LECTURE 2

FRANZ LEMMERMEYER

Last time we have seen that the proof of Fermat's Last Theorem for the exponent 4 provides us with two elliptic curves ($y^2 = x^3 + x$ and $y^2 = x^3 - 4x$) in the guise of the quartic equations ($X^4 + Y^4 = Z^2$ and $X^4 - 4Y^4 = Z^2$). Moreover, in the actual proof we used connections between these quartic curves and the 'underlying conic', namely the quadratic curves $x^2 + y^2 = z^2$ and $x^2 - 4y^2 = z^2$, which actually both represent the unit circle after a little change of coordinates.

What we will do today is sketch the basic theory of elliptic curves, and at the same time compare it with the much simpler theory of conics.

1. The Objects

In modern arithmetic geometry, curves of the form $Y^2 = f(X)$ for some polynomial f without multiple roots play an important role. We distingish the following cases:

degree	genus	curve
$1 \le \deg f \le 2$	0	conics
$3 \le \deg f \le 4$	1	elliptic curves
$\deg f \ge 5$	≥ 2	hyperelliptic curves

Let us assume here and below that the coefficients of f are integers. The main problem of diophantine analysis is to describe the rational and integral points on these curves. The following table summarizes our current knowledge:

genus	rational points	integral points
0	$\varnothing$ or infinite	finite or infinite
1	finite or infinite	finite
≥ 2	finite	finite

The claims for curves of genus 0 are easy to prove. The fact that elliptic curves have only finitely many integral points is a deep theorem of Siegel; the same result for hyperelliptic curves is of course a corollary of the fact that these do only have finitely many *rational* points, which was conjectured by Mordell and proved by Faltings in the 1980s using advanced algebraic geometry.

2. Group Laws

2.1. **Conics.** Nonsingular conics $\mathcal{C}$ can be given a group structure as follows: pick any point N on $\mathcal{C}$; the sum of the points P and Q is the second point of intersection of the parallel to PQ through N. Associativity follows from Pascal's Theorem, the other group axioms are clear. If $\mathcal{C}$ is defined over $\mathbb{Z}$ ($\mathbb{Q}$, $\mathbb{F}_p$, ...), and if $N \in \mathcal{C}(\mathbb{Z})$ ($\mathcal{C}(\mathbb{Q})$, $\mathcal{C}(\mathbb{F}_p)$, ...), then this construction induces a group law on the set $\mathcal{C}(\mathbb{Z})$ of integral points on a conic (resp. on $\mathcal{C}(\mathbb{Q})$, $\mathcal{C}(\mathbb{F}_p)$, ...).

Conics if the special form $\mathcal{C} : Y^2 = \Delta X^2 + 4$ are called Pell conics. Identifying the point $(y, x) \in \mathcal{C}(\mathbb{Q})$ on a Pell conic with the element $\frac{y+x\sqrt{\Delta}}{2}$ of norm 1 in the quadratic number field $K = \mathbb{Q}(\sqrt{\Delta})$ with discriminant Δ, we find that $\mathcal{C}(\mathbb{Q})$ is isomorphic to the unit group of the quadratic field K. The group structure on $\mathcal{C}(\mathbb{Q})$ induced by this identification agrees with the structure defined above using geometry.

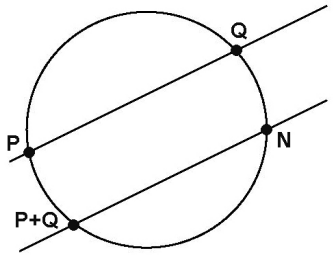

FIGURE 1. Group Law on the Unit Circle

2.2. **Cubics.** The Weierstrass equation $Y^2 = X^3 + aX^2 + bX + c$ (with $a, b, c \in \mathbb{Q}$) describes an elliptic curve E defined over $\mathbb{Q}$ if its discriminant Δ is nonzero, that is, if the polynomial on the right hand side does not have repeated roots. The set $E(\mathbb{Q})$ of rational points (i.e. points with rational coordinates) on E, together with some 'point at infinity' $\mathcal{O}$, forms an abelian group: three points $P, Q, R \in E(\mathbb{Q})$ satisfy $P + Q + R = \mathcal{O}$ if and only if they are collinear. The neutral element is the point $\mathcal{O}$ at infinity, the inverse of P is its reflection at the x-axis.

