{E}}(\mathbb{Q}) \setminus \{\mathcal{O}, (0,0)\} \longrightarrow \mathcal{T}^{(\psi)}(\mathbb{Q})$ defined by $(\widehat{x}\,, \widehat{y}\,) \longmapsto (n, m)$.

As long as we only look at the affine parts of these curves, we don't get a bijection between rational points: in fact, if the point $(0, 0)$ on $\widehat{\mathrm{E}}$ is in the image of the map $\mathcal{T}^{(\psi)} \longrightarrow \widehat{\mathrm{E}}$, then it must come from a point with $t = 0$. But this implies $-n = m^2 + \frac{1}{2}a$, hence $n^2 = m^4 + am^2 + \frac{1}{4}a^2$, and so this point is on $\mathcal{T}^{(\psi)}$ if and only if $a^2 - 4b = 0$, that is, if and only if $\widehat{\mathrm{E}}$ is singular.

We have proved:

Proposition 4.1. *Assume that $a^2-4b\ne0$. Then the map $(n,m)\longmapsto(x,y)$ with $x=2m^2+2n+a$ and $y=2mx$ defines a bijection between the set of rational points on the affine curve (4.15) and $\widehat{\mathrm{E}}(\mathbb{Q})\setminus\{\mathcal{O},(0,0)\}$.*

Remark. A special case of this result is the fact that there is a bijection between rational points on $n^2=m^4+1$ (the Fermat equation for exponent 4) and rational points on $\widehat{\mathrm{E}}: y^2=x(x^2-4)$ different from $\mathcal{O}$ and $(0,0)$. Using Tate's method, the rank of $\widehat{\mathrm{E}}$ is easily computed to be 0, hence $\widehat{\mathrm{E}}(\mathbb{Q})=\widehat{\mathrm{E}}(\mathbb{Q})_{\mathrm{tors}}$, and a simple application of Nagell-Lutz reveals that $\widehat{\mathrm{E}}(\mathbb{Q})_{\mathrm{tors}}=\{\mathcal{O},(0,0),(-2,0),(2,0)\}$. By the proposition above, the only rational points on $n^2=m^4+1$ are $(n,m)=(\pm1,0)$, hence we have proved Fermat's Last Theorem for the exponent 4.

We also remark that Fermat's Last Theorem for the exponent 7 can be proved in a similar way (see [1]); for the exponent 3, on the other hand, we need to study 3-descents. The remaining exponents apparently cannot be treated directly by performing descents on elliptic curves, though some of them possibly may be treated by working on hyperelliptic curves or abelian varieties.

Now we compose the map $\widehat{\mathrm{E}}(\mathbb{Q})\setminus\{\mathcal{O},(0,0)\}\longrightarrow\mathcal{T}^{(\psi)}(1)$ with the map $\mathcal{T}^{(\psi)}(1)\longrightarrow E(\mathbb{Q})$ constructed in Lecture 1; this defines a map $\psi:\widehat{\mathrm{E}}(\mathbb{Q})\setminus\{\mathcal{O},(0,0)\}\longrightarrow E(\mathbb{Q})$. Let us compute where ψ sends a point $(\widehat{x}\,,\widehat{y}\,)\in\widehat{\mathrm{E}}(\mathbb{Q})\setminus\{\mathcal{O},(0,0)\}$; first it gets mapped to

$$(n,m)=\Big(\frac{2\widehat{x}\,+\widehat{a}}{4}-\frac{\widehat{y}^{\,2}}{4\widehat{x}^{\,2}},\frac{\widehat{y}}{2\widehat{x}}\Big)\in\mathcal{T}^{(\psi)}(1).$$

Now $(n,m)\longmapsto(m^2,nm)$ under the map $\mathcal{T}^{(\psi)}(1)\longrightarrow\mathrm{E}(\mathbb{Q})$, and since

$$\frac{2\widehat{x}\,+\widehat{a}}{4}-\frac{\widehat{y}^{\,2}}{4\widehat{x}^{\,2}}=\frac{2\widehat{x}^{\,3}+\widehat{a}\,\widehat{x}^{\,2}-\widehat{y}^{\,2}}{4\widehat{x}^{\,2}}=\frac{\widehat{x}^{\,3}-b\widehat{x}}{4\widehat{x}^{\,2}}$$

we find that $(\widehat{x}\,,\widehat{y}\,)\in\widehat{\mathrm{E}}(\mathbb{Q})\setminus\{\mathcal{O},(0,0)\}$ gets mapped to

$$\psi(\widehat{x}\,,\widehat{y}\,)=\Big(\frac{\widehat{y}^{\,2}}{4\widehat{x}^{\,2}},\frac{\widehat{y}\,(\widehat{x}^{\,2}-\widehat{b}\,)}{8\widehat{x}^{\,2}}\Big).\tag{4.17}$$

Proposition 4.2. *Formula* (4.17)*, together with $\psi(0,0)=\psi(\mathcal{O})=\mathcal{O}$, defines a homomorphism $\psi:\widehat{\mathrm{E}}(\mathbb{Q})\longrightarrow\mathrm{E}(\mathbb{Q})$ with kernel $\ker\psi=\{\mathcal{O},(0,0)\}$. Moreover, if $\alpha:\mathrm{E}(\mathbb{Q})\longrightarrow\mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ is the map defined by (1.7), then α is a group homomorphism with $\ker\alpha=\mathrm{im}\,\psi$. In other words: there is an exact sequence*

$$0\longrightarrow\{\overline{\mathcal{O}},(0,0)\}\longrightarrow\widehat{\mathrm{E}}(\mathbb{Q})\xrightarrow{\ \psi\ }\mathrm{E}(\mathbb{Q})\xrightarrow{\ \alpha\ }\mathbb{Q}^\times/\mathbb{Q}^{\times\,2}.$$

Proof. The proofs of the claims that the maps ϕ, ψ, α, β are group homomorphisms as well as the computation of their kernels are well known; see e.g. Silverman & Tate [6].

