Order of the reductions of a non-torsion point of an elliptic curve over a number field

Louise Nataf, supervised by Yunqing Tang at University of California, Berkeley

1 Summary

Elliptic curves are smooth algebraic curves defined by an equation of the type

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

for some fixed $a_1, \dots, a_6$ in a field K. After some definitions and generalities on elliptic curves (such as introducing the usual group law which makes them into abelian groups), we pick K to be a number field and look at its non-archimedian places v, which are extensions of the p-adic valuations on $\mathbb{Q}$ to K. We then consider the reductions modulo these valuations (analogous to reduction modulo primes) of the coefficients of a given elliptic curve, which yield elliptic curves over finite fields (up to some technical details). We pick a point P of the original elliptic curve and look at the order of its image in the reduced curves. After introducing the Néron and Néron-Tate heights, we use these tools to prove the following:

Main Theorem. *Let A be an infinite subset of $\mathbb{N}$. There exist infinitely many places v of K such that the order of the reduction of P mod. v divides an element of A.*

There are many possibilities for A, but here are the applications we had in mind for proving the theorem:

Corollary 1. *Let p be a prime. There exist infinitely many places v of K such that the order of the reduction of P mod. v is a multiple (and even a power) of p.*

Corollary 2. *There exist infinitely many places v of K such that the order of the reduction of P mod. v is a prime.*

We then present a new estimate of the Néron height in the case of archimedian places (extensions of the usual absolute value on $\mathbb{Q}$ to K), under some assumption on the point P. Finally, we discuss potential refinements to the main theorem.

2 Preliminaries on elliptic curves

2.1 Affine and projective varieties

Let $\overline{K}[X] = \overline{K}[X_1, \dots, X_n]$ be the ring of polynomials in n variables with coefficients in $\overline{K}$.

If I is an ideal in $\overline{K}[X]$, one can define the set

$$V_I = \{\, P \in \overline{K}^n \mid f(P) = 0 \text{ for all } f \in I \,\}$$

Definition 2.1. An *(affine) algebraic set* is any set of the form V_I.

If V is an algebraic set, the *ideal of V* is the ideal

$$I(V) = \{\, f \in \overline{K}[X] \mid f(P) = 0 \text{ for all } P \in V \,\}$$

An algebraic set V is said to be *defined over K* if its ideal $I(V)$ can be generated by polynomials in $K[X]$. This is denoted by V/K.

If V is defined over K, the *set of K-rational points of V* is

$$V(K) = V \cap K^n$$

Definition 2.2. An affine algebraic set V is called an *affine variety* if $I(V)$ is prime in $\overline{K}[X]$.

If V/K is a variety, the *affine coordinate ring of* V/K is

$$K[V] = \frac{K[X]}{I(V) \cap K[X]}$$

Its quotient field, denoted $K(V)$, is the *function field of* V/K.

Definition 2.3. If V is an affine variety, the *dimension of* V is the transcendance degree of $\overline{K}(V)$ over $\overline{K}$ (that is, the largest cardinality of a subset $S \subseteq \overline{K}(V)$ such that there is no integer m and no non-trivial $F \in \overline{K}[X_1, \ldots, X_m]$ such that $F(x_1, \ldots, x_m) = 0$ for some $x_1, \ldots, x_m$ in S).

Definition 2.4. Let V be a variety, P a point of V and $f_1, \ldots, f_m$ in $\overline{K}[X]$ a set of generators for $I(V)$. Then V is *smooth* at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

has rank $n - \dim(V)$.

For compactness reasons, it can be useful to extend an affine variety V to a closed subset of a projective space. To accomplish this, one can embed $\overline{K}^n$ in $\mathbb{P}^n(\overline{K})$ through a map of the type

$$\phi_i : (x_1, \ldots, x_n) \mapsto [x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n]$$

for some i and consider the process of *homogenization with respect to* X_i which for f in $\overline{K}[X]$ yields the polynomial

$$f^*(X_0, \ldots, X_n) = X_i^d f\left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right)$$

where d is the smallest integer such that f^* is in $\overline{K}[X_0, \ldots, X_n]$. Then, f^* is homogeneous (of degree d) and such that

$$f^*(X_1, \ldots, X_i, 1, X_{i+1}, \ldots, X_n) = f(X_1, \ldots, X_i, X_{i+1}, \ldots, X_n).$$

Let I be the ideal of $\overline{K}[X_0, \ldots, X_n]$ generated by the f^* for f in $I(V)$.

Definition 2.5. The *projective closure of* V is the set

$$\overline{V} = \{\, P \in \mathbb{P}^n(\overline{K}) \mid g(P) = 0 \text{ for all homogeneous } g \in I \,\}$$

Remark. The vanishing of a homogeneous polynomial at a point of $\mathbb{P}^n(\overline{K})$ is well defined since it does not depend on the representative of the point in $\overline{K}^{n+1}$.

$\overline{V}$ contains the copy of V that has been embedded in $\mathbb{P}^n(\overline{K})$.

Definition 2.6. A *projective variety* V is any $\overline{W}$ for some affine variety W. It is *defined over* K if and only if W is. The *dimension of* V and its *function field* $K(V)$ are, by definition, the dimension of W and $K(W)$. If P is a point of $V \cap W$, V is *smooth at* P if W is.

Remark. The last definition allows to check the smoothness of a projective variety V at any point: if $\phi_i(\overline{K}^n) \cap V$ is not empty, it is an affine variety such that V is the projective closure of $\phi_i(\overline{K}^n) \cap V$ ([1], I.2.6). If a variety is smooth at every point, it is said to be a *smooth variety*.

Definition 2.7. A projective variety of dimension 1 is called a *curve*.

2.2 Weierstrass equations and elliptic curves

Definition 2.8. A *Weierstrass equation* over K is an equation of the form

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

for some fixed $a_1, \ldots, a_6$ in K.

Let V be the set of the (x, y) in $\overline{K}^2$ that satisfy the equation.

Proposition 1. *V is an affine variety defined over K.*

Proof. V is an affine algebraic set with ideal $f\overline{K}[X, Y]$ for

$$f = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6).$$

It is defined over K since f has coefficients in K.

We just need to check that $f\overline{K}[X, Y]$ is prime in $\overline{K}[X, Y]$. It is enough to show that f is irreducible in $\overline{K}[X, Y]$.

Assume $f = gh$ with g, h in $\overline{K}[X, Y]$.

If both g and h have degree 1 as polynomials in Y, one can write

$$g = PY + Q,\ h = RY + S$$

for some P, Q, R, S in $\overline{K}[X]$. Expanding the product gives

$$f = PRY^2 + (PS + QR)Y + QS,$$

which implies that P and R are in $\overline{K}^*$ (let's rename them p, r) and

$$pS + rQ = a_1X + a_3,\ QS = -(X^3 + a_2X^2 + a_4X + a_6).$$

Since $deg(Q) + deg(S) = 3$, we have $deg(Q) \neq deg(S)$, so $deg(pS + rQ) = max(deg(Q), deg(S))$. Hence,

$$3 = deg(QS) = deg(Q) + deg(S) < max(deg(Q), deg(S)) = 1,$$

which is bothersome.

