ON THE TAYLOR COEFFICIENTS OF THETA FUNCTIONS OF CM ELLIPTIC CURVES

FERNANDO RODRIGUEZ VILLEGAS

Dedicated to the memory of Enzo R. Gentile

Abstract. Let θ be the standard theta function associated to a CM elliptic curve E and a nowhere vanishing differential ω on E, both defined over a number field. What is the significance, if any, of the Taylor coefficients of θ at 0? In this paper we do two things. First, we reformulate joint results with D. Zagier showing a relation between these coefficients and square roots of central values of Hecke L-series for certain curves. Second, we give two new proofs of a p-adic interpolation (due to A. Sofer and originally conjectured by N. Koblitz) of those square roots (suitably modified) in the case of good ordinary reduction; one of the proofs uses the relation just mentioned. For simplicity, details are only given for five curves defined over $\mathbf{Q}$; what to expect for arbitrary CM elliptic curves remains unclear, though we suspect there is a more general phenomenon.

Contents

Date: November 24, 1993.
1991 *Mathematics Subject Classification.* Primary 11G40, 11F33; Secondary 11F27, 11G05.
Key words and phrases. theta functions, elliptic curves, p-adic L-functions.
Research of the author was supported in part by an NSF grant.
This paper is in final form and no version of it will be submitted for publication elsewhere.

1. Introduction

1) Let (E,ω) be an elliptic curve with complex multiplication together with a nowhere vanishing differential on it, both defined over a number field F. Let $L \subset \mathbf{C}$ be the lattice of periods of ω and $\theta(u,L)$ for $u \in \mathbf{C}$ the standard theta function associated to L (see (2.9) for the exact definition). A fundamental result of Damerell implies that the Taylor coefficients of θ at $u=0$ are in F. We may ask:

Question: *What is the significance, if any, of the Taylor coefficients of θ at the origin?*

The relation between theta functions and Eisenstein series via logarithmic differentiation has proved to be crucial in the study of the arithmetic of the curve. However, the relation between the Taylor coefficients of a function and those of its logarithmic derivative may be very intricate (consider $1-e^u$ for example), and it is not a priori clear to us what the Taylor coefficients of θ itself might mean.

Our intention in this paper is to present some evidence for the relevance of the question we have raised. Indeed, in §3 we show how the main results of [15] can be reformulated in this setting, obtaining an answer to the question for the curves $A(l)$ studied by Gross [3], for a prime $l \equiv 3 \bmod 8$. For clarity of exposition we restrict ourselves to the simplest possible cases (five in all) where the curve $A(l)$ is defined over $\mathbf{Q}$. We obtain:

Partial answer: *For the curves $A(l)$ with $l = 11, 19, 43, 67$ or 163 the square of the $(k-1)$-st Taylor coefficient of θ at the origin is essentially the central value $L(\psi^{2k-1}, k)$, where ψ is its associated Hecke character.*

We refer the reader to §3.1 for a description of the five curves in question and to the theorem in §3.2 for the precise statement.

For other curves $A(l)$ with $l \equiv 3 \bmod 8$ prime (no longer defined over $\mathbf{Q}$) the central value is the square of *linear combinations* of Taylor coefficients of theta series associated to Galois conjugates of the curve. At present, is not clear to us what exactly to expect for arbitrary CM elliptic curves, though we suspect there is a more general phenomenon.

2) Koblitz conjectured in [10] that there exists a consistent choice of square roots of suitably modified central values $L^*(\psi^{2k-1}, k)$ having p-adic interpolation properties for all primes $p > 2$ of good ordinary reduction (we emphasize that the choice must be made independently of p). This has interesting implications in the Iwasawa theory of CM elliptic curves (cf. the work of Li Guo [4]).

The conjecture was first proved by A. Sofer in her thesis for all curves $A(l)$ with $l \equiv 3 \mod 4, l > 3$ prime. We present here two new proofs of her results (again we give details for the above curves only). The first is conceptually simple (see §4.4 for a short sketch): for primes $p > 2$ of good ordinary reduction, θ becomes a function on the formal group of E, hence a fortiori on $\hat{\mathbf{G}}_m$, to which we may associate a p-adic measure on $\mathbf{Z}_p$ by Cartier duality. The interpolation now follows from the above relation between the Taylor coefficients of θ and central values. The second is along the lines of [15] and might be of independent interest (see §4.1-4.3). We show how we can associate to any quadratic form Q (positive definite, even integral, and of even rank) a measure on the underlying lattice with values in the ring of

Katz' p-adic modular forms (extending an idea of B. Perrin-Riou [14]). For Q the norm form of certain imaginary quadratic fields we find that when evaluated at a specific trivialized elliptic curve the two variable measure associated to Q splits as the product of two identical one variable measures. This p-adic version of the factorization formula (25) of [15] then yields the desired interpolation. The precise statements are given in: §4.1 (general theta measures), §4.2 (complex and p-adic factorization formulas), and §4.3 (final p-adic interpolation).

We begin by collecting in §2 various classical results on modular forms and elliptic functions that we need, including a recursion, essentially due to Jacobi and Weierstrass, for the Taylor coefficients of θ. The reader should compare this recursion with the ones in [15].

In a way, the main theme underlying the whole paper is the heat equation, which allows us to pass from the modular variable (z in the upper-half plane) to the elliptic variable ($u \in \mathbf{C}$).

1.1. **Acknowledgments.** We would like to thanks N. Katz for his help with the theory of p-adic modular forms.

2. Preliminaries

2.1. **Classical Modular Forms.** We will consider functions f of pairs of complex numbers (ω_1, ω_2) with $\Im(\omega_2/\omega_1) > 0$. We say that such a function has weight $k \in \mathbf{Z}$ if

$$f(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k} f(\omega_1, \omega_2), \qquad \text{for all non-zero } \lambda \in \mathbf{C}.$$

We let $Sl_2(\mathbf{R})$ act on (ω_1, ω_2) via

$$(\omega_1, \omega_2) \mapsto (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2), \qquad \text{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl_2(\mathbf{R}).$$

A function invariant by $Sl_2(\mathbf{Z})$ depends then only on the lattice $L = [\omega_1, \omega_2] \subset \mathbf{C}$.

