Submitted exclusively to the London Mathematical Society
DOI: 10.1112/S0000000000000000

ON p-ADIC HEIGHTS IN FAMILIES OF ELLIPTIC CURVES

CHRISTIAN WUTHRICH

1. *Introduction*

About twenty years ago, following an initial idea of Bernardi [**2**] and Néron [**14**], Perrin-Riou [**16**] and Schneider [**18**] defined a canonical p-adic height pairing on abelian varieties over number fields; here p is an odd prime number such that the abelian variety has good ordinary reduction at all places above p of its field of definition. They proved formulae as they should appear in the p-adic version of the conjecture of Birch and Swinnerton-Dyer for the L-function coming from the Iwasawa theory of the Selmer-group, but only under the assumption that this pairing is non-degenerate. Schneider conjectured the non-degeneracy of the p-adic height pairing should be true, just as it is for the real-valued Néron-Tate height. In particular, the p-adic height of a non-torsion point on an elliptic curve of rank one should be a non-zero p-adic number. This is still not known except for elliptic curves with complex multiplication defined over the rational numbers $\mathbb{Q}$ as was proven by Bertrand in [**3**] using transcendental methods. For function fields, there is a result by Papanikolas [**15**].

This article investigates the particular case of elliptic curves over number fields. Here the p-adic height is composed of two terms, a term involving the denominator of the x-coordinate and a term using the canonical p-adic sigma function explicitly described in [**11**] by Mazur and Tate. See section 6 for a detailed definition.

We analyse the variation of the p-adic height in a family of elliptic curves. For the classical Néron-Tate height, this was considered, for instance, in [**26**] by Tate. We restrict our attention to the case of an elliptic surface fibred over the affine line over a number field. The behaviour of the p-adic height of points varying in a section of the surface is analysed via the local decomposition mentioned above. In the classical case, this was first done by Call in [**6**]. Later, a finer study of the variation was given by Silverman in the three articles [**22**], [**23**] and [**24**]. Our method is quite similar to this analysis of the local real analytic properties of the Néron-Tate height. We refer to the end of section 4 for a comparison.

It turns out that the variation is p-adically continuous, see theorem 2. From this, we can conclude in theorem 3 that for a sufficiently nice set of sections in a family of elliptic curves over $\mathbb{Q}$, the p-adic regulator is either constant zero or has at most a finite number of zeros. This can be used to check the non-degeneracy of the p-adic height simultaneously for an infinite number of elliptic curves in a family. Meanwhile, in corollary 5, we find that arbitrarily small p-adic heights are possible in contrast to case of the Néron-Tate height.

In the final sections, we explain some conjectures on the valuation of p-adic

2000 *Mathematics Subject Classification* 11G05 (primary), 11G50, 14J27 (secondary).

The author was supported by an External Research Studentship of Trinity College

heights, based on calculations listed in the tables at the end. As a consequence one can conjecture that the rank of the Mordell-Weil group over the cyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ of an elliptic curve over $\mathbb{Q}$ is equal to the rank of the Mordell-Weil group over $\mathbb{Q}$ for a set of density 1 among the primes p where E has good ordinary reduction.

But first, we include the study of the denominator of a section in a family of elliptic curves. In section 4, we explain the inevitable hypothesis that we have to impose on our sections, where they come from (as explained in the example after corollary 4) and why they are rather harmless (see proposition 3 and 6).

Acknowledgements. I would like to express my warmest thanks to John Coates, Tony Scholl, Paola Argentin and Sylvia Guibert. I am thankful to Joseph Silverman for drawing my attention to his articles [**22**], [**23**] and [**24**].

2. *Cancellation*

The first three sections contain a detailed study of the denominator of the x-coordinate of a point on an elliptic curve. In particular, we are interested in its behaviour when the point is multiplied by an integer.

Let A be a unique factorisation domain. We will study the points of an elliptic curve E over the fraction field F of A, given by a Weierstrass equation

$$y^2 + a_1\,xy + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6 \tag{Weq}$$

with coefficients a_i in the ring A. A non-zero point P can always be written in the form

$$P = (x(P), y(P)) = \left(\tfrac{a(P)}{e(P)^2}\,,\,\tfrac{b(P)}{e(P)^3}\right), \tag{2.1}$$

where $a(P)$, $b(P)$ and $e(P)$ are elements of A such that $e(P)$ is relatively prime to both $a(P)$ and $b(P)$. Of course, these expressions are only well-defined up to the multiplication by units in $A^\times$.

The symbol t will always stand for the uniformizer $-\frac{x}{y}$ at the origin O of E in $F(E)$. Let $m > 0$ be an integer. The m-th division polynomial f_m (with respect to the chosen Weierstrass equation) is defined to be the function in $F(E)$ having divisor $[m]^\star(O) - m^2 \cdot (O)$ and normalised to have $m \cdot t^{1-m^2}$ as the leading term at the origin O. A detailed description of these functions can be found in the first appendix of [**11**]. It will be used repeatetly that the square of f_m can be written as a polynomial in the function x of the form

$$f_m^2 = m^2\,x^{m^2-1} + \text{ lower order terms in } x \tag{2.2}$$

whose coefficients turn out to be polynomials in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$, in particular they are in A. Similarly, the functions $g_m = x \cdot f_m^2 - f_{m+1} \cdot f_{m-1}$, defined for all integers $m > 1$, are polynomials of degree m^2 in x with integral coefficients. These polynomials appear in the formula describing multiplication by m:

$$\frac{a(mP)}{e(mP)^2} = x(mP) = \frac{g_m(P)}{f_m(P)^2} = \frac{g_m(P) \cdot e(P)^{2m^2}}{(f_m(P) \cdot e(P)^{m^2})^2}, \tag{2.3}$$

valid for $m > 1$ and points $P \in E(F)$ that are not m-torsion. The expression on the right is written as a fraction of elements in A, since the power of $e(P)$ is sufficient to eliminate all the denominator. More precisely

$$f_m(P)^2 \cdot e(P)^{2m^2} = m^2\, a(P)^{m^2-1}\, e(P)^2 + \text{ higher order terms in } e(P) \tag{2.4}$$

is a polynomial in $A[a(P), e(P)]$. But there is no reason to believe that this expression on the right of (2.3) is a reduced fraction. By definition of $e(mP)$, the largest common factor of the numerator and the denominator in this fraction will be the square of the following element of A which will be called the *cancellation* of P when multiplied with m :

$$\delta_m(P) = \frac{f_m(P) \cdot e(P)^{m^2}}{e(mP)}. \tag{2.5}$$

This is well-defined up to a unit in $A^\times$ whenever $m > 1$ and $P \in E(F)$ is not a m-torsion point, but depends on the equation (Weq).

LEMMA 1. *Under a change of equation of the form*

$$x = u^2 \cdot x' + r_1, \qquad y = u^3 \cdot y' + u^2 r_2 \cdot x' + r_3, \tag{2.6}$$

with u being a unit in $A^\times$ and the r_i in A, the cancellation $\delta_m(P)$ can only change by a unit.

The main result on cancellations is the following non-cancellation proposition. It can be deduced from the explicit formula for the local non-archimedian real-valued height functions (Theorem VI.4.1 in [**21**]). We give a short independent proof here.

PROPOSITION 1. *Let E be an elliptic curve given by an equation* (Weq) *over a ring A which is complete with respect to a discrete valuation v with residue field $\mathbb{F}_v$. If a point $P \in E(F)$ reduces to a non-singular point in the reduction $\tilde{E}(\mathbb{F}_v)$ then the cancellation $\delta_m(P)$ is a unit for all $m \neq 0$, provided $mP \neq O$.*

Proof. We split the proof into three cases. First suppose that $e(mP)$ and $e(P)$ are both units. Then the reduction $\tilde{P}$ of P and the reduction $m\tilde{P}$ of mP are two non-zero points in the group $\tilde{E}_{\text{ns}}(\mathbb{F}_v)$ of non-singular points on the reduction $\tilde{E}$. The multiplication formula (2.3) is also valid in this group and so the denominator must be invertible in $\mathbb{F}_v$. This is what we want to prove, since the valuation of $f_m(P) \cdot e(P)^{m^2}$ is zero.

