Elliptic Curves over p-adic Numbers

Zawad Chowdhury (zawadx@mit.edu)

18.784 Final Paper, Fall 2021

1 Introduction

Elliptic curves are one of the most well-studied objects in modern number theory. Their study lies at the intersection of algebraic number theory and algebraic geometry, and is the basis of rich theory in both fields. An insightful connection between elliptic curves and modular forms lies at the heart of Wiles's proof of Fermat's Last Theorem. Elliptic curves also have real world applications in elliptic curve cryptography and integer factorization. For an in-depth introduction to elliptic curves, see [4].

The p-adic numbers are analytic constructions, extending the rational numbers into a complete field $\mathbb{Q}_p$ using a different metric from the one we are used to (which produces $\mathbb{R}$). In a sense, $\mathbb{Q}_p$ captures all the modulo p power information about elements of $\mathbb{Q}$. This allows us to understand global properties of functions and objects by looking at their local properties in $\mathbb{Q}_p$ for all p. A wonderful introduction to the theory of p-adic numbers is provided in [1].

In this paper, we will study the group of solutions to an elliptic curve defined over $\mathbb{Q}_p$ (i.e. $\mathbb{Q}_p$ points on the curve). We can use these solutions to study the points on the curve defined over $\mathbb{Q}$, which has an isomorphism type that is hard to calculate. We explicitly calculate this group $E(\mathbb{Q}_p)$ in terms of the p-adic integers $\mathbb{Z}_p$, and the solutions to the elliptic curve over $\mathbb{F}_p$ (which is well understood). This leads to the following theorem:

Theorem 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}_p$, such that the corresponding curve $\tilde{E}$ with coefficients reduced into $\mathbb{F}_p$ is also an elliptic curve. Assume there exists a homomorphism $\tilde{E}(\mathbb{F}_p) \to E(\mathbb{Q}_p)$ which composed with the reduction map gives the identity on $\tilde{E}(\mathbb{F}_p)$. Then we have the group isomorphism*

$$E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \tilde{E}(\mathbb{F}_p).$$

Remark 1.2. *There are several details in the statement of the theorem which might be unclear for now, such as how the reduced elliptic curve is well defined for any elliptic curve over $\mathbb{Q}_p$. The statement is supposed to provide a brief overview for now, and more details will be fleshed out in the rest of the paper.*

1.1 Organization of the paper

This paper assumes familiarity with the theory of p-adic numbers. See [1] for an excellent introduction to the topic, as well as a reference for results. Properties of the p-adic valuation, the algebraic structure of $\mathbb{Z}_p$ and Hensel's lemma are used in this paper without prior introduction.

The paper does not assume familiarity with algebraic geometry and the theory of elliptic curves. Some background definitions are provided in section 2, describing plane curves (with their properties like singularities, genus) and the projective plane (with an introduction to Bezout's Lemma). Then, section 3 introduces elliptic curves, describing the group law and elliptic curves over finite fields.

Then we begin studying elliptic curves specifically over $\mathbb{Q}_p$. A key tool is the reduction map and the reduced elliptic curve $\tilde{E}$, which is introduced in section 4. Finally, section 5 describes some important subgroups of $E(\mathbb{Q}_p)$, which leads to a proof for Theorem 1.1.

2 Background: Projective Geometry and Plane Curves

Before we can begin working with elliptic curves, we must develop some understanding of plane curves in general, and the spaces they live in.

2.1 Plane Curves

Broadly speaking, over a field k *plane curves* are the subsets of k^2 comprised of solutions to equations of the form $f(x, y) = 0$. In algebraic geometry, we are interested in *algebraic* plane curves, where f is a polynomial. In the rest of this paper, we only work with algebraic plane curves and thus often omit the word algebraic.

Definition 2.1 (Plane Curve)**.** *Let $f(x, y) = \sum a_{ij}x^i y^j \in k[x, y]$ be a polynomial. Then the plane curve X is defined by the equation $f(x, y) = 0$. We*

define the degree of X to be the same as that of f.

While a plane curve X can be defined abstractly by some polynomial f, it is concretely realized by its k-points, which are the solutions in k to the equation $f(x, y) = 0$. The set of all such points is denoted $X(k)$.