Here I'll present the proof that α is a homomorphism; we have to show that $\alpha(P_1+P_2)=\alpha(P_1)\alpha(P_2)$, and we distinguish several cases:

- $P_1 = \mathcal{O}$: then $\alpha(P_1 + P_2) = \alpha(P_2) = \alpha(P_1)\alpha(P_2)$.

- $P_1 + P_2 = \mathcal{O}$: then $\alpha(P_1 + P_2) = \mathbb{Q}^{\times 2}$; but since P_1 and P_2 have the same x-coordinate, we have $\alpha(P_1) = \alpha(P_2)$ and hence $\alpha(P_1)\alpha(P_2) = \mathbb{Q}^{\times 2}$.

- $P_1 = P_2$, but $P_1 \notin E(\mathbb{Q})[2]$: doubling points on curves on E : $y^2 = x(x^2 + ax + b)$ is done by applying the following formula:

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

  This implies that the x-coordinate of $2P_1$ is a square, hence $\alpha(2P_1) = \mathbb{Q}^{\times 2} = \alpha(P_1)\alpha(P_2)$.

- general case: assume that $P_1 + P_2 + P_3 = \mathcal{O}$ and $P_j = (x_j, y_j)$. The line through these three points has the form $y = mx + c$, and the x_j satisfy the equation $x(x^2 + ax + b) - (mx + c)^2 = 0$. Thus the left hand side equals $(x - x_1)(x - x_2)(x - x_3)$, and comparing constant terms yields $x_1x_2x_3 = c^2$. Therefore $\alpha(P_1)\alpha(P_2)\alpha(P_3) = \mathbb{Q}^{\times 2}$, i.e., $\alpha(P_1)\alpha(P_2) = \alpha(P_3) = \alpha(-P_3) = \alpha(P_1 + P_2)$.

This completes the proof. □

We can play the same game with the roles of E and $\widehat{\mathrm{E}}$ switched: rational points on $\widehat{\mathrm{E}}$ correspond to solutions of torsors

$$\mathcal{T}^{(\phi)}(b_1) : N^2 = \widehat{b}_1 M^4 + \widehat{a}\, M^2 e^2 + \widehat{b}_2 e^4 \tag{4.18}$$

with $\widehat{b}_1\widehat{b}_2 = \widehat{b}$, and we can define

$$W(\mathrm{E}/\mathbb{Q}) = \{\widehat{b}_1\mathbb{Q}^{\times 2} : \quad 0 \neq \widehat{b}_1 \in \mathbb{Z} \text{ squarefree}, \ \widehat{b}_1 \mid \widehat{b}, \\ \text{and } \mathcal{T}^{(\phi)}(\widehat{b}_1) \text{ has an integral solution}\}.$$

As for E, we can define a Weil map $\beta : \widehat{\mathrm{E}}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ by sending $\mathcal{O}$ to $1\mathbb{Q}^{\times 2}$, $\widehat{T} = (0, 0)$ to $\widehat{b}\,\mathbb{Q}^{\times 2}$, and $P = (x, y) \neq \widehat{T}$ to $x\mathbb{Q}^{\times 2}$, and the fact that $\widehat{\widehat{\mathrm{E}}}$ is isomorphic to E gives us a 'dual' exact sequence

$$0 \longrightarrow \{\mathcal{O}, (0, 0)\} \longrightarrow \mathrm{E}(\mathbb{Q}) \xrightarrow{\phi} \widehat{\mathrm{E}}(\mathbb{Q}) \xrightarrow{\beta} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

In fact, $\widehat{\widehat{\mathrm{E}}}$ is given by

$$\widehat{\widehat{\mathrm{E}}} : y^2 = x(x^2 + 4ax + 16b),$$

since $-2\widehat{a} = 4a$ and $\widehat{a}^{\,2} - 4\widehat{b} = 4a^2 - 4(a^2 - 4b) = 16b$. The change of coordinates $x \longmapsto 4x, y \longmapsto 8y$ shows that $\widehat{\widehat{\mathrm{E}}}$ is isomorphic to E.

4.2 The Snake Lemma

A sequence of abelian groups is a diagram

$$\xrightarrow{f} A \xrightarrow{g} B \xrightarrow{h} C \xrightarrow{i} \dots$$

where $A, B, C, \dots$ are abelian groups, and where $f, g, h, i, \dots$ are group homomorphism. Such a sequence is said to be exact at A if $\operatorname{im} f = \ker g$; similarly it is exact at B if $\operatorname{im} g = \ker i$ etc. The sequence is said to be exact if it is exact (except at the beginning and at the end).

Lemma 4.3. *If the sequence*

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow \dots \longrightarrow A_n \longrightarrow 0$$

of finite abelian groups is exact, then the alternating product of the group orders is trivial, i.e., $\#A_1 \cdot \#A_3 \cdots = \#A_2 \cdot \#A_4 \cdots$.