Next, we prove the statement when $e(mP)$ and $e(P)$ have the same valuation $k > 0$. Here our two points P and mP lie in the same layer $\hat{E}(\mathfrak{m}^k)$ of the formal group $\hat{E}$ where $\mathfrak{m}$ is the maximal ideal in A. (We refer to chapter IV of [**20**] for everything we need about formal groups.) Since there is a canonical isomorphism of groups

$$\frac{\hat{E}(\mathfrak{m}^k)}{\hat{E}(\mathfrak{m}^{k+1})} \cong \frac{\mathfrak{m}^k}{\mathfrak{m}^{k+1}},$$

we see that m must have valuation 0 as an element in A, otherwise mP would belong to $\widehat{E}(\mathfrak{m}^{k+1})$. The valuation of the expression in (2.4) is $2k$ since $a(P)$ is a unit when $e(P)$ is not, so both terms in the definition (2.5) of $\delta_m(P)$ have valuation k.

Finally, we look at the case when $e(mP)$ has a strictly bigger valuation than $e(P)$. If so, mP lies in a layer closer to O, and therefore the points $(m-1)P$ and

$(m+1)P$ must lie in the same layer as P. Using what we just proved about such multiples, we see that the expressions

$$f_{m+1}(P)\cdot e((m+1)P)^{(m+1)^2} \qquad \text{and} \qquad f_{m-1}(P)\cdot e((m-1)P)^{(m-1)^2}$$

must have the same valuation as $e(P)$. Consider the numerator of the multiplication formula (2.3):

$$\begin{aligned} g_m(P)\, e(P)^{2m^2} =& (f_m(P)^2\, x(P) - f_{m+1}(P)\, f_{m-1}(P))\cdot e(P)^{2m^2} \\ =& f_m(P)^2\, e(P)^{2m^2}\cdot a(P)\, e(P)^{-2} \\ & - f_{m+1}(P)\, e(P)^{(m+1)^2}\cdot f_{m-1}(P)\, e(P)^{(m-1)^2}\cdot e(P)^{-2}. \end{aligned}$$

The previous argument shows that the second term is a unit. Meanwhile, because the cancellation $\delta_m(P)^2$ is an integral element, the first term must have valuation at least as big as the valuation of $e(mP)^2\cdot e(P)^{-2}$, which is strictly positive in our case. So we see that the square of the cancellation

$$\delta_m(P)^2 = \frac{(f_m(P)\cdot e(P)^{m^2})^2}{e(mP)^2} = \frac{g_m(P)\cdot e(P)^{2m^2}}{a(mP)}$$

is a unit. This concludes the proof. □

Conversely one can prove that the cancellation is not a unit when P reduces to the singular point. The valuation of $\delta_2(P)$ is smaller than half the valuation of the discriminant Δ, but in most cases it is 1 or 2. This leads to a numerical interpretation of the term $(j_v(X,\mathfrak{a})$ in théorème III.4.1 in [**13**]) that has to be added in the formula for the Néron-Tate height as an intersection pairing on the Néron model.

3. *The Class Group Pairing*

Let A be a Noetherian Krull domain with class group $\mathrm{Cl}(A)$ (written additively) and fraction field F. Let E be an elliptic curve over F given by an equation (Weq) with coefficients in the ring A. The subgroup $E^\circ(F)$ of $E(F)$ of points with non-singular reduction at all primes of height 1 is of finite index by Tate's algorithm [**25**]. For a non-zero point P in $E^\circ(F)$ and a prime $\mathfrak{p}$ of height 1, the localisation $A_\mathfrak{p}$ of A at $\mathfrak{p}$ is a principal ideal domain, and so we can define an element $e_\mathfrak{p}(P)\in A_\mathfrak{p}$ using the construction in section 2. As a consequence of proposition 1 for the completion of $A_\mathfrak{p}$, we get a formula as in excerise 6.4 in [**21**].

COROLLARY 1. *Let $m>1$ and let P be a point in $E^\circ(F)$ that is not m-torsion, then, for all $\mathfrak{p}$,*

$$e_\mathfrak{p}(m\cdot P) = e_\mathfrak{p}(P)^{m^2}\cdot f_m(P), \qquad \textit{up to a unit in } A_\mathfrak{p}^\times.$$

According to remark 3.5.3 in [**10**], there is a pairing on $E(F)$ with values in the class group. We give an explicit description of this here. If F is a function field of a curve this is just the canonical height on the minimal model considered by Manin.

Define a map

$$\begin{aligned} q\colon E^\circ(F) &\to \mathrm{Cl}(A) \\ P &\mapsto \text{ the class of } \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(e_{\mathfrak{p}}(P)) \cdot \mathfrak{p} \end{aligned}$$

where the sum runs over all primes $\mathfrak{p}$ of height 1. The previous corollary allows us to calculate $q(mP)$ for an integer m: it is the class of

$$\sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(e_{\mathfrak{p}}(mP)) \cdot \mathfrak{p} = m^2 \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(e_{\mathfrak{p}}(P)) \cdot \mathfrak{p} + \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f_m(P)) \cdot \mathfrak{p}.$$

But the second term is just the principal divisor $(f_m(P))$, so we conclude that $q(mP) = m^2 \cdot q(P)$. One can show furthermore that the parallelogram law holds for q and so it induces a bilinear form on $E^\circ(F)$ with values in $\mathrm{Cl}(A)$. But we are only interested in the following consequence:

PROPOSITION 2. *Suppose that the class group* $\mathrm{Cl}(A)$ *is finite. There exists a subgroup of finite index* $E^\bullet(F)$ *of points* P *in* $E^\circ(F)$ *such that* $q(P) = 0$*, so there are elements* $a(P)$*,* $b(P)$ *and* $e(P)$ *in* A*, defined up to multiplication by* $A^\times$*, such that* $(e(P))$ *is coprime to both* $(a(P))$ *and* $(b(P))$ *and*

$$P = \left(\tfrac{a(P)}{e(P)^2}, \tfrac{b(P)}{e(P)^3}\right).$$

Combining this with the corollary 1, we get the

COROLLARY 2. *In this subgroup* $E^\bullet(F)$*, we have the formula*

$$e(m \cdot P) = e(P)^{m^2} \cdot f_m(P), \qquad \textit{up to a unit in } A^\times. \tag{3.1}$$

4. *Families*

Now we fix a number field K with its ring of integers R. Moreover, K_v denotes the completion of K at a finite place v, R_v its integers, $\mathfrak{m}_v$ the maximal ideal and $\mathbb{F}_v$ the residue field.

By $\mathcal{E}$ we will denote in what follows a Weierstrass equation (Weq) with coefficients in the ring of polynomials $R[T]$ whose discriminant $\Delta \in R[T]$ is not zero. Such an $\mathcal{E}$ will be called a *family* over R.

When taking the same equation but considered over $K[T]$, we obtain a scheme $\mathcal{E}_K$ fibred over the affine line $\mathbb{A}^1_K$, that is, a birational equivalence class of elliptic surfaces defined over K (see chapter III of [**21**]). In particular, there is a group of sections $\mathcal{E}_K(K)$, which can be viewed as the points, defined over $K(T)$, of the generic fibre, i.e. the elliptic curve given by the equation of $\mathcal{E}$ over $K(T)$. For short, we write $\mathcal{E}(K)$ for this group and we will call its non-zero elements sections of $\mathcal{E}$; they are *not* sections over R of the scheme associated to the equation $\mathcal{E}$. Denote by $\mathcal{E}^\circ(K)$ its subgroup of finite index containing the sections that do not meet any singularity of a fibre.

For $\tau \in K$, the fibre above $(T - \tau)$ will be denoted by $\mathcal{E}_\tau$ and, given a section $P \in \mathcal{E}(K)$, the point P_τ is where P meets the fibre $\mathcal{E}_\tau$. For a finite place v of R, $\tilde{\mathcal{E}}_v$ stands for the reduction of $\mathcal{E}$ at v, which is a Weierstrass equation over $\mathbb{F}_v[T]$. The reductions of the fibre $\mathcal{E}_\tau$ are denoted by $\tilde{\mathcal{E}}_{\tau,v}$.

