LECTURE 1

FRANZ LEMMERMEYER

1. Historical Remarks

Elliptic curves occurred for the first time, if only implicitly, in the work of Diophantus, and the topic has remained close to Diophantine Geometry throughout the centuries. A typical example from Diophantus is the following: given a number, say 7, that can be written as a difference of two cubes ($7 = 8 - 1$), find two rational numbers such that $7 = a^3 + b^3$ (all of Diophantus' numbers are positive rational numbers – otherwise the problem would be trivial). Diophantus succeeded with clever substitutions, and it was discovered much later by Newton, Lucas, and Sylvester that there is a very geometric interpretation. In the example above, consider the curve $E : x^3 - y^3 = 7$ and the rational point $P = (x, y) = (2, 1)$. Then the tangent to E at P will intersect E in a third rational (!) point Q. If its coordinates are not positive, try intersecting the curve with the secant PQ etc.

These kind of Diophantine problems were a big thing for Fermat and Euler, but then Gauss started giving number theory a new direction by proving quadratic and biquadratic reciprocity laws. Generalizing these to higher powers was a central occupation for the main number theorists like Jacobi, Eisenstein, Kummer, and Hilbert until, in 1920, Takagi put the finishing touches on this theme by creating class field theory. During these times, elliptic curves were studied mainly by less known number theorists like Cauchy, Lucas, Sylvester, Poincaré and Beppo Levi (most of whom are known for their contributions to other areas of mathematics) as well as by what we would classify as complex algebraic geometers like Clebsch or Juel.

Once the general reciprocity law had been proved, more first-class mathematicians started looking at elliptic curves: Mordell proved a tacit assumption in one of Poincarés articles, namely that the group of rational points on elliptic curves is generated by finitely many points (there are finitely many rational points such that every rational point can be constructed from these using the classical chord and tangent process). André Weil, one of the greatest mathematicians of the 20th century, gave a new (and much clearer) proof of Mordell's theorem and generalized it to abelian varieties over number fields. Emil Artin, who a little later would turn Takagi's class field theory upside down with his new reciprocity law, studied hyperelliptic curves in his thesis and came up with a 'Riemann conjecture' for the zeta function of such objects. Hasse, who had worked on reciprocity laws together with Artin in the 1920s, succeeded in proving the Riemann hypothesis for elliptic curves, and during World War II André Weil generalized these conjectures to (smooth) algebraic varieties (they became known as the Weil conjectures) and proved them for curves. Grothendieck, another mathematician that should be on the top ten list of the 20th century, started inventing the most abstract machinery mathematics has seen so far in order to prove the Weil conjectures; this program was successful, and in the 1970s Deligne proved the last of them, namely the Riemann conjecture.

The Weil conjectures had put elliptic curves on the back bench again, but now they came back with a vengeance: Lenstra found that elliptic curves could be used for factoring integers, Frey discovered that they could be used for proving Fermat's Last Theorem (which, with a little help from Serre, Ribet, and Taylor, was actually done by Wiles in 1994), and by now there are cell phones that use elliptic curves for safe communication.

2. Fermat's Last Theorem for Exponent 4

Elliptic curves came up in connection with Fermat's Last Theorem long before Wiles. Actually Fermat's own proof of FLT for the exponent 4 uses (implicitly) two elliptic curves and an isogeny between them. In this section we will present his proof; much of this semester will be spent on generalizing this proof to general elliptic curves.

Consider the equation

$$X^4 + Y^4 = Z^4; \tag{1}$$

if this equation has solutions in nonzero integers, then so does the equation

$$X^4 + Y^4 = z^2. \tag{2}$$

Thus proving that (2) has no nontrivial solutions is more than doing this for (1); yet working with (2) turns out to be much simpler: the reason is that (2) is an elliptic curve, while (1) is not.

Theorem 1. *The equation* (2)*, and therefore the Fermat equation (1) for the exponent* 4*, does not have any integral solution* (x, y, z) *with* $xyz \neq 0$*.*

Proof. Assume that $x, y, z \in \mathbb{N} \setminus \{0\}$ satisfy (2); we may (and will) assume that these integers are pairwise coprime (otherwise we can cancel common divisors). Since (x^2, y^2, z) is a Pythagorean triple, z is odd, and we may assume that x is odd and y is even. Thus there exist integers m, n such that $x^2 = m^2 - n^2$, $y^2 = 2mn$ and $z = m^2 + n^2$. Clearly $\gcd(m, n)$ divides both x and y, hence m and n are coprime; moreover, since x is odd, we have $1 \equiv x^2 = m^2 - n^2 \bmod 4$, which implies that m is odd and $n = 2k$ is even. Thus $(y/2)^2 = mk$ with m and k coprime, hence $m = a^2$ and $k = b^2$, giving $x^2 = a^4 - 4b^4$.

Now we repeat the trick: from $x^2 + 4b^4 = a^4$ we see that $(x, 2b^2, a^2)$ is a Pythagorean triple; thus $x = m_1^2 - n_1^2$, $2b^2 = 2m_1n_1$ and $a^2 = m_1^2 + n_1^2$, where m_1 and n_1 are (necessarily coprime) positive integers. From $m_1n_1 = b^2$ we deduce that $m_1 = r^2$ and $n_1 = s^2$, hence $a^2 = r^4 + s^4$, and we have found a new solution $(X, Y, Z) = (r, s, a)$ of (2).

Since $z = m^2 + n^2 = a^4 + 4b^4$, we find that $0 < a < z$; this means that for every solution (x, y, z) in natural numbers there exists another solution (r, s, a) with $a < z$. This is impossible, so there can't be a nontrivial solution to the Fermat equation in the first place. □

Fermat called this method of proof 'descente infinie' (infinite descent): one descends from a solution in integers to a smaller one, and this cannot be done indefinitely. He used it also to prove e.g. that primes of the form $4n + 1$ are sums of two squares.

3. Elliptic Curves in Weierstrass Form

There were two elliptic curves hiding in our proof of FLT for the exponent 4: one is $X^4 + Y^4 = Z^2$, the other is $X^4 - 4Y^4 = Z^2$.

Consider $X^4 + Y^4 = Z^2$ and divide through by Y^4; putting $x = X/Y$ and $z = Z/Y^2$ we get $x^4 + 1 = z^2$, that is, $1 = z^2 - x^4 = (z - x^2)(z + x^2)$. Now we put $t = z + x^2$; then $z - x^2 = \frac{1}{t}$, hence $t - \frac{1}{t} = 2x^2$. Multiplying through by $8t^2$ gives $8t^3 - 8t = 16x^2t^2$. Putting $u = 4xt$ and $v = 2t$ we get the Weierstrass elliptic curve $u^2 = v^3 - 4v$.

A large part of the course will be devoted to understanding this proof and generalizing it to more general elliptic curves. Eventually we will see that the two elliptic curves in Fermat's proofs are connected by a 2-isogeny, and that the points (x, y, z) and (r, s, a) in the proof satisfy the relation $(x, y, z) = 2(r, s, a)$ if interpreted as addition in the group of points on this elliptic curve.