Descent by 2-isogeny on elliptic curves: from Fermat to Weil

Julian Salazar* (jsalazar01@college.harvard.edu)

May 16, 2016

Abstract

In this expository article, we start with Fermat's method of infinite descent as applied to the congruent number problem, and show how it is generalized by the strategy of descent by 2-isogeny on elliptic curves over number fields. Along the way, we examine Fermat's original proof and reframe it as an argument of morphisms on elliptic curves; we introduce Weil's theory of heights to prove the Mordell-Weil theorem; and we use algebraic number theory to prove the weak Mordell-Weil theorem and to see how rational 2-torsion makes the computation of $E(K)/2E(K)$ sometimes (but not always!) tractable.

*This article was written at Harvard University under the supervision of Prof. Noam Elkies, in the context of an independent reading course (Math 91r). It fulfills the author's *junior paper* requirement for the Mathematics concentration.

1 The method of infinite descent

Our story begins with a technique devised by Fermat in the 1600's with regards to solving Diophantine equations: the method of *infinite descent*. In Fermat's letters to other mathematicians about his solutions to Diophantine problems, he would quite often reference descent as one of his essential techniques. However, there exists only one written record of Fermat explicitly working out a descent argument. It comes from the marginalia of his copy of Diophantus' *Arithmetica*, an edition that was published with commentary by Bachet [2]. Via this example, we will motivate the later work of Mordell, Weil, and their eponymous theorem.

1.1 Fermat's right triangle theorem

The question that led to Fermat's "marginal" proof was one of the problems Bachet posed at the end of Diophantus' book VI. Bachet asked which rational numbers are areas of right triangles with rational sides. In modern parlance we call such possible areas *congruent numbers*. Bachet's question is known today as:

Question 1.1 (Congruent number problem)**.** Which rational numbers are congruent numbers?

Fermat addresses the special case of asking whether there are square congruent numbers, that is, whether there are rational right triangles with square area. Fermat's proof of this proposition is historically notable, as it is the only truly detailed proof he ever furnished with regards to number theory (appearing only in his personal notes, at that). This has lead some authors to call it "Fermat's one proof" [3].

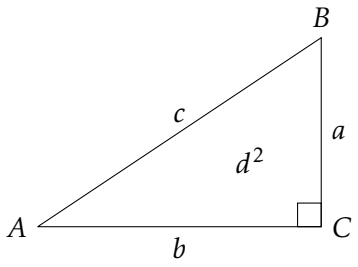

Figure 1: When does this occur for $a, b, c, d \in \mathbb{Q}$?

Theorem 1.2 (Right triangle theorem)**.** *There are no rational right triangles with square area.*

Remark. Fermat boldly writes:

> *"Hoc nempè demonſtrandi genus miros in arithmeticis ſuppeditabit progreſſus, ſi area trianguli eſſet quadratus darentur duo quadratoquadrati quorum differentia eſſet quadratus."*

The first phrase is Fermat stating that that his demonstration would enable "extraordinary developments to be made in the theory of numbers" [4]. The second phrase begins his proof, stating that if a rational right triangle with square area existed, it would give two fourth-powers whose difference is a square; that is, a *non-trivial solution* (a solution with no zeros) to the equation $x^4 - y^4 = z^2$.

One deduces this as follows: it is well-known that we can scale a rational right triangle to a similar *primitive right triangle* whose sides a, b, c are relatively prime and can be written in terms of coprime m, n such that

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

where $m > n$ and m, n are not both odd (otherwise a, b, c are all even). Passing to a primitive triangle preserves the condition of having a square area, as scaling the sides by $\lambda \in \mathbb{Q}$ scales the area by λ^2.

Either way, we want a rational d such that

$$d^2 = \frac{1}{2}ab = mn(m^2 - n^2).$$

Therefore, in the case of the primitive triangle d is also an integer. The coprimality of m, n implies that the factors on the right are square. Therefore, there exist relatively prime positive integers p, q, r such that

$$m = p^2, \quad n = q^2, \quad m^2 - n^2 = r^2.$$

The last equation becomes

$$p^4 - q^4 = r^2,$$

showing that (p, q, r) is a non-trivial solution to $x^4 - y^4 = z^2$. To prove the theorem, it suffices to show that no such solutions exist for this new equation, giving a contradiction. To do this, Fermat performs "descent" on the equation.

Fermat's proof (with details). If there were a rational right triangle with square area, then $x^4 - y^4 = z^2$ would have a non-trivial *primitive solution* of positive integers (p, q, r) with p, q

coprime and of opposite parity. Factoring gives $(p^2 - q^2)(p^2 + q^2) = r^2$. Since the factors are also coprime, there exist coprime s, t with

$$p^2 - q^2 = s^2, \quad p^2 + q^2 = t^2.$$

It follows that s, t are odd, and that $t^2 = s^2 + 2q^2$. This gives

$$\left(\frac{t+s}{2}\right)\left(\frac{t-s}{2}\right) = \frac{1}{2}q^2$$

where the factors on the left are also coprime. The left side is an integer, so q was even, giving $4 \mid q^2$ and implying one of the coprime factors is also even. Dividing by 2 gives

$$\left(\frac{t \pm s}{2}\right)\left(\frac{t \mp s}{4}\right) = \left(\frac{q}{2}\right)^2$$

where the choice of sign depends on which factor was originally even. Thus, there exist odd coprime u, v with

$$\frac{t \pm s}{2} = u^2, \quad \frac{t \mp s}{4} = v^2.$$

Then $\pm s = u^2 - 2v^2$, $t = u^2 + 2v^2$, and $q = 2uv$ (take the square root of our factorization). Finally,

$$p^2 = q^2 + s^2 = (2uv)^2 + (u^2 - 2v^2)^2 = u^4 + 4v^4.$$

Thus, $(u^2, 2v^2, p)$ is a primitive right triangle as the sides are relatively prime, with an area u^2v^2 that is square. By the Remark, such a triangle (via parameterization with coprime m', n') induces another primitive solution (p', q', r') to $x^4 - y^4 = z^2$, where

$$p' < p'^4 + q'^4 = m'^2 + n'^2 = p.$$

(where m', n' are defined as in the Remark). Therefore, repeating this entire procedure produces a strictly decreasing sequence $p > p' > p'' > \cdots$, which contradicts the well-ordering principle (there is a least positive integer in the sequence). Thus, our original assertion that $x^4 - y^4 = z^2$ has a non-trivial solution is false, and we conclude there is no rational right triangle with square area. □

Interestingly, this proof is rarely reproduced as-is. It is often modified to directly tackle the following corollary instead [3]:

Corollary 1.3 (Fermat's Last Theorem, $n = 4$)**.** *There are no non-trivial integer solutions to*

$$x^4 + y^4 = z^4.$$

Proof. Suppose (a, b, c) were a non-trivial integer solution to $x^4 + y^4 = z^4$. Then

$$a^4 + b^4 = c^4 \implies c^4 - b^4 = (a^2)^2,$$

making (c, b, a^2) a solution to $x^4 - y^4 = z^2$ and contradicting Fermat's right triangle theorem. □

1.2 Points on elliptic curves

It was Descartes and Fermat who pioneered the viewpoint of analytic geometry, and from this perspective, one views rational solutions to the equation $x^4 - y^4 = z^2$ as points on that surface whose coordinates are in $\mathbb{Q}$. However, it is more natural to view them as curves in the 2-dimensional weighted projective space $\mathbb{P}^2_{[1,1,2]}$ with coordinates $[x, y, z]$. This identifies the non-zero triples of solutions that are the same up to weighted scaling; for example, $[1, 0, 1] \equiv [3, 0, 9] \in \mathbb{P}^2_{[1,1,2]}$.

