The Hare and the Wolf

An Essay on
p–adic heights on elliptic curves

By Chris Wuthrich

Supervisor: John Coates

Unless where explicitly stated, the results in this essay are my own research results, except for the second chapter which is a review on the subject. Nothing is the outcome of work done in collaboration.

AT THE DEPARTMENT OF PURE MATHEMATICS
AND MATHEMATICAL STATISTICAL
UNIVERSITY OF CAMBRIDGE

Abstract

This essay deals with different heights on elliptic curves. Intuitively the height of a point on an elliptic curve should measure its arithmetic complexity.

The first part is devoted to the study of local heights from a new point of view, everything is deduced from considerations of cancellations in certain fractions. The second chapter contains well-known definitions of different global heights. The main focus are p-adic heights, some explicit calculations and a discussion of the conjecture on the non-degeneracy are included. Next the notions of forests are introduced, they are special kinds of families of elliptic curves and the previous definitions are applied to these forests. In the last chapter the variation of p-adic heights in forests is analysed. Some new results are mentioned here, including families of curves with non-zero heights. In the appendix are added a few tables and the computer programs written for the calculations.

Thanks

I have the pleasure to thank the persons without whose help this essay wouldn't have been possible: Hannu Harkonnen and Christopher Voll for many interesting discussions, Gianluigi Sechi for a very inspiring time in Sardinia, Paola Argentin, Sylvia Guibert and Eugenio Rodriguez for their help in Geneva. But most of all, I would like to thank my supervisor John Coates for the encouragement and guidance in this first year of my PhD.

Contents

The Wolf And The Hare

> La Nature est un temple où de vivants piliers
> Laissent parfois sortir de confuses paroles;
> L'homme y passe à travers des forêts de symboles
> Qui l'observent avec des regards familiers
>
> (Baudelaire)

In the deepest forest in a cold and rainy land, there lived a Wolf as mean and evil as a Wolf can be. His wickedness was well-known[1] ever since he killed an innocent lamb under the pretence of having made muddy the water of river Cam. Driven by his never satiated hunger, he went hunting often and cruelly killed many inhabitants of the large forest.

Some day a young Hare got caught by the evil Wolf while reading a yellow book. He dragged the poor Hare to his den where he intended to roast him "à petit feu". But the Hare trembling of fear said to the Wolf: 'Dear master Wolf, please let me live one more day. I would then tell you a story that might well interest you. I heard you have been working on p-adic heights on elliptic curves just as I did. If you give me one more day, I could tell you about the discoveries I made concerning their non-degeneracy. If you killed me I would take these things with me to the grave.'

The Wolf still wasn't convinced. 'What could you tell me that I don't know yet?' he asked.

'I found another way of looking at heights,' his victim regaining some hope tried to explain, 'I can reformulate the theory of heights by looking at cancellations in the denominator when multiplying a point on an elliptic curve by an integer m. The results on local and global canonical heights, that you, dear master Wolf, certainly are aware of, follow then easily using the knowledge on cancellations. While trying to reformulate the results on the variation of heights in families of elliptic curves, I realized that one can get interesting results on p-adic heights in such families.'

'What kind of p-adic heights?' interrupted the Wolf, getting more and more interested.

'The p-adic height constructed via the canonical p-adic sigma function found by Mazur and Tate. It was also found by Schneider and Perrin-Riou who used it in Iwasawa theory of elliptic curves. Unlike the usual Néron-Tate height, its non-degeneracy is still an open problem. But if you would like me to tell more about it, then please give a pencil and some paper.'

The Wolf, although he was as mean and evil as a Wolf can be, he was also a Wolf of great intellect and knowledge and so he knew about the importance of the question for the p-adic version of the Birch–Swinnerton-Dyer conjecture. He decided to allow the Hare to teach him his results, but he never forgot about the tasty "lièvre à la Royale à la Graisse d'Oie".

[1] see Fable X de [Fontaine, 1709]

Chapter 1

Local Heights on Elliptic Curves

1.1 The denominator e

The Wolf brought the Hare paper and pen and asked him: ‘So by *denominator* you meant the denominator of the x-coordinate?’

So the Hare started his explanations using the pen to write down the equations. ‘Yes. But not too hasty,’ he said, remembering well what fate would expect him in the end. ‘I will carefully define everything, now. Suppose we are working over a principal ring R with fraction field K. Our elliptic curve E over K is 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 R. I don’t want to assume that it is minimal. We are looking at a nonzero point P in $E(K)$ and the valuation of its coordinates at the finite places of R. It’s not difficult to see that if either the x or the y-coordinate of P has negative valuation at some prime v then so has the other and we have $3 \cdot v(x) = 2 \cdot v(y)$ and ... ’

‘Oh yeah, I see because the valuations of the coefficients a_i are positive and then it can be read out of our equation (Weq),’ interrupted him the Wolf.

‘Exactly. So we can write our point as

$$P = (x(P), y(P)) = \Big(\frac{a(P)}{e(P)^2}, \frac{b(P)}{e(P)^3}\Big)$$

for some numbers $a(P)$, $b(P)$ and $e(P)$ where the $e(P)$ is relatively prime to both $a(P)$ and $b(P)$. If R were merely a Dedekind ring, we would have to do all this with ideals. But most things can be done locally, so that I avoid these generalities by now.’

‘I guess that by “numbers” you meant elements in R; but tell me, even over the integers $\mathbb{Z}$ this is not well defined because of the sign, no?’

‘I know, the quantities are defined up to a unit in $R^\times$. In the case of $\mathbb{Z}$, I always take $e(P)$ to be positive and for discrete valuation rings I normally would take it to be a power of a chosen uniformizer. Anyway, we will only be interested in the valuation of $e(P)$ most of the time.’

1.2 Division polynomials

‘I think,’ the Hare continues his explanations. ‘I have to tell you something about *division polynomials*. Here we can take E to be an elliptic curve over any field K. For every integer $m \neq 0$, I want to define a function f_m in $K(E)$ with divisor $[m]^*(O) - \deg([m]) \cdot (O)$. Unless the characteristic of K divides m, the degree of $[m]$ is m^2. If you allow me I shall continue assuming this, although everything can be done in general, adapting correctly the notations. It is not difficult to see that the divisor above is of degree 0 and sums to O. So there are functions with this divisor, among them I can pick one by choosing the first coefficient of the development at the origin O, say

$$f_m = m\,t^{1-m^2} + \text{higher terms in } t$$

where $t = -\frac{x}{y}$ with respect to a fixed (Weq).’

‘That is not extremely explicit,’ commented cynically his worst enemy.

'Well, you can find a good description of the explicit recursion formulae in the first appendix to the paper[1] where MAZUR and TATE defined the p-adic sigma function. This will also convince you that the square f_m^2 can be written as a polynomial in x of degree m^2-1. More precisely, it looks like

$$f_m(P)^2 = m^2\, x(P)^{m^2-1} + \text{ lower terms in } x(P). \tag{1.1}$$

Moreover f_m turns out to be a polynomial in $\mathbb{Z}[a_1,a_2,a_3,a_4,a_6][x,y]$, hence in our situation above $f_m(x,y)\in R[x,y]$. If m is odd then $f_m(x)\in R[x]$ is of degree $\frac{m^2-1}{2}$.

Unfortunately f_m depends on the chosen equation: A change of variables[2] can be written in the form

$$\begin{aligned} x' &= u^2\, x + r_1 \\ y' &= u^3 y + u^2\, r_2\, x + r_3\,, \end{aligned} \tag{1.2}$$

for some constants u, r_1, r_2 and r_3 in R. The new parameter $t' = -\frac{x'}{y'}$ can be written as

$$t' = u^{-1}\cdot t + \cdots$$

in an expansion at O. The division polynomial f'_m with respect to the new coordinates evaluated at the image P' of a point P must be a multiple of $f_m(P)$ as the functions have the same divisor. The expansion at O is

$$f_m = m\,(u\,t' + \cdots)^{1-m^2} + \cdots\,,$$

implying the result

$$f'_m(P') = u^{m^2-1}\, f_m(P). \tag{1.3}$$

Or in other words the function

$$P \longmapsto f_m(P)^{12}\cdot\Delta^{1-m^2}$$

is independent of the equation.

You, dear master Wolf, might know that these polynomials are related to the multiplication-by-m. Let me write down a first little lemma.[3]'

Lemma 1.1. *If m is neither 0, -1 nor 1, then*

$$\frac{f_{m+1}\cdot f_{m-1}}{f_m^2} = x - x\circ[m] \tag{1.4}$$

Then he asked the Wolf if he remembered the proof. This one grabbed the pencil and wrote that the divisor on both sides should equal

$$[m-1]^*(O) + [m+1]^*(O) - 2\cdot[m]^*(O) - 2(O).$$

Then he calculated on both side the leading term in the development with respect to the uniformizer t and found correctly

$$\left(1-\frac{1}{m^2}\right)\cdot t^{-2} + \cdots$$

for both expressions. □

'In other words,' his prisoner continued, 'the multiplication-by-m can be written as

$$x(mP) = \frac{g_m(P)}{f_m(P)^2}$$

where $g_m = x\cdot f_m^2 - f_{m+1}\cdot f_{m-1}\in K(E)$ is a function that happens to be a polynomial in x of degree m^2.'

[1] here the Hare was talking about [Mazur and Tate, 1991]. Other descriptions are in [Silverman, 1992, Excercise III.7, page 105] or in the formulary of [Cassels, 1991] on page 133.

[2] can be found in different sources, for instance [Silverman, 1992, p. 49] or [Deligne, 1975].

[3] see proposition 1 in the first appendix to [Mazur and Tate, 1991].

1.3 The Cancellation

'This formula can now be used to define the cancellation. Since both, numerator and denominator, are polynomials in $x(P)$, I can multiply both with a certain power of $e(P)$ to guarantee that both expressions represent elements of R again:

$$\frac{a(mP)}{e(mP)^2} = x(mP) = \frac{g_m(P) \cdot e(P)^{2m^2}}{(f_m(P) \cdot e(P)^{m^2})^2} \tag{1.5}$$

As the denominator is a square again, we could expect it to be $e(mP)$, but it might be that the fraction on the right in this formula is not reduced while the one on the left is. I will call

$$\delta_m(P) = \frac{f_m(P) \cdot e(P)^{m^2}}{e(mP)} \tag{1.6}$$

the *cancellation of P when multiplying with m*. This is an element in R defined up to a unit.'

'Unless $e(mP)$ is zero,' added the still suspicious Wolf.

'Ah, I forgot. Of course this make only sense if P is not an m-torsion point. Note also that the cancellation depends on the chosen equation. Even worse, there is no possible definition that is independent.'

'What do you mean by that?'

'Let me formulate a first part as a

Lemma 1.2. *Under a change of equation of the form* (1.2) *with u being a unit in R, the cancellation $\delta_m(P)$ can only change by a unit.*

In (1.3), I showed you that the division polynomial only changes by a unit. Furthermore, we can read out the equations (1.2) that the valuation of $e(P)$ and $e'(P')$ at all primes are equal since r_1 is an integral element. This should close the proof. □

But if u is not a unit, we have some problems. First, if u divides $e(P)$ and $e(mP)$, then we have $e'(P') = \frac{e(P)}{u}$ and $e'(mP') = \frac{e(mP)}{u}$ and so

$$\delta'_m(P') = \frac{u^{m^2-1} f_m(P) \cdot u^{-m^2} e(P)^{m^2}}{u^{-1} e(mP)} = \delta_m(P).$$

which is good. But when u is prime to both $e(P)$ and $e(mP)$, then $\delta'_m(P') = u^{m^2-1} \delta_m(P)$. In other words: The minimal Weierstrass equation for E over R is one with minimal cancellation.'

'Can you give me some examples of cancellations?'

'I beg you to wait a little bit,' the scared Hare answered to the impatient and hungry Wolf, 'first I am going to prove to you that often there is no cancellation.'

1.3.1 The Non-Cancellation

So the Hare started to talk about the first little non-trivial result that he would use often later. He wrote the following

Non-Cancellation Proposition 1.3. *Let E be an elliptic curve given by an equation* (Weq) *over a ring R which is complete with respect to a discrete valuation*[4] *v. If a point $P \in E(K)$ 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 $mP \neq O$.*

'Let me explain you the proof, dear master Wolf,' the Hare said. 'We split up 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 $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_v)$ of non-singular points on the reduction

[4] valuations are always assumed to be normalised such that their image is exactly the group of integers $\mathbb{Z}$.

$\tilde{E}$. The multiplication formula (1.5) is also valid in the this group and so the denominator must be invertible in $\mathbb{F}_v$, that is the valuation of $f_m(P) \cdot e(P)^{m^2}$ is zero, and that's what we want.

Next, I will prove you 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 R. Since there is a canonical isomorphism of groups[5]

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

we see that m must have valuation 0 as an element in R, otherwise mP would have to belong to $\widehat{E}(\mathfrak{m}^{k+1})$. The expression

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

copied from (1.1) must have valuation $2k$ since $a(P)$ is a unit when $e(P)$ is not. Both terms in the definition (1.6) of $\delta_m(P)$ have valuation k.

Finally, we should look at the case when $e(mP)$ has a strictly bigger valuation than $e(P)$. If so, mP lies in a layer closer O, and therefore the points $(m-1)P$ and $(m+1)P$ must lie in the same layer as P. I can now use what I just proved about such multiples: The expressions

$$f_{m\pm1}(P)\, e\left((m \pm 1)P\right)^{(m\pm1)^2}$$

must have the same valuation as $e(P)$. Let's look at the numerator of the multiplication formula (1.5).

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

I just convinced you 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. Hence we are done.' □

'And we can use it now for an elliptic curve over $\mathbb{Z}$,' commented the Wolf who followed with a lot of interest the proof of the Hare.

'Or more generally for any elliptic curve E over a Dedekind ring R, like a number ring or a ring of polynomials over a field. In the sub-group of points with nowhere singular reduction, I usually write it $E^{\circ}(K)$, there is no cancellation.'

1.3.2 The Cancellation When Multiplying With 2

'I will now give you some examples of cancellations,' the Hare, still fearing the angry Wolf, resumed his talk. 'Suppose we have a point P which reduces to a singular point. We can always achieve that our point is $P = (0, 0)$ without changing the cancellation, according to lemma 1.2. For the coefficients of our Weierstrass equation, this means that $a_6 = 0$ and that a_3 and a_4 must have strictly positive valuation.

I want to calculate the cancellation of P when multiplying with 2. Here is the duplication formula

$$x(2P) = -\frac{b_8}{b_6} = \frac{a_1\, a_3\, a_4 - a_2\, a_3^2 + a_4^2}{a_3^2}.$$

[5] this is Proposition IV.3.2 in [Silverman, 1992].

written in such a way that $\delta_2(P)^2$ is exactly the cancellation of this fraction. That is

$$2 \cdot v(\delta_2(P)) = \min(v(b_6), v(b_8)) = 2 \cdot \min(v(a_3), v(a_4))$$

where the last equality follows from a closer look at the numerator in the second fraction. Conclusion: If a point P reduces to a singular point then $\delta_2(P)$ is not a unit. A partial converse to the non-cancellation proposition 1.3.

From the equality $b_4^2 = b_2\,b_6 - 4\,b_8$, we learn that $v(b_4) \geq v(\delta_2(P))$. So every term in the expression for the discriminant

$$\Delta = -b_2^2\,b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2\,b_4\,b_6$$

has valuation at least twice as big as the valuation of $\delta_2(P)$. So we have

$$0 < v(\delta_2(P)) \leq \tfrac{1}{2}v(\Delta). \tag{1.7}$$

This is a slight (but easy) improvement to the inequality[6] used to give a lower bound for the naive height of $2P$.

Then I ran through the algorithm of Tate[7] to see if I can write it down explicitly. Except when the reduction is multiplicative, this is possible.'

Just as every unorganised mathematician, it took the Hare some time to search through his pile of papers that he brought with him in his yellow book, until he found the one he was looking for:

TYPE	III	IV	$\mathrm{I}_0^\star$	$\mathrm{I}_1^\star$	$\mathrm{I}_{2n}^\star$	$\mathrm{I}_{2n+1}^\star$	$\mathrm{IV}^\star$	$\mathrm{III}^\star$
$v(\delta_2(P))$	1	1	2	2	2 or $n+1$	2 or $n+1$	2	2
c_v	2	3	2, 3 or 4	2 or 4	2 or 4	2 or 4	3	2

'Why didn't you include the II and II*?' asked curiously the Wolf.

'Because the Tamagawa factor c_v is 1, so no-one can reduce to the singularity. For this table I assumed for once that the equation was minimal, otherwise you get cancellations as large as you want. Moreover in the cases $\mathrm{I}_n^\star$, if the valuation of a_4 is bigger than 2, then the cancellation has valuation $n+1$ and there are 4 components in the Néron model; otherwise $\delta_2(P)$ has only valuation 2.'

1.3.3 Other cancellations

'But let me continue with more general facts about cancellations. There is a useful lemma for calculations of cancellations for $m > 2$.'

Lemma 1.4. *For all non-zero n and m, the formula*

$$\delta_{nm}(P) = \delta_n(P)^{m^2} \cdot \delta_m(nP) \tag{1.8}$$

holds and, for all $m > 1$, we have

$$\frac{\delta_{m+1}(P) \cdot \delta_{m-1}(P)}{\delta_m(P)^2} = (x(P) - x(mP)) \cdot \frac{e(P)^2 \cdot e(mP)^2}{e((m+1)P) \cdot e((m-1)P)}. \tag{1.9}$$

Then the Hare showed his proof to the Wolf. 'The first equation comes from the equation[8]

$$f_{nm} = f_n^{m^2} \cdot (f_m \circ [n])$$

[6] see on page 204 of [Silverman, 1992].

[7] originally published in [Tate, 1975], a longer explication is in paragraph IV.9 of [Silverman, 1994].

[8] in appendix I of [Mazur and Tate, 1991] this is proposition 2.

which holds for the division polynomials and which can be check as usual by looking at the divisor and the first term in the development in t. Multiplying this somewhat, we get

$$\frac{f_{nm}(P)\cdot e(P)^{n^2m^2}}{e(nmP)} = \frac{f_n(P)^{m^2}\cdot e(P)^{n^2m^2}}{e(nP)^{m^2}}\cdot\frac{f_m(nP)\cdot e(nP)^{m^2}}{e(nmP)}$$

which is the equality (1.8). The second can be deduced in the same way from the relation (1.4) between division polynomials. □

As an example how to apply this, I will calculate all cancellations for a point P such that $2P$ doesn't reduce to a singular point. For instance, this happens to every P which has bad reduction if E has type I_2, III, III* and I_{2n}^*. The first relation (1.8), gives

$$v(\delta_{2m}(P)) = v\left(\delta_2(P)^{m^2}\cdot\delta_m(2P)\right) = m^2\cdot v(\delta_2(P))$$

and the other equality (1.9) allow us to calculate

$$\begin{aligned} v(\delta_{2m+1}(P)) + v(\delta_{2m-1}) =& v(x(P)-x(2mP)) + 2v(e(P)) + 2v(e(2mP)) \\ & - v(e((2m+1)P)) - v(e((2m-1)P)) + 2v(\delta_{2m}(P)) \\ =& 2v(e(2mP)) + m^2\,v(\delta_2(P)), \end{aligned}$$

as P, $(2m-1)P$ and $(2m+1)P$ do not belong to the formal group at all, and since the reduction of P and $2mP$ can't be equal. By induction, this is

$$v(\delta_{2m+1}(P)) = m(m+1)\cdot v(\delta_2(P)) \qquad \text{if } 2\,k\,P\notin\widehat{E}(K) \text{ for all } 1\le k\le m.\text{'}$$

1.3.4 Cancellations in the multiplicative case

'But you still didn't show me what the cancellation is in type I_n,' roared the Wolf.

'So, in the multiplicative case,' said the intimidated Hare, 'instead of explicit blow-ups, we can do it with Tate uniformisation.[9]

Let E be an elliptic curve over a local field K of reduction type I_n an let P be a point with singular reduction. Write an Weierstrass equation for E in the form

$$y^2 + x\,y = x^3 + a_4\,x + a_6 \qquad \text{with } v(\Delta) = v(a_4) = v(a_6) = n,$$

and then E is isomorphic to the rigid analytic quotient $K^\times/q^{\mathbb{Z}}$ for a certain element q in $K^\times$ of valuation n. The x-coordinate is calculated with the series

$$x(P) = \sum_{k\in\mathbb{Z}}\frac{q^k\,u}{(1-q^k\,u)^2} - 2\sum_{k\geq 1}\frac{q^k}{(1-q^k)^2}$$

for any element $u\in K^\times$ corresponding to P. In particular, a point with singular reduction corresponds to a u of valuation $0<l<n$. The valuation of $x(P)$ can be read out of the series: If $l<\frac{n}{2}$, then the term with smallest valuation has $k=0$, so $v(x(P))=l$, but if $l>\frac{n}{2}$ then it is the previous term, that is when $k=-1$ and so $v(x(P))=n-l$. In the middle, if $l=\frac{n}{2}$ then all terms have valuation at least $\frac{n}{2}$.

