On p-adic elliptic logarithms and p-adic approximation lattices

Christian Wuthrich

April 26, 2006

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime number. Based on numerical evidence, we formulate a conjecture on the height of rational points on E whose coordinates have high powers of p in the denominator. On one hand, this conjecture is linked to a p-adic elliptic analogue of a conjecture of Lang-Waldschmidt on linear forms of logarithms. On the other hand, we reformulate the conjecture in terms of p-adic approximation lattices; namely the lattice type of a certain point on $\mathbb{P}^1(\mathbb{Q}_p)$ should be maximal. We show that the average lattice type of points on $\mathbb{P}^1(\mathbb{Q}_p)$ is indeed maximal.

1 Introduction

Let E be an elliptic curve defined over the field of rational numbers $\mathbb{Q}$ given by a fixed Weierstrass equation

$$y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6.$$

We suppose that the rank r of the Mordell-Weil group $E(\mathbb{Q})$ is positive. Let p be a prime number. For each $k \geqslant 1$ we define the following subgroup of $E(\mathbb{Q})$:

$$B_p(k) = \{P \in E(\mathbb{Q}) \mid \mathrm{ord}_p(x(P)) \leqslant -2k\}$$

If the equation is minimal at p, we may also characterise $B_p(k)$ as $E(\mathbb{Q}) \cap \widehat{E}(p^k\mathbb{Z}_p)$ where $\widehat{E}$ is the formal group associated to $E/\mathbb{Q}_p$. The index of $B_p(k)$ in $E(\mathbb{Q})$ divides $c_p \cdot \#\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p) \cdot p^{k-1}$ with c_p being the Tamagawa number and $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ the group of non-singular points on the reduction of E at p.

Furthermore, we define $\hat{m}_k$ to be

$$\hat{m}_p(k) = \min\left\{ \sqrt{\hat{h}(P)} \;\middle|\; 0 \neq P \in B_p(k) \right\}$$

Here $\hat{h}(P)$ denotes the canonical height of P.

Conjecture 1. *There exists constants $C > c$ depending on E and p such that for all k, we have*

$$\frac{1}{r} \cdot \log(p) \cdot k + C \quad \geqslant \quad \log\big(\hat{m}_p(k)\big) \quad \geqslant \quad \frac{1}{r} \cdot \log(p) \cdot k + c$$

where r is the rank of E.

We may also announce a weaker form of the conjecture :

Conjecture 2. *For any p, there exists constants $D > d$ such that for all k*

$$D \quad > \quad \frac{\log(\hat{m}_k)}{\log(p) \cdot k} \quad > \quad d \quad > \quad 0.$$

This paper is about different reformulations of these conjectures and evidence in their favour. Here is a first easy result in this direction.

Proposition 1. *The conjecture 1 holds if the rank r is equal to 1.*

Proof. Let P_1 be a point of minimal height in $B_p(1)$. By the quadraticity of the canonical height, we know that $P_k = p^k \cdot P_1$ is a point of minimal height in $B_p(k)$. Now we compute

$$log\big(\hat{m}_p(k)\big) = \log \sqrt{\hat{h}(P_k)} = \tfrac{1}{2}\log\big(p^{2k} \cdot \hat{h}(P_1)\big) = \log(p) \cdot k + \tfrac{1}{2}\log \hat{h}(P_1).$$

□

Using the convex body theorem of Minkowski we will show in section 2 the upper bound in the stronger conjecture, namely

Proposition 2. *There exists a constant C, depending on E and p, such that*

$$\frac{1}{r} \cdot \log(p) \cdot k + C \quad \geqslant \quad \log\big(m_p(k)\big).$$

In section 3, we will present numerical evidence in favour of the conjectures. The values obtained are in good agreement with both conjectures and not surprisingly the error terms C and c in conjecture 1 seem to be related to the regulator of the curve.

There are links between these conjectures and linear forms in p-adic elliptic logarithms. Unfortunately the results in this field known to the author do not permit to prove any of the two conjectures. The stronger of the two conjectures is similar to a well-known conjecture of Lang and Waldschmidt. We present a version of it in section 4.

Since the growth of the formula is linear in conjecture 1, we may create a generating function and the statement of the conjectures becomes a question about the domain of convergence of this analytic function.

The most important reformulation is concerned with so-called p-adic approximation lattices. Let k be an integer. Given a point $z = (z_1, : z_2 : \ldots : z_r)$ in the projective space $\mathbb{P}^{r-1}(\mathbb{Q}_p)$ over the p-adic numbers, one may consider the lattice

$$L(z,k) = \{(x_1, x_2, \ldots x_r) \in \mathbb{Z}^r \;\mid\; x_1 \cdot z_1 + \cdots + x_r \cdot z_r \equiv 0 \pmod{p^k}\}.$$

The conjectures can now be reformulated as a formula for the growth of the length of the minimal vector

$$\mathrm{minL}(z,k) = \min\{\|x\| \;\mid\; 0 \neq x \;\in L(z,k)\}$$

in the lattice $L(z,k)$ when z is formed by the values of the p-adic elliptic logarithm evaluated on a certain set of r linearly independent points in $E(\mathbb{Q})$.

For the sake of simplicity, the theory is only developed in the case $r = 2$. We say that $z \in \mathbb{P}^1(\mathbb{Q}_p)$ is of lattice type α if the length of the minimal vector satisfies

$$\log(\mathrm{minL}(z,k)) = \alpha \cdot k + \mathbf{O}(1) \qquad \text{as } k \longrightarrow \infty.$$

The notion is independent on the choice of the norm $\|\cdot\|$ on $\mathbb{Z}^2 \otimes \mathbb{R}$. The main result is concerned with the average value of the lattice type on $\mathbb{P}^1(\mathbb{Q}_p)$. In theorem 10 and theorem 11, we prove the following precise statement. If $\bar{z}$ is an element of $\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$ write simply $L(\bar{z})$ for $L(z,k)$ where z is any lift of $\bar{z}$ to $\mathbb{P}^1(\mathbb{Z}_p)$.

Theorem 3.
Let $\mu(p^k)$ be the average of the logarithms of the length of the minimal vectors in all the lattices $L(\bar{z})$ where $\bar{z}$ runs over all elements in $\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$. Then

$$\frac{1}{2}\log(p) \cdot k - 0.428079 + \mathbf{O}(k \cdot p^{-k/2}) \geqslant \mu(p^k) \geqslant \frac{1}{2}\log(p) \cdot k - 0.725791 + \mathbf{O}(k^2 \cdot p^{-k/2}).$$

Numerical computation of a large amount of exact values of $\mu(n)$ (here n may be any integer and the definition of $\mu(n)$ is similar to $\mu(p^k)$) suggests that the value $\mu(n) - \frac{1}{2}\log(m)$ converges to a certain value close to -0.485. This is contained in conjecture 4.