A C^∞ function $f(\omega_1, \omega_2)$ fixed by $(\omega_1, \omega_2) \mapsto (\omega_1, \omega_2 + \omega_1)$ has a Fourier expansion

$$f(2\pi i, 2\pi i z) = \sum_{n \in \mathbf{Z}} a_n(y) q^n, \qquad \Im(z) > 0, \quad q = e^{2\pi i z}.$$

This is the usual q-expansion (at $i\infty$) if f is holomorphic, in which case the $a_n(y)$'s are simply constants, and if in addition, f is also holomorphic at $i\infty$ then the a_n's are zero for $n < 0$. Any f of weight $k \in \mathbf{Z}$ may be recovered from its expansion via

$$f(\omega_1, \omega_2) = \left(\frac{2\pi i}{\omega_1}\right)^k \sum_{n \in \mathbf{Z}} a_n(y) q^n, \qquad \text{where } z = \omega_2/\omega_1 \text{ and } q = e^{2\pi i z}.$$

In particular, a classical modular form of weight k on a subgroup of $Sl_2(\mathbf{Z})$ gives rise to a holomorphic function $f(\omega_1, \omega_2)$ of weight k invariant by that subgroup.

Given (ω_1, ω_2) with $\Im(\omega_2/\omega_1) > 0$ we let $L = [\omega_1, \omega_2] \subset \mathbf{C}$ be the associated lattice and define

$$A(L) = \frac{1}{\pi} \mathrm{Area}(\mathbf{C}/L) = (\omega_2\bar{\omega}_1 - \bar{\omega}_2\omega_1)/2\pi i, \tag{2.1}$$

We let W be the differential operator acting on C^∞ functions of (ω_1, ω_2) by

$$W = \frac{-1}{A(L)}(\bar{\omega}_1 \frac{\partial}{\partial\omega_1} + \bar{\omega}_2 \frac{\partial}{\partial\omega_2}). \tag{2.2}$$

It does not preserve holomorphicity but does preserve the action of $Sl_2(\mathbf{R})$ and sends functions of weight k to functions of weight $k+2$. Moreover, if $f(\omega_1,\omega_2)$ has weight $k \in \mathbf{Z}$ then $(Wf)(2\pi i, 2\pi i z) = \partial_k(f(2\pi i, 2\pi i z))$, where ∂_k is the differential operator (acting on C^∞ functions of the upper-half plane)

$$\partial = \partial_k = \frac{1}{2\pi i}\frac{d}{dz} - \frac{k}{4\pi y}, \qquad y = \Im(z) > 0, \tag{2.3}$$

(notice that $A([2\pi i, 2\pi i z]) = 4\pi y$).

2.2. **Formulaire Elliptique.** We recall various facts from the classical theory of elliptic functions. Our basic reference will be chapter VI of Jordan's book Cours d'Analyse [7].

Given a lattice $L \subset \mathbf{C}$ we have the Weierstrass functions

$$\sigma(u, L) = u \prod_{\omega \in L\setminus\{0\}} (1 - \frac{u}{\omega}) e^{\frac{u}{\omega} + \frac{u^2}{2\omega^2}}, \qquad u \in \mathbf{C}$$

$\zeta = \sigma'/\sigma$, and $\wp = -\zeta'$, where prime indicates d/du. The function σ has weight -1 in the sense that

$$\sigma(\lambda u, \lambda L) = \lambda \sigma(u, L), \qquad \text{for all non-zero } \lambda \in \mathbf{C}. \tag{2.4}$$

We let

$$s_2(L) = \lim_{s \to 0^+} \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^2 \mid \omega \mid^{2s}},$$

$$g_2(L) = 60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^4}, \qquad \text{and} \qquad g_3(L) = 140 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^6},$$

of weights $2, 4$ and 6 respectively. It turns out that s_2 is not holomorphic while g_2 and g_3 clearly are.

Given (ω_1, ω_2) with $\Im(\omega_2/\omega_1) > 0$ we consider the associated lattice $L = [\omega_1, \omega_2]$, and define $\eta_j = \zeta(u + \omega_j, L) - \zeta(u, L)$ for $j = 1, 2$. We let $z = \omega_2/\omega_1 = x + iy$ and $q = e^{2\pi i z}$.

Remark 2.1. The definition of s_2 is due to Hecke [5, 468-474] and does not appear in [7]. We only need to know that

$$s_2(L) = \frac{\eta_1}{\omega_1} + (\frac{2\pi i}{\omega_1})^2 \frac{1}{4\pi y}. \tag{2.5}$$

We let D be the differential operator acting on C^∞ functions of (ω_1, ω_2) by

$$D = -2(\eta_1 \frac{\partial}{\partial \omega_1} + \eta_2 \frac{\partial}{\partial \omega_2}). \tag{2.6}$$

Notice that D, unlike W, preserves analyticity. It also preserves the action of $Sl_2(\mathbf{R})$ and sends functions of weight k to functions of weight $k+2$; in fact, if f has weight k then

$$Wf = \frac{1}{2} Df - k s_2 f. \tag{2.7}$$

We have

$$Dg_2 = 12 g_3, \qquad Dg_3 = \frac{2}{3} g_2^2, \qquad Ds_2 = 2 s_2^2 + \frac{1}{6} g_2,$$

and

$$D\sigma = \sigma'' + \frac{1}{12} g_2 u^2 \sigma. \tag{2.8}$$

As Jordan shows [7, p. 463] this differential equation for σ is essentially equivalent to the heat equation.

Finally, we let

$$\theta(u, L) = e^{-\frac{1}{2} s_2(L) u^2} \sigma(u, L). \tag{2.9}$$

As a function of u, θ is odd, entire, and its only zeroes are simple zeroes at points of L. It satisfies

$$\theta(u + \omega, L) = \pm e^{(\frac{1}{2}|\omega|^2 + u\omega)/A(L)} \theta(u, L) \qquad (+ \text{ if } \omega \in 2L, - \text{ if not}),$$

and therefore $e^{-\frac{1}{2}|u|^2/A(L)} |\theta(u, L)|$ is L-periodic.

