Elliptic curves over p-adic numbers: Nagell-Lutz Theorem

Anqi Li

1 Where are we headed?

A significant part of "classical" number theory constitutes the study of Diophantine equations: solutions of polynomial equations in rationals (or equivalently, integers). For monovariate polynomials, such a question is fully resolved by the rational roots theorem; if $a_n x^n + \cdots + a_0 x_0 = 0$ has a rational solution p/q then $q \mid a_n$ and $p \mid a_0$. The upshot is that we have turned what was apriori an infinite problem of sorts into the checking of a finite number of possibilities. The natural next step would be to ask the same sort of questions for bivariate polynomials $f(x, y)$. Here the behavior becomes much more subtle. Let us begin with some easy cases. The degree 1 case of $f(x, y) = ax + by + c$ is sometimes known as "Chicken McNugget Theorem" where there are infinitely many solutions iff $c \mid \gcd(a, b)$. The degree 2 case turns out to also be resolvable fairly easily; such polynomials are conics, and their solutions can be described via geometry. The first interesting case, as it turns out, is when we start to try to solve degree 3 bivariate polynomial equations over rationals; more tellingly, equations such as $y^2 = x^3 + ax + b$ is what is known as the short Weierstrass form of elliptic curves.

Although much is still unknown about elliptic curves, we do have a characterization of the number of rational points on elliptic curves. In fact, we have an algorithm for obtaining all such rational points: given a set of generators we can obtain any rational point on an elliptic curve E by successively intersecting, for finitely many times, tangents and chords between the points already identified with the elliptic curve. This fact was first proven by Mordell, and Weil extended the argument from $\mathbb{Q}$ to all number fields in general.

Theorem 1 (Mordell-Weil Theorem)**.** *Let E be an elliptic curve defined over a number field K. Then the group of K-valued points $E(K)$ is a finitely generated Abelian group. Thus, $\mathbb{E}(K) \simeq \mathbb{Z}^r \oplus T$ where T is the finite torsion subgroup.*

For the rest of the paper we will work in the setting of $K = \mathbb{Q}$ for simplicity. There are some technical details we have yet to unpack, namely the Mordell-Weil theorem only makes sense and is interesting if we can give a group law on $E(\mathbb{Q})$ to make it into an Abelian group. This will be further discussed in the next section. For now, we move on with the main idea for the proof of the theorem.

(a) First, we prove the *weak Mordell-Weil theorem*, which states that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite for any positive integer m. As part of this step, we will show that the torsion points of $E(\mathbb{Q})$ is finite.

(b) Next, we study the heights of points on the curve; vaguely heights is the measure of the "size" of a point. Using the machinery of heights, we can prove that there are not too many 'small' points. Along with a descent argument from $E(\mathbb{Q})/mE(\mathbb{Q})$, we can conclude that $E(\mathbb{Q})$ is finitely generated.

We will not be able to prove the Mordell-Weil theorem in this article, and will instead focus on (a). It will turn out that one of the reasons for studying elliptic curves over $\mathbb{Q}_p$ is to characterize the torsion points on an elliptic curve. The aim of this paper is to investigate torsion points and prove the following theorem.

Theorem 2 (Nagell-Lutz Theorem). *The group of rational torsion points on an elliptic curve $E(\mathbb{Q})$ is finite. If $(x, y) \neq \mathcal{O}$ is a point of finite order, then $x, y \in \mathbb{Z}$.*

We will give a high-level sketch, and should therefore be taken with a grain of salt, of a roadmap for this note. The idea is to instead study the kernel of $E(\mathbb{Q}_p)$ under a well-defined reduction map to $E(\mathbb{F}_p)$. It turns out that if we have a torsion point with order coprime to p, then we end up getting a torsion of the same order in $E(\mathbb{F}_p)$. Since $E(\mathbb{F}_p)$ is a finite group, this makes it possible to calculate and identify the torsion points. By looking at different values of p, we are able to derive restrictions on the order of the torsion group of $E(\mathbb{Q})$ and in fact even obtain a precise result classifying torsion points as in Theorem 2.

Outline. Section 2 is intended to be a brief crash course on elliptic curves, which sets the stage for analyzing the group structure on $E(\mathbb{Q})$. In section 3, we talk about the operation of the reduction map to $E(\mathbb{F}_p)$ as mentioned above. The key point is that this reduction is a group homomorphism and preserves the group structure. In section 4, we prove that $E_1(\mathbb{Q}_p)$ is torsion-free by introducing the p-adic filtration on $E_1(\mathbb{Q}_p)$. It turns out that it is easier to handle points with order coprime to p, but we will be able to boost our result to the general setting. Finally, we soup everything up in section 5 and give a proof of the Nagell-Lutz theorem.

Acknowledgements. This paper was written as part of MIT's 18.784 (Seminar in Number Theory). We would like to express our gratitude towards Tony Feng for his suggestion of the topic as well as references. Additionally, we would also like to thank Mark Jabbour and Tristan Shin for their comments and suggestions on a draft version of this paper.