Example 2.2. *We have a polynomial $y^2 - x^3$ which defines a plane curve E. The point $(0, 0)$ lies in $E(\mathbb{Q})$. Similarly, E' is defined by $y^2 - x^3 + x$ and both $(0, 0), (1, 0)$ lie in $E'(\mathbb{Q})$.*

We want to understand two properties of plane curves: its singularities and its genus.

Definition 2.3. *A plane curve X defined by the polynomial f is said to be* singular *at a point P, if $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are both 0 at the point P. A plane curve with no singular points is said to be* nonsingular *or* smooth.

Example 2.4. *Continuing from Example 2.2, E is singular at the point $(0, 0)$ but E' is not. In fact, E' has no singular points and thus is a smooth curve.*

Genus is more abstract as a concept, and so we do not provide a rigorous definition in this paper. Intuitively, if the field k is embedded in $\mathbb{C}$, one can think about the curve $X(\mathbb{C})$ which will be a compact Riemann surface. Then the topological genus of the surface, which you can think of as the number of holes, will equal the genus of the curve. See [2] for definitions of genus which work in general.

Genus is more abstract. For our purposes, we will define the genus of a plane curve X to be the topological genus of $X(\mathbb{C})$. Notably, $X(\mathbb{C})$ will be a compact Riemann surface, and thus this definition is well defined if k is embedded in $\mathbb{C}$. There are rigorous definitions of the genus of a curve which work in all cases, but we skip those in this paper.

Elliptic curves are smooth genus 1 projective plane curves. However, before we can discuss them, first we must understand what spaces such a curve would be defined over.

2.2 Affine and Projective Space

Definition 2.5 (Affine Space)**.** *Given a field k, the affine space $\mathbb{A}^n(k)$ is simply the set of points with n coordinates in k. Formally,*

$$\mathbb{A}^n(k) = \{(a_1, \ldots, a_n) | a_i \in k\}.$$

$\mathbb{A}^n(k)$ can be viewed as n copies of the field k.

Affine space is a good tool for visualization, but it has some algebraic deficiencies. As an example, you can define lines in affine space as solutions to the equation

$$c_0 + \sum_{i=1}^{n} a_i c_i = 0$$

for constants $c_i \in k$. Then it is not guaranteed that two lines will intersect at a point in $\mathbb{A}^n(k)$. This makes algebraic geometry difficult, as the theory would have to account for parallel lines and intersecting lines separately. We compactify $\mathbb{A}^n(k)$ to create a space that does not have this difficulty.

Definition 2.6 (Projective Space)**.** *Given a field k, the projective space $\mathbb{P}^n(k)$ is defined formally as*

$$\mathbb{P}^n(k) = (\mathbb{A}^{n+1}(k) - \{0\})/x \sim \lambda x.$$

Thus it is the set of coordinates $a = (a_0, a_1, \ldots, a_n)$, not all zero, where two tuples a and b are said to be the same if $a_i = \lambda b_i$ for some $\lambda \in k$. The equivalence class of a_i is written as $[a_0 : a_1 : \cdots : a_n]$.

The set $\mathbb{A}^n(k)$ is embedded into $\mathbb{P}^n(k)$ by $(a_1, \ldots, a_n) \mapsto [1 : a_1 : \cdots : a_n]$. The points in $\mathbb{P}^n(k)$ which do not come from this embedding are thus of the form $[0 : a_1 : \cdots : a_n]$. They form a copy of $\mathbb{P}^{n-1}(k)$. Thus we have the equality of sets:

$$\mathbb{P}^n(k) = \mathbb{A}^n(k) \sqcup \mathbb{P}^{n-1}(k) = \bigsqcup_{i=0}^{n} \mathbb{A}^i(k).$$

Note that if two points are in the same line through the origin, their coordinates will be a multiple of each other. Thus another way to interpret $\mathbb{P}^n(k)$ is as the space of lines through the origin in $\mathbb{A}^{n+1}(k)$. This interpretation highlights how projective space is produced by the compactification. Setting $a_0 = 1$, we obtain a hyperplane such that any point on the hyperplane lies on exactly one line through the origin. But this leaves all the lines which are parallel to the hyperplane, which represent intersection points of similarly oriented lines on the hyperplane.

We may now define curves in projective space.