We have the following expansions

$$s_2(L) = (\frac{2\pi i}{\omega_1})^2 (\frac{1}{4\pi y} + \frac{-1}{12}(1 - 24 \sum_{n=1}^{\infty} n q^n/(1 - q^n))), \tag{2.10}$$

$$g_2(L) = (\frac{2\pi i}{\omega_1})^4 \frac{1}{12}(1 + 240 \sum_{n=1}^{\infty} n^3 q^n/(1 - q^n)), \tag{2.11}$$

$$g_3(L) = (\frac{2\pi i}{\omega_1})^6 \frac{-1}{216}(1 - 504 \sum_{n=1}^{\infty} n^5 q^n/(1 - q^n)), \tag{2.12}$$

$$\theta(u, L) = \left(\frac{2\pi i}{\omega_1}\right)^{-1} e^{-\frac{1}{2}\frac{1}{4\pi y} v^2} \frac{\vartheta(v, z)}{\eta^3(z)}, \tag{2.13}$$

where

$$\vartheta(v, z) = \sum_{n \in \mathbf{Z}} (-1)^n e^{\pi i (n + \frac{1}{2})^2 z} e^{(n + \frac{1}{2})v}, \qquad v = \frac{2\pi i}{\omega_1} u, \tag{2.14}$$

and $\eta = e^{\pi i z/12} \prod_{n=1}^{\infty} (1 - q^n)$ is Dedekind's eta function.

2.3. **The Taylor coefficients of θ.** We let $r_n(L)$ be the n-th Taylor coefficient of θ about $u = 0$; precisely,

$$\theta(u, L) = \sum_{n=0}^{\infty} r_n(L) \frac{u^n}{n!}. \tag{2.15}$$

Notice that r_n is identically zero for even n.

For odd n, the Fourier expansion of r_n is of the form $\sum_{m=0}^{\infty} a_m^{(n)}(y) q^m$, where $a_m^{(n)}$ is a polynomial in $1/4\pi y$ with rational coefficients and degree $(n-1)/2$. Let $a_{m,0}^{(n)}$ be the constant term of this polynomial, then it is not hard to see from (2.13) that

$$\sum_{m=0}^{\infty} a_{m,0}^{(n)} q^m = \frac{1}{2^{n-1}} \frac{\sum_{m=0}^{\infty} (-1)^m (2m+1)^n q^{\frac{1}{2}m(m+1)}}{\prod_{m=1}^{\infty} (1 - q^m)^3}, \qquad n \text{ odd} \tag{2.16}$$

(this is, in fact, the p-adic q-expansion of r_n). In particular, $2^{n-1} a_{m,0}^{(n)} \in \mathbf{Z}$.

By (2.4) r_n has weight $n - 1$ and the same is true of the n-th Taylor coefficient of σ, which, in contrast to r_n however, is holomorphic everywhere (including $i\infty$), but its q-expansion is only integral outside 2 and 3. It follows that the n-th Taylor coefficient of σ is an isobaric polynomial in g_2 and g_3 of degree n. This together with the differential equation (2.8) allowed Weierstrass [17, V, p. 38] to give a simple recursion for these polynomials. However, we want a recursion for the Taylor coefficients of θ, which are polynomials in s_2, g_2 and g_3. We indicate below one way of doing this (compare with Jacobi [6, II, p.393]).

Lemma 2.1. *Let c be any C^∞ function of (ω_1, ω_2) independent of u. For (ω_1, ω_2) with $\Im(\omega_2/\omega_1) > 0$ let*

$$f(u, \omega_1, \omega_2) = e^{cu^2}\sigma(u, [\omega_1, \omega_2]) = \sum_{n=0}^{\infty} c_n(\omega_1, \omega_2)\frac{u^{2n+1}}{(2n+1)!}.$$

Then f satisfies the differential equation

$$Df = f'' - 4cuf' + (4c^2 + Dc + \frac{1}{12}g_2)u^2 f - 2cf,$$

where prime means d/du and D is the derivation defined in (2.6). Furthermore, the Taylor coefficients c_n satisfy, and are uniquely determined by, the following recursion

$$\begin{aligned} c_0 &= 1 \\ c_1 &= 6c \\ c_{n+1} &= Dc_n + 2c(4n+3)c_n - (2n+1)2n(4c^2 + Dc + \frac{1}{12}g_2)c_{n-1}, \qquad \text{for } n > 0. \end{aligned}$$

Proof. It follows from a calculation using the differential equation (2.8) that we leave to the reader. □

Proposition 2.2. *Fix a lattice $L \subset \mathbf{C}$. Let $s_2, g_2, g_3, \theta(u)$ be as in §1.2 and let*

$$\theta(u) = \sum_{n=0}^{\infty} c_n \frac{u^{2n+1}}{(2n+1)!}$$

be the Taylor expansion of θ about $u = 0$. Let $\Delta = g_2^3 - 27g_3^2$, $R_0 = \mathbf{Z}[\frac{1}{6}, s_2, \Delta]$, and $R = R_0[x, y]/(x^3 - 27y^2 - \Delta)$ with x, y indeterminates. Finally, let $\mathcal{D}$ be the derivation of R/R_0 satisfying $\mathcal{D}(x) = 12y$ (hence $\mathcal{D}(y) = \frac{2}{3}x^2$) and let $C_n(x, y) \in R$ be defined recursively by

$$\begin{aligned} C_0 &= 1 \\ C_1 &= -3s_2 \\ C_{n+1} &= \mathcal{D}C_n - s_2(4n+3)C_n - (2n+1)2n(s_2^2 + \frac{x}{12})C_{n-1}, \qquad \text{for } n > 0. \end{aligned}$$

Then $c_n = C_n(g_2, g_3)$.

Proof. A calculation shows that $D(g_2^3 - 27g_3^2) = 0$; now our claim follows from the previous lemma using $c = s_2$ as a constant. □

Remark 2.2. If we take $L = [2\pi i, 2\pi z]$ and let $z \to i\infty$ then $q \to 0$ and by the expansions of §1.2 $s_2 \to -1/12$, $g_2 \to 1/12$, and $g_3 \to -1/216$. Also by (2.16) we have $r_n \to 1/2^{n-1}$ for all $n \geq 0$; therefore, if we run the recursion with $s_2 = -1/12$, and $\Delta = 0$ we should get $C_n(1/12, -1/216) = 1/4^n$ for all $n \geq 0$. This can be easily verified for small n providing a consistency check on our formulas.