2 A brief primer on elliptic curves

In this section, we recall some basic facts about elliptic curves that we will need. For a more detailed discussion, we refer the reader to the textbooks cited in the references ([Cas95], [ST15] and [Sil09]) or Prof. Drew Sutherland's 18.783 lecture notes. An abstract definition of elliptic curve is the following.

Definition 1. An *elliptic curve* is a non-singular projective curve of genus 1 with a distinguished point.

We will give a more explicit equivalent definition of elliptic curve which we will work with for the rest of the paper. But we will begin by explaining some key terms in the abstract definition above, because it sets up the groundwork for what is to come.

We begin by defining the projective plane and projective curves. We work with the projective plane instead of the more familiar affine plane $\mathbb{A}^2(k) = \{(x, y) : x, y \in k\}$ because it is in some sense more "complete".

Definition 2.

$$\mathbb{P}^2 = \mathbb{P}^2(k) = \{(a, b, c) : a, b, c \in k, (a, b, c) \neq (0, 0, 0)\}/\sim$$

where we are modding out by the equivalence $\sim$ with $(a, b, c) \sim (a', b', c')$ iff there exists some $t \in \mathbb{C}^*$ such that $a = ta', b = tb'$ and $c = tc'$. We will write the equivalence class of a point as $(a : b : c)$.

We will think of $(x : y : 1)$ as affine points since these form a copy of $\mathbb{A}^2(k)$ embedded in $\mathbb{P}^2(k)$. The points $(x : y : 0)$ are thought of as the points at infinity.

Definition 3. A *projective curve* C of degree d over k is a homogeneous degree d polynomial $f \in k[x, y, z]$. The k-rational points of C (with corresponding homogeneous polynomial f) is given by the set $C(k) = \{(x : y : z) \in \mathbb{P}^2(k) : f(x, y, z) = 0\}$.

Definition 4. A point $P \in C(k)$ is *singular* if $\partial f/\partial x$, $\partial f/\partial y$ and $\partial f/\partial z$ all vanish at P. We say that C is *non-singular* if there are no singular points in $C(\overline{k})$.

It turns out that we work with genus 1 curves, because genus 0 ones correspond to quadratic forms which we already know how to characterize via Hasse-Minkowski theorem and the like. But instead of defining what a genus is, we will unwind the definition and use the following explicit description of an elliptic curve for the rest of this note.

Definition 5. An *elliptic curve* over a field k is a non-singular projective curve where the corresponding homogenous polynomial is given by

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$$

with $a_1, \ldots, a_6 \in k$. The unique point at infinity is given by $\mathcal{O} = (0 : 1 : 0)$.

Remark 1. Although we have defined an elliptic curve this way, in many texts a more abstract definition is used and one then shows that any elliptic curve can be put in the form given in the definition, which is known as the *Weierstrass equation*.

We will be working with elliptic curves over $\mathbb{Q}$, which we will study by considering the local fields $\mathbb{Q}_p$. Both of these have characteristic 0. In the context of characteristic 0, the following reduction will be convenient.

Definition 6. When the characteristic of the field we are working with is not 2 or 3, it turns out that elliptic curves can be written as a *short Weierstrass equation* of the form $y^2z = x^3 + axz^2 + bz^3$.

We will thereafter primarily work with the short Weierstrass equation form of elliptic curves. We will often work with the *dehomogenization* of the elliptic curve by intersecting with an affine plane; effectively we will treat $z = 0$ as the line at infinity, so that on the affine patch we work with $z \neq 0$. Besides the point $\mathcal{O}$ which is a point at infinity, on this affine patch the elliptic curve can be written in the form $y^2 = x^3 + ax + b$ which is much easier to work with. In what follows, when we specify an affine point on an elliptic curve, we will interchangeably write (x, y) and $(x : y : 1)$ depending on the context.

Remark 2. In fact, the relative convenience of being able to work with short Weierstrass equation is why we choose to stay in the specific instance of $\mathbb{Q}_p$ rather than following Silverman's treatment in [Sil09, Section VII.2] where he develops in greater generality the theory of elliptic curves over local fields (which may be of characteristics 2 or 3).

The next goal in this section is to elucidate what we mean when we say that $E(\mathbb{Q})$ is an Abelian group. To do that, we recall Bézout's theorem, which vaguely states that if two non-singular projective curves C_1, C_2 (with corresponding polynomials f_1, f_2) intersect "somewhat generically " (precisely, we mean their intersections are transversal) then $\#(C_1 \cap C_2) = \deg f_1 \deg f_2$, which concurs with our intuition. For aesthetic reasons, we will not define Bézout's theorem formally. Conceivably, this means if we take a rational point P on an elliptic curve E and a line ℓ through it with rational slope, then unless ℓ is tangent to E then it would intersect E at two other points. These need not be rational points. It turns out however that if we start with rational points P, Q then the line $\ell = \overline{PQ}$ intersects E at another rational point. This will provide us with the mechanism to define a group law on $E(\mathbb{Q})$, since given two rational points we can use this geometric procedure to obtain another rational point.

