TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 355, Number 10, Pages 4137–4149
S 0002-9947(03)03277-X
Article electronically published on June 18, 2003

HEEGNER ZEROS OF THETA FUNCTIONS

JORGE JIMENEZ-URROZ AND TONGHAI YANG

Abstract. Heegner divisors play an important role in number theory. However, little is known on whether a modular form has Heegner zeros. In this paper, we start to study this question for a family of classical theta functions, and prove a quantitative result, which roughly says that many of these theta functions have a Heegner zero of discriminant -7. This leads to some interesting questions on the arithmetic of certain elliptic curves, which we also address here.

0. Introduction

Let $N \geq 1$ be an integer and let f be a nonzero meromorphic modular form of level N with algebraic Fourier coefficients. Then f can be viewed as a (meromorphic) section of a line bundle on the modular curve $X_0(N)$, and thus its zeros and poles give a divisor in $X_0(N)$ that is algebraic. These important divisors appear in the beautiful works of Rohrlich ([R]) on Jensen's formula and more recently of Bruinier, Kohnen, and Ono ([B-K-O]) on the values of modular functions. However, if we let τ be a zero or a pole of f on the upper half plane $\mathbb{H}$, then it is well known that τ is either quadratic (a Heegner point) or transcendental. So it is very interesting to isolate and understand the Heegner zeros/poles of f. We recall that a Heegner point on $X_0(N)$ of discriminant $-D$ is represented by a quadratic number $\tau = \frac{b+\sqrt{-D}}{2aN}$ with integers $a > 0$ and b.

Although Heegner points play very important roles in many branches of number theory, such as the Gross-Zagier formula, Kolyvagin's Euler system, and the Borcherds product theory, to name a few, little is known about the Heegner zeros of modular forms.

In this paper, we study the Heegner zeros for a family of classical theta functions

$$\theta_d(z) = \sum_{(x,d)=1} \left(\frac{d}{x}\right) e(x^2 z), \tag{0.1}$$

where $d \equiv 1 \pmod 4$ is a square-free integer and $e(z) = e^{2\pi i z}$. It is a modular form for $\Gamma_0(4d^2)$ of weight $\frac{1}{2}$.

When $d = 1$, the classical theta function has no zeros in the upper half plane. When $d = 5$, it is proved in [Y, Proposition 3.8] that $\theta_5(z)$ does not vanish at any Heegner points of $X_0(100)$ of any fundamental discriminant. In general, for a fixed

Received by the editors February 25, 2002 and, in revised form, December 20, 2002.

2000 *Mathematics Subject Classification.* Primary 11G05, 11M20, 14H52.

Key words and phrases. Theta functions, elliptic curves, Heegner points.

The first author was partially supported by PB90-0179 and Ramon y Cajal program of MCYT. The second author was partially supported by NSF grant DMS-0070476.

d, there are obviously only finitely many D such that θ_d vanishes at a Heegner point of $X_0(4d^2)$ of discriminant $-D$.

On the other hand, for a fixed D one may ask if there are infinitely many twisted theta functions $\theta_d(z)$ vanishing at a Heegner point of $X_0(4d^2)$ of discriminant $-D$. We first note that $X_0(4d^2)$ has a Heegner point of discriminant $-D$ if and only if every prime factor of $2d$ splits in $K_D = \mathbb{Q}(\sqrt{-D})$, and so one has to have $D \equiv 7 \mod 8$. In this paper we will settle the case where $D = 7$.