Suppose $2P$ is not in the formal group. Then

$$v(\delta_2(P)) = v(f_2(P)) = \tfrac{1}{2}v(4x^3+x^2+4a_4\,x+4a_6) = \tfrac{1}{2}v(x(P)^2) = v(x(P))$$

but this mustn't be bigger than $\frac{n}{2}$ by (1.7); hence if $2P$ is not in the formal group, then

$$v(\delta_2(P)) = v(x(P)) = \min(l, n-l) \qquad \text{even for } l=\tfrac{n}{2}.$$

[9] as explained in [Silverman, 1994, chapter V].

I will show you how to find the cancellation of a point P with $l = 1$. But I want to suppose that nP which has non-singular reduction doesn't fall into the formal group. If m is smaller than $n-1$, then $v(x(P) - x(mP)) = 1$. Now to the case $m = n-1$: From the series, I can deduce

$$\begin{aligned} x(P) - x((n-1)P) &= \left(\frac{u}{(1-u)^2} + \cdots\right) - \left(\frac{q^{-1}\,u^{n-1}}{(1-q^{-1}\,u^{n-1})^2} + \cdots\right) \\ &= \left(\frac{u}{(1-u)^2} + \cdots\right) - \left(\frac{q\,u^{1-n}}{(1-q\,u^{1-n})^2} + \cdots\right) \\ &= (u + 2\,u^2 + 3u^3 + \cdots) - (q\,u^{1-n} + 2\,q^2\,u^{2-2n} + \cdots) \\ &= u(1 - q\,u^{-n}) + \cdots \end{aligned}$$

On the other hand, if nP is not in the formal group, then the valuation of

$$x(nP) = \frac{q^{-1}u^n}{(1-q^{-1}u^n)^2} + \cdots$$

must be zero, so the expression $q\,u^{-n}\,(1 - q^{-1}\,u^n) = q\,u^{-n} - 1$ must be a unit. In other words, our assumption on nP is equivalent to $v(x(P) - x((n-1)P) = 1$.

The formula (1.9) permits me to give a recursion formula for the cancellation, namely the second difference of the sequence $v(\delta_m(P))$ is one:

$$v(\delta_{m+1}(P)) - 2v(\delta_m(P)) + v(\delta_{m-1}(P)) = v(x(P) - x(mP)) = 1 \quad \text{as long as } m < n$$

as all the e's must be units and so is the difference of x-coordinates. A little calculation proves immediately that

$$v(\delta_m(P)) = \frac{m(m-1)}{2} \qquad \text{if } 0 < m \leq n \text{ and } v(x(P)) = 1$$

More generally, we would get

$$v(\delta_n(P)) = \frac{n\,l\,(n-l)}{2} \tag{1.10}$$

where u corresponds to P such that $0 < l = v(u) < n$.'

1.4 The Local Height

'Next I shall tell you about the connection with the local height function. I will keep my notation as before: R a discrete valuation ring which is complete with respect to its valuation v, then K its fraction field, $\mathbb{F}_v$ its residue field and $\mathfrak{m}$ the maximal ideal. E an elliptic curve given by an equation (Weq) over R and $\tilde{E}$ its reduction. I told you that $E^{\circ}(K)$ is the subgroup of $E(K)$ of points with non-singular reduction.'

' ... which is of finite index,' was the Hare interrupted by the Wolf.

'Indeed, as it is an open subgroup of a compact thing. This is important to know later. It fails miserably when the curve E is not an elliptic curve, but has a node or a cusp simply because the group of non-singular points is not compact any longer. Anyway, this is not what I was aiming at.

Suppose P is a non-zero point in $E^{\circ}(K)$. The expression

$$\lambda(P) = v(e(P)) + \tfrac{1}{12}v(\Delta)$$

is called the *local height* of P. It is independent of the choice of $e(P)$ and, moreover, it is independent of the equation provided P is still a point with non-singular reduction in the new coordinates. Why? Well, it is easy when the coordinate change (1.2) has a unit as its u using our little lemma 1.2. Otherwise the valuation of u shouldn't be bigger than the one of $e(P)$ if we want the image of P to have non-singular reduction. In this case the change in the two terms cancel.'

'You really love the word, don't you?' said the Wolf jokingly.

'Yes,' replied the Hare who was released by the drop of tension between them. 'I am a big fan of cancellations, they simplify things greatly. For instance, I will deduce the properties of the local height on E from my non-cancellation proposition 1.3:

Note that the function

$$\lambda\colon E^{o}(K)\setminus\{O\}\to\tfrac{1}{12}\mathbb{Z}\subset\mathbb{Q}$$

is continuous in the υ-adic topology. If t is any parameter at O, the limit $\lambda(P)-\upsilon(t(P))$ has a limit as P approaches υ-adically O. If $t=-\frac{x}{y}$ then this limit is simply $\frac{1}{12}\upsilon(\Delta)$. Next the equality called *quasi-quadraticity*:

$$\begin{aligned}\lambda(mP)&=\upsilon(e(mP))+\tfrac{1}{12}\upsilon(\Delta) && \text{if } mP\neq O\\ &=\upsilon(f_m(P)\,e(P)^{m^2})+\tfrac{1}{12}\upsilon(\Delta) && \text{by 1.3}\\ &=\upsilon(f_m(P))+m^2\,\upsilon(e(P))+\tfrac{1}{12}\upsilon(\Delta)\\ &=m^2\,\lambda(P)+\upsilon(f_m(P))-\tfrac{m^2-1}{12}\upsilon(\Delta).\text{'}\end{aligned}$$

Then he wrote down the following theorem and said that it could be found in Silverman II,[10] but where the map $x\mapsto-\log|x|_{\upsilon}$ was used rather than the valuation.

Theorem 1.5.
There exist a unique function

$$\lambda\colon E(K)\setminus\{O\}\to\mathbb{Q},$$

called the local Néron height function*, with the following three properties:*

1. *λ is continuous and bounded on the complement of any υ-adic neighbourhood of O.*
2. *The limit $\lambda(P)-\upsilon(t(P))$ as P approaches O υ-adically in $E(K)$ exists.*
3. *For any $P\in E(K)$ that is not m-torsion*

$$\lambda(mP)=m^2\,\lambda(P)+\upsilon(f_m(P))-\frac{m^2-1}{12}\upsilon(\Delta). \tag{1.11}$$

Moreover the function λ is independent of the chosen Weierstrass equation and, for every extension w of υ in a finite extension $K':K$, we have

$$\lambda_w(P)=\lambda_\upsilon(P)\cdot e_{K':K} \tag{1.12}$$

where $e_{K':K}$ denotes the ramification index of the extension.

The Hare added a few words about the proof: 'As I explained you before, the definition of λ satisfies already everything for a subgroup of finite index. Now if P is not yet in that subgroup, there is an m such that mP is. Then we simply define $\lambda(P)$ by the formula (1.11). By the way, this gives an explicit formula: From

$$\begin{aligned}m^2\,\lambda(P)&=\upsilon(e(mP))+\tfrac{1}{12}\upsilon(\Delta)-\upsilon(f_m(P))+\tfrac{m^2-1}{12}\upsilon(\Delta)\\ &=m^2\,\upsilon(e(P))-\upsilon(\delta_m(P))+\tfrac{m^2}{12}\upsilon(\Delta)\end{aligned}$$

we get

$$\lambda(P)=\upsilon(e(P))+\tfrac{1}{12}\upsilon(\Delta)-\tfrac{1}{m^2}\,\upsilon(\delta_m(P)). \tag{1.13}$$

[10] of course, the Hare was talking about [Silverman, 1994, theorem VI.4.1.].

The only thing that is not clear yet is the stated uniqueness. Suppose Λ is the difference of two such functions. The second property shows that $\Lambda(P)$ has a limit as $P \to O$. Together with the first property the function Λ must then be bounded on the whole of $E(K)$. Finally the third property tells us that $\Lambda(P) = m^{-2}\,\Lambda(mP)$ for any P that is not m-torsion. Letting $m \in \mathbb{Z}$ getting v-adically closer to 0, we must conclude that $\Lambda(P) = 0$. By continuity $\Lambda = 0$. Convinced? Even if it was a bit fast?' □

The Wolf nodded his head. 'Can you prove the *quasi-parallelogram law* just as easy as this?' he asked.

'It is not quite that easy,' answered the Hare. 'but let me prove it anyway. The statement, I recall, is'

Quasi-Parallelogram Law 1.6. *Let P and Q be two points in $E^o(K)$. The quasi-parallelogram law holds :*

$$\lambda(P+Q) + \lambda(P-Q) = 2\lambda(P) + 2\lambda(Q) + v(x(P) - x(Q)) - \tfrac{1}{6}v(\Delta) \tag{1.14}$$

'We can use the definition to rewrite the equation as

$$v\left(\frac{e(P+Q)\,e(P-Q)}{e(P)^2\,e(Q)^2}\right) = v(x(P) - x(Q)) \tag{1.15}$$

which we are going to prove now, splitting up into several cases.

First I assume that both points are in the formal group. Let's take the usual parameter $t = -\frac{x}{y}$ at O. We can profit from $v(e(P+Q)) = v(t(P+Q)) = v(t(P) + t(Q))$ to write the left hand side as

$$\begin{aligned} v\left(\frac{e(P+Q)\,e(P-Q)}{e(P)^2\,e(Q)^2}\right) &= v\left(\frac{(t(P)+t(Q))\,(t(P)-t(Q))}{t(P)^2\,t(Q)^2}\right) \\ &= v\left(\frac{1}{t(Q)^2} - \frac{1}{t(P)^2}\right). \end{aligned}$$

On the right hand side we get

$$v(x(P) - x(Q)) = v\left(\frac{1}{t(Q)^2} - \frac{1}{t(P)^2}\right) \cdot v(-1 + a_1\,t(P) + a_1\,t(Q) + \cdots),$$

using the expansion of x in t.

Now to the second case: Suppose P is not in the formal group and neither is $P+Q$ or $P-Q$. Then the left hand side in (1.15) has valuation $-2\,v(e(Q))$. If Q is in the formal group then the right hand side has the same valuation $-2\,v(e(Q))$, and if Q is not in the formal group then both sides have valuation 0 as Q is not allowed to reduce to the same point as P or $-P$, so their x-coordinates are not congruent modulo $\mathfrak{m}$.

Similarly if we swapped P and Q. So we have to deal with the last case when $S = P - Q$ is in the formal group while P is not. The case when $T = P + Q$ is in the formal group is symmetric to what we do here. It follows that Q can't be in the formal group, that is the quantities $e(P)$, $e(Q)$ and $e(P+Q)$ are units and P reduces to the same point as Q. Let me show you how we can use the case we have already treated on S an T to prove the quasi-parallelogram law in this case:

$$\begin{aligned} 2\lambda(P+Q) + 2\lambda(P-Q) =& 2\lambda(T) + 2\lambda(S) \\ =& \lambda(T+S) + \lambda(T-S) - v(x(T) - x(S)) + \tfrac{1}{6}v(\Delta) \\ =& \lambda(2P) + \lambda(2Q) - v(x(P+Q) - x(P-Q)) + \tfrac{1}{6}v(\Delta) \end{aligned}$$

Apply the quasi-quadraticity (1.11).

$$\begin{aligned} =& 4\lambda(P) + v(f_2(P)) - \tfrac{1}{4}v(\Delta) + 4\lambda(Q) + v(f_2(Q)) \\ & - \tfrac{1}{4}v(\Delta) - v(x(P+Q) - x(P-Q)) + \tfrac{1}{6}v(\Delta) \\ =& 4\lambda(P) + 4\lambda(Q) + 2v(x(P) - x(Q)) - \tfrac{1}{3}v(\Delta) \end{aligned}$$

This last equality comes from the relation

$$-f_2(P) \cdot f_2(Q) = (x(P+Q) - x(P-Q)) \cdot (x(P) - x(Q))^2$$

which you can verify by either straight forward calculation using the addition formula or as usual by comparing divisors and so on. And this concludes then the proof of 1.6.' □

The Wolf stared long at the proof of his victim. Not only did he seem to be convinced by it, he was also impressed by the Hare's ideas. He wanted to know more, but it was night and he was tired.

'What a strange and lovely story,' the Wolf said.

'What is this compared with what I shall tell you tomorrow night if you spare me and let me live. I would tell you how to construct global height starting from these local heights.'

The Wolf shared the vegetable soup with his future-feast and went to sleep not without locking the Hare in a small cell in the darkest part of his den.

Chapter 2

Global height Pairings

Early the next day, the Wolf left his den to do the usual paper work. When he came back in the evening he asked the Hare to continue his teaching.

2.1 The Ideal Class Pairing

'I promised you, master Wolf, to talk about the global heights that we can get out of the local heights of yesterday. The easier case is when we are working over a function field K. Geometrically this is the function field of a non-singular projective curve C over a field k. All places are discrete and they correspond to Galois-orbits of points on the curve C, or better to closed points of the k-scheme C. I will start to call them $\tau \in C$ instead of υ, for another reason than the pure pleasure of confusing you: Later, we will have τ's and υ's. And I'd better write the corresponding valuation as ord_τ.

Let E be an elliptic curve over K, or a birational equivalence class of elliptic surfaces[1] over C, if you prefer. Once the elliptic curve is written as a (Weq), coefficients in K, this equation will be an equation with integral coefficients in a completion K_τ at a place $\tau \in C$, unless the coefficients have poles at τ. For these finitely many places, we could choose other equations. Gluing them together gives a model of the elliptic surface over C.

I want to define a subgroup $E^o(K)$. Being as careful as a hare is, I want a point $P \in E(K)$ to be in $E^o(K)$ if it does not reduce to an eventual singularity in the reduction $\tilde{E}(\mathbb{F}_\tau)$ in every Weierstrass equation of our model which is integral at τ. Here $\mathbb{F}_\upsilon$ is the residue field of K_τ The subgroup $E^o(K)$ is of finite index[2] as there are only finitely many bad fibres.'

'Why don't you take the Néron model?' asked the Wolf puzzled.

'I could,' answered the Hare, 'only they don't have nice equations. But, if at all places the corresponding equation is minimal then the subgroup $E^o(K)$ consists of sections that are in the connected component of the minimal regular model of E.

Ok, now we can use our construction from yesterday to build functions λ_τ from $E(K)$ to $\mathbb{Q}$ for every place $\tau \in C$. They are independent of the chosen Weierstrass equation in the model. This gives us the *ideal class height*

$$\begin{aligned} q\colon E^o(K) &\longrightarrow \mathrm{Pic}_k(C)\otimes\mathbb{Q} \\ P &\longmapsto \text{class of } \sum_{\tau\in C}\lambda_\tau(P)\cdot(\tau) \end{aligned} \tag{2.1}$$

with values in the group of linear equivalence classes of k-rational divisors on C. Let me write down a first proposition:'

Proposition 2.1. *The map q is quadratic and satisfies the parallelogram law. That is*

$$q(mP) = m^2\, q(P)$$
$$q(P+Q) + q(P-Q) = 2\,q(P) + 2\,q(Q)$$

for all integers $m \neq 0$ and all P and Q in $E^o(K)$.

[1] all geometric things can be found in chapter III of [Silverman, 1994].

[2] see lemma III.9.4 in [Silverman, 1994] for the case when the model is minimal regular.

Then the Hare started to prove what he just wrote down: 'The main input for the proof is the *product formula* that holds in K:

$$\sum_{\tau\in C} \operatorname{ord}_\tau(f)\cdot(\tau) \sim 0 \in \operatorname{Pic}_k(C)$$

for all global functions $f \in K = k(C)$.'

'But that is just the definition of Pic, isn't it?'

'Indeed. I just emphasis this because later, we have more complicated product formulae. To prove the proposition quickly, I first use the quasi-quadraticity

$$q(mP) = \sum_{\tau\in C}\Bigl(m^2\lambda_\tau(P) + \operatorname{ord}_\tau(f_m(P)) - \tfrac{m^2-1}{12}\operatorname{ord}_\tau(\Delta)\Bigr)\cdot(\tau).$$

Then we can simply observe that $f_m(P)^{12}\cdot\Delta^{1-m^2}$ is an element of K as it is independent of the equation, remember (1.3). For the second part we need to sum over the quasi-parallelogram law and to see that $(x(P)-x(Q))^6\cdot\Delta$ is independent. □

In particular, there is a bilinear, symmetric pairing

$$\begin{aligned} E^{\mathrm{o}}(K)\times E^{\mathrm{o}}(K) &\longrightarrow \operatorname{Pic}_k(C)\otimes\mathbb{Q}\\ (P,Q) &\longmapsto q(P+Q)-q(P)-q(Q).\text{'}\end{aligned}$$

The Wolf, more and more interested, asked: 'This looks a bit like there the pairing of MANIN.[3] Is there a connection?'

'It is the same pairing. MANIN only defined it on a minimal model. This decomposition is also in the bi-extension-paper[4] of MAZUR and TATE. Moreover, when taking the degree, which is a map $\deg\colon \operatorname{Pic}_k(C)\to\mathbb{Z}$, we recover an other well known height:'

Proposition 2.2. *The map*

$$\begin{aligned} \hat h\colon E^{o}(K) &\longrightarrow \mathbb{Q}\\ P &\longmapsto \deg q(P)\end{aligned}$$

is quadratic and satisfies the parallelogram law. We can extend its definition to the whole group $E(K)$ independently of the considered model. Let $x\in K$ be the x-coordinate of any Weierstrass equation (Weq) *of E viewed as a map $x(P)\colon C\to\mathbb{P}^1_k$ for every $P\in E(K)$. Then the expression*

$$\hat h(P) - \tfrac12\deg(x(P))$$

is bounded for all $P\in E(K)$. In other words $\hat h$ is the canonical height[5] *of* NÉRON *and* TATE *on E.*

'Except for a finite number of places, including the places with bad fibres and those where the coefficients have poles, the local height of a point with good reduction in a model involving this equation equals

$$\lambda_\tau(P) = \operatorname{ord}_\tau(e(P)) = \tfrac12\max(-\operatorname{ord}_\tau(x(P)),0),$$

if $e(P)$ is taken with respect to the Weierstrass equation of x. For the finitely many other places, the local height differs from the right hand side by a fixed amount depending on the valuation of the discriminant or on the valuation of an u for an eventual change of equation. Hence the height $\hat h(P)$ differs from

$$\sum_{\tau\in C}\tfrac12\max(-\operatorname{ord}_\tau(x(P)),0) = \tfrac12\deg(x(P))$$

[3] see [Manin, 1964] or theorem III.9.3 in [Silverman, 1994].

[4] he talks about the paragraph 3.5.2 in [Mazur and Tate, 1983].

[5] see for example theorem III.4.3 in [Silverman, 1994].

by something that is bounded for all P.' □

'Now, master Wolf,' the Hare continued after a sip of "Mike's marvellous chocolate-coffee, 'we can define in a similar manner a canonical height[6] on elliptic curve E over a number field K with values in the class group C_K of K. Here we make things integral. Let P be a point in $E^{\circ}(K)$, the subgroup of $E(K)$ of points lying in $E^{\circ}(K_v)$ for all finite places v. Define a map

$$\begin{aligned}[\hat{h}]\colon E^{\circ}(K) &\longrightarrow C_K\\ P &\longmapsto \text{class of} \prod_{\text{finite } v} \mathfrak{p}_v^{12\lambda_v(P)}\end{aligned}$$

where $\mathfrak{p}_v$ is the prime ideal corresponding to the place v. Similarly as before, it satisfies the parallelogram law and it is quadratic. But we don't gain much information from it as C_K is a finite group. Actually $[\hat{h}](P)$ is the class of $\mathfrak{e}(P)^{12}$ where $\mathfrak{e}(P)^2$ is the denominator ideal of the fractional ideal $(x(P))$.'

2.2 The Sigma Functions

'Indeed.' commented the Wolf. 'I guess we have to include the infinite places.'

'True. We need to include the archimedian places. So I will work with $\mathbb{I}_K$, the idèles of the number field K. Let ρ be a continuous group-homomorphism from $\mathbb{I}_K$ to a uniquely divisible thing; actually we will only be interested in $\mathbb{R}$ or $\mathbb{Q}_p$. Our ρ's will contain $K^{\times}$ in its kernel.