3. Taylor Coefficients of θ and Square Roots of Central Values

In this section we reformulate the main theorem of [15] for the simplest cases of class number one, showing that the central value $L(\psi^{2k-1}, k)$ is essentially the square of the $(k-1)$-st Taylor coefficient of the associated theta function. We start by recalling various facts about the elliptic curves in question and state the theorem in (3.5).

3.1. **The Elliptic Curves** $A(l)$**.** For a prime $l \equiv 3 \bmod 4$ let $K = \mathbf{Q}(\sqrt{-l})$ and let $A(l)$ be the elliptic curve studied by Gross in [3], which has CM by the ring of integers of K. We will only consider the cases where $l > 7$ and K has class number 1, namely, $l = 11, 19, 43, 67$, and 163; the curve $A(l)$ is then defined over $\mathbf{Q}$ and $A(l)(\mathbf{Q}) \cong \mathbf{Z}$.

For the sake of completeness we include a table of minimal models taken directly from [3, pp. 82, 86]. We use the standard notation for a generalized Weierstrass model

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

l	a_1	a_2	a_3	a_4	a_6
11	0	-1	1	-7	10
19	0	0	1	-38	90
43	0	0	1	-860	9707
67	0	0	1	-7370	243528
163	0	0	1	-2174420	1234136692

The period lattice of the Neron differential $\omega = dx/(2y+1)$ is

$$L = \Omega_{\mathbf{R}}\mathcal{D}^{-1}, \qquad \text{where } \mathcal{D} = (\sqrt{-l}), \tag{3.1}$$

and

$$\Omega_{\mathbf{R}} = \int_{A(l)(\mathbf{R})} |\omega|$$

is its positive fundamental real period. This period can be given explicitly by

$$\Omega_{\mathbf{R}} = (2\pi)^{(3-l)/4} \prod_{\substack{0<r<l \\ (\frac{r}{l})=1}} \Gamma(r/l) = 2\pi l^{1/4} \mid \eta(\frac{1+\sqrt{-l}}{2}) \mid^2, \tag{3.2}$$

where Γ is the gamma function and η is Dedekind's eta function. The first formula is due to Lerch and Chowla-Selberg and the second follows from the fact that the discriminant of ω is $-l^3$.

$A(l)$ has good reduction everywhere except at l, where it has additive reduction of Kodaira type III, and hence its conductor is l^2.

Let now $\mathcal{O}_K$ be the ring of integers of K and ψ the unique Hecke character of K that satisfies

$$\psi((\alpha)) = \varepsilon(\alpha)\alpha, \qquad \text{for } \alpha \in \mathcal{O}_K \quad \text{prime to } l, \tag{3.3}$$

where ε is the quadratic character of K of conductor $\mathcal{D}$. Then the L-series of $A(l)/\mathbf{Q}$ is $L(\psi, s)$.

We refer the reader to [3] for proofs of the above assertions about the curves $A(l)$.

We give below a table of the relevant quantities associated to the lattices (3.1); for s_2, g_2 and g_3 we used the q-expansions of §1.2 choosing $\omega_1 = \Omega_{\mathbf{R}}/\sqrt{-l}$, with $\Omega_{\mathbf{R}}$ as in (3.2), and $z = (1+\sqrt{-l})/2$; notice that then $A(L) = \Omega_{\mathbf{R}}^2/(2\pi\sqrt{l})$. Naturally, we could also have gotten g_2 and g_3 directly from the minimal model for $A(l)$.

l	s_2	g_2	g_3	$\Omega_{\mathbf{R}}$	$A(L)$
11	-2/3	88/3	-847/27	4.80242132 ...	1.10673668 ...
19	-2	152	-361	4.19055001 ...	0.64118800 ...
43	-12	3440	-38829	2.89054107 ...	0.20278890 ...
67	-38	29480	-974113	2.10882279 ...	0.08646949 ...
163	-724	8697680	-4936546769	0.79364722 ...	0.00785201 ...

Also, if $\theta(u, L) = \sum_{n=0}^{\infty} c_n u^{2n+1}/(2n+1)!$ then, using the recursion of proposition 2.2 with the values of s_2, g_2 and g_3 tabulated above, we get the following values for c_n.

n\ l	11	19	43	67	163
0	1	1	1	1	1
1	2	6	36	114	2172
2	-8	-16	440	6920	3513800
3	14	-186	-19026	-156282	3347376774
4	304	4176	-8352	-34999056	-238857662304
5	-352	-33984	33708960	3991188960	-3941159174330400

Remark 3.1. Notice that the coefficients c_n appear to be integers when a priori (by (2.16)) we expect them to be, at best, in $\mathbf{Z}[\frac{1}{2}]$; we will prove this fact in §4.2.

3.2. **The Formula.** Let ψ be the Hecke character of K defined in (3.3). For any positive integer k we may consider the L-series $L(\psi^{2k-1}, s)$; it has a functional equation as $s \mapsto 2k - s$ with root number $(-1)^k$. We will be interested in the central values $L(\psi^{2k-1}, k)$ for even k (by the above considerations these values are zero for odd k).

Theorem 3.1. *Let $l = 11, 19, 43, 67,$ or 163, $K = \mathbf{Q}(\sqrt{-l})$, and $A(l)/\mathbf{Q}$ the elliptic curve of §2.1. Let ψ be the Hecke character of K associated to $A(l)$, L the lattice of periods of a Neron differential on $A(l)$, and $\Omega_{\mathbf{R}}$ the positive fundamental real period (these are described in (3.3), (3.1), and (3.2) respectively). Let $A(L)$, $\theta(u, L)$, and $r_n(L)$ be as in (2.1), (2.9), and (2.15) respectively, so that*

$$\theta(u, L) = \sum_{n=0}^{\infty} r_n(L) \frac{u^n}{n!}, \tag{3.4}$$

is the Taylor expansion of θ about $u = 0$. Then

$$\frac{2(k-1)!}{A(L)^{k-1}\Omega_{\mathbf{R}}} L(\psi^{2k-1}, k) = r_{k-1}(L)^2, \qquad \textit{for all integers } k \geq 1. \tag{3.5}$$

Proof. Using the expansion for θ in (2.13), it is not hard to see that our claim follows from the main theorem of [15]; we leave the details of the calculation to the reader. □

Remark 3.2. It is not very difficult to extend the theorem to all curves $A(l)$ with $l \equiv 3 \bmod 8$ prime (cf. the introduction).