Let us reconcile this with Fermat's proof. Define

$$C = \left\{[x, y, z] \in \mathbb{P}^2_{[1,1,2]} : x^4 - y^4 = z^2\right\}, \quad \hat{C} = \left\{[x, y, z] \in \mathbb{P}^2_{[1,1,2]} : x^4 + 4y^4 = z^2\right\}.$$

We write $C(K)$ and $\hat{C}(K)$ to restrict ourselves to equivalence classes of points arising from when $x, y, z \in K$, where K is a number field. Fermat's implicit appeal to a primitive solution is the statement that for any $[p, q, r] \in C(\mathbb{Q})$, there exist $p^*, q^*, r^* \in \mathbb{Z}$ with p^*, q^*, r^* coprime such that

$$[p, q, r] \equiv [p^*, q^*, r^*] \in C.$$

Thus, Fermat's argument involves making a passage

$$[p, q, r] \in C \longrightarrow [u, v, p] \in \hat{C} \longrightarrow [p', q', r'] \in C,$$

which he describes in terms of primitive solutions $(p^*, q^*, r^*), (u^*, v^*, p^*)$, etc., that represent these underlying equivalence classes in $\mathbb{P}^2_{[1,1,2]}$. His argument is that one cannot keep going from $[p, q, r]$ to $[p', q', r']$ ad infinitum, as the coordinates of these primitive representatives would get "too small." This implies there were no such point $[p, q, r] \in C$ to begin with, giving the contradiction.

In fact, both $C, \hat{C}$ are elliptic curves. To see this, we *dehomogenize* their equations (formally, we restrict to the open subvariety $y \neq 0$). This involves choosing a different representative

$$[p, q, r] \equiv \left[\frac{p}{q}, 1, \frac{r}{q^2}\right] \in C,$$

which exists under the assumption $q \neq 0$. These representatives satisfy

$$x^4 - 1 = z^2, \quad x^4 + 4 = z^2,$$

as can be seen by taking $y = 1$ in the equations of $C, \hat{C}$ respectively. One might already recognize these as elliptic curves in Jacobi quartic form.

More convincingly, we can transform these curves to their more familiar Weierstrass equations. Inspired by [5, §III.D], we take $z \mapsto z + x^2$ to get

$$z^2 + 2x^2 z + 1 = 0, \quad z^2 - 2x^2 z - 4 = 0.$$

We now *homogenize* these equations as if we were in the $y \neq 0$ subvariety of a regular $\mathbb{P}^2$ space. This gives

$$yz^2 - 2x^2z + y^3 = 0, \quad yz^2 - 2x^2z - 4y^3 = 0.$$

Dehomogenizing into the open subvariety where $z \neq 0$ gives

$$y - 2x^2 + y^3 = 0, \quad y - 2x^2 - 4y^3 = 0.$$

Taking $x \mapsto \frac{1}{4}y$, $y \mapsto \frac{1}{2}x$, and multiplying the equations by 8 produces

$$y^2 = x^3 + 4x, \quad y^2 = -4(x^3 - x).$$

Finally, working (without loss of generality) in complex projective space lets us take $y \mapsto 2iy$ to turn the latter into $y^2 = x^3 - x$.

Let $E, \hat{E}$ denote the elliptic curves

$$E : y^2 = x^3 + 4x, \quad \hat{E} : y^2 = x^3 - x.$$

By our sequence of transformations, the non-trivial solutions on $C, \hat{C}$ give points on the affine parts of $E, \hat{E}$ respectively. We get a schematic of the type

$$\begin{array}{ccccc} [p,q,r] \in C & \longrightarrow & [u,v,p] \in \hat{C} & \longrightarrow & [p',q',r'] \in C \\ \downarrow & & \downarrow & & \downarrow \\ (a_1,a_2) \in E & \dashrightarrow & (b_1,b_2) \in \hat{E} & \dashrightarrow & (a_1',a_2') \in E \end{array}$$

where the dashed arrows represent indicate an implicit passage of points.

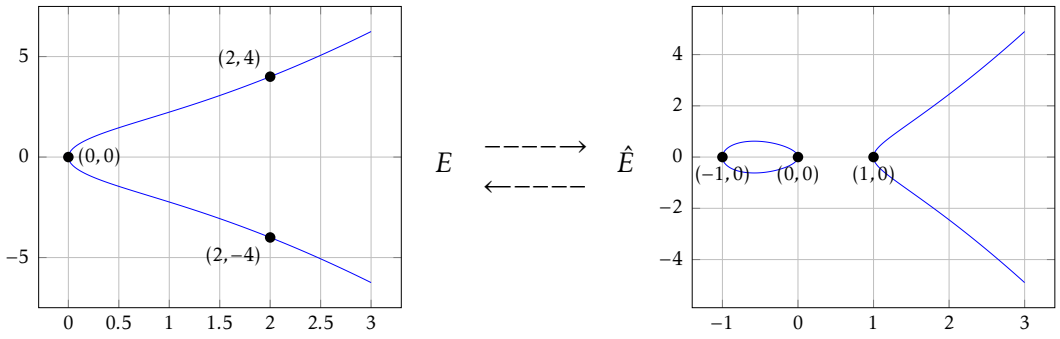

Figure 2: The curves E and $\hat{E}$ drawn over $\mathbb{R}$, along with some rational points

If we trace our transformation from the equations of C to the equations of E, we get the following maps:

$$[p,q,r] \in C \longmapsto (a_1,a_2) = \left(\frac{2q^2}{p^2+r}, \frac{4pq}{p^2+r}\right) \in E,$$
$$(a_1,a_2) \in E \longmapsto [p,q,r] \equiv \left[a_2, 2a_1, 8a_1 - a_2^2\right] \in C.$$

Likewise, for $\hat{C}$ and $\hat{E}$ we get:

$$[u,v,p] \in \hat{C} \longmapsto (b_1,b_2) = \left(\frac{2v^2}{u^2+p}, \frac{8iuv}{u^2+p}\right) \in \hat{E},$$
$$(b_1,b_2) \in \hat{E} \longmapsto [u,v,p] \equiv \left[\frac{b_2}{2i}, 2b_1, 8b_1 - \left(\frac{b_2}{2i}\right)^2\right] \in \hat{C}.$$

Furthermore, if we correspond the base points $[1,0,1] \in \mathbb{P}^2_{[1,1,2]}$ and $[0,1,0] \in \mathbb{P}^2$, and we correspond the 2-torsion points $[1,0,-1] \in \mathbb{P}^2_{[1,1,2]}$ and $(0,0) = [0,0,1] \in \mathbb{P}^2$, then our maps extend to elliptic curve isomorphisms $C \cong E$ and $\hat{C} \cong \hat{E}$.

We will now turn our schematic "backwards" with the following observation: When we passed from $[p,q,r]$ to $[u,v,p]$ and so forth in Fermat's proof, we always took positive roots and defined our primitive solutions as accordingly, as this made sense in the context of right triangles. However, from the viewpoint of passing between projective curves, this was an arbitrary choice. For example, we could take $[p,q,r]$ to $[u,v,p]$ or $[u,-v,p]$, where the latter two are not equivalent in $\mathbb{P}^2_{[1,1,2]}$

In this way, the passage $C \to \hat{C} \to C$ required, at each stage, a choice between two points. (Note: this choice is distinct from choosing which of $\frac{t\pm s}{2}$ was even, which was needed more for keeping the argument in the integers.) This suggests a more natural viewpoint: each stage is actually a degree-2 map in the *opposite* direction. That is,

$$[p,q,r] \in C \xleftarrow{\psi} [u,v,p] \in \hat{C} \xleftarrow{\phi} [p',q',r'] \in C.$$

Fermat's descent argument is actually passing from a point P to a point in its preimage under these maps. The fact that ϕ, ψ are 2-isogenies can be verified by noting that these opposite maps are describable as (weighted) homogeneous equations involving squares.