2.2.1 The Complex Sigma Function

As a first example we take the map[7]

$$\begin{aligned}\rho\colon \mathbb{I}_K &\longrightarrow \mathbb{R}\\ \mathbf{c} = (c_v)_v &\longmapsto \sum_{\text{finite } v} v(c_v)\cdot\log(q_v) - \sum_{\text{infinite } v} n_v \cdot \log|i_v(c_v)|\end{aligned}$$

where q_v is the number of elements in the residue field $\mathbb{F}_v$ at the finite places v and i_v is an embedding $K \to \mathbb{C}$ corresponding to the infinite places v. Moreover n_v means always the local degree $K_v : \mathbb{Q}_v$. Do you see why $K^{\times}$ is in the kernel?"

'Honestly, your notation doesn't help to see that, but I suppose that it is the usual product formula, isn't it?'

'You are right. In fact, it is usually written as the negative logarithm of the content of the idèle, that is

$$\rho(\mathbf{c}) = -\sum_v n_v \cdot \log|c_v|_v$$

for all places and then $\prod_v |c|_v^{n_v} = 1$ for an element in $c \in K^{\times}$ will prove it.

Let us take a point P in $E^{\circ}(K)$, now. I define an idèle $\mathbf{i}(P) = (i_v(P))_v$ using the local height functions on P: I want to impose that $v(i_v(P)) = 12\,\lambda_v(P) \in \mathbb{Z}_{\geq 0}$ for finite places v. Then the natural thing is to put

$$\hat{h}_\infty(P) = \frac{1}{12\cdot[K:\mathbb{Q}]}\cdot\rho(\mathbf{i}(P)). \tag{2.2}$$

[6] according to 3.5.2 to [Mazur and Tate, 1983] this has been studied by Duncan Buell.

[7] one could also work with Arakelov divisors instead. They are elements of

$$\bigoplus_{\text{finite } v} \mathbb{Z}\log(q_v)\cdot(v) \oplus \bigoplus_{\text{infinite } v} \mathbb{R}\cdot(v).$$

The map ρ is then simply the degree map as described in paragraph 2.6 of [Lang, 1983].

The only little problem is that we don't have a local height at infinite places, yet. If we want $\hat{h}$ to satisfy the usual two things, the $\lambda_v\colon E(K_v) \longrightarrow K_v$ must have certain properties, namely exactly the statements 1., 2. and 3. in theorem 1.5 with v replaced by the map $x \mapsto -\log|i_v(x)|$. The proof that there is not more than one such function can just be copied from what I showed you for finite places. Whereas to the existence: there is indeed such a function; it is linked to the complex σ-function.[8] But I don't want to go into details for I prefer working only with the p-adic version of it, but of course the resulting height is nothing else than the usual canonical Néron-Tate height.'

2.2.2 The p-adic Sigma Function

'Let me explain you the p-adic construction, now,' said the Hare. 'Fix a prime p. Here we start with a non-trivial continuous homomorphism ρ from $\mathbb{I}_K$ to the p-adic numbers for some prime p. Multiplying somewhat maybe, we can assume that the image is in $\mathbb{Z}_p$. From a look on the topology of $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}_p$, we see that the archimedian part of ρ, I mean the maps ρ_v, when v is infinite, must be zero.

How do we get such a map ρ? Well, we could start with a continuous representation ρ_G from the absolute Galois-group of our number field K into $\mathbb{Z}_p$, then the reciprocity map induces us a ρ. Such a ρ_G cuts out a $\mathbb{Z}_p$-extensions of K.'

The Hare saw the question mark on face of the Wolf. So he added: 'The kernel of ρ_G is the Galois-group of some extension K_∞ of K with Galois-group embedding into $\mathbb{Z}_p$.

Anyway, I will only concentrate on one such $\mathbb{Z}_p$-extension, the cyclotomic one. I just wanted to let you know that there exists[9] other p-adic heights, at least when K is larger than $\mathbb{Q}$.

In the cyclotomic case, the map is nothing else than the p-adic version of the real valued one:

$$\begin{aligned}\rho\colon \mathbb{I}_K &\longrightarrow \mathbb{Z}_p\\ \mathbf{c}=(c_v)_v &\longmapsto \sum_{\text{finite } v\nmid p} v(c_v)\cdot\log_p(q_v) - \sum_{v\mid p}\log_p(\mathrm{N}_{K_v:\mathbb{Q}_p}(c_v)),\end{aligned}$$

here I took the p-adic logarithm extended to all $\mathbb{Q}_p^\times$ by setting[10] $\log_p(p)=0$.'

'And you think that $K^\times$ is in the kernel of this ρ?' doubted the Wolf.

'Oh yes, I do think so. Again we could have written[11]

$$\rho(\mathbf{c}) = -\sum_{\text{finite } v\nmid p} \log_p|\mathrm{N}_{K_v:\mathbb{Q}_\ell}(c_v)|_\ell - \sum_{v\mid p}\log_p(\mathrm{N}_{K_v:\mathbb{Q}_p}(c_v)).$$

For $K=\mathbb{Q}$, it follows from the fact that $-\sum_{\ell\neq p}\log_p|c|_\ell = \log_p(|c|_\infty) = \log_p(c)$ for all $c\in\mathbb{Q}^\times$ as $\log_p(p) = \log_p(-1) = 0$. For an arbitrary number field K, we can reduce the calculation to the previous one if we use that $\prod_{v\mid\ell}\mathrm{N}_{K_v:\mathbb{Q}_\ell}(c) = \mathrm{N}_{K:\mathbb{Q}}(c)$ for all $c\in K^\times$. Do you agree?'

'Yesyes.'

'Moreover the image of the local units $R_v^\times$ into $\mathbb{I}_K$ is also in the kernel of ρ whenever v is a finite place not dividing p.

Let me go back to an elliptic curve E over our number field K as always given by a (Weq). I create a idèle $\mathbf{i}(P)$ for a point $P\in E^\circ(K)$ by letting

$$i_v(P) = \begin{cases} 1 & \text{if } v \text{ is infinite}\\ \text{has valuation } 12\lambda_v(P) & \text{if } v \text{ is finite not dividing } p\\ \sigma_v^{12}\cdot\Delta & \text{if } v \text{ divides } p\end{cases} \tag{2.3}$$

[8] see theorem VI.3.2 or theorem VI.1.1 of [Silverman, 1994].

[9] the Hare didn't mention that there are some extra conditions on the $\mathbb{Z}_p$-extension, namely the elliptic curve has to be ordinary at all places where the extension is ramified. For more details see paragraph 4 in [Mazur and Tate, 1983].

[10] the choice of the branch shouldn't matter in the end.

[11] which is, except for the sign, exactly the way this map is defined in the first paragraph of [Schneider, 1982b].

Then we are defining the *p-adic height* of P to be

$$\hat{h}_p(P) = \frac{1}{12}\rho(\mathbf{i}(P)) \in \tfrac{1}{12}\mathbb{Z}_p.\text{'} \tag{2.4}$$

'Stopstop!' shouted the Wolf. 'You hared a bit too fast for me. What is σ_v? Why don't you divide by the global degree?'

'I am sorry,' said the Hare kindly. 'I could divide by $[K:\mathbb{Q}]$, but it seems to me that one usually doesn't bother about the compatibility with extensions.

Now to the v-adic sigma function σ_v. Let us look for properties that this function should satisfy. We want the height to be quadratic, so $\sigma_v : E^\circ(K_v) \to K_v$ should be such that

$$\sigma_v(mP) = \sigma_v(P)^{m^2} \cdot f_m(P), \tag{2.5}$$

because of the following calculations, keeping in mind the quasi-quadraticity (1.11) at the finite places:

$$(\sigma_v(mP))^{12} \cdot \Delta = (\sigma_v(P)^{12}\,\Delta)^{m^2} \cdot f_m(P)^{12} \cdot \Delta^{1-m^2}$$

and so the idèle $\mathbf{i}(mP)$ differs from the idèle $\mathbf{i}(P)^{m^2} \cdot f_m(P)^{12} \cdot \Delta^{1-m^2}$ only by units at the places not dividing p, in particular they have the same image under ρ.

$$\begin{aligned} \hat{h}_p(mP) &= \tfrac{1}{12}\,\rho(\mathbf{i}(mP)) \\ &= \tfrac{1}{12}\,\rho\left(\mathbf{i}(P)^{m^2} \cdot f_m(P)^{12} \cdot \Delta^{1-m^2}\right) \\ &= \tfrac{m^2}{12}\,\rho(\mathbf{i}(P)) \\ &= m^2\,\hat{h}_p(P) \end{aligned}$$

Furthermore, I am sure you would agree that we should try to guarantee the parallelogram law, as well. Here we must ask σ_v to satisfy

$$\frac{\sigma_v(P+Q)\,\sigma_v(P-Q)}{\sigma_v(P)^2\,\sigma_v(Q)^2} = x(Q) - x(P).\text{'} \tag{2.6}$$

' ... and you think σ_v will be so kind? At least, the formulae (2.5) and (2.6) are true for the complex sigma function, so we could hope to use a similar construction. Tell me now, does it exist?'

'Yes, master Wolf,' announced the Hare proudly.[12] 'Only the uniqueness causes problems. As usual $t = -\frac{x}{y}$ is a my favourite parameter of the formal group $\widehat{E}$ of our (Weq). Remember v is a place above p. Let $\mathscr{L}_v \colon \widehat{E}(\mathfrak{m}_v) \to K_v$ be the logarithm of the formal group and Φ its inverse. Write the *Weierstrass $\wp$-function* in terms of a parameter $z = \mathscr{L}_v(t)$ of the additive group:

$$\wp(z) = x(\Phi(z)) + \frac{a_1^2 + 4\,a_2}{12} = \frac{1}{z^2} + d_2\,z^2 + d_3\,z^4 + d_4\,z^6 + \cdots$$

The coefficients, by the way, are quite complicated expressions in $\mathbb{Q}[a_1, a_2, a_3, a_4, a_6]$ like

$$d_2 = \frac{a_1^4 + 8\,a_1^2 a_2 + 16\,a_2^2 - 24\,a_1 a_3 - 48\,a_4}{240}$$

Formally integrating twice the "holomorphic" part and taking the formal exponential map on minus the result, we get a series

$$z \cdot \exp\left(-\frac{d_2}{3\cdot 4}\,z^4 - \frac{d_4}{5\cdot 6}z^6 - \cdots\right) \in K_v[\![z]\!]$$

[12] the Hare has simply copied [Bernardi, 1981], see also the lecture 2 of[Coates, 1991].

The *Bernardi sigma-function* $\sigma_v^{(0)}(P)$ evaluated on a point P is obtained by evaluating the above series on $z(P) = \mathscr{L}(t(P))$. This looks like[13]

$$\sigma_v^{(0)}(P) = t(P) + \frac{a_1}{2}\,t(P)^2 + \frac{a_1^2 + a_2}{3}\,t(P)^3 + \cdots \quad \in K_v[\![t(P)]\!] \tag{2.7}$$

But this probably only converges as good as the exponential map does, namely if $v(t(P)) > \frac{v(p)}{p-1}$.

The series $\sigma_v^{(0)}(t)$ will fulfil our requirement to satisfy the relations (2.5) and (2.6), since as a formal power series in z it satisfies the same properties as the complex sigma-function. But unfortunately it is not the only such function, any other can be obtained[14] from this by multiplying it with an exponential factor

$$\sigma_v^{(\alpha)}(P) = \exp\left(\alpha \cdot z(P)^2\right) \cdot \sigma_v^{(0)}(P) \tag{2.8}$$

$$= t(P) + \frac{a_1}{2}\,t(P)^2 + \left(\frac{a_1^2 + a_2}{3} + \alpha\right)\,t(P)^3 + \left(\frac{a_1^3 + 2\,a_1 a_2 + 3\,a_3}{4} + \frac{3\,a_1}{2}\alpha\right)\,t(P)^4 + \cdots \tag{2.9}$$

with α in K_v.

But the good news is, that among all these sigma functions, there is an even better choice than the Bernardi sigma-function … ' told the Hare to the Wolf and waited for his reply. But the Wolf, once an angry beast, looked now absent-minded and mumbled that he had to think about it, calculate maybe some examples. The Hare said: 'I shall show you some tomorrow, if you, dear master Wolf, spare me and let me live.'

They wolfed down the supper and the Wolf locked the Hare away and went to bed.

The day after, a rainy autumn day, the Wolf did all the things a Wolf has to do in a Wolf's day and came back home in the late afternoon, gave paper and pen to the Hare who continued where had stopped the day before:

'You might have heard, dear master Wolf, that Mazur and Tate found a *canonical sigma function*. I am writing down a part of the main theorem in their paper[15] about it:'

Theorem 2.3.
Let p be an odd prime. Given an elliptic curve E given by a fixed (Weq) *over a field K_v complete with respect to a discrete valuation v with residue characteristic p. Suppose E has* good ordinary *reduction.*

There is a unique sigma-function $\sigma_v(t)$ in $t \cdot (1 + t\,R_v[\![t]\!])$ satisfying (2.5) *for all $m \neq 0$ and $P \in \widehat{E}(\mathfrak{m}_v)$. It is also satisfies* (2.6) *for all P and Q in $\widehat{E}(\mathfrak{m}_v)$.*

'From the stated uniqueness,' added the Hare, 'it is not difficult to see that $\sigma_v^{12} \cdot \Delta$ is independent of the equation. For P in the subgroup

$$E^p(K) = E^0(K) \cap \bigcap_{v|p} \widehat{E}(K_v) \subset E(K) \tag{2.10}$$

of finite index, it makes sense to define the idèle $\mathbf{i}(P)$ by (2.3) using the canonical sigma-function. This is now independent of the equation and the calculations after (2.5) together with the consequences of (2.6) gives rise to an *idèle pairing*[16]

$$\begin{aligned} E^p(K) \times E^p(K) &\longrightarrow {}_{K^\times}\backslash^{\mathbb{I}_K}/_{\prod_{v\nmid p} R_v^\times \cdot \prod_{v|\infty} K_v^\times} \\ (P,Q) &\longmapsto \mathbf{i}(P+Q)\,\mathbf{i}(P)^{-1}\,\mathbf{i}(Q)^{-1} \end{aligned}$$

[13] see [Perrin-Riou, 1983].

[14] proven for instance in [Perrin-Riou, 1984] in paragraph 2.

[15] see theorem 3.1 in [Mazur and Tate, 1991].

[16] explained in paragraph II.4 of [Mazur et al., 1986].

which is bilinear and symmetric, but its value group is something that I wouldn't like to write down twice. Thanks to our map ρ we can define,[17] as in (2.4), the *canonical p-adic height*[18] as

$$\begin{aligned} \hat{h}_p \colon E^p(K) &\longrightarrow \mathbb{Q}_p \\ P &\longmapsto \tfrac{1}{12}\rho(\mathbf{i}(P)) \end{aligned}$$

taking values in $\frac{p}{12}\mathbb{Z}_p$. It is wonderfully quadratic and parallelogrammic, so its definition can be extended beyond the subgroup of finite index to the whole of $E(K)$. There is a corresponding bilinear and symmetric pairing, called the *p-adic height pairing*,

$$\begin{aligned} \langle\cdot,\cdot\rangle_p \colon E(K) \times E(K) &\longrightarrow \mathbb{Q}_p \\ (P,Q) &\longmapsto \langle P,Q\rangle_p = \hat{h}_p(P+Q) - \hat{h}_p(P) - \hat{h}_p(Q) \end{aligned}$$

For any given set of points $P_i \in E(K)$, the quantity

$$\det(\langle P_i, P_j\rangle_p) \in \mathbb{Q}_p$$

could be called the *p-adic regulator* of the set. If it were a set of generators of the Mordell-Weil group $E(K)$ we could called it the *p-adic regulator of E*.

Just as the usual elliptic regulator is expected to appear in the Birch–Swinnerton-Dyer–formula, the p-adic regulator should appear in the p-adic version of the Birch–Swinnerton-Dyer–formula,[19] unless the whole universe collapses down.'

'May the sylvan spirit beware us,' commented the wolf.

'I would even pray for less. Namely, for that the p-adic regulator is non-zero, or even weaker, that the p-adic height $\hat{h}_p(P)$ of a non-torsion point P is never zero. But this is an old question and ...'

'Please, tell me more about it.'

2.3 The Story of p-adic Heights

So the Hare started to tell the story of p-adic heights.

'The first appearance of p-adic height and the question if they are non-degenerate goes back to Néron, if I am not mistaken. He constructed a pairing between abelian varieties with values in $\mathbb{Q}_p$ using his symbols. He wrote[20]

> [...] on sait que $\gamma_{X,\infty}$ est non-dégénéré lorsque le diviseur X est lui-même non dégénéré et que, par suite, δ_∞ met en dualité les deux groupes $\hat{A}(K)$ et $A(K)$. Il serait très intéressant de déterminer si les mêmes proporiétés ont lieu pour les accouplements $\gamma_{X,p}$ et δ_p qui correspondent aux valeurs absolues p-adiques.

But we have to wait until the beginning of the 80ies, before p-adic heights got fashionable. On the basis of a never-published idea of Abramov and Rosenblum on the subject of a pairing modulo p, Bernardi presented his p-adic height. His problem was that he found all the sigma-functions as above and he didn't know which one to choose unless the curve had complex multiplication. In this case one can take an α related to the second Eisenstein series which turns out to be an algebraic thing. But he couldn't answer if the pairing is non-degenerated. He wrote[21]

> Néron pose alors, sans répondre, le problème crucial qui reste en supense dans toute cette étude : la forme bilinéaire ainsi construite est-elle non dégénérée? S'il est facile de le vérifier pour $E(K)$ dans quelques cas particuliers, la non-dégénérence sur $E(\bar{K})$ pour toute E et tout p, si elle est vraisemblamble, est probablement assez profondément cachée.

[17] for other $\mathbb{Z}_p$-extensions, i.e. other ρ the definitions are the the same, so strictly speaking we should write $\hat{h}_p^{(\rho)}$.

[18] the Hare is not careful enough here. If $p = 2$, the σ_v-function doesn't exist, but it square does and so the definition of the height still makes sense, see the remark after theorem 3.1 in [Mazur and Tate, 1991].

[19] of course, the reference here is [Mazur et al., 1986].

[20] see seventh paragraph of [Néron, 1976].

[21] see the end of [Bernardi, 1981].

A fundamental article[22] of BLOCH, where he redefined the canonical Néron-Tate height using a splitting of group-extensions, lead to the definition of a canonical p-adic height in a Galois cohomological context. This was done by PERRIN-RIOU[23] in the case of complex multiplication. and in general by SCHNEIDER.[24] SCHNEIDER asks the question of the non-degeneracy of his canonical height.[25] Both used the so obtained p-adic regulator, to prove a Birch–Swinnerton-Dyer-like formula for the p-adic L-function coming from Iwasawa theory, but, of course, only under the assumption that it was non-zero. While in the case of complex multiplication, it turned out that this height was the canonical choice of BERNARDI using Eisenstein series,[26] it was not clear at first what the corresponding sigma-function in the other case could look like; until MAZUR and TATE gave their construction of the canonical p-adic height using bi-extensions.[27] It is the same as the canonical pairing found by SCHNEIDER. This article gave rise to another one, about the p-adic sigma function[28] in the case of an elliptic curve and to a precise formulation of the p-adic analogue of the Birch–Swinnerton-Dyer-formula.[29] There is a good overview in an article[30] of the link between the different p-adic height, written by PERRIN-RIOU. She shows that the original pairing of NÉRON is nothing else than the one obtained by BERNARDI and she gives a relation to a naive height.[31]'

'Maybe I should quickly say what the cohomological interpretation looks like. Instead of constructing the pairing on the group $E(K)$ only, one can extend it to the Selmer group $\mathfrak{S}(E/K)$ which contains the group $E(K)\otimes\mathbb{Z}_p$ in it. They are equal if the the p-primary part of the Tate-Shavarevich-group $\text{Ш}(E/K)$ is finite. The kernel of the pairing will contain the "universal norms", that is the intersection of the images of the norm maps when climbing up the cyclotomic $\mathbb{Z}_p$-extension K_∞ above K. The non-degeneracy of the pairing can then be expressed as an isomorhpism between a subgroup of $\mathfrak{S}(E/K)$ and the $\mathrm{Gal}(K_\infty : K)$-invariant part of the Pontryagin dual of the other Selmer group $S_p(E/K_\infty)$'

'You are going to tell me that there is nothing known about this conjecture?' interfered the Wolf in the story of the Hare.

