New York Journal of Mathematics

New York J. Math. **5** (1999) 115–120.

Explicit Local Heights

Graham Everest

Abstract. A new proof is given for the explicit formulae for the non-archimedean canonical height on an elliptic curve. This arises as a direct calculation of the Haar integral in the elliptic Jensen formula.

Contents

1. The Elliptic Jensen Formula

In complex analysis, Jensen's formula is the following statement

$$\int_0^1 \log |e^{2\pi it} - a|\, dt = \log \max\{1, |a|\},$$

where a denotes any complex number. This formula is fundamental to the development of Mahler's measure of a polynomial. For a full discussion of this subject, and a proof of Jensen's formula, see [2]. It is known (see [1]–[3]) that the global canonical height of a rational point on an elliptic curve defined over $\mathbf{Q}$ is analogous to Mahler's measure. In [1] and [2], we gave a new approach to the canonical height where each local height arises as an integral of the kind in Jensen's formula.

Let K denote any local field containing $\mathbf{Q}$, with $|.|$ denoting the absolute value on K. Let E denote an elliptic curve defined over K and let $Q \in E(K)$ denote a K-rational point. Write $Q = (x_Q, y_Q)$ for the coordinates of Q with respect to a minimal defining equation. Let $\lambda(Q)$ denote the local canonical height of Q. In [1], we pointed out the formula

$$\int_G \log |x - x_Q| d\mu_G = 2\lambda(Q), \tag{1}$$

where G is any compact group containing Q and μ_G denotes the Haar measure on G, normalised to give measure 1 to G itself. The proof of (1) is trivial: just

Received July 19, 1999.
Mathematics Subject Classification. 11C08.
Key words and phrases. Elliptic Curve, Canonical Height, Jensen's Formula.
My thanks go to the referee for helpful comments.

ISSN 1076-9803/99

integrate the local parallelogram law. In particular, (1) holds with $G = \overline{< Q >}$, the topological closure of the group generated by Q. If Q is torsion then the group G is finite with the discrete topology.

The point of view in this paper is to assume (1) and use this, with $G = \overline{< Q >}$, to give a new proof of the explicit formulae for the local canonical heights. This is a different point of view to that in [3], where the explicit formulae are shown to be the unique functions which satisfy the parallelogram law. What is gained is a new interpretation for the exotic formulae for the local canonical heights. Presumably, one could take (1) as the definition of the local canonical height and work back to the parallelogram law, but this is not pursued here.

The explicit formula in the archimedean case was worked out in [2] so it is sufficient to look at the non-archimedean case. Let p denote a prime and let K denote a finite extension of $\mathbf{Q}_p$, the p-adic rational field. Write $|.|$ for the unique extension of the p-adic absolute value to K, so that $|p| = 1/p$. Let O_K denote the valuation ring of K and let F denote the residue field. The curve and points upon it can be reduced to give a curve $E(F)$. The reduced curve might be singular. If the reduced curve is singular, the reduction of Q might or might not be singular.

Theorem 1. *Suppose Q is a point of non-singular reduction and $G = \overline{< Q >}$. Then*

$$\int_G \log|x - x_Q|\, d\mu_G = \log\max\{1, |x_Q|\}.$$

Theorem 1 is the elliptic analogue of Jensen's formula and it is true for any compact group G which contains Q by (1). Theorem 1 gives an alternative derivation of the explicit formula for the local canonical height of Q (see [3]) in the good reduction case. Note that in [3], the height is normalised to make it isomorphism invariant.

I am going to give a proof of Theorem 1 assuming $p \neq 2, 3$. This assumption allows me to use the usual Weierstrass equation,

$$y^2 = x^3 + ax + b, \quad a, b \in O_K. \tag{2}$$

Also, I assume Q is non-torsion: it makes little difference.

Proof. Let H denote the subgroup of G such that for all $P \in H$ we have

$$|x_P| > \max\{1, |x_Q|\}.$$

Then H is topologically cyclic, generated by mQ say, where $1 < m \in \mathbf{N}$. The measure of H itself is $1/m$. For any $R \in G$, consider the integral over the coset $R + H$, written

$$I_R = \int_H \log|x_{P+R} - x_Q|\, dP. \tag{3}$$

The integral in (3) is written in the classical notation to signify P as the variable of integration.

Suppose firstly that $|x_Q| > 1$. Then $|y_Q| > 1$ and (2) gives

$$|y_Q|^2 = |x_Q|^3 \quad \text{also} \quad |y_P|^2 = |x_P|^3 \text{ for } P \in H. \tag{4}$$

By the translation invariance of the measure,

$$I_R = \int_H \log|x_P|\, dP, \quad \text{for } R \equiv O \bmod H. \tag{5}$$

If $2 < m$ then the cosets $\pm Q + H$ are distinct. For $P \in H$, consider

$$|x_{P\pm Q} - x_Q| = \left| \left(\frac{y_P}{x_P}\right)^2 \left(1 \pm \frac{y_Q}{y_P}\right)^2 \left(1 - \frac{x_Q}{x_P}\right)^{-2} - x_P - 2x_Q \right|. \tag{6}$$