Definition 2.7 (Projective Curve)**.** *Let $f(x, y, z) = \sum a_{ij}x^i y^j z^l \in k[x, y]$ be a homogenous polynomial, i.e. all of its terms have the same degree. Then the projective curve X associated with f is*

$$\{[x : y : z] \in P^2(k) | f(x, y, z) = 0\}.$$

A key result about projective curves is Bezout's Theorem, which generalizes our earlier notion that "any two lines have an intersection point":

Theorem 2.8 (Bezout's Theorem)**.** *Suppose k is an algebraically closed field. Let $F(x, y, z) = 0$ and $G(x, y, z) = 0$ be curves in $\mathbb{P}^2(k)$ of degree m and n respectively, with no nontrivial common factor. Then the curves intersect at exactly mn points, up to multiplicity.*

Corollary 2.9. *Let L be a line and E a plane curve of degree three over an algebraically closed field k. Then, taking multiplicities into account, L and E have three exactly intersection points.*

3 Elliptic Curves

We are now ready to dive into the theory of elliptic curves. But first, what is an elliptic curve?

Definition 3.1 (Elliptic Curve)**.** *An elliptic curve over a field k is a nonsingular projective genus 1 curve equipped with a k-rational point O. We always take O to be the point at infinity* $[0 : 1 : 0]$.

This definition is quite abstract, and so to concretely work with elliptic curves we often look at their defining equations. These are called *Weierstrass equations*, and have the following form:

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

with the $a_i \in k$. To create a projective curve, we look at the *projectivization* of the Weierstrass equation (i.e. homogenize it with a third variable):

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Notice that if (X, Y, Z) is a solution to the equation, then $(\lambda X, \lambda Y, \lambda Z)$ will be a solution too. Thus we can define solutions of the equation over $\mathbb{P}^2(k)$, and these solutions make up the elliptic curve $E(k)$.

Remark 3.2. *If k is a field of characteristic $p \neq 2, 3$, we can perform a change of coordinates to go from the full Weierstrass equation to one of the form*

$$y^2 = x^3 + Ax + B$$

and it can be shown that the curve is nonsingular if and only if a quantity $\Delta = -16(4A^3 + 27B^2)$ (called the discriminant*) is nonzero.*

3.1 Group Law of an Elliptic Curve

One of the most interesting properties about elliptic curves is that the set of rational points inherits an abelian group structure. Thus if E is an elliptic curve defined over field k, there exists a commutative "addition" operation $E(k) \times E(k) \to E(k)$. This operation can be defined geometrically by the following rules:

1. The distinguished point $O = [0 : 1 : 0]$ is the identity of the group. Geometrically, this is the point at infinity in the vertical direction (where two lines parallel to the y-axis meet).

2. By Theorem 2.9, any line L intersects E at three points P, Q, R (with multiplicity). When the line is defined over k, all of these points are in $E(k)$, and the *group law* states that $P + Q + R = O$.

Remark 3.3. *The group law determines the elliptic curve $E(k)$, and it is defined in terms of intersections of lines. Thus we can make a linear change in variables to x, y, and the resulting elliptic curve $E'(k)$ will be isomorphic to $E(k)$ as groups.*

Example 3.4. *Consider a point $P \in E(k)$ such that $P \neq O$. Then from the Weierstrass equation, we can see that the third coordinate of P is not zero, and thus P is a point on the plane curve. The vertical line through P thus passes through O, and therefore it intersects the curve at a third point $-P$.*

Example 3.5. *Consider the equation $y^2 = x^3 - 36x$. The projective closure of this equation $Y^2Z = X^3 - 36XZ^2$ can be checked to be nonsingular, and thus defines an ellliptic curve. One can easily find two solutions of this equation: $P = (0, 0)$, and $Q = (-2, 8)$. They both lie on the line $y = -4x$. Taking the third intersection of this line with the curve, we get a third point $R = (18, -72)$. Thus by the group law, $P + Q = -R = (18, 72)$.*

Consider the line $X = 0$. It intersects the curve at $[0 : 1 : 0] = O$ and $[0 : 0 : 1] = P$. The line is tangent to the curve at P, thus it has multiplicity

2. Thus we have $P + P + O = O$, or $2P = O$. Therefore P is a point of order 2 on this elliptic curve (also known as a 2-torsion point*).*

3.2 Elliptic Curves over Finite Fields

One interesting case for our exploration is when the field of definition of the elliptic curve is set to be the finite field $\mathbb{F}_q$. Recall the definition:

Definition 3.6. *The field $\mathbb{F}_q$ is the unique field of q elements. Such a field exists if and only if q is the power of a prime p. One can construct this field by fixing an algebraic closure of $\mathbb{F}_p$, and then taking the roots of the polynomial $x^q - x$.*

$E(\mathbb{F}_q)$ is a subset of $\mathbb{P}^2(\mathbb{F}_q)$, and thus it is a finite abelian group. The number of elements of this group is approximately q:

Theorem 3.7 (Hasse-Weil Bound)**.** *Let $\#E(\mathbb{F}_q)$ be the number of points in the elliptic curve $E(\mathbb{F}_q)$. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Using this bound, one can find an algorithm to compute the order of $E(\mathbb{F}_q)$ by finding the order of a generic element. This operation involves $O(\sqrt{q})$ operations. An algorithm of Schoof vastly improves this, computing $\#E(\mathbb{F}_q)$ in $O((\log q)^{O(1)})$ operations, which is polynomial in the number of digits of q. Thus it can calculate the value for $q \approx 2^{80}$ in a few seconds.

Example 3.8. *Let E be the elliptic curve $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_3$. By the Hasse-Weil bound, we have $2 \leq \#E(\mathbb{F}_q) \leq 10$. In fact, over $\mathbb{F}_3$ every element satisfies $x^3 = x = -2x$. Also, $y^2 = 1$ has two roots. Thus this elliptic curve has 6 solutions over $\mathbb{F}_3^2$. Including the point at infinity, we get 7 projective solutions. The group $E(\mathbb{F}_q)$ must be the only group of 7 elements, $\mathbb{Z}/7\mathbb{Z}$.*

Example 3.9. *Let E be the elliptic curve $y^2 = x^3 + 2x + 2$ over $\mathbb{F}_3$. Then there are no solutions to this equation besides the point at infinity, and thus $E(\mathbb{F}_3) = \{O\}$. The group is the trivial group.*

4 The Reduced Elliptic Curve

We now begin the study of elliptic curves defined over the p-adic numbers. An important tool in this endeavor is reduction modulo p.

For any element $x \in \mathbb{Z}_p$, taking the first digit of the p-adic expansion defines a natural reduction map which we call $x \pmod p$. In the rest of this paper, we use $\tilde{x}$ to refer to $x \mod p$ for $x \in \mathbb{Z}_p$.

Definition 4.1 (Reduced Elliptic Curve)**.** *Let E be an elliptic curve defined over $\mathbb{Q}_p$, with a Weierstrass equation whose coefficients are in $\mathbb{Z}_p$. Reducing every coefficient mod p, we obtain a new Weierstrass equation over $\mathbb{F}_p$, which we call the* reduced elliptic curve *and refer to by $\tilde{E}(\mathbb{F}_p)$.*

We can similarly reduce points in $\mathbb{P}^2(\mathbb{Q}_p)$.

Definition 4.2 (Reduction of a Point)**.** *Let $P \in \mathbb{P}^2(\mathbb{Q}_p)$ be a point. We can adjust coordinates to write $P = [x : y : z]$, where $x, y, z \in \mathbb{Z}_p$ and at least one is in $\mathbb{Z}_p^\times$. The reduction of P is then defined to be $\tilde{P} = [\tilde{x} : \tilde{y} : \tilde{z}] \in \mathbb{P}^2(\mathbb{F}_p)$.*

Now, if $P \in E(\mathbb{Q}_p)$ and E has a Weierstrass equation with coefficients in $\mathbb{Z}_p$, we have $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$. Thus the reduction map $\mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$ is well defined when restricted to a map $E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p)$.

Remark 4.3. *Based on the above discussion, we can only reduce elliptic curves with a Weierstrass equation with coefficients all in $\mathbb{Z}_p$. In fact, this is all elliptic curves defined over $\mathbb{Q}_p$! Consider the change of variables $(X, Y) = (u^{-2}x, u^{-3}y)$. This produces a Weierstrass equation with the coefficient a_i replaced by $u^i a_i$. Now, we can choose u such that $u^i a_i \in \mathbb{Z}_p$ for all i. Since this is a linear change in variables, we have a Weierstrass equation with coefficients all in $\mathbb{Z}_p$ for the original elliptic curve, which can thus be reduced mod p.*

5 Computing $E(\mathbb{Q}_p)$

Our main goal is to compute the structure of $E(\mathbb{Q}_p)$, as described in Theorem 1.1. In that theorem, the group splits into $\mathbb{Z}_p$ and $\tilde{E}(\mathbb{F}_p)$. Thus we expect the structure of $E(\mathbb{Q}_p)$ to come in part from the reduction mod p, and in part from some subgroup isomorphic to $\mathbb{Z}_p$ which does not contain information about reduction. We first study some subgroups which fit this bill.