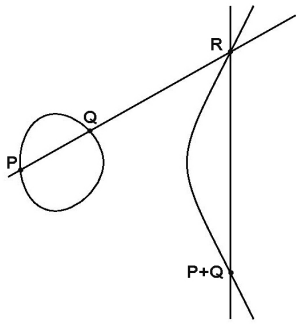

FIGURE 2. Group Law on Elliptic Curves

2.3. **Quartics.** Consider a quartic $Y^2 = f(X)$, where f is a polynomial of degree 4. If this curve has a rational point $P_+ = (x_0, y_0)$, then there is birational map transforming the quartic into an elliptic curve in Weierstrass form and sending $P_- = (x_0, -y_0)$. The birational map can be used to add points on the quartic, but it is often simpler to use the following construction explained by Elkies: take P_- as the neutral element of the group law, and put $Q = P_+ + P_-$. If a parabola $Y = aX^2 + bX + c$ meets the quartic in four points P_1, P_2, P_3, P_4, then the points corresponding to these P_* on the Weierstrass elliptic curve satisfy the relation $P_1 + P_2 + P_3 + P_4 = 2Q$ there.

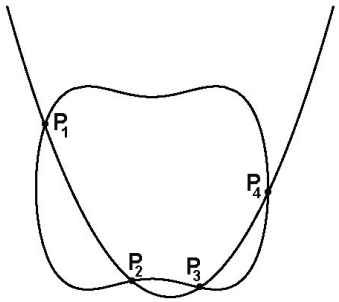

FIGURE 3. Group Law on Quartics

3. The analytic theory

Everybody knows that the unit circle can be parametrized using the trigonometric functions. The analog of these in the elliptic world are elliptic functions.

Conics. Define the series

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} \mp \ldots = \frac{e^{ix} + e^{-ix}}{2},$$
$$\sin z = x - \frac{x^3}{3!} + \frac{x^5}{5!} \mp \ldots = \frac{e^{ix} - e^{-ix}}{2i}.$$

It is easily checked that these series converge for all $x \in \mathbb{R}$ (actually in the whole complex plane) and that they represent analytic functions with 'period lattice' $\Lambda = 2\pi\mathbb{Z}$, hence actually are smooth functions on $\mathbb{R}/\Lambda$. Moreover, $\sin x$ and its derivative $\cos x$ parametrize the unit circle $C : X^2 + Y^2 = 1$ via

$$X = \cos x, \quad Y = \sin x.$$

Note that the map $\mathbb{R}/2\pi\mathbb{Z} \longrightarrow C$ is bijective; as a matter of fact, it is also an isomorphism of abelian groups: the factor group on the left hand side inherits its group structure from $\mathbb{R}$, the unit circle has a group law as defined above.

The analogy with the elliptic is more visible if we use the cotangent; it is defined as

$$\cot x = \sum_{k \in \mathbb{Z}} \frac{1}{x - k\pi}.$$

Actually this is not really a definition since the series does not converge absolutely; by fixing a summation order we can get rid of this problem and write

$$\cot x = \frac{1}{x} + \sum_{k=1}^{\infty} \Big(\frac{1}{x-k\pi} + \frac{1}{x+k\pi} \Big) = \frac{1}{x} + \sum_{k=1}^{\infty} \frac{2x}{x^2 - k^2\pi^2}.$$

Now $p(x) = \cot x$ and its derivative $p'(x) = -\frac{1}{\sin^2 x}$ satisfy the differential equation $-p' = p^2 + 1$; multiplying this through by $\sin^2 x$ we get the parametrization $1 = \cos^2 x + \sin^2 x$ of the unit circle.