The theorem can be interpreted loosely by saying that the average lattice type of a p-adic number is $\frac{1}{2}\log(p)$, which is also the maximal possible lattice type. Hence if we believe that the p-adic elliptic logarithms of elements in $E(\mathbb{Q})$ are in some sense random numbers, or say not too particular, we must believe in the conjectures to be true. Though a proof of them seems not within the reach of the presented methods.

2 Other norms

It is well-known (see [Sil92]) that for all k (expect when $k = 1$ and $p = 2$, which we may exclude), the group $B_p(k)$ is free of rank r. We choose a basis $\{P_1, \dots P_r\}$ of the free part of $E(\mathbb{Q})$ and consider it as a lattice with the bilinear form provided by the canonical height pairing. The subgroups $B_p(k)$ form then a sequence of sublattices and we investigate the length $\hat{m}_p(k)$ of the minimal vector of the $B_p(k)$. The function

$$\|P\|_h = \sqrt{\hat{h}(P)}$$

induces a norm on $E(\mathbb{Q}) \otimes \mathbb{R}$. Let $\|\cdot\|$ be any other norm on $E(\mathbb{Q}) \otimes \mathbb{R}$. Define $m_p(k)$ to be the length of the minimal vector of $B_p(k)$ with respect to this norm, i.e.

$$m_p(k) = \min\{\|P\| \ \mid 0 \neq P \in B_p(k)\}.$$

There exists two constants c_1 and c_2 such that

$$c_1 \cdot \sqrt{\hat{h}(P)} \geqslant \|P\| \geqslant c_2 \cdot \sqrt{\hat{h}(P)}.$$

Hence we deduce the inequalities

$$\log c_1 + \log\big(\hat{m}_p(k)\big) \geqslant \log\big(m_p(k)\big) \leqslant \log c_2 + \log\big(\hat{m}_p(k)\big)$$

and we may therefore replace in both conjectures $\hat{m}_p(k)$ by $m_p(k)$, if we allow the constants C and c to depend on the chosen norm. This proves the following lemma.

Lemma 4. *The conjecture 1 is equivalent to the statement that, for any norm on $E(\mathbb{Q}) \otimes \mathbb{R}$, there exists constants C and c with*

$$\frac{1}{r} \cdot \log(p) \cdot k + C \quad \geqslant \quad \log\big(m_p(k)\big) \quad \geqslant \quad \frac{1}{r} \cdot \log(p) \cdot k + c$$

for all k.

In what follows we will mainly consider the usual norm with respect to a chosen basis $\{P_1, \dots P_r\}$ of the free part of $E(\mathbb{Q})$:

$$\|\alpha_1 P_1 + \cdots \alpha_r P_r\| = \sqrt{\alpha_1^2 + \cdots \alpha_r^2}$$

This interpretation gives us easily the following

Proposition 5. *There exists a constant C such that*

$$\frac{1}{r} \cdot \log(p) \cdot k + C \quad \geqslant \quad \log\big(m_p(k)\big).$$

In particular, the first half of the conjecture 1 is true.

Proof. By the convex body theorem of Minkowski (see for instance [Cas97], Theroem 3.II), there exists a constant γ such that

$$\gamma \cdot \det(B_p(k))^{\frac{1}{r}} \geqslant m_p(k).$$

Since we know that the index of $B_p(k)$ is of the form $c \cdot p^k$ for some constant $c \in \mathbb{Q}$, which is depending on p, we have

$$\log(\gamma) + \frac{1}{r}\log(c \cdot p^k) \geqslant \log\big(m_p(k)\big).$$

□

Note that the constant C is effectively computable.

3 Numerical results supporting the conjectures

Even though the conjectures may appear too daring at first, the numerical evidence in favour of them is overwhelming.

First, we stick to a single curve

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

labelled 389a1 in the tables of Cremona. The points $P_1 = (0, 0)$ and $P_2 = (1, 0)$ form a basis of $E(\mathbb{Q})$ of minimal canonical height.

If for instance $p = 3$, we may explicitly compute the the subgroup $B_3(1)$: the points $Q_1 = P_1 + 2\,P_2 = (\frac{1}{9}, -\frac{19}{27})$ and $Q_2 = 2 \cdot P_1 - 2 \cdot P_2 = (\frac{10}{9}, \frac{8}{27})$ form a $\mathbb{Z}$-basis.

As we noticed in lemma 4, we may as well work with the minima of the $\|\cdot\|_2$-norm with respect to the given basis $\{Q_1, Q_2\}$. Moreover, we may skip the computations of the minimal vectors of $B_p(k)$. In fact the first vector of an LLL-reduced basis of $B_p(k)$ will do as the following lemma shows

Lemma 6. *Let R_k be the first vector of an LLL-reduced basis of $B_p(k)$, then $m_p(k) \geqslant A \cdot \|R_k\|_2$ with $A = 2^{-(r-1)/2}$.*

This is Lemma 3.4 in [dW89]. In particular, the growth of $\log \|R_k\|_2$ as $k \longrightarrow \infty$ is the same as for $\log(\hat{m}_p(k))$.

The figure 1 shows the values of $\log(\hat{m}_p(k))$ for the primes p between 2 and 30 and for k up to 100. The lines represent the predicted slopes $\frac{1}{2} \cdot \log(p) \cdot k$. Conjecture 1 states that for every given p the dots do not differ from the line by more than a fixed constant.

Next, we provide evidence for the consistency by varying the curve but fixing the prime $p = 3$. We use five curves of rank 2 and five curves of rank 3. Namely they are

389a1, 433a1, 446d1, 563a1, 571b1 and
5077a1, 11197a1, 11642a1, 13766a1.

Figure 2 shows the values of $\log(\hat{m}_3(k))$ for all of these curves. one sees immediately that the values of the curves of rank 2 (corresponding to the darker points) are close to the line $\frac{1}{2}\log(3) \cdot k$, while the curves of rank 3 stay near the line of slope $\frac{1}{3}\log(3)$.

In order to refine this statement, we give a list here of the maximum of the difference

$$\delta_k = |\log(\hat{m}_3(k)) - \tfrac{1}{r}\log(p) \cdot k|$$

for the curves listed above and $k \leqslant 100$.

