Elliptic curves, modularity, and Fermat's Last Theorem

For background and (most) proofs, we refer to [1].

1 Weierstrass models

Let K be any field. For any $a_1, a_2, a_3, a_4, a_6 \in K$ consider the plane projective curve C given by the equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{1}$$

An equation as above is called a *Weierstrass equation*. We also say that (1) is a *Weierstrass model* for C.

L-Rational points

For any field extension L/K we can consider the L-rational points on C, i.e. the points on C with coordinates in L:

$$C(L) := \{(x : y : z) \in \mathbb{P}^2_L : \text{ equation (1) is satisfied }\}.$$

The point at infinity

The point $O := (0 : 1 : 0) \in C(K)$ is the only K-rational point on C with $z = 0$. It is always smooth. Most of the time we shall instead of a homogeneous Weierstrass equation write an affine Weierstrass equation:

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

which is understood to define a plane projective curve.

The discriminant

Define

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, \\ b_4 &:= 2a_4 + a_1a_3, \\ b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

For any Weierstrass equation we define its discriminant

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Note that if $\mathrm{char}(K) \neq 2$, then we can perform the coordinate transformation $y \mapsto (y - a_1x - a_3)/2$ to arrive at an equation $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$. The discriminant (w.r.t. x) of the right-hand side of this equation is simply $2^4\Delta$, which follows from a straightforward computation using the identity $b_4^2 = b_2b_6 - 4b_8$. If $a_1 = a_3 = 0$, so the Weierstrass equation is of the form $y^2 = f(x)$ with f a cubic monic polynomial (in x), then $\Delta = 2^4 \operatorname{disc}_x(f)$.

Proposition 1. *A curve C/K given by a Weierstrass equation ((1) or (2)) has $\Delta \neq 0$ if and only if C is smooth.*

Nonsmooth points

Suppose C is not smooth, then there is exactly one singular point $P \in C(\overline{K})$. Let

$$c_4 := b_2^2 - 24b_4$$

(we know $\Delta = 0$). We distinguish two possibilities:

- C has a node at P (i.e. a double point); this happens if and only if $c_4 \neq 0$.
- C has a cusp at P; this happens if and only if $c_4 = 0$.

Changing equations

We allow the coordinate transformations

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + su^2x' + t \end{aligned}$$

with $r, s, t, u \in K$ and $u \neq 0$. The discriminant changes as

$$\Delta = \Delta' u^{12}.$$

If $r = s = t = 0$, then the coefficients of the Weierstrass equation transform as

$$a_i = a_i' u^i.$$

2 Elliptic curves

When studying elliptic curves, there is (in theory) nothing lost, when one restricts to (nonsingular) curves given by Weierstrass equations.

Proposition 2. *Let (E, P) be an elliptic curve over the field K, i.e. E is a smooth algebraic curve of genus one over K and $P \in E(K)$. Then there exists a curve C given by a Weierstrass model with $a_1, a_2, a_3, a_4, a_6 \in K$ and an isomorphism $\phi : E \to C$ with $\phi(P) = (0 : 1 : 0)$. Conversely, for every curve C defined by a Weierstrass equation with $\Delta \neq 0$, we have that (C, O) is an elliptic curve.*

Usually we just refer to E/K as an elliptic curve over K (the point $P \in E(K)$ is understood). Using e.g. the well-known 'chord and tangent addition', the

rational points $E(K)$ get the structure of an abelian group. If K is a number field, then the Mordell-Weil theorem states that $E(K)$ is finitely generated, i.e.

$$E(K) \simeq T \oplus \mathbb{Z}^r$$

for some finite abelian group T and some $r \in \mathbb{Z}_{\geq 0}$. The number r is called the rank of $E(K)$, denoted $\mathrm{rank}(E(K))$.

Minimal models and the discriminant

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Among all possible Weierstrass models for E with $a_1, \ldots, a_6 \in \mathbb{Z}$ there are models with $\mathrm{ord}_p(\Delta)$ minimal. Such a model for E is called *minimal* at p.