1.3 From infinite descent to Mordell-Weil

It is quite revealing to examine the net effect of these maps from the perspective of the Weierstrass models. That is, let us explicitly write out the composite map:

$$(a_1',a_2') \in E \xrightarrow{\sim} [p',q',r'] \in C \xrightarrow{\phi} [u,v,p] \in \hat{C} \xrightarrow{\psi} [p,q,r] \in C \xrightarrow{\sim} (a_1,a_2) \in E,$$

Using the substitutions from the previous sections, one gets:

$$\begin{aligned} a_1 &= \frac{2q^2}{p^2+r} = \frac{8u^2v^2}{(u^4+4v^4)-(u^2-2v^4)(u^2+2v^4)} = \frac{u^2}{v^4} = \frac{r'^2}{p'^2q'^2} \\ &= \frac{(8a_1'-a_2'^2)^2}{(a_2')^2(2a_1')^2} = \frac{(8a_1'-(a_1'^3+4a_1))^2}{(a_1'^3+4a_1)(2a_1')^2} = \frac{(4-a_1'^2)^2}{4(a_1'^3+4a_1')} \\ &= \frac{a_1'^4-8a_1'^2+16}{4a_1'^3+16a_1'}. \end{aligned}$$

This is the doubling formula for the x-coordinate of the Weierstrass model [5, §III.4]! Solving for a_2 in terms of a_1', a_2' will also give the doubling formula for the y-coordinate of the Weierstrass model (which also gives $y = \infty$ at the appropriate points, namely the 2-torsion points $a_2 = 0$). We conclude that

$$\psi \circ \phi = [2]_E,$$

and therefore ϕ, ψ are dual 2-isogenies. This will be the last time we make reference to $\hat{C}$ in this chapter; however, observe that we could have started with $\hat{C}$ and proceeded accordingly. We will revisit the existence of this *dual curve* in Chapter 4.

This remarkable correspondence allows us to comprehensively view Fermat's proof as an argument on elliptic curves:

- Fermat's passage from $[p,q,r] \in C(\mathbb{Q})$ to $[p',q',r'] \in C(\mathbb{Q})$ generalizes as going from a point $P \in E(K)$ to a specific choice (out of up to four) for $\frac{1}{2}P \in E(K)$, its preimage under the $\psi \circ \phi = [2]_E$ map. This preimage is guaranteed to be non-empty if we were working over $\mathbb{C}$ or $\overline{\mathbb{Q}}$. Fermat's proof notes that working with non-trivial solutions suffices to allow the passage for $K = \mathbb{Q}$. From the elliptic curve viewpoint, the passage is fine as long as P is not in $E(K)/2E(K)$ (equivalence classes of points which are not "doubles" of points in $E(K)$).

- Fermat notes that $|p| \geq |p'|$ holds for primitive solutions (p,q,r) and (p',q',r'), with strict inequality if the solutions are non-trivial. If one wanted to work over other number fields K and arbitrary projective varieties, there exists a representative-independent generalization known as the Weil height, which we shall encounter next chapter. For now, it suffices to note that a "primitive representative" exists when working with points over $\mathbb{Q}$.

- The passage of P to $\frac{1}{2}P$ produces a sequence of points of decreasing "size". When P is non-trivial, then $\frac{1}{2}P$ is non-trivial and distinct from the rest of the sequence, as the decreasing is strict under this condition. However, given a constant K, only finitely many points have "size" at most K (in this case, at most $2K+1$ points). Taking sizes is what allows us to apply the well-ordering principle, which gives Fermat's contradiction.

In this way, Fermat essentially showed that non-trivial points on $C(\mathbb{Q})$ do not exist. What about trivial points? We can enumerate these by substituting $x = 0$, $y = 0$, and $z = 0$, and from this one gets a finite number of possibilities:

- $x = 0$: This gives $-y^4 = z^2$, which has no solutions over $\mathbb{Q}$.
- $y = 0$: This gives $x^4 = z^2$, which gives $[1, 0, 1]$ and $[1, 0, -1]$ in $C(\mathbb{Q})$.
- $z = 0$: This gives $x^4 - y^4 = 0$, which gives $[1, 1, 0]$ and $[1, -1, 0]$ in $C(\mathbb{Q})$.

In all, we conclude that

$$C(\mathbb{Q}) = \{O = [1, 0, 1], [1, 0, -1], [1, 1, 0], [1, -1, 0]\}.$$

Passing to $E(\mathbb{Q})$, these points respectively become

$$E(\mathbb{Q}) = \{O = [0, 1, 0], (0, 0), (2, 4), (2, -4)\}.$$

Furthermore, the duplication formula (geometrically, taking the other intersection point after drawing tangents on the Weierstrass curve, then reflecting over the x-axis) shows that $(2, 4), (2, -4) \in E[4]$ map via $[2]_E$ to the 2-torsion point $(0, 0) \in E[2]$, which maps via $[2]_E$ to the point at infinity, O.

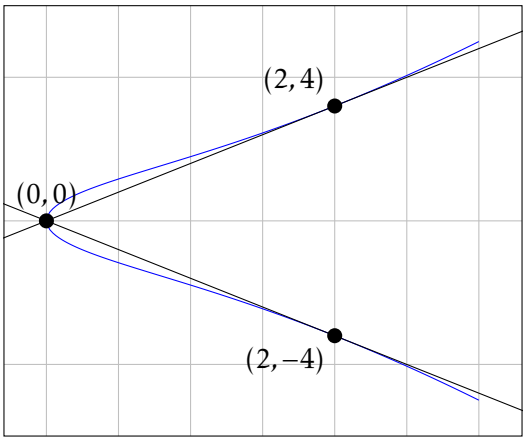

Figure 3: Torsion points in $E(\mathbb{Q})$; tangents give the $[2]_E$ map from $(2, \pm 4)$ to $(0, 0)$

If one further checks the additive structure, one concludes that

$$C(\mathbb{Q}) \cong E(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}.$$

Where do the obstructions to a passage of the form P to $\frac{1}{2}P$ over $\mathbb{Q}$ occur? Taking the quotient with $2E(\mathbb{Q})$ gives

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z},$$

corresponding to the points $(2,4)$, $(2,-4)$, whose preimages under $[2]_E : E \to E$ do not have rational coordinates.

To summarize: from Fermat's perspective we have fully solved the Diophantine equation $x^4 - y^4 = z^2$. From our perspective, we have fully solved for the variety $E(\mathbb{Q})$ where $E : y^2 = x^3 + 4x$. Where does one go from here? If one were Louis Mordell, one realizes that Fermat's technique is not intrinsic to the choice of elliptic curve equations $x^4 - y^4 = z^2$ or $y^2 = x^3 + 4x$. Rather, one can go further and make structural claims about the groups $E(\mathbb{Q})/2E(\mathbb{Q})$ and $E(\mathbb{Q})$ in general via a similar strategy [6]. Furthermore, if one were André Weil, one realizes that the "size" construction can be generalized to arbitrary number fields K (and in fact, from elliptic curves to abelian varieties in general) [9], broadening the scope of these structural results.

Here is how the remainder of the article will proceed:

- *Chapter 2:* We formalize the concept of a point's "size" using the *Weil height*. Under the assumption that $E(K)/2E(K)$ is finite, we prove the *Mordell-Weil theorem*, which states that $E(K)$ is finitely generated.
- *Chapter 3:* Using concepts from algebraic number theory, we prove the *weak Mordell-Weil theorem*, which states that $E(K)/mE(K)$ for all $m \geq 2$.
- *Chapter 4:* We overview the strategies of *complete 2-descent* and *descent by 2-isogeny*, whereby one can explicitly solve for $E(\mathbb{Q})/2E(\mathbb{Q})$ and thus $E(\mathbb{Q})$ in some cases, via dual curves like $\hat{C}$.