Remark 3.3. Note that the theorem is trivial for odd k since in that case both sides of the equation are zero.

Remark 3.4. We may view this result as a sort of abelian version of Waldspurger's theorem for these particular cases. That is: not only central values of L-series are essentially squares of algebraic numbers in a fixed finite extension of $\mathbf{Q}$, but there are systematic ways of choosing their square roots along certain families so that they are coefficients in the expansion of a particular sort of function. In the case of Waldspurger this family is formed by the quadratic twists of the L-series of a fixed modular form f of integral weight and the systematic choice determined by a form of half integral weight in Shimura correspondance with f .

In our case the family is given by the L-series of odd powers of a fixed Hecke character ψ (which we can think as twisting $L(\psi, s)$ by powers of $\psi/\bar{\psi}$) and the systematic choice determined by a theta function.

Remark 3.5. The relation between $\theta(u, L)$ and values of L-series for CM elliptic curves via the logarthmic derivative is well known and plays a crucial role in the arithmetic of these curves. We are not aware of any previous arithmetic interpretation of the Taylor coefficients of $\theta(u, L)$ itself.

Remark 3.6. Combining the theorem with the fact that $e^{-\frac{1}{2}|u|^2/A(L)}\,|\theta(u, L)|$ is L-periodic (cf. §2.2) we get the bound $L(\psi^{2k-1}, k) \leq C\sqrt{k}$, with C a constant independent of k. This type of bound is the same one gets by applying convexity arguments to the L-series directly.

4. Interpolation

4.1. ***P*-adic Modular Forms and Theta Measures.** We start with a brief discussion of theta funtions of positive quadratic forms with coefficients. We refer the reader to [13, ch. VI] for details.

Let (V, Q) be a positive definite quadratic space over $\mathbf{Q}$ of dimension $2k$, i.e: a $\mathbf{Q}$ vector space V of dimension $2k$ together with a positive definite quadratic form $Q : V \longrightarrow \mathbf{Q}$, and let $B(x, y) = \frac{1}{2}(Q(x+y)-Q(x)-Q(y))$ be the associated bilinear form. We consider even integral lattices $L \subset V$ of a rank $2k$; i.e: lattices of full rank for which $Q(m)$ is an even integer for every $m \in L$. Given a basis $v_1, \cdots, v_{2k}$ of L we form the Gram matrix $A = (B(v_i, v_j))$ and define the level of L to be the least positive integer N such that NA^{-1} is integral with even diagonal entries (this does not depend on the choice of basis). Also, we let χ be the character of $\mathbf{Q}(\sqrt{(-1)^k N})/\mathbf{Q}$. Then the theta series

$$\Theta_Q(z) = \sum_{m \in L} q^{\frac{1}{2}Q(m)}, \qquad \Im(z) > 0, \quad q = e^{2\pi i z},$$

is a modular form of weight k on $\Gamma_0(N)$ with character χ.

Given a function $f : L \to \mathbf{C}$, the series

$$\sum_{m \in L} f(m) q^{\frac{1}{2}Q(m)},$$

will not in general be a modular form of any level unless f is of a special type, two typical examples being: (1) f given by congruence conditions (increasing the level but not the weight), and (2) f a harmonic polynomial with respect to Q (increasing the weight but not the level).

In contrast, if we consider the same question p-adically we find that there is no restriction on f as long as it is continuous, since any such f can be approximated by functions of type (1). Before stating the precise result we need to introduce some notation. We refer the reader to [8] and [9] for details on p-adic modular forms and their use in p-adic interpolations.

For the rest of the paper we fix the following: $\bar{\mathbf{Q}}$ an algebraic closure of $\mathbf{Q}$, p a prime number, $\mathbf{C}_p$ the completion of an algebraic closure of $\mathbf{Q}_p$ and two embeddings $\iota_p : \bar{\mathbf{Q}} \mapsto \mathbf{C}_p$, and $\iota_\infty : \bar{\mathbf{Q}} \longrightarrow \mathbf{C}$. In what follows we will tacitly use these embeddings to pass to and from complex and p-adic settings. We let $\mathcal{O}$ be the ring of integers of $\mathbf{C}_p$.

Let $A = \bar{\mathbf{Q}} \bigcap \iota_p^{-1}(\mathcal{O})$ and for integers k and N, with $N \geq 1$ prime to p, let $M_k(\Gamma_1(Np^\infty), A)$ be the space of true modular forms of weight k on $\Gamma_1(Np^n)$ for some $n \geq 0$, which are defined over A in the sense of Katz [8, 2.4]. Concretely, these correspond (via ι_∞ on q-expansions) to classical modular forms of weight k on $\Gamma_1(Np^n)$ for some $n \geq 0$ whose q-expansion (at $i\infty$) have coefficients in $\iota_\infty(A)$.

There is an inclusion of $M_k(\Gamma_1(Np^\infty), A)$ into $\mathbf{V}$, the full ring of Katz' modular forms on $\Gamma_1(N)$ with coefficients in $\mathcal{O}$, which preserves q-expansions (via ι_p). We let $\mathbf{M}_k(\Gamma_1(Np^\infty), \mathcal{O})$ be the closure of $M_k(\Gamma_1(Np^\infty), A)$ in $\mathbf{V}$ (the inherited topology is then that of uniform limits of q-expansions).

We may now turn to the theorem, which was inspired by a similar statement in [14, 2.2.1].