So either g or h (say, g) has degree 0 as a polynomial in Y. Looking at the term in Y^2 in the expression of f yields that g is invertible in $\overline{K}[X]$, hence g is in $\overline{K}$. □

This variety has dimension 1. This is a consequence of the general fact that if $V \subseteq \overline{K}$ is defined by a single non-constant polynomial equation $f(X_1, \ldots, X_n) = 0$, then $\dim(V) = n - 1$ ([1], I.1.4).

Hence, its projective closure is a curve. It is the set of the $[X : Y : Z]$ in $\mathbb{P}_3(\overline{K})$ that satisfy the equation

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

(this is also called a *Weierstrass equation*).

If a point in the curve is such that $Z = 0$, then the equation yields $X = 0$, so the point is $[0 : 1 : 0]$, which does belong to the curve. Hence, one point at infinity, $O = [0 : 1 : 0]$, has been added to the affine variety when taking its projective closure.

We now have all the ingredients to define the notion of elliptic curve:

Definition 2.9. An *elliptic curve* is a smooth curve defined by a Weierstrass equation.

Notation 1. For a Weierstrass equation with coefficients $a_1, \ldots, a_6$, let

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 - 36b_2b_4 - 216b_6$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\ j = \frac{c_4^3}{\Delta}$$

Δ is called the *discriminant* of the Weierstrass equation, and j its *j-invariant*.

Proposition 2 ([1], III.1.4)**.** A curve defined by a Weierstrass equation with discriminant Δ is smooth if and only if $\Delta \neq 0$.

Hence, elliptic curves can be characterized as curves defined by Weierstrass equations with non-zero discriminant.

Definition 2.10. Two elliptic curves defined over K are said to be *isomorphic over K* if there exists a linear change of variables of the form

$$x = u^2x' + r, y = u^3y' + su^2x' + t$$

for some u, r, s, t in K with $u \neq 0$, between the equations defining E and E'.

Two isomorphic elliptic curves will often be considered as the same: we will say that we have two Weierstrass equations defining the same curve.

Remark. Considering elliptic curves up to isomorphism over a certain field allows for much simpler formulae ([1], III., §1). Indeed, starting from a Weierstrass equation with coefficients $a_1, \ldots, a_6$:

- If $\mathrm{char}(\overline{K}) \neq 2$, replacing y by $\frac{1}{2}(y - a_1x - a_3)$ yields
$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$
- If furthermore $\mathrm{char}(\overline{K}) \neq 3$, replacing (x, y) by $(\frac{1}{36}(x - 3b_2), \frac{1}{108}y)$ yields
$$y^2 = x^3 - 27c_4x - 54c_6$$

Hence, if $\mathrm{char}(\overline{K}) \neq 2, 3$, we can assume an elliptic curve defined over K has equation of the form

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

for $A, B \in K$. Then, we have the simple formulae

$$\Delta = -16(4A^3 + 27B^2),\ j = -\frac{1728(4A)^3}{\Delta}$$

Proposition 3 ([1], III.1.4)**.** Two elliptic curves are isomorphic over $\overline{K}$ if and only if they have the same j-invariant.

Hence, j can be called j-invariant *of the elliptic curve.*

2.3 The group law

Let's define a composition law $+$ on an elliptic curve with Weierstrass coefficients $a_1, \ldots, a_6$ by saying that if P_1 and P_2 are points of E, the point $P_3 = P_1 + P_2$ is the following (with notation $P = (x, y)$ if $P = [x : y : 1] \neq O$):

- If $x_1 = x_2$ and $y_1 + y_2 + a_1X_2 + a_3 = 0$, then $P_3 = O$.
- Otherwise, let
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \text{ if } x_1 \neq x_2$$
$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},\ v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \text{ if } x_1 = x_2$$
Then
$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$
$$y_3 = -(\lambda + a_1)x_3 - v - a_3$$

Remark. This definition (which is a little more palatable when $a_1 = a_3 = a_2 = 0$) corresponds to a geometric construction. If L is the line connecting P_1 and P_2 (or the tangent line to E if $P_1 = P_2$), then L has equation $y = \lambda x + v$. From a special case of Bézout's theorem ([1], §2), either L has a third point of intersection with E (let's call it Q), or L is tangent to E at exactly one of the points P_1 and P_2, and call that point Q. Let L' be the line connecting Q and O (or tangent to O if $Q = O$). Then similarly as what we did with P_1 and P_2 to get Q, we get a point in L'. This point is $P_3 = P_1 + P_2$.

Proposition 4 ([1], III.2.2)**.** The composition $+$ makes E into an abelian group with identity element O. If E is defined over K, then $E(K)$ is a subgroup of E.

This proposition allows us to define by induction the multiplication-by-m group homomorphisms for m in $\mathbb{Z}$: $[0]P = 0$, $[m + 1]P = [m]P + P$, $[-m]P = -[m]P$.

3 Reduction of an elliptic curve at a place

3.1 Absolute values

Let K be a field.

Definition 3.1. An *absolute value* on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ that satisfies:

1. $|x| = 0$ if and only if $x = 0$
2. $|xy| = |x| \cdot |y|$
3. $|x + y| \leq |x| + |y|$

If the condition $|x + y| \leq \max(|x|, |y|)$ holds, then $|\cdot|$ is said to be *non-archimedean*. If $|x| = 1$ for all $x \neq 0$, $|\cdot|$ is said to be *trivial*.

Example 3.1 ($K = \mathbb{Q}$)**.** If p is a prime, $|\cdot|_p$ defined by $|p^n \frac{a}{b}|_p = p^{-n}$ if $a, b \in \mathbb{Z}$ are such that $\gcd(p, ab) = 1$ is a non-archimedian absolute value on $\mathbb{Q}$. It is called the *p-adic* absolute value. The usual absolute value $|\cdot|_\infty = |\cdot|$ corresponding to the complex modulus is an archimedian absolute value.

If $|\cdot|$ is an absolute value on K, setting $d(x, y) = |x - y|_v$ for x, y in K defines a distance on K (which is ultrametric if and only if $|\cdot|$ is non-archimedian), hence a topology on K.

Definition 3.2. Two absolute values $|\cdot|_1, |\cdot|_2$ on K are called *equivalent* if they define the same topology on K. From [3], 1.2.3, this is true if and only if there is a real number $s > 0$ such that for all x in K,

$$|x|_1 = |x|_2^s.$$

Definition 3.3. A *place* v of K is an equivalence class of non-trivial absolute values on K.

Example 3.2. The non-archimedian places of $\mathbb{Q}$ are all represented by the inequivalent absolute values $|\cdot|_p$ for p prime (hence, we will sometimes say "the place p" to talk about the place that corresponds to $|\cdot|_p$). $\mathbb{Q}$ has only one archimedian place (which is represented by $|\cdot|_\infty$). ([3], 1.2.5.)

Notation 2. We will denote by $|\cdot|_v$ an absolute value in the equivalence class v.

Definition 3.4. If the field L is an extension of K and v is a place of K, we write $w|v$ for a place w of L if and only if the restriction to K of any representative of w is a representative of v, and say that w *lies over* v, or equivalently w *extends* v.

If v is a place of K, it extends uniquely to a place of the completion K_v of the metric space $(K, |\cdot|_v)$. By uniqueness, we will also call this place v.

Example 3.3. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is called $\mathbb{Q}_p$. The completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ is $\mathbb{R}$.