As we finish this introductory chapter, recall that Fermat's right triangle theorem is just one special case of the congruent number problem, which remains unsolved. Interestingly, there is a result known as Tunnell's theorem which can test whether a given number is congruent; however, it assumes the famous unproven conjecture of Birch and Swinnerton-Dyer, which relates the *rank* of $E(K)$ (see Chapter 2) to a specific *L-function* on E [8]. In all, the surprising relationship between areas of triangles and elliptic curves is undergirded by correspondences between Diophantine equations and curves, like the ones we saw here.

2 Heights and the Mordell-Weil theorem

In Fermat's elliptic curve, we took integral representatives with relatively prime coordinates and implicitly defined a well-defined "size" function

$$f([x,y,z]) : C(\mathbb{Q}) \to \mathbb{Z}_{\geq 0} \subseteq \mathbb{R}, \quad [x,y,z] \mapsto |x|,$$

which we used to derive a contradiction regarding the structure of $C(\mathbb{Q}) \subseteq \mathbb{P}^2_{[1,1,2]}(\mathbb{Q})$, for our choice of C (equivalently, $E(\mathbb{Q}) \subseteq \mathbb{P}^2$ for our choice of E). Specifically, we used it to

deduce that there is no infinitude of points in $E(\mathbb{Q})$ when $E : y^2 = x^3 + 4x$. We say that $E(\mathbb{Q})$ has *rank 0* or is *torsion*. However, this is not true in general; the argument that worked before might fail in general since the repeated passage of P to $\frac{1}{2}P$ could terminate at some element of $E(K)/2E(K)$ that does not represent a torsion point. This is a self-consistent state of affairs that did not occur when E was Fermat's curve.

The upside is that this suggests that representatives for $E(K)/2E(K)$ can be used to help generate all of $E(K)$. This intuition is formalized by the descent theorem in the next section. Of course, this is useful only if $E(K)$ is a finitely generated abelian group. Our ultimate goal is to prove the Mordell-Weil theorem, which asserts that this is case.

2.1 The descent theorem

There are certain properties that we would like to require of our "size" functions, to make them useful in justifying the existence of a finite basis for $E(K)$. The following axiomatic treatment is based on [7, §VIII.3]:

Definition 2.1. An *additive height function* is a map $h : A \to \mathbb{R}$ from an abelian group A satisfying the following properties:

a) For any $Q \in A$, there exists a dependent constant $C_1(Q)$ such that for all $P \in A$,

$$h(P + Q) \leq 2h(P) + C_1.$$

b) There exists an integer $m \geq 2$ and a constant C_2 such that for all $P \in A$,

$$h(mP) \geq m^2 h(P) + C_2.$$

c) For every constant C_3, the set

$$\{P \in A : h(P) \leq C_3\}$$

is finite.

It turns out that these properties suffice to ensure that the argument of finite-generation that we want to make on $A = E(K)$ by appealing to $E(K)/2E(K)$ will succeed. Explicitly:

Proposition 2.2 (Descent theorem)**.** *Let h be an additive height function on A, and let $m \in \mathbb{Z}$ be the number for which Property (b) is satisfied. If the group A/mA is finite, then A is finitely generated.*

Proof. Let $\{Q_1, \ldots, Q_s\} \in A$ represent the elements of A/mA. For arbitrary $P \in A$, we want P's difference from some linear combination of Q_i's to be the multiple of a point whose height is smaller than an independent constant. Hence, every P would be linear dependent on the Q_i and the finitely many points with height less than the constant.

With this in mind, note that for any $P \in A$ we can construct a sequence $P = P_0, P_1, \ldots$ via

$$P_{i-1} = mP_i + Q_{j_i}.$$

This gives an associated sequence of points $Q_{j_1}, Q_{j_2}, \ldots$. From this we get

$$h(P_i) \leq \frac{h(mP_i) + C_2}{m^2} = \frac{h(P_{i-1} - Q_{j_1}) + C_2}{m^2} \leq \frac{2h(P_{i-1}) + \max_{1\leq k\leq s} C_1(Q_k) + C_2}{m^2}$$

where the inequalities follow from Properties (b) and (a) respectively. Expanding the recursive formula up to any n gives

$$P = P_0 = m^n P_n + \sum_{i}^{n} m^{i-1} Q_{j_i}.$$

Repeated application of the inequality gives

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\max_{1\leq k\leq s} C_1(Q_k) + C_2\right) \sum_{\ell=1}^{n} \frac{2^{\ell-1}}{m^{2\ell}} \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{\max_{1\leq k\leq s} C_1(Q_k) + C_2}{m^2 - 2} \\ &\leq 2^{-n} h(P) + \left(\max_{1\leq k\leq s} C_1(Q_k) + C_2\right), \end{aligned}$$

since $m \geq 2$. Then for large n,

$$h(P_n) \leq 1 + \max_{1\leq k\leq s} C_1(Q_k) + C_2.$$

From our formula for P_0, we conclude that P is a linear combination of

$$\{Q_1, \ldots, Q_s\} \cup \left\{Q \in A : h(Q) \leq 1 + \max_{1\leq k\leq s} C_1(Q_k) + C_2\right\}.$$

The right-hand side of the inequality is independent of Q, so by property (c) this set is finite. Hence, A is finitely generated. □

Sadly, the function f is not the general additive height function we desire. After all, the definition of being an additive height function encapsulates the properties that are sufficient for the descent theorem to hold, not the necessary ones. Our hope is that there exists a function similar to f, defined on $A = E(K)$, which plays the "same role" but more immediately so (by satisfying the axioms of an additive height function and making the descent theorem applicable).

2.2 Weil heights

To construct such a function, we begin by borrowing from f the same idea of passing to a "primitive representative". This gives a well-defined function from projective space over $\mathbb{Q}$ to $\mathbb{R}$:

Definition 2.3. The *(Weil) height on* $\mathbb{P}^n(\mathbb{Q})$ is given by

$$H_{\mathbb{Q}} : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}, \quad [x_0, \ldots, x_n] \mapsto \max_{0 \le i \le n} |x_i|,$$

which is well-defined upon passing to a "primitive representative", i.e., taking

$$x_0, \ldots, x_n \in \mathbb{Z}, \quad \gcd(x_0, \ldots, x_n) = 1.$$

One views this as a type of generalization for f: taking the maximum over all the coordinates instead of just the first makes $H_{\mathbb{Q}}$ work more uniformly over all of rational projective space, not just on some $C(\mathbb{Q})$ where taking the primitive's first coordinate happened to suffice.

How do we generalize this construction to an arbitrary number field K? Simply put, the idea of looking for a "primitive representative" falls apart when one loses unique factorization. This encourages us to look for a more representative-independent approach. Since we are hoping to define a "size", our natural instinct is to look to the normalized valuations introduced by passing to a (number) field extension. See [1, §2] for an introduction to valuation theory, which gives the following concepts:

Definition 2.4. The *normalized valuations on* K, written M_K, are the set of valuations that restrict on $\mathbb{Q}$ to either the regular (archimedean) absolute value $|\ |_\infty$, or to one of the (multiplicative, non-archimedean) p-adic valuations $|\ |_p$.

Definition 2.5. Let $v \in M_K$. The *completion of* K *with respect to* v, written K_v, is given by taking the completion of K as a metric space with respect to v. One verifies by continuity that this is a field.

Definition 2.6. Let $v \in M_K$. The *local degree at* v is given by

$$n_v = [K_v : \mathbb{Q}_v].$$

One verifies this is well-defined by proving that a number field $K/\mathbb{Q}$ induces the finite field extension $K_v/\mathbb{Q}_v$.