Cubics. Let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ be a lattice in $\mathbb{C}$ (this means that $\omega_1, \omega_2 \in \mathbb{C}$ are linearly independent over $\mathbb{R}$). Define

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

This converges absolutely and uniformly on any compact subset of $\mathbb{C} \setminus \Lambda$ to a meromorphic function (the Weierstrass $\wp$-function) whose only poles are poles of order 2 at $w \in \Lambda$. Moreover, $\wp(z+w) = \wp(z)$ for any $w \in \Lambda$, so Λ is the period lattice of $\wp$.

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

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

where

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

Thus the Weierstrass elliptic function and its derivative parametrize elliptic curves $E : y^2 = 4x^3 - g_2x - g_3$ (in fact it can be shown that for any given values $g_2, g_3 \in \mathbb{C}$ with $\Delta = g_2^3 - 27g_3^2 \neq 0$ there is a corresponding lattice Λ). The map $\mathbb{C} \longrightarrow E$ defined by $z \longmapsto (\wp(z), \wp'(z))$ (with elements in Λ going to the point at infinity on E) is a group homomorphism with kernel Λ, hence $\mathbb{C}/\Lambda \simeq E$.

This interpretation of elliptic curves is important because it generalizes to complex abelian varieties: consider a lattice Λ in $\mathbb{C}^n$; then the quotient space $\mathbb{C}^n\Lambda$ is called a torus, and if this torus can be embedded into some projective space, it is called an abelian variety.

Quartics. Elliptic functions associated to quartics are much older than the Weierstrass function: they were studied by Fagnano, Legendre, Gauss, Abel, Jacobi and Eisenstein, to name a few. They came into being as the inverse functions of integrals of the form

$$z = \int_0^w \frac{dt}{\sqrt{(1-t^2)(1-k^2x^2)}}$$

and are called Jacobi elliptic functions. Almost all the literature on elliptic functions before the 20th century is written in the language of Jacobi elliptic functions; everyhting can be translated into the Weierstrass language: every elliptic function with period lattice Λ is a rational function of $\wp$ and $\wp'$.

4. Solvability modulo p

When solving diophantine equations in integers, it is in general a good idea to look first at solutions in finite fields $\mathbb{F}_p$, lift these (if possible) to solutions in the rings $\mathbb{Z}_p$ of p-adic integers, and then see what this implies for rational or integral solutions.

In this section, we will discuss what is known about the $\mathbb{F}_p$-rational points on conics, cubics, and quartics.

There are three questions of increasing difficulty:

(1) Is there an $\mathbb{F}_p$-rational point at all?
(2) Is there a good bound for the number of $\mathbb{F}_p$-rational points?
(3) Is there an explicit formula for the number of $\mathbb{F}_p$-rational points?

In case the $\mathbb{F}_p$-rational points form a group (i.e. for Pell conics and elliptic curves) we may even ask whether the group structure can be given explicitly.

4.1. **Conics.** The question about the existence of $\mathbb{F}_p$-rational points on conics

$$Y^2 = aX^2 + bX + c \tag{1}$$

is easily answered:

Proposition 1. *Let (1) be a conic defined over $\mathbb{F}_p$, where p is an odd prime, and assume that $a \neq 0$. Then $\mathcal{C}(\mathbb{F}_p) \neq \varnothing$.*

Proof. Assume not; then the values of the polynomial $f(X) = aX^2 + bX + c$ are nonsquares for every $x \in \mathbb{F}_p$. Thus, by Euler's criterion, $f(X) = (aX^2 + bX + c)^{(p-1)/2} + 1 \in \mathbb{F}_p[X]$ is a polynomial of degree $p-1$ (here we use that $a \neq 0$) with $f(x) = 0$ for all $x \in \mathbb{F}_p$: this is a contradiction because polynomials f over fields have at most $\deg f$ roots.