It is also possible to extend v to a finite separable extension L of K (pick a primitive element ξ), but uniqueness does not hold anymore:

Proposition 5 ([3], 1.2.7 and 1.3.1)**.** Let K be a field with an absolute value $|\cdot|_v$, let L be a finite extension of K generated by a single element ξ. Let $f(t)$ be the minimal polynomial of ξ over K and

$$f(t) = f_1^{k_1}(t) \dots f_r^{k_r}(t)$$

the decomposition of $f(t)$ into different irreducible monic factors $f_1(t), \dots, f_r(t) \in K_v[t]$.

Then for each $j \in \{1, \dots, r\}$, if we denote $K_j = K_v[t]/(f_j(t))$, there is an injective homomorphism

$$\iota \ : \ L \to K_j, \ \xi \mapsto t$$

of field extensions over K, and there is a unique extension $|\cdot|_j$ of $|\cdot|_v$ to K_j, given by

$$|x|_j = |N_{K_j/K_v}(x)|_v^{1/\deg f_j} \text{ for } x \in K_j,$$

where $N_{K_j/K_v}(x)$ is the determinant of the K_v-linear map $m_x \ : \ K_j \to K_j, \ y \mapsto xy$.

For any $|\cdot|_w$ extending $|\cdot|_v$ to L, there is a unique j such that $|\cdot|_j$ restricted to L is $|\cdot|_w$, and furthermore K_j is the closure of L with respect to w.

Example 3.4. Let's compute the extensions of $|\cdot|_\infty$ from $K = \mathbb{Q}$ to $L = \mathbb{Q}[\xi]$, where ξ is the only real root of $t^3 - 2$.

We have $f(t) = t^3 - 2 = f_1(t)f_2(t)$, with $f_1(t) = t - \xi$ and $f_2(t) = t^2 + \xi t + \xi^2$.

1. $\iota : L \to \mathbb{R}[t]/(t-\xi),\ \xi \mapsto t$ is the usual inclusion $\mathbb{Q}[\xi] \to \mathbb{R}$, and $N_{\mathbb{R}/\mathbb{R}}$ is just identity on $\mathbb{R}$, so $|a + b\xi|_1 = |a + b\xi|_\infty$ if $a, b \in \mathbb{Q}$.

2. Let's look at $\iota : L \to \mathbb{R}[t]/(t^2 + \xi t + \xi^2),\ \xi \mapsto t$. For $x, y \in \mathbb{R}$, we have

$$N_{K_2/\mathbb{R}}(x + yt) = \begin{vmatrix} x & -y\xi^2 \\ y & x - y\xi \end{vmatrix} = x^2 - xy\xi + y^2\xi^2,$$

so $|a + b\xi|_2 = |a^2 - ab\xi + b^2\xi^2|_\infty^{1/2}$ if $a, b \in \mathbb{Q}$.

3.2 Reduction of a field at a non-archimedian place

Let v be a non-archimedian place of K. The ring

$$R_v = \{x \in K \mid |x|_v \leq 1\}$$

is independant on the representative $|\cdot|_v$ and called the *valuation ring* of v. The fraction field of R_v is K. Since $|x^{-1}|_v = |x|_v^{-1}$ for all x in K^*, x is invertible in R_v if and only if $|x|_v = 1$. Hence, R_v is a local ring (i.e. has only one maximal ideal) with maximal ideal

$$\mathfrak{m}_v = \{x \in K \mid |x|_v < 1\}$$

Its residue field is $k_v = R_v/\mathfrak{m}_v$, we denote the reduction map

$$R_v \to k_v,\ x \mapsto \tilde{x}.$$

Example 3.5. When $K = \mathbb{Q}$ and v corresponds to a prime p, the valuation ring is called $\mathbb{Z}_p$. Its maximal ideal is $p\mathbb{Z}_p$, and its residue field is $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

If $|K^*|_v$ is discrete, v is called *discrete*. Then, $\mathfrak{m}_v$ is a principal ideal ([3], 1.2), so there exists a *uniformizer* π_v such that $\pi_v R_v = \mathfrak{m}_v$.

Example 3.6. $|\mathbb{Q}^*|_p = \{p^{-n} \mid n \in \mathbb{Z}\}$ so the place p is discrete (and indeed, the maximal ideal of the valuation ring is principal). Fields that, like $\mathbb{Q}_p$, are complete with respect to a topology induced by a discrete place and have finite residue field are called *local fields*.

Remark. Often, $-\log|\cdot|_v \in \mathbb{R} \cup \{\infty\}$ is considered instead of $|\cdot|_v$ and called the corresponding *additive absolute value* or *valuation*. Then, a place v can be seen as both an equivalence class of absolute values and an equivalence class of valuations modulo proportionality. For that reason, v is sometimes called a *valuation* itself. We will write $v(\cdot) = -\log|\cdot|_v$ for $|\cdot|_v$ a chosen representative of its class. When v is discrete, we can (and often will) choose the representative such that $v(K^*) = \mathbb{Z}$. When $K = \mathbb{Q}$ and $v = p$, this process yields the well-known p-adic valuation v_p on $\mathbb{Q}$.

3.3 Reduced curves

Let v be a discrete valuation on a field K and E/K be an elliptic curve, with Weierstrass equation

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

Since replacing x, y with $u^{-2}x, u^{-3}y$ turns a_i into $u^i a_i$, we can assume the a_i are in R_v (up to choosing u divisible by a large power of π_v).

Then, the discriminant of the equation has non-negative valuation. Since this valuation lives in a discrete group, it is possible to minimize it with respect to the coefficients $a_1, \ldots, a_6 \in R_v$.

An equation with minimal discriminant and coefficients in R_v is called a *minimal Weierstrass equation for* E. In practice, it is helpful to know that if the a_i are in R_v and $v(\Delta) < 12$, or $v(c_4) < 4$, or $v(c_6) < 6$, the equation is minimal ([1], VII.1.1).

Then, reducing the a_i of a minimal equation modulo π_v yields a Weierstrass equation for a curve $\tilde{E}_v$ defined over k_v.

If P is in $E(K)$, there exists a choice of homogeneous coordinates

$$P = [x_0 : y_0 : z_0]$$

such that $x_0, y_0, z_0 \in R_v$ and at least one of x_0, y_0, z_0 is in R_v^* (group of invertible elements of R_v). Then, the point

$$\tilde{P}_v = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}]$$

is in $\tilde{E}_v(k_v)$ (recall that $\tilde{x} = x \text{ mod. } \pi_v$). Hence there is a *reduction map*

$$E(K) \to \tilde{E}_v(k_v),\ P \mapsto \tilde{P}_v.$$

Remark. The equation for $\tilde{E}_v$ is unique up to the change of variables described earlier, but with coefficients in k_v. That is the point of choosing a *minimal* Weierstrass equation for E ([1], VII.1.3).

Definition 3.5. E has *good reduction at* v if the curve $\tilde{E}_v$ is smooth, hence an elliptic curve (that is, if its discriminant is non-zero). If not, E is said to have *bad reduction at* v.