Proposition 3. *For an elliptic curve $E/\mathbb{Q}$ there exists a Weierstrass model with $a_1, \ldots, a_6 \in \mathbb{Z}$ which is minimal at p for all primes p.*

A Weierstrass model as in the proposition is called a *global minimal model*, or simply a *minimal model*, for E. This minimal model is not unique in general, but its discriminant is uniquely determined by E. This invariant of E is called the *minimal discriminant* of E and denoted by $\Delta_{\min}(E)$.

Reduction

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Choose a Weierstrass model for E with $a_1, \ldots, a_6 \in \mathbb{Z}$ which is minimal at p. This model can be reduced modulo p by simply mapping a_i to $\overline{a_i} := a_i (\mathrm{mod}\ p) \in \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$. This gives a Weierstrass model with $\overline{a_1}, \ldots, \overline{a_6} \in \mathbb{F}_p$ and defines a curve over the finite field $\mathbb{F}_p$. As it turns out, (the isomorphism class of) this curve $\tilde{E}/\mathbb{F}_p$ is independent of the choice of Weierstrass model for E minimal at p. In particular, its number of points over $\mathbb{F}_p$, i.e. $\#\tilde{E}(\mathbb{F}_p)$, is an invariant of E, as is

$$a_p(E) := p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

If $\tilde{E}/\mathbb{F}_p$ is nonsingular, then we say that E has *good reduction* at p, otherwise we say that E has *bad reduction* at p. In the latter case, we say that E has *multiplicative reduction* if $\tilde{E}/\mathbb{F}_p$ has a node, and we say that E has *additive reduction* at p if $\tilde{E}/\mathbb{F}_p$ has a cusp.

Remark 4. *Obviously, any Weierstrass model for E with $a_1, \ldots, a_6 \in \mathbb{Z}$ can be reduced modulo p to a Weierstrass model with $\overline{a_1}, \ldots, \overline{a_6} \in \mathbb{F}_p$. The latter defines again a curve over the finite field $\mathbb{F}_p$, but (the isomorphism class of) this curve may depend on the chosen Weierstrass model for E. In particular, is it easy to see that for every prime p there always exists a choice of model for E such that the resulting reduction of the model modulo p yields a Weierstrass model for a curve over $\mathbb{F}_p$ with a cuspidal singularity.*

Minimal models at primes where the reduced curve has a node are easily characterized as follows.

Proposition 5. *Let $E/\mathbb{Q}$ be an elliptic curve and choose a Weierstrass model for it with $a_1, \ldots, a_6 \in \mathbb{Z}$. Let p be a prime, then the following are equivalent*

- $\tilde{E}/\mathbb{F}_p$ *has a node and the model is minimal at* p*;*
- $p|\Delta$ *and* $p \nmid c_4$*.*

If $p|\Delta$ and $p|c_4$, then it might still be possible that $\tilde{E}/\mathbb{F}_p$ has a node, but in that case the model is necessarily not minimal at p.

The Conductor

There is an important representation theoretic invariant associated to any $E/\mathbb{Q}$, called the *conductor* of E, denoted $N(E)$. The full definition is quite subtle, see Chapter 4, §10 of [2]. We state a partial definition here: $N(E) \in \mathbb{Z}_{>0}$ and for all primes p we have

$$\mathrm{ord}_p(N(E)) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2+\delta_p & \text{if } E \text{ has additive reduction at } p \end{cases}$$

where $\delta_p \in \mathbb{Z}_{\geq 0}$. Furthermore, $\delta_2 \leq 6$, $\delta_3 \leq 3$, and $\delta_p = 0$ for $p \geq 5$. In particular, if E has good or multiplicative reduction at 2 and 3, then this completely defines $N(E)$.