The argument above goes back to Lagrange; a different proof starts with the observation that the polynomial $f(X) = aX^2 + bX + c$ attains exactly $\frac{p+1}{2}$ different values (by completing the square the claim can be reduced to counting values of $f(X) = X^2$). Since there are only $\frac{p-1}{2}$ nonsquares in $\mathbb{F}_p$, the claim follows. □

Since conics are curves of genus 0 and therefore rational, knowing one $\mathbb{F}_p$-rational point means that we know them all: a standard parametrization gives us

Proposition 2. *The number of $\mathbb{F}_p$-rational points on conics (1) is*

$$\#\mathcal{C}(\mathbb{F}_p) = p - \left(\tfrac{a}{p}\right),$$

where $p \nmid \Delta = b^2 - 4ac$ is prime.

We also can give the explicit structure of these groups:

Proposition 3. *The group of $\mathbb{F}_p$-rational points on a nonsingular conic (1) defined over $\mathbb{F}_p$ is cyclic of order $p - \left(\frac{a}{p}\right)$.*

4.2. **Cubics.** Here we consider cubic curves in Weierstrass form $Y^2 = X^3 + aX + b$. Proving the existence of an $\mathbb{F}_p$-rational point in the affine plane is not too hard.

Von Sterneck (1908) proved that cubic polynomials $f(X) = X^3 + aX + b$ attain $\frac{2p \pm 1}{3}$ values modulo primes $p \nmid 6a$. Since $\frac{2p\pm1}{3} > \frac{p-1}{2}$, the polynomial attains at least $\frac{p\pm1}{6}$ square values.

With a slightly more elaborate approach, Postnikov (1966) gave a very simple proof of

Proposition 4. *The number N of $\mathbb{F}_p$-rational points (including the point $\mathcal{O}$ at infinity) on a Weierstrass elliptic curve satisfies $|N-(p+1)| \le \frac{p+3}{2}$.*

This takes care of the existence of $\mathbb{F}_p$-rational points as well as of a bound for the number of $\mathbb{F}_p$-rational points. Already in the 1930s, a much sharper bound had been given by Hasse:

Theorem 5. *The number N of $\mathbb{F}_p$-rational points on an elliptic curve $Y^2 = X^3 + aX + b$ over $\mathbb{F}_p$ (including the point $\mathcal{O}$ at infinity) satisfies $|N-(p+1)| \le 2\sqrt{p}$.*

Finally we have to address the question whether there are any explicit formulas. Such formulas exist, but are much harder to find. Gauss did this in special cases; translating his results into the language of elliptic curves, what he found was that the number of $\mathbb{F}_p$-rational points $E : y^2 = x(x^2-4)$ equals $p+1$ if $p \equiv 3 \bmod 4$, and $p+1-a_p$ if $p \equiv 1 \bmod 4$, where a_p is determined as follows: write $p = a^2+4b^2$ for unique positive integers a, b; then $a_p = \pm 2a$, where the sign is chosen in such a way that $a_p \equiv 2 \bmod 8$.

The result is so simple because E has 'complex multiplication' (here this means that the maps $x \longmapsto -x$, $y \longmapsto iy$ transform the curve into itself; we say that E has complex multiplication by $\mathbb{Z}[i]$). Elliptic curves with elliptic multiplication are very special and well understood; they are related to abelian extensions of the associated quadratic number fields, and thus can be understood properly only with class field theory.

Eichler and Shimura later found that there are (much more complicated) formulas for some non-CM curves that they called modular; Taniyama, Shimura and Weil conjectured which every elliptic curve defined over $\mathbb{Q}$ is modular (hence that there are 'explicit' formulas for a_p for every elliptic curve), and after the breakthrough by Wiles in 1995, this was proved in the 1990s by Breuil, Conrad, Diamond & Taylor (2000).

Thus the order of the groups $E(\mathbb{F}_p)$ is known; what about their structure?