Example 3.7. The elliptic curve $E : y^2 = x^3 + x$, defined over $\mathbb{Q}$, has $j = 1728$ and $\Delta = -2^6$. For p prime, $v_p(\Delta) < 12$ so the equation defining E is minimal with respect to the place p. So the reduction $\tilde{E}_p$ of E mod. p has discriminant the reduction of Δ mod. p, hence E has good reduction at p if and only if $p \neq 2$.

4 Formulation of the question

Let K be a number field, let E/K be an elliptic curve with j-invariant in $\mathcal{O}_K$ (ring of integers of K).

Lemma 1. *It is possible to find an algebraic extension K'/K such that E/K' has good reduction at all (non-archimedian) places.*

Remark. It makes sense to consider the reduction of E at all non-archimedian places of K (or K') because all of these places are discrete.

Indeed, if L is a number field, any non-archimedian place v on L stems from a p-adic valuation p on $\mathbb{Q}$, and if we pick ξ a primitive element for $L/\mathbb{Q}$, there is a monic irreducible factor $f_j(t) \in \mathbb{Q}_p[t]$ of the minimal polynomial $f(t)$ of ξ over $\mathbb{Q}$ such that a representative $|\cdot|_v$ for v is a restriction of

$$x \in K_j \mapsto |N_{K_j/\mathbb{Q}_p}(x)|_p^{1/\deg f_j}$$

(here, we denoted $K_j = \mathbb{Q}_p[t]/(f_j(t))$ like in the relevant proposition). So

$$|L^*|_v \subseteq |\mathbb{Q}_p^*|_p^{1/\deg f_j}$$

which is discrete, so v is discrete, and we have shown that all non-archimedian places of a number field are discrete.

The proof of the lemma relies on the following proposition:

Proposition 6 ([1], VII.5.5)**.** Let E/K be an elliptic curve, v a valuation on K. Then E has potential good reduction at v (that is, there exists a finite extension K'/K such that E, seen as a curve over K', has good reduction at v) if and only if the j-invariant of E is in R_v.

Proof of the lemma. Let E/K be an elliptic curve with $j \in \mathcal{O}_K$.

1. If v is a discrete place of K, we have $j \in R_v$.

   Indeed, if $f \in \mathbb{Z}[X]$ is such that $f(j) = 0$, we have $f \in R_v[X]$ (since from the strong triangle inequality, $|b|_v \leq 1$ for $b \in \mathbb{Z}$). So it is enough to prove that R_v is integrally closed.

Let's assume by contradiction that there is a $g \in R_v[X]$ and an $x \notin R_v$ such that $g(x) = 0$. Then, $x \neq 0$ and since $|x^{-1}|_v = |x|_v^{-1}$, we have $x^{-1} \in R_v$. So if $b_1, \ldots, b_n \in \mathbb{Z}$ are such that

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0,$$

we have

$$x = -b_1 - b_2 x^{-1} - \cdots - b_n (x^{-1})^{n-1}.$$

But then,

$$|x|_v \leq \max(|-b_1|_v, |-b_2|_v |x^{-1}|_v, \ldots, |-b_n|_v (|x^{-1}|_v)^{n-1}) \leq 1;$$

contradiction.

2. From [1], 1.3.: let $a_1, \ldots, a_6 \in K$ be the coefficients of a Weierstrass equation for E, Δ its discriminant. Then for all but finitely many non-archimedian v, we have $v(a_i) \geq 0$ for all i and $v(\Delta) = 0$. Then for such v, the equation is minimal and the reduced curve is smooth. So E has good reduction at v for all but finitely many v.

3. If a curve E/K has good reduction at v and w is an extension of v to some finite extension K' of K, then E/K' has good reduction at v. ([1], 5.4 (b))

Hence, we can use the proposition to extend K successively for all the finitely many places v such that E has bad reduction at v. This process will yield a K' such that E/K' has good reduction at all places. □

Then, up to finite extension of K, we can suppose E/K has good reduction at all places. Let P be a non-torsion point of E. If v is a place of K, the image $\tilde{P}_v$ of P by the reduction map modulo v has finite order, since $\tilde{E}_v(k_v)$ is finite (its elements have coefficients in k_v, which is finite by definition of a place). Then, we can study the orders of the $\tilde{P}_v$ for all v; this is going to be the topic of the rest of this paper.

5 Computer simulations

The first step to answering this question was using the computer algebra system SageMath to examine what happened on elliptic curves defined over $\mathbb{Q}$.

First, I searched for elliptic curves with integer j-invariant that had non-torsion points by computing ranks ($E(K)$ is finitely generated by the Mordell-Weil theorem (see the section on heights), so it is isomorphic to $\mathbb{Z}^r \times E_{tor}$ where r is the rank of the elliptic curve). Then, I computed the orders of the reductions modulo various primes.

In Figures 1 and 2 are the orders of the P mod. p (y axis) as a function of p (x axis) for the first 500 primes p (removing those for which the curve has bad reduction). Here, I chose the elliptic curve

$$E \ : \ y^2 = x^3 + 2,$$

which has rank 1 and j-invariant 1728. The non-torsion points of E are generated by

$$P_0 = [-1 : 1 : 1]$$

(according to Sage); I picked

$$P = [3]P_0.$$

The points on the graph were colored according to conditions on the order of the reduced point: its congruence modulo 3 (Figure 1), and whether it is prime or a square (Figure 2).

It seems, in this example as well as in the others I computed, that all of these conditions appear at infinitely many places. Let's introduce a new tool to study the question further.

Figure 1: Congruence of the order of the reduced points: 0 mod. 3 (blue), 1 mod. 3 (green), 2 mod. 3 (pink)