5.1 Some key subgroups of $E(\mathbb{Q}_p)$ and $\tilde{E}(\mathbb{F}_p)$

Proposition 3.2.5 in [5] establishes an isomorphism between the nonsingular points on a degree three curve and the additive or multiplicative group of

the field of definition. Thus, we can define an abelian group

$$\tilde{E}_{ns}(\mathbb{F}_p) = \{P \in \tilde{E}(\mathbb{F}_p) \mid P \text{ nonsingular}\}.$$

We define E_0 to be the preimage of this group under the reduction map:

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \tilde{P} \in \tilde{E}_{ns}(\mathbb{F}_p)\}.$$

We hope to split E_0 into two: the part that carries information about its reduction into $\tilde{E}_{ns}$, and the part which doesn't. The latter must be trivial under the reduction map, which motivates the following definition:

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \tilde{P} = O\}.$$

To relate these three groups, we need a standard algebraic construction called an exact sequence.

Definition 5.1 (Exact Sequence)**.** *A sequence of groups $G_0, G_1, \ldots G_n$ with homomorphisms $f_i : G_{i-1} \to G_i$ for $i = 1, \ldots n$ is said to be* exact *at G_i if* $\operatorname{im} f_i = \ker f_{i+1}$. *The whole sequence*

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \ldots \xrightarrow{f_n} G_n$$

is said to be exact if it is exact at each G_i.

Example 5.2. *For the sequence $0 \to A \xrightarrow{f} B$, the image of the first map is $\{0\}$. Thus the sequence is exact if and only if* $\ker f$ *is trivial, i.e. if f is injective.*

Example 5.3. *For the sequence $A \xrightarrow{f} B \to 0$, all of B is in the kernel of the second map. Thus the sequence is exact if and only if* $\operatorname{im} f = B$*, i.e. if f is surjective.*

Exact sequences are relevant for us due to the following lemma.

Theorem 5.4 (Splitting Lemma)**.** *Consider a short exact sequence of abelian groups*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

If there exists a homomorphism $h : C \to B$ such that $g \circ h$ is the identity on C, then there is an isomorphism $B \cong A \oplus C$.

Proof. See [3] for the proof of the lemma in its full generality. □

Theorem 5.4 gives us a blueprint to relate E_0, E_1 and $\tilde{E}_{ns}$. Intuitively, reduction is like a quotient, and E_1 is the kernel of that quotient. This leads us to a key theorem.

Theorem 5.5. *The sequence*

$$0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \tilde{E}_{ns}(\mathbb{F}_p) \to 0$$

is exact, where the second map is inclusion and the third map is the reduction map.

Proof. First let us understand what it would mean for this sequence to be exact. First, all the maps must be group homomorphisms. Thus the exactness of the sequence would imply that the reduction map $E_0(\mathbb{Q}_p) \to \tilde{E}_{ns}(\mathbb{F}_p)$ is a group homomorphism. Note that this homomorphism would then have kernel $E_1(\mathbb{Q}_p)$. The kernel is a subgroup of the preimage, and thus the set inclusion $E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p)$ would also be a group homomorphism.

Now, set inclusions are naturally injective. This means we naturally have exactness at $E_1(\mathbb{Q}_p)$. Also, the image of this inclusion is by definition the kernel of the reduction map, giving us exactness at $E_0(\mathbb{Q}_p)$. Finally, for exactness at $\tilde{E}_{ns}(\mathbb{F}_p)$, we must show that the reduction map from E_0 is surjective.

Therefore, to prove the theorem it suffices to show that the reduction map $E_0 \to \tilde{E}_{ns}$ is a group homomorphism, and is surjective. The proofs of these facts are straightforward calculations, which we omit for brevity. The details can be found in 3.2.4 and 3.2.5 in [6], or in 7.2.1 in [5].