This is easily proved by induction using the observation that if

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow \dots$$

is an exact sequence of finite abelian groups, then so is

$$0 \longrightarrow B/A \longrightarrow C \longrightarrow \dots$$

Theorem 4.4 (Snake Lemma). *Assume that*

$$\begin{array}{ccccc} A & \xrightarrow[f]{} & B & \xrightarrow[g]{} & C \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' \end{array}$$

is a commutative diagram of abelian groups with exact rows. Then there exists a homomorphism $\delta : \ker\gamma \cap \operatorname{im} g \longrightarrow A'/(\operatorname{im}\alpha + \ker f')$ *such that the following sequence is exact:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & \ker f' \circ \alpha & \longrightarrow & \ker\beta & \longrightarrow & \ker\gamma \cap \operatorname{im} g \\ & & & & & & & & \downarrow{\scriptstyle\delta} \\ 0 & \longleftarrow & \operatorname{coker} g' & \longleftarrow & \operatorname{coker}\gamma \circ g & \longleftarrow & \operatorname{coker}\beta & \longleftarrow & A'/(\operatorname{im}\alpha + \ker f') \end{array}$$

If f' *is injective, then* $\ker f' \circ \alpha = \ker\alpha$ *and* $A'/(\operatorname{im}\alpha + \ker f') = \operatorname{coker}\alpha$*; if* g *is surjective, then* $\operatorname{coker}\gamma \circ g = \operatorname{coker}\gamma$ *and* $\ker\gamma \cap \operatorname{im} g = \ker\gamma$*. Thus if* f' *is injective and* g *is surjective, then we get the following exact sequence:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & \ker\alpha & \longrightarrow & \ker\beta & \longrightarrow & \ker\gamma \\ & & & & & & & & \downarrow{\scriptstyle\delta} \\ 0 & \longleftarrow & \operatorname{coker} g' & \longleftarrow & \operatorname{coker}\gamma & \longleftarrow & \operatorname{coker}\beta & \longleftarrow & \operatorname{coker}\alpha \end{array}$$

Corollary 4.5. *Assume that $\alpha : A \longrightarrow B$ and $\beta : B \longrightarrow C$ are homomorphisms of abelian groups. Then the sequence*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker\alpha & \longrightarrow & \ker(\beta\circ\alpha) & \longrightarrow & \ker\beta \\ & & & & & & \downarrow \\ 0 & \longleftarrow & \operatorname{coker}\beta & \longleftarrow & \operatorname{coker}(\beta\circ\alpha) & \longleftarrow & \operatorname{coker}\alpha \end{array}$$

is exact.

Proof. Apply the snake lemma to the diagram

$$\begin{array}{ccccccccc} & & A & \xrightarrow{\alpha} & B & \longrightarrow & \operatorname{coker}\alpha & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta\circ\alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow & & \\ 0 & \longrightarrow & C & \xrightarrow{\mathrm{id}} & C & \longrightarrow & 0 & & \end{array}$$

□

4.3 Tate's formula

Consider the sequence

$$\mathrm{E}(\mathbb{Q}) \xrightarrow{\phi} \widehat{\mathrm{E}}(\mathbb{Q}) \xrightarrow{\psi} \mathrm{E}(\mathbb{Q}).$$

Corollary 4.5 then gives us the exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker\phi & \longrightarrow & \ker(\psi\circ\phi) & \longrightarrow & \ker\psi \\ & & & & & & \downarrow \\ 0 & \longleftarrow & \operatorname{coker}\psi & \longleftarrow & \operatorname{coker}(\psi\circ\phi) & \longleftarrow & \operatorname{coker}\phi \end{array}$$

Now $\ker\phi = \{\mathcal{O}, T\}$, $\ker(\psi\circ\phi) = \mathrm{E}(\mathbb{Q})[2]$, $\ker\psi = \{\mathcal{O}, \widehat{T}\}$, $\operatorname{coker}\phi = \widehat{\mathrm{E}}/\operatorname{im}\phi \simeq \widehat{\mathrm{E}}/\ker\beta \simeq \operatorname{im}\beta$, $\operatorname{coker}(\psi\circ\phi) = \widehat{\mathrm{E}}(\mathbb{Q})/2\widehat{\mathrm{E}}(\mathbb{Q})$ and $\operatorname{coker}\psi \simeq \mathrm{E}/\ker\alpha \simeq \operatorname{im}\alpha$, so the above exact sequence becomes

$$\begin{array}{ccccccc} 0 & \longrightarrow & \{\mathcal{O}, T\} & \longrightarrow & \mathrm{E}(\mathbb{Q})[2] & \longrightarrow & \{\mathcal{O}, \widehat{T}\} \\ & & & & & & \downarrow \\ 0 & \longleftarrow & \operatorname{im}\alpha & \longleftarrow & \mathrm{E}(\mathbb{Q})/2\mathrm{E}(\mathbb{Q}) & \longleftarrow & \operatorname{im}\beta \end{array}$$

If we put $\#E(\mathbb{Q})[2] = 2^t$, and if we assume that $\mathrm{E}(\mathbb{Q})$ is finitely generated (the proof will be sketched in the next section), then the classification theorem for finitely generated abelian groups says that $\mathrm{E}(\mathbb{Q}) = \mathrm{E}(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$, where $r \in \mathbb{N}$ is called the (Mordell-Weil-) rank of $\mathrm{E}(\mathbb{Q})$. Thus $\#\mathrm{E}(\mathbb{Q})/2\mathrm{E}(\mathbb{Q}) = 2^{r+t}$, and we find $2 \cdot 2 \cdot 2^{r+t} = 2^t \cdot \#\operatorname{im}\alpha \cdot \#\operatorname{im}\beta$, that is,

$$2^r = \frac{\#\operatorname{im}\alpha \cdot \#\operatorname{im}\beta}{4}.$$

Exchanging the roles of E and $\widehat{\mathrm{E}}$ shows immediately that 2-isogenous curves have the same rank.

4.4 Heights

Let us now quickly sketch the theory of heights which is needed for the second part of the proof of the theorem of Mordell-Weil. Recall that the height $H(x)$ of rational numbers $x = \frac{m}{n}$ with $\gcd(m,n) = 1$ was defined as $H(x) = \max\{|m|, |n|\}$.