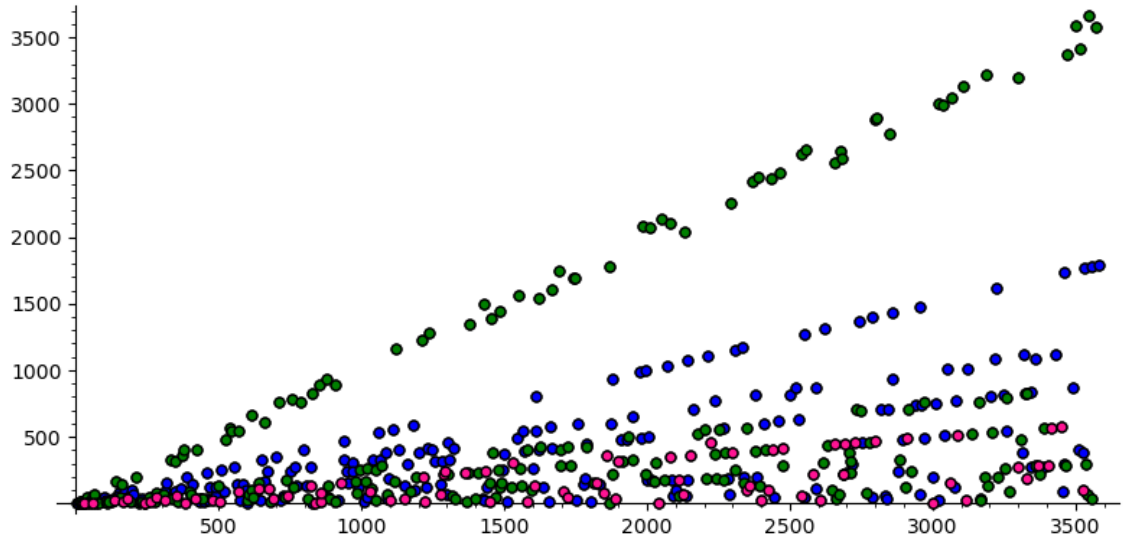
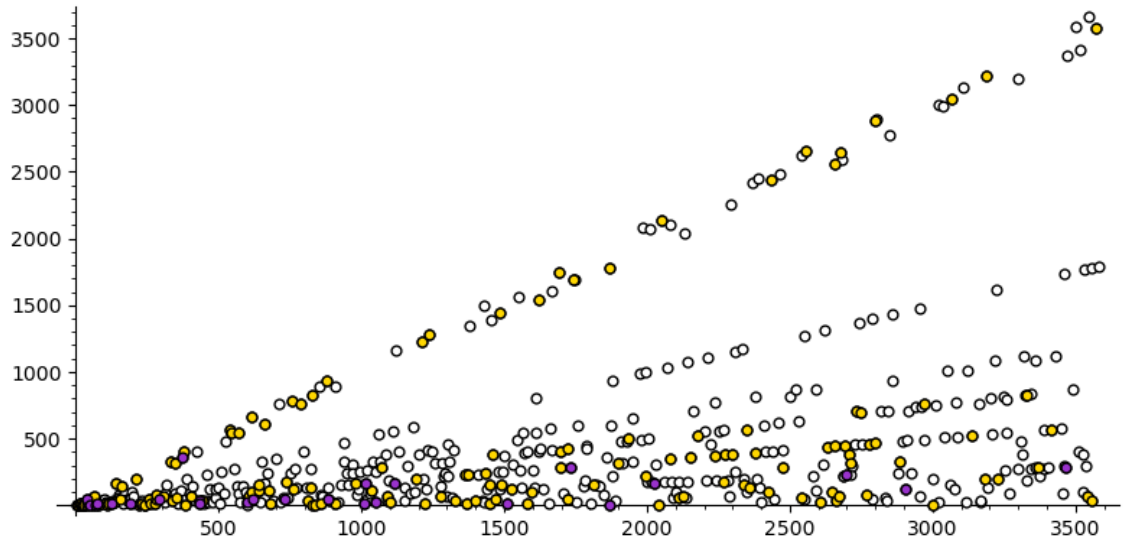


Figure 2: Whether the order of the reduced points is prime (yellow), a square (purple) or neither (white)



6 Heights on elliptic curves

The Néron-Tate height was defined at around the same time by André Néron and John Tate. While Tate's construction was global (the height is defined as a limit of quasi-quadratic heights), Néron's uses local quasi-quadratic terms.

6.1 The Néron height

Before defining these local terms, we need to define topologies on elliptic curves.

Definition 6.1. Let K be a field and let $|.|_v$ be an absolute value on K. The *v-adic topology on* $E(K)$ is defined by the following:

- If $P_0 = (x_0, y_0) \in E(K) - \{O\}$, a basis of open neighborhoods of P_0 consists in the sets

$$U_\varepsilon = \{(x, y) \in E(K) \mid \max(|x - x_0|_v, |y - y_0|_v) < \varepsilon\} \text{ for } \varepsilon > 0.$$

- A basis of open neighborhoods of O consists in the sets

$$U_\varepsilon = \{(x, y) \in E(K) \mid |x|_v > \varepsilon^{-1}\} \cup \{O\} \text{ for } \varepsilon > 0.$$

Theorem 1 ([2], VI.1.1)**.** *Let K be a field complete with respect to an absolute value $|\cdot|_v$, and define $v(\cdot) = -\log|\cdot|_v$ the corresponding additive absolute value. Let E/K be an elliptic curve. Choose a Weierstrass equation for E with coefficients $a_1, \ldots, a_6 \in K$. Let Δ be the discriminant of the equation.*
There exists a unique function $h_v : E(K) - \{O\} \to \mathbb{R}$ such that:

1. *h_v is continuous on $E(K) - \{O\}$ and bounded on the complement of any v-adic neighborhood of O.*
2. *The v-adic limit*
$$\lim_{P \to O} h_v(P) + \frac{1}{2} v(x(P))$$
exists.
3. *For all $P, Q \in E(K)$ with $P, Q, P \pm Q \neq O$,*
$$h_v(P + Q) + h_v(P - Q) = 2h_v(P) + 2h_v(Q) + v(x(P) - x(Q)) - \frac{1}{6} v(\Delta)$$
*(*quasi-parallelogram law*).*

h_v is called the local Néron height function on E associated to *v. It is independent of the choice of Weierstrass equation for E over K. If L/K is a finite extension and w is the extension of v to L, then $h_w(P) = h_v(P)$ for all P in $E(K) - \{O\}$.*

6.2 The Néron-Tate height

Definition 6.2. Let K be a number field, M_K the set of valuations on K and $n_v = [K_v : \mathbb{Q}_v]$ the local degree of $v \in M_K$. For $P \in E(K) - \{O\}$, the *Néron-Tate height (or canonical height)* of P is

$$h(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v h_v(P)$$

Remark. The local degree of $v \in M_K$ is well-defined because the closure of $\mathbb{Q}$ in K_v is $\mathbb{Q}_v$. The sum is also well-defined because for all $P \in E(K) - \{O\}$, $h_v(P) = 0$ for all but finitely many $v \in M_K$ ([2], proof of VI.2.1). We will keep the notation M_K throughout this paper.

Theorem 2 (Néron-Tate, [1], VII.9.3 and [2], VI.2.1)**.** *Let E/K be an elliptic curve and h the canonical height on E.*

1. *For all $P, Q \in E(\overline{K})$,*
$$h(P+Q) + h(P-Q) = 2h(P) + 2h(Q)$$
*(*parallelogram law*).*

2. *For all $P \in E(\overline{K})$ and $m \in \mathbb{Z}$,*
$$h([m]P) = m^2 h(P)$$

3. *h is a quadratic form on E. That is, h is even and the pairing $E(\overline{K}) \times E(\overline{K}) \to \mathbb{R}, (P,Q) \mapsto h(P+Q) - h(P) - h(Q)$ is bilinear.*

4. *Let P in $E(\overline{K})$. Then $h(P) \geq 0$, and $h(P) = 0$ if and only if P is a torsion point.*

Remark. The Néron-Tate height is used in the proof of an important theorem on elliptic curves:

Mordell-Weil Theorem. ([1], VIII) Let E be an elliptic curve defined over a number field K. Then, the group $E(K)$ is finitely generated.

7 Proof of the main theorem

Let $A \subseteq \mathbb{N}$. We want to show that there exist infinitely many places v of K such that the order of $\tilde{P}_v$ divides an element of A (this way, if A is, for example, $\{p^n \mid n \in \mathbb{N}\}$ for p a prime, then we know that there are infinitely many places v of K such that $\mathrm{ord}(\tilde{P}_v) = 0 \bmod p$, up to controlling the places at which $\mathrm{ord}(\tilde{P}_v) = 1$).