'Almost,' answered this one, 'there is one little result. BERTRAND and his transcendental methods produces a proof that the p-adic height of a point of infinite order on a curve with complex multiplication defined over the field $\mathbb{Q}$ can never be zero.[32] It should also be true for quadratic imaginary fields if p splits. But that is all there is known. We could expressed it in the words of WALDSCHMIDT when he was asked the question if the non-vanishing of the p-adic regulator was still unknown: "Malheureusement non, c'est bien triste." '

The Wolf was astonished and so the Hare asked: 'Would you give me back my freedom, if I showed you a proof of it?' But the Wolf didn't listen.

'In the function field case,' told the Hare to the Wolf, 'PAPANIKOLAS[33] found some hypothesis that implies that the p-adic height is non-degenerate. But that's is really all there is. Once I show you how to actually calculate these things you might see why it is a difficult problem.'

2.4 Calculations of p-adic Heights

'Let me first rewrite the definition of the p-adic height a little bit. I will use the symbol $\mathbf{N}(\mathfrak{b})$ for the positive generator of the norm $\mathrm{N}_{K:\mathbb{Q}}(\mathfrak{b})$ of an ideal $\mathfrak{b}$, in particular $\mathbf{N}(\mathfrak{p}_v) = q_v$ for the prime

[22] see [Bloch, 1980], better explained in [Oesterlé, 1982] and in chapter 11.6 of [Lang, 1983].

[23] see [Perrin-Riou, 1982/83] and [Perrin-Riou, 1982].

[24] as in [Schneider, 1982b], [Schneider, 1985] and less formal in [Schneider, 1982a].

[25] paragraph 3 in[Schneider, 1982b].

[26] see théorème 4.1 in [Perrin-Riou, 1982/83].

[27] this is the article [Mazur and Tate, 1983]; MUMFORD's explanations in [Mumford, 1969] could be helpful to avoid the frustration caused by "bi-extensions of toric completions in the category of formal group schemes".

[28] [Mazur and Tate, 1991], of course.

[29] see [Mazur et al., 1986].

[30] that's [Perrin-Riou, 1984].

[31] see also [Perrin-Riou, 1983].

[32] corrolaire 4 in [Bertrand, 1982].

[33] in an article [Papanikolas, 2000] following his thesis.

ideal corresponding to a finite place v. Suppose P is a point in the subgroup $E^p(K)$, we can use the explicit formula for the local height $12\lambda_v(P) = 12v(e_v(P)) + v(\Delta)$, using the definition of e_v over the completion R_v, and we then have

$$\begin{aligned}\hat{h}_p(P) &= \tfrac{1}{12}\rho(\mathbf{i}(P)\cdot\Delta^{-1}) \\ &= \sum_{\text{finite } v} v(e_v(P))\, \log_p(q_v) - \tfrac{1}{2}\sum_{v|p}\log_p(\mathrm{N}_{K_v:\mathbb{Q}_p}(\sigma_v^2(P))) \\ &= \log_p(\mathbf{N}(\mathfrak{e}(P))) - \tfrac{1}{2}\sum_{v|p}\log_p(\mathrm{N}_{K_v:\mathbb{Q}_p}(\sigma_v^2(P))) \qquad (2.11)\end{aligned}$$

and in the case of $K = \mathbb{Q}$ and $p \neq 2$, it can written even shorter

$$\hat{h}_p(P) = \log_p(e(P)) - \log_p(\sigma_p(P)) = \log_p\left(\frac{e(P)}{\sigma_p(P)}\right)$$

How do we actually calculate[34] the height? I didn't even show you the construction of the p-adic sigma function, yet. But we can actually determine its value by using the Bernardi sigma-function. Suppose that v doesn't lie above 2. Since the canonical p-adic sigma function satisfies the two crucial equalities (2.5) and (2.6), there must be a α as in (2.8), in the special case here we will call it $-\frac{1}{2}s_{2,v}$,[35] such that

$$\sigma_v(P) = \exp\left(-\tfrac{1}{2}s_{2,v}\cdot z(P)^2\right)\cdot\sigma_v^{(0)}(P).$$

The $s_{2,v}$ must be the unique element of K_v such that the series

$$\sigma_v(P) = t(P) + \frac{a_1}{2}t(P)^2 + \left(\frac{a_1^2 + a_2}{3} - \frac{s_{2,v}}{2}\right)t(P)^3 + \left(\frac{a_1^3 + 2\,a_1a_2 + 3\,a_3}{4} + \frac{3\,a_1}{4}s_{2,v}\right)t(P)^4 + \cdots$$

lies in $R_v[\![t(P)]\!]$. So we write down the first coefficients and that the fact that they should be integral, give us congruence relations for $s_{2,v}$. It is worth knowing that $s_{2,v}$ lies in $\frac{1}{3}R_v$. Calculating more and more coefficients, we are able to find an v-adic approximation of $s_{2,v}$. If we know it with an error of valuation bigger than k, then we have also an approximation of $\sigma_v(P)$ up to an error of valuation $k + 3v(t(P))$. Maybe I should give an example here.'

'Oh yes, please!' said enthusiastically the Wolf.

2.4.1 An Example

'Let

$$E_{37A}\colon\quad y^2 + y = x^3 - x \qquad (2.12)$$

a curve over $\mathbb{Z}$ with conductor 37. It is actually the smallest conductor such that the curve has a point of infinite order, namely $P = (0,0)$ is a generator of $E_{37A}(\mathbb{Q})$. Let's calculate the 5-adic height of P. Write $a = -\frac{3}{2}s_{2,(5)}$ which must lie in $\mathbb{Z}_5$. The series in t for the canonical sigma-function is

$$\sigma_5(t) = t + \frac{a}{3}t^3 + \frac{1}{2}t^4 + \frac{2a^2 - 15}{36}t^5 + \frac{a}{2}t^6 + \frac{20\,a^3 - 1314\,a + 2781}{3240}t^7 + \cdots$$

and if this last written coefficient is in $\mathbb{Z}_5$, then we should better have $a + 1 \equiv 0 \pmod{5\mathbb{Z}_5}$. So I write $a = 4 + 5b$ and I rewrite the series above. This time the first coefficient having a denominator divisible by 5 is the one for t^{11}, namely

$$\frac{87500\,b^5 + 350000\,b^4 - 1214500\,b^3 + 3885550\,b^2 + 12524473\,b + 2247727}{816480}.$$

[34] the method explained here is also suggested in paragraph II.2., bottom of page 29, of [Mazur et al., 1986].

[35] the reason for this is that this object is actually a p-adic Eisenstein series. This is explained in [Mazur and Tate, 1991].

Here we conclude that $b \equiv 1$ modulo 5. And so on. After one more step, we have an approximation

$$a = 4 + 1 \cdot 5 + 1 \cdot 5^2 + \mathbf{O}(5^3).$$

Plugging this in the series for σ_5 gives

$$\sigma_5(t) = t + (3 + 2 \cdot 5^2 + \mathbf{O}(5^3))\, t^3 + (3 + 2 \cdot 5 + \mathbf{O}(5^2))\, t^4 + (2 + \mathbf{O}(5))\, t^5 + \mathbf{O}(5^{3+3v(t)}).$$

In order to calculate the 5-adic height of $P = (0,0)$, we have to multiply it first into the 5-adic formal group and check that the point has good reduction everywhere. As the product of the Tamagawa factor is 1, no point actually could ever reduce to a singular point. Now $8P = (\frac{21}{25}, \frac{-69}{125})$ is the first multiple lying in the formal group. We find

$$\hat{h}_5(8P) = 2 \cdot 5 + 3 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + \mathbf{O}(5^5)$$

and so

$$\hat{h}_5(P) = 3 \cdot 5 + 0 \cdot 5^2 + 3 \cdot 5^3 + 2 \cdot 5^4 + \mathbf{O}(5^5).\text{'}$$

2.4.2 The First Digit

The Hare said that he would continue with another very explicit calculation.[36]

'Let P be a point in $E^p(K)$ for some elliptic curve over a number field K. Since the unknown $s_{2,v}$ doesn't appear in the first terms of the series of the v-adic sigma-function, we can hope to find an approximation of the p-adic height. Note that the p-adic logarithm takes values in $p\mathbb{Z}_p$. I will be able to give a formula for the first digit of the p-adic height, that is to determine $\hat{h}_p(P)$ modulo p^2.

Assume $p \neq 2$. Just as we took the discriminant out of the formula (2.11), we can put the expression $x(P)$ into it:

$$\begin{aligned}\hat{h}_p(P) &= \tfrac{1}{24}\rho\left(\mathbf{i}(P)^2 \cdot x(P)\right) \\ &= \tfrac{1}{2}\log_p(\mathbf{N}(\mathfrak{e}(P)^2 \cdot (x(P)))) - \tfrac{1}{2}\sum_{v|p}\log_p(\mathrm{N}_{K_v:\mathbb{Q}_p}(\sigma_v(P)^2 \cdot x(P)))\end{aligned} \tag{2.13}$$

Remembering the definition of $\mathfrak{e}$, we see that $\mathfrak{e}(P)^2 \cdot (x(P))$ is exactly the numerator ideal $\mathfrak{a}(P)$ of the fractional ideal $(x(P))$. Furthermore the series in $t(P)$ of the thing in the second expression looks like

$$\sigma_v(P)^2 \cdot x(P) = 1 + \left(\frac{a_1^2 + 4a_2}{12} + s_{2,v}\right) t(P)^2 + \left(\frac{a_1^3 + 4\,a_1a_2}{12} + a_1\, s_{2,v}\right) t(P)^3 + \mathbf{O}(t(P)^4).$$

In particular, if the extensions $K_v : \mathbb{Q}_p$ are unramified for all $v \mid p$, then its norm in $\mathbb{Q}_p$ will lie in the $1 + p^2\,\mathbb{Z}_p$ and so second term in the formula (2.13) will be in $p^2\mathbb{Z}_p$. So in this case, we have the approximation

$$\begin{aligned}\hat{h}_p(P) &\equiv \tfrac{1}{2}\log_p(\mathbf{N}\,\mathfrak{a}(P)) \pmod{p^2} \\ &\equiv \frac{\mathbf{N}(\mathfrak{a}(P))^{p-1} - 1}{2\,(p-1)} \pmod{p^2}\end{aligned}$$

So we have a first simple condition here: For any point $P \in E^p(K)$,

$$\hat{h}_p(P) \equiv 0 \pmod{p^2} \text{ if and only if } \mathbf{N}(\mathfrak{a}(P))^{p-1} \equiv 1 \pmod{p^2}.$$

In the interesting case of $K = \mathbb{Q}$, one could just write $\log_p(a(P))$ and $a(P)^{p-1} \equiv 1$ in the last line. This is a very good criterion to check if the p-adic height has valuation 1. It is not a big

[36] such as they can found in [Perrin-Riou, 1983].

surprise that this happens in most cases. But unfortunately it is not always that easy to decide if the p-adic height is non-zero. For the curve E_{37A}, there are only 3 odd primes below 1000 for which the criterion doesn't answer the question.[37]'

After that the Wolf promised the Hare that he would let him live for another day, they both went to sleep, the Wolf in his comfortable bed and the Hare in the dark, dark prison.

[37] see the tables in B.

Chapter 3

Height Functions in Forests

When the Wolf came back in the afternoon from his daily round through the forest, he was in a good humour; maybe it was because the sun was shining or because he had visited his Lady-Wolf. He chained the Hare's paw to his arm and he asked the Hare to teach him more on a walk along the edge of the forest. The Hare was happy to leave the dark den for a while.

3.1 Elliptic Forests

'I will tell you, master Wolf,' said the Hare, once they were outside, 'about an unfamiliar concept. It might be that there is a better way of formulating all of this, but until now I didn't find anything. Let K be the fraction field of a Dedekind ring R of characteristic 0. In a first approach, the notion of *elliptic forest* will design a scheme $\mathcal{E}$ given by a Weierstrass equation (Weq) with coefficients that are polynomials in $R[\tau]$ and whose discriminant $\Delta \in R[\tau]$ is not zero. This would be a scheme with a morphism π to the affine line $\mathbb{A}^1_R$ over R. When considering the equation over $K[\tau]$, we are looking at the elliptic curve[1]

$$\mathcal{E}_K = \mathcal{E} \times_R \operatorname{Spec} K \quad \text{ over } \mathbb{A}^1_K.\text{'}$$

'Oh, you know that I love Speck,' said the Wolf.

'I will call this elliptic curve over $\mathbb{A}^1_K$ the *lisière*[2] *of the forest*,' continued the Hare, trying to ignore the remark that made him feel less comfortable on this evening walk. 'The fibres of π should be seen as *fir trees*. Finally the base $\mathbb{A}^1_R$ could be called *soil*.'

'You are introducing now the whole vocabulary of forestry, like Hironaka[3] did?'

'Don't worry, its the vocabulary of the forest animals. You should think of the lisière as a family of curves $\mathcal{E}_\tau$ defined over R parametrised by τ in R. Almost all of them are elliptic curves over R, but some might have a node or a cusp, namely when the discriminant has a zero at the corresponding τ. This is the first tree, the one visible from the outside, but behind it, inside the forest, there are planted its reduction at different primes v. So walking perpendicularly into the forest, we see a picture of an arithmetic scheme.'

The Hare was drawing the picture for the Wolf shown in the figure on top of the next page.

'The difference with the scheme $\mathcal{E}$ is that I would like to better distinguish the reductions. If we replace τ in the equation of $\mathcal{E}$ by a value $\tau \in R$ or if we replace it by $\tau + r$ where r is an element in the prime ideal $\mathfrak{p}_v$ associated to v, the reduction $\mathcal{E}_{\tau,v}$ at the prime v has the same equation as the reduction $\mathcal{E}_{\tau+r,v}$. In the scheme-theoretic setting this is the same fibre. But I wish to analyse them separately, you will see why, and that is why I plant copies of the reduction in the line of trees behind every $\mathcal{E}_\tau$ having this curve as a reduction.

The lisière $\mathcal{E}_K$ is an elliptic curve over a principal ideal domain $K[\tau]$. Its generic fibre is an elliptic curve over the field $K(\tau)$, its Mordell-Weil group will be denoted by $\mathcal{E}_K(K)$ whose elements will be called *sections of $\mathcal{E}$* for short. Since $\mathcal{E}_K$ is an elliptic curve over a function field, there is a well-defined subgroup $\mathcal{E}^0_K(K)$ of finite index of sections not passing through any singularity for $\tau \in \overline{K}$, the algebraic closure of K.

Do you remember the definitions I gave you in the very beginning? Since $K[\tau]$ is principal we can define for every section $P \in \mathcal{E}_K(K)$ the polynomials $a(P)$, $b(P)$ and $e(P)$ in $K[\tau]$. As we can

[1] maybe the term 'degenerated elliptic curve' would be more precise.

[2] sounds so much better than "edge of the forest".

[3] the Wolf thought of [Hironaka, 1972].

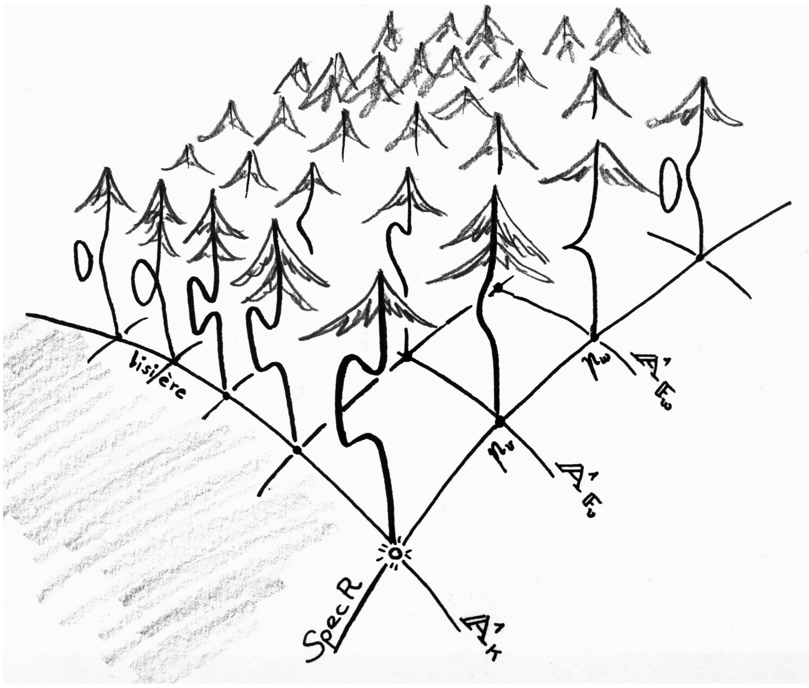

Figure 3.1: A picture of a forest

multiply by units in $K[\tau]$, we can even guarantee that they are polynomials over $R[\tau]$, defined up to units in $K^\times$.

Let P be a section of $\mathcal{E}(K)$. The *specialisation* at a $\tau \in R$ gives a point P_τ of the pine tree $\mathcal{E}_\tau$ in the lisière $\mathcal{E}_K$ of the forest. That is $P_\tau \in \mathcal{E}_\tau(K)$. So P is nothing but a point varying with τ in the family.'

They stopped in front of a huge pine tree because they saw a squirrel jumping from tree to tree. The Wolf thought of the last time he eat meat, but when the Hare resumed his teaching, he quickly forgot about it.

'Next, we have already a way of reducing points on $\mathcal{E}_\tau$ at primes v as it is a curve over R, if $\tau \in R$. So there are points $P_{\tau,v}$ in the trees $\mathcal{E}_{\tau,v}(\mathbb{F}_v)$. Here it is important to distinguish between the reduction $\mathcal{E}_{\tau,v}$ and $\mathcal{E}_{\tau+r,v}$, for the point $P_{\tau,v}$ doesn't need to be equal to $P_{\tau+r,v}$. The reason for this is, I am proud to say, another form of cancellation.

Let me introduce my standard example

$$\mathcal{E}\colon \quad y^2 = x^3 - \tau^2 x + \tau^2 \qquad \text{over } \mathbb{Z} \tag{3.1}$$

with the point $P = (\tau, \tau)$ of infinite order in $\mathcal{E}(\mathbb{Q})$. Here some multiples of it.'

The Hare showed the Wolf the following list

$$\begin{aligned}
2\,P =&(\tau^2 - 2\tau\,,\ -\tau^3 + 3\tau^2 - \tau)\\
3\,P =&\left(\frac{\tau^3 - 2\tau^2 - 3\tau + 4}{(\tau-3)^2}\,,\ \frac{3\tau^4 - 15\tau^3 + 21\tau^2 - 9\tau + 8}{(\tau-3)^3}\right)\\
a(6\,P) =&\tau^{12} - 18\tau^{11} + 156\tau^{10} - 840\tau^9 + 2958\tau^8 - 6540\tau^7 + 7524\tau^6 + 312\tau^5\\
&- 12711\tau^4 + 14446\tau^3 - 5096\tau^2 - 192\tau + 64\\
b(6\,P) =& -\tau^{18} + 27\tau^{17} - 315\tau^{16} + 2070\tau^{15} - 8217\tau^{14} + 18909\tau^{13} - 19683\tau^{12}\\
&+ 9036\tau^{11} - 156123\tau^{10} + 928677\tau^9 - 2583033\tau^8 + 4136166\tau^7 - 3829803\tau^6\\
&+ 1654659\tau^5 + 176727\tau^4 - 437352\tau^3 + 106464\tau^2 - 2304\tau + 512\\
e(6\,P) =&(\tau - 3)\,(3\tau^4 - 15\tau^3 + 21\tau^2 - 9\tau + 8)
\end{aligned}$$

‘How did you calculate that?’ asked the astonished Wolf.

‘Every clever Hare has `pari-gp` at home,’ answered the other and went on with his explanation. ‘For instance, the point $3P$ specialises to $(0, -1)$ at $\tau = 1$, at $\tau = 3$ it is O and for $\tau = 7$ we have $(3P)_{\tau=7} = (\frac{57}{4}, \frac{379}{8})$. At the place $\upsilon = (2)$, the second and the third point reduce to O, but the first doesn’t.’