With these definitions in hand, we can now define the following "size" function:

Definition 2.7. The *Weil height on* $\mathbb{P}^n(K)$ is given by

$$H_K : \mathbb{P}^n(K) \to \mathbb{R}, \quad [x_0, \ldots, x_n] \mapsto \prod_{v \in M_K} \left(\max_{0 \le i \le n} v(x_i) \right)^{n_v}.$$

Homogeneous coordinates are equivalent under scaling by some λ. However, since M_K is the set of normalized valuations, the product formula from valuation theory gives

$$\prod_{v \in M_K} v(\lambda)^{n_v} = 1.$$

This implies that the Weil height is well-defined on $\mathbb{P}^n(K)$.

In a sense, the Weil height takes the maximum over all the coordinates, across the valuations of K. This is similar to our definition for $H_{\mathbb{Q}}$, and in fact conservatively extends it! To see why this and the earlier definition for $H_{\mathbb{Q}}$ coincide, take $P \in \mathbb{P}^n(\mathbb{Q})$ and consider a primitive representative as before, with $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$.

If $v \in M_{\mathbb{Q}}$ we have $v = |\,|_p$ for some p, or $v = |\,|_\infty$. Since the coordinates are relatively prime, no prime divides all the x_i and hence $\max_{0 \le i \le n} v(x_i) = 1$ in the former case. The latter case gives the

$$H_{\mathbb{Q}}(P) = \max_{0 \le i \le n} v(x_i) = \max_{0 \le i \le n} |x_i|_\infty$$

definition that we saw earlier.

One more thing: in valuation theory, discrete valuations give us the choice of working additively or multiplicatively. In defining the Weil height, we have chosen the multiplicative convention for reasons of familiarity (e.g., the regular absolute value is multiplicative). However, we will actually be using the additive version in our work:

Definition 2.8. The *additive Weil height on* $\mathbb{P}^n(K)$ is given by

$$h_K(P) = \log H_K(P).$$

The reason we want this formulation is that our goal is to pass from the (additive) Weil height to an additive height function on $E(K)$. The properties chosen to characterize additive height functions rely on the addition structure of $\mathbb{R}$ (hence the name). For example, Property (a) compares $h(P+Q)$ and $2h(P)$, as opposed to comparing $h(P+Q)$ and $h(P)^2$. The deeper reason for this choice is that under the additive formulation, h is "almost" a quadratic form, which we will not explore here (cf. *canonical height* in [5, §IV.5]).

2.3 The Mordell-Weil theorem

Finally, from algebraic geometry or complex analysis, one recalls that a function f in the function field of E/K naturally defines a surjection $f : E \twoheadrightarrow \mathbb{P}^1$ by assigning $[1,0]$ to the poles (and $[f(P), 1]$ elsewhere). Using this notation, we can finally define our desired function:

Definition 2.9. The *additive height on E* (relative to K) is given by

$$h_{E(K)}(P) = h_K(x(P))$$

where x denotes the x-coordinate of P, as dependent on a choice of Weierstrass equation.

Unlike the Weil heights, this is not a canonically-defined function. However, it is at least a function that can be easily evaluated (after choosing one's equation). Proving that $h_{E(K)}$ is an additive height function requires a number of non-trivial but elementary steps [7, §VIII.5-6], which we summarize here:

- *Properties (a) and (b):* These follow from manipulating the Weierstrass equation, its addition formula, the fact that $x(P)$ is an even function, and that morphisms do not change the Weil height "too much."
- *Property (c):* This follows from the Weil heights H_K having the same property, i.e., height-bounded sets have finite cardinality. It is easy to see this for $H_{\mathbb{Q}}$, for which

  $$\#\{P \in \mathbb{P}^n(\mathbb{Q}) : H_{\mathbb{Q}} \leq C\} \leq (2C+1)^{n+1}$$

  is a bound. For general K, a technical argument is required. It involves viewing the homogeneous coordinates of P as the coefficients of a polynomial, and then bounding the height of P in terms of the heights of the polynomial's roots.

We combine our results to prove the Mordell-Weil theorem, conditional on the weak Mordell-Weil theorem in the next chapter:

Theorem 2.10 (Mordell-Weil theorem)**.** *The group $E(K)$ is finitely generated.*

Proof. Note that $h_{E(K)}$ is an additive height function for $A = E(K)$ with $m = 2$. The weak Mordell-Weil theorem, which we will prove in the next chapter, asserts that $E(K)/2E(K)$ is finite. By the descent theorem, $E(K)$ is finitely generated. □

Can we say anything more about $E(K)$? By the Mordell-Weil theorem, we can write

$$E(K) \cong E_{\text{tors}}(K) \times \mathbb{Z}^r.$$

where r is the rank of $E(K)$. That is,

Definition 2.11. The *rank* of an elliptic curve over K is the dimension of the torsion-free part of $E(K)$.

Solving for the rank r is generally an intractable problem. However, we will see in the next two chapters that working in $E(K)/mE(K)$, especially with the case $K = \mathbb{Q}$ and $m = 2$, can ultimately lead to effective results (in the same way it did for $E : y^2 = x^3 + x$).

3 The weak Mordell-Weil theorem

In the previous chapter, we encountered the quotient group $E(K)/mE(K)$ when we encoded Fermat's infinite descent argument into the descent theorem. This led us to prove the Mordell-Weil theorem, which is conditional on the following non-trivial result:

Theorem 3.1 (Weak Mordell-Weil theorem)**.** *Let E/K be an elliptic curve. The group $E(K)/mE(K)$ is finite.*

Mordell's 1922 proof used explicit formulas (namely, the group law on the Weierstrass cubic) to specifically resolve the $m = 2$, $K = \mathbb{Q}$ case [6]. Instead, we will take advantage of Kummer theory and global field theory (with ideas from cohomology hidden in the background) to prove the more general result.

3.1 The Kummer pairing

The following approach is motivated by Kummer theory, which studies *Kummer extensions* of K (a concise reference is [1, §III]). This is the situation where K contains the m-th roots of unity for some m, and then one takes the field extension L/K whose Galois group is abelian and whose elements' orders divide m (i.e., $G_{L/K}$ has *exponent* m). These extensions turn out to be exhausted by the extensions which adjoin m-th roots to K.

Notation 3.2. Let $\overline{K}$ denote the algebraic closure of K. Let $K^{1/m}$ denote K adjoined with all its m-th roots in $\overline{K}$.

In Kummer theory, there is a natural pairing

$$K^\times \times G_{\overline{K}/K} \to \mu_m, \quad (a, \sigma) \mapsto \sqrt[m]{a}^\sigma / \sqrt[m]{a}.$$

which is independent of the choice of square root of a. If one takes the extension $K^{1/m}$ of all m-th roots of K, checking the kernels on the left and right shows that one gets the perfect bilinear pairing

$$K^\times/K^{\times m} \times G_{K^{1/m}/K} \to \mu_m, \quad (a, \sigma) \to \sqrt[m]{a}^\sigma / \sqrt[m]{a}.$$

By *perfect*, we mean that the partial evaluation maps induced by fixing a term in one of the factors are actually isomorphisms. For example, one gets the isomorphism

$$K^\times/K^{\times m} \xrightarrow{\sim} \mathrm{Hom}(G_{\overline{K}/K}, \mu_m),$$

which states that all homomorphisms $G_{\overline{K}/K} \to \mu_m$ are of the form $\sigma \mapsto \beta^\sigma/\beta$, for some $\beta \in \overline{K}^\times$ with $\beta^m \in K^\times$. This is an instance of Hilbert's Theorem 90, which generalizes this result.

There is an analogous construct on elliptic curves. However, to define it we need to assume that $E[m] \subseteq E(K)$, in the same way that K needed to contain the m-th roots of unity. Under this assumption, we make the following definition:

Definition 3.3. The *Kummer pairing* is given by

$$\kappa : E(K) \times G_{\overline{K}/K} \to E[m], \quad (P, \sigma) \mapsto Q^\sigma - Q.$$

where $Q \in E(\overline{K})$ satisfies $P = [m]Q$ (i.e., P is the m-multiple of some Q in the algebraic closure).