Lemma 2. *If Q is a point of $E(K)$, $h_v(Q) \neq 0 \Leftrightarrow \tilde{Q}_v = 0$.*

The proof of this lemma relies on the following theorem:

Theorem 3 ([2], VI.4.1)**.** *Let K be a field complete with respect to a non-archimedian absolute value v on K. Let E/K be an elliptic curve that has good reduction modulo v, pick a minimal Weierstrass equation for E with coefficients in R_v. Then the Néron local height function is given by the formula*
$$h_v(P) = \frac{1}{2}\max\{v(x(P)^{-1}), 0\} \quad \textit{for} \quad P \in E(K) - \{O\}.$$

Proof (of the lemma). Let $Q \in E(K)$.

- If $h_v(Q) \neq 0$, $|x(Q)|_v > 1$ so $x(Q) \notin R_v$. Recall that $\tilde{Q}_v = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}]$ where $[x_0 : y_0 : z_0]$ is a choice of homogeneous coordinates for Q such that $x_0, y_0, z_0 \in R_v$ (and at least one of x_0, y_0, z_0 is in R_v^*). Since $|x(Q)|_v > 1$, $x(Q) \neq 0$ and we have that $z_0 = \frac{x_0}{x(Q)}$ has absolute value $|x_0|_v |x(Q)|_v^{-1} < 1$, so $z_0 \in \mathfrak{m}_v$ and $\tilde{z}_0 = 0$, hence $\tilde{Q}_v = 0$.

- If $h_v(Q) = 0$, $|x(Q)|_v \leq 1$ so $x(Q) \in R_v$ and since we chose to define E by a Weierstrass equation with coefficients in R_v, $y(Q)$ is integral over R_v and (we have seen previously that R_v is integrally close) $y(Q) \in R_v$. So taking $(x_0, y_0, z_0) = (x(Q), y(Q), 1)$, we get $\tilde{z}_0 \neq 0$ and $\tilde{Q}_v \neq 0$.

□

Hence, it is enough to check that there exist infinitely many places v of K such that $h_v([m]P) \neq 0$ for some m in A. Let's assume by contradiction that the set $M_K^{\#}$ of the places v such that $h_v([m]P) \neq 0$ for some m in A is finite.

We know that
$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v h_v([m]P) = h([m]P) = m^2 h(P)$$

Now we use the following theorem from Panda:

Theorem 4 ([4])**.** *Let E be an elliptic curve defined over a number field K, $P \in E(K) - \{0\}$, $v \in M_K$. Then the local Néron height function on E associated to v is such that*

$$h_v([m]P) = O(\log m) \text{ as } m \to \infty.$$

Hence, $m^2 h(P)$ is a sum of finitely many terms which are all $o(m^2)$ when $m \to \infty$. Since $h(P) \neq 0$ (P is non-torsion), we get a contradition, which completes the proof of the following theorem:

Main Theorem. *Let A be an infinite subset of $\mathbb{N}$. There exist infinitely many places v of K such that the order of the reduction of P mod. v divides an element of A.*

There are many possibilities for A, but here are the applications we had in mind for proving the theorem:

Corollary 1. *Let p be a prime. There exist infinitely many places v of K such that the order of the reduction of P mod. v is a multiple (and even a power) of p.*

Proof. Take $A = \{p^n \mid n \in \mathbb{N}\}$ for p a prime, then we know that there are infinitely many places v of K such that the order of P mod. v divides a power of p. But P mod. v is 0 for only finitely many v, since we have seen previously that $h_v(P) \neq 0$ for only finitely many places v, hence the corollary. □

Corollary 2. *There exist infinitely many places v of K such that the order of the reduction of P mod. v is a prime.*

Proof. Take A to be the set of prime numbers. There are infinitely many v such that that the order of the reduction of P mod. v divides a prime, so is either 1 or a prime. We conclude as for the previous corollary. □

8 A slightly better bound on the local height in the archimedian case, up to some assumption on P

Let v be an archimedian valuation on K.

K_v is either $\mathbb{R}$ or $\mathbb{C}$, because these two are the only complete archimedian fields according to Ostrowski's theorem ([3], Theorem 1.2.6). $\mathbb{C}$ being a finite extension of $\mathbb{R}$, it is enough to compute h_v if $K_v = \mathbb{C}$ by the restriction property given in the definition of h_v. Hence, we can pick $|\cdot|_v = |\cdot|$ the usual complex modulus. Then, we can use the following proposition:

Proposition 7 (Uniformization, [1], VI.5.1.1)**.** Let $E/\mathbb{C}$ be an elliptic curve. Then there exists a lattice $\Lambda \subseteq \mathbb{C}$ (that is, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for some ω_1, ω_2 in $\mathbb{C}$ which are $\mathbb{R}$-linearly independent) such that

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}), z \text{ mod. } \Lambda \mapsto [\wp(z, \Lambda) : \wp'(z, \Lambda) : 1],$$

where

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

is the Weierstrass $\wp$-function relative to Λ, is a complex analytic isomorphism of complex Lie groups.

Since P has infinite order in $E(\mathbb{C})$, $\phi^{-1}(P)$ has infinite order in $\mathbb{C}/\Lambda$, so if we set $\alpha, \beta \in [0, 1[$ such that $\alpha\omega_1 + \beta\omega_2$ is a representative of $\phi^{-1}(P)$, at least one of α, β (say, α) is irrational.

Proposition 8. If α is algebraic, there exists a constant $C_v > 0$ such that for all $\varepsilon' > 0$, there exists an integer $N_{v,\varepsilon'}$ such that for all $m \geq N_{v,\varepsilon'}$, $h_v([m]P) \leq C_v + (1 + \varepsilon') \log m$.

Proof. Since $h_v(Q)+\frac{1}{2}v(x(Q))$ has a v-adic limit when Q approaches O, there is a constant $C_v > 0$ and a v-adic neighbourhood U_ε of O such that for all Q in U_ε,

$$h_v(Q) \leq C_v - \frac{1}{2}v(x(Q)).$$

The uniformization allows us to write $x(Q) = \wp(\phi^{-1}(Q), \Lambda)$. We have

$$[\wp(\phi^{-1}(O), \Lambda) : \wp'(\phi^{-1}(O), \Lambda) : 1] = [0 : 1 : 0]$$

So since $\wp$ is holomorphic on $\mathbb{C} - \Lambda$, $\phi^{-1}(O)$ has to be 0 mod. Λ. Let $r > 0$ be such that

$$\psi : D(r) \subseteq \mathbb{C} \to D(r) + \Lambda \subseteq \mathbb{C}/\Lambda$$

is a homeomorphism of the disk of radius r onto its image in the torus. Then, for Q close enough to O, $\phi^{-1}(Q)$ is in $D(r) + \Lambda$, so

$$z = z(Q) = (\phi \circ \psi)^{-1}(Q)$$

is well-defined and satisfies $x(Q) = \wp(z, \Lambda)$. The meromorphic function $\wp$ has a double pole at every lattice point, so there is a holomorphic function g defined and non-vanishing on some neighborhood of the origin such that on this same neighborhood, $\wp(z) = z^{-2}g(z)$. So for Q close enough to O,

$$x(Q) = z^{-2}g(z) \text{ and } v(x(Q)) = -\log|z^{-2}g(z)| = 2\log|z| - \log|g(z)|.$$