Theorem 4.1. *Let p, $\mathcal{O}$ and $\mathbf{M}_k(\Gamma_1(Np^\infty), \mathcal{O})$ be as above, with $N \geq 1$ prime to p. Let (V, Q) be a positive definite quadratic space over $\mathbf{Q}$ of dimension $2k$, $L \subset V$ a (positive definite) even integral lattice of rank $2k$ and level N. Let $L_p = L \bigotimes \mathbf{Z}_p$ and $Cont(L_p, \mathcal{O})$ the space of continuous functions on L_p with values in $\mathcal{O}$. Then the following map defines a continuous linear map and hence a measure on L_p with values in $\mathbf{M}_k(\Gamma_1(Np^\infty), \mathcal{O})$.*

$$\begin{array}{ccc} Cont(L_p, \mathcal{O}) & \longrightarrow & \mathbf{M}_k(\Gamma_1(Np^\infty), \mathcal{O}) \\ \\ f & \mapsto & \sum_{m \in L} f(m) q^{\frac{1}{2}Q(m)}. \end{array}$$

Proof. It suffices to approximate f by locally constant A-valued functions (recall that $A = \bar{\mathbf{Q}} \bigcap \iota_p^{-1}(\mathcal{O})$) and notice that these give forms in $M_k(\Gamma_1(Np^\infty), A)$. $\square$

We will denote this measure by μ_L and its value on f by $\int_{L_p} f d\mu_L$.

Given a triple $\kappa = (E, \varphi, \beta)$, consisting of an elliptic curve E, an isomorphism of formal groups $\varphi : \hat{E} \longrightarrow \hat{\mathbf{G}}_m$, and an arithmetic $\Gamma_1(N)$ level structure β, all defined over $\mathcal{O}$, we may evaluate at κ to obtain a measure $\mu_{L,\kappa}$ on L_p with values in $\mathcal{O}$.

4.2. **P-adic Factorization Formulas.** Now we specialize the results of the last section to binary lattices. More specifically, let $l = 11, 19, 43, 67$, or 163 and $K \subset \bar{\mathbf{Q}}$ be the quadratic imaginary field of discriminant $-l$ and $\mathcal{O}_K$ its ring of integers. The level N of §4.1 will now be l, which we assume is not p. The symbol $\sqrt{-l}$ will always denote that square root of $-l$ in K for which $\Im(\iota_\infty(\sqrt{-l})) > 0$. Consider $(K, 2\mathbf{N}_{K/\mathbf{Q}})$ as quadratic space over $\mathbf{Q}$; then $\mathcal{O}_K$ is an even integral lattice of level l and rank 2. Let $\mu_{\mathcal{O}_K}$ be the associated measure given by theorem 4.1.

We want to interpret p-adically the factorization formula (25) of [15] as saying that the measure $\mu_{\mathcal{O}_K}$ evaluated at a particular triple κ splits as the product of two identical measures. Let us start by recalling the factorization formula.

For non-negative even integers h we define

$$\Theta^{(h)} = \sum_{\alpha \in \mathcal{O}_K} \alpha^h q^{\mathbf{N}(\alpha)} \in \mathbf{Z}[[q]]. \tag{4.1}$$

Then $\Theta^{(h)}(z)$ (with $q = e^{2\pi i z}$) is a classical modular form of weight $h+1$ on $\Gamma_0(l)$ and character $\left(\frac{*}{l}\right)$ (this is a particular case of example (2) of §4.2). Notice that the q-expansion coefficients of $\Theta^{(h)}$ at $i\infty$ are indeed in $\mathbf{Z}$. For odd h we set $\Theta^{(h)} \equiv 0$.

Theorem 4.2. *Let $l = 11, 19, 43, 67,$ or 163, $K \subset \bar{\mathbf{Q}}$ the imaginary quadratic field of discriminant $-l$, and L as in (3.1) the lattice of periods of a Neron differential of the elliptic curve $A(l)$ of §2.1. For $n \geq 0$ let $r_n = r_n(L)$ be the Taylor coefficients of $\theta(u, L)$ as in (2.15). Then for all non-negative integers j and h,*

$$\left(\frac{2\pi i}{\Omega_{\mathbf{R}}}\right)^{2j+h+1} \partial^j \Theta^{(h)}\left(\frac{l+\sqrt{-l}}{2l}\right) = r_j r_{j+h} \sqrt{-l}, \tag{4.2}$$

where $\Theta^{(h)}, \partial,$ and $\Omega_{\mathbf{R}}$ are defined in (4.1), (2.3) and (3.2) respectively and $\Im(\sqrt{-l}) > 0$.

Proof. This is a restatement of (25) of [15] applied to these cases. $\square$

Corollary 4.3. *With the notation of the theorem $r_j \in \mathbf{Z}$ for all $j \geq 0$.*

Proof. On one hand, the recursion of §2.4 shows that r_j is integral outside 2 and 3. On the other, we can rewrite (4.2) for $j = 1$ in the homogeneous form (see §1.1)

$$W\Theta^{(k)}\left(\Omega_{\mathbf{R}}, \Omega_{\mathbf{R}} \frac{l+\sqrt{-l}}{2l}\right) = r_{k+1}\sqrt{-l},$$

since $r_1 = 1$ in all cases; then the cohomological description of the operator W (see [8, IV]) guarantees that r_{k+1} is integral outside l proving that $r_j \in \mathbf{Z}$ as claimed.

Concretely, we may decompose the operator W (in its non-homogeneous form (2.3)) as:

$$\partial_k = \left(\frac{1}{2\pi i}\frac{d}{dz} - k\phi\right) + k\left(\phi - \frac{1}{4\pi y}\right),$$

where $\phi(z) = (rE_2(rz) + E_2(z))/24$, $E_2(z) = 1 - 24\sum_{n=1}^{\infty} nq^n/(1-q^n)$, $q = e^{2\pi i z}$, $y = \Im(z) > 0$, and r is an auxiliary prime (compare with (2.7)). We then verify our claim using the values of $s_2(L)$ of §3.1 and chosing r appropiately. We leave the details to the reader. $\square$

Remark 4.1. We should point out that this corollary is not entirely trivial. There is no a priori reason why the powers of 2 in the denominator of the Fourier expansion of $r_n(L)$ (cf. (2.16)) should cancel out (and indeed they do not for the curve $A(7)$ for example). The reason they do is probably related to the fact that for primes inert in K the valuations of values of modular forms typically grows along families. On the other hand, our proof works because the theorem relates r_j to values of other modular forms, which do have integral q-expansions.