More precisely, we will take the distinguished point at infinity $\mathcal{O}$ to stand in for the function of 0 in our group. Given rational points P, Q, we will define $\overline{PQ} \cap E = R$ to be the point such that $P + Q + R = 0$. This means to find $P + Q$, we first $\overline{PQ} \cap E = R$. Then $P + Q = -R$. Considering $R + (-R) + \mathcal{O} = 0$, $P + Q$ can be found by intersecting the line through R and $\mathcal{O}$ with the elliptic curve again, which corresponds to reflecting R across the x axis.

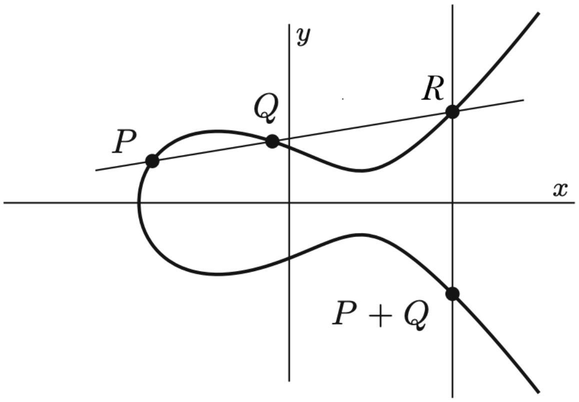

Figure 1: An illustration of the group law on an elliptic curve.

Of course, it is not immediately obvious that such a construction does produce for us a group law. For instance, it is far from obvious that we even have associativity $(A + B) + C = A + (B + C)$ since we would be intersecting very different lines with the elliptic curves when doing the computations on either sides of the equation. We will state the properties that need to be checked, and leave the checking to the interested reader.

Lemma 1. *There exists a binary operation $\oplus$ on $E(\mathbb{Q})$ with the following properties:*

(i) $P \oplus Q = Q \oplus P$.

(ii) $P \oplus \mathcal{O} = P$.

(iii) If a line L meets E at points P, Q, R, then $(P \oplus Q) \oplus R = \mathcal{O}$.

(iv) Given $P \in E(\mathbb{Q})$, there exists $R \in E(\mathbb{Q})$ such that $P \oplus R = \mathcal{O}$.

(v) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

Therefore, $(E(\mathbb{Q}), \oplus)$ is an Abelian group.

3 Reduction modulo p

The general philosophy for understanding $\mathbb{Q}$-rational points is to instead study $\mathbb{Q}_p$-rational points. We now begin investigating the properties of elliptic curves defined over p-adics. Let $E/\mathbb{Q}_p$ be an elliptic curve, say

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

Note that we may ensure that the coefficients $a, b \in \mathbb{Z}_p$ by performing suitable coordinate transformations. Indeed, by setting $t = \max\{|a|_p, |b|_p\}$, then the substitution $(x, y) \mapsto (t^{-2}x, t^{-3}y)$ gives

$$t^{-6}y^2 = t^{-6}x^3 + at^{-2}x + b,$$

which upon multiplying through by t^6 gives

$$y^2 = x^3 + (at^4)x + (bt^6)$$

where $at^4, bt^6 \in \mathbb{Z}_p$.

Now, since we my assume we are working with elliptic curves where the coefficients lie in $\mathbb{Z}_p$, writing bars to mean reduction $\pmod p$, we can define the reduction $\pmod p$ of E over $\mathbb{F}_p$ as

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

Remark 3. This sort of operation can be extended to any local field K with associated ring of integers R and discrete valuation v. It turns out that by working with the *minimal Weierstrass equation* of an elliptic curve E, which is the elliptic curve obtained with coefficients lying in R and minimizes $v(\Delta)$ where Δ is the discriminant, we can ensure that the equation of $\overline{E}$ is unique up to the standard change of coordinates for Weierstrass equations.

It would be good if such reductions produced an elliptic curve $\overline{E}$. It is not immediately obvious if $\overline{E}$ is non-singular - and it will turn out that there could be singular points - but it is also not obvious what such a reduction would do to the group law. To that end, we need to first understand what the reduction map does to the ambient projective space, so that we can understand how to intersect lines with the elliptic curve.

For a point $P = (x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q}_p)$, we may scale to ensure that all coordinates actually lie in $\mathbb{Z}_p$ and that not all coordinates are divisible by p. Then we can define the reduction of P as $\overline{P} = (\overline{x_0} : \overline{x_1} : \cdots : \overline{x_n})$. This also allows us to reduce lines $\pmod p$. Indeed, given a line $ax + by + cz = 0$ in $\mathbb{P}^2(\mathbb{Q}_p)$, we can instead think of it as a triple $(a : b : c) \in \mathbb{P}^2(\mathbb{Q}_p)$. We can then recover the reduced line as $\overline{a}x + \overline{b}y + \overline{c}z = 0$.