3.2 Local Forests

‘But let me come back to the general forest. Suppose now $\mathcal{E}$ is an elliptic forest over a discrete valuation ring R. Let’s look at one pine tree in the lisière $\mathcal{E}_\tau$ for a $\tau \in R$. Since R is principal, you know what I mean by the e of the point P_τ in $\mathcal{E}_\tau(K)$, to avoid confusion I will write this now $e(P, \tau)$. In the same manner we write $a(P, \tau)$ and $b(P, \tau)$. That is, in R, we write with reduced fractions

$$P_\tau = \left(\frac{a(P,\tau)}{e(P,\tau)^2}, \frac{b(P,\tau)}{e(P,\tau)^3} \right) \tag{3.2}$$

On the other hand, we have polynomials $a(P)$, $b(P)$ and $e(P)$ in $R[\tau]$. *A priori* they are defined up to a unit in $K^\times$, but since we are working over a principal ideal domain R, we can further cancel out the contents of the polynomials. Then we have polynomials in $R[\tau]$ defined up to a unit in $R^\times$. Back on to the one particular tree, we can replace the value τ in the polynomial $e(P)$. So we can write

$$P_\tau = \left(\frac{a(P)(\tau)}{e(P)(\tau)^2}, \frac{b(P)(\tau)}{e(P)(\tau)^3} \right) \tag{3.3}$$

Comparing the two expressions (3.2) and (3.3), we see that the second, which is not necessary written in reduced fractions, might have some “cancellation”. More precisely, there is an element $\gamma(P, \tau) \in R$ defined by the equation

$$e(P,\tau) \cdot \gamma(P,\tau) = e(P)(\tau).\text{'} \tag{3.4}$$

It is defined, as everything, up to a unit in $R^\times$. How shall we call it? *Simplification*, maybe to distinguish it from the cancellation.

‘All right,’ said the Wolf, ‘are you going to explain me now that the other cancellation has something to do with this one?’

‘Later, first I will prove you that there is not too much simplification.’

Proposition 3.1. *Let P be a section of an elliptic forest $\mathcal{E}$ defined over a discrete valuation ring R. The map*

$$\begin{aligned} R &\longrightarrow \mathbb{Z}_{\geq 0} \\ \tau &\longmapsto \upsilon(\gamma(P,\tau)) \end{aligned}$$

is bounded and υ-adically continuous.

‘If there is a simplification in (3.3), then the resultant $r(P)$ of the polynomial $a(P)$ and $e(P)$ can’t be a unit. Even better, its valuation $\upsilon(r(P))$ is a bound for $\upsilon(\gamma(P, \tau))$ for all τ.

Now if the simplification for some $\tau \in R$ has valuation k, then changing τ by a small amount ε of valuation larger than k to $\mathrlap{\tau}{\rho} = \tau + \varepsilon$, then the simplification doesn’t change:[4] $\gamma(P, \mathrlap{\tau}{\rho}) = k$, because of the following congruence and the equivalent thing for $e(P)$:

$$\frac{a(P)(\tau)}{\pi^k} \equiv \frac{a(P)(\mathrlap{\tau}{\rho})}{\pi^k} \pmod{\pi}.$$

So the function is locally constant.’ □

[4] its seems that the Hare is familiar with the New Greek Letters; here he uses ’Taurho’ $\mathrlap{\tau}{\rho}$.

3.3 Global Forests

'Let me come to the next thing, master Wolf,' continued the Hare. 'Until now we looked at the "local" situation; local in the sense that there was only the lisière of the forest and one row of trees behind it, something like this alley over there.'

The Hare pointed to a path that had a row of trees on each every side. The Wolf nodded, not interested.

'So let's look at an elliptic forest $\mathcal{E}$ over a number ring R. For every prime υ, by working in the localisation $R_{(\upsilon)}$ of R at υ, we can define numbers $\gamma_\upsilon(P,\tau)$ as we just did. We can enlarge our knowledge about γ:

Proposition 3.2. *Let P be a section in an elliptic forest $\mathcal{E}$ over a number field. The map $\tau \mapsto \upsilon(\gamma_\upsilon(P,\tau))$ is zero for almost all primes υ.*

Let $r(P) \in R$ be the resultant between the polynomials $a(P)$ and $e(P)$ in $R[\tau]$. The local polynomials $a_\upsilon(P)$ and $e_\upsilon(P)$ in $R_{(\upsilon)}[\tau]$ are obtained by simplifying the content of the polynomials $a(P)$ and $e(P)$. Therefore the valuation $\upsilon(r(P))$ of the global resultant must be bigger than $\upsilon(r_\upsilon(P))$ which bounded $\upsilon(\gamma_\upsilon(P,\tau))$ in 3.1. Since almost all valuation of $r(P)$ must be zero, this concludes the proof of the proposition.' □

Proposition 3.3. *Let P be a section in an elliptic forest $\mathcal{E}$ over a number field. Suppose that P belongs to $\mathcal{E}^o_K(K)$. Then for all but a finite number of primes υ, all the points $P_{\tau,\upsilon}$ with $\tau \in R$ are a non-singular.*

'One way of proving that,' told the Hare to the Wolf, 'is to note that for the primes for which $\gamma_\upsilon(P,\tau)$ is a unit, and there are only finitely many of those, the conditions for P to be a singular point can be written as equations in polynomials.

$$\begin{aligned}\left(2b(P) + a_1\, a(P)\, e(P)^2 + a_3\, e(P)^3\right)(\tau) &\equiv 0 \pmod{\mathfrak{p}_\upsilon}\\ \left(3a(P)^2 + 2a_2\, a(P)e(P)^2 + a_4\, e(P)^4 - a_1\, b(P)\, e(P)\right)(\tau) &\equiv 0 \pmod{\mathfrak{p}_\upsilon}\end{aligned}$$

If there is a τ such that $P_{\tau,\upsilon}$ is singular, then the resultant of the two polynomials above must be in the ideal $\mathfrak{p}_\upsilon$. This happens only for a finite number of υ's,' ended the Hare the proof. □

'All these resultants they look to me as if we are calculating intersections in geometry.'

'Maybe, in a geometric setting, a soil like $\mathbb{A}^2_K$ over a field K for instance, I would expect that one can multiply a section out of any singularity. But this is not the case here. We are not out of the wood, so to speak.

Let me illustrate this with two characteristic examples. The first is my favourite forest (3.1), apart of our own forest maybe, and the point $P = (\tau,\tau)$. Here the discriminant is

$$\Delta(\tau) = 16 \cdot \tau \cdot (4\tau^2 - 27).$$

By the way, this is *not* a regular model for $\mathcal{E}_K$, the point $\tau = x = y = 0$ is singular for the elliptic surface $\mathcal{E}_K$. The bad fibres of $\mathcal{E}_K$ are of type IV for $\tau = 0$, I_1 for the place when $4\tau^2 = 27$ and $\mathrm{I}_0^\star$ for $\tau = \infty$. It is not hard to see that $Q = 6P$ doesn't meet any singularity in the lisière, that is $Q \in \mathcal{E}^o_K(K)$. The problem is that Q_τ reduces sometimes to a singular point at $p = 2$, if you allow me to concentrate on $K = \mathbb{Q}$. More precisely, for odd $\tau \in \mathbb{Z}$ and τ with $\tau \equiv 0 \pmod 8$, the reduction lies in the formal group $\widehat{\mathcal{E}}_\tau(\mathbb{Q}_2)$, so everything is ok. While for the other τ things are not so good, they reduce to the singular point modulo 2. Nevertheless, we are not lost: If $\tau \equiv 4 \pmod 8$ the point $5Q$ is no longer singular modulo 2, and for $\tau \equiv 2, 6 \pmod 8$ $2Q$ has this properties. As a conclusion, we can say that $10Q = 60P$ is everywhere good in reduction, I will call it *good in the forest*.

Now to a second example, not as nice as the first. Let $\mathcal{E}$ be the forest given by

$$y^2 + x\, y = x^3 - \tau^3 + 2\,\tau^2$$

over $\mathbb{Z}$ with the point $P = (\tau, \tau)$. The discriminant is

$$\Delta(\tau) = -\tau \cdot (\tau - 2) \cdot (432\,\tau^3 - 864\,\tau^2 - 1)$$

This time already $2P$ is in $\mathcal{E}^o_K(K)$. But things are very bad, call it evil, maybe, at $\tau = 0$. The multiples of P on $\mathcal{E}_{\tau=0}$ look like

$$\begin{array}{lll} (2P)_{\tau=0} = (-\frac{2}{9}, \frac{4}{27}) & (4P)_{\tau=0} = (\frac{4}{9}, -\frac{16}{27}) & (6P)_{\tau=0} = (-\frac{8}{9^2}, \frac{64}{9^3}) \\ (8P)_{\tau=0} = (\frac{16}{15^2}, -\frac{256}{15^3}) & (10P)_{\tau=0} = (\frac{64}{33^2}, -\frac{4096}{33^3}) & \cdots \end{array}$$

and this means that this point when multiplying gets worse and worse modulo 2. As a consequence, *no* multiple of P can be good in the whole forest, because its 'evil' at $\tau = 0$. A little bit like you, dear master Wolf!'

The Hare continued after the Wolf threw a dangerous glance at him. 'The phenomena can be linked to the following observation. Suppose the lisière $\mathcal{E}_K$ of an elliptic forest over a local field K has an additive fibre at some τ. The set of non-singular points in $\mathcal{E}_\tau(K)$ is a group isomorphic to the additive group K. The subgroup of points $\mathcal{E}^o_\tau(K)$ reducing to a nonsingular point corresponds to R in K. So the quotient is an infinite torsion group K/R.

Now in the split multiplicative case, the elements in this quotient won't be of finite order: The quotient looks this time like $K^\times/R^\times$ which is isomorphic to $\mathbb{Z}$. There should be infinitely many components in a thing that generalizes Néron-model to forests, that's unlucky.

Back to the general case. Here is as good as it gets. Because of the previous proposition 3.3, the question is now local.'

Proposition 3.4. *Let P be a section in $\mathcal{E}^o_K(K)$ of a forest $\mathcal{E}$ defined over a discrete valuation ring R with finite residue field $\mathbb{F}_v$. Let $\varepsilon > 0$. There exists an open U in R of measure $1 - \varepsilon$ and an number $m \geq 1$ such that the point mP has non-singular reduction for all $\tau \in U$. Moreover U can be taken to be the whole of R if $\mathcal{E}_K$ has only additive bad fibres.*

'The discriminant $\Delta \in R[\tau]$,' began the Hare his proof, 'is a continuous function. Take U to be R minus some sufficiently small balls around the τ's with bad fibres. On U the valuation of the discriminant is bounded. I will show you now that the index of $\mathcal{E}^o_\tau(K)$ in $\mathcal{E}_\tau(K)$ is bounded for all $\tau \in U$. Let me formulate it as a

Lemma 3.5. *Let E be an elliptic curve* (Weq) *over R. The index of the subgroup $E^o(K)$ in $E(K)$ is bounded by an expression depending only on the valuation of the discriminant Δ and the field $\mathbb{F}_v$.*

To see this, let $u \in R$ be the constant in the change of coordinates of E used to obtain a minimal equation. We have that $v(\Delta) = 12v(u) + v(\Delta_{\min})$ and so both expressions are bounded by the valuation of Δ. Now, the index of $E^o(K)$ in $E(K)$ is bounded by

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

Where does this formula come from? Just look at who are the points who are pushed out of $E^o(K)$ when you change equation.

From the algorithm of Tate[5] we have a bound for the index in the minimal case, namely the maximum between 4 and $v(\Delta_{\min})$. The number of points in the reduction is bounded by an expression only depending on the number of points in the field $\mathbb{F}_v$ by Hasse-Weil. Hence every factor is bounded by the valuation of the discriminant. This should prove this lemma and so the first part of the proposition.

Now, I should have a look at the small balls around the additive fibres at τ. I told you that the sections in $\mathcal{E}^o_K(K)$ can be multiplied, say $Q = mP$, such that there reduction at τ is non-singular due to the fact that the 'group of components' of $\mathcal{E}_\tau$ is torsion. For a sufficiently small change in τ,

[5] see [Tate, 1975].

the expressions $e(Q,\tau)$ and $a(Q,\tau)$ won't change modulo π. So Q will have non-singular reduction on the small ball around τ. □

The last part is not true for multiplicative fibres, nevertheless we could be lucky and P is already smooth in reduction at τ and then we could enlarge U, otherwise the section is 'evil' and there is no hope to get out of the singularities in the reduction, just as in the second example.'

'The main application I have in mind is the following consequence,' said the Hare and wrote

Corollary 3.6. *Let P be a point in $\mathcal{E}_K^o(K)$ of an elliptic forest over a number ring R. Suppose that for a certain tree $\mathcal{E}_\tau$ in the lisière, the point P_τ has everywhere non-singular reduction. It exists then a sub-forest $\mathcal{E}'$ containing this tree such that P is good on the whole of this sub-forest.*

'What is a sub-forest?' asked the Wolf.

'I will be more precise,' was the answer of the Hare.

'I claim that there is an arithmetic progression $\tau_0 + g \cdot R$ for some τ_0 and $g \neq 0$ in R such that the reduction of P_τ is everywhere non-singular for all trees with τ in this arithmetic progression. This is more or less a direct consequence of what we just did.

Now the sub-forest $\mathcal{E}'$ is simply obtained replacing τ by $\tau_0 + g \cdot \tau$ in the Weierstrass equation for $\mathcal{E}$. This gives a new forest as the equations are again defined over $R[\tau]$. You can think of it as if a lumberjack would cut down every row of trees except every g^{th} row. In this way the trees that are bad for P are cut out of the forest.'

'What a sad thing!'

'Indeed we loose many trees, but at least not the one we are interested in. If we just want to be sure that there is a multiple with everywhere non-singular reduction on the whole of a sub-forest, we would have to chop down much less trees.'

The Wolf and the Hare passed underneath a tree which a Raven was sitting on. The bird was so surprised by when he saw the two talking friendly that he dropped the cheese he held in his beak. It was the Wolf who ate the cheese and destroyed the Raven's dream of a nice creamy "fondue" that night.

3.4 Variation of the Local Height in Forests

The Hare and the Wolf turned back on the way towards the cave. The Hare told the Wolf some more of what he knew about elliptic forests.

'Let $\mathcal{E}$ be an elliptic forest over a number ring R. Replace in the Weierstrass equation τ by $\frac{1}{\rho}$ and multiply the new equation sufficiently often with ρ. Then we have another Weierstrass equation over the ring $R[\rho]$, that is a second elliptic forest $\mathcal{E}'$ over R. Glued together $\mathcal{E}_K$ and $\mathcal{E}'_K$ along $\operatorname{Spec} K[\tau,\rho]$ represents a model of an elliptic surface $\mathbf{E}$ over the curve $\mathbb{P}^1_K$, with two charts $\mathcal{E}_K \to U = \operatorname{Spec} K[\tau]$ and $\mathcal{E}'_K \to U' = \operatorname{Spec} K[\rho]$.

Let P be a section in $\mathbf{E}(K)$ that avoids the singularities of the bad fibres, so a section in $\mathcal{E}_K^o(K)$ and $(\mathcal{E}'_K)^o(K)$ glued together. Define a Cartier divisor on PP^1, by the functions

$$\begin{aligned} \tau &\mapsto (e(P)^{12}\cdot\Delta)(\tau) && \text{on } U \text{ and} \\ \rho &\mapsto (e'(P')^{12}\cdot\Delta')(\rho) && \text{on } U'. \end{aligned}$$

Do we know it? Yes, we do. Its class is nothing else than the thing I called $12 \cdot q(P)$ in (2.1), the ideal class pairing into $\operatorname{Pic}\mathbb{P}^1$.'

Proposition 3.7. *Let $\mathcal{E}$ be an elliptic forest over a number ring R and suppose that we are given a section P that is good in the whole forest. Then the function*

$$\begin{aligned} \mathbb{P}^1(K) \times \{\textit{places of } K\} &\longrightarrow \mathbb{R} \\ (\tau, v) &\longmapsto \lambda_v(P_\tau) \end{aligned}$$

is a Weil function[6] *associated to the divisor class $q(P)$.*

[6] definitions for the theory of local heights can be found in chapter 10 of [Lang, 1983].

‘But what is λ_∞?’ asked helplessly the Wolf.

‘Until now I was only looking at finite places v of R. If v is an infinite place, I will take the local height that is giving the canonical real-valued Néron-Tate height, so it is build from the complex sigma function $\sigma_v(z)$ and the quasi-periodic map η extended linearly to $\mathbb{C}$.’

‘Yesyes, I remember,[7] it's something like

$$\lambda_v(z) = -\log\left|\exp(-\tfrac{1}{2}z\cdot\eta(z))\cdot\sigma_v(z)\cdot\Delta^{\frac{1}{12}}\right|_v \quad \text{, isn't it?'}$$

‘We only need very little information about it anyway. Let me prove the proposition that I just wrote down. First for infinite paces v, we have to show that for every v-adically bounded set the function $\tau \mapsto 12\,\lambda_v(P_\tau)$ differs only by a continuous and bounded function from the expression $-\log\left|e(P)^{12}\Delta(\tau)\right|_v$. Since both expressions have a $\log|\Delta|_v$ in them it drops out of our considerations. The problem is now to bound the function

$$\log\left|\frac{e(P)(\tau)}{\exp(-\frac{1}{2}z\cdot\eta(z))\cdot\sigma_v(z)}\right|_v, \tag{3.5}$$

that is to bound the fraction from above and away from zero for τ on a bounded set of complex numbers. But by

$$\frac{a(P)(\tau)}{e(P)(\tau)^2} = \frac{1}{z(P_\tau)^2} + \frac{a_1}{z(P_\tau)} + \cdots$$

we see[8] that the order of vanishing of $e(P)$ and $\tau \mapsto z(P_\tau)$ must be equal, and then $\sigma_v(z) = z + \cdots$ permits to conclude it.

Now to the finite places. Since P_τ has everywhere good reduction, we know a formula for $\lambda_v(P_\tau)$, namely

$$\begin{aligned} 12\,\lambda_v(P_\tau) &= 12\,v(e(P,\tau)) + v(\Delta(\tau)) \\ &= 12\,v(e(P)(\tau)) - 12v(\gamma_v(P,\tau)) + v(\Delta(\tau)). \end{aligned}$$

The second line is just the definition (3.4) of γ. Now the propositions 3.1 and 3.2 tell us that on the v-adically bounded set $\{\tau \mid \tau \in R_v\}$, the function $12\,\lambda_v(P_\tau)$ differs from $v(e(P)^{12}\Delta(\tau))$ by a bounded, v-adically continuous function and that this bound is almost always zero. Choosing a different equation, I can shift any bouded set into an R_v like above. □

Now I want to sum over the places v as in the definition (2.2). I can show you the

Proposition 3.8. *Let $\mathcal{E}$ be an elliptic forest over a number field R and P a section of it that is good in the whole forest. Denote by $h_{\mathbb{P}^1}$ the usual normalized height function and by $\hat{h}(P)$ the degree of $q(P)$ as in proposition 2.2. There exist a constant C, depending on P, such that*

$$\left|\hat{h}_\infty(P_\tau) - \hat{h}(P)\cdot h_{\mathbb{P}^1}(\tau)\right| < C$$

for all τ on the curve $\mathbb{P}^1$.

This is nothing else that the theorem of Tate.[9] But his proof is incomparably more elegant and he actually prove something different and better: His theorem says that this difference is bounded for all sections P in the connected component of a minimal model of an elliptic surface over any non-singular projective curve.

Our version here comes nevertheless from a local decomposition while Tate's proof is global. Alas, even this has been done, Call has shown that Tate's argument work also for Weil functions.[10]

[7] for who doesn't remember like the Wolf, this is explained in VI.3.2 of [Silverman, 1994].

[8] maybe its good to remember that $e(P)$ and $a(P)$ can't have a common zero, since the fraction is simplified in $K[\tau]$.

[9] in [Tate, 1983], the argument is reproduced as theorem III.11.1 in [Silverman, 1994] and as theorem 12.5.2 in [Lang, 1983], where it is generalized to certain families of abelian varieties.

[10] see [Call, 1989].

It is important to realize that I could not do such a thing for the p-adic height. The problem is that for the p-adic logarithm we would have to bound the fraction in (3.5) away from the roots of unity rather than away from 0. This will be the main subject of what I shall tell you tomorrow, if you, master Wolf, spare me and let me live.'

The sun was about to hide behind the trees, when the Wolf and the Hare arrived back at the den of the Wolf. The Hare cooked some carrot-purée, but after the meal he had to return to his prison and the Wolf went to bed. In his sleep, the Wolf dreamt of a hot and tasty "filets de lièvre en sauce balsamique au vin rouge".

Chapter 4

p-adic Heights in Forests

After a long day of work, the Wolf came back in the early evening, tired but happy that he would listen to the Hare. The Hare continued his explanations.

4.1 p-adic Sigma-Function of Forests

‘The previous things on local heights in elliptic forests show that the $e(P,\tau)$ doesn’t behave too bad badly when varying the elliptic curve in a forest. Now to the other term in the p-adic height, the p-adic sigma function.