It is important to note that $R[T]$ is a Noetherian Krull domain with finite class group $\mathrm{Cl}(R[T]) \cong \mathrm{Cl}(R)$ according to proposition 13 and 18 in chapter VII.1.9 and VII.1.10 of [**5**]. Therefore, we can define a subgroup $\mathcal{E}^\bullet(K)$ as in proposition 2 and, for each section in $\mathcal{E}^\bullet(K)$, a polynomial $e(P)$ in $R[T]$ well-defined up to a unit in $R[T]^\times = R^\times$.

Let τ be an element of the principal ideal domain R_v. On the one hand, the coordinates of the point $P_\tau \in \mathcal{E}_\tau(K)$ can be written according to (2.1) as reduced fractions of elements in R_v, say

$$P_\tau = \left(\frac{a_v(P_\tau)}{e_v(P_\tau)^2}, \frac{b_v(P_\tau)}{e_v(P_\tau)^3} \right),$$

at least if $P_\tau \neq O_\tau$.

On the other hand, when replacing T by τ in $e(P)$, written $e(P)(\tau)$, we will also obtain fractions of elements in R_v, namely

$$P_\tau = \left(\frac{a(P)(\tau)}{e(P)(\tau)^2}, \frac{b(P)(\tau)}{e(P)(\tau)^3} \right). \tag{4.1}$$

Once again, we have two fractions that we can compare: we might have some cancellation in the expression (4.1), which allows us to define, for every $\tau \in R_v$ and section $P \in \mathcal{E}^\bullet(K)$ with $P_\tau \neq O_\tau$, an element $\gamma_v(P, \tau)$ in R_v by

$$e_v(P_\tau) \cdot \gamma_v(P, \tau) = e(P)(\tau), \tag{4.2}$$

which is defined up to a unit in $R_v^\times$.

Proposition 3. *Let $P \in \mathcal{E}^\bullet(K)$ be a section in a family $\mathcal{E}$ as described above. The map*

$$\tau \mapsto \mathrm{ord}_v(\gamma_v(P, \tau))$$

from R_v to the integers is bounded and v-adically continuous. Moreover it is the zero map for all but a finite number of places.

Proof. Consider the resultant $r \in R$ of the polynomials $e(P)$ and $a(P)$. The valuation of r at v, which is almost always zero, bounds the valuation of $\gamma_v(P, \tau)$ for all τ. It is clear that the cancellation of $a(P)$ and $e(P)$ has locally constant valuation. □

Proposition 4. *Let P be a section of a family $\mathcal{E}$. Suppose that P belongs to $\mathcal{E}^\bullet(K)$. Then for all but a finite number of places v, the points P_τ have non-singular reduction $\tilde{P}_{\tau,v}$ in $\tilde{\mathcal{E}}_{\tau,v}(\mathbb{F}_v)$ for all $\tau \in R$.*

Proof. One way of proving this is to note that for the places v for which $\gamma_v(P, \tau)$ is a unit, and this excludes only finitely many by the previous proposition, the conditions for P_τ to have singular reduction can be written as congruences in polynomials modulo the prime ideal $\mathfrak{p}_v$ associated to the place v:

$$\begin{gathered}\big(2b(P) + a_1\, a(P)\, e(P)^2 + a_3\, e(P)^3\big)\,(\tau) \equiv 0 \pmod{\mathfrak{p}_v},\\ \big(3a(P)^2 + 2a_2\, a(P) e(P)^2 + a_4\, e(P)^4 - a_1\, b(P)\, e(P)\big)\,(\tau) \equiv 0 \pmod{\mathfrak{p}_v}.\end{gathered}$$

If there is a τ such that $\tilde{P}_{\tau,v}$ is singular, then the resultant of the two polynomials above must be in the ideal $\mathfrak{p}_v$. This happens only for a finite number of v. □

The best case is, of course, when a section $P \in \mathcal{E}(K)$ has non-singular reduction for all finite places v and all fibres $\tau \in R$, i.e. $P_\tau \in \mathcal{E}^\circ_\tau(K)$ for all τ. In this case we say that the section has *good reduction everywhere.*

COROLLARY 3. *Let E be an elliptic curve over a number field K with a point $Q \in E^\bullet(K)$ of infinite order. E can be embedded into a non-constant family $\mathcal{E}$ with a section $P \in \mathcal{E}^\bullet(K)$ having good reduction everywhere that meets E at Q. Moreover we can even achieve that $\gamma_v(P,\tau) = 1$ for all τ and all v.*

Proof. By varying the coefficients of E with a parameter T, we can construct a linear pencil of cubic curves that all pass through the point Q and have an inflection point at O. In order to have $P \in \mathcal{E}^\circ(K)$, we want $\mathcal{E}$ such that P is not a singularity of any cubic of the pencil. This pencil can be written as an equation $\mathcal{E}$ over $R[T]$ with a section P that has *constant* coordinates and we may assume that $\mathcal{E}_0 = E$. Now P is in $\mathcal{E}^\bullet(K)$ as $e_v(P_\tau) = e(P)(\tau) = e(Q)$ and Q belongs to $E^\bullet(K)$. Moreover $\gamma_v(P,\tau) = 1$. Proposition 4 says that we need to be concerned only about a finite number of places v, if we want P_τ to have good reduction for all τ and v. Since P_τ has good reduction everywhere for $\tau = 0$, it has good reduction at v for all $\tau \equiv 0 \pmod{\mathfrak{p}_v}$. Therefore we can replace the variable T by $a \cdot T$ for an a in all $\mathfrak{p}_v$ where P has possibly some singular reduction. □

PROPOSITION 5. *Let P be a section of a family $\mathcal{E}$ that belongs to $\mathcal{E}^\bullet(K)$ and which has good reduction everywhere. Then P_τ belongs to $\mathcal{E}^\bullet_\tau(K)$ for all $\tau \in R$. There exists an element $\gamma(P,\tau)$ in R, defined up to $R^\times$, such that $e(P_\tau)\cdot\gamma(P,\tau) = e(P)(\tau)$. It satisfies $\gamma(mP,\tau) = \gamma(P,\tau)^{m^2}$.*

Proof. For the first part, note that $q(P) = q(P_\tau)$ under the isomorphism from $\mathrm{Cl}(R[T])$ to $\mathrm{Cl}(R)$. The existence of $\gamma(P,\tau)$ follows now exactly like in (4.2). The final statement follows from the following calculation, with equalities always up to $R^\times$,

$$\begin{aligned}
\gamma(mP,\tau)\cdot e(P_\tau)^{m^2}\cdot f_m(P_\tau) &= \gamma(mP,\tau)\cdot e(mP_\tau) && \text{by (3.1)}\\
&= e(mP)(\tau) && \text{by definition}\\
&= e(P)(\tau)^{m^2}\cdot f_m(P)(\tau) && \text{by (3.1)}\\
&= \gamma(P,\tau)^{m^2}\cdot e(P_\tau)^{m^2}\cdot f_m(P)(\tau).
\end{aligned}$$

Next we see that the definition of the m-th division polynomial is such that the restriction of $f_m(P)$ to $\mathcal{E}_\tau$ must be the m-th division polynomial of this fibre. Hence $\gamma(mP,\tau) = \gamma(P,\tau)^{m^2}$. □

COROLLARY 4. *If $\gamma(P,\tau)$ belongs to $R^\times$ for all τ, then $\gamma(mP,\tau)$ is also in $R^\times$.*

On an elliptic curve over a global field F, every point P can be multiplied by a sufficiently big integer to guarantee that P has good reduction at every place v, due to the fact that the subgroup $E^\circ(F)$ is of finite index. Unfortunately, it is not true for families as the following example over the rational numbers shows:

$$\mathcal{E}:\quad y^2 + xy = x^3 - T^3 + 2T^2.$$

$\mathcal{E}$ has a section $P = (T,T)$ and $2P = (T^2 - \frac{5}{3}T - \frac{2}{9}, -T^3 + 2T^2 + \frac{4}{27})$ is in the subgroup $\mathcal{E}^\circ(\mathbb{Q}) = \mathcal{E}^\bullet(\mathbb{Q})$. The family has multiplicative reduction at $\tau = 0$ with singularity $(0,0)$, the multiples of the section $2P$ meet the fibre $\mathcal{E}_0$ at

$$\begin{array}{lll} (2P)_0 = (-\frac{2}{9}, \frac{2^2}{27}) & (4P)_0 = (\frac{2^2}{9}, -\frac{2^4}{27}) & (6P)_0 = (-\frac{2^3}{9^2}, \frac{2^6}{9^3}) \\ (8P)_0 = (\frac{2^4}{15^2}, -\frac{2^8}{15^3}) & (10P)_0 = (-\frac{2^5}{33^2}, \frac{2^{10}}{33^3}) & \cdots \end{array}$$

So there is no hope that any multiple of P will have non-singular reduction at the place $v = 2$. In terms of Néron-models, this reflects the fact that the Néron flt-model of $\mathbb{G}_m$ over a discrete valuation ring has an infinite cyclic group of connected components (see Example 10.1.5 in [**4**]). For an additive fibre, this "group of connected components" would have to be an infinite torsion K/R, but here not even the Néron flt-model exists.