Note that $N(E)$ and $\Delta_{\min}(E)$ have exactly the same prime divisors, namely the primes where E has bad reduction. If E has only good or additive reduction, then E is said to be *semi-stable*. This amounts to the same thing as saying that $N(E)$ is squarefree.

L-series and BSD

For an elliptic curve $E/\mathbb{Q}$ we define its L-series

$$L_E(s) := \prod_p (1 - a_p(E)p^{-s} + 1_{N(E)}(p)p^{1-2s})^{-1}$$

where the product is over all primes p and $1_{N(E)}$ denotes the trivial Dirichlet character modulo $N(E)$. It can be shown that for all primes p we have $|a_p(E)| \leq 2\sqrt{p}$ and that as a consequence we have that the Dirichlet series corresponding to $L_E(s)$ converges to a holomorphic function for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 3/2$.

It is natural to ask if there exists an analytic continuation of $L_E(s)$ to the whole complex plane $\mathbb{C}$. If this is possible, then we have a meromorphic (possibly holomorphic) function on $\mathbb{C}$ defined by

$$\xi_E(s) := N(E)^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s).$$

For this function (also called $\Lambda_E(s)$ in the literature) it is natural to expect a functional equation

$$\xi_E(s) = \pm\xi_E(2-s) \tag{3}$$

for all $s \in \mathbb{C}$ and some choice of sign $\pm$ depending only on E (conjecturally $(-1)^{\mathrm{rank}(E(\mathbb{Q}))}$).

Suppose it is possible to analytically continue $L_E(s)$ to a region containing a neighborhood of $s = 1$. It is conjectured that at $s = 1$ the function $L_E(s)$ reflects arithmetic information about $E/\mathbb{Q}$. Introduce the *analytic rank* $r_{\mathrm{an}}(E) := \mathrm{ord}_{s=1}(L_E(s))$, i.e. the order of vanishing of $L_E(s)$ at $s = 1$. Also introduce the *algebraic rank* $r_{\mathrm{al}}(E) := \mathrm{rank}(E(\mathbb{Q}))$.

Conjecture 6 (Weak Birch and Swinnerton-Dyer conjecture)**.** *For any elliptic curve $E/\mathbb{Q}$ we have*

$$r_{\mathrm{an}}(E) = r_{\mathrm{al}}(E).$$

There is also a stronger version of the conjecture, relating the first nonzero coefficient of the Taylor expansion of $L_E(s)$ around $s = 1$ to other (arithmetic) invariants of E, most notably the order of its so-called Shafarevich-Tate group, which is only conjecturally known to be finite.

Some important cases of the Birch and Swinnerton-Dyer conjure were proved by Coates-Wiles, Gross-Zagier, and Kolyvagin. The latter result is that if $E/\mathbb{Q}$ is a *modular* elliptic curve (see below for a definition) we have

$$r_{\mathrm{an}}(E) \leq 1 \Rightarrow r_{\mathrm{an}}(E) = r_{\mathrm{al}}(E). \tag{4}$$

3 Modularity

We use the term *newform* instead of the term *primitive form* (found in the other notes).

Definition 7. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E is said to be* modular *if there exists a newform $f \in S_2(\Gamma_0(N(E)))$ such that $a_p(E) = a_p(f)$ for all primes p.*

There are many equivalent definitions of modularity. For instance, if there exists some $M \in \mathbb{Z}_{>0}$ and a newform $f \in S_2(\Gamma_0(M))$ such that $a_p(E) = a_p(f)$ for all but possibly finitely many primes p, then $M = N(E)$ and $a_p(E) = a_p(f)$ for all primes p.

The conjecture that all elliptic curves over $\mathbb{Q}$ are in fact modular is known as the Shimura-Taniyama-Weil conjecture (and under many other names, including most permutations of subsets of the three names).

Theorem 8 (Modularity)**.** *Every elliptic curve over $\mathbb{Q}$ is modular.*

This was proved for semi-stable elliptic curves in 1994 by Wiles, with help from Taylor. This sufficed to complete the proof of Fermat's Last Theorem. Subsequently, the methods of Wiles and Taylor were generalized until finally in 1999 the full modularity theorem above was proved by Breuil, Conrad, Diamond, and Taylor.