Let R be a complete discrete valuation ring of residue characteristic p. As usual π denotes a uniformizer of R. Let $\mathcal{E}$ be an elliptic forest over R, that is, I recall you a Weierstrass equation (Weq) with coefficients in $R[\tau]$. I can do the usual calculations in the formal group of $\mathcal{E}$ over $R[\tau]$ to construct a Bernardi sigma-function such as I did show you before. This will be a function $\sigma_v^{(0)}(t) \in R[\tau][\![t]\!]$ and the same formula (2.7) with a_i’s in $R[\tau]$ is valid. The big question is therefore, how does the constant $s_{2,v}$ vary when walking along the lisière of the forest. It is not hard to imagine that the equations that we would have to solve to get approximations to $s_{2,v}$ produce polynomials in τ whose coefficients converge v-adically to some value in R, just as in the constant case. But at the same time the the degree will grow, so we can’t hope to find a $s_{2,v}$ in $R[\tau]$, but rather in $R\langle\tau\rangle$, the ring[1] of series in $R[\![\tau]\!]$ who converge for all τ in R, in other word, whose coefficients converge v-adically to zero.

Actually, I never explained the construction of the canonical v-adic sigma function. So I will do it now in this more general setting, this will then prove the above remark as well. So I am actually presenting parts of the second appendix to the p-adic sigma function paper[2] of Mazur and Tate

I have to impose a heavy restriction on the forest $\mathcal{E}$: I want that, for every integral τ in the algebraic closure $\in \bar{R}$ of R, the reduction of the tree $\mathcal{E}_\tau$ is a good and ordinary curve $\mathcal{E}_{\tau,v}$. In this case I will call the forest *good and ordinary* in reduction. In practice, we can always concentrate on a v-adic neighbourhood of a tree $\mathcal{E}_{\tau_0}$, say using the lumberjack by replacing τ by some polynomial with constant reduction like $\pi\,\tau + \tau_0$. Such a forest is then good and ordinary if the tree at τ_0 was. Even better, the reduction is constant.

Fix an integer n. For every tree $\mathcal{E}_\tau$ with $\tau \in R$ the formal group has exactly p^n torsion points defined over R of order p^n as the reduction is ordinary. We can build an isogeny b_n defined over K from $\mathcal{E}_\tau$ to an elliptic curve $\mathcal{E}_\tau^{(n)}$ having this cyclic subgroup as its kernel. There is a dual isogeny a_n, so $a_n \circ b_n = [p^n]$. The isogeny a_n, when restricted to the formal group, must induce an isomorphism $\widehat{a_n}$ of formal groups between $\bigl(\mathcal{E}_\tau^{(n)}\bigr)^\wedge$ and $(\mathcal{E}_\tau)^\wedge$ as b_n has already killed all the p^n-torsion in there. Define a divisor

$$D_n = a_n^*(O_{\mathcal{E}_\tau}) - p^n \cdot (O_{\mathcal{E}_\tau^{(n)}})$$

on the new curve $\mathcal{E}_\tau^{(n)}$. Over the field K, the divisor must be the divisor of a function ϕ_n on the curve $\mathcal{E}_\tau^{(n)}$, as D_n sums to O and has degree 0.’

‘This divisor looks quite similar to the one you used to define the division polynomial.’

‘Indeed, a certain normalisation of this function with respect to the chosen Weierstrass equations, is called the division polynomial of the isogeny a_n,’ replied the Hare to the question of he Wolf.

[1] this is a Tate-algebra as explained in [Schneider, 1998], reference I found thanks to Tony Scholl.

[2] see Appendix II, entitled “Existence of σ over more general bases, modularity, and $\mathbb{E}_2$” in [Mazur and Tate, 1991].

'Now, if we look at the restriction of the divisor to the formal group, we have simply

$$\operatorname{div}(\phi_n)\Big|_{(\mathcal{E}_\tau^{(n)})^\wedge} = (1-p^n)\cdot(O_{\mathcal{E}_\tau^{(n)}}).$$

The restriction of ϕ_n to the formal group can be pulled-back to the formal group $(\mathcal{E}_\tau)^\wedge$ of the original curve since $\widehat{a_n}$ is an isomorphism there, denote this function on $(\mathcal{E}_\tau)^\wedge$ by $\hat{\phi}_{\tau,n}$. It is therefore a non-zero element of the fraction field of $R\llbracket t\rrbracket$ and when we apply the Weierstrass preparation theorem to it, we can use the information on its restricted divisor to conclude that there is a unique non-zero element β_τ in K such that

$$\hat{\phi}_{\tau,n}(t) = \beta_\tau \cdot t^{1-p^n} + \cdots \qquad \in \beta_\tau \cdot t^{1-p^n}\cdot(1+t\cdot R\llbracket t\rrbracket).$$

Of course, $\hat{\phi}_{\tau,n}(t)$ is only defined up to a scalar multiplication by a non-zero element in K. If I divided $\hat{\phi}_{\tau,n}$ by β_τ and multiplied it with t^{p^n}, you would see appearing a series in $R\llbracket t\rrbracket$. The limit as n grows is the canonical sigma-function on $\mathcal{E}_\tau$.

But as you remembered, I wanted to show you how the canonical sigma function varies with τ. For this, we pass from the ring $R[\tau]$ to its v-adic completion $R\langle\tau\rangle$. The formal group $\widehat{\mathcal{E}}/R\langle\tau\rangle$ of the equation over $R\langle\tau\rangle$ plays the same role as the formal group of the single tree. Note that there is again an exact sequence

$$0 \longrightarrow \mathcal{E}_1(Q\langle\tau\rangle) \longrightarrow \mathcal{E}(Q\langle\tau\rangle) \longrightarrow \tilde{\mathcal{E}}(\mathbb{F}_v(\tau)) \longrightarrow 0.$$

With the notation $\tilde{\mathcal{E}}/\mathbb{F}_v(\tau)$ for the elliptic curve over the function field $\mathbb{F}_v(\tau)$ obtained by reduction, $Q\langle\tau\rangle$ should mean the fraction field of the ring $R\langle\tau\rangle$ and $\mathcal{E}_1$ is simply defined as being the kernel of reduction. The surjectivity comes as usual from Hensel's lemma valid in the complete ring $R\langle\tau\rangle$. Next the kernel has also the usual interpretation, since it consists of points in $\mathcal{E}(Q\langle\tau\rangle)$ where the parameter t has value in $\pi R\langle\tau\rangle$, and because the series converge in the complete ring $R\langle\tau\rangle$, $\mathcal{E}_1(Q\langle\tau\rangle)$ could also be denoted by $\widehat{\mathcal{E}}(\pi R\langle\tau\rangle)$.[3]

Now, there is a isogeny b_n defined over $Q\langle\tau\rangle$ whose kernel are the p^n-torsion points in the formal group from the elliptic curve $\mathcal{E}/Q\langle\tau\rangle$ to a new elliptic curve $\mathcal{E}^{(n)}/Q\langle\tau\rangle$. Its dual a_n is again an isomorphism when restricted to the formal groups. Then the divisor D_n as before, but defined over $Q\langle\tau\rangle$ this time, is principal and so we have a function ϕ_n on $\mathcal{E}^{(n)}$ with divisor D_n defined up to a non-zero element in $Q\langle\tau\rangle$.'

'I am in a wood!' said the lost Wolf.

'Don't worry!' tried the Hare to reassure him. 'Intuitively, this should work. The better and more sophisticated description is in this p-adic sigma-function paper. Let me continue anyway.

Imagine the function ϕ_n written as a fraction of polynomials in the coordinates x and y with coefficients in $Q\langle\tau\rangle$. Some of these coefficients could have poles at τ_0's. If that's the case, we can multiply the function by $(\tau-\tau_0)$ without changing its divisor over $Q\langle\tau\rangle$ and similar we do if ϕ_n vanishes for some τ_0. So in the end, I will have a function ϕ_n whose specialisations at all $\tau_0 \in \overline{R}$ has the restriction of D_n to the tree as its divisor. So it specialisation differs only by an element in $\overline{K}$ from the function $\phi_{\tau,n}$ constructed before.[4]

Again the restriction of ϕ_n to the formal group can be taken back to the group $\widehat{\mathcal{E}}$ by $\widehat{a_n}$, leaving us with a function $\hat{\phi}_n$ that lives in the fraction field of $R\langle\tau\rangle\llbracket t\rrbracket$. We take a look at the function $\sigma_n = t^{p^n}\cdot\hat{\phi}_n$ viewed over the fraction field of the ring $R\llbracket\tau\rrbracket\llbracket t\rrbracket$. Here the Weierstrass preparation theorem applies again as the ring $R\llbracket\tau\rrbracket$ is a complete discrete valuation ring, hence σ_n can be written as a product of an element in the fraction field of $R\llbracket\tau\rrbracket$, a distinguished polynomial in the variable t and someone in $(1+t\cdot R\llbracket\tau\rrbracket\llbracket t\rrbracket)$. If we plug $\tau=0$ into this we find an expression in $K^\times\cdot t^{\text{some power}}\cdot(1+t\cdot R\llbracket t\rrbracket)$. Comparing with the function $\hat{\phi}_{\tau,n}$ for $\tau=0$, we know that the power of t must be 1. Finally, comparing with all other $\hat{\phi}_{\tau,n}$ the σ_n must give a nice series for all τ, so the things in $R\llbracket\tau\rrbracket$ must converge for all τ, that is they lie in $R\langle\tau\rangle$. You should be convinced now that

[3] basically this is the argument in VII.2.2 [Silverman, 1992] but without assuming the ring to be local.

[4] what he did here is using the fact that the he is working over an affine scheme and so one can move the fibral part of the divisor of the function ϕ_n viewed over $R\langle\tau\rangle$ out of sight.

σ_n is a product of a nonzero element in $Q\langle\tau\rangle$, a polynomial of the form $(t+\text{some polynomial in }\tau)$ and an element of $(1+t\cdot R\langle\tau\rangle[\![t]\!])$. But note that f must vanish exactly once for all τ, so even the 'polynomial in τ' doesn't have any other choice than to be zero. The final thing, we can do on σ_n is to change the first coefficient to one by multiplying it with its inverse, since $\hat{\phi}_n$ was defined anyway only up to such a factor.[5]

As a conclusion I can claim to have found a unique function σ_n in $t\cdot(1+t\cdot R\langle\tau\rangle[\![t]\!])$ coming from the divisor D_n. The last step is to show that one can go with n to infinity and to define

$$\sigma_{\mathcal{E}}(t)=\lim_{n\to\infty}\sigma_n\in t\cdot(1+t\cdot R\langle\tau\rangle[\![t]\!])$$

to be the *canonical sigma function of the forest $\mathcal{E}$*.'

'Wait. Why should this converge?' asked the Wolf and the Hare said: 'Hmm. The thing is that we can get from $\hat{\phi}_n$ to $\hat{\phi}_{n+1}$ by multiplying it with a p^n-th power of an element in $(1+t\cdot R\langle\tau\rangle[\![t]\!])$. This factor is what you get when you look at the isogeny going from $\mathcal{E}^{(n)}$ to $\mathcal{E}^{(n+1)}$ ... Basically a chain rule between division polynomials when normalized correctly.[6]

The fact that this function satisfies our formulae (2.5) and (2.6) is in the paper[7] of Mazur and Tate.

Something else can be read out of all this. If we reduce the formal group $\widehat{\mathcal{E}}$ over $R\langle\tau\rangle$ to the formal group over $\mathbb{F}_v[\tau]$, the reduction of the sigma function is a function $\tilde{\sigma}\in t\cdot(1+t\cdot\mathbb{F}_v[\tau][\![t]\!])$ satisfying the formulae in question, so it should be the canonical p-adic sigma-function of the elliptic curve $\tilde{\mathcal{E}}$ over $\mathbb{F}_v(\tau)$. Here we meet with the thesis[8] of Papanikolas who found a closed formula for calculating this p-adic sigma function involving only division polynomials of power of p and the expression for the multiplication by p in the formal group. This would give us a first approximation to the coefficients in our sigma function on the forest. I couldn't find a similar formula for better approximations, say over $R/\pi^2R[\tau]$.

I guess we have to stop for today,' suggested the tired Hare.

But the Wolf wanted to hear more and asked him to continue although it was quite late.

4.2 Results and Examples

'To present you some of the results on p-adic heights that one can get out of these notions, I would prefer to restrict myself to the case when $K=\mathbb{Q}$ and $p\neq 2$. The first forests that I was looking at were forests with $a_6=0$. They have a section $P=(0,0)$ naturally on them.

We can actually move to such an example coming from any[9] curve. Let E be an elliptic curve with a Weierstrass equation over $\mathbb{Z}$ with good ordinary reduction at p. Take a non-torsion point $P\in E(\mathbb{Q})$ on it whose denominator is *not* divisible by p, that is $P\notin\widehat{E}(\mathbb{Q}_p)$. If there is any such point, of course. I want this because it helps me to assure that we can move the point to the origin, using $e(P)^{-1}$ as u in the coordinate change (1.2). After multiplying the new equation with $e(P)$ it will have coefficients a_i in $\mathbb{Z}$ and the reduction at p is still *good* and ordinary, because $p\nmid e(P)$. If P had the luck to be everywhere non-singular in reduction, then so does $P=(0,0)$ on the new equation.

Next we take the coefficients a_i and vary some of them, but not $a_6=0$. We could take them to be things like $p\cdot\tau+a_i$. This guarantees me that the reduction is constant good and ordinary for all $\tau\in\mathbb{Z}$. Then the lumberjack 3.6 can help me to make the whole section $P=(0,0)$ good in the whole forest.'

'So we can do this with any curve of rank 1,' expressed the Wolf his believes.

'Unfortunately, it could happen that $E^{\circ}(\mathbb{Q})$ lies inside of $\widehat{E}(\mathbb{Q}_p)$, then we can't find a point of infinite order to move to $(0,0)$ without changing the reduction at p.

[5] probably some generalisation of the Weierstrass preparation theorem would give this immediately.

[6] proposition I.2. in [Mazur and Tate, 1991].

[7] as theorem 3.1 in [Mazur and Tate, 1991].

[8] partly published in his article [Papanikolas, 2000].

[9] not exactly as stated later. Maybe over a finite extension we could do it.

Anyway, let me suppose that we are in this situation, so we have an elliptic forest $\mathcal{E}$ with $a_6 = 0$, constant, good and ordinary reduction at p and $P = (0,0)$ is not a torsion section and it is good in the forest. Since the reduction at p is constant, the number of points N_p in the reduction is constant, and multiplying by it, we can carry the point $P_\tau = (0,0)$ in the subgroup $\widehat{\mathcal{E}}_\tau(\mathbb{Q}_p)$. Hence $Q_\tau = N_p \cdot P_\tau$ is in $\mathcal{E}^p(\mathbb{Q})$.

Here we have $e(P)(\tau) = e(P,\tau) = 1$ for all τ. Therefore $e(Q)(\tau) = e(Q,\tau) = f_M(P)(\tau)$ is a polynomial in τ with coefficients in $\mathbb{Z}$ which takes values in $p\mathbb{Z}$. The parameter $t(Q,\tau) = t(Q)(\tau)$ is a fraction of polynomials in $\mathbb{Z}[\tau]$, but its denominator is the polynomial $b(Q,\tau) = b(Q)(\tau)$ who takes only values prime to p, so it is a unit in $\mathbb{Z}_p\langle\tau\rangle$. This is why $t(Q)$ lives there as well.

Finally the p-adic sigma function has to be a series in $t(Q)(\tau)$ with coefficients in $\mathbb{Z}_p\langle\tau\rangle$ starting like

$$\sigma_p(Q,\tau) = t(Q)(\tau) + c_2(\tau)\cdot t(Q)(\tau)^2 + \cdots \quad \in \mathbb{Z}_p\langle\tau\rangle[\![t(Q)(\tau)]\!]$$

and so

$$\frac{\sigma_p(Q,\tau)}{e(Q,\tau)} = \frac{a(Q)(\tau)}{b(Q)(\tau)}\cdot\left(1 + c_2(\tau)\cdot t(Q)(\tau) + \cdots\right) \quad \in \mathbb{Z}_p\langle\tau\rangle$$

as $t = \frac{ae}{b}$. The p-adic height of the point P_τ on $\mathcal{E}_\tau$ is $-M^{-2}$ times the p-adic logarithm of the above expression, if P_τ is not torsion. To find possible values where the p-adic height could be zero, we would have to solve equations like

$$\zeta = \frac{\sigma_p(Q,\tau)}{e(Q,\tau)} \tag{4.1}$$

For all different roots of unity $\zeta \in \mu_{p-1}$. Such an equation can only have a *finite number* of solutions in $\mathbb{Z}_p$ unless the function on the right hand side is constant. Actually one of them is enough: If $\sigma_p(Q,\tau) = \zeta\cdot e(Q,\tau)$ for some $(p-1)^{\text{st}}$ root of unity ζ then

$$\begin{aligned}\sigma_p\left((p-1)\cdot Q,\tau\right) &= f_{p-1}(Q)(\tau)\cdot\sigma_p(Q,\tau)^{(p-1)^2}\\ &= f_{p-1}(Q)(\tau)\cdot\zeta^{(p-1)^2}\cdot e(Q,\tau)^{(p-1)^2} = e\left((p-1)\cdot Q,\tau\right)\end{aligned}$$

because of the non-cancellation 1.3 and the formula for the sigma-function (2.5). In order to have a point with p-adic height zero, the curve must have an infinite number of points were the p-adic sigma function takes integer values, I mean values in $\mathbb{Z}$. That's unlikely even though the integers are dense in $\mathbb{Z}_p$ as we would guess that σ is sufficiently transcendental.

It is not difficult to find forests for which there are no p-adic solutions to the equation (4.1), so all elliptic curves in the family must have a non-zero height for non-torsion $P = (0,0)$. On the other hand, it is easy to give examples where there is a p-adic τ for which the height of P would be zero. To determine whether this τ is a rational integer is equivalent to the original conjecture, it seems to me. Nevertheless, it tells us something else: The p-adic height of a point $P \in E(\mathbb{Q})$ can have arbitrary small p-adic height. This is in contrast with the canonical Néron-Tate height with real values where one expects[10] that this shouldn't be the case.'

'Could you, my dear teacher and future meal, give some examples?'

4.2.1 Forests with non-vanishing p-adic height

'Of course. Let me embed, or shall I say "implant" the curve E_{37A} into a forest. Say we want to look at the 13-adic height, then one choice could be the following forest:

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

Here $\mathcal{E}_0$, the tree in the lisière when $\tau = 0$, is E_{37A} and $(0,0)$ is a section. By chance the section $(0,0)$ is good in the whole forest, simply because $a_3 = 1$ and $a_4 = 13\,\tau - 1$ never have a common

[10] see the generalisation of a conjecture of Lang, in [Silverman, 1992] as conjecture 8.9.9.

divisor. The number of points in the (good, ordinary) reduction is 16. Some values of 13-adic heights:

$$\begin{array}{lrl}
\tau = 0: & \hat{h}_{13}(P_0) = & \phantom{11\cdot 13+{}} 6\cdot 13^2 + 9\cdot 13^3 + \mathbf{O}(13^4) \\
\tau = 1: & \hat{h}_{13}(P_1) = & 11\cdot 13 + 9\cdot 13^2 + 9\cdot 13^3 + \mathbf{O}(13^4) \\
\tau = 2: & \hat{h}_{13}(P_2) = & 9\cdot 13 + 3\cdot 13^2 + 6\cdot 13^3 + \mathbf{O}(13^4) \\
\tau = 3: & \hat{h}_{13}(P_3) = & 7\cdot 13 + 10\cdot 13^3 + \mathbf{O}(13^4) \\
\tau = 4: & \hat{h}_{13}(P_4) = & 5\cdot 13 + 6\cdot 13^3 + \mathbf{O}(13^4)
\end{array}$$

until the first digit is zero again

$$\tau = 13: \quad \hat{h}_{13}(P_{13}) = \quad 4\cdot 13^2 + 5\cdot 13^3 + \mathbf{O}(13^4)$$

Maybe some of the formulae to get there. First, the 13-adic sigma function obtained by approximation of $s_{2,(13)}$ (which happens to be constant modulo 13, namely $1 + \mathbf{O}(13)$):

$$\sigma_{13}(t) = t + (6 + \mathbf{O}(13))\, t^3 + \mathbf{O}(13^4)$$

Next the parameter of the formal group evaluated on $Q = 16\,P$

$$\begin{aligned} t(Q,\tau) = {} & (11\cdot 13 + 8\cdot 13^2 + 4\cdot 13^3 + \mathbf{O}(13^4)) + (12\cdot 13 + 12\cdot 13^2 + 5\cdot 13^3 + \mathbf{O}(13^4))\cdot\tau + \\ & (2\cdot 13^2 + \mathbf{O}(13^4))\cdot\tau^2 + (11\cdot 13^3 + \mathbf{O}(13^4))\cdot\tau^3 + \mathbf{O}(13^4) \end{aligned}$$

and the denominator, written 13-adically, though strictly speaking there is no interpretation for it outside $\tau \in \mathbb{Z}$

$$\begin{aligned} e(Q,\tau) = {} & (8\cdot 13 + 12\cdot 13^2 + 12\cdot 13^3 + \mathbf{O}(13^4)) + (4\cdot 13 + 10\cdot 13^2 + 5\cdot 13^3 + \mathbf{O}(13^4))\cdot\tau + \\ & (11\cdot 13^2 + 11\cdot 13^3 + \mathbf{O}(13^4))\cdot\tau^2 + (7\cdot 13^3 + \mathbf{O}(13^4))\cdot\tau^3 + \mathbf{O}(13^4) \end{aligned}$$

Some more calculations will lead you to the following expression for the p-adic height of P

$$\begin{aligned} \hat{h}_{13}(P) &= -\frac{1}{16^2}\cdot\log_p\left(\frac{\sigma_{13}(t(Q,\tau))}{e(Q,\tau)}\right) \\ &= (6\cdot 13^2 + \mathbf{O}(13^3)) + (11\cdot 13 + 8\cdot 13^2 + \mathbf{O}(13^3))\cdot\tau + (8\cdot 13^2 + \mathbf{O}(13^3))\cdot\tau^2 + \mathbf{O}(13^3) \end{aligned}$$

showing why the first digit in the list above is “linear”. As a conclusion, you notice that for all $\tau \not\equiv 0 \pmod{13}$ the 13-adic height of the point $(0,0)$ has height of valuation 1.’