It turns out that this reduction is a group homomorphism. In light of our discussion so far, this may be fairly intuitive. "Generically", we should expect that collinear points P, Q, R on an elliptic curve stay collinear after reduction since we are reducing everything $\pmod p$ "the same way". What could go wrong is for example it could happen that the reduced curve contains the line $\overline{PQ}$. We need to check that these scenarios do not arise.

Lemma 2. *Let E be an elliptic curve with coefficients in $\mathbb{Z}_p$. If $P_1, P_2, P_3 \in E(\mathbb{Q}_p)$ are collinear then so are the reductions $\overline{P_1}, \overline{P_2}, \overline{P_3}$. Moreover the reduction of the tangent to E at P_1 is a tangent to $\overline{E}$ at $\overline{P_1}$.*

Proof. Suppose $P_1, P_2, P_3 \in \ell$ such that $\ell : ax + by + cz = 0$. Write $P_i = (x_i : y_i : z_i)$. As we have discussed, we may assume that all coordinates of P_i lie in $\mathbb{Z}_p$ and they are not all divisible by p. Similarly, we may also assume $a, b, c \in \mathbb{Z}_p$ and WLOG $p \nmid c$. Then we can rewrite the line as

$\ell : z = a_1 x + b_1 y$. Suppose that the polynomial equation corresponding to e is $F(x, y, z) = 0$, where F is a homogeneous cubic that arises from homogenizing the short Weierstrass equation. The intersection points of ℓ and F are the roots of $G(x, y) = F(x, y, a_1 x + b_1 y)$. We reduce this equation $\pmod{p}$, which gives $\overline{G}(x, y) = \overline{F}(x, y, \overline{a_1} x + \overline{b_1} y) = 0$.

Let us observe that $\overline{G}$ does not vanish identically. Note that the case of $\overline{G}$ vanishing identically is the case of the reducted curve containing a line that we mentioned could possibly go wrong. Note that because we are working with short Weierstrass equations, this does not happen; any curve of the form $y^2 = f(x)$ where f is a monic polynomial of odd degree remains irreducible after reducing $\pmod{p}$.

Now, observe that $(\overline{x_i}, \overline{y_i}) \neq (0, 0)$ as otherwise $\overline{z_i} = \overline{a_1 x_i} + \overline{b_1} \overline{z_i} = 0$ which is a contradiction to the assumption that not all coordinates of P_i are divisible by p. In particular, if we consider $H(x, y) = (y_1 x - x_1 y)(y_3 x - x_3 y)(y_3 x - x_2 y)$ then the reduction of H cannot vanish identically and by assumption we also have that there exists some $\lambda \in \mathbb{Q}_p$ such that $F(x, y, a_1 x + b_1 y) = \lambda H(x, y)$. Now, $\lambda \in \mathbb{Z}_p$; otherwise, $p^{-1}\lambda \in p\mathbb{Z}_p$ and we would have that $0 = \overline{\lambda F} = \overline{H}$ which is a contradiction to our earlier result on H not vanishing identically. Consequently, this means if we reduce $\pmod{p}$ we get that $\overline{F}(x, y, a_1 x + b_1 y) = \overline{\lambda H}(x, y)$ for some $\overline{\lambda} \in \mathbb{F}_p^\times$, since $\overline{F}$ is not identically zero. Unwinding what this means, we have that the reduced points $\overline{P_i}$ are collinear as desired. □

Next, observe that if P lies on E then evidently $\overline{P}$ lies on $\overline{E}$. It seems natural to ask about the converse. In fact, we will we show that the reduction map is also surjective on the non-singular points.

Lemma 3. *If Q is a non-singular point on $\overline{E}$, then there is a $P \in E(\mathbb{Q}_p)$ such that $Q = \overline{P}$.*

Since we are "lifting" points, it is perhaps unsurprising that the proof goes through via Hensel's lifting.

Proof. Let $F(x, y, z)$ be the homogeneous polynomial corresponding to E. As before, assume that $Q = (x_1 : y_1 : z_1)$ such that $x_1, y_1, z_1 \in \mathbb{Z}_p$. Since Q is a non-singular point on $\overline{E}$, it follows that $\frac{\partial \overline{F}}{\partial x}(x_1, y_1, z_1) \neq 0$. Then we can apply Hensel's lifting to $G(t) = F(t, y_1, z_1)$ where we initiate with $t = x_1$. Suppose the output of Hensel's lifting is x', then it is easy to see that $P = (x' : y_1 : z_1)$ is the point that we desire. □

We can package all of the above information into an exact sequence. First, we define some of the terms that will appear in our exact sequence.

Definition 7. Let $\overline{E}_{ns}(\mathbb{F}_p)$ denote the set of non-singular points on the reduced curve $\overline{E}$. Define also:

- $E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \overline{P} \in \overline{E}_{ns}(\mathbb{F}_p)\}$,
- $E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \overline{P} = \overline{O}\}$,

where we can think of E_0 as the points with nonsingular reduction and E_1 as the kernel of reduction.

Definition 8. We say that $E/\mathbb{Q}_p$ has *good reduction at p* if $\overline{E}$ is non-singular.