The difference with this new pairing, however, is that the kernel on the right will not be $G_{\overline{K}/K^{1/m}}$. The following, more restrictive extension will play the role of $K^{1/m}$:

Notation 3.4. Let $K^\dagger = K([m]^{-1}E(K))$ denote the extension that adjoins (the coordinates of) all the points $Q \in E(\overline{K})$ such that $[m]Q \in E(K)$.

With this object defined, it turns out that our Kummer pairing has similar properties to the original pairing from Kummer theory:

Proposition 3.5. *The Kummer pairing κ is well-defined and bilinear. Its kernel on the left is $mE(K)$, and its kernel on the right is $G_{\overline{K}/K^\dagger}$.*

Finally, why can we assume that $E[m] \subseteq E(K)$? This is because we can always take a sufficiently large K and use the following result:

Lemma 3.6 (Reduction lemma)**.** *Let E/K be an elliptic curve and L/K a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is finite.*

Proofs for the Kummer pairing's properties and this reduction lemma can be found in [7, §VIII.1]. One could examine these proofs, or if one is familiar with Galois cohomology, one could note that these proofs are just manual explications of properties of the Kummer exact sequence. Either way, it follows that the induced pairing

$$E(K)/mE(K) \times G_{K^\dagger/K} \to E[m]).$$

is perfect, which gives the isomorphism

$$\delta_{K^\dagger} : E(K)/mE(K) \xrightarrow{\sim} \mathrm{Hom}(G_{K^\dagger/K}, E[m]).$$

This suggests the following strategy of proving the weak Mordell-Weil theorem: if $K^\dagger/K$ is finite, then since $E[m] \cong \mu_m \times \mu_m$ is finite, this isomorphism $\delta_{K^\dagger}$ lets us conclude that $E(K)/mE(K)$ is finite as well. However, the definition of $K^\dagger/K$ is dependent on the coordinates of $E(K)$. Meanwhile, the extension of all m-th roots $K^{1/m}/K$ is certainly not finite.

The ideal strategy involves taking an extension L/K that is guaranteed to extend $K^\dagger/K$, while remaining a finite extension. Then $\delta_{K^\dagger}$ would extend to the injection

$$\delta_L : E(K)/mE(K) \rightarrowtail \mathrm{Hom}(G_{L/K}, E[m])$$

where the codomain is still finite.

The beauty of these δ-maps is that our work has now passed into the realm of algebraic number theory (Galois groups of number field extensions), which we will now use to construct an L with the desired properties.

3.2 The role of algebraic number theory

We overview some results that should be familiar from a first course in class field theory. The statements and their developments can be found in [1, §1-2]. K always denotes a number field.

Definition 3.7. Let S be a finite set of (multiplicative) valuations that include the Archimedean valuations. The *ring of S-integers* is

$$\mathcal{O}_{K,S} := \{b \in K : v(b) \geq 0 \text{ for all } v \in M_K - S\} \subseteq K.$$

The *group of S-units* are the multiplicative elements in the ring of S-integers:

$$\mathcal{O}_{K,S}^{\times} := \{b \in K : v(b) = 0 \text{ for all } v \in M_K - S\} \subseteq K^{\times}.$$

Theorem 3.8 (Dirichlet S-unit theorem)**.** *The abelian group of S-units is finitely generated. It is the direct sum of a finite cyclic group and a free abelian group of rank $\#S - 1$.*

Note that these are natural generalizations of more well-known results (taking S to be trivial, i.e., strictly the Archimedean valuations, gives the regular ring of integers, the regular units, and the regular Dirichlet unit theorem respectively).

Notation 3.9. We fix the following notation:

$$K(S,m) = \{b \in K^{\times}/K^{\times m} : \operatorname{ord}_v(b) \equiv 0 \pmod{m} \text{ for all } v \in M_K - S\},$$

$$K^S/K = \begin{cases} \text{The maximal abelian extension of } K \text{ with exponent} \\ m \text{ which is unramified outside of } S. \end{cases}$$

It turns out that for an appropriate choice of S, we will have $L = K^S$ as the extension that let us complete the proof of the weak Mordell-Weil theorem. First, we show that K^S/K is finite. This hinges on the following lemma:

Lemma 3.10. *If $\mathcal{O}_{K,S}$ is a principal ideal domain (PID), then $K(S,m)$ is finite.*

Proof. Consider the group homomorphism

$$\mathcal{O}_{K,S}^{\times} \to K(S,m)$$

induced by the quotient map $K^{\times} \to K^{\times}/K^{\times m}$. To show it is a surjection, let $b \in K^{\times}$ represent an element of $K(S,m)$. Then $b\mathcal{O}_{K,S}$ is the m-th power of an ideal of $\mathcal{O}_{K,S}$. Since $\mathcal{O}_{K,S}$ is a PID, this implies $b\mathcal{O}_{K,S} = r^m\mathcal{O}_{K,S}$. Hence $b = ur^m$ for some S-unit $u \in \mathcal{O}_{K,S}^{\times}$. Modulo $K^{\times m}$, $a \equiv u$ and so $u \in \mathcal{O}_{K,S}^{\times}$ gives b.

Furthermore, the kernel of the map contains $\mathcal{O}_{K,S}^{\times m}$, and so we get the further surjection

$$\mathcal{O}_{K,S}^{\times}/\mathcal{O}_{K,S}^{\times m} \twoheadrightarrow K(S,m).$$

By Dirichlet's S-unit theorem, we know that $\mathcal{O}_{K,S}^{\times}$ is finitely generated, making the quotient group finite. This surjection shows that $K(S,m)$ is finite. □

Proposition 3.11. *K^S/K is a finite extension for all K.*

Proof. We follow [7, VIII.1.6]:

- Let K'/K be a finite extension, and suppose the proposition were true for K'; that is, $K'^{S'}/K'$ is finite for S' (which here, we take to be the set of valuations that restrict to S). Then $K^S K'/K'$ is abelian with exponent m and unramified outside of S', which means it is a finite extension. Hence K^S/K is also finite. Thus, we can assume we are working in a larger field where $\mu_m \subseteq K$ (this is analogous to the reduction lemma).
- Likewise, we can work with a larger $S' \supseteq S$, as this gives $K^{S'}/K^S/K$. Since the class number of S is finite, we can add a finite number of elements to make a larger S' where $\mathcal{O}_{K,S'}$ is a principal ideal domain. One could further enlarge S' so that $v(m) = 0$ for all $v \in M_K - S'$.
- From Kummer theory, we know that $K^{S'}$ is a subfield of $K^{1/m}$; in fact, it is the largest one under the the constraint of being unramified outside of S'. For $v \in M_K - S'$, consider $X^m - a = 0$ over the local field K_v. Under the assumption $v(m) = 0$, then $K_v(\sqrt[m]{a})/K_v$ is unramified exactly when $\mathrm{ord}_v(b) \equiv 0 \pmod{m}$.

Hence

$$K^{S'} = K(\{\sqrt[m]{a} : a \in K(S', m)\}).$$

Since $K(S', m)$ is finite by our previous lemma, then $K^{S'}/K$ is a finite field extension and so is our original K^S/K. □

3.3 Proof of the main result

We now pass back to the context of elliptic curves. Namely, we were working with $E(K)$, which gave us the associated, coordinate-dependent field extension $K^\dagger/K$. As outlined earlier, our goal was to find a finite extension L containing $K^\dagger$. We finish by concluding that $K^S/K^\dagger/K$ is always a tower of extensions; this follows from the following proposition:

Proposition 3.12. *$K^\dagger/K$ is an abelian extension with exponent m that is unramified outside S, where*

$$S = \{v \in M_K : v \text{ is Archimedean, or } E \text{ has bad reduction at } v, \text{ or } v(m) \neq 0\}$$

is a finite set.