Our first task is to study how heights change when x is replaced by $f(x)$ for some polynomial $f \in \mathbb{Z}[X]$.

Lemma 4.6. *If $f(X) = a_nX^n + \ldots + a_1X + a0 \in \mathbb{Z}[X]$, then $H(f(x)) \le (n+1)mH(x)^n$ for all $x \in \mathbb{Q}$, where $m = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$.*

We shall give the proof to give you an idea of the techniques used here:

Proof. Write $x = \frac{p}{q}$ with $\gcd(p,q) = 1$; then $H(x) = \max\{|p|, |q|\}$, and in particular we have $|p| \le H(x)$ and $|q| \le H(x)$. Now

$$\begin{aligned} |q^n f(x)| &= |a_np^n + a_{n-1}p^{n-1}q + \ldots + a_1q^{n-1}p + a_0q^n| \\ &\le |a_n||p|^n + |a_{n-1}||p|^{n-1}|q| + \ldots + |a_1||p||q|^{n-1} + |a_0||q|^n \\ &\le (n+1)mH(x)^n, \end{aligned}$$

because $|a_k| \le m$ and $|p|^r|q|^{n-r} \le H(x)^rH(x)^{n-r} = H(x)^n$. □

Finding a lower bound of the same order of magnitude is much more difficult. Yet it can be done:

Lemma 4.7. *Let $f, g \in \mathbb{Z}[X]$ be coprime, and put $n = \max\{\deg f, \deg g\}$. Then there exist constants $C_1, C_2 > 0$ such that for all $x \in \mathbb{Q}$ we have*

$$C_1H(x)^n \le H\Big(\frac{f(x)}{g(x)}\Big) \le C_2H(x)^n.$$

The proof of this lemma is elementary but rather involved.

The height of a rational point $P \in E(\mathbb{Q})$ on an elliptic curve E is defined by

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

It is often convenient to use the logarithmic height $h(P) = \log H(P)$.

A first simple observation is the following:

Lemma 4.8. *Let* E *be an elliptic curve defined over $\mathbb{Q}$. Then for all $\kappa > 0$, the set $\{P \in \mathrm{E}(\mathbb{Q}) : H(P) < \kappa\}$ of rational points with bounded height is finite.*

The height on elliptic curves satisfies certain relations that will be needed in our proof of the Mordell-Weil theorem. We'll start with

Lemma 4.9. *Let* E *an elliptic curve defined over $\mathbb{Q}$. Then there exists some $C > 0$ such that $H(2P) \ge CH(P)^4$ for all $P \in \mathrm{E}(\mathbb{Q})$.*

The second estimate we need is

Lemma 4.10. *Let* E *be an elliptic curve defined over* $\mathbb{Q}$*, and let* $P_0 \in \mathrm{E}(\mathbb{Q})$*. Then there is a* $C_0 > 0$ *such that* $H(P + P_0) \le C_0 H(P)^2$ *for all* $P \in \mathrm{E}(\mathbb{Q})$*.*

Both of these lemmas are simple applications of Lemma 4.7. Now we can prove

Theorem 4.11 (Mordell's Theorem). *Let* E *be an elliptic curve defined over* $\mathbb{Q}$*. If* $\mathrm{E}(\mathbb{Q})/2\mathrm{E}(\mathbb{Q})$ *is finite, then* $\mathrm{E}(\mathbb{Q})$ *is finitely generated.*

Proof. The following proof is taken from the notes [7] of Bart de Smit. Note that we have proved that $\mathrm{E}(\mathbb{Q})/2\mathrm{E}(\mathbb{Q})$ is finite for elliptic curves $\mathrm{E} : y^2 = x(x^2 + ax + b)$.

Let S be a set of rational points P on E such that the P represent all cosets of $\mathrm{E}(\mathbb{Q})/2\mathrm{E}(\mathbb{Q})$. Since $\mathrm{E}(\mathbb{Q})/2\mathrm{E}(\mathbb{Q})$ is finite, we can choose S to be finite as well.

By Lemma 4.10, for each $P_j \in S$ there is a constant $c_j > 0$ such that $H(Q - P_j) \le c_j H(Q)^2$. Thus for $C = \max\{c_j : P_j \in S\}$ (here we use the fact that $\mathrm{E}(\mathbb{Q})/2\mathrm{E}(\mathbb{Q})$ is finite) we have $H(Q - P) \le C \cdot H(Q)^2$ for all $Q \in \mathrm{E}(\mathbb{Q})$ and all $P \in S$. Moreover, we have $H(2Q) \ge C_1^{-1} H(Q)^4$ for all $Q \in \mathrm{E}(\mathbb{Q})$.

Now let T denote the union of S and the (finitely many) rational points $R \in \mathrm{E}(\mathbb{Q})$ of height $H(R) < B := 4\sqrt{C_1 C}$. We claim that $\mathrm{E}(\mathbb{Q})$ is generated by the points in T.

We shall prove this by induction on the height. Clearly every $Q \in \mathrm{E}(\mathbb{Q})$ with $H(Q) < B$ is generated by a point in T since $Q \in T$.