Theorem 3. *There is an exact sequence of Abelian groups*

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

In particular, if $E/\mathbb{Q}_p$ has good reduction at p, then we have

$$0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p) \to 0.$$

4 $E_1(\mathbb{Q}_p)$ is torsion-free

In this section, we will study $E_1(\mathbb{Q}_p)$ more closely, following the treatment as in [Cas95] with the goal of establishing the title of this section. In [Sil09], there is a cleaner characterization of $E_1(\mathbb{Q}_p)$ using the machinery of formal groups. We opted for the current presentation because it takes less background to develop.

Our goal in the first part of this section is to establish the following "$\mathbb{Q}_p$-analogue" of the Nagell-Lutz theorem.

Lemma 4. *Let $(x, y) \in E(\mathbb{Q}_p)$ be a point with finite order n such that $(n, p) = 1$. Then we have that $x, y \in \mathbb{Z}_p$.*

The next part of the section will then be focused on removing this $(n, p) = 1$ condition.

4.1 Filtration on $E_1(\mathbb{Q}_p)$

The proof of Lemma 4 will follow once we further understand the structure of E_1. Before we get there, we begin by giving a characterization of $\mathbb{Q}_p$-rational points on the E.

Lemma 5. *Let $P = (x, y)$ be a $\mathbb{Q}_p$-rational point on the elliptic curve $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}_p$. Then there exists some $x', y', q \in \mathbb{Z}_p$ such that $x = x'/q^2$ and $y = y'/q^3$ such that $(x', q) = (y', q) = 1$.*

The same proof would also give the same conclusion for $\mathbb{Q}$-rational points on an elliptic curve with coefficients in $\mathbb{Z}$.

Remark 4. Actually we only used the property of $\mathbb{Z}$ and $\mathbb{Z}_p$ being UFDs, so we can also formulate a version of this lemma for general UFDs.

Proof. Let $x = r_1/s_1$ and $y = r_2/s_2$ with $r_1, r_2 \in \mathbb{Z}_p$ and $s_1, s_2 \in \mathbb{Z}_p$ such that $(r_1, s_1) = (r_2, s_2) = 1$. Since we are working with $\mathbb{Z}_p$ where there is unique factorization, it suffices to prove that $s_1^3 \mid s_2^2$ and $s_2^2 \mid s_1^3$. This is because if this divisibility is true then there exists $u \in \mathbb{Z}_p^\times$ such that $s_1^3 = us_2^2$ with $(us_1)^3 = (u^2 s_2^2)^2$. Consider replacing s_1 by us_1 and s_2 by us_2^2, then $s_1^3 = s_2^2$ which gives the desired conclusion that $s_1 = q^2$ and $s_2 = q^3$ for some $q \in \mathbb{Z}_p$ by unique factorization on $\mathbb{Z}_p$.

Plugging in our values for x and y and then clearing denominators, we get $s_1^3 r_2^2 = s_2^2 r_1^3 + as_2^2 s_1^2 r_1 + cs_2^2 s_1^3$. Since $(s_2, r_2) = 1$ it follows that s_2^2 which divides the RHS must divide s_1^3. Similarly, since s_1 divides the LHS, it must also divide the RHS and in particular $s_1 \mid s_2^2 r_1^3$. But $(s_1, r_1) = 1$ and so $s_1 \mid s_2$. Now, s_1^3 divides the LHS and $s_1^3 \mid as_2^2 s_1^2 r_1 + cs_2^2 s_1^3$ since $s_1 \mid s_2$. This in turn implies that $s_1^3 \mid s_2^2 r_1^3$ which implies that $s_1^3 \mid s_2^2$, as desired. □

Utilizing Lemma 5, note that the projective $\mathbb{Q}_p$-rational points on our elliptic curve are of the form $(x : y : 1) = (x'/q^2 : y'/q^3 : 1) = (qx' : y' : q^3)$. This allows us to put a structure to the kernel of reduction $E_1(\mathbb{Q}_p)$ by studying the *level* of the points.

Definition 9. The *level* function $\ell : E_1(\mathbb{Q}_p) \to \mathbb{N}$ maps a point $(qx' : y' : q^3)$ to $v_p(q)$.

Note that $\ell(x, y) \geq 1$ iff $(x, y) \in E_1(\mathbb{Q}_p)$. Consider the set E_n of points of level at least n; precisely, let $E_n = \{(x, y) \in E_1 : \ell(x, y) \geq n\}$. It is clear that we have the nesting $E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_n \supset \cdots$. It will turn out that actually E_n are groups.

Lemma 6. *The group E_n satisfy $E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_n \supset \cdots$. Additionally, we have the exact sequence for $n \geq 1$ of*

$$0 \to E_{n+1} \to E_n \to \mathbb{Z}/p\mathbb{Z} \to 0$$

and when $n = 0$ we have

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

In technical jargon, this is called the *p-adic filtration on* $E_1(\mathbb{Q}_p)$. To prove that E_n are groups, we will reduce this to the proof that reduction modulo p is a group homomorphism.

Proof. We want to pick out level n points on E, preferably via some suitable coordinate transformation and then studying reduction modulo p of E.