The next part of this section is devoted to the following proposition that tells us that the above phenomenon is the only obstacle for finding a multiple with good reduction everywhere.

Proposition 6. *Let $\mathcal{E}$ be a family and let P be a section. There are multiples Q of P such that Q_τ has good reduction at every finite place v for all $\tau \in R\backslash U$, where U is a set of arbitrarily small density which is the union of arithmetic progressions. Moreover, if no fibre $\mathcal{E}_\tau$ for $\tau \in R$ is of multiplicative type, then one can take U to be empty.*

Proof. First one may assume that P is in $\mathcal{E}^\bullet(K)$. Proposition 4 shows that one has only to care about a finite number of places v. Let us consider the discriminant $\Delta \in R_v[T]$. By excluding τ in the congruence classes of the zeros of Δ modulo a power of $\mathfrak{p}_v$, we can guarantee that the valuation of the discriminant $\operatorname{ord}_v(\Delta(\tau))$ stays bounded. Taking a high power of $\mathfrak{p}_v$, we are sure to have excluded a set of sufficiently small density. in other words, we excluded small v-adic neighbourhoods around the τ where the fibre $\mathcal{E}_\tau$ is singular.

The following lemma will prove the first part.

Lemma 2. *Let E be an elliptic curve* (Weq) *defined over a discrete valuation ring R_v with finite residue field $\mathbb{F}_v$. The index of the subgroup $E^\circ(K)$ in $E(K)$ is bounded by an expression depending only on the valuation of the discriminant Δ and the residue field $\mathbb{F}_v$.*

Proof. To see this, let $u \in R_v$ be the constant in the change of coordinates (2.6) of E used to obtain a minimal equation. We have that

$$\operatorname{ord}_v(\Delta) = 12 \operatorname{ord}_v(u) + \operatorname{ord}_v(\Delta_{\min}) \tag{4.3}$$

and so, both expressions on the right are bounded by the valuation of Δ. Now, the index of $E^\circ(K)$ in $E(K)$ is bounded by

$$\#(\tilde{E}(\mathbb{F}_v)) \cdot (\#\mathbb{F}_v)^{\operatorname{ord}_v(u)-1} \cdot (\text{the index in the minimal case}).$$

This is just saying how many points are pushed out of $E^\circ(K)$ when changing the equation.

From the algorithm of Tate (see [**25**]) we have a bound for the index in the minimal case, namely the maximum between 4 and $\operatorname{ord}_v(\Delta_{\min})$. The number of points in the reduction is bounded by an expression only depending on the cardinality of the field $\mathbb{F}_v$ by Hasse-Weil. Hence every factor is bounded by the valuation of the discriminant. □

The second part can be deduced from the calculations in the above lemma. If the bad fibre is not of multiplicative type, then the reduction of fibres close to it must be additive. Hence the minimal-case index is bounded by 4, furthermore the valuation of u will also be bounded when τ is sufficiently v-adically close to the bad fibre. So the index is bounded in a neighbourhood even though the valuation of Δ is not. In other words, we only have to remove small v-adic neighbourhoods of multiplicative fibres for finitely many v. □

It is not difficult to deduce a variant of Tate's theorem on the variation of the canonical height in a family of elliptic curves (see [**26**]) from the above consideration using local height functions.

We will now compare our results here to the non-archimedian calculations in the articles [**22**], [**23**] and [**24**]. In the first one, Silverman considers three examples to illustrate the general theorems that follow in [**23**] for the local real-valued height functions and in [**24**] for the Néron-Tate height.

Let us look at the last of his examples. It is the section $P = (0,0)$ in the family

$$\mathcal{E}\colon\quad y^2 \;+\; T\cdot xy \;+\; T\cdot y \;=\; x^3 \;+\; 2T\cdot x \tag{4.4}$$

over $\mathbb{Z}$ with $\Delta(T) = T^4\cdot(T+1)^2\cdot(2T+27)$. In fact, P passes through the singularity of the additive fibre at $T = x = y = 0$; but the multiple $Q = 3P = (\frac{-2T+1}{4}, \frac{-6T-1}{8})$ is a section that has good reduction everywhere, $\gamma(Q,\tau) = \pm 1$ for all $\tau \in \mathbb{Z}$ and so $e(Q_\tau) = e(Q)(\tau) = \pm 2$. According to [**21**, Theorem VI.4.1], we have an explicit formula for the local height functions $\hat\lambda$

$$\hat\lambda_{\mathcal{E}_\tau,p}(Q_\tau) = \operatorname{ord}_p(e(Q_\tau))\cdot\log(p) + \tfrac{1}{12}\operatorname{ord}_p(\Delta(\tau))\cdot\log(p)$$

for all primes p, since Q_τ has good reduction. It is then easy to deduce proposition I.6.1 of [**22**] using the quasi-quadraticity of $\hat\lambda$:

$$\begin{aligned} 9\cdot\hat\lambda_{\mathcal{E}_\tau,p}(P_\tau) &= \hat\lambda_{\mathcal{E}_\tau,p}(Q_\tau) - \operatorname{ord}_p(f_3(P_\tau))\cdot\log(p) + \tfrac{2}{3}\operatorname{ord}_p(\Delta(\tau))\cdot\log(p)\\ &= \operatorname{ord}_p(2)\cdot\log(p) - \operatorname{ord}_p(2\tau^3)\cdot\log(p) + \tfrac{9}{12}\cdot\operatorname{ord}_p(\Delta(\tau))\log(p)\\ \hat\lambda_{\mathcal{E}_\tau,p}(P_\tau) &= \tfrac{1}{12}\operatorname{ord}_p(\Delta(\tau)/\tau^4)\log(p)\end{aligned}$$

The main difference to his treatment is that we are multiplying the section with a sufficiently large integer until we can work with the nice explicit formula for the local height function. A combination of proposition 3 and proposition 6 can even be used to prove the "potential good reduction" case of theorem II.0.1 in [**23**].

But of course, we fail to calculate anything when there is no multiple that has good reduction everywhere. It is no surprise that this happens precisely when there are terms in $\frac{1}{\log t}$ appearing in Silverman's formulae. We would have to work with explicit cancellations in the multiplicative case.

For instance, we change the above Weierstrass equation to a minimal model at $T = \infty$. Let $S = \frac{1}{T}$, $x' = S^2\cdot x$ and $y' = S^3\cdot y$, then

$$\mathcal{E}'\colon\quad {y'}^2 \;+\; x'y' \;+\; S^2\cdot y' \;=\; {x'}^3 \;+\; 2S\cdot {x'}^2 \quad\text{ and }\quad P' = (0,0).$$

The fibre at $S = 0$ is multiplicative and only $5P$ will not encounter the singularity anymore, but it hits the fibre at $(\frac{4}{9}, \frac{4}{27})$. There is no multiple of P that will have good reduction at 2 for all $S \in \mathbb{Z}$.

5. *The canonical p-adic sigma function*

We recall the following theorem due to Mazur and Tate. It is a special case of the results in the second appendix of [**11**].