Hence, up to increasing C_v and diminishing ε, we have for all Q in U_ε

$$h_v(Q) \leq C_v - \log|z| \qquad (*)$$

Let m be such that $[m]P \in U_\varepsilon$. ϕ is a group morphism, so $\phi^{-1}([m]P) = m\phi^{-1}(P)$. Hence, $z([m]P) = m(\alpha\omega_1 + \beta\omega_2) - a\omega_1 - b\omega_2$ with $a, b \in \mathbb{Z}$. So

$$|z([m]P)| = |\omega_2| \left|(m\alpha - a)\frac{\omega_1}{\omega_2} + (m\beta - b)\right| \geq |\omega_2| \left|Im\left(\frac{\omega_1}{\omega_2}\right)\right| |m\alpha - a|.$$

Up to increasing C_v (in a manner irrespective of m), for all m such that $[m]P \in U_\varepsilon$ we have

$$h_v([m]P) \leq C_v - \log|m\alpha - a|$$

Now we use the following theorem:

Theorem 5 (Roth)**.** *Let $\alpha \in \overline{\mathbb{Q}}$, $v \in M_\mathbb{Q}$ (extended to $\mathbb{Q}(\alpha)$) and $C, \varepsilon > 0$. Denote*

$$H_\mathbb{Q}(x) = \max(|p|, |q|) \text{ if } x = \frac{p}{q} \in \mathbb{Q},\ \gcd(p, q) = 1.$$

Then the $x \in \mathbb{Q}$ such that

$$|x - \alpha|_v < C H_\mathbb{Q}(x)^{-2-\varepsilon}$$

are only finitely many.

Let $\varepsilon' > 0$. From Roth's theorem, for all but finitely many $x \in \mathbb{Q}$, we have $|x-\alpha| \geq H_\mathbb{Q}(x)^{-2-\varepsilon'}$. So for all but finitely many m,

$$\left|\frac{a}{m} - \alpha\right| \geq H_\mathbb{Q}\left(\frac{a}{m}\right)^{-2-\varepsilon'}$$

We have $H_\mathbb{Q}\left(\frac{a}{m}\right) \leq \max(|a|, |m|)$, and since

$$D(r) \subseteq \left\{\gamma\omega_1 + \delta\omega_2 \mid \gamma, \delta \in \left]-\frac{1}{2}, \frac{1}{2}\right[\right\}$$

we have $m\alpha - a > -\frac{1}{2}$ so $a < m\alpha + \frac{1}{2} \leq m + \frac{1}{2}$ and $m\alpha - a < \frac{1}{2}$ so $a > m\alpha - \frac{1}{2} \geq -\frac{1}{2}$. Hence, $0 \leq a \leq m$ so $\max(|a|, |m|) = m$ and $H_\mathbb{Q}\left(\frac{a}{m}\right) \leq m$. This implies that for all but finitely many m,

$$|m\alpha - a| > m^{-1-\varepsilon'}.$$

So for all but finitely many m such that $[m]P \in U_\varepsilon$,

$$h_v([m]P) \leq C_v + (1+\varepsilon')\log m.$$

Since if $[m]P \notin U_\varepsilon$ we have

$$h_v([m]P) \leq \sup_{Q \notin U_\varepsilon} h_v(Q) < \infty$$

(recall that a local height is bounded on the complement of any neighborhood of O), up to increasing C_v again (in a manner independent of ε'), for all m large enough (say, greater than an integer $N_{v,\varepsilon'}$),

$$h_v([m]P) \leq C_v + (1+\varepsilon')\log m.$$

□

Remark. Now, it would be good to know when α is algebraic (and if it ever is!). It is known that the image of an algebraic number by a Weierstrass $\wp$ function corresponding to an elliptic curve with algebraic coefficients is transcendental ([6], (3.1), p. 645), so $\alpha\omega_1 + \beta\omega_2$ cannot be algebraic (since its image by $\wp$ is $x(P) \in K$). But since $\frac{\omega_1}{\omega_2}$ is algebraic ([1], proof of VI.5.5), we could *a priori* have $\alpha\omega_1 + \beta\omega_2 = \left(\alpha\frac{\omega_1}{\omega_2} + \beta\right)\omega_2$ to be transcendental if both α and β are algebraic and ω_2 is transcendental (the product of an algebraic and a transcendental number is transcendental; if it were algebraic, we could multiply by the inverse of the algebraic one (which is algebraic), and it would still be algebraic)...

Panda's theorem (which we discovered after doing the computation above) still holds if α is algebraic because after establishing in her Lemma 19 that $h_v([m]P) = O(\log|a_m|)$, where $a_m \in \mathbb{C}$ is the representative of $m\phi^{-1}(P)$ in the fundamental parallelogram for Λ, she uses the following theorem, which makes no hypothesis on P:

Theorem 6 ([5], 3.3). *Let E/K be an elliptic curve defined over a number field $K \subseteq \mathbb{C}$. Fix an isomorphism $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ for an appropriate lattice Λ generated by ω_1, ω_2. Let $P \in E(K)$ be a non-torsion point and $z \in \mathbb{C}$ such that $\phi(z \text{ mod. } \Lambda) = P$. Then there is a constant $C = C(P) > 0$ such that for all rational numbers $\frac{l_1}{m}, \frac{l_2}{m}$ with $l_1, l_2, m \in \mathbb{Z}$,*

$$\left| z - \left(\frac{l_1}{m}\omega_1 + \frac{l_2}{m}\omega_2\right)\right| \geq e^{-C\max(1,\log|m|)}$$

Using this theorem in our situation, starting from $(*)$ and choosing m such that $[m]P \in U_\varepsilon$, we get

$$|z([m]P)| = m\left|\alpha\omega_1 + \beta\omega_2 - \left(\frac{a}{m}\omega_1 + \frac{b}{m}\omega_2\right)\right| \geq me^{-C\max(1,\log m)}$$

So the equation $(*)$ yields, when $\log m \geq 1$:

$$h_v([m]P) \leq C_v + (C(P)-1)\log m$$

where unfortunately we do not have much control over $C(P)$.

9 Ideas for further developments

Now that we know there exist infinitely many places v of K such that $h_v([m]P) \neq 0$ for some m, it could be interesting to know more about how many places are such that $h_v([m]P) \neq 0$ for a given m. Indeed, for a fixed $m \in \mathbb{N}$, we know that $h_v([m]P) \neq 0$ for only finitely many $v \in M_K$, so we can set

$$C(m) = \max\{p \text{ prime} \mid \text{there exists } v \in M_K \text{ such that } h_v([m]P) \neq 0 \text{ and } v|p\}$$

Then, for $p > C(m)$ and $v \in M_K$ such that $v|p$, the order of P mod. v does not divide m.