Now assume that all rational points of height $< h$ are generated by points in T, and assume that $H(Q) < 2h$. There is a $P \in S$ such that $Q - P = 2R$, and we find

$$H(R)^4 \le C_1 \cdot H(Q - P) \le C_1 C \cdot H(Q)^2.$$

If $H(R) > H(Q)/2$, then $H(Q)^4/16 < H(R)^4 \le C_1 C \cdot H(Q)^2$, that is, $H(Q) < B$ and therefore $Q \in T$; if $H(R) \le H(Q)/2 = h$, then R is generated by points in T by induction assumption, hence so is $Q = P + 2R$. □

4.5 Selmer and Tate-Shafarevich Groups

For computing the rank of an elliptic curve $\mathrm{E} : y^2 = x(x^2 + ax + b)$ we have to decide whether certain torsors have rational points or not, that is, we have to compute $\#\mathrm{im}\,\alpha$ and $\#\mathrm{im}\,\beta$. This is a difficult problem. On the other hand, it is relatively easy to decide whether these torsors have local solutions everywhere, that is, whether they have solutions modulo all prime powers and in the reals. The classes $b_1 \mathbb{Q}^{\times 2}$ corresponding to such everywhere locally solvable torsors $\mathcal{T}^{(\psi)}(b_1)$ (these are the torsors that have solutions modulo every prime power as well as real solutions) form a group $\mathrm{Sel}^{(\psi)}(\widehat{\mathrm{E}}/\mathbb{Q})$ containing $W(\widehat{\mathrm{E}}/\mathbb{Q}) := \mathrm{im}\,\alpha$ as a subgroup. The following exact sequence then defines the ψ-part of the Tate-Shafarevich group of $\widehat{\mathrm{E}}$:

$$0 \longrightarrow W(\widehat{\mathrm{E}}/\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(\psi)}(\widehat{\mathrm{E}}/\mathbb{Q}) \longrightarrow \mathbf{Ш}(\widehat{\mathrm{E}}/\mathbb{Q})[\psi] \longrightarrow 0$$

Note that both $W(\widehat{\mathrm{E}}/\mathbb{Q})$ and $\mathrm{Sel}^{(\psi)}(\widehat{\mathrm{E}}/\mathbb{Q})$ are finite elementary-abelian 2-groups, hence so is their quotient $\mathbf{Ш}(\widehat{\mathrm{E}}/\mathbb{Q})[\psi]$. Using Galois cohomology one can define the full Tate-Shafarevich group $\mathbf{Ш}(\widehat{\mathrm{E}}/\mathbb{Q})$; the conjecture that this group is always finite is an important part of the Birch–Swinnerton-Dyer conjecture.

Of course there is a 'dual' sequence

$$0 \longrightarrow W(\mathrm{E}/\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(\phi)}(\mathrm{E}/\mathbb{Q}) \longrightarrow \mathbf{Ш}(\mathrm{E}/\mathbb{Q})[\phi] \longrightarrow 0;$$

note that although $\mathrm{E}(\mathbb{Q})$ and $\widehat{\mathrm{E}}(\mathbb{Q})$ have the same rank r, their torsion subgroups, Selmer groups, and Tate-Shafarevich groups are in general different.

Lecture 5.
Nontrivial Elements in Ш[2]

In this lecture we will present various techniques for constructing nontrivial elements in the Tate-Shafarevich group.

5.1 Pépin's Claims

The following is taken from [1].

It is well known that curves of genus 0 defined over $\mathbb{Q}$ satisfy the Hasse principle: they have a rational point if and only if they have a $\mathbb{Q}_p$-rational point for every completion $\mathbb{Q}_p$ of $\mathbb{Q}$. It is similarly well known that the Hasse principle fails to hold for curves of genus 1, the first counter example $2z^2 = x^4 - 17y^4$ being due to Lind [Li] and Reichardt [Re].

In a series of articles [P1, P2, P3, P4], Théophile Pépin announced 93 theorems asserting that certain equations of the type $aX^4 + bY^4 = Z^2$ were not solvable in integers (nontrivially, that is). In order to get nontrivial results, Pépin looks at equations whose underlying conics $ax^2 + by^2 = z^2$ do have rational solutions (see [P1]):

> Les cas où l'équation indéterminée $aX^4 + bY^4 = Z^2$ n'admet pas de solution rationnelle sont fort nombreux, même quand l'équation $ax^2 + by^2 = z^2$ est résoluble en nombres entiers. Néanmoins on ne connait encore qu'un petit nombre de théorèmes sur ce sujet.

He then starts listing his results without proof, and among his examples there are some that claim the nonexistence of rational points on some curves of genus 1 that are everywhere locally solvable. To the best of my knowledge no proofs for Pépin's claims have been supplied yet. The proofs that we give below are based on connections with the 2-class groups of complex quadratic number fields.

5.2 Applications of Genus Theory

Let us start with the following assertion taken from [P2]:

Proposition 5.1. *Let p be a prime of the form $p = 5m^2+4mn+9n^2$; then the equation $px^4 - 41y^4 = z^2$ does not have rational solutions.*

Proof. First observe that we may assume that x, y, z are integers; moreover, if q is a prime dividing x and y then $q^2 \mid z$ since $41p$ is squarefree, hence we may assume that x and y are coprime. Since any common prime divisor of x and z divides y, we also see that $(x, z) = 1$, and similarly $(y, z) = 1$.

Now write the equation in the form $px^4 = N(z+y^2\sqrt{-41}\,)$, where N denotes the norm from the quadratic field $k = \mathbb{Q}(\sqrt{-41}\,)$. It is easily seen that x is always odd and that either y or z is even. In particular, the ideals $(z + y^2\sqrt{-41}\,)$ and $(z - y^2\sqrt{-41}\,)$ are coprime. This implies that $(z + y^2\sqrt{-41}\,) = \mathfrak{p}\mathfrak{a}^4$, where $\mathfrak{p}$ denotes a prime ideal above p in k (note that p splits since $5p = (5m+2n)^2+41n^2$ is a norm): in particular, the ideal class of $\mathfrak{p}$ is a 4th power.