Once we show that the reduction map is a surjective group homomorphism, by the above discussion it follows that the sequence is exact. □

5.2 Proof of Theorem 1.1

We now try to understand the structure of the groups E_1 and $\tilde{E}_{ns}$, in an attempt to pinpoint the group $E(\mathbb{Q}_p)$.

Theorem 5.6. *Let E be an elliptic curve defined over $\mathbb{Q}_p$ for odd prime p. Then $E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$.*

Proof Sketch. We only do a brief sketch of the key ideas of the proof, as the details regarding formal groups are beyond the scope of this paper. Note that by Remark 4.3, we can find a Weierstrass equation for E with coefficients $a_i \in \mathbb{Z}_p$. Now, Section 4 of [5] develops the theory of formal groups of an

elliptic curves. It defines two power series $x(z), y(z)$ written in terms of the coefficients a_i, such that $(x(z), y(z))$ is a solution to the Weierstrass equation (formally, i.e. all the terms cancel). If we have $z \in p\mathbb{Z}_p$, then the power series $x(z), y(z)$ converge to values in $\mathbb{Q}_p$.

The group structure of the formal group shows that these power series also respect the group law. Thus any $z \in p\mathbb{Z}_p$ generates an element $x(z), y(z)$ of the formal group, which therefore is isomorphic to $p\mathbb{Z}_p$ as a group.

Following Proposition 4.2.2 in [5], we have an isomorphism between $E_1(\mathbb{Q}_p)$ and the formal group. Thus we conclude that $E_1(\mathbb{Q}_p) \cong p\mathbb{Z}_p$. But $\mathbb{Z}_p \cong p\mathbb{Z}_p$ as groups, and thus we have $E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$. □

Now, $\tilde{E}_{ns}$ consists of all the nonsingular points. If $\tilde{E}$ were itself an elliptic curve, we would have $\tilde{E}_{ns} = \tilde{E}$. In that case, since the reduction map is a surjective group homomorphism, we would also have $E_0 = E$. This is the case referred to in Theorem 1.1, which we are now ready to prove:

Theorem 5.7 (Restatement of Theorem 1.1)**.** *Let E be an elliptic curve defined over $\mathbb{Q}_p$, such that the corresponding curve $\tilde{E}$ with coefficients reduced into $\mathbb{F}_p$ (using Remark 4.3 if needed) is also an elliptic curve. Assume there exists a homomorphism $\tilde{E}(\mathbb{F}_p) \to E(\mathbb{Q}_p)$ which composed with the reduction map gives the identity on $\tilde{E}(\mathbb{F}_p)$. Then we have the group isomorphism*

$$E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \tilde{E}(\mathbb{F}_p).$$

Proof of Theorem 1.1. Since $\tilde{E}$ is non-singular, we have an exact sequence from Theorem 5.5:

$$0 \to \mathbb{Z}_p \to E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p) \to 0.$$

Here the equivalence $E_1 \cong \mathbb{Z}_p$ follows from Theorem 5.6. Now, by hypothesis we have a group homomorphism which is a right inverse to the reduction map. Then, by the Theorem 5.4, the exact sequence splits. Therefore, $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \tilde{E}(\mathbb{F}_p)$. □

The group $E(\mathbb{Q}_p)$ is a wildly infinite structure, which is a priori hard to understand. But Theorem 1.1 shows that in many cases, $E(\mathbb{Q}_p)$ has a representation in terms of two objects that are easier to understand. One is the ring $\mathbb{Z}_p$, which we can efficiently represent in terms of p-adic expansions (see [1] for details). The other is the group $\tilde{E}(\mathbb{F}_p)$, which is small by the Hasse-Weil Bound (Theorem 3.7). Therefore, this theorem provides a first step in building a richer understanding of the elliptic curve over p-adic numbers.

References

[1] Fernando Q Gouvêa. *p-adic Numbers - An Introduction*. Springer, 1997.

[2] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[3] Allen Hatcher. "Algebraic topology". In: (2005).

[4] Bjorn Poonen. "Elliptic curves". In: *Published online at http://math. mit. edu/ poonen* (2001).

[5] Joseph H Silverman. *The arithmetic of elliptic curves*. Springer, 2009.

[6] Rosa Winter. "Elliptic curves over Qp". In: *Universiteit Leiden* (2011).