Proposition 6. *For an elliptic curve E defined over a finite field $\mathbb{F}_q$, we have*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}, \quad \text{where } n_2 \mid n_1 \text{ and } n_2 \mid q-1.$$

4.3. **Quartics.** Postnikov's method does not give a nontrivial result in this case. A general theorem due to F.K. Schmidt (also proved by Châtelet) says that smooth curves of genus 1 over a finite field $\mathbb{F}_q$ always have $\mathbb{F}_q$-rational points. Here we will give an elementary proof of a special case of this result:

Theorem 7. *The quartic $Y^2 = b_1X^4 + aX^2 + b_2$ has nontrivial solutions modulo every prime p not dividing $2(a^2 - 4b_1b_2)$.*

Quartics with an $\mathbb{F}_p$-rational point can be transformed into Weierstrass form by a birational isomorphism, which means that the number of $\mathbb{F}_p$-rational points is essentially governed by the Hasse bound.

5. Local Solvability

The Hensel Lift. In the preceding section we have studied the existence of $\mathbb{F}_p$-rational points on curves $Y^2 = f(X)$ for polynomials f of degree 2, 3, and 4. Now we will investigate whether these points can be lifted to solutions in the p-adic numbers.

We will discuss the construction of p-adic numbers in some detail; for now suffice it to say that a p-adic number is the limit of congruence classes modulo p^n for $n \longrightarrow \infty$ in very much the same way as a real number like $\sqrt{2}$ is the limit of rational numbers 'given' by the decimal expansion of $\sqrt{2}$. The p-adic numbers form a field $\mathbb{Q}_p$ called the p-adic completion, and we set $\mathbb{R} = \mathbb{Q}_\infty$. By construction, we have $\mathbb{Q} \subseteq \mathbb{Q}_p$ for all p (including ∞), and this means: if a curve has a rational point, then it must have p-adic points for all p. A class of curves is said to satisfy Hasse's Local-Global principle if the converse is also true, that is, if the existence of p-adic solutions for all p implies that there must be some rational point.

Newton's method for computing zeros of differentiable functions has an analogue in the p-adic world and is called

Lemma 8 (Hensel's Lemma)**.** *Let $f \in \mathbb{Z}[X]$ be a polynomial; if p is a prime with $p \nmid 2 \operatorname{disc} f$, then every solution of $Y^2 - f(X) \equiv 0 \bmod p$ can be lifted to a solution modulo p^k for any $k \geq 1$.*

Or in more fancy terms: if $p \mid 2 \operatorname{disc} f$, then every $\mathbb{F}_p$-rational point on $Y^2 = f(X)$ can be lifted to a solution in $\mathbb{Q}_p$.

5.1. **Conics.** We have shown that the conic $\mathcal{C} : Y^2 = f(X)$, where $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$, has an $\mathbb{F}_p$-rational point for all primes $p \nmid a$. The discussion above shows that this point can be lifted to a point in $\mathcal{C}(\mathbb{Z}_p)$ if $p \nmid 2 \operatorname{disc} f$:

Proposition 9. *Let $\mathcal{C} : Y^2 = aX^2 + bX + c$ be a conic defined over $\mathbb{Z}$. Then $\mathcal{C}(\mathbb{Z}_p) \neq \varnothing$ for all primes $p \nmid 2a(b^2 - 4ac)$.*

The structure of $\mathcal{C}(\mathbb{Z}_p)$ for primes p is given by

Proposition 10. *If p is an odd prime not dividing Δ, then*

$$\mathcal{C}(\mathbb{Z}_p) \simeq \begin{cases} \mathbb{Z}/(p-1) \oplus \mathbb{Z}_p & \text{if } (\frac{\Delta}{p}) = +1, \\ \mathbb{Z}/(p+1) \oplus \mathbb{Z}_p & \text{if } (\frac{\Delta}{p}) = -1, \\ \mathbb{Z}/2 \oplus \mathbb{Z}_p & \text{if } p \mid \Delta \neq -3, \\ \mathbb{Z}/6 \oplus \mathbb{Z}_p & \text{if } p = 3,\ \Delta = -3. \end{cases}$$