Having exponent m follows from our earlier perfect Kummer pairing, which gives the isomorphism

$$G_{K^\dagger/K} \xrightarrow{\sim} \mathrm{Hom}(E(K)/mE(K), E[m]).$$

Regarding to being unramified on S, we have not yet discussed what is meant by a good or a bad reduction. Let $v \in M_K$ and call its uniformizer π. Given a minimal Weierstrass equation, reduce the coefficients of E/K modulo π. If the resulting curve $\tilde{E}/(K/\pi K)$ is non-singular, we say E has *good reduction* at v. For us, it will suffice to say that almost all v give good reductions, so we expect S to be finite. The full proof of our proposition can be found in [7, VIII.1.5].

In all we must conclude that K^S, being the maximal abelian extension with the same property, extends $K^\dagger$ as desired. We summarize our argument as follows:

Proof of weak Mordell-Weil. We want $E(K)/mE(K)$ to be finite. Given K, the reduction lemma shows it suffices to assume $E[m] \subseteq E(K)$. Using this we constructed our Kummer pairing on $E(K)$, which gave the isomorphism $E(K)/mE(K) \cong \mathrm{Hom}(G_{K^\dagger/K}, E[m])$. To show finiteness, it sufficed to view this as a injection into a larger codomain $\mathrm{Hom}(G_{L/K}, E[m])$ that is also finite. Choosing $L = K^S$ works, as we have shown it is also a finite extension. Hence $E(K)/mE(K)$ is finite by the isomorphism. □

Moving forward, we now have the injection

$$\delta_E : E(K)/mE(K) \rightarrowtail \mathrm{Hom}(G_{K^s/K}, E[m]).$$

To conclude this chapter, we observe that our approach now gives us perspective to prove some explicit results. For example:

Proposition 3.13 (Quantitative weak Mordell-Weil)**.** *Suppose $E[m] \subseteq E(K)$ and let $\mathcal{H}_K$ denote the ideal class group of K. Then*

$$rk_{\mathbb{Z}/m\mathbb{Z}} E(K)/mE(K) \leq 2(\#S + rk_{\mathbb{Z}/m\mathbb{Z}} \mathcal{H}_K[m]).$$

Proof. This follows from examining our proof that K^S/K is a finite extension for all K. There, we constructed a larger set S' so that $v(m) = 0$ for all $v \in M_K - S'$. To ensure this, we needed to add the $\mathrm{rk}_{\mathbb{Z}/m\mathbb{Z}} \mathcal{H}_K[m]$ generators of $\mathcal{H}_K[m]$ to S. We have the further injection

$$E(K)/mE(K) \rightarrowtail \mathrm{Hom}(G_{K^s/K}, E[m]) \rightarrowtail \mathrm{Hom}(G_{K^{s'}/K}, E[m]).$$

Take the $\mathbb{Z}/m\mathbb{Z}$-rank of the domain and the codomain. To do this, recall that $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Finally, Dirichlet's S-unit theorem states that $\mathcal{O}_{K,S'}^\times$ has $\mathbb{Z}$-rank $S' - 1$. However, the finite cyclic group gives us a $\mathbb{Z}/m\mathbb{Z}$-rank of S' for the quotient $\mathcal{O}_{K,S'}^\times / \mathcal{O}_{K,S'}^{\times m}$. Hence

$$\mathrm{rk}_{\mathbb{Z}/m\mathbb{Z}} E(K)/mE(K) \leq (\mathrm{rk}_{\mathbb{Z}/m\mathbb{Z}} E[m]) \cdot (1 + (\#S' - 1)) = 2(\#S + \mathrm{rk}_{\mathbb{Z}/m\mathbb{Z}} \mathcal{H}_K[m])$$

as desired. □

A result like this can be elevated to bounds on the rank of $E(K)$ itself in some cases. For example [5, IV.4.19]:

Theorem 3.14. *Suppose $E(\mathbb{Q})$ has full 2-torsion (its Weierstrass equation has integer roots r_1, r_2, r_3). Then the rank r of $E(\mathbb{Q})$ is bounded by*

$$r \leq n_1 + 2n_2 - 1,$$

where n_1 is the number of primes dividing one of $r_1 - r_2$, $r_2 - r_3$, $r_3 - r_1$, and n_2 is the number of primes dividing all of these differences.

4 Computing $E(K)/2E(K)$

From Kummer theory, we saw that

$$K^\times/K^{\times m} \xrightarrow{\sim} \mathrm{Hom}(G_{\overline{K}/K}, \mu_m),$$

is an isomorphism. Hidden inside this is the restricted isomorphism

$$K(S,m) \xrightarrow{\sim} \mathrm{Hom}(G_{K^s/K}, \mu_m).$$

Finally, since $E[m] \cong \mu_m \times \mu_m$, we can compose with the injection from the end of last chapter to conclude there exists an injection

$$E(K)/mE(K) \rightarrowtail \mathrm{Hom}(G_{K^s/K}, E[m]) \cong K(S,m) \times K(S,m),$$

where the latter isomorphism is fixed by a choice of generators T_1, T_2 for $E[m]$ as a module. If the injection is specified by a pair of functions f_{T_1}, f_{T_2}, then to see if a point

$$(b_1, b_2) \in K(S,m) \times K(S,m) \subseteq K^\times/K^{\times m} \times K^\times/K^{\times m}$$

originates from $E(K)/mE(K)$, then we want to solve

$$b_1 z_1^m = f_{T_1}(P), \quad b_2 z_2^m = f_{T_2}(P)$$

for $z_1, z_2 \in K^\times$ and $P \in E(K)$.

While we have shown that an injection into $K(S,m) \times K(S,m)$ exists for all m (under the assumption $E[m] \subseteq E(K)$), the case $m = 2$ in conjunction with a Weierstrass equation is particularly special. To see why, note that we can always factor the right side over $\overline{K}$ as

$$E/\overline{K} : y^2 = (x - r_1)(x - r_2)(x - r_3),$$

with no repeated roots (as that would imply a singular point). Recalling the group law, it is clear that $(r_1, 0), (r_2, 0), (r_3, 0) \in E[2]$. Since the point at infinity $O \in E[2]$ as well, it follows that we have exhausted the points in $E[2] \cong \mu_2 \times \mu_2$. Therefore, as long as $E[2] \subseteq E(K)$, we must have $r_1, r_2, r_3 \in K$.

4.1 Complete 2-descent

This explicit description of the 2-torsion points as coordinates is encouraging with respect to deducing a formula for the injection. In the notation of the previous section, it turns out that taking $T_1 = (r_1, 0)$, $T_2 = (r_2, 0)$, and defining $f_{T_i}(P) = x(P) - r_i$ describes the following choice of injection:

Proposition 4.1 (Complete 2-descent)**.** *The map*

$$\delta : E(K)/2E(K) \to K(S,2) \times K(S,2)$$

given by

$$(x,y) \mapsto \begin{cases} (x - r_1, x - r_2) & \text{if } x \neq r_1, r_2 \\ \left(\frac{r_1 - r_3}{r_1 - r_2}, r_1 - r_2\right) & \text{if } x = r_1 \\ \left(r_2 - r_1, \frac{r_2 - r_3}{r_2 - r_1}\right) & \text{if } x = r_2 \\ (1,1) & \text{if } x = \infty \text{ (i.e., } P = O\text{)} \end{cases}$$

is an injective homomorphism.