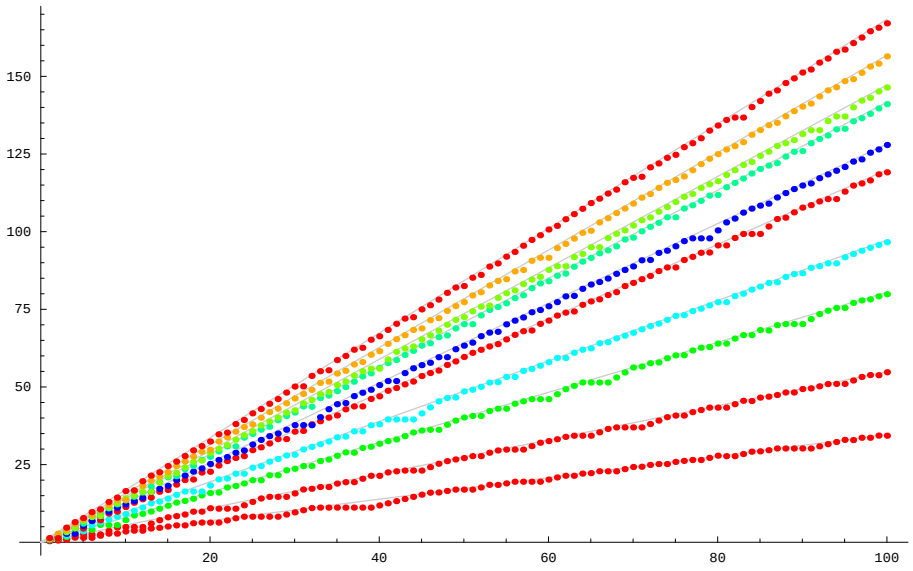


Figure 1: The values of $\log(\hat{m}_p(k))$ for the curve 389a1

Curve	$\max(\delta_k)$
389a1	1.5278
433a1	0.9759
446d1	1.5396
563a1	2.1167
571b1	1.7373
5077a1	1.9941
11197a1	1.1494
11642a1	1.3730
13766a1	0.9662

4 Linear forms in p-adic elliptic logarithms

Let $\mathscr{L}_p\colon \widehat{E}(p\mathbb{Z}_p) \longrightarrow p\mathbb{Z}_p$ be the formal p-adic elliptic logarithm on E. Write $u_i = \mathscr{L}_p(Q_i)$ where $\{Q_1, \ldots, Q_r\}$ is a basis (of the free part) of $B_p(1)$. Let $\Lambda = \alpha_1 u_1 + \cdots + \alpha_r u_r$ with α_i integers not all equal to zero. We write $\|\vec{\alpha}\|_\infty = \max\{|\alpha_i| \mid 1 \leqslant i \leqslant r\}$ for the sup-norm on $B_p(1) \otimes \mathbb{R}$.

To say that $|\Lambda|_p = p^{-k}$ is the same as to say that $Q = \alpha_1 Q_1 + \cdots \alpha_r Q_r$ belongs to $B_p(k)$. According to the strong conjecture 1, there should exist a constant c such that

$$\log \|\vec{\alpha}\|_\infty \geqslant \log\big(m_p(k)\big) \geqslant \frac{1}{r} \cdot \log(p) \cdot k + c$$

where $m_p(k)$ is with respect to the norm $\|\cdot\|_\infty$. We may rewrite this as

$$\log |\Lambda|_p = -\log p \cdot k \geqslant -r \log \|\vec{\alpha}\|_\infty + rc$$

and conclude that the conjecture implies the existence of a constant c_1 such that

$$\log |\Lambda|_p \geqslant -r \log\big(\max\{|\alpha_i|\}\big) + c_1.$$

The constant c_1 would depend on the curve E, the base field (which we fixed anyway to $\mathbb{Q}$), the prime p and the chosen u_i. The proposition 5 shows that this is the strongest possible conjecture in this direction.

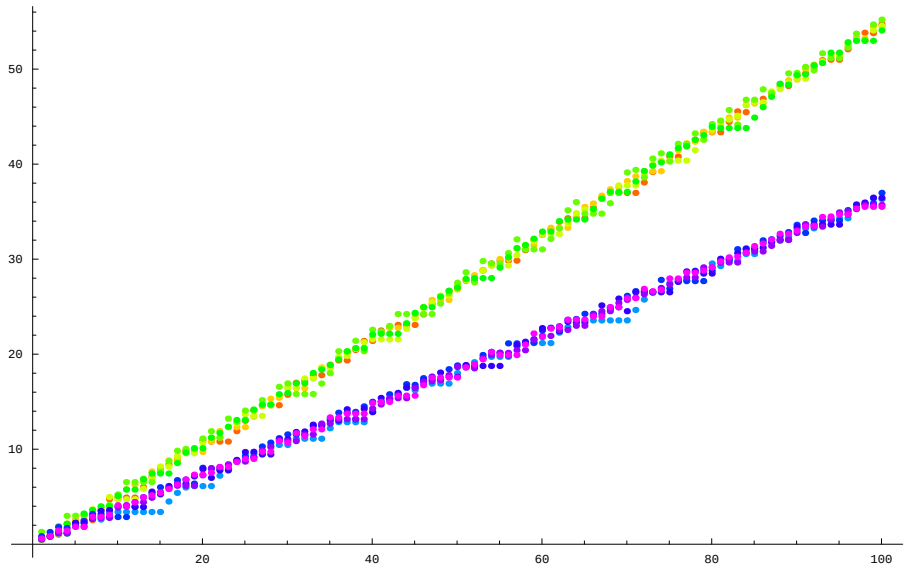


Figure 2: The values of $\log(\hat{m}_3(k))$ for some curves of rank 2 and 3

This conjecture is far away from the known bounds for linear forms in p-adic elliptic logarithms. In [Ber78], Bertrand proves (under the assumption that the curve has complex multiplication) that

$$\log|\Lambda|_p > d_1 \cdot \log\big(\max\{|\alpha_i|\}\big)^{16}.$$

In the more recent article [RU96], the authors restrict themselves to the case of rank $r = 2$. They show that

$$\log|\Lambda|_p > d_2 \cdot \big(\log\max\{|\alpha_i|\}\big) \cdot \big(\log\log\max\{|\alpha_i|\}\big)^3. \tag{1}$$

with a explicit and astronomic constant $d_2 < 0$. If the last factor were not there we could prove conjecture 2. The best we can do is

Proposition 7. *Let $E/\mathbb{Q}$ be an elliptic curve of rank 2. For any prime p, there exists a constant $d' > 0$ such that for all k we have*

$$\frac{\log\big(\hat{m}_p(k)\big)}{\log(p)\cdot k} > \frac{d'}{\log(k)^3}.$$

Proof. Defining the left hand side of (1) to be $-\log(p)\cdot k$, we obtain the estimate

$$\frac{\log\big(\hat{m}_p(k)\big)}{\log(p)\cdot k} > \frac{|d_2|}{\log\log\big(m_p(k)\big)^3}.$$

Now we may use the proposition 5 to get the bound

$$\frac{\log\big(\hat{m}_p(k)\big)}{\log(p)\cdot k} > \frac{|d_2|}{\log\big(\frac{1}{2}\log(p)\cdot k + C\big)^3}.$$

which is of the desired form. □

We hope that a forthcoming paper of Noriko Hirata-Kohno will actually proof better bounds that should imply conjecture 2.