Expand the brackets in (6) using the binomial theorem, use (2) and extract the dominant term to give

$$|x_{P\pm Q} - x_Q| = \left|\frac{y_P y_Q}{x_P^2}\right| = \left|\frac{y_Q x_P}{y_P}\right|. \tag{7}$$

Therefore the total contribution from the cosets $O, \pm Q + H$ is

$$2\int_H \log\left|\frac{y_Q x_P}{y_P}\right| dP + \int_H \log|x_P|\, dP = \int_H \log\left|\frac{y_Q^2 x_P^3}{y_P^2}\right| dP. \tag{8}$$

Using (2) and (4), and remembering to give measure $1/m$ to H, (8) collapses to

$$\frac{3}{m}\log|x_Q|. \tag{9}$$

For cosets with R not $O, \pm Q$ mod H, $|x_{P+R} - x_Q| = |x_Q|$ so each coset contributes $\frac{1}{m}\log|x_Q|$. There are $m-3$ of these cosets in total so

$$\int_G \log|x - x_Q|\, d\mu_G = \frac{m-3}{m}\log|x_Q| + \frac{3}{m}\log|x_Q| = \log|x_Q|.$$

In the case where $m = 2$, the identity coset gives the formula in (5). For the non-identity coset, note that when $m = 2$, $|y_Q| < |x_Q|$. Then a new dominant term emerges in (6) giving

$$|x_{P+Q} - x_Q| = |1/x_P| \quad \text{that is } I_Q = -\int_H \log|x_P|\, dP. \tag{10}$$

Clearly the contributions from the two cosets cancel each other.

Next suppose that $|x_Q| \le 1$. Deal firstly with the case that $m > 2$. The integrals I_R, for R not $O, \pm Q$ mod H all vanish. This uses the non-singular reduction hypothesis. The reduced curve $E(F)$ is a group and $|x_{P+R} - x_Q| < 1$ if and only if $R \pm Q$ reduces to the point at infinity. As in (8), the total contribution from the cosets with $R \equiv O, \pm Q$ mod H is

$$\frac{2}{m}\log|y_Q|. \tag{11}$$

But the term in (11) must vanish because we cannot have $|y_Q| < 1$, otherwise $m = 2$. In the case when $m = 2$, for the identity coset, the formula in (5) remains valid. For the non-identity coset, we note that $|y_Q| < 1$ and this causes a new dominant term to emerge in (6) giving (10) as above. Once again the two contributions cancel and the proof of Theorem 1 is complete. □

2. Singular Reduction

I am going to compute the local height only in the case when Q is point of split multiplicative singular reduction on E. It is always possible to assume the reduction is of this type, by passing to a finite extension of K. Use the Tate curve together with the q-parametrisation. All the definitions needed come from Chapter V of [3]. The Tate curve has the form

$$y^2 + xy = x^3 + ax + b, \quad a, b \in O_K. \tag{12}$$

The points on the projective curve are isomorphic to the group $K^*/q^{\mathbf{Z}}$ where $q \in K$ has $|q| < 1$. The explicit formula for the x and y-coordinates of a non-identity point are given in terms of the parameter $u \in K^*$ as follows:

$$x = x_u = \sum_{n \in \mathbf{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2 \sum_{n \geq 1} \frac{n q^n}{(1 - q^n)^2}, \tag{13}$$

$$y = y_u = \sum_{n \in \mathbf{Z}} \frac{q^{2n} u^2}{(1 - q^n u)^3} + \sum_{n \geq 1} \frac{n q^n}{(1 - q^n)^2}. \tag{14}$$

Formula (13) makes it obvious that $x_u = x_{uq}$ and $x_u = x_{u^{-1}}$. Similarly for formula (14) and the y-variable. If Q corresponds to the point $u \in K^*$, take $G = \overline{< u >}$, a compact group. Assume u is chosen to lie in a fundamental domain, which means that $|q| = p^{-k} < |u| = p^{-r} \leq 1$, where r and k denote rationals.

Theorem 2. *Suppose Q is a point of split multiplicative reduction corresponding to $u \in K^*$ with $|q| = p^{-k} < |u| = p^{-r} \leq 1$ and $G = \overline{< u >}$. Then*

$$\int_G \log |x - x_u| \, d\mu_G = \begin{cases} -2 \log |1 - u| & \text{if } |u| = 1, \\ \left(\frac{r}{k} - \left(\frac{r}{k}\right)^2\right) \log |q| & \text{if } |u| < 1. \end{cases} \tag{15}$$

Theorem 2 gives an alternative derivation of the explicit formula for the local canonical height of Q in the case of split multiplicative reduction. This formula agrees with the one in Chapter VI of [3] but note that in [3], heights are normalised to make them isomorphism invariant.