First some notation: A denotes a complete discrete valuation ring with residue field $\mathbb{F}_v$ of characteristic $p \neq 2$. The Tate-algebra $A\{T\}$ is defined to be the v-adic completion of the polynomial ring $A[T]$, it coincides with the algebra of power-series in $A[\![T]\!]$ whose coefficients tend v-adically to zero.

Theorem 1 (B. Mazur and J. Tate). *Let $\mathcal{E}$ be a Weierstrass equation* (Weq) *defined over the Tate-algebra $A\{T\}$. We suppose that every fibre $\mathcal{E}_\tau$, for τ in the algebraic closure $\bar{A}$ of A, is an elliptic curve with good and ordinary reduction. Then there exists a unique function $\sigma_{\mathcal{E}}(T)(t)$, called the* sigma function, *on the formal group $\hat{\mathcal{E}}/A\{T\}$ of the form $t\cdot(1+t\cdot A\{T\}[\![t]\!])$, where $t=-\frac{x}{y}$, such that one of following two equivalent conditions holds (we write $\sigma(Q,\tau)$ for $\sigma_{\mathcal{E}}(\tau)(t(Q_\tau))$ when Q is a point of the formal group $\hat{\mathcal{E}}_\tau(\bar{A})$):*

- *For all non-zero points P and Q in the formal group $\hat{\mathcal{E}}_\tau(A)$, we have*

$$\frac{\sigma(P-Q,\tau)\cdot\sigma(P+Q,\tau)}{\sigma(P,\tau)^2\cdot\sigma(Q,\tau)^2}=x(Q_\tau)-x(P_\tau). \tag{5.1}$$

- *For all integers $m\neq 0$ and points Q in $\hat{\mathcal{E}}_\tau(\bar{A})$, there is the formula*

$$\sigma(m\cdot Q,\tau)=\sigma(Q,\tau)^{m^2}\cdot f_m(Q)(\tau), \tag{5.2}$$

where $f_m(Q)$ is the m-th division polynomial as defined in section 2, which is a function on $\mathcal{E}$ that, restricted to the formal group, is in

$$t(Q)^{1-m^2}\cdot A\{T\}[\![t(Q)]\!].$$

In particular, we are granted a sigma function for every elliptic curve E in Weierstrass form over the ring A with good ordinary reduction, that is, a function

$$\sigma_E(t)\in t\cdot(1+t\cdot A[\![t]\!]), \tag{5.3}$$

as described in theorem 3.1 of [**11**]. Our version here states moreover that the sigma functions of fibres in a family fit well together.

Our assumption that the reduction of every geometric fibre is ordinary implies that the Hasse-invariant modulo v is a constant element of $\mathbb{F}_v^\times$. The reduction of the coefficients of the sigma function $\sigma_{\mathcal{E}}$ above gives the sigma function $\tilde{\sigma}(T)(t)\in t\cdot(1+t\cdot\mathbb{F}_v[T][\![t]\!])$ at all places of $\mathbb{F}_v[T]$ of the reduced elliptic surface $\tilde{\mathcal{E}}$ as considered by Papanikolas in [**15**], for instance in his lemma 7.6.

6. *The p-adic height*

Let p be an odd prime. Let E be an elliptic curve over the number field K given by a Weierstrass equation (Weq) over R. We suppose that the elliptic curve E has good, ordinary reduction at all primes above p. Inside $E^\bullet(K)$, there is a subgroup of finite index, that we will denote by $E^p(K)$, contained in the intersection of the formal groups $\widehat{E}(\mathfrak{m}_v)$ of all places v above p. For a non-torsion point $P\in E^p(K)$, the (cyclotomic) *p-adic height* is defined by

$$\hat{h}_p(P) = \sum_{v\nmid p} \mathrm{ord}_v(e_v(P)) \cdot \log_p(\#\mathbb{F}_v) - \sum_{v|p} \log_p(\mathrm{N}_{K_v:\mathbb{Q}_p}(\sigma_v(P))),$$

where $\log_p\colon \mathbb{Q}_p^\times \to p\mathbb{Z}_p$ denotes the p-adic logarithm defined as usual with $\log_p(p) = 0$. Here $\sigma_v(t)$ denotes the canonical v-adic sigma function of E over the field K_v. But since we assumed that P belongs to $E^\bullet(K)$, we have a single $e(P)$ for all places v, and then we can simplify the expression above to

$$\begin{aligned}\hat{h}_p(P) &= \log_p(\mathrm{N}_{K:\mathbb{Q}}(e(P))) - \sum_{v|p} \log_p(\mathrm{N}_{K_v:\mathbb{Q}_p}(\sigma_v(P)))\\ &= \sum_{v|p} \log_p \circ \mathrm{N}_{K_v:\mathbb{Q}_p}\left(\frac{e(P)}{\sigma_v(P)}\right)\\ &= \log_p\Bigl(\prod_{v|p} \mathrm{N}_{K_v:\mathbb{Q}_p}\Bigl(\frac{e(P)}{\sigma_v(P)}\Bigr)\Bigr). \qquad (6.1)\end{aligned}$$

From the formulae (3.1) and (5.2), it is immediate that

$$\hat{h}_p(m \cdot P) = m^2 \cdot \hat{h}_p(P). \qquad (6.2)$$

Moreover $\hat{h}_p$ satisfies the parallelogram law and so it induces a bilinear form $\langle\cdot \mid \cdot\rangle_p$ on $E^\bullet(K)$ with values in $p\mathbb{Z}_p$ that can be extended then to all of $E(K)$ by defining the p-adic height of a point P via the formula (6.2), where m is such that the multiple mP belongs to $E^p(K)$; and we let $\hat{h}_p(O) = 0$.

Given points $P^{(1)}, \dots, P^{(r)}$ in $E(K)$, we define their *p-adic regulator*

$$\mathrm{Reg}_p(P^{(1)}, \dots, P^{(r)}) \in \mathbb{Q}_p$$

to be the determinant of the $r \times r$-matrix $(\langle P^{(i)} \mid P^{(j)}\rangle_p)_{i,j}$. The regulator of a full set of generators of the non-torsion part of $E(K)$ should appear in the p-adic version of the Birch and Swinnerton-Dyer formula (see [**12**]). But, as explained in the introduction, it is not even known if it is non-zero in general.

7. *Heights in Families*

Let $\mathcal{E}$ be a family over the number ring R with a section Q. Let p be an odd prime and suppose $\mathcal{E}$ has good ordinary reduction at all primes above p as in theorem 1. We will assume that Q has good reduction everywhere. Furthermore we want $Q \in \mathcal{E}^\bullet(K)$ and that Q_τ belongs to the formal group $\hat{\mathcal{E}}_\tau(\mathfrak{m}_v)$ for all τ and all places v above p. This can always be achieved by multiplying with a sufficiently large integer as $\mathcal{E}^\bullet(K)$ is of finite index and there are only finitely many different reductions at a place v for different $\tau \in R$. In particular, Q_τ belongs now to $\mathcal{E}^p_\tau(K)$ by proposition 5 and so we can calculate the p-adic height of Q_τ according to (6.1), at least if it is not torsion:

$$\begin{aligned}\hat{h}_p(Q_\tau) &= \log_p\Bigl(\prod_{v|p} \mathrm{N}_{K_v:\mathbb{Q}_p}\Bigl(\frac{e(Q_\tau)}{\sigma_v(Q,\tau)}\Bigr)\Bigr)\\ &= \log_p\Bigl(\prod_{v|p} \mathrm{N}_{K_v:\mathbb{Q}_p}\Bigl(\frac{e(Q)(\tau)}{\sigma_v(Q,\tau)}\Bigr)\Bigr) - \log_p \circ \mathrm{N}_{K:\mathbb{Q}}(\gamma(Q,\tau)), \qquad (7.1)\end{aligned}$$

where we used the definition of $\gamma(Q,\tau)$ in proposition 5.