On the other hand we have $p = 5m^2 + 4mn + 9n^2$. This implies $5p = (5m + 2n)^2 + 41n^2$, hence $\mathfrak{p}$ is in the same ideal class as one of the primes above 5. Now a simple computation shows that each prime $\mathfrak{q}$ above 5 generates an ideal class of order 4 (note that $5^4 = 16^2 + 3^2 \cdot 41$); since $\mathrm{Cl}\,(k)$ is cyclic of order 8, the class $[\mathfrak{q}]$ is not a fourth power: contradiction. □

Proposition 5.2. *Let p be a prime of the form $p = 9a^2+4b^2$; then the equation $px^4 - 36y^4 = z^2$ does not have rational solutions.*

Proof. As above, $px^4 = N(z + 6y^2i)$ implies that the class of the prime ideal $\mathfrak{p}$ above p in $k = \mathbb{Q}(i)$ is a fourth power in the ray class group $\mathrm{Cl}_k\{6\}$ modulo 6 of k. On the other hand, $p = 9a^2 + 4b^2$ implies that $[\mathfrak{p}]$ has order 2 in $\mathrm{Cl}_k\{6\} \simeq \mathbb{Z}/4\mathbb{Z}$, and this is a contradiction. □

Theorem 5.3. *Assume that $p = \alpha^2a^2 + 2\beta ab + \gamma b^2$ is a prime, and put $m = \alpha^2\gamma - \beta^2$. Then the conic $px^2 - my^2 = z^2$ has the rational point $(x, y, z) = (\alpha, b, \alpha^2a + \beta b)$, hence infinitely many.*

If, in addition, $m \equiv 1 \bmod 8$ and $\alpha \equiv 3 \bmod 4$ are prime, then the equation $px^4 - my^4 = z^2$ does not have nontrivial rational solutions.

Proof. If a conic defined over $\mathbb{Q}$ has a rational point P, then any line through P with a rational slope t will intersect the conic in another rational point, thus producing a rational parametrization of the conic.

Assume that $px^4 - my^4 = z^2$ is solvable, and that x, y and z are pairwise coprime integers. Since $(-m/p) = (-m/\alpha) = 1$, we find that $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$ and $\alpha\mathcal{O}_k = \mathfrak{a}\mathfrak{a}'$ split in $k = \mathbb{Q}(\sqrt{-m}\,)$. Now $px^4 = N(z + y^2\sqrt{-m}\,)$, and since x must be odd we deduce that $(z + y^2\sqrt{-m}\,) = \mathfrak{p}\mathfrak{b}^4$ for some ideal $\mathfrak{b}$. This shows that the ideal class of $\mathfrak{p}$ is a fourth power.

On the other hand, $p = \alpha^2a^2 + 2\beta ab + \gamma b^2$ gives $p\alpha^2 = (\alpha^2a + \beta b)^2 + mb^2$, hence $\mathfrak{p} \sim \mathfrak{a}^2$. Since $m \equiv 1 \bmod 4$, one of the genus characters of $k/\mathbb{Q}$ is the nontrivial character modulo 4. Now genus theory implies that the ideal classes of prime ideals above primes $\equiv 3 \bmod 4$ are not squares: since α is such a prime, $[\mathfrak{a}]$ is not a square, and we have a contradiction since the 2-class group of k is cyclic of order divisible by 4. □

5.3 Using 2-descent

In this section we will study the elliptic curve $E : y^2 = x(x^2 - 4pq^2)$ using a 2-descent, where $p \equiv 1 \bmod 8$ and $q \equiv 3 \bmod 4$ are primes such that $(p/q) = +1$ (for $q = 3$, this is the curve occurring in Proposition 5.2). The curve E is 2-isogenous to $\widehat{\mathrm{E}} : y^2 = x(x^2 + pq^2)$, and it is easy to see that $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) = \langle p\mathbb{Q}^{\times 2}\rangle = W(E/\mathbb{Q})$. A simple calculation reveals that

$$\mathrm{Sel}^{(\psi)}(\widehat{\mathrm{E}}/\mathbb{Q}) = \langle -\mathbb{Q}^{\times 2}, 2\mathbb{Q}^{\times 2}, p\mathbb{Q}^{\times 2}, q\mathbb{Q}^{\times 2}\rangle,$$

and that $W(\widehat{\mathrm{E}}/\mathbb{Q}) \supseteq \langle -p\mathbb{Q}^{\times 2}\rangle$.

Next we consider some torsors in detail; since $-p\mathbb{Q}^{\times 2} \in W(\widehat{\mathrm{E}}/\mathbb{Q})$, it is sufficient to look at $\mathcal{T}^{(\psi)}(b_1)$ for $b_1 \in \{p, \pm 2, \pm q, \pm 2q\}$.

The following (partial) result can be proved by elementary number theory alone:

Proposition 5.4. *If the torsor $\mathcal{T}^{(\psi)}(b_1)$ has a nontrivial rational point, then the conditions in the following table are satisfied:*

b_1	$-pb_1$	condition
2	$-2p$	$(2/p)_4 = +1$
-2	$2p$	$(2/p)_4 = +1$
q	$-pq$	$(q/p)_4 = +1$
$-q$	pq	$(q/p)_4 = +1$
$2q$	$-2pq$	$(2q/p)_4 = +1$
$-2q$	$2pq$	$(2q/p)_4 = +1$

The proof proceeds case by case:

- $b_1 = q$. Here we find $N = qn$ and $qn^2 = M^4 - 4pe^4$; this implies $2 \mid M$, hence $qn^2 = 4m^4 - pe^4$, which gives $(q/p)_4 = (2n/p) = (n/p) = (p/n) = +1$.