As an example of modularity, consider the elliptic curve E given by the Weierstrass equation

$$y^2 + y = x^3 - x^2.$$

One computes that $\Delta = -11$ and $c_4 = 16 \not\equiv 0 \pmod{11}$. So the model is minimal and E has only bad reduction at $p = 11$, where it has a node. This yields for the conductor $N(E) = 11$. Furthermore, for all primes p we have very concretely

$$\#\tilde{E}(\mathbb{F}_p) = \#\{(x, y) \in \mathbb{F}_p^2 : y^2 + y = x^3 - x^2\} + 1.$$

The extra $+1$ comes from the point at infinity. We can make a little table for $\#\tilde{E}(\mathbb{F}_p)$ and consequently for $a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$.

p	2	3	5	7	11	13	17	19	...	2017	...	1000003
$\#\tilde{E}(\mathbb{F}_p)$	5	5	5	10	11	10	20	20	...	2035	...	999720
$a_p(E)$	-2	-1	1	-2	1	4	-2	0	...	-17	...	284

By the modularity theorem there must exist a newform $f \in S_2(\Gamma_0(11))$ such that $a_p(E) = a_p(f)$ for all primes p. One easily checks that $S_2(\Gamma_0(11))^{\text{new}} = S_2(\Gamma_0(11))$ is one-dimensional and that $\eta(\tau)^2\eta(11\tau)^2 = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$ defines a normalized form in this space. So this must be the newform f given by the modularity theorem. Indeed, by (formally) expanding the product, we get

$$f = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + \ldots - 17q^{2017} + \ldots + 284q^{1000003} + \mathcal{O}(q^{1000004}).$$

Here is a little table for $a_p(f)$.

p	2	3	5	7	11	13	17	19	...	2017	...	1000003
$a_p(f)$	-2	-1	1	-2	1	4	-2	0	...	-17	...	284

We see that indeed for the prime p in the previous tables, we have $a_p(E) = a_p(f)$.

Consequences for BSD

By modularity, the L-series of an elliptic curve E over $\mathbb{Q}$ equals the L-series of a newform in $S_2(\Gamma_0(N(E)))$. For such an L-series we have well-known analytic continuation and functional equation results, showing that indeed L_E and ξ_E can be analytically continued to the whole complex plane and satisfy the expected functional equation. In particular, $r_{\text{an}}(E)$ is at least well-defined. Furthermore, the result (4) holds unconditionally now!

4 More on Weierstrass models

Recall that for a Weierstrass model with $a_1, a_2, a_3, a_4, a_6 \in K$ (some field) we defined b_2, b_4, b_6, b_8 in terms of the a_i and subsequently

$$\Delta := -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6,$$

$$c_4 := b_2^2 - 24b_4.$$

If $a_1 = a_3 = 0$, then this reduces to

$$\Delta = 2^4 \operatorname{disc}_x(x^3 + a_2x^2 + a_4x + a_6) = 2^4(a_2^2a_4^2 - 4a_4^3 - 4a_2^3a_6 + 18a_2a_4a_6 - 27a_6^2),$$

$$c_4 = 2^4(a_2^2 - 3a_4).$$

A Weierstrass model for an elliptic curve has $\Delta \neq 0$, in this case we define the j-invariant as

$$j := \frac{c_4^3}{\Delta}.$$

For $r, s, t, u \in K$ with $u \neq 0$ we considered coordinate transformations

$$\begin{aligned} x &= u^2 x' + r \\ y &= u^3 y' + s u^2 x' + t. \end{aligned}$$

The new Weierstrass model has

$$\Delta' = \frac{\Delta}{u^{12}},$$

$$c_4' = \frac{c_4}{u^4}.$$

As a consequence, we have in the case of elliptic curves

$$j' = j.$$

So the j-invariant of an elliptic curve is a quantity that is independent of a chosen Weierstrass model, and hence a true invariant of the curve alone. So two isomorphic elliptic curves have the same j-invariant. A converse also holds: if two elliptic curves over K have the same j-invariant, then they are isomorphic over $\overline{K}$. (It can definitely happen that two elliptic curves over K with the same j-invariant are *not* isomorphic over K.)