Theorem 0.1. *Let $N(X)$ be the set of positive square-free integers $d \equiv 1 \mod 4$, $d \le X$, such that every prime factor of d splits in $\mathbb{Q}(\sqrt{-7})$ and the Heegner point τ_d of $X_0(4d^2)$ with discriminant -7 is a zero of θ_d. Then*

$$|N(X)| \gg X^{1/3}/\log X.$$

The proof is based on the relation given by F. Rodriquez Villegas and T. Yang in [RV-Y] between Heegner zeros of twisted theta functions $\theta_d(z)$ and the arithmetic of a precise family of CM elliptic curves $A(D)$ constructed by B. Gross in [G1]. (See section 3 for a brief summary.) This relation allows us to restate the problem in terms of zeros of Hasse-Weil L-functions. In particular, let $A(D)$ be the elliptic curve constructed in [G1]. For any $d > 1$ let $A(D)^d$ be the d-quadratic twist of $A(D)$, and let $L(s, A(D)^d)$ be its Hasse-Weil L-function over its definition field $F_D = \mathbb{Q}(j)$ with $j = j(\frac{1+\sqrt{-D}}{2})$. Corollary 3.5 in [RV-Y] is the following:

Theorem A. *Assume $d > 1$ and $D \equiv 7 \pmod 8$. If all the prime factors of d split in K_D, then the following are equivalent.*

i) *The theta function θ_d vanishes at one (and all) of the Heegner points of $X_0(4d^2)$ with discriminant $-D$.*
ii) $L(1, A(D)^d) = 0$.

On the other hand, a celebrated theorem of Kolyvagin and Logachev ([K-L]) states in our case that $L(1, A(D)^d) = 0$ whenever $A(D)^d$ has positive rank. Therefore, the proof of Theorem 0.1 is reduced to the following theorem.

Theorem 0.2. *Let $N(X)$ be the set of positive square-free integers $d \equiv 1 \mod 4$, $d \le X$, such that $A(7)^d(\mathbb{Q})$ has a point of infinite order, and every prime factor of d splits in $\mathbb{Q}(\sqrt{-7})$. Then*

$$|N(X)| \gg X^{1/3}/\log X.$$

This kind of problem has already been considered by many authors ([G-M], [S-T], [J]), where different lower bounds are given on the number of d such that the quadratic twist $E^d(\mathbb{Q})$ has positive rank for any elliptic curve E over $\mathbb{Q}$. We will now use this type of technique for $A(7)^d$ with the extra condition that every prime factor of d is split in $\mathbb{Q}(\sqrt{-7})$. We will use polynomial twists $d = d(t)$, which arise naturally from the Weierstrass equation of the elliptic curve.

A Weierstrass equation for $A(7)$ is already given by Gross in [G2]:

$$A(7) : y^2 + xy = x^3 - x^2 - 2x - 1. \qquad (0.2)$$

In fact, in [G2] a minimal model (a Weierstrass equation with minimal discriminant) is given for any $A(D)$ whenever $D = p$ is a prime, although in general it is defined over the number field F_D. However, there is no known minimal model for $A(D)$ for composite D. This raises two interesting questions in order to extend Theorem 0.1 for a general discriminant $-D$. First of all,

Question 0.3. Is there always a minimal model of $A(D)$ for composite D? How can one construct it if it exists?

A constructive answer to these questions is expected when D is relatively prime to 6. Furthermore, for a fixed D we need pairs (d, P), where d is rational and P is of infinite order in $A(D)^d$, and so

Question 0.4. Given $D > 7$, are there infinitely many square-free integers $d > 0$ prime to D such that $A(D)^d(F_D)$ is infinite?

More generally, given an elliptic curve E over a number field F that does not descend to $\mathbb{Q}$, are there always infinitely many non-equivalent rational quadratic twists E^d having an F-point of infinite order, subject to some root number condition?

We will give an answer to both questions for $D = 15$ in section 3.

Another natural way to extend Theorem 0.1 is to study the arithmetic of d. In particular, one may ask the following question.

Question 0.5. Are there infinitely many primes p such that θ_p vanishes at a Heegner point of $X_0(4p^2)$ of discriminant -7?

An affirmative answer would follow from a general conjecture about the rank of prime twists (see [J]). In section 2, using a weighted sieve inequality in a similar way as in [J], we will prove the following theorem. Let us write $d = P_r$ if the number of primes dividing d, counting multiplicities, is bounded by r.