‘Moreover, in the whole forest there is maximum *one* elliptic curve whose point $(0,0)$ has vanishing 13-adic height,’ added the Wolf.

‘Very good, yes. Everything makes me believe that this τ for which the function above vanishes is not an integral value, for otherwise this single curve would have to be a very particular one. But who knows?’

4.2.2 Arbitrary small p-adic heights

‘Let me, dear master Wolf, examine another example. For the above justification that the p-adic height of the section as a function of τ is rigid analytic applies to other examples as well. To illustrate that I turn back to my favourite forest 3.1 with its section (τ,τ). I showed you that the section $Q = 6P$ was good on the sub-forest of odd τ's. As I would like to investigate the 5-adic height this time, I will consider the sub-forest given by

$$y^2 = x^3 - (10\,\tau + 1)^2\, x + (10\,\tau + 1)^2$$

with its section $(10\,\tau+1, 10\,\tau+1)$ of infinite order on it. I wouldn't like to show you the coefficients, but I can tell you that $a(Q) \in (1 + 10\mathbb{Z}\cdot\tau)$ and that $e(Q) \in (-2 + 10\mathbb{Z}\cdot\tau)$. The resultant of them is $2^{24} \cdot 5^{60}$, but obviously neither 2 nor 5 can divide both expressions at the same time for $\tau \in \mathbb{Z}$. What I've just proven is that $\gamma(Q, \tau) = 1$ for all integers τ. Now the consideration of before carry over and we have a 5-adic height in $\mathbb{Z}_5\langle\tau\rangle$. Here the 5-adic sigma function looks like

$$\sigma_5(t) = t + (12 + \mathbf{O}(5^2))\, t^3 + \mathbf{O}(5^5)$$

In this example I will try to find an approximation of the unique $\tau \in \mathbb{Z}_5$ with vanishing "height":

$$\begin{aligned}
\tau = 1 : &\qquad \hat{h}_5(P_1) = 4 \cdot 5 + 2 \cdot 5^2 + 5^3 + \mathbf{O}(5^4)\\
\tau = 2 : &\qquad \hat{h}_5(P_2) = 2 \cdot 5 + 4 \cdot 5^2 + 5^3 + \mathbf{O}(5^4)\\
\tau = 3 : &\qquad \hat{h}_5(P_3) = 3 \cdot 5^2 + 2 \cdot 5^3 + \mathbf{O}(5^4)\\
\tau = 4 : &\qquad \hat{h}_5(P_4) = 3 \cdot 5 + 3 \cdot 5^2 + 5^3 + \mathbf{O}(5^4)\\
\tau = 5 : &\qquad \hat{h}_5(P_5) = 5 + 5^2 + 2 \cdot 5^3 + \mathbf{O}(5^4)
\end{aligned}$$

So we should concentrate on the $\tau \equiv 3 \pmod 5$

$$\begin{aligned}
\tau = 8 : &\qquad \hat{h}_5(P_8) = 5^2 + 2 \cdot 5^3 + 5^4 + \mathbf{O}(5^5)\\
\tau = 13 : &\qquad \hat{h}_5(P_{13}) = 4 \cdot 5^2 + 5^3 + 5^4 + \mathbf{O}(5^5)\\
\tau = 18 : &\qquad \hat{h}_5(P_{18}) = 2 \cdot 5^2 + 5^3 + 3 \cdot 5^4 + \mathbf{O}(5^5)\\
\tau = 23 : &\qquad \hat{h}_5(P_{23}) = 3 \cdot 5^3 + 2 \cdot 5^4 + \mathbf{O}(5^5)
\end{aligned}$$

and so on ...

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

Maybe I should better write $3 + 4 \cdot 5 + 3 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + \mathbf{O}(5^5)$ will have vanishing pseudo-height.'

Because the Wolf looked somewhat puzzled, the Hare explained better: 'You see, the definition of "height" doesn't make much sense if the τ is not in $\mathbb{Z}$, since the quantity $e(Q)$ is something global.

What I did here was nothing else than the Newton algorithm, also called Hensel's lemma. This is what I meant when I said that the p-adic height could get as small as it wished ... and to me it seems without any reason for I can't see what is particular about this $\mathcal{E}_\tau$.'

4.2.3 Modulo p^2

'Let me come back quickly to the previous construction. From the construction of the p-adic sigma-function, it is clear that its values modulo p^2 only depend on the coefficients of the curve modulo p^2 and the point it is evaluated on. But in our previous example, when the point P is $(0, 0)$ and its a point that reduces everywhere to a non-singular point, then the values of a b and e of the multiple $Q = m \cdot P$ that lies in the formal group can be written as polynomials with coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4]$. They are just the constant terms of the division polynomials f_m, by the way. Hence the value of these modulo p^2 only depends upon the coefficients of the curve modulo p^2 and so does the value of the sigma function evaluated on Q. When I take the logarithm, I would have to be careful if $p = 2$, but we excluded it all the time. So finally the p-adic height modulo p^2, more precisely its first digit, is only depending on the coefficients of the equation modulo p^2.

I ran a long calculation for $p = 3$ and $p = 5$. Out of the 2916 choices for the vector (a_1, a_2, a_3, a_4) over $\mathbb{Z}/9\mathbb{Z}$ which give rise to an elliptic curve with good ordinary reduction at 3, there were 983 cases where the first digit vanishes, that are 33.71% .

In the case $p = 5$, out of 250000 cases, I found 50008 exceptions, that is 20.0032% . I would think that the probability of a point outside the formal group to have a vanishing first digit for the p-adic height is approximatively equal to $\frac{1}{p}$.'

4.2.4 Some other forests

'There is another way of constructing forests,' the Hare went on telling about his calculations. 'Suppose we are given distinct points P_1, P_2, P_3 and P_4 on an elliptic curve E, all non-torsion points in the nice subgroup $E^p(\mathbb{Q})$. From basic algebraic geometry we learn that there should be a one-parameter pencil of elliptic curves in Weierstrass equations passing through these four points. Plugging the coordinates of the points into a general equation (Weq) gives four linear relations for the coefficients a_i. We can write the solutions depending on one parameter τ; and if we multiply it a little bit with integers, we will have polynomials in $\mathbb{Z}[\tau]$. This is then an elliptic forest $\mathcal{E}$ with four sections P_j having constant coordinates.

In case of the curve $E_{433} : y^2 + xy = x^3 + 1$ of conductor 433, rank 2 with generators $P = (-1, 0)$ and $Q = (0, 1)$ which have everywhere good reduction this looks like that: Say, we want a family including this curve with two sections in the formal group for $p = 3$. First, we can jump into the formal group of E_{433} by looking at $3P$ and $6Q$. Plugging these into a general equation, we can even add further conditions like $a_1 = a_6 = 1$. After some multiplication, we find the forest

$$\begin{aligned} y^2 + x\,y - 397654919751915\,\tau \cdot y = \\ x^3 - 153005939006598\,\tau \cdot x^2 + 639566005639789\,\tau \cdot x - 1.\text{'} \end{aligned}$$

'Oh, I can't see the wood for trees!' said the Wolf and they both laughed.

'Back to the general construction,' continued the Hare. 'We can call the lumberjack to cut down enough trees so that the four sections P_j of our elliptic forest $\mathcal{E}$ have everywhere good reduction and the reduction of all trees is constant, good and ordinary at p. Provided, of course, our first tree E with its points P_j had these properties.

Here the denominators of P_j are constants $e(P_j, \tau) = e(P_j)(\tau) = e_j$ and so are t_j, b_j and a_j. Aïeaïe, this is an unlucky choice of symbols $a_j \neq a_i$, never mind it shouldn't lead to confusion, I hope.

The p-adic sigma function is of the form

$$\sigma_p(P_j, \tau) = t_j + c_2(\tau)\, t_j^2 + c_3(\tau)\, t_j^3 + \cdots \quad \in \mathbb{Z}_p\langle\tau\rangle.$$

Even better, the p-adic height isn't too difficult either:

$$\begin{aligned} \hat{h}_p(P_j, \tau) &= -\log_p\left(\frac{\sigma_p(P_j, \tau)}{e_j}\right) \\ &= -\log_p(\tfrac{t_j}{e_j}) - \log_p\left(1 + c_2(\tau)\, t_j + c_3(\tau)\, t_j^2 + \cdots\right) \end{aligned}$$

that looks like

$$= \log_p(b_j) - \log_p(a_j) + (c_2(\tau) + c_3(\tau)\, t_j \cdots) \cdot t_j + + \tfrac{1}{2}\,(c_2(\tau) + c_3(\tau)\, t_j \cdots)^2 \cdot t_j^2 + \tfrac{1}{3} \cdots$$

which is a series in $\mathbb{Z}_p\langle\tau\rangle$. They can't have more than a finite number of zeros except if they are zero. In particular, we could have started with a set of points P_j that span a subgroup of rank 4; the elliptic surface $\mathcal{E}_{\mathbb{Q}}$ has then at least rank 4 as well and the specialisation theorem[11] of SILVERMAN shows that the $(P_j)_\tau$ spans a subgroup of rank 4 of $\mathcal{E}_\tau(\mathbb{Q})$ for almost all τ. The p-adic regulator of these points, being a nice determinant of sums of p-adic heights like above, can then not vanish for more than a finite number of points, unless it is constant zero. The same, of course, can be done for smaller ranks. Again it is easy to give families of curves of rank 2 all of which have non-zero p-adic regulator. Furthermore there is [...] awkward forest in [...] twice [...]'

Epilogue of the Editor

This is the last part of this document that was readable. The world will never know if the Hare really had a proof of the conjecture or if he continued his teaching for another 996 nights. Or if the Wolf enjoyed finally a delicious meal.

[11] see in [Silverman, 1994] as theorem III.11.4.

Appendix A

Algorithms

Here are programs written in `pari-gp` Batut et al. [1999], that I used to do calculations of p-adic heights.

A.1 Basic definitions

Some basic definitions for the arithmetic with curves over $\mathbb{Z}$. First, the numerators and denominators of a point `x`. The complicated definitions apply also to elliptic forest as defined in 3.1.

```
aasimple(x)=numerator(x[1])
bbsimple(x)=numerator(x[2])
eesimple(x)=denominator(x[2])/denominator(x[1])

aa(x)=
 {local(aas,ees,d);
  aas=aasimple(x);
  if(aas,
  ees=eesimple(x);
  d=content(aas)/content(ees)^2;
  return(aas*numerator(d)/content(aas)),
  return(0))}

bb(x)=
 {local(bbs,ees,d);
  bbs=bbsimple(x);
  if(bbs,
  ees=eesimple(x);
  d=content(bbs)/content(ees)^3;
  return(bbs*numerator(d)/content(bbs)),
  return(0))}

tt(x)=-x[1]/x[2]

ee(x)=if(aa(x)*x[2],bb(x)/aa(x)*x[1]/x[2],1)
```

For working with reductions: the Tamagawa factor, the numbers of components of the Néron model over $\mathbb{Q}_p$, and the conductor of a curve `el`.

```
tama(el,p)=elllocalred(el,p)[4]
conductor(el) = ellglobalred(el)[1]
```

`badprimes` gives the list of primes for which a given equation `el` has bad reduction.

```
badprimes(el)=
 { if(factor(el.disc)[1,1]==-1,
      vecextract(factor(el.disc)[,1]~,"^1"),
      factor(el.disc)[,1]~);}
```

Then the number of non-singular points in the reduction $\tilde{E}(\mathbb{F}_p)$ of a minimal equation of E.

```
ellnp(el,p)=
 { local(elll);
   elll=ellchangecurve(el,ellglobalred(el)[2]);
   return(if(el.disc % p,
             p+1-ellap(elll,p),
             p-ellap(elll,p)))}
```

To determine if `el` is good and ordinary at `p`, we have

```
isordinary(el,p)=if(el.disc % p && (p+1-ellnp(el,p)) % p,1,0)
```

Here some programs concerning the subgroup $E^0(\mathbb{Q})$. The first answers if the point `P` has singular reduction at `p`.

```
issmooth(el,P,p) =
 { local(xp,yp,ep);
   if(el.disc %p,
      return(1),
      if(Mod(ee(P),p)==0,
         return(1),
         ep=Mod(ee(P),p);
         yp=Mod(bb(P),p)*ep^(-3);
         xp=Mod(aa(P),p)*ep^(-2);
         if((el.a1*yp == 3*xp^2+2*el.a2*xp+el.a4)&&(2*yp + el.a1*xp+el.a3 ==0),
             return(0),
             return(1)))) }
```

To check if it is non-singular in every reduction, there is the following command

```
isallsmooth(el,P)=
{ local(bprimes,ind);
  bprimes=badprimes(el);
  return(prod(ind=1,length(bprimes),issmooth(el,P,bprimes[ind])))}
```

Finally two procedures, the first to calculate an integer which is certainly a multiple of the index of points with everywhere good reduction, that is $[E(\mathbb{Q}) : E^0(\mathbb{Q})]$. If the equation is minimal, it is simply the lowest common multiple of the local Tamagawa factors. The second program gives back a vector `[Q,m]` where `Q` is the first multiple of `P` that is everywhere non-singular and `m` is the corresponding factor.

```
bindex(el) =
{ local(ellmin,bprimes,u,ind,produit,pri);
   produit=1;
   bprimes=badprimes(el);
   ellmin=ellchangecurve(el,ellglobalred(el)[2]);
   u=ellglobalred(el)[2][1];
   for(ind=1,length(bprimes),
       pri=bprimes[ind];
       if(u %pri,
          produit=lcm(tama(el,pri),produit),
          produit=lcm(pri^(valuation(u,pri)-1) * ellnp(ellmin,pri)*tama(el,pri),
          produit)));
   return(produit) }

smoothmult(el,P)=
 { local(mp,d);
```

```
    fordiv(bindex(el),d,
           mp=ellpow(el,P,d);
           if(isallsmooth(el,mp),
    return([mp,d]);break();)); }
```

A.2 The division polynomial

We need a certain number of auxiliary functions

```
A6(el) = - y^2 - el[1]*x*y - el[3]*y + x^3 + el[2]*x^2 + el[4]*x + el[5];

A3(el) = 2*y + el[1]*x + el[3];

B8(el) = 3*x^4 + (el[1]^2+4*el[2])*x^3 + 3*(2*el[4]+el[1]*el[3])*x^2  \
           + 3*(el[3]^2+4*el[5])*x + el[1]^2*el[5]+4*el[2]*el[5] \
           - el[1]*el[3]*el[4]+el[2]*el[3]^2-el[4]^2;

B6(el) = 1/3 * deriv(B8(el),x);

A3square(el)= B6(el);

B4(el) = 1/2 * deriv(B6(el),x);

B2(el) = deriv(B4(el),x);
```

Then the function described in appendix I of Mazur and Tate [1991], denoted there by g_n. It can be calculated using the explicit recursion formulae given there in proposition 4.

```
divisiong(el,n) =
 { if(n == 1,
     1,
     if(n == 2,
      -1,
      if(n==3,
       B8(el),
       if(n==4,
        B6(el)^2-B4(el)*B8(el),
        if(n>0,
         if(n%2,
          if((n-1)%4,
           divisiong(el,(n+3)/2) * divisiong(el,(n-1)/2)^3 \
             - B6(el)^2 * divisiong(el,(n-3)/2) * divisiong(el,(n+1)/2)^3,
           B6(el)^2 * divisiong(el,(n+3)/2) * divisiong(el,(n-1)/2)^3 \
             - divisiong(el,(n-3)/2) * divisiong(el,(n+1)/2)^3  ),
           -divisiong(el,n/2+2) * divisiong(el,n/2) * divisiong(el,n/2-1)^2 \
             + divisiong(el,n/2) * divisiong(el,n/2-2) * divisiong(el,n/2+1)^2
           )))))) }
```

Here the definition of the division polynomial f_n of the elliptic curve `el`, a polynomials in `x` and `y`, and its square as a polynomial only in `x`.

```
fdivision(el,n) = if(n%2, divisiong(el,n), A3(el)*divisiong(el,n) );

fdivisionsquare(el,n) =
  { if(n%2, divisiong(el,n)^2, A3square(el)*divisiong(el,n)^2 ); }
```

Finally the numerator polynomial, denoted by g_n in 1.5.

```
gdivision(el,n) = x * fdivision(el,n)^2 - fdivision(el,n-1)*fdivision(el,n+1);
```

We can add the definition of the cancellation $\delta_m(P)$ here.

```
delta(el,pt,m) =
 { abs(subst(subst(fdivision(el,m),x,pt[1]),y,pt[2])*
    ee(pt)^(m^2)/ee(ellpow(el,pt,m)))}
```

A.3 p-adic Heights

Here the contents of the file that I called `hell.gp`, not because it looked for a long time like hell, but rather as a short name for "heights on elliptic curves". It should work for any given elliptic curve by a Weierstrass equation (Weq) over the integers and for a prime different from 2.
In the beginning a technical detail that I had to include because `pari-gp` still can't handle polynomials and series in several variables correctly.

```
{if(hellisinitalized == 1, ,
   print("First initialisation of hell.gp.\
          I will kill the variables t,w,a and z");
   kill(t); kill(w); kill(a); kill(z);
   w;t;a;);}
hellisinitalized=1;
```

The command `hellinit` replaces `ellinit`. It is defined for a 5-term vector $[a_1, a_2, a_3, a_4, a_6]$ with integer values, representing a Weierstrass equation (Weq) of an elliptic curve over $\mathbb{Q}$. Moreover it has one parameter `bigO` which is the precision of the formal group law. Usually values like 20 or 50 will give sufficient precision. The output is a vector `[el,xeris,zeries,sigmacoeff]` where `el` is the elliptic curve (resulting from `ellinit`), `xeries` is the series $x(t) = t^{-2} + \cdots$, `zeries` is the formal logarithm of the formal group looking like $z(t) = t + \cdots$ and finally `sigmacoeff` is a list of polynomials in $\mathbb{Q}[\mathrm{a}]$ as they appear in the undetermined sigma-functions (2.9) associated to $\alpha = \frac{1}{3}\mathrm{a}$, see also the example in section 2.4.1.

```
hellinit(el,bigO) =
 { local(e,s,f,xs,zs,ys,si0,si,sico);
    e=ellinit(el);

    f = Mod(t^3,t^bigO) + Mod(e.a1 * t  + e.a2 * t^2,t^bigO) * w \
          + Mod(e.a3 + e.a4 * t,t^bigO) * w^2 + Mod(e.a6,t^bigO)* w^3;
    s = f;
    while(poldegree(s,w)>0,
          s=truncate(subst(s,w,f)+O(w)^bigO));
    ws = (lift(s)+O(t)^bigO);
    ys = -1 / ws;
    xs = -t * ys;
    zs = intformal(1/(2*ys+e.a1*xs+e.a3)*deriv(xs,t),t);

    si0 = z*exp(a/3*z^2-intformal(intformal(ellwp(e,z)-1/z^2)));

    si= subst(si0,z,zs);
    sico=Vec(si);
    return([e,xs,zs,sico]) }
```

The series for $x(t)$ are calculated using the formal group law as described in [Silverman, 1992, section IV.1].