Let now v be a place above p. We know that $e(Q)$ is a polynomial in $R[T]$, so in particular it lives in $R_v\{T\}$. Next we look at

$$t(Q) = -\frac{x(Q)}{y(Q)} = -\frac{a(Q)\cdot e(Q)}{b(Q)} \in K(T).$$

Since Q is in the formal group at v, the polynomial $e(Q)$ takes values in $\mathfrak{m}_v$, therefore $b(Q)$ is always a unit in $R_v^\times$. Hence $t(Q)$ is a converging power series in $R_v\{T\}$. Replacing this series in the sigma function gives a power series $\sigma_v(Q)$ in $R_v\{T\}$ such that

$$\sigma_v(Q)(\tau) = \sigma_v(Q,\tau) = \sigma_{v,\mathcal{E}_\tau}(Q_\tau).$$

Note that $e(Q_\tau)$, $t(Q_\tau)$ and $\sigma_\sigma(Q)(\tau)$ must have the same valuation, and so the valuation of $e(Q)(\tau)/\sigma_v(Q)(\tau)$ is bounded between 0 and the valuation of $\gamma(Q,\tau)$ at v. The latter is bounded itself as shown in proposition 3. We conclude that

$$g_v(Q) = \frac{e(Q)}{\sigma_v(Q)} \in R_v\{T\} \tag{7.2}$$

and that it has neither zeros nor poles.

We identify $\prod_{v|p} R_v$ with $R\otimes\mathbb{Z}_p$ in $K\otimes\mathbb{Q}_p$. Putting the functions g_v together, we get a continuous function

$$G(Q) = \prod_{v|p} g_v(Q)\colon R\otimes\mathbb{Z}_p \to R\otimes\mathbb{Z}_p$$

that has the property that every value can only be taken a finite number of times unless all the $g_v(Q)$ are constant functions. This is a consequence of (7.2) and the Weierstrass preparation theorem. $G(Q)$ is linked to the p-adic height in (7.1) by

$$\hat{h}_p(Q_\tau) = \log_p \circ \mathrm{N}\big(G(Q)(\tau)\big) - \log_p \circ \mathrm{N}\big(\gamma(Q,\tau)\big) \qquad \text{for all } \tau \in R, \tag{7.3}$$

whenever Q_τ is not torsion. Here N is the norm map from $K\otimes\mathbb{Q}_p$ to $\mathbb{Q}_p$.

THEOREM 2. *Let p be an odd prime and let $\mathcal{E}$ be a family of elliptic curves over a number ring R. Suppose $P \in \mathcal{E}^\bullet(K)$ is a section that has good reduction everywhere and that $\gamma(P,\tau)$ is a unit for all $\tau\in R$. Then the map $\tau \mapsto \hat{h}_p(P_\tau)$ extends to a continuous map from $R\otimes\mathbb{Z}_p$ to $\mathbb{Z}_p$.*

Proof. Most parts of the statement were obtained above when deriving the formula (7.3). We need to multiply our section P by a sufficiently large integer to obtain a section Q that satisfies the hypotheses made on Q. Moreover, the second term disappears because of corollary 4. □

In particular, it is interesting to see that the right hand side of (7.3) is defined even when the point Q_τ is torsion, or even if it is equal to O_τ. This can be seen as a partial p-adic analogue to Tate's theorem in [**26**].

THEOREM 3. *Let p be an odd prime and let $r > 0$ be an integer. Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Z}$ with sections $P^{(1)},\dots,P^{(r)}$. We suppose that $\mathcal{E}$ has good ordinary reduction at p and that every section $P^{(i)}$ has a multiple $Q^{(i)}$ which has good reduction everywhere and for which $\gamma(Q^{(i)},\tau)$ is constant for all $\tau\in\mathbb{Z}$. Then the regulator $\mathrm{Reg}_p(P_\tau^{(1)},\dots,P_\tau^{(r)})$ is either constant 0 or there are only finitely many τ in $\mathbb{Z}$ for which it vanishes.*

Proof. By multiplying $Q^{(i)}$ with an integer, we may suppose that it has everywhere good reduction and that $Q^{(i)}_\tau$ belongs to the formal group $\hat{\mathcal{E}}_\tau(p\mathbb{Z}_p)$ for all τ. By proposition 5, $\gamma^{(i)} = \gamma(Q^{(i)}, \tau)$ is still constant. So the above calculations apply to $Q^{(i)}$ and give the formula

$$\hat{h}_p(Q^{(i)}_\tau) = \log_p(g_p(Q^{(i)})(\tau)) - \log_p(\gamma^{(i)})$$

with $g_p(Q^{(i)}) \in \mathbb{Z}_p\{T\}$. Finally, the regulator $\operatorname{Reg}_p(P^{(1)}_\tau, \dots, P^{(r)}_\tau)$ is a linear combination of products of the functions $\tau \mapsto \hat{h}_p(Q^{(i)}_\tau)$. Therefore, it belongs to $\mathbb{Z}_p\{T\}$ as well, and the Weierstrass preparation theorem proves the statement. □

The same proof generalizes immediately to imaginary quadratic fields, but not for fields K with units of infinite order.

The theorem gives a weaker version of Silverman's specialisation theorem III.11.4 in [**21**]. If the regulator $\operatorname{Reg}_p(P^{(1)}_\tau, \dots, P^{(r)}_\tau)$ is non-zero for some $\tau \in \mathbb{Z}$, then the sections $P^{(1)}, \dots, P^{(r)}$ are linearly independent in $\mathcal{E}(K)$ and so the points $P^{(1)}_\tau, \dots, P^{(r)}_\tau$ will be independent in $\mathcal{E}_\tau(K)$ for almost all $\tau \in \mathbb{Z}$.

Unfortunately, we are unable to prove that the regulator is not constant zero if the sections are independent.

Here is an example to illustrate the theorem for $r = 1$: let

$$\mathcal{E}\colon\ y^2 + y = x^3 + (13T - 1) \cdot x$$

be a family over $\mathbb{Z}$ with constant, good and ordinary reduction at $p = 13$. We will study the section $P = (0, 0)$. The section happens to have good reduction everywhere and, since it has constant coordinates, $\gamma(P, \tau)$ is always ± 1. Using successive approximation of the coefficients of $\sigma_{\mathcal{E}}(\tau)(t)$ modulo powers of 13, one finds an approximation for the series for the 13-adic height

$$\begin{aligned}\hat{h}_{13}(P_\tau) = (6 \cdot 13^2 + \mathbf{O}(13^3)) + (11 \cdot 13 + 8 \cdot 13^2 + \mathbf{O}(13^3)) \cdot \tau \\ +(8 \cdot 13^2 + \mathbf{O}(13^3)) \cdot \tau^2 + \mathbf{O}(13^3)\end{aligned}$$

valid for all $\tau \in \mathbb{Z}$. Hence it is easy to see that for all $\tau \not\equiv 0 \pmod{13}$, the valuation of the 13-adic height of P_τ is 1. Moreover, in this example, there is only one single zero τ in $\mathbb{Z}_{13}$ of the function on the right and it seems unlikely that it will be an element of $\mathbb{Z}$.

There are conjectures of Lang and Silverman on lower bounds for the real valued Néron-Tate height, such as conjecture 9.9 in [**20**]. As stated in the introduction, this is certainly not true for the p-adic height, for we have the following

COROLLARY 5. *The p-adic height can become arbitrarily small.*

This is best explained with another example. The family

$$\mathcal{E}\colon\ y^2 = x^3 - (10T + 1)^2 \cdot x + (10T + 1)^2$$

has a section $P = (10T + 1, 10T + 1)$. It has a multiple $Q = 6P$ that satisfies the hypotheses of theorem 3 for $p = 5$. Again the 5-adic height of P_τ is a power series in τ with coefficients in $\mathbb{Z}_5$ converging to 0. There is a unique 5-adic integer $\tau_0 \in \mathbb{Z}_5$ that is a zero of this function. By taking integers $\tau \in \mathbb{Z}$ close enough to τ_0, we will obtain points with arbitrarily small 5-adic height:

$$\begin{aligned}
\tau = 98 &= 3+4\cdot 5+3\cdot 5^2 : & \hat{h}_5(P_\tau) &= 5^4+3\cdot 5^5+4\cdot 5^6+\mathbf{O}(5^7)\\
\tau = 473 &= 3+4\cdot 5+3\cdot 5^2+3\cdot 5^3 : & \hat{h}_5(P_\tau) &= \qquad 2\cdot 5^5+4\cdot 5^6+\mathbf{O}(5^7)\\
\tau = 1098 &= 3+4\cdot 5+3\cdot 5^2+3\cdot 5^3+5^4 : & \hat{h}_5(P_\tau) &= \qquad\qquad 4\cdot 5^6+\mathbf{O}(5^7)
\end{aligned}$$

8. *Further calculations and conjectures*

The p-adic height of a point P, which does not lie in the formal group at p, on an elliptic curve $E/\mathbb{Q}$ with good ordinary reduction at p is, by definition, in $p\,\mathbb{Z}_p$, unless p is anomalous (meaning that p divides $\#\tilde{E}(\mathbb{F}_p)$), in which case it belongs to $p^{-1}\,\mathbb{Z}_p$. It seems that its valuation is most of the time equal to 1 (or -1 in the anomalous case). See also the tables, included at the end of this article, for a list of exceptionally small height.