- $b_1 = -q$. Now $-qN^2 = M^4 - 4pe^4$; here M is odd, hence $(-q/p)_4 = (N/p) = (p/N) = +1$. Note that $(-1/p)_4 = 1$ since $p \equiv 1 \bmod 8$.

- $b_1 = 2pq$. Here we get $2qn^2 = pM^4 - e^4$; hence $(2q/p)_4 = (n/p) = (n'/p) = (p/n') = 1$, where $n = 2^j n'$ for some odd integer n'.

- $b_1 = -2pq$. Here $-2qn^2 = pM^4 - e^4$, and as above we find $(2q/p)_4 = 1$.

- $b_1 = 2$. Here we start with $N^2 = 2M^4 - 2pq^2e^4$. Put $N = 2n$; then $2n^2 = M^4 - pq^2e^4$ gives $(2/p)_4 = (qn/p)$. But $(q/p) = 1$ and $(n/p) = (n'/p) = (p/n') = 1$, hence $(2/p)_4 = 1$.

- $b_1 = -2$. Then $N^2 = -2M^4 + 2pq^2e^4$. Then $N = 2qn$, thus $-2n^2 = M^4 - pq^2e^4$. This implies $(2/p)_4 = 1$ as usual, and the other case is treated similarly.

A similar consideration of $\mathcal{T}^{(\psi)}(p)$ produces nothing, although we know by Pépin's result in the special case $q = 3$, plus the fact that $p = 9a^2 + 4b^2$ is equivalent to $(-3/p)_4 = -1$, that solvability implies $(3/p)_4 = 1$. So we better have a second look at our torsor $\mathcal{T}^{(\psi)}(p)$.

Here $N^2 = pM^4 - 4q^2e^4$, where MN is odd and e is even; we also know that $q \nmid M$ since otherwise reduction modulo q would imply that $(-1/q) = +1$. Then $pM^4 = N^2 + 4q^2e^4 = (N + 2qe^2i)(N - 2qe^2i)$ and thus $N + 2qe^2i = \pi\mu^4$, where $\pi \in \mathbb{Z}[i]$ is a prime $\equiv 1 \bmod 2$ and $\mu\overline{\mu} = M$. Subtracting its conjugate from this equation gives $4qe^2i = \pi\mu^4 - \overline{\pi}\,\overline{\mu}^4$, and reducing modulo $\overline{\pi}$ shows that $(q/p)_4(-1/p)_8(e/p) = [\pi/\overline{\pi}]_4$. Now $[\pi/\overline{\pi}]_4 = (-4/p)_8$ (see Lemma 5.7 below) and $(e/p) = (e'/p) = (p/e') = 1$ (where $e = 2^je'$ for some odd e') implies that $(q/p)_4(-1/p)_8 = (-4/p)_8$, hence $(2q/p)_4 = +1$.

Now we have found a necessary condition but it isn't the one we were expecting. So let's have another try and factor the torsor over $k = \mathbb{Q}(\sqrt{p}\,)$:

$$-q^2e^4 = \Big(\frac{N + M^2\sqrt{p}}{2}\Big)\Big(\frac{N - M^2\sqrt{p}}{2}\Big).$$

Assume for the moment that k has class number 1. Then we get $N + M^2\sqrt{p} = 2\varepsilon\lambda^2\alpha^4$, where ε is some unit in $\mathcal{O}_k$ and $N\lambda = q$. Taking the norm of both sides shows that $N\varepsilon = -1$, so up to squares (which we may subsume into λ) we have $\varepsilon = \pm\varepsilon_p$, where $\varepsilon_p > 1$ is the fundamental unit of k. We see that $N + M^2\sqrt{p} > 0$ under the embedding that takes $\sqrt{p}$ to the positive real square root of p, so we must have $N + M^2\sqrt{p} = 2\varepsilon_p\lambda^2\alpha^4$. Subtracting this equation from its conjugate yields $M^2\sqrt{p} = \varepsilon_p\lambda^2\alpha^4 + \overline{\varepsilon}_p\overline{\lambda}^2\overline{\alpha}^4$, and now reduction modulo $\overline{\lambda}$ gives $[\varepsilon_p\sqrt{p}/\overline{\lambda}] = 1$. But Kummer theory and a few arguments about ramification show that $\mathbb{Q}(\sqrt{\varepsilon_p\sqrt{p}}\,)$ is the quartic subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$, hence $[\varepsilon_p\sqrt{p}/\overline{\lambda}] = (q/p)_4$, which is exactly what we wanted.

For the general case, we need a lemma:

Lemma 5.5. *Let p and q be odd primes and $h \ge 1$ an odd integer such that $r^2 - ps^2 = q^h$ with $2r, 2s \in \mathbb{Z} \setminus q\mathbb{Z}$. Then $(r + s\sqrt{p}\,)^h - (r - s\sqrt{p}\,)^h = 2S\sqrt{p}$, and $(S/q) = (s/q)$.*

Proof. We have $S = \binom{h}{1}r^{h-1}s + \binom{h}{3}r^{h-3}s^3p + \ldots + \binom{h}{h}s^hp(h-1)/2$. Since $r^2 \equiv ps^2 \bmod q$, this implies that $S \equiv s^hp^{(h-1)/2}[\binom{h}{1} + \binom{h}{3} + \ldots + \binom{h}{h}] = 2^{h-1}s^hp^{(h-1)/2} \bmod q$. Since h is odd and $(p/q) = +1$, this implies $(S/q) = (s/q)$. □

Now let h be the class number of $k = \mathbb{Q}(\sqrt{p}\,)$; since the discriminant of k is a prime, h is odd by genus theory. The factorization above implies $(N+M^2\sqrt{p}\,) = 2\mathfrak{q}^2\mathfrak{a}^4$ for ideals $\mathfrak{q}$ and $\mathfrak{a}$ of norm q and e, respectively. Writing $\mathfrak{q}^h = (\lambda)$ and $\mathfrak{a}^h = (\alpha)$ we get

$$(N + M^2\sqrt{p}\,)^h = 2^h\varepsilon_p\lambda^2\alpha^4$$

with $\varepsilon_p > 1$ as above. Again we form the difference between this equation and its conjugate and then reduce modulo $\overline{\lambda}$. With the help of Lemma 5.5 we now

see that $[\sqrt{p}/\overline{\lambda}] = [\varepsilon_p/\overline{\lambda}]$, and this proves as above that $(q/p)_4 = 1$ is necessary for $\mathcal{T}^{(\psi)}(p)$ to be solvable.