Note that the transformation properties of Δ and c_4 immediately lead to sufficient conditions for minimality at p for a model with $a_1, \ldots, a_6 \in \mathbb{Z}$.

Proposition 9. *A Weierstrass model for an elliptic curve with $a_1, \ldots, a_6 \in \mathbb{Z}$ is minimal at a prime p if*

$$\mathrm{ord}_p(\Delta) < 12 \quad \text{or} \quad \mathrm{ord}_p(c_4) < 4. \tag{5}$$

It turns out that for $p \geq 5$ the condition (5) is both sufficient and necessary to be minimal at p.

We also note the following.

Proposition 10. *Consider the Weierstrass model*

$$E : y^2 = x^3 + a_2 x^2 + a_4 x + a_6 =: f(x)$$

with $a_2, a_4, a_6 \in \mathbb{Z}$ and $\Delta \neq 0$. Let p be an odd prime. If for some $a, b \in \mathbb{Z}$ with $a \not\equiv b \pmod{p}$ we have

$$f(x) \equiv (x-a)^2(x-b) \pmod{p},$$

then the model is minimal at p and E has multiplicative reduction at p.

Proof. We compute $\Delta \equiv 0 \pmod{p}$ and $c_4 \equiv 2^4(a-b)^2 \not\equiv 0 \pmod{p}$. So $\mathrm{ord}_p(c_4) = 0 < 4$ and the previous proposition tells us that the model is minimal at p. Furthermore, the model has $p | \Delta$ and $p \nmid c_4$, so $\tilde{E}/\mathbb{F}_p$ has a node, i.e. E has multiplicative reduction at p. □

5 Isogenies

Definition 11. *Let K be a field of characteristic 0 (e.g. $\mathbb{Q}$) and let $n \in \mathbb{Z}_{>0}$. An elliptic curve E/K has a K-*rational isogeny of degree n *if there exists a subgroup $G \subset E(\overline{K})$ if order n with $\sigma G = G$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.*

There is a complete classification of $\mathbb{Q}$-rational isogenies. Here is a partial result.

Theorem 12 (Mazur et al.)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let l be a prime. Then E does not have a $\mathbb{Q}$ rational l-isogeny in any of the following situations*

- *$l > 163$;*
- *$l \geq 11$ and $E(\mathbb{Q})$ contains a point of order 2;*
- *$l \geq 5$, $E(\mathbb{Q})$ contains three points of order 2, and E is semi-stable.*

Write the elliptic curve as $y^2 = f(x)$ with $f \in \mathbb{Q}[x]$ of degree 3. Then the number of points of order 2 in $E(\mathbb{Q})$ equals the number of roots in $\mathbb{Q}$ of $f(x)$. The j-invariant contains useful information about $\mathbb{Q}$-rational l-isogenies. We have for example:

Theorem 13. *An elliptic curve $E/\mathbb{Q}$ has no $\mathbb{Q}$-rational l-isogeny in both of the following situations*

- *$l = 7$, $E(\mathbb{Q})$ contains a point of order 2, and $j \notin \{-3^3 \cdot 5^3, 3^3 \cdot 5^3 \cdot 17^3\}$;*
- *$l = 5$ and there is no $t \in \mathbb{Q}$ such that $j = (t^2 + 10t + 5)^3/t$.*

6 Level lowering

An element a in a ring containing $\mathbb{Z}$ (e.g. $\mathbb{C}$ or $\overline{\mathbb{Q}}$) is called an *algebraic integer* if $f(a) = 0$ for some monic polynomial $f \in \mathbb{Z}[x]$. For an algebraic integer a there is a unique monic $f \in \mathbb{Z}[x]$ of minimal degree with $f(a) = 0$, called the *minimal polynomial* of a.