The conjecture 1 is a actually slight modification of the conjecture of Lang-Waldschmidt (see page 212 in [Lan78]). We refer to the "conjecture optimiste" of Pilippon in [Phi99] which concerns the ordinary p-adic logarithm rather than the elliptic p-adic logarithm. His conjecture gives a more precise form of the constant c but a slightly weaker growth coefficient. We state here a reformulated and weakened form of this conjecture :

Conjecture 3. *(Version of Lang-Waldschmidt) Let $a_1, \dots a_r$ be fixed positive integers and p a fixed prime. Given any $\varepsilon > 0$, there exists a constant c_ε with the following property: if the integers $b_1, \dots b_r$ are such that*

$$0 \neq b_1 \cdot \log_p(a_1) + \cdots + b_r \cdot \log_p(a_r) \in p^k \, \mathbb{Z}_p$$

then, writing $\|b\|_\infty$ for the maximum of $|b_i|$ as $1 \leqslant i \leqslant r$, we have

$$\log(\|b\|_\infty) \geqslant \frac{1}{(1+\varepsilon) \cdot r} \cdot \log(p) \cdot k + c_\varepsilon.$$

Needless to say that this conjecture seems to be out of reach by the current methods of linear forms of logarithms.

5 Siegel's theorem

Of course, there is a close link to the following theorem of Siegel (see [Sil92, Theorem IX.3.1]) on integral points in $E(\mathbb{Q})$. Define the logarithmic p-adic distance on $E(\mathbb{Q}_p)$ to be

$$\delta_p(P-Q) = \log(p) \cdot k \quad \text{ if and only if } \quad P - Q \in \widehat{E}(p^k \mathbb{Z}_p) \setminus \widehat{E}(p^{k+1} \mathbb{Z}_p)$$

Let Q be a point in $E(\mathbb{Q})$ and let P_n be a sequence of points in $E(\mathbb{Q})$ approaching Q in the p-adic topology. Siegel's theorem asserts that, if the naive height of P_n tends to infinity as $n \longrightarrow \infty$ then

$$\lim_{n \to \infty} \frac{\delta_p(P_n - Q)}{h_{\text{naive}}(P_n)} = 0$$

In fact the weak conjecture 2 implies that the quotient

$$\theta_p(P_n) = \frac{\delta_p(P_n - Q)}{\log(\hat{h}(P_n))}$$

is bounded from above and the strong conjecture 1 would claim that the lim sup of these quotients is less or equal to $\frac{r}{2}$.

It is plausible that a proof of either one of the conjectures would give rise to a better way of computing S-integral points in $E(\mathbb{Q})$.

6 Generating function

There is an obvious way of encoding the conjectures into an analytic function. Given an elliptic curve $E/\mathbb{Q}$ and a prime p, we may write

$$\zeta_p(T) = \sum_{k \geqslant 0} \hat{m}_p(k) \cdot T^k \quad \in \mathbb{Z}[\![T]\!]$$

where $\hat{m}_p(0)$ is simply the minimum of the canonical height for all points in $E(\mathbb{Q})$ of infinite order. Obviously $\zeta_p(T) = 0$ if the rank of the curve is zero.

Proposition 8. *Let $p > 2$ be a prime. If the curve E has rank 1, then*

$$\zeta_p(T) = R \cdot \left(1 + \frac{b_p \, T}{1 - p \, T}\right)$$

where $R = \sqrt{\text{Reg}(E/\mathbb{Q})}$ is the square root of the regulator of $E(\mathbb{Q})$ and b_p is the index of $B_p(1)$ in $E(\mathbb{Q})$ modulo its torsion subgroup.

Proof. Let P_0 be a generator of the free part of $E(\mathbb{Q})$. We may take P_0 of minimal height. The points $b_p \cdot p^{k-1} \cdot P_0$ are points of minimal height in $B_p(k)$. Hence

$$\begin{aligned}\zeta_p(T) &= \sqrt{\hat{h}(P_0)} + \sum_{k\geqslant 1} \sqrt{\hat{h}(b_p\, p^{k-1}\, P_0)} \cdot T^k \\ &= \sqrt{\hat{h}(P_0)} \cdot \Big(1 + \frac{b_p}{p} \sum_{k\geqslant 1} (p\,T)^k\Big) \\ &= R \cdot \Big(1 + \frac{b_p}{p} \frac{p\,T}{1-p\,T}\Big)\end{aligned}$$

□

In particular, for a curve of rank 1, the generating function $\zeta_p(T)$ is a rational function with a single simple pole at $T = \frac{1}{p}$ of residue $-R\,b_p/p^2$.

Theorem 9.
Let $E/\mathbb{Q}$ be a curve of rank $r > 0$ and let p be a prime.

- *$\zeta_p(T)$ is an analytic function on the disc centred at $T = 0$ of radius $\rho = p^{-1/r}$.*
- *Conjecture 2 would imply that the radius of convergence of $\zeta_p(T)$ is less than 1.*
- *Conjecture 1 is equivalent to the statement that $\zeta_p(T)$ has a simple pole at $T = p^{-1/r}$.*

Proof. The first part is a consequence of Proposition 5. We know that there exists a constant C and conjecture 2 claims that there are constants d and c such that

$$\frac{1}{r}\log(p)k + C \geqslant \log m_p(k) \geqslant d\log(p)k + c$$

Moreover the stronger conjecture 1 is equivalent to $d = \frac{1}{r}$. We compute

$$e^C \cdot p^{\frac{k}{r}} \geqslant m_p(k) \geqslant e^c \cdot p^{d\,k}$$

and deduce from it that

$$m_p(0) + e^C \cdot \frac{p^{\frac{1}{r}}\,T}{1-p^{\frac{1}{r}}\,T} \geqslant \zeta_p(T) \geqslant m_p(0) + e^c \cdot \frac{p^d\,T}{1-p^d\,T}$$

and the theorem follows. □

The results in [RU96] as formulated in 7 only give that the radius of convergence of $\zeta_p(T)$ is less or equal to 1, which is obvious anyway for a series with integer coefficients.

7 p-adic approximation lattices

For the following considerations, we will stick to the situation when $E(\mathbb{Q})$ has rank 2. We fix a basis $\{Q_1, Q_2\}$ of $B_p(1)$. Let $z_1 = \mathscr{L}_p(Q_1)$ and $z_2 = \mathscr{L}_p(Q_2)$. Note that we can describe $B_p(k)$ by the following formula

$$B_p(k) = \{a_1Q_1 + a_2Q_2 \mid a_1z_1 + a_2z_2 \equiv 0 \pmod{p^k}\}.$$

This follows from the fact that $P = a_1Q_1 + a_2Q_2$ is in $B_p(k)$ if and only if $\mathscr{L}_p(P) = a_1z_1 + a_2z_2$ belongs to p^k.

Write z for the point $(z_1 : z_2)$ in $\mathbb{P}^1(\mathbb{Q}_p)$. Since $\{Q_1, Q_2\}$ is a basis of $B_p(1)$, we know that z_1 or z_2 is of valuation 1. So we may reduce the point $(\frac{z_1}{p} : \frac{z_2}{p})$ to obtain a point $\bar{z}_k$ of $\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$. The point $\bar{z}_k$ defines a line in $\mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}$ passing through $(0,0)$ and $B_p(k)$ is the preimage of this line under the map $B_p(1) \approx \mathbb{Z} \times \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}$.