One possible coordinate transformation is to consider $x_n = p^{2n}x$, $y_n = p^{3n}y$ and $z_n = z$. It can be checked that $(x_n : y_n : z_n)$ lie on the elliptic curve $E_n : y^2z = x^3 + p^{4n}axz^2 + p^{6n}bz^3$. If we reduce E_n modulo p then we get $\overline{E_n} : y^2z = x^3$. Write this reduction map as $\pi_n : E(K) \to \overline{E_n}(\mathbb{F}_p)$.

Let us study the image of point $P = (x : y : 1) = (x'q : y' : q^3)$ under π_n. It is the reduction modulo p of $(p^{2n}x'q : p^{3n}y' : q^3)$. In particular, we have the following cases:

- If $1 \leq \ell(P) < n$, then we have that under the coordinate change it maps to

$$(p^{2n}x'q : p^{3n}y' : q^3) = (p^{2n-\ell(P)}x'q : p^{3n-3\ell(P)}y' : p^{-3\ell(P)}q^3)$$

  where by definition of $\ell(P)$ we have that $p^{-3\ell(P)}q^3$ is a p-adic unit. The first two coordinates are divisible by p, and so $\pi_n(P) = [0 : 0 : 1]$ is the singular point.

- If $1 \leq \ell(P) = n$, then by considering $(p^{2n-\ell(P)}x'q : y' : p^{-3\ell(P)}q^3)$ as before and since $(y', p) = (y', q) = 1$ it follows that $\pi_n(P)$ is an affine non-singular point.

- If $\ell > n$, then we have that under the coordinate change it maps to

$$(p^{2n}x'q : p^{3n}y' : q^3) = (p^{-n}x'q : y' : p^{-3n}q^3)$$

  and so $\pi_n(P) = (0 : 1 : 0) = \mathcal{O}$, which is the point at infinity.

Souping that up, we have that E_{n+1} is the kernel of π_n. By Lemma 2, it follows that E_{n+1} is a group. We can package all of this into a short exact sequence, where we recall that the modulo p reduction is surjection as given by Lemma 3. Let the non-singular points on $\overline{E_m}$ be $\overline{E^m_{\text{ns}}}(\mathbb{F}_p)$. Then we can write

$$0 \to E_{m+1} \to E_m \to \overline{E^m_{\text{ns}}}(\mathbb{F}_p) \to 0.$$

To finish up, it suffices to observe that $\overline{E^m_{\text{ns}}}(\mathbb{F}_p) \simeq \mathbb{Z}/p\mathbb{Z}$. □

We end this section by deducing Lemma 4 from our work so far. We recall the statement of the lemma.

Lemma 7. *Let $P = (x, y) \in E(\mathbb{Q}_p)$ be a point with finite order n such that $(n, p) = 1$. Then we have that $x, y \in \mathbb{Z}_p$.*

Proof. Suppose otherwise. Then it follows that $\ell(P) \geq 1$. Since $\bigcap_n E_n = \{\mathcal{O}\}$, we can find some m such that $P \in E_m \backslash E_{m+1}$. The (chain of) homomorphism $E \to E_m \to E_m/E_{m+1}$ sends P to a nonzero element, and therefore an element of order p in E_m/E_{m+1}. But this is a contradiction to the fact that $(n, p) = 1$. □

In particular, it follows that if P has order n coprime to p then $\ell(P) = 0$ so that $P \notin E_1(\mathbb{Q}_p)$, as desired. It remains to consider points of order not necessarily coprime to p.

Remark 5. The proof of Lemma 4 given here is reminiscent of that for a problem in Problem Set 8, which was to prove that two different roots of unity in $\mathbb{Z}_p^\times$ of order prime to p cannot be congruent to each other modulo $p\mathbb{Z}_p$. It is fruitful to note the similarities in the set-up: there we had the p-adic filtration on $\mathbb{Z}_p$ given by the U_i, where $U_i/U_{i-1} \simeq \mathbb{F}_p$.

4.2 Removing the coprime condition on order

We begin with the observation that E_1 cannot contain points of the form $(x, 0) \in E_1$. This is to be expected since our endgoal is that E_1 is torsion-free, and points of the form $(x, 0)$ have order 2. (Why?)

Lemma 8. *Let $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}_p$. If $P = (x, 0)$, then $P \in E(\mathbb{Q}_p)\backslash E_1(\mathbb{Q}_p)$.*

Proof. We know that $x^3 + ax + b = 0$. Note that $x \in \mathbb{Z}_p$. Indeed, suppose otherwise. Then we have that $v_p(x^3) = 3v_p(x)$, and $v_p(ax + b) \leq \max\{v_p(x) + v_p(a), v_p(b)\}$ but since $v_p(a), v_p(b) \leq 0$ while $v_p(x) < 0$ it follows that $v_p(x^3) \neq v_p(-ax - b)$, which is a contradiction.

Since $x \in \mathbb{Z}_p$, it follows that $\ell(P) = 0$. Recall that $P \in \mathbb{E}_1(\mathbb{Q}_p)$ iff $\ell(P) \geq 1$. This is the desired constradction.