Theorem 14. *Let $f = \sum_{n=1}^{\infty} a_n(f) q^n$ be a newform. Then $a_n(f)$ is an algebraic integer for all $n \in \mathbb{Z}_{>0}$.*

We are now ready to state a level lowering theorem due to Ribet. This is a special case suitable for applications to Diophantine problems. Before the proof of modularity of elliptic curves over $\mathbb{Q}$, the theorem was only known to hold for modular elliptic curves over $\mathbb{Q}$.

Theorem 15. *Let $E/\mathbb{Q}$ be an elliptic curve and let l be an odd prime. Define*

$$S_l := \{p \text{ prime } : \mathrm{ord}_p(N(E)) = 1 \text{ and } \mathrm{ord}_p(\Delta_{\min}(E)) \equiv 0 \pmod{l}\}.$$

If E is modular and does not have a $\mathbb{Q}$-rational l-isogeny, then there exists a newform

$$f \in S_2\left(\Gamma_0\left(\frac{N(E)}{\prod_{p \in S_l} p}\right)\right)$$

such that for all primes $p \nmid N(E)l$ we have

$$l | m_p(a_p(E)) \tag{6}$$

where m_p denotes the minimal polynomial of $a_p(f)$.

Thanks to the modularity theorem, we can of course remove the assumption that E is modular in the theorem above.

Remark 16. *The congruence (6) is usually stated as a congruence between $a_p(E)$ and $a_p(f)$ modulo some prime ideal. In case $a_p(f) \in \mathbb{Z}$ we note that $m_p(x) = x - a_p(f)$, so (6) reduces to $l | a_p(E) - a_p(f)$, which means the same as*

$$a_p(E) \equiv a_p(f) \pmod{l}.$$

Example 17. *Consider the elliptic curve*

$$E : y^2 + xy = x^3 + x^2 - 19x + 685.$$

For this model we calculate

$$\Delta = -2^{16} \cdot 3^5 \cdot 13, \quad c_4 = 937 \text{ (a prime)}$$

We see that there is no prime with $\mathrm{ord}_p(\Delta) \geq 12$ and $\mathrm{ord}_p(c_4) \geq 4$, hence the model is a global minimal model. Furthermore, if $p | \Delta$, then $p \nmid c_4$, so at the primes of bad reduction, the reduction is multiplicative. We conclude

$$\Delta_{\min}(E) = -2^{16} \cdot 3^5 \cdot 13, \quad N(E) = 2 \cdot 3 \cdot 13.$$

For $l = 5$ we want to apply the level lowering theorem. We compute

$$S_5 = \{3\}.$$

We know of course that E is modular, and the absence of a $\mathbb{Q}$-rational 5-isogeny is also readily checked using Theorem 13. The theorem above now guarantees the existence of a newform $f \in S_2(\Gamma_0(2 \cdot 13))$ such that for all primes $p \notin \{2, 3, 5, 13\}$ we have $l | m_p(a_p(E))$ (with $m_p(x)$ the minimal polynomial of $a_p(f)$). Using e.g. Sage, we compute that there are two newforms $f_1, f_2 \in S_2(\Gamma_0(26))$, both with Fourier coefficients in $\mathbb{Z}$. Here is a little table containing values of $a_p(f_1), a_p(f_2)$, and $a_p(E)$ for primes $p \leq 17$.

p	2	3	5	7	11	13	17
$a_p(E)$	-1	-1	2	4	-4	1	2
$a_p(f_1)$	-1	1	-3	-1	6	1	-3
$a_p(f_2)$	1	-3	-1	1	-2	-1	-3

We see that $a_7(f_1) \equiv a_7(E) \pmod 5$, while $a_7(f_2) \not\equiv a_7(E) \pmod 5$. So we must have $a_p(E) \equiv a_p(f_1) \pmod 5$ for all primes $p \neq 3$ (the cases $p = 2, 5, 13$ can be checked by inspection).