Then if the prime number $p > 2$ is known we can directly calculate the $s_{2,(p)}$. `hellinitp` give as an output a vector `[el,alpha,sigma]` where `e` is the again the elliptic curve, `alpha` is $-\frac{3}{2}s_{2,(p)}$, which must be a p-adic integer, and `sigma` representing is the canonical p-adic sigma-function, here as a polynomial $t + ...$ with coefficients in $\mathbb{Z}_p$.

```
hellinitp(el,p,bigO) =
 {local(e,s,f,xs,zs,ys,si0,si,sico,al,ind,co,cod,co0,co1);
   e=ellinit(el);
   if(isordinary(e,p),
      f = Mod(t^3,t^bigO) + Mod(e.a1 * t  + e.a2 * t^2,t^bigO) * w \
            + Mod(e.a3 + e.a4 * t,t^bigO) * w^2 + Mod(e.a6,t^bigO)* w^3;
      s = f;
      while(poldegree(s,w)>0,
            s=truncate(subst(s,w,f)+O(w)^bigO));

      ws = (lift(s)+O(t)^bigO);
      ys = -1 / ws;
      xs = -t * ys;
      zs = intformal(1/(2*ys+e.a1*xs+e.a3)*deriv(xs,t),t);

      si0 = z*exp(a/3*z^2-intformal(intformal(ellwp(e,z)-1/z^2)));
      si= subst(si0,z,zs);
      sico=Vec(si);

      al=a;
      for(ind=3, length(sico),
          co=subst(sico[ind],a,al);
          cod=denominator(content(co));
          if(cod % p,,
             co0=Mod(cod*polcoeff(co,0),p);
             co1=Mod(cod*polcoeff(co,1),p);
             al=subst(al,a, p* a+lift(-co0/co1));));
          al=subst(al,a,O(p^0));

      si=t*Polrev(subst(sico,a,al),t);

      return([e,p,al,si]),
      print(p" is not an ordinary good prime");
      return(0)) }
```

Then `hellatp` can be used to specify the prime p in a output of `hellinit` to get a result like in `hellinitp`.

```
hellatp(he,p) =
 { local(e,si,sico,al,ind,co,cod,co0,co1);
    e=he[1];
    sico=he[4];
    if(isordinary(e,p),
       al=a;
       for(ind=3, length(sico),
           co=subst(sico[ind],a,al);
           cod=denominator(content(co));
           if(cod % p,,
              co0=Mod(cod*polcoeff(co,0),p);
              co1=Mod(cod*polcoeff(co,1),p);
              al=subst(al,a, p* a+lift(-co0/co1));));
```

```
        al=subst(al,a,O(p^0));
        si=t*Polrev(subst(sico,a,al),t);
        return([e,p,al,si]),
        print(p" is not an ordinary good prime");
        return(0)) }
```

And here: the p-adic height. As parameters it takes an output from either `hellinitp` or `hellatp` and a point `pt`. The output is the p-adic height in $\mathbb{Q}_p$.

```
 hellheight(hep,pt)=
  { local(e,ptp,d,np,p,m,tval,ttt,al,si,sigmaval);
     if(hep,
        e=hep[1];
        if(ellisoncurve(e,pt),
           p=hep[2];
           al=hep[3];
           si=hep[4];

           ptp = smoothmult(e,pt);
           d=ptp[2];
           ptp=ptp[1];

           np=ellnp(e,p);
           while(ee(ptp) % p != 0,
                 m=divisors(np)[2];
                 ptp=ellpow(e,ptp,m);
                 d=d*m;
                 np=np/m;);
           tval=valuation(tt(ptp),p);
           ttt=tt(ptp)+O(p^(padicprec(al,p)+2*tval+1));

           sigmaval=subst(si,t,ttt);

           if(sigmaval % p^padicprec(sigmaval,p),
              return(1/d^2*log(ee(ptp)/sigmaval)),
              print("division by zero");
              return(0)),
        print(pt" is not on the elliptic curve");
        return(0)),
     print(p" is not a ordinary good prime");
     return(0))}
```

The first block checks if everything is ok. Then the point is multiplied first into the subgroup of good reduction everywhere, next into the formal group over $\mathbb{Q}_p$. In the end, the p-adic sigma-function pre-calculated before is evaluated on the point.

Appendix B

Tables

B.1 p-adic heights on the curve E_{37A}

The first table gives the p-adic height for the point $(0, 0)$ on the elliptic curve given by the equation

$$E_{37A}: \quad y^2 + y = x^3 - x.$$

See section 2.4.1. The symbol "no" means that the curve is not good ordinary at this prime.
As a summary, we can say that except for the following list, all p-adic heights of $(0, 0)$ have p-adic valuation 1 for $2 < p < 1000$.

37.	$\tilde{E}$ is singular.
3, 17, 19, 257, 311, 577	$\tilde{E}$ is not ordinary.
53, 127, 443, 559	Anomalous primes. These are primes where the number of points in the reduction at p is divisible by p, then the valuation drops naturally by 2. Here they all have valuation -1.
13, 67, 547	The real exceptions, here the valuation happens to be 2.

The method described in 2.4.2 to calculate the first digit gives immediately the p-adic valuation of the p-adic height except in the last three cases for all primes $2 < p < 1000$.

p-adic heights on E_{37A}			
3	no	5	$3 \cdot 5 + 3 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + O(5^6)$
7	$4 \cdot 7 + 5 \cdot 7^3 + O(7^5)$	11	$9 \cdot 11 + 4 \cdot 11^2 + 9 \cdot 11^3 + O(11^4)$
13	$6 \cdot 13^2 + 9 \cdot 13^3 + O(13^4)$	17	no
19	no	23	$10 \cdot 23 + 5 \cdot 23^2 + 9 \cdot 23^3 + O(23^4)$
29	$24 \cdot 29 + 16 \cdot 29^2 + 27 \cdot 29^3 + O(29^4)$	31	$23 \cdot 31 + 20 \cdot 31^2 + O(31^3)$
37	no	41	$15 \cdot 41 + 41^2 + O(41^3)$
43	$15 \cdot 43 + 15 \cdot 43^2 + O(43^3)$	47	$29 \cdot 47 + 18 \cdot 47^2 + O(47^3)$
53	$13 \cdot 53^{-1} + 15 + O(53^1)$	59	$44 \cdot 59 + O(59^2)$
61	$2 \cdot 61 + O(61^2)$	67	$O(67^2)$
71	$20 \cdot 71 + O(71^2)$	73	$25 \cdot 73 + O(73^2)$
79	$26 \cdot 79 + O(79^2)$	83	$38 \cdot 83 + O(83^2)$
89	$22 \cdot 89 + O(89^2)$	97	$75 \cdot 97 + O(97^2)$
101	$65 \cdot 101 + O(101^2)$	103	$84 \cdot 103 + O(103^2)$
107	$32 \cdot 107 + O(107^2)$	109	$62 \cdot 109 + O(109^2)$
113	$45 \cdot 113 + O(113^2)$	127	$89 \cdot 127^{-1} + O(127^0)$
131	$58 \cdot 131 + O(131^2)$	137	$64 \cdot 137 + O(137^2)$
139	$62 \cdot 139 + O(139^2)$	149	$5 \cdot 149 + O(149^2)$
151	$15 \cdot 151 + O(151^2)$	157	$45 \cdot 157 + O(157^2)$
163	$28 \cdot 163 + O(163^2)$	167	$32 \cdot 167 + O(167^2)$
173	$35 \cdot 173 + O(173^2)$	179	$2 \cdot 179 + 159 \cdot 179^2 + O(179^3)$
181	$51 \cdot 181 + O(181^2)$	191	$56 \cdot 191 + O(191^2)$
193	$90 \cdot 193 + O(193^2)$	197	$34 \cdot 197 + O(197^2)$
199	$43 \cdot 199 + O(199^2)$	211	$101 \cdot 211 + O(211^2)$
223	$97 \cdot 223 + O(223^2)$	227	$65 \cdot 227 + O(227^2)$
229	$179 \cdot 229 + O(229^2)$	233	$32 \cdot 233 + O(233^2)$
239	$115 \cdot 239 + O(239^2)$	241	$106 \cdot 241 + O(241^2)$

p-adic heights on E_{37A}			
251	$128 \cdot 251 + O(251^2)$	257	no
263	$161 \cdot 263 + O(263^2)$	269	$130 \cdot 269 + O(269^2)$
271	$201 \cdot 271 + O(271^2)$	277	$58 \cdot 277 + O(277^2)$
281	$201 \cdot 281 + O(281^2)$	283	$11 \cdot 283 + O(283^2)$
293	$215 \cdot 293 + O(293^2)$	307	$280 \cdot 307 + O(307^2)$
311	no	313	$256 \cdot 313 + O(313^2)$
317	$114 \cdot 317 + O(317^2)$	331	$221 \cdot 331 + O(331^2)$
337	$55 \cdot 337 + O(337^2)$	347	$165 \cdot 347 + O(347^2)$
349	$232 \cdot 349 + O(349^2)$	353	$87 \cdot 353 + O(353^2)$
359	$289 \cdot 359 + O(359^2)$	367	$254 \cdot 367 + O(367^2)$
373	$161 \cdot 373 + O(373^2)$	379	$332 \cdot 379 + O(379^2)$
383	$234 \cdot 383 + O(383^2)$	389	$307 \cdot 389 + O(389^2)$
397	$361 \cdot 397 + O(397^2)$	401	$302 \cdot 401 + O(401^2)$
409	$47 \cdot 409 + O(409^2)$	419	$306 \cdot 419 + O(419^2)$
421	$13 \cdot 421 + O(421^2)$	431	$324 \cdot 431 + O(431^2)$
433	$318 \cdot 433 + O(433^2)$	439	$325 \cdot 439 + O(439^2)$
443	$65 \cdot 443^{-1} + O(443^0)$	449	$338 \cdot 449 + O(449^2)$
457	$39 \cdot 457 + O(457^2)$	461	$414 \cdot 461 + O(461^2)$
463	$389 \cdot 463 + O(463^2)$	467	$295 \cdot 467 + O(467^2)$
479	$404 \cdot 479 + O(479^2)$	487	$243 \cdot 487 + O(487^2)$
491	$45 \cdot 491 + O(491^2)$	499	$285 \cdot 499 + O(499^2)$
503	$380 \cdot 503 + O(503^2)$	509	$134 \cdot 509 + O(509^2)$
521	$110 \cdot 521 + O(521^2)$	523	$15 \cdot 523 + O(523^2)$
541	$510 \cdot 541 + O(541^2)$	547	$O(547^2)$
557	$64 \cdot 557 + O(557^2)$	563	$335 \cdot 563 + O(563^2)$
569	$303 \cdot 569 + O(569^2)$	571	$508 \cdot 571 + O(571^2)$
577	no	587	$157 \cdot 587 + O(587^2)$
593	$219 \cdot 593 + 287 \cdot 593^2 + O(593^3)$	599	$565 \cdot 599^{-1} + O(599^0)$
601	$432 \cdot 601 + O(601^2)$	607	$50 \cdot 607 + O(607^2)$
613	$275 \cdot 613 + O(613^2)$	617	$54 \cdot 617 + O(617^2)$
619	$417 \cdot 619 + O(619^2)$	631	$462 \cdot 631 + O(631^2)$
641	$267 \cdot 641 + O(641^2)$	643	$620 \cdot 643 + O(643^2)$
647	$117 \cdot 647 + O(647^2)$	653	$441 \cdot 653 + O(653^2)$
659	$220 \cdot 659 + O(659^2)$	661	$434 \cdot 661 + O(661^2)$
673	$293 \cdot 673 + O(673^2)$	677	$570 \cdot 677 + O(677^2)$
683	$577 \cdot 683 + O(683^2)$	691	$688 \cdot 691 + O(691^2)$
701	$383 \cdot 701 + O(701^2)$	709	$314 \cdot 709 + O(709^2)$
719	$626 \cdot 719 + O(719^2)$	727	$146 \cdot 727 + O(727^2)$
733	$52 \cdot 733 + O(733^2)$	739	$519 \cdot 739 + O(739^2)$
743	$642 \cdot 743 + O(743^2)$	751	$175 \cdot 751 + O(751^2)$
757	$410 \cdot 757 + O(757^2)$	761	$177 \cdot 761 + O(761^2)$
769	$511 \cdot 769 + O(769^2)$	773	$648 \cdot 773 + O(773^2)$
787	$315 \cdot 787 + O(787^2)$	797	$22 \cdot 797 + O(797^2)$
809	$37 \cdot 809 + O(809^2)$	811	$32 \cdot 811 + O(811^2)$
821	$162 \cdot 821 + O(821^2)$	823	$44 \cdot 823 + O(823^2)$
827	$401 \cdot 827 + O(827^2)$	829	$677 \cdot 829 + O(829^2)$
839	$831 \cdot 839 + O(839^2)$	853	$393 \cdot 853 + O(853^2)$
857	$572 \cdot 857 + O(857^2)$	859	$703 \cdot 859 + O(859^2)$
863	$655 \cdot 863 + O(863^2)$	877	$402 \cdot 877 + O(877^2)$
881	$158 \cdot 881 + O(881^2)$	883	$120 \cdot 883 + O(883^2)$
887	$466 \cdot 887 + O(887^2)$	907	$412 \cdot 907 + O(907^2)$
911	$288 \cdot 911 + O(911^2)$	919	$665 \cdot 919 + O(919^2)$
929	$133 \cdot 929 + O(929^2)$	937	$124 \cdot 937 + O(937^2)$

p-adic heights on E_{37A}			
941	$91 \cdot 941 + O(941^2)$	947	$410 \cdot 947 + O(947^2)$
953	$15 \cdot 953 + O(953^2)$	967	$410 \cdot 967 + O(967^2)$
971	$956 \cdot 971 + O(971^2)$	977	$446 \cdot 977 + O(977^2)$
983	$581 \cdot 983 + O(983^2)$	991	$35 \cdot 991 + O(991^2)$
997	$246 \cdot 997 + O(997^2)$		

B.2 p-adic heights of other curves with small conductor

We look at further three examples:

$$\begin{aligned} E_{43A} &: \; y^2 + y = x^3 + x^2 \\ E_{53A} &: \; y^2 + xy + y = x^3 - x^2 \\ E_{57A} &: \; y^2 + y = x^3 - x^2 - 2x + 2. \end{aligned}$$

which are curve or rank 1 with indicated conductor. For the first two the point $(0,0)$ is of infinite order, while E_{57A} has the point $(2,1)$. Here the results for primes $2 < p < 1000$. Followed by even more examples.

E	E_{43A}	E_{53A}	E_{57A}
$[a_i]$	$[0,1,1,0,0]$	$[1,-1,1,0,0]$	$[0,-1,1,-2,2]$
P	$(0,0)$	$(0,0)$	$(2,1)$
$\tilde{E}$ is singular.	43.	53.	3, 19.
$\tilde{E}$ is not ordinary.	7, 37	3, 5, 11, 239, 751	3, 19, 37, 41, 151, 163, 491, 571, 599, 601
$\tilde{E}$ is anomalous.	3, 5, 103, 127, 541	71, 97	11
Exceptions	no	no	5

E	E_{58A}	E_{61A}	E_{65A}
$[a_i]$	$[1,-1,0,-1,1]$	$[1,0,0,-2,1]$	$[1,0,0,-1,0]$
P	$(0,1)$	$(1,0)$	$(1,0)$
$\tilde{E}$ is singular.	29	61	5, 13
$\tilde{E}$ is not ordinary.	3, 23, 83, 139, 191, 283, 311, 317, 587	31, 101, 281, 439	139, 191, 439, 659
$\tilde{E}$ is anomalous.	53, 109, 673, 739	3, 7, 13, 113	3
Exceptions	31	71	43

E	E_{77A}	E_{79A}	E_{82A}
$[a_i]$	$[0,0,1,2,0]$	$[1,1,1,-2,0]$	$[1,0,1,-2,0]$
P	$(2,3)$	$(0,0)$	$(0,0)$
$\tilde{E}$ is singular.	7, 11	79	41
$\tilde{E}$ is not ordinary.	3, 283	113, 271, 409, 479, 521, 947	29, 103, 131, 191, 251, 421, 443, 599, 811, 859, 983
$\tilde{E}$ is anomalous.	31, 71, 179, 223		3
Exceptions	5	41, 83, 131	5, 229, 283, 499

Bibliography

C. Batut, d. Bernardi, H. Cohen, M. Olivier, and K. Belabas. `pari-gp`. `http://www.parigp--home.de/`, 1999.

Dominique Bernardi. Hauteur p-adique sur les courbes elliptiques. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 1–14. Birkhäuser Boston, Mass., 1981.

Daniel Bertrand. Valuers de fonctions thêta et hauteur p-adiques. In *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*, volume 22 of *Progr. Math.*, pages 1–11. Birkhäuser Boston, Boston, MA, 1982.

Spencer Bloch. A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture. *Invent. Math.*, 58(1):65–76, 1980.

Gregory S. Call. Variation of local heights on an algebraic family of abelian varieties. In *Théorie des nombres (Quebec, PQ, 1987)*, pages 72–96. de Gruyter, Berlin, 1989.

John W. S. Cassels. *Lectures on elliptic curves.* Cambridge University Press, Cambridge, 1991.

John Coates. Height Pairings and Galois Cohomology. Course given at the University of Cambridge, 1991.

Pierre Deligne. Courbes elliptiques: formulaire d'après J. Tate. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 53–73. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

La Fontaine. *Fables.* Charpentier, Paris, 1709.

Heisuke Hironaka. Gardening of infinitely near singularities. In *Algebraic geometry, Oslo 1970 (Proc. Fifth Nordic Summer School in Math.)*, pages 315–332. Wolters-Noordhoff, Groningen, 1972.

Serge Lang. *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

Yuri Iwanovich Manin. The Tate height of points on an Abelian variety, its variants and applications. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:1363–1390, 1964.

Barry Mazur and John Tate. Canonical height pairings via biextensions. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 195–237. Birkhäuser Boston, Boston, MA, 1983.

Barry Mazur and John Tate. The p-adic sigma function. *Duke Math. J.*, 62(3):663–688, 1991.

Barry Mazur, John Tate, and J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986.

David Mumford. Bi-extensions of formal groups. In *Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968)*, pages 307–322. Oxford Univ. Press, London, 1969.

André Néron. Hauteurs et fonctions thêta. *Rend. Sem. Mat. Fis. Milano*, 46:111–135, 1976.

Joseph Oesterlé. Construction de hauteurs archimédiennes et p-adiques suivant la methode de Bloch. In *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*, volume 22 of *Progr. Math.*, pages 175–192. Birkhäuser Boston, Boston, MA, 1982.

Matthew A. Papanikolas. Canonical heights on elliptic curves in characteristic p. *Compositio Math.*, 122(3):299–313, 2000.

Bernadette Perrin-Riou. Descente infinie et hauteur p-adique sur une courbe elliptique. In *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*, volume 22 of *Progr. Math.*, pages 209–219. Birkhäuser Boston, Mass., 1982.

Bernadette Perrin-Riou. Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe. *Invent. Math.*, 70(3):369–398, 1982/83.

Bernadette Perrin-Riou. Sur les hauteurs p-adiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(6): 291–294, 1983.

Bernadette Perrin-Riou. Hauteurs p-adiques. In *Seminar on number theory, Paris 1982–83 (Paris, 1982/1983)*, volume 51 of *Progr. Math.*, pages 233–257. Birkhäuser Boston, Boston, MA, 1984.

Peter Schneider. Height pairings in the Iwasawa theory of abelian varieties. In *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*, volume 22 of *Progr. Math.*, pages 309–316. Birkhäuser Boston, Mass., 1982a.

Peter Schneider. p-adic height pairings. I. *Invent. Math.*, 69(3):401–409, 1982b.

Peter Schneider. p-adic height pairings. II. *Invent. Math.*, 79(2):329–374, 1985.

Peter Schneider. Basic notions of rigid analytic geometry. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, pages 369–378. Cambridge Univ. Press, Cambridge, 1998.

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

Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York, 1994.

John Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

John Tate. Variation of the canonical height of a point depending on a parameter. *Amer. J. Math.*, 105(1):287–294, 1983.