□

In this subsection, we will work with the map $u : E_1 \to \mathbb{Z}_p$ given by $u(P) = x/y$ for $P = (x, y)$ and we also set $u(\mathcal{O}) = 0$. The result that we just proved shows that this is a well-defined map since we do not need to worry about $y = 0$. By Lemma 5, we can write $P = (x'/q^2, y'/q^3)$ and so $u(P) = q{\cdot}x'/y'$. In particular, we have that $p^{\ell(P)} \mid u(P)$ or equivalently, $|u(P)| \leq p^{-\ell(P)}$. We can express this information compactly in the following diagram.

$$\begin{tikzcd}
E(\mathbb{Q}_p) & E_0 \arrow[l, hook'] & E_1 \arrow[l, hook'] \arrow[d, "u"] & E_2 \arrow[l, hook'] \arrow[d, "u"] & E_3 \arrow[l, hook'] \arrow[d, "u"] & \cdots \arrow[l, hook'] \\
 & & p\mathbb{Z}_p & p^2\mathbb{Z}_p \arrow[l] & p^3\mathbb{Z}_p \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

Remark 6. If one knows some Lie groups, then it is natural to want to study the group of points on the elliptic curve in a neighborhood of the identity, which in this case is $\mathcal{O} = (0 : 1 : 0)$. The coordinate transformation of $(x/y, 1/y)$ serves to bring $\mathcal{O}$ to the origin and then we can study the transformed elliptic curve in a neighborhood around the origin. This can be thought of as the motivation for u.

Since by Lemma 6 it follows that $E_n/E_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$ has order p, for any point $P \in E_n \backslash E_{n+1}$, we have that $mP \in E_n \backslash E_{n+1}$ for $(m, p) = 1$. On the other hand, we can only conclude that $pP \in E_{n+1}$. We would ideally like to show that $pP \in E_{n+1} \backslash E_{n+2}$ which would conceivably allow us to do some form of induction to show that there is no points of prime power order, and then piecing things together we can then show that $E_1(\mathbb{Q}_p)$ is torsion-free. We can equivalently write $pP \in E_{n+1}$ as $\ell(pP) \geq n+1$ and so $|u(pP)| \leq |p||u(P)|$. Inducting, we see that $|u(mP)| \leq |m||u(P)|$ for all integers m. To get conclusions of the form $pP \in E_{n+1} \backslash E_{n+2}$, we would really like equality to hold.

Lemma 9. *For all $P \in E_1$ and all integers m we have that $|u(mP)| = |m| \cdot |u(P)|$.*

There is actually an easier way to deduce that $E_1(\mathbb{Q})$ is torsion-free from this lemma.

Corollary 1. *$E_1(\mathbb{Q})$ is torsion-free.*

Proof. Suppose for the sake of contradiction that $P \in E_1$ has finite order m. Then applying Lemma 9, we get that $0 = |u(mP)| = |m| \cdot |u(P)|$. But $m \geq 1$ implies that $|m| \neq 0$ so that $P = \mathcal{O}$, a contradiction. □

If u was a homomorphism then Lemma 9 is straightforward. However, since we are effectively zooming in to a neighborhood of the elliptic curve around $\mathcal{O}$, we would not expect the group law to be preserved and in general u may not be a homomorphism. While $u(P_1+P_2) - u(P_1) - u(P_2)$ is not necessarily 0, it turns out that its value is small p-adically, and this approximate homomorphism is good enough for us.

Lemma 10. *For all $P_1, P_2 \in E_1$, we have the inequality*

$$|u(P_1 + P_2) - u(P_1) - u(P_2)| \leq \max\{|u(P_1)|^5, |u(P_2)|^5\}.$$

Proof. It is easy to check if one of P_1, P_2, P_1+P_2 is $\mathcal{O}$. For example, if $P_1+P_2 = \mathcal{O}$ then $P_2 = -P_1$ and so $|u(P_1+P_2) - u(P_1) - u(P_2)| = |u(\mathcal{O}) - u(P_1) - u(-P_1)| = 0$.

So WLOG P_1, P_2, P_1+P_2 all lie in the affine patch and $|u(P_2)| \leq |u(P_1)| = p^{-n}$. We aim to get the inequality in question via applications of Vieta's formulas, since the group law tells us P_1+P_2, P_1 and P_2 lie on the same line. We can then intersect this line with the elliptic curve to obtain the relevant coordinates.

Recall the coordinate transformation we made earlier, where we send $(x : y : z)$ on $E : y^2z = x^3 + axz^2 + bz^3$ to $(p^{2n}x : p^{3n}y : z)$ on $E_n : y_n^2 z_n = x_n^3 + p^{4n}ax_nz_n^2 + p^{6n}bz_n^3$. Under this coordinate transformation, note that since by definition $P_1, P_2 \in E_1$ so that upon reduction they do not map to the singular point $(0,0)$, the line through the reductions of P_1 and P_2 and $-P_1 - P_2$ does not go through the origin. After reduction the line is therefore of the form $z = rx + sy$ for some $r, s \in \mathbb{F}_p^\times$. This implies that before reduction, in (x_n, y_n, z_n) coordinates, the line ℓ_n has the form $z_n = rx_n + sy_n$ for some $r, s \in \mathbb{Z}_p$.