Proof. Assume firstly that $|u| = 1$. If $|u - 1| < 1$ then Theorem 1 applies so assume $|u - 1| = 1$ and show the integral in (15) vanishes. Write H for the subgroup of G consisting of all $v \in G$ with $|v - 1| < 1$. Then H is topologically cyclic, generated by u^m say. Consider the integral over the coset wH, written

$$I_w = \int_H \log |x_{wv} - x_u| \, dv, \tag{16}$$

where in (16), the classical notation is chosen once again to point to the variable $v \in H$. Assuming firstly that $m > 2$, and referring to the explicit formula for the x-coordinate in (14), the only non-zero integrals come from the cosets with $w = 1, u^{\pm 1}$. Obviously,

$$I_w = \int_H \log |x_v| dv, \quad \text{when } w = 1. \tag{17}$$

When $w = u^{\pm 1}$, take note that $x_u = x_{u^{-1}}$ and use the addition formula for the Tate curve,

$$x_{vu^{\pm 1}} = \left(\frac{y_v - y_u}{x_v - x_u}\right)^2 + \left(\frac{y_v - y_u}{x_v - x_u}\right) - x_v - x_u.$$

Therefore

$$(18)\qquad |x_{vu^{\pm 1}} - x_u| = \left| \left(\frac{y_v}{x_v}\right)^2 \left(\frac{1 - y_u/y_v}{1 - x_u/x_v}\right)^2 + \frac{y_v}{x_v}\left(\frac{1 - y_u/y_v}{1 - x_u/x_v}\right) - x_v - 2x_u \right|.$$

From (14), $|x_u| = |y_u| = 1$ when $|u| = |u-1| = 1$. Also, from (12), for any $v \in H$,

$$(19)\qquad |y_v|^2 = |x_v|^3.$$

Just as in (6), expand the brackets in (18) using the binomial theorem, use (12) and (19) then extract the dominant term, to obtain

$$(20)\qquad |x_{vu^{\pm 1}} - x_u| = |y_v/x_v^2|, \text{ that is } I_{u^{\pm 1}} = \int_H \log|y_v/x_v^2|\,dv.$$

Sum the contribution from the three cosets with $w = 1, u^{\pm 1}$, and use (19), to give

$$(21)\qquad 2\int_H \log|y_v/x_v^2|\,dv + \int_H \log|x_v|\,dv = \int_H \log|y_v^2/x_v^3|\,dv = 0.$$

These calculations assumed $m > 2$. In the case when $m = 2$, (17) remains valid. For the non-identity coset, the cancelling in (18) works out differently. From the addition law,

$$x_{u^2} = \left(\frac{3x_u^2 + a}{2y_u + x_u}\right)^2 + \left(\frac{3x_u^2 + a}{2y_u + x_u}\right) - 2x_u.$$

Therefore, if $|x_{u^2}| > 1$, it follows that $|2y_u + x_u| < 1$. It is this fact which causes two extra terms in (18) to cancel and leaves

$$(22)\qquad |x_{vu} - x_u| = |1/x_v|, \text{ that is } I_u = -\int_H \log|x_v|\,dv.$$

Clearly now the contributions from the two cosets cancel each other.

Finally, deal with the case where $|u| < 1$. To ease the computation, assume $k = mr$, where $m \in \mathbf{N}$. To ease the computation further, assume $|u^m/q - 1| < 1$. In general, one would take $m \in \mathbf{N}$ smallest with $q|u^m \in O_K$ and $|u^m/q - 1| < 1$. Suppose firstly that $m > 2$. Let $H = \overline{< u^m >}$. Using the same notation as before, the contributions from the cosets wH with $w \neq 1, u^{\pm 1}$ are all equal to $\frac{1}{m}\log|x_u|$, remembering that the measure of each coset is $1/m$. There are $m-3$ of these cosets giving a total contribution of

$$(23)\qquad \frac{(m-3)}{m}\log|x_u|.$$

For the cosets $u^{\pm 1}H$, take account that $|x_{u^{\pm 1}}| < 1$. Taking the dominant term in (18),

$$(24)\qquad I_{u^{\pm 1}} = \int_H \log|x_u y_v/x_v^2|\,dv.$$

Including now the contribution from the identity coset gives

$$(25)\qquad I_1 + I_u + I_{u^{-1}} = \int_H \log|x_u^2 y_v^2/x_v^3|\,dv = \frac{2}{m}\log|x_u|,$$

where, in (25), (19) has been used. Combining (23) and (25) gives

$$\left(1 - \frac{1}{m}\right)\log|x_u| = \left(\frac{1}{m} - \frac{1}{m^2}\right)\log|q|,$$

as required. If $m = 2$ then it is easy to check that the integrals over the two cosets combine to give $\frac{1}{4}\log|q|$ as they should. $\square$

References

[1] Graham Everest and Brid Ni Fhlathuin, *The elliptc Mahler measure*, Math. Proc. Camb. Phil. Soc. **120** (1996), 13–25, MR 97e:11064, Zbl 865.11068.
[2] Graham Everest and Thomas Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer-verlag, Berlin, 1999.
[3] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-verlag, New York, 1994, MR 96b:11074, Zbl 911.14015.

School of Mathematics, University of East Anglia, Norwich, Norfolk, NR4 7TJ, England
g.everest@uea.ac.uk http://www.mth.uea.ac.uk/~h090/

This paper is available via http://nyjm.albany.edu:8000/j/1999/5-9.html.