Finding better estimates for the local heights could be a way to estimate $C(m)$ using the equation that links local and global heights. For example, since we have the easy inequality

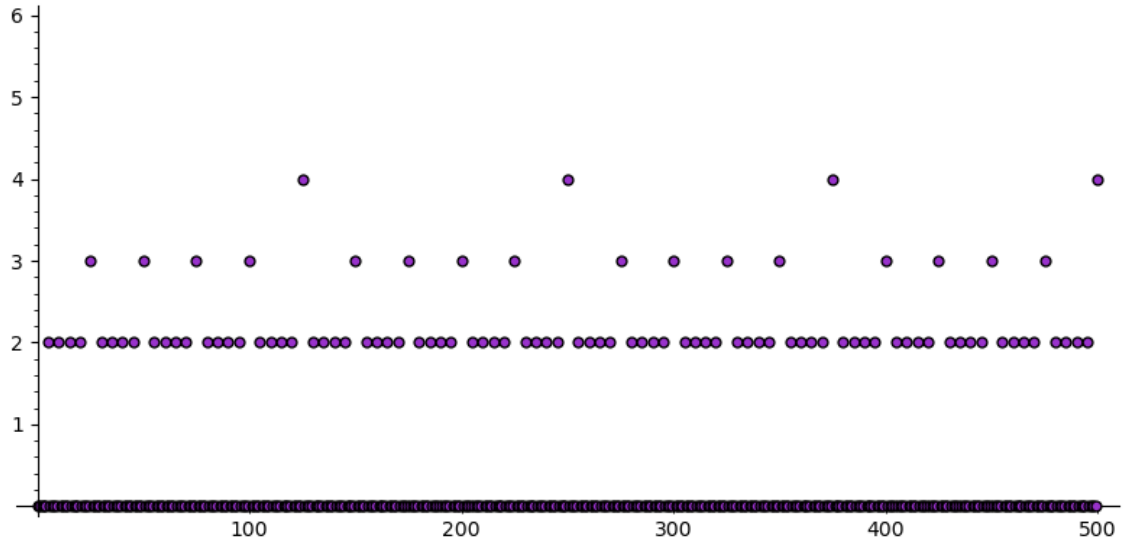
$h_v([m]P) \leq m^2 h(P)$, a formula linking $h_v([m]P)$ to the prime p such that v lies over p could yield an upper bound for $C(m)$.

To see what the $h_v([m]P)$ look like, I used Sage again to compute the $h_p([m]P)$ for $m \leq 500$ for curves of the type

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

with $A, B \in \mathbb{Z}$ such that E has non-zero rank and integer j-invariant. Figure 3 gives an example of what one can get this way (of course, I also looked at the actual values, not just the graph).

Figure 3: 5-adic height of $[m]P$ (y axis) as a function of m (x axis), for the elliptic curve $y^2 = x^3 + 3x + 2$ and $P = (2, 4)$.



In all the examples I tried, $h_p([m]P)$ as a function of m looked fractal and seemed to have a quite simple expression. In the following table, I gathered a few examples I computed. I always picked P to be a generator (or one of the generators) for torsion points, except for $[3] * (-1, 1)$ (curve $y^2 = x^3 + 2$) when Sage ran for 25 minutes.

Equation	Rank	j-invariant	Discriminant	P	p	$h_p([m]P)$ for $m \leq 500$
$y^2 = x^3 + 2$	1	1728	-3456	(-1,1)	5	$\mathbb{1}_{6\|m}(2 + v_5(m))$
					7	$\mathbb{1}_{3\|m}(1 + v_7(m))$
				[3]*(-1,1)	5	$\mathbb{1}_{2\|m}(2 + v_5(m))$
$y^2 = x^3 + 3x$			-1728	(1,2)		$\mathbb{1}_{5\|m}(1 + v_5(m))$
$y^2 = x^3 + 3x + 2$		864	-3456	(2,4)		
$y^2 = x^3 + 5$		0	-10800	(-1,2)	7	$\mathbb{1}_{7\|m}(1 + v_7(m))$
					11	$\mathbb{1}_{12\|m}(1 + v_{11}(m))$
$y^2 = x^3 + 6x + 4$	2	1728	-20736	(0,2)	5	$\mathbb{1}_{9\|m}(1 + v_5(m))$

To partly explain this, we can look at Panda's proof of the fact that $h_v([m]P) = O(\log m)$ if v is non-archimedian (her Theorem 24), where she almost proves, but does not state explicitly, a stronger result. In that proof, she establishes that if v is normalized,

$$h_v([m]Q) = v(m) + O(1) \text{ if } Q \text{ mod. } v \text{ is } 0. \qquad (**)$$

Let's denote $E_1(K)$ the kernel of the reduction map $E(K) \to \tilde{E}_v(k_v)$, which is a group homomophism according to the proof of [1], VII.2.1. Then, $E(K)/E_1(K)$ is isomorphic to $\tilde{E}_v(k_v)$ which is finite, so she calls r the order of P mod. $E_1(K)$ (equivalently, the order of P mod. v).

- If r does not divide m, $[m]P$ is in $E(K) - E_1(K)$ and we know that h_v is constant (and zero in our case) on this subset.

- If r divides m,

$$h_v([m]P) = h_v\left(\left[\frac{m}{r}\right][r]P\right) = v\left(\left[\frac{m}{r}\right]\right) + O(1) = v(m) + O(1).$$

So we get the following estimate:

Proposition 9. Let v be a normalized discrete valuation on K, let r be the order of P mod. v. Then

$$h_v([m]P) = v(m) + O(1) \text{ when } m \to \infty,\ m \in r\mathbb{Z},$$

and

$$h_v([m]P) = 0 \text{ for } m \notin r\mathbb{Z}.$$

Now, the indicator functions in the previous table correspond to the $\mathbb{1}_{r|m}$, where r is the order of P mod. v (this was confirmed computing the relevant orders on Sage), and the estimate for $m \in r\mathbb{Z}$ corresponds to what I observed. As for the simple and noise-free quality of the formulae I observed for $m \in r\mathbb{Z}$, which suggest possible refinements to $(**)$, I do not have an explanation for this yet.

10 Other studied topics

I studied the most part of [1], including the distinction between supersingular and ordinary curves over finite fields (this aspect, which was a big part of my SageMath simulations, ended up not being relevant to the main result so I removed it here).

11 Working conditions

I worked with Yunqing Tang at University of California, Berkeley, from April to August 2023. I was able to attend a few seminars on number theory, algebraic geometry and logics at the university before the end of the academic year. I also attended a few seminars at MSRI, including some from a diophantine geometry workshop (24th to 28th of July). I took part in a workshop on algebraic geometry (1st to 5th of May), which included problem sets organized by Hector Pasten.

References

[1] Silverman, J. H. (2009). *The arithmetic of elliptic curves*. Springer Science & Business Media. https://doi.org/10.1007/978-0-387-09494-6 2, 3, 4, 6, 7, 8, 11, 12, 14, 15, 16

[2] Silverman, J. H. (2013). *Advanced topics in the arithmetic of elliptic curves*. Springer Science & Business Media. https://doi.org/10.1007/978-1-4612-0851-8 10, 11

[3] Bombieri, E., & Gubler, W. (2007). *Heights in Diophantine geometry*. Cambridge University Press. https://doi.org/10.1017/CBO9780511542879 5, 6, 12

[4] Panda, C. B. (2013). *Néron local height functions for elliptic curves* (Master's thesis, Leiden University, Leiden, Netherlands). Retrieved from https://algant.eu/documents/theses/panda.pdf 12

[5] Baker, M., Ih, S.-I., & Rumely, R. (2005). A finiteness property of torsion points. https://doi.org/10.48550/ARXIV.MATH/0509485 14

[6] Lang, S. (1971). Transcendental numbers and diophantine approximations. *Bulletin of the American Mathematical Society, 77*(5), 635–678. https://doi.org/10.1090/s0002-9904-1971-12761-1 14