In order to check this intuition, one can do the following calculation: all families with $a_6 = 0$ have a section $P = (0,0)$ that does not belong to the formal group at p. Instead of working with $\mathbb{Z}\{T\}$, one can do a similar reasoning for $\mathbb{Z}\{a_1, a_2, a_3, a_4\}$.

Look at all coefficients $[a_1, a_2, a_3, a_4, a_6 = 0]$ with the same reduction modulo p. Since these curves have the same reduction, there is a multiple $Q = mP$ which lies in the formal group at p for all curves. The p-adic height of Q turns out to be a function in $\mathbb{Z}_p\{a_1, a_2, a_3, a_4\}$ if the point has good reduction at all primes on the corresponding curve. If so, the p-adic height of $(0,0)$ modulo p^k only depends on the coefficients a_i modulo p^k for all $k > 1$.

For $p = 3$, there are 2916 choices for the vector $[a_1, a_2, a_3, a_4, a_6 = 0]$ modulo 9 such that the corresponding curve has good ordinary reduction at 3. For each vector, one can find an elliptic curve with coefficients in $\mathbb{Z}$ such that the point $(0,0)$ has non-singular reduction for all primes, and calculates the 3-adic height modulo 9 of it. This is, by the above remark, independent of the chosen coefficients in $\mathbb{Z}$. In this way, we find 983 cases where the 3-adic height is exceptionally small. In other words, we have proved the follwing

- In 33.71% of all cases the 3-adic height of a point P outside the formal group with good reduction at every prime on an elliptic curve with good ordinary reduction at 3 has valuation higher than the expected valuation 1(or -1 in the anomalous case).
- A similar calculation for $p = 5$ leads to the affirmation that 20.0032% have smaller 5-adic height than expected.

This leads to the following

Conjecture 1. Let E be an elliptic curve defined over $\mathbb{Q}$ and P a point of infinite order in $E(\mathbb{Q})$.

- Among the primes p for which E has good, ordinary, non-anomalous reduction, the set of p for which the p-adic height of P belongs to $p^2\mathbb{Z}_p$ has density zero.
- Among these primes p there are only finitely many such that the p-adic height of P belongs to $p^3\mathbb{Z}_p$.
- Among anomalous, good and ordinary primes p, the set of p for which the p-adic height of P belongs to $\mathbb{Z}_p$ is of density zero and there are only finitely many for which it belongs to $p\mathbb{Z}_p$.

We describe a consequence of these conjectures for the Iwasawa-theory of elliptic curves. As a general reference for Iwasawa-theory on elliptic curves we refer the reader to [**8**] or [**7**].

Let $E/\mathbb{Q}$ be an elliptic curve of rank r and suppose that the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is finite. Assume E has good ordinary reduction at an odd prime p. By $\mathbb{Q}^{p\text{-cyc}}$, we mean the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, i.e. the unique Galois extension of $\mathbb{Q}$ with Galois group Γ isomorphic to $\mathbb{Z}_p$. Let X be the Pontryagin-dual of the p-Selmer group $\mathrm{Sel}_p(E/\mathbb{Q}^{p\text{-cyc}})$, which is, by a theorem of Kato [**9**], a torsion module over the Iwasawa-algebra $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \approx \mathbb{Z}_p[\![T]\!]$. When the p-adic regulator Reg_p of a set of generators $P^{(1)}, \ldots, P^{(r)}$ of $E(\mathbb{Q})$ modulo torsion is non-zero, a theorem of Perrin-Riou [**17**] and Schneider [**19**] asserts that the lowest term of the characteristic power series $f_X(T)$ of X in $\mathbb{Z}_p[\![T]\!]$ is $c \cdot T^r$, where c is given explicitly by

$$c \sim \frac{\mathrm{Reg}_p \cdot (\#\tilde{E}(\mathbb{F}_p)(p))^2}{p^r} \cdot \frac{\prod_v c_v \cdot \#(Ш(E/\mathbb{Q})(p))}{(\#E(\mathbb{Q})(p))^2}$$

with equality up to multiplication by a unit in $\mathbb{Z}_p^\times$. Here the c_v are the local Tamagawa factors. For all but finitely many primes p, the leading coefficient c is then equal, up to a unit in $\mathbb{Z}_p^\times$, to

$$c \sim \tfrac{1}{p^r} \cdot \mathrm{Reg}_p \cdot (\#\tilde{E}(\mathbb{F}_p)(p))^2.$$

If c is a unit, then we conclude that X is pseudo-isomorphic to $\Lambda/(T^r) \approx \mathbb{Z}_p^r$. The Pontryagin-dual of the exact sequence (see page 17 of [**8**])

$$0 \to E(\mathbb{Q}^{p\text{-cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_p(E/\mathbb{Q}^{p\text{-cyc}}) \to Ш(E/\mathbb{Q}^{p\text{-cyc}})(p) \to 0$$

shows that the dual of the group $E(\mathbb{Q}^{p\text{-cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is a quotient of X. Thus the rank of the Mordell-Weil group $E(\mathbb{Q}^{p\text{-cyc}})$ is at most r. On the other hand it contains already the group $E(\mathbb{Q})$ and so it is of rank r. This also shows that $Ш(E/\mathbb{Q}^{p\text{-cyc}})(p)$ is $\mathbb{Z}_p$-cotorsion and hence finite.

So we can reformulate the above conjecture and extend it to larger ranks:

Conjecture 2. Let $E/\mathbb{Q}$ be an elliptic curve of rank $r > 0$ and suppose that $Ш(E/\mathbb{Q})$ is finite.

- The coefficient c is a unit in $\mathbb{Z}_p^\times$ for a set of density 1 among the primes p with good ordinary reduction.
- The same is true for anomalous primes.
- For a set of density 1 among the primes p where E has good ordinary reduction, the rank of the Mordell-Weil group $E(\mathbb{Q}^{p\text{-cyc}})$ is equal to r and the group $Ш(E/\mathbb{Q}^{p\text{-cyc}})(p)$ is finite.

Note that for curves of rank $r = 0$, this is the statement of proposition 5.1 in [**7**] on page 105. But unlike in the case $r = 0$, the above conjecture claims that the behaviour for anomalous primes does not differ from the behaviour for non-anomalous primes, if $r > 0$.

Appendix A. *Tables*

The following tables list primes with special behaviours for some curves of rank 1 of small conductor. The elliptic curve E will be given by the coefficients of the minimal form $[a_1, a_2, a_3, a_4, a_6]$. All calculations have been done for odd primes smaller than 1000. We will list the primes with bad reduction, those with supersingular reduction. The next line contains the anomalous primes. Then the last line contains the most interesting information: the primes for which the p-adic height of the point P of infinite order is exceptionally small. For all other good and ordinary primes the valuation of the p-adic height of P is 1, if p is non-anomalous, and -1 for the anomalous. We found only one exception among the anomalous primes, namely $p = 3$ on the curve 91B.

Finally, we add a small list of values of heights in some exceptional cases above. All calculation were done using Pari-GP [1] and Mathematica.