This motivates the following definition. Let $n > 1$ be an integer. Given a point $\bar{z}$ in $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$, we define a sublattice

$$L(\bar{z}) = \{(a_1, a_2) \in \mathbb{Z}^2 \mid a_1 z_1 + a_2 z_2 \equiv 0 \pmod{n}\}$$

of $\mathbb{Z}^2$ of index n. If n is a power of p, a sublattice of this form will be called a *p-adic approximation lattice* in $\mathbb{Z}^2$, following [dW89]. See also [Sma98] for a more recent treatment of the topic. The minimum of this lattice with respect to the usual bilinear form is denoted by

$$\mathrm{minL}(\bar{z}) = \min\Big\{ \sqrt{a_1^2 + a_2^2} \;\Big|\; 0 \neq (a_1, a_2) \in L(\bar{z}) \Big\}$$

Note that there is are some easy relations, like $\mathrm{minL}(z_1 : z_2) = \mathrm{minL}(z_1 : -z_2) = \mathrm{minL}(z_2 : z_1) = \mathrm{minL}(z_2 : -z_1)$. By Minkowski's bound, there is an inequality

$$\log\big(\mathrm{minL}(\bar{z})\big) \leqslant \log\big(\gamma \cdot \sqrt{n}\big) = \frac{1}{2}\log(n) + \log(\gamma)$$

with $\gamma = \sqrt{2}/\sqrt[4]{3} = 1.07457\ldots$. The value of this lattice constant can be found in the appendix to [Cas97].

We are interested in the following mean

$$\mu(n) = \frac{1}{\#\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})} \cdot \sum_{\bar{z} \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})} \log\big(\mathrm{minL}(\bar{z})\big)\,.$$

Conjecture 4. *There exists a constant $\hat{\gamma}$ such that*

$$\mu(n) \sim \frac{1}{2} \cdot \log(n) + \hat{\gamma} \qquad \text{as } n \longrightarrow \infty.$$

In order to illustrate the above conjecture we include in figure 3 here a graphic of the first few values of $\mu(n) - \frac{1}{2}\log(n) - \log(\gamma) + \frac{1}{2}$. The darker points correspond to values of n which are prime. The numerical experience would suggest that the value of $\hat{\gamma}$ is around -0.485. The

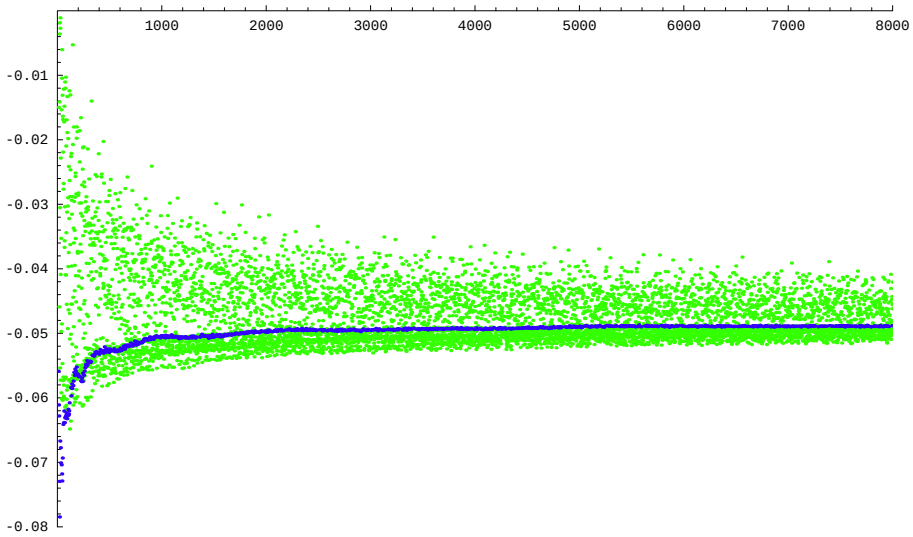


Figure 3: The difference between $\mu(n)$ and $\frac{1}{2}\log(n) + \log(\gamma) - \frac{1}{2}$

following theorem shows that $\hat{\gamma}$, if it exists, is smaller than $\log(\gamma) - \frac{1}{2} = -0.428079$.

Theorem 10.
We have

$$\frac{1}{2}\log(n) + \log(\gamma) - \frac{1}{2} + \mathbf{O}(\log(n)\cdot n^{-1/2}) \geqslant \mu(n).$$

We do not claim that the error term in the theorem is optimal. The bounds on the numbers of integral points inside discs used in the proof are the easy and obvious bounds rather than the best known bounds in [Hux03].

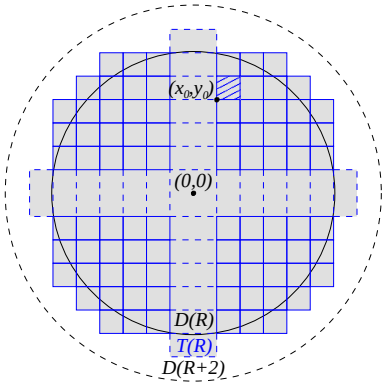
Proof. For any $r > 0$, we denote by $D(r)$ the closed disc of radius r centred at 0. Let $B(r) = \mathbb{Z}^2 \cap D(r)$ denote the set of integral points $(x, y) \in \mathbb{Z}^2$ inside $D(r)$. Let $R = \gamma \cdot \sqrt{n}$. By Minkowski's convex body theorem, we know that every lattice $L(\bar{z})$ has at least one point in $B(R)$, but not every point in $B(R)$ figures among the smallest vectors; hence $\mu(n)$ is smaller than the mean of $\frac{1}{2}\log(x^2+y^2)$ on $B(R)$, i.e.

$$\mu(n) \leqslant \frac{1}{\#B(R)} \cdot \sum_{(x,y)\in B(R)} \log\sqrt{x^2+y^2}\,.$$

For each $(x_0, y_0) \in B(R)$ with $x_0, y_0 \neq 0$, we let $Q(x_0, y_0)$ denote the unit square containing (x_0, y_0) such that $\log(x^2+y^2)$ has its minimum on $Q(x_0, y_0)$ exactly at (x_0, y_0). For instance if $x_0, y_0 > 0$, then $Q(x_0, y_0) = [x_0, x_0+1] \times [y_0, y_0+1]$. For the remaining points (x_0, y_0) in $B(R)$ situated on the axes, we define $Q(x_0, y_0)$ to be the reunion of all such unit squares, e.g. if $x_0 > 0$, then $Q(x_0, 0) = [x_0, x_0+1] \times [-1, 1]$. Let

$$T(R) = \bigcup_{(x,y)\in B(R)} Q(x, y),$$

which is represented by the grey surface in the picture. Note that $D(R+2) \supset T(R) \supset D(R)$. We have



$$\begin{aligned}
\mu(n) &\leqslant \frac{1}{\#B(R)} \cdot \int_{T(R)} \log\sqrt{x^2+y^2}\,dx\,dy \\
&\leqslant \frac{1}{\#B(R)} \cdot \int_{D(R+2)} \log\sqrt{x^2+y^2}\,dx\,dy \\
&= \frac{1}{\#B(R)} \cdot 2\pi \cdot \int_0^{R+2} \log(r)\cdot r\,dr \\
&= \frac{1}{\#B(R)} \cdot \frac{\pi}{2} \cdot (R+2)^2 \cdot (2\log(R+2) - 1)
\end{aligned}$$