This is an exercise in algebraic manipulation [7, X.1.4]. Ultimately, this suggests the following strategy of solving for $E(K)/2E(K)$:

- By factoring the discriminant Δ, one can deduce S and thus $K(S,2)$.
- One then examines the possible tuples $(b_1, b_2) \in K(S,2) \times K(S,2)$ and asks which ones have a preimage in $E(K)/2E(K)$.
- This is done by solving the system of equations

  $$b_1 z_1^m = f_{T_1}(P), \quad b_2 z_2^m = f_{T_2}(P)$$

  under the constraint of being in $E(K)$ (a third equation).
- These determine a variety known as a *principal homogeneous space*.
- Finding a K-rational point on this variety is possible as long as the Hasse principle holds (i.e., finding K_v-rational points over all v gives a K-rational point).
- However, this is not always true. Here, objects like the *Selmer group* and the *Tate-Shafarevich group* come into play to quantify the "extent" to which the Hasse principle fails.

Does this suffice to tackle the case of $E : y^2 = x^3 + 4x$ that we saw in the first chapter? Somewhat. Over $\mathbb{Q}$, we have

$$E/\mathbb{Q} : y^2 = x(x^2 + 4)$$

as the best factorization available to us (hence $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ only). Of course, passing to the extension $\mathbb{Q}(i)/\mathbb{Q}$ gives

$$E/\mathbb{Q}(i) : y^2 = x(x - 2i)(x + 2i)$$

and therefore we get $E[2] \subseteq E(\mathbb{Q}(i))$. While rather unnatural, one could prove Fermat's theorem by proving that $E(\mathbb{Q}(i))$ has rank 0 in this manner (enumerating the elements of $E(K)/2E(K)$ using the procedure outlined above) and showing they are torsion). However, having to pass to a splitting field is in general, a losing proposition.

4.2 Descent by 2-isogeny: Fermat revisited

If we recall our elliptic curve "translation" of Fermat's right triangle proof, note that we observed the back-and-forth passage between

$$E : y^2 = x^3 + 4x, \quad \hat{E} : y^2 = x^3 - x$$

via dual 2-isogenies ϕ and ψ. Although we had collapsed the two maps into $\psi \circ \phi = [2]_E$ and used that to prove $E(\mathbb{Q})$ is finite, imagine if instead we had collapsed the maps as $\phi \circ \psi = [2]_{\hat{E}}$ and proceeded thusly. Certainly, we would have reached the same conclusion of finiteness for $\hat{E}(\mathbb{Q})$, and then $E(\mathbb{Q})$ again. The difference is that here, $\hat{E}$ does split over $\mathbb{Q}$ as $x^3 - x = x(x - 1)(x + 1)$, saving us work when applying techniques like complete 2-descent.

Motivated by this final revisit of Fermat's proof, it turns out that the strategy of complete 2-descent can actually be viewed as a specialization of the more general strategy known as descent by 2-isogeny. The idea is that in some cases, the multiplication isogeny

$$E(K) \xrightarrow{[2]} E(K)$$

implicit in the complete 2-descent nicely decomposes into

$$E(K) \xrightarrow{\phi} \hat{E}(K) \xrightarrow{\hat{\phi}} E(K)$$

where $\hat{\phi} \circ \phi = [2]_E$, i.e., into the composition of some 2-isogeny ϕ and its dual.

Before, the object of interest was $E(K)/2E(K)$, which we can think of as the cokernel of the $[2]_E$ isogeny. Now, the objects of interest are the cokernels $\hat{E}(K)/\phi(E(K))$ and $E(K)/\hat{\phi}(E(K))$.

This time, we have two injective homomorphisms (they decompose the single injective homomorphism into $K(S,2)\times K(S,2)$ that occurred in the $E(K)/2E(K)$ case):

$$\delta : \hat{E}(K)/\phi(E(K)) \to K(S,2),$$
$$\hat{\delta} : E(K)/\hat{\phi}(\hat{E}(K)) \to K(S,2).$$

How does this connect back to our original goal of solving for $E(K)/2E(K)$? What happens now is similar to the complete 2-descent case. If one did have a curve E, since we are working with 2-torsion points, we hope that we can transform E to some Weierstrass equation that is obviously 2-isogenous to some other curve $\hat{E}$, such that both δ and $\hat{\delta}$ have explicit formulas as well!

This seems implausible at first glance, but it turns out that the assumption $E(K)[2] \neq \emptyset$ gives a sufficient restriction for this happen. Then, we can transform E to an equivalent model where one of the 2-torsion points is at $(0,0)$. Hence we can assume E has the equation

$$E : y^2 = x^3 + ax^2 + bx.$$

One can verify that

Proposition 4.2. *Let $E : y^2 = x^3 + ax^2 + bx$. Then the curve*

$$\hat{E} : y^2 = x^3 + \hat{a}x^2 + \hat{b}x$$

with $\hat{a} = -2a$ and $\hat{b} = a^2 - 4b$ is 2-isogenous with E via the dual isogenies

$$\phi : E \to \hat{E}, \quad (x,y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right)$$
$$\hat{\phi} : \hat{E} \to E, \quad (x,y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(b-x^2)}{8x^2}\right).$$

This gives the two 2-isogenous curves. The injections look like, e.g.,

$$\delta : \hat{E}(K)/\phi(E(K)) \to K(S,2), \quad (x,y) \mapsto \begin{cases} a^2 - 4b & \text{if } x = 0 \text{ (i.e., P = (0,0))} \\ 1 & \text{if } x = \infty \text{ (i.e., P = O)} \\ x & \text{otherwise.} \end{cases}$$

Once more, one retrieves a similar strategy: examine the discriminant Δ to deduce S and thus the two copies of $K(S,2)$. One then tries to solve for which points have a preimage in $\hat{E}(K)/\phi(E(K))$ (or $E(K)/\hat{\phi}(\hat{E}(K))$ as appropriate). Again, this requires checking whether the principal homogeneous spaces that arise have K-rational points, which may not always be possible.

As a final note, take E as above with $a = 0$ and $b = 4$. Then $\hat{E}$ has coefficients $\hat{a} = 0$ and $\hat{b} = -16$. Hence

$$E : y^2 = x^3 + 4x, \quad \hat{E} : y^2 = x^3 - 16x$$

are 2-isogenous curves with isogenies and injections described as above. A projective transformation $x \mapsto 4x$ and $y \mapsto 8y$ shows that without loss of generality, $\hat{E} : y^2 = x^3 - x$. Hence $E, \hat{E}$ are our original pair of curves in Chapter 1.

In this method of descent by 2-isogeny, we find a *computational* generalization of Fermat's proof of the right triangle theorem. Along the way we encountered plenty of 20th-century mathematics, via heights, Mordell and Weil, glimpses of cohomology, and hints of unsolved mathematical problems. They all arise from this bridge that we have built from Fermat's world into the contemporary study of elliptic curves.

"Extraordinary developments," indeed.

5 Bibliography

[1] J. W. S. Cassels and Frohlich A. *Algebraic number theory: proceedings of an instructional conference*. Thompson Book Co., 1967.

[2] Leonard E. Dickson. *History of the theory of numbers*, volume 2. Carnegie Institution of Washington, 1919.

[3] Harold M. Edwards. *Fermat's last theorem: a genetic introduction to algebraic number theory*. Springer, 1996.

[4] Thomas Little Heath and Leonhard Euler. *Diophantus of Alexandria: a study in the history of Greek algebra*. Dover Publications, 1964.

[5] Anthony W. Knapp. *Elliptic curves*. Princeton University Press, 1992.

[6] Louis Joel Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc Cam. Phil. Soc.*, 21:179–192, 1922.

[7] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[8] J. B. Tunnell. A classical diophantine problem and modular forms of weight 3/2. *Inventiones Mathematicae Invent Math*, 72(2):323334, 1983.

[9] André Weil. L'arithmétique sur les courbes algébriques. *Acta Mathematica Acta Math.*, 52(1):281315, 1929.