5.2. **Cubics.** Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve defined over $\mathbb{Q}$, and assume that $a, b \in \mathbb{Z}$. By reducing the coordinates of a point $(x, y) \in E(\mathbb{Q}_p)$ modulo p, we get a map $E(Q_p)$ to $E(\mathbb{F}_p)$; if $p \mid \Delta$, the curve $E/\mathbb{F}_p$ will be singular, but the nonsingular points form a group $E_{\mathrm{ns}}(\mathbb{F}_p)$. Its inverse image under reduction is a subgroup $E_0(\mathbb{Q}_p) \subseteq E(\mathbb{Q}_p)$; the kernel of the reduction map is a subgroup $E_1(\mathbb{Q}_p) \subseteq E_0(\mathbb{Q}_p)$. It is known that $E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \simeq E_{\mathrm{ns}}(\mathbb{F}_p)$, and that $c_p = (E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p))$ is a finite number called the Tamagawa number. We have $c_p = 1$ for all primes not dividing the discriminant of E). Finally, the structure of E_1 can be determined explicitly:

Theorem 11. *In the chain of subgroups $E_1(\mathbb{Q}_p) \subseteq E_0(\mathbb{Q}_p) \subseteq E(\mathbb{Q}_p)$ we have $E_1(\mathbb{Q}_p) \simeq \mathbb{Z}_p$, $E_0/E_1 \simeq E_{ns}(\mathbb{F}_p)$, and E/E_0 is a finite group whose order is 1 for all primes $p \nmid \Delta$.*

This result is essential for proving results about torsion points on elliptic curves.

5.3. **Quartics.** Quartics of the form

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

will play a central role in the computation of the Mordell-Weil rank of elliptic curves with a rational point of order 2.

As a first step in deciding whether (2) has a nontrivial rational solution, one checks whether (2) has solutions in all completions $\mathbb{Q}_p$ of the rationals. Here is what we know so far: $\mathcal{T}(b_1)$ has $\mathbb{F}_p$-rational points for every prime $p \nmid 2(a^2-4b)$, where $b = b_1b_2$. Note that $a^2 - 4b = \operatorname{disc} g$, where $g(X) = b_1X^2 + aX + b_2$.

Now the polynomial $f(X) = b_1X^4+aX^2+b_2$ has discriminant $\operatorname{disc} f = 16b(a^2-4b)^2 = 16b(\operatorname{disc} g)^2$. Although $p \nmid 2\operatorname{disc} g$ was sufficient to guarantee solvability modulo p, for lifting these solutions to the completions via Hensel's Lemma we need the stronger condition $p \nmid \operatorname{disc} f$. Thus we have proved the following

Theorem 12. *The quartic $\mathcal{T}(b_1)$ has a solution in $\mathbb{Z}_p$ for all primes p not dividing $2b(a^2-4b)$.*

6. Global Solvability

By now we have studied points of conics, cubics and quartics defined over finite fields and over the p-adic numbers. It is now a natural question to ask what this implies for solutions in rational numbers or in integers:

> Assume that a curve $\mathcal{C}$ defined over $\mathbb{Q}$ satisfies $\mathcal{C}(\mathbb{Q}_p) \neq \varnothing$ for every completion $\mathbb{Q}_p$ including $\mathbb{Q}_\infty = \mathbb{R}$; does this mean there must be a rational point, i.e., does this imply that $\mathcal{C}(\mathbb{Q}) \neq \varnothing$?

Unfortunately not! There actually are curves for which this principle is true: Hasse showed in the 1920s that it holds for conics; thus the diophantine equation

$$aX^2 + bY^2 + cZ^2 = 0 \tag{3}$$

has a nontrivial rational solution if and only if it has a nontrivial solution in every localization $\mathbb{Q}_p$. It didn't take long, however, until during the 1940s Lind and Reichardt exhibited the first examples of curves of genus 1 without rational points that had solutions in every completion of $\mathbb{Q}$.