On the other hand, it is easy to see that $\#B(R)$ is larger than the area of $D(R-2)$. Hence, we get

$$\begin{aligned}
\mu(n) &\leqslant \frac{\pi\cdot(R+2)^2}{\pi\cdot(R-2)^2} \cdot \frac{1}{2} \cdot (2\log(R+2) - 1) \\
&= \left(1 + \mathbf{O}(\tfrac{1}{R})\right)^2 \cdot \left(\log(R) - \frac{1}{2} + \mathbf{O}(\tfrac{1}{R})\right) \\
&= \log(R) - \frac{1}{2} + \mathbf{O}\left(\frac{\log(R)}{R}\right)
\end{aligned}$$

□

In the next theorem, we prove a lower bound for $\mu(n)$. We only treat the case when n is a prime power as we are mainly interested in such lattices. If the constant $\hat{\gamma}$ exists, then this theorem shows that it is larger than -0.725791.

Theorem 11.
Let p be a prime. Then

$$\mu(p^k) \geqslant \frac{1}{2}\log(p)\cdot k + \frac{1}{2}\log\left(\frac{2}{\pi}\right) - \frac{1}{2} + \mathbf{O}(k^2\cdot p^{-k/2})$$

Proof. The proof is far more complicated than the upper bound in theorem 10. We will need several lemmas of which the first is the following.

Lemma 12. *Let $k \geqslant 1$ and $(x,y) \in \mathbb{Z}^2$. Suppose p^d is the highest power of p dividing the greatest common divisor of x and y. If $k > d$, then (x,y) belongs to $L(\bar{z})$ for exactly p^d different elements $\bar{z}$ in $\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$.*

Proof. Write $x = p^d\,x'$ and $y = p^d\,y'$. By interchanging x and y if necessary, we may suppose that y' is not divisible by p. Any $\bar{z} \in \mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$ can be written as $\bar{z} = (a:b)$ with $a = p^l$ for some $0 \leqslant l \leqslant k$ and $p \nmid b$ if p divides a.

$$\begin{aligned}
(x,y) \in L(\bar{z}) \quad &\Leftrightarrow \quad p^{l+d}\,x' + b\,p^d\,y' \equiv 0 \pmod{p^k} \\
&\Leftrightarrow \quad p^l\,x' + b\,y' \equiv 0 \pmod{p^{k-d}} \\
&\Leftrightarrow \quad l = 0 \quad \text{and} \quad x' + b\,y' \equiv 0 \pmod{p^{k-d}}
\end{aligned}$$

The last equation has exactly one solution for b modulo p^{k-d} and hence we may find p^d solutions in $\mathbb{Z}/p^k\mathbb{Z}$. □

Let R be the radius of a large circle. Write p^l for the largest power of p which is smaller than R. Define $\Sigma(R)$ to be the number of integral points inside the disc $D(R)$, but where we count every point (x,y) exactly p^d times if p^d is the largest power of p dividing both x and y. The point $(0,0)$ is not counted at all.

Lemma 13. *There is a constant A such that*

$$\Sigma(R) \leqslant (1+\tfrac{1}{p})\,\pi\,R^2 + A\cdot\log(R)\,R$$

for all $R > 10$.

Proof. For any given radius r, the number of integral points $B(r)$ is less than $\pi\,(r+2)^2$. Hence, using lemma 12, we have

$$\begin{aligned}
\Sigma(R) &= \#B(R) + \sum_{d=1}^{l}(p^d - p^{d-1})\cdot\#B\left(\frac{R}{p^d}\right) \\
&\leqslant \pi\,(R+2)^2 + \sum_{d=1}^{l}(p^d - p^{d-1})\cdot\pi\cdot\left(\frac{R}{p^d}+2\right) \\
&= \pi\,(R+2)^2 + (1-\tfrac{1}{p})\cdot\pi\cdot\sum_{d=1}^{l}\left(\frac{R^2}{p^d} + 4\,R + 4\,p^d\right) \\
&\leqslant \pi\,(R^2 + 4\,R + 4) + (1-\tfrac{1}{p})\cdot\pi\cdot\left(\frac{R^2}{p}\cdot\frac{1}{1-\frac{1}{p}} + 4\,l\,R + 4\,p\,\frac{p^l-1}{p-1}\right) \\
&\leqslant \pi\,R^2 + 4\,\pi\,R + 4\,\pi + \pi\,\frac{R^2}{p} + 4\,\frac{p-1}{p}\pi\cdot l\,R + 4\,\pi\,p^l - 4\pi \\
&\leqslant (1+\tfrac{1}{p})\,\pi\,R^2 + 4\,\pi\,\left(\frac{p-1}{p}\cdot l + 1\right)R + 4\,\pi\,p^l
\end{aligned}$$

We note that the definition of l implies that $p^l < R$ and $l < \log(R)/\log(p)$. We obtain

$$\Sigma(R) \leqslant (1+\tfrac{1}{p})\,\pi\,R^2 + 4\,\pi\,\left(\frac{p-1}{p}\cdot\frac{1}{\log(p)} + \frac{2}{\log(R)}\right)\log(R)\cdot R$$

Hence for $R > 10$, we may take $A = 10$. □

For any given point (x, y) write r for $\sqrt{x^2+y^2}$. We wish to compute the average $\tilde{\mu}(R)$ of $\log(r)$ on the non-zero integral points in $D(R)$, but again counting each point p^d times just as in the definition of $\Sigma(R)$. More precisely, we define $\tilde{\mu}(R)$ by

$$\Sigma(R)\cdot\tilde{\mu}(R) = \sum_{(x,y)\in B(R)}{}' \log(r) + \sum_{d=1}^{l}(p^d - p^{d-1})\cdot \sum_{(x,y)\in B\left(\frac{R}{p^d}\right)}{}' \log(p^d\cdot r) \tag{2}$$

where the $\sum'$ means that we are excluding $(x, y) = (0, 0)$ from the sum.