Recall that ω is a Neron differential on $A(l)$ with period lattice L. The choice of basis $\Omega_{\mathbf{R}}[1, (l+\sqrt{-l})/2l]$ of L determines an arithmetic $\Gamma_1(l)$ structure β on $A(l)$, defined over $\mathbf{Z}[1/l, \zeta_l]$, where $\zeta_l \in \bar{\mathbf{Q}}$ is a primitive l-th root of unity (see [8, chap. II]).

From now on we assume that $A(l)$ has good ordinary reduction at p or, equivalently, that p splits in $K = \mathbf{Q}(\sqrt{-l})$, so that, in particular, $p > 2$. We let

$\mathcal{P} = \iota_p^{-1}(p\mathcal{O}) \cap \mathcal{O}_K$ be one of the primes of K above p and $\pi = \psi(\mathcal{P})$ the generator of $\mathcal{P}$ given by the Hecke character ψ of (3.3); the other prime is then $\bar{\mathcal{P}}$, with generator $\bar{\pi} = \psi(\bar{\mathcal{P}})$.

Let $K^\infty \subset \bar{\mathbf{Q}}$ be the union of the ray class fields of K of conductor $l\bar{\mathcal{P}}^n$ for some $n \geq 0$, $K^\infty_{\mathcal{P}}$ be its completion in $\mathbf{C}_p$, and $\mathcal{O}^\infty_{\mathcal{P}}$ be the ring of integers of $K^\infty_{\mathcal{P}}$. Finally, let $\sigma \in \mathrm{Gal}(K^\infty/K)$ be the Artin symbol at $\mathcal{P}$; it induces the Frobenius automorphism of $K^\infty_{\mathcal{P}}/\mathbf{Q}_p$.

We choose an isomorphism of formal groups over $\mathcal{O}^\infty_{\mathcal{P}}$

$$\varphi : \hat{A}(l) \longrightarrow \hat{\mathbf{G}}_m,$$

and let c be the associated p-adic period; i.e: $c \in \mathcal{O}^{\infty\times}_{\mathcal{P}}$ is such that the pull-back via φ of the standard differential on $\hat{\mathbf{G}}_m$ is $c\omega$, then

$$c^{\sigma-1} = \bar{\pi}. \tag{4.3}$$

See [8, 8.3] for this setup.

We have now a triple $\kappa = (A(l), \varphi, \beta)$ over $\mathcal{O}^\infty_{\mathcal{P}} \subset \mathcal{O}$ at which we can evaluate the measure $\mu_{\mathcal{O}_K}$ obtaining the measure $\mu_{\mathcal{O}_K,\kappa}$. It will be convenient to consider instead the measure $\mu_{\mathcal{O}_K,\kappa}/\sqrt{-l}$ (whose value on a function is that of $\mu_{\mathcal{O}_K,\kappa}$ divided by $\sqrt{-l}$).

Finally, we choose an isomorphism $\nu : \mathcal{O}_K \bigotimes \mathbf{Z}_p \longrightarrow \mathbf{Z}_p \bigoplus \mathbf{Z}_p$ so that if x, y are the standard coordinates functions on $\mathbf{Z}_p \bigoplus \mathbf{Z}_p$, then for all $\alpha \in \mathcal{O}_K$, $x \circ \nu(\alpha) = \iota_p(\bar{\alpha})$ and $y \circ \nu(\alpha) = \iota_p(\alpha)$. To ease the notation we denote by μ^* and μ respectively the measures μ_{OK} and $\mu_{\mathcal{O}_K,\kappa}/\sqrt{-l}$ transported to $\mathbf{Z}_p \bigoplus \mathbf{Z}_p$ via ν.

We fix the notation and hypothesis above for the rest of the paper. We can now reformulate the previous theorem p-adically.

Theorem 4.4. *For all non-negative integers j and k we have*

$$c^{j+k+1} \int_{\mathbf{Z}_p \bigoplus \mathbf{Z}_p} x^j y^k d\mu = r_j r_k. \tag{4.4}$$

Proof. We may assume that $j \leq k$ since both sides of (4.4) are symmetric in j and k. It is easy to check then that

$$\int_{\mathbf{Z}_p \bigoplus \mathbf{Z}_p} x^j y^k d\mu^* = (q\frac{d}{dq})^j \Theta^{(k-j)},$$

as modular forms in $\mathbf{V}$, by comparing their q-expansions (via ι_p and ι_∞). Also, in homogeneous form (see §1.1), theorem 4.2 gives

$$W^j \Theta^{(k-j)}(\Omega_{\mathbf{R}}, \Omega_{\mathbf{R}} \frac{l+\sqrt{-l}}{2l}) = r_j r_k \sqrt{-l}.$$

Now the theorem follows from the comparison theorem 8.09 and the formula 5.10.1 of [8] by evaluating at the chosen triple κ. □

We immediately get the following corollary.

Corollary 4.5. *Let $c_0 \in \mathcal{O}^\times$ be a square root of c. Then there exists an $\mathcal{O}$-valued measure μ_0 on $\mathbf{Z}_p$ such that for all non-negative integers j*

$$c_0^{2j+1} \int_{\mathbf{Z}_p} x^j d\mu_0 = r_j, \tag{4.5}$$

and

$$\mu = \mu_0 \bigoplus \mu_0,$$

as measures on $\mathbf{Z}_p \bigoplus \mathbf{Z}_p$.

Proof. Given a continuous function f on $\mathbf{Z}_p$ with values in $\mathcal{O}$ we define

$$\int_{\mathbf{Z}_p} f\,d\mu_0 = c_0^3 \int_{\mathbf{Z}_p \bigoplus \mathbf{Z}_p} f(x)y\,d\mu.$$

This clearly gives a well defined measure satisfying (4.5) since $r_1 = 1$ in all cases. Now the measures μ and $\mu_0 \bigoplus \mu_0$ agree on all functions $x^j y^k$ and hence, by Mahler's theorem, agree on all f. □

Remark 4.2. The measure is only defined up to ± 1 and we found no way of making a canonical choice.