6.1. **Conics.** For conics $\mathcal{C}$, Hasse's Local-Global Principle is valid:

$$\mathcal{C}(\mathbb{Q}_p) \neq \varnothing \text{ for all primes } p \implies \mathcal{C}(\mathbb{Q}) \neq \varnothing.$$

Here $p = \infty$ is counted as a prime, the corresponding localization being $\mathbb{Q}_\infty = \mathbb{R}$.

Thus deciding whether a conic has a rational point is easy: just check whether $\mathcal{C}(\mathbb{Q}_p) \neq \varnothing$ for the finitely many primes $p \mid 2\Delta$.

In the case of Pell conics $\mathcal{C} : Y^2-\Delta X^2 = 4$, we can determine the group structure of $\mathcal{C}(\mathbb{Z})$:

Theorem 13. *Let Δ be the discriminant of a quadratic number field. Then*

$$\mathcal{C}(\mathbb{Z}) = \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } \Delta = -3, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } \Delta = -4, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } \Delta < -4, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} & \text{if } \Delta > 0. \end{cases}$$

The groups $\mathcal{C}(\mathbb{Q})$ are not finitely generated. Any torsion point (a point with finite order) on a Pell conic is an integral point: $\mathcal{C}(\mathbb{Q})_{\text{tors}} \subseteq \mathcal{C}(\mathbb{Z})$, and in fact the torsion group is either trivial (i.e. equal to $\{(\pm 1, 0)\} \simeq \mathbb{Z}/2\mathbb{Z}$) or one of the groups $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$ occurring above.

6.2. **Cubics.** Here we have the famous theorem of Mordell:

Theorem 14. *If E is an elliptic curve defined over $\mathbb{Q}$, then $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$ for some finite group T and an integer $r \geq 0$ called the Mordell-Weil rank.*

The Hasse principle is not valid for elliptic curves, so determining whether E has a rational point except the one at infinity cannot be reduced to checking local solvability. One of the biggest unsolved problems in the theory of elliptic curves is to find a criterium by which one can decide whether an elliptic curve has nontrivial rational points (different from the one at ∞).

The 2-descent we will discuss in detail will reduce the determination of the rank r (for curves with a rational point of order 2) to checking rational solvability of certain quartics.

Selmer (1950) gave an example of a cubic curve of genus 1 without a rational point but with points in every localization of $\mathbb{Q}$, namely the cubic $3X^3+4Y^3+5Z^3 = 0$.

Although finding the rank is difficult, the torsion group $T = E(\mathbb{Q})_{\text{tors}}$ can be determined rather easily with the following result due to Elisabeth Lutz (a student of A. Weil) and Nagell:

Theorem 15. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with coefficients in $\mathbb{Z}$. Then any point of finite order $(x, y) \in E(\mathbb{Q})$ has integral coordinates, and in fact we have $y = 0$ or $y^2 \mid \Delta$.*

The following much deeper result due to Mazur describes all possible torsion groups:

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

6.3. **Quartics.** As for cubics with genus 1, the rational solvability of a quartic cannot be proved by just checking local solvability everywhere. The first counterexamples were constructed by Reichardt and and Lind in the 1940s.

7. Summary

Let us summarize the analogy between integral points on Pell conics and rational points on elliptic curves in a table:

	Pell conics	elliptic curves
group structure on	affine plane	projective plane
defined over	rings	fields
group elements	integral points	rational points
associativity	Pascal's Theorem	Bezout's Theorem
parametrized by	trig functions	Weierstrass $\wp$
finite fields	$\lvert\#\mathcal{C}(\mathbb{F}_q)-q\rvert\le 1$	$\lvert\#E(\mathbb{F}_q)-(q+1)\rvert\le 2\sqrt{q}$
Mordell-Weil	$C(\mathbb{Z})_{\rm tors}\oplus\mathbb{Z}^r$	$E(\mathbb{Q})_{\rm tors}\oplus\mathbb{Z}^r$
torsion	$\#C(\mathbb{Z})_{\rm tors}\le 6$	$\#E(\mathbb{Q})_{\rm tors}\le 16$
Nagell-Lutz	$y=0$ or $y=1$	$y=0$ or $y^2\mid\Delta$