Lemma 14. *We have*

$$\tilde{\mu}(R) \geqslant \frac{(1+\frac{1}{p})\,\pi\,R^2}{\Sigma(R)}\cdot\left(\log(R) - \tfrac{1}{2} + \mathbf{O}\left(\frac{\log(R)}{R}\right)\right)$$

Proof. An argument similar to the one used in the computations of theorem 10 shows that for any radius $\rho > 2$ and any $a > 0$, we have

$$\begin{aligned}\sum_{(x,y)\in B(\rho)}{}' \log(a\cdot r) &\geqslant 2\,\pi\int_0^{\rho-2}\log(a\cdot r)\,r\,dr\\ &= \pi\cdot(\log(a\cdot(\rho-2)) - \tfrac{1}{2})\cdot(\rho-2)^2\end{aligned}$$

Let $p^{l'}$ be the largest power such that $2\cdot p^{l'} < R$. The value of $\tilde{\mu}(R)$ would only decrease if we replace l by l' in the definition (2). Thus we have

$$\begin{aligned}\frac{\Sigma(R)}{\pi\cdot R^2}\cdot\tilde{\mu}(R) &\geqslant (\log(R-2) - \tfrac{1}{2})\cdot(1-\tfrac{2}{R})^2\\ &\quad + (1-\tfrac{1}{p})\sum_{d=1}^{l'} p^d\left(\log\left(p^d\cdot\left(\tfrac{R}{p^d}-2\right)\right) - \frac{1}{2}\right)\cdot\left(\tfrac{R}{p^d}-2\right)^2\tfrac{1}{R^2}\\ &= (\log(R) + \log(1-\tfrac{2}{R}) - \tfrac{1}{2})\cdot(1-\tfrac{2}{R})^2\\ &\quad + (1-\tfrac{1}{p})\sum_{d=1}^{l'} p^{-d}\cdot(\log(R) + \log(1-\tfrac{2p^d}{R}) - \tfrac{1}{2})\cdot(1-\tfrac{2p^d}{R})^2\\ &= \log(R) - \tfrac{1}{2} + \mathbf{O}\left(\frac{\log(R)}{R}\right)\\ &\quad + (1-\tfrac{1}{p})\cdot(\log(R) - \tfrac{1}{p})\sum_{d=1}^{l'}(\tfrac{1}{p^d} - \tfrac{4}{R} + \tfrac{4p^d}{R^2})\\ &\quad + (1-\tfrac{1}{p})\sum_{d=1}^{l'} p^{-d}\cdot\log\left(1-\tfrac{2p^d}{R}\right)\cdot\left(1-\tfrac{2p^d}{R}\right)^2\end{aligned}$$

For the first sum, we find

$$(1-\tfrac{1}{p})\sum_{d=1}^{l'}\left(\tfrac{1}{p^d}-\tfrac{4}{R}+\tfrac{4p^d}{R^2}\right)\geqslant(1-\tfrac{1}{p})\cdot\left(\frac{1}{p}\cdot\frac{1-\frac{1}{p^{l'}}}{1-\frac{1}{p}}-\frac{4\,l'}{R}+\frac{4}{R^2}\,p\,\frac{p^{l'}-1}{p-1}\right)$$
$$\geqslant\frac{1}{p}+\mathbf{O}\left(\frac{\log(R)}{R}\right).$$

The second sum can be written as

$$\sum_{d=1}^{l'}\log(1-\tfrac{2p^d}{R})\cdot(\tfrac{1}{p^d}-\tfrac{4}{R}+\tfrac{4p^d}{R^2})$$

in which the first factor is negative and it takes the smallest value for $d=1$. The second factor is positive and it likewise it is maximal when $d=1$. Hence we have

$$\left|\sum_{d=1}^{l'}\log(1-\tfrac{2p^d}{R})\cdot(\tfrac{1}{p^d}-\tfrac{4}{R}+\tfrac{4p^d}{R^2})\right|\leqslant l'\cdot\left|\log(1-\tfrac{2p}{R})\right|\cdot(\tfrac{1}{p}-\tfrac{4}{R}+\tfrac{4p}{R^2})$$
$$=\mathbf{O}(\log(R))\cdot\mathbf{O}(\tfrac{1}{R})\cdot(\tfrac{1}{p}+\mathbf{O}(\tfrac{1}{R}))\quad=\mathbf{O}\left(\tfrac{\log(R)}{R}\right).$$

□

Let k be a large integer. Then define R to be the real number satisfying

$$(1+\tfrac{1}{p})\,\pi\,R^2+A\cdot\log(R)\,R=2p^k(1+\tfrac{1}{p}),$$

if k is sufficiently large so that $R>10$. Note that the expression on the right is equal to $\#\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$.

Lemma 15. *We have* $R=\sqrt{2/\pi}\cdot p^{k/2}+\mathbf{O}(k)$.

Proof. We write $X^2=p^k$ and $C^2=\frac{2}{\pi}$. If we denote by T the expression such that $R=C\,X\,(1-T)$ then

$$1+\frac{A}{\pi\,(1+\frac{1}{p})}\,\frac{\log(R)}{R}=\left(\frac{C\,X}{R}\right)^2=\left(\frac{1}{1-T}\right)^2=1+2\,T+3\,T^3+\cdots$$

with R growing this expression tends to 1, hence T is tending to 0.

$$\frac{A}{\pi\,(1+\frac{1}{p})\,C}\cdot\frac{\log(X)+\log(C)+\log(1-T)}{X}=(1-T)\,(2\,T+3\,T^2+4\,T^3+\cdots)=2\,T+\cdots$$

which proves that $T=\mathbf{O}(\frac{\log(X)}{X})$. Thus $R=C\cdot p^{k/2}+C\,X\,T=C\cdot p^{k/2}+\mathbf{O}(\log(X))=C\cdot p^{k/2}+\mathbf{O}(k)$. □

We finally start now, the proof of the theorem. Every lattice $L(\bar{z})$ has at most two shortest vector different except for maybe two values of $\bar{z}$, corresponding to $\pm i$, if they belong to $\mathbb{Z}_p$. In this situation there are four shortest vectors. We have chosen R in such a way that the number of points counted with the multiplicity at which they may appear at most as a shortest vector of a lattice $L(\bar{z})$ is smaller than the total number of such lattices. Hence we have that

$\mu(p^k) \geqslant \tilde{\mu}(R)$, i.e. $\Sigma(R) \leqslant 2 \cdot \#\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$ or $\Sigma(R) \leqslant 2 \cdot \#\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z}) + 2$ if i belongs to $\mathbb{Z}_p$. Thus we obtain

$$\begin{aligned}\mu(p^k) \geqslant \tilde{\mu}(R) &\geqslant \frac{1+\frac{1}{p})\,\pi\,R^2}{(1+\frac{1}{p})\,\pi\,R^2 + A\cdot\log(R)\,R} \cdot \left(\log(R) - \tfrac{1}{2}\right) + \mathbf{O}\left(\frac{\log(R)}{R}\right)\\ &= \left(1 + \mathbf{O}\left(\frac{\log(R)}{R}\right)\right) \cdot \left(\log(R) - \tfrac{1}{2}\right) + \mathbf{O}\left(\frac{\log(R)}{R}\right)\\ &= \log\left(\sqrt{\frac{2}{\pi}} \cdot p^{\frac{k}{2}}\right) - \frac{1}{2} + \mathbf{O}\left(\frac{k^2}{p^{k/2}}\right)\end{aligned}$$

which finishes the proof. □

8 The lattice type

Let $z \in \mathbb{P}^1(\mathbb{Z}_p) = \mathbb{P}^1(\mathbb{Q}_p)$. For any $k \geqslant 1$, we obtain a p-adic approximation lattice $L(z,k) = L(z \bmod p^k)$ and we may consider the sequence $\mathrm{minL}(z,k) = \mathrm{minL}(z \bmod p^k)$. We say that z is of *lattice type* α if there is a constant $C > 0$ such that

$$|\log(\mathrm{minL}(z,k)) - k\cdot\alpha| < C.$$

The previous section suggests that the most frequent lattice type is $\frac{1}{2}\log(p)$ which is also the largest lattice type possible by Minkowski's bound. The next lemma shows that the lattice type is some sort of a measure of the irrationality of z.