7 Fermat's Last Theorem

Let $n \in \mathbb{Z}_{\geq 2}$ and consider the Diophantine equation

$$a^n + b^n = c^n, \quad a, b, c \in \mathbb{Z}. \tag{7}$$

Solutions to (7) with $abc = 0$ are called trivial solutions. The statement of Fermat's Last Theorem is that for all integers $n \geq 3$ the only solutions to (7) are the trivial ones. The cases $n = 3$ and $n = 4$ are solved, $n = 4$ by Fermat himself and $n = 3$ (more or less) by Euler. Since any integer $n \geq 3$ is divisible by an odd prime or 4, it only remains to solve (7) for primes $n \geq 5$. In fact, before the proof of FLT by Wiles et al. there were many prime exponent $n \geq 5$ for which (7) was solved. However, we do not need these results, since the 'elliptic curves/modular forms proof' of FLT below works for all primes $n \geq 5$.

So let us assume that there are nonzero $a, b, c \in \mathbb{Z}$ and a prime $l \geq 5$ such that $a^l + b^l = c^l$. We are going to arrive at a contradiction, which then proves FLT. Without loss of generality we assume that

$$\gcd(a, b, c) = 1, \quad 2|b, \quad a \equiv -1 \pmod 4.$$

We consider the so-called Frey curve, which is the following elliptic curve.

$$E : y^2 = x(x - a^l)(x + b^l).$$

We compute

$$\Delta = 2^4(abc)^{2l}, \quad c_4 = 2^4(a^{2l} + a^l b^l + b^{2l}).$$

Using Proposition 10, we get that for *odd* primes $p|abc$ the model is minimal at p and $\mathrm{ord}_p(N(E)) = 1$. If $p \nmid abc$, then $p \nmid \Delta$, so in this case the model is minimal at p as well and $\mathrm{ord}_p(N(E)) = 0$ of course. So in order to compute $N(E)$ and $\Delta_{\min}(E)$ it remain to compute $\mathrm{ord}_2(N(E))$ and $\mathrm{ord}_2(\Delta_{\min}(E))$. For this, we consider the change of coordinates

$$x = 4x', \quad y = 8y' + 4x'.$$

This give us a model with integers coefficients

$$E : y'^2 + x'y' = x'^3 + \frac{b^l - a^l - 1}{4}x'^2 - \frac{a^l b^l}{16}x'$$

with

$$\Delta' = \frac{\Delta}{2^{12}} = \frac{(abc)^{2l}}{2^8}, \quad c_4' = \frac{c_4}{2^4} = a^{2l} + a^l b^l + b^{2l}.$$

Since $2 \nmid c_4'$ we get that this model is minimal at 2 and consequently it is a global minimal model. Finally $2|\Delta'$, so $\mathrm{ord}_2(N(E)) = 1$. We summarize

$$\Delta_{\min}(E) = \frac{(abc)^{2l}}{2^8}, \quad N(E) = \prod_{p|abc} p.$$

By Theorem 12 we get that there are no $\mathbb{Q}$-rational l-isogenies. Together with the modularity of E we are in a position to apply Theorem 15. We compute

$$S_l := \{p \text{ prime } : p|abc, p \neq 2\}.$$

So $N(E)/\prod_{p\in S_l} p = 2$ and we arrive at the existence of a newform f in $S_2(\Gamma_0(2))$. We claim that such a newform does not exist, a contradiction which finishes the proof of Fermat's last Theorem.

One way to prove the claim using computer algebra would be to check that the Sage command `Newforms(2)` returns an empty list. Another way would be to use the valence formula for congruence subgroups to show that $\dim(S_2(\Gamma_0(2))) = 0$.

References

[1] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.

[2] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151, Springer-Verlag, New York, 1994.