We summarize our discussion in the following

Theorem 5.6. *Consider the elliptic curve $E : y^2 = x(x^2 - 4pq^2)$, where $p \equiv 1 \bmod 8$ and $q \equiv 3 \bmod 4$ are primes such that $(p/q) = +1$. If the torsor $\mathcal{T}^{(\psi)}(p) : N^2 = pM^4 - 4q^2e^4$ has a rational solution, then $(2/p)_4 = (q/p)_4 = +1$. Moreover, we always have $\mathbf{Ш}(E/\mathbb{Q})[2] = 0$, and $\mathbf{Ш}(\widehat{\mathrm{E}}/\mathbb{Q})[2]$ has order divisible by 4 unless possibly when $(2/p)_4 = (q/p)_4 = +1$.*

Our results aren't as complete as we might want them: if $(2/p)_4 = 1$ and $(q/p)_4 = -1$, for example, then we know that the torsors $\mathcal{T}^{(\psi)}(b_1)$ are not solvable for $b_1 \in \{-1, q, -q\}$, and we also know that one of $\mathcal{T}^{(\psi)}(2)$ and $\mathcal{T}^{(\psi)}(-2)$ is not solvable (assuming the finiteness of $\mathbf{Ш}(\widehat{\mathrm{E}}/\mathbb{Q})$ we can even predict that exactly one of them is solvable), but we can not tell which. It would be interesting to find criteria that allow us to do this.

We still have to provide a proof for

Lemma 5.7. *Let $\pi = a + bi$ be a prime in $\mathbb{Z}[i]$ with norm $p \equiv 1 \bmod 8$, and assume that $4 \mid b$ and $a \equiv 1 \bmod 4$. Then $[\pi/\overline{\pi}]_4 = (-4/p)_8$.*

Proof. Since $\pi = a + bi \equiv 2bi \bmod \overline{\pi}$, we find $[\pi/\overline{\pi}]_4 = [2i\overline{\pi}]_4[b/\overline{\pi}]_4$. Now $[2i/\overline{\pi}]_4 = (-4/p)_8$ since $-4 = (2i)^2$, hence it is sufficient to prove that $[b/\overline{\pi}]_4 = 1$.

Assume first that $b \equiv 4 \bmod 8$; then $b = 4b'$ for some odd b', and using $[-1/\overline{\pi}]_4 = +1$ we find $[b/\overline{\pi}]_4 = (2/p)[b'/\overline{\pi}]_4 = [b'/\overline{\pi}]_4 = [\overline{\pi}/b']_4 = [a/b']_4$. But quartic residue symbols whose entries are rational integers are trivial and our claim follows. If $8 \mid b$, then $[2/\overline{\pi}]_4 = (2/p)_4 = +1$, hence writing $b = 2^j b'$ for some odd b' gives $[b/\overline{\pi}]_4 = [b'/\overline{\pi}]_4 = [\overline{\pi}/b']_4 = [a/b']_4 = +1$. □

References

[Li] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Diss. Univ. Uppsala 1940

[P1] Th. Pépin, *Théorèmes d'analyse indéterminée*, C. R. Acad. Sci. Paris **78** (1874), 144–148

[P2] Th. Pépin, *Théorèmes d'analyse indéterminée*, C. R. Acad. Sci. Paris **88** (1879), 1255–1257

[P3] Th. Pépin, *Nouveaux théorèmes sur l'équation indéterminée $ax^4 + by^4 = z^2$*, C. R. Acad. Sci. Paris **91** (1880), 100–101

[P4] Th. Pépin, *Nouveaux théorèmes sur l'équation indéterminée $ax^4 + by^4 = z^2$*, C. R. Acad. Sci. Paris **94** (1882), 122–124

[Re] H. Reichardt, *Einige im Kleinen überall lösbare, im Großen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18

Bibliography

[1] F. Lemmermeyer, *A note on Pépin's counter examples to the Hasse principle for curves of genus* 1, Abh. Math. Sem. Hamburg **69** (1999), 335–345 30, 37

[2] F. Lemmermeyer, *On Tate-Shafarevich groups of some elliptic curves*, Proc. Conf. Graz 1998, (2000), 277–291

[3] F. Lemmermeyer, *Some families of non-congruent numbers*, Acta Arith., to appear

[4] P. Shastri, *Integral points on the unit circle*, J. Number Theory **91** (2001), 67–70 23

[5] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag 14

[6] J. Silverman, J. Tate, *Rational points on elliptic curves*, Springer-Verlag 30

[7] B. de Smit, *Handouts*, Seminar Leiden 2001, at `http://www.math.leidenuniv.nl/~desmit/ell/` 35

[8] Lin Tan, *The group of rational points on the unit circle*, Math. Mag. **69** (1996), no. 3, 163–171 23

[9] M.Z. Zhang, *Factoring integers with conics* (Chinese. English summary), Sichuan Duxue Xuebao **33** (1996), 356–359 22