In particular, we can intersect ℓ_n and E_n to obtain $0 = c_3(x_n/y_n)^3 + c_2(x_n/y_n)^2y_n + c_1(x_n/y_n) + c_0$, where $c_3 = 1 + p^{4n}ar^2$ and $b_2 = 2p^{4n}ars + 3p^{6n}br^2s$. Note that the roots to this equation are given by $-p^{-n}u(P_1+P_2)$, $p^{-n}u(P_1)$ and $p^{-n}u(P_2)$ and by Vieta's formulas the sum of these roots is $-c_2/c_3$. In other words, we get that $p^{5n} \mid p^nc_2/c_3 = u(P_1+P_2) - u(P_1) - u(P_2)$ as desired. □

We will now be able to deduce Lemma 9, which we restate here for convenience.

Lemma 11. *Let G be a group. Suppose $u : G \to p\mathbb{Z}_p$ is a map (not necessarily a homomorphism!) such that:*

- $u(-g) = -u(g)$,
- $|u(ag)| \leq |a| \cdot |u(g)|$,
- $|u(g+h) - u(g) - u(h)| \leq \max\{|u(g)|^5, |u(h)|^5\}$,

for all $g, h \in G$. Then we have that $|u(ag)| = |a| \cdot |u(g)|$ for all $a \in \mathbb{Z}$ and $g \in G$.

Proof. We will first show that $u(ag)$ and $au(g)$ are p-adically close in value. Specifically, we prove that $|u(ag) - au(g)| \leq |u(g)|^5$. Write $|u(g)| = p^{-k}$ so that it suffices for us to prove that $p^{5k} \mid u(ag) - a \cdot u(g)$. This follows from induction, where bases cases $a = 0, 1$ are straightforward. The induction step follows from $|u((a+1)g) - u(ag) - u(g)| \leq \max\{|u(ag)|^5, |u(g)|^5\}$.

Now, for the actual lemma, note that when $(a, p) = 1$ it is relatively straightforward: writing $|u(g)| = p^{-k} < 1$, if $p \nmid a$ then $p^k \parallel au(g)$ but we also know from our earlier work that $p^{5k} \mid u(ag) - au(g)$ and so it follows that $p^k \parallel u(ag)$ as well, which proves the desired.

To finish up, we effectively induct on the largest power of p dividing a. In particular, it suffices to show that if the lemma is true for a then it is also true for pa. Begin with $|u(pag) - pu(ag)| \leq |u(ag)|^5$. Similarly as before, it follows that we must have $|u(pag)| = |pu(ag)| = |pa||u(g)|$, as desired. □

5 Proof of the Nagell-Lutz theorem

Now we are finally in a position to prove the Nagell-Lutz theorem, which we recap here for convenience.

Theorem 4 (Nagell-Lutz Theorem)**.** *The group of rational torsion points on an elliptic curve $E(\mathbb{Q})$ is finite. If $(x, y) \neq \mathcal{O}$ is a point of finite order, then $x, y \in \mathbb{Z}$.*

The strategy is to study the torsion points on $\mathbb{Q}_p$, which we by now we have the tools to understand, for various values of p which taken together would allow us to deduce properties of torsion points over $\mathbb{Q}$.

Proof. Let $\mathcal{O}$ be the group of points on $E(\mathbb{Q})$ and $\mathcal{O}_p$ be the group of points on $E(\mathbb{Q}_p)$ for some prime p.

Suppose $P = (x, y) \in \mathcal{O}$ is a torsion point and since $\mathcal{O} \subset \mathcal{O}_p$, we can use our results in the previous sections about $\mathbb{Q}_p$-rational torsion points. In the previous section we showed that E_1 is torsion-free, and in particular $\ell(P) = 0$ so that $x, y \in \mathbb{Z}_p$. Since this is true for all choices of p, it follows that $x, y \in \mathbb{Z}$.

Further, since E_1 is torsion free, it follows that the group of torsion points is isomorphic to a subgroup of $E_0/E_1 \simeq \overline{E}_{ns}(\mathbb{F}_p)$ by Theorem 3 for any prime p with good reduction. Note that any prime p that does not divide the discriminant of E is a prime with good reduction. (Why?) It immediately follows that the torsion group is finite, as desired. □

Remark 7. Barry Mazur [Maz78] actually gave a complete characterization of the possibilities for the group of torsion points. He showed that the torsion group of $E(\mathbb{Q})$ is isomorphic to either $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ where $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ and $m \in \{1, 2, 3, 4\}$.

References

[Cas95] J. W. S. Cassels. *Lectures on elliptic curves*. Cambridge University Press, 1995.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, 2009.

[ST15] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer Publishing Company, 2nd edition, 2015.