References

1. C. Batut, D. Bernardi, H. Cohen, M. Olivier and K. Belabas, pari-gp, available at http://www.parigp-home.de/, 1999.
2. Dominique Bernardi, Hauteur p-adique sur les courbes elliptiques, Seminar on Number Theory, Paris 1979–80, Progr. Math., vol. 12, 1981, pp. 1–14.
3. Daniel Bertrand, Valuers de fonctions thêta et hauteur p-adiques, Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981), Progr. Math., vol. 22, 1982, pp. 1–11.
4. Siegfried Bosch, Werner Lütkebohmert and Michel Raynaud, Néron models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, 1990.
5. Nicolas Bourbaki, Éléments de mathématique. Fasc. XXXI. Algèbre commutative. Chapitre 7: Diviseurs, Hermann, Paris, 1965.
6. Gregory S. Call, Variation of local heights on an algebraic family of abelian varieties, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 72–96.
7. John Coates, Ralph Greenberg, Kenneth A. Ribet and Karl Rubin, Arithmetic theory of elliptic curves, Lecture Notes in Mathematics, vol. 1716, Springer-Verlag, 1999.
8. John Coates and Ramdorai Sujatha, Galois cohomology of elliptic curves, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 88, Narosa, 2000.
9. Kazuya Kato, p-adic Hodge theory and values of zeta functions of modular curves, Preprint Series, Graduate School of Mathematical Sciences, The University of Tokyo.
10. Barry Mazur and John Tate, Canonical height pairings via biextensions, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, 1983, pp. 195–237.
11. Barry Mazur and John Tate, The p-adic sigma function, Duke Math. J. 62 (1991), no. 3, 663–688.
12. Barry Mazur, John Tate and Jeremy Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. 84 (1986), no. 1, 1–48.
13. André Néron, Quasi-fonctions et hauteurs sur les variétés abéliennes, Ann. of Math. (2) 82 (1965), 249–331.
14. André Néron, Hauteurs et fonctions thêta, Rend. Sem. Mat. Fis. Milano 46 (1976), 111–135.
15. Matthew A. Papanikolas, Canonical heights on elliptic curves in characteristic p, Compositio Math. 122 (2000), no. 3, 299–313.
16. Bernadette Perrin-Riou, Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe, Invent. Math. 70 (1982/83), no. 3, 369–398.
17. Bernadette Perrin-Riou, Théorie d'Iwasawa et hauteurs p-adiques, Invent. Math. 109 (1992), no. 1, 137–185.
18. Peter Schneider, p-adic height pairings. I, Invent. Math. 69 (1982), no. 3, 401–409.
19. Peter Schneider, p-adic height pairings. II, Invent. Math. 79 (1985), no. 2, 329–374.
20. Joseph H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.
21. Joseph H. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer-Verlag, New York, 1994.
22. Joseph H. Silverman, Variation of the canonical height on elliptic surfaces I: Three examples, J. reine angew. Math. 426 (1992), 151–178.
23. Joseph H. Silverman, Variation of the Canonical Height on Elliptic Surfaces II: Local Analycity Properties, Journal of Number Theory 48 (1994), 291–329.
24. Joseph H. Silverman, Variation of the Canonical Height on Elliptic Surfaces III: Global Boundedness Properties, Journal of Number Theory 48 (1994), 330–352.
25. John Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp,

E	$[a_i]$	P	bad	supersingular	anomalous	**exceptions**	E
37A	$[0,0,1,-1,0]$	$(0,0)$	37	3, 17, 19, 257, 311, 577	53, 127, 443, 599	**13, 67, 547**	37A
43A	$[0,1,1,0,0]$	$(0,0)$	43	7, 37	3, 5, 103, 127, 541	**none**	43A
53A	$[1,-1,1,0,0]$	$(0,0)$	53	3, 5, 11, 239, 751	71, 97	**none**	53A
57A	$[0,-1,1,-2,2]$	$(2,1)$	3, 19	37, 41, 151, 163, 491, 571, 599, 601	11	**5**	57A
58A	$[1,-1,0,-1,1]$	$(0,1)$	29	3, 23, 83, 139, 191, 283, 311, 317, 587	53, 109, 673, 739	**31**	58A
61A	$[1,0,0,-2,1]$	$(1,0)$	61	31, 101, 281, 439	3, 7, 13, 113	**71**	61A
65A	$[1,0,0,-1,0]$	$(1,0)$	5, 13	139, 191, 439, 659	3	**43**	65A
77A	$[0,0,1,2,0]$	$(2,3)$	7, 11	3, 283 , 503, 701, 911	31, 71, 179, 223	**5**	77A
79A	$[1,1,1,-2,0]$	$(0,0)$	79	113, 271, 409, 479, 521, 947	none	**41, 83, 131**	79A
82A	$[1,0,1,-2,0]$	$(0,0)$	41	29, 103, 131, 191, 251, 421, 443, 599, 811, 859, 983	3	**5, 229, 283, 499**	82A
83A	$[1,1,1,1,0]$	$(0,0)$	83	47, 73, 89, 199, 281, 311, 503, 661	853, 991	**none**	83A
88A	$[0,0,0,-4,4]$	$(2,2)$	11	3, 13, 241, 271, 547, 761	23, 383, 797	**29, 41, 401**	88A
89A	$[1,1,1,-1,0]$	$(0,0)$	89	29, 41, 101, 359, 421, 433, 811, 911	733	**5**	89A
91A	$[0,0,1,1,0]$	$(0,0)$	7, 13	3, 151, 269, 457, 877	277, 673	**17, 181, 607**	91A
91B	$[0,1,1,-7,5]$	$(-1,3)$	7, 13	11, 59, 101, 149, 347, 383, 521, 563, 827, 863	**3**	**3, 991**	91B
92A	$[0,0,0,-1,1]$	$(1,1)$	23	3, 59, 97, 109, 157, 227	none	**193**	92A

FIGURE A.1. *Calculations of p-adic heights for elliptic curves of rank one with small conductor and* $2 < p < 1000$.

E	p	p-adic height of P	its valuation
37A	13	$6 \cdot 13^2 + 9 \cdot 13^3 + 3 \cdot 13^4 + \mathbf{O}(13^5)$	2
37A	67	$27 \cdot 67^2 + 4 \cdot 67^3 + \mathbf{O}(67^4)$	2
57A	5	$3 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + \mathbf{O}(5^5)$	2
58A	31	$13 \cdot 31^2 + 5 \cdot 31^3 + \mathbf{O}(31^4)$	2
61A	71	$37 \cdot 71^2 + 18 \cdot 71^3 + \mathbf{O}(71^4)$	2
65A	43	$17 \cdot 43^2 + 13 \cdot 43^3 + \mathbf{O}(43^4)$	2
77A	5	$4 \cdot 5^2 + 1 \cdot 5^4 + \mathbf{O}(5^5)$	2
79A	41	$6 \cdot 41^2 + 7 \cdot 41^3 + \mathbf{O}(41^4)$	2
79A	83	$14 \cdot 83^2 + \mathbf{O}(83^3)$	2
79A	131	$99 \cdot 131^2 + \mathbf{O}(131^3)$	2
82A	5	$2 \cdot 5^2 + 1 \cdot 5^3 + 1 \cdot 5^4 + \mathbf{O}(5^5)$	2
82A	229	$67 \cdot 229^2 + \mathbf{O}(229^3)$	2
82A	283	$241 \cdot 283^2 + \mathbf{O}(283^3)$	2
88A	29	$1 \cdot 29^2 + 14 \cdot 29^3 + \mathbf{O}(29^4)$	2
88A	41	$29 \cdot 41^2 + 20 \cdot 41^3 + \mathbf{O}(41^4)$	2
89A	5	$1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \mathbf{O}(5^5)$	2
91A	17	$15 \cdot 17^2 + 8 \cdot 17^3 + \mathbf{O}(17^4)$	2
91A	181	$85 \cdot 181^2 + \mathbf{O}(181^3)$	2
91B	3	$2 \cdot 3^3 + 3^6 + 3^7 + \mathbf{O}(3^8)$	**3**
92A	193	$23 \cdot 193^2 + \mathbf{O}(193^3)$	2

FIGURE A.2. *Some small p-adic heights on curves of rank one*

Antwerp, 1972), Springer, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

26. JOHN TATE, Variation of the canonical height of a point depending on a parameter, Amer. J. Math. 105 (1983), no. 1, 287–294.

Christian Wuthrich
Trinity College
Cambridge

c.wuthrich@dpmms.cam.ac.uk