Remark 4.3. The measure μ^* is not a product measure; what we have shown is that it is when evaluated at a particular κ.

4.3. **P-adic Interpolation.** We fix a choice of c_0 as in the above corollary hence obtaining a choice of measure μ_0. In the usual manner, we restrict μ_0 to $\mathbf{Z}_p^\times$ (still calling it μ_0) to obtain the p-adic interpolation of suitable variants of r_j.

Proposition 4.6. *Let π and $\bar{\pi}$ be the generators of the primes of K above p described earlier. Then for all non-negative integers j*

$$c_0^{2j+1} \int_{\mathbf{Z}_p^\times} x^j\,d\mu_0 = (1 - \bar{\pi}^{-1-j}\pi^j) r_j. \tag{4.6}$$

Proof. By definition,

$$\int_{p\mathbf{Z}_p} x^j\,d\mu_0 = c_0^3 \int_{p\mathbf{Z}_p \bigoplus \mathbf{Z}_p} x^j y\,d\mu.$$

On the other hand,

$$\begin{aligned} \int_{p\mathbf{Z}_p \bigoplus \mathbf{Z}_p} x^j y\,d\mu^* &= \bar{\pi}\pi^j \sum_{\alpha \in \mathcal{O}_K} \bar{\alpha}^j \alpha\, q^{p\mathbf{N}(\alpha)} \\ &= \bar{\pi}\pi^j\ \mathrm{Frob}\,(\sum_{\alpha \in \mathcal{O}_K} \bar{\alpha}^j \alpha\, q^{\mathbf{N}(\alpha)}) \end{aligned}$$

where Frob is the Frobenius map of $\mathbf{V}$ ([8, 5.5]). When we evaluate at κ we get $\bar{\pi}\pi^j c^{-\sigma(j+2)} r_j$ where σ is the Artin map at $\mathcal{P}$ as described in §4.2 ([8, 8.3]). A calculation using (4.3) gives our claim. □

Remark 4.4. If we let $a_p = \pi + \bar{\pi}$ then the proposition implies the following congruences

$$r_{j+p-1} \equiv a_p r_j \bmod p, \qquad \text{for all } j \geq 1.$$

Remark 4.5. If for some prime $p > 2$, split in $\mathbf{Q}(\sqrt{-l})$ we find that r_j is not zero modulo p for $j = 1, 3, 5, \ldots, p-2$ then the above congruences imply that r_j is non-zero for all odd j. In our case we find that we may take e.g. $p = 3, 5, 13, 23, 41$ for $l = 11, 19, 43, 57, 163$ respectively, proving that all $r_j's$ under consideration are in fact non-zero for odd j.

4.4. **P-adic θ.** As we mentioned in the introduction there is another way of proving the interpolation properties of r_j, which we describe very briefly now and hope to investigate further in a future publication.

To give an $\mathcal{O}$-valued measure on $\mathbf{Z}_p$ is the same as giving a function on the formal multiplicative group $\hat{\mathbf{G}}_m$ over $\mathcal{O}$; given such a function f, the integral of x^j against its associated measure is the value of $D^j f$ at the identity (where D is the standard derivation on $\hat{\mathbf{G}}_m$), see e.g. [9].

The function θ is not a function on the elliptic curve but it turns out that in the case of good ordinary reduction (and $p > 2$) it is in fact a function on the formal group of the curve (see [11] and also [1], [2], [12] and their references). Moreover, in that case the formal group of the curve is (non-canonically) isomorphic to $\hat{\mathbf{G}}_m$ over $\mathcal{O}$ and we may therefore associate a measure to θ whose moments are the r_j's.

References

1. I. Barsotti. Considerazione sulle funzione theta. Symp. Math. **3**, 23-63, (1970).
2. V. Cristante. p-adic theta series with integral coefficients. Astérisque **119-120**, 169-182,(1984).
3. B. Gross. Arithmetic of elliptic curves with complex multiplication. Springer Lecture Notes **776**, Springer Verlag, (1979).
4. L. Guo. General Selmer groups ans critical values of Hecke $L-$functions, to appear in Math. Ann.
5. E. Hecke. Math. Werke. Vandenhoeck & Ruprecht, Göttingen, (1959).
6. C. G. J. Jacobi. Gesammelte Werke. Chelsea Publ. Co. (1969).
7. C. Jordan. Cours d'Analyse Chap. VI Gauthier-Vilars, Paris, (1894).
8. N. Katz. p-adic interpolation of real analytic Eisenstein series. Annals of Math. **104**, 459-571, (1976).
9. N. Katz. p-adic L-functions, Serre-Tate local moduli, and ratios of solutions of differential equations. Proc. of the Int. Congress of Mathematicians, Helsinski, 365-371, (1978).
10. N. Koblitz, p-Adic congruences and modular forms of half integer weight. Math. Ann. **274** (1986) 199-220.
11. B. Mazur and J. Tate. p-adic sigma function. Duke Math. Journal (3) **62** (3), 663-688, (1991).
12. P. Norman. P-adic theta functions. Amer. Journal of Math. **107** (3), 617-661, (1985).
13. A. Ogg. Modular forms and Eisenstein series. NY, Benjamin, (1969).
14. B. Perrin-Riou. Points de Heegner et dérivéées de fonctions L p-adiques. Invent. Math. **89**, 455-510, (1987).
15. F. Rodriguez Villegas and D. Zagier. Square roots of central values of L-series. Proceedings of the Third Conference of the Canadian Number Theory Assoc., Kingston Ontario, 1991. F. Gouvea and N. Yui eds. Clarendon Press, Oxford, (1993).
16. A. Sofer. p-adic interpolation of square roots of central values of Hecke L-series. Thesis, The Ohio State University, 1993.
17. K. Weierstrass. Math. Werke Berlin, Mayer & Müller, (1915).

Department of Mathematics, Princeton University, Princeton, New Jersey 08544
E-mail address: `villegas@math.princeton.edu`