Proposition 16. *The elements in $\mathbb{P}^1(\mathbb{Q}_p)$ of lattice type 0 are exactly $\mathbb{P}^1(\mathbb{Q})$.*

Proof. If $z \in \mathbb{P}^1(\mathbb{Q})$ then, we may write $z = (a : b)$ with a and b two integers which are prime to each other. Then every one of the lattices $L(z,k)$ contains the point $(-b, a)$ and hence $\mathrm{minL}(z,k)$ is bounded by $\sqrt{a^2+b^2}$, i.e. z is of lattice type 0.

Conversely if z is of lattice type 0, there is a constant C such that all of the $L(z,k)$ contain an element of norm less than $\exp(C)$. Since there are only finitely many integral points in this disc, there is a point (x,y) which belongs to $L(z,k)$ for infinitely many k. Write $z = (p^n : z_2)$ for some $n \geqslant 0$ and $z_2 \in \mathbb{Z}_p$. Hence $p^n x + z_2\, y \equiv 0 \pmod{p^k}$ for infinitely many k. So z_2 must be equal to $-p^n\, x\, y^{-1}$ which lies in $\mathbb{Q}$. □

The next proposition gives a lot of algebraic numbers of maximal lattice type.

Proposition 17. *Let $\theta \in \mathbb{Q}_p$ be an algebraic integer such that $\mathbb{Z}[\theta]$ is the number ring in a quadratic imaginary field K. Then θ is of maximal lattice type $\frac{1}{2}\log(p)$.*

Proof. The embedding $\mathbb{Z}[\theta] \hookrightarrow \mathbb{Q}_p$ defines a prime ideal $\mathfrak{p} = \mathbb{Z}[\theta] \cap p\,\mathbb{Z}_p$ above p. The powers of the ideal $\mathfrak{p}^k$ may be written as

$$\mathfrak{p}^k = \{x + y\cdot\theta \mid x, y \in \mathbb{Z} \text{ with } x + y\cdot\theta \in p^k\mathbb{Z}_p\},$$

in other words it is the lattice $L(\theta,k)$ in $\mathbb{Z}[\theta] \approx \mathbb{Z}^2$. Let h be the class number of K. For $1 \leqslant i \leqslant h$, let α_i be the element of $\mathfrak{p}^i$ whose value of $|\,\mathrm{N}_{K/\mathbb{Q}}(\alpha_i)| \in \mathbb{N}$ is minimal. Since $\mathfrak{p}^h$ is principal, we may take $\alpha_h = \alpha$ to be the generator of $\mathfrak{p}^h$; moreover the minimal values of the norm for $\mathfrak{p}^{h\cdot k+i}$ is taken by $\alpha^k \cdot \alpha_i$. Hence we obtain for any $1 \leqslant i \leqslant h$

$$\mathrm{minL}(\theta, k\cdot h + i) = \min_{\beta \in \mathfrak{p}^{k\cdot h+i}} |\,\mathrm{N}_{K/\mathbb{Q}}(\beta)| = |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)|^k \cdot |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha_i)|$$

Now, we note that $|\,\mathrm{N}_{K/\mathbb{Q}}(\cdot)|^{1/2}$ extends to a norm on the vector space $\mathbb{Z}[\theta] \otimes \mathbb{R}$ and as such it is equivalent to the usual norm. So the growth of the minimal vector is given by

$$\log \mathrm{minL}(L(\theta, k\cdot h + i)) = \log(p^{h\cdot k}) + \log|\,\mathrm{N}_{K/\mathbb{Q}}(\alpha_i)|$$

since the norm of α is equal to p^h. This proves the proposition. □

Apart from these two propositions there is a long list of questions that one might ask about lattice types. Is it possible to construct p-adic integers that do not have a lattice type ? Can transcendental numbers have non-trivial and non-maximal lattice type ? Can one give any inequalities on the lattice type of sums or products of numbers ? ...

The most important question with respect to our initial question is of course whether one can find a criterion for deciding if a number has maximal lattice type. Most of all p-adic numbers have maximal lattice type. The original conjecture 1 for curves of rank 2 can be reformulated as follows.

Proposition 18. *Let E be an elliptic curve of rank 2 over $\mathbb{Q}$ and p be a prime number. Let Q_1 and Q_2 be two linearly independent points in $B_p(1)$. Then the strong conjecture 1 is equivalent to the statement that $z = (\mathscr{L}_p(Q_1) : \mathscr{L}_p(Q_2)) \in \mathbb{P}^1(\mathbb{Q}_p)$ has maximal lattice type*

The notion of lattice type of dimension 2 can easily be generalised to higher dimensions and the above proposition can be extended accordingly. The main results of section 7 should also be valid in a suitable generalised form.

The conjecture of Lang and Waldschmidt as formulated in conjecture 3 implies that if $(\log_p(a_1) : \log_p(a_2)) \in \mathbb{P}^1(\mathbb{Q}_p)$ has a lattice type then it is of maximal lattice type and we can put $\varepsilon = 0$.

References

[Ber78] Daniel Bertrand, *Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe*, Compositio Math. **37** (1978), no. 1, 21–50.

[Cas97] J. W. S. Cassels, *An introduction to the geometry of numbers*, Classics in Mathematics, Springer-Verlag, Berlin, 1997, Corrected reprint of the 1971 edition.

[dW89] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract, vol. 65, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[Hux03] M. N. Huxley, *Exponential sums and lattice points. III*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 591–609.

[Lan78] Serge Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 231, Springer-Verlag, Berlin, 1978.

[Phi99] Patrice Philippon, *Quelques remarques sur des questions d'approximation diophantienne*, Bull. Austral. Math. Soc. **59** (1999), no. 2, 323–334.

[RU96] Gaël Rémond and Florent Urfels, *Approximation diophantienne de logarithmes elliptiques p-adiques*, J. Number Theory **57** (1996), no. 1, 133–169.

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Sma98] Nigel P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998.