Theorem 0.6. *Let $N_r(X)$ be the P_r elements in $N(X)$. Then*

$$|N_6(X)| \gg X^{1/3}/\log^2 X.$$

Acknowledgment. We thank Ken Ono and D. Rohrlich for their help and suggestions during the preparation of this paper. We thank M. Stoll for his help on the proof of Proposition 3.1 with MAGMA. We thank J. Gonzalez, H. Diamond, and the referee for carefully reading an early version of this paper and for their numerous valuable comments.

1. Proof of Theorem 0.2

To clarify the exposition, let us make the following definition.

Definition. A positive integer d is "good" if $d \equiv 1 \pmod{4}$ is square-free with only prime factors splitting in $\mathbb{Q}(\sqrt{-7})$ and such that $A(7)^d(\mathbb{Q})$ has a point of infinite order.

For convenience, let $E = A(7)$ be as in (0.2). By the change of variables $16x \mapsto 28x + 1$ and $64y \mapsto y + 56x + 2$ in (0.2), we find that

$$E: \quad y^2 = (28x - 31)((28x + 11)^2 + 28) = p(x)F(x). \tag{1.1}$$

For any integer $t > 1$ let us write $p(t)F(t) = d(t)B(t)^2$ for $d(t)$ square-free and $B(t)$ a positive integer. We will consider the twist $E^{d(t)}$ together with the point $(t, B(t)) \in E^{d(t)}(\mathbb{Q})$. For these twists we have the following lemma.

Lemma 1.1. *Let the notation be as above. If $p(t) = 28t - 31$ is prime, then $d(t)$ is good and the root number of $E^{d(t)}$ is $+1$, with at most a finite number of exceptions.*

Proof. Clearly $p(t) \equiv F(t) \equiv 1 \pmod 4$. So $B(t)$ is odd and $B(t)^2 \equiv 1 \pmod 4$, and thus $d(t) \equiv 1 \pmod 4$. Next, for every prime $l | d(t)$, either $l = p(t)$ or $F(t) \equiv 0 \pmod l$. When $l = p(t)$, one has $(\frac{l}{7}) = (\frac{-31}{7}) = 1$, and so l is split in $\mathbb{Q}(\sqrt{-7})$. When

$$F(t) = (28t + 11)^2 + 28 \equiv 0 \mod l,$$

one sees that -7 is a square modulo l. So l is again split in $\mathbb{Q}(\sqrt{-7})$, and thus every prime factor of $d(t)$ is split in $\mathbb{Q}(\sqrt{-7})$.

On the other hand, in [G-M] the authors proved that for all but finitely many t, the point $(t, B(t))$ of $E^{d(t)}(\mathbb{Q})$ has infinite order. Finally, $d(t) > 0$ implies that $E^{d(t)}$ has root number 1 (see [G1, Cor. 19.2.8]). □

Lemma 1.2. *Let the notation be as above. For any integer d, let $P(d)$ be the set of primes $p = 28t - 31 \in (T^{1/2}, T)$ such that $d(t) = d$. Then $|P(d)| \leq 5$ for $T \gg 1$.*

Proof. For $0 \leq i \leq r$, let t_i be such that $p(t_i) \in P(d)$. Noting that

$$F(x) = (28x + 53)(28x - 31) + 2^8 \times 7,$$

we see that $(F(t), p(t)) = 1$ for any integer t. In particular, it immediately follows that $p(t_i) | d$ for $0 \leq i \leq r$. Hence,

$$F(t_0) = B(t_0)^2 (d/p(t_0)) = B(t_0)^2 \frac{d}{\prod_{i=0}^r p(t_i)} \prod_{i=1}^r p(t_i) \geq B(t_0)^2 \prod_{i=1}^r p(t_i) \geq T^{r/2},$$

since $p > T^{1/2}$ for any $p \in P(d)$.

On the other hand $t_0 \leq T$; so $F(t_0) \ll T^2$ and thus $r \leq 4$, which completes the proof of the lemma. □

Proof of Theorem 0.2. For $T \gg 1$, let $X = p(T)F(T) \asymp T^3$. Lemmas 1.1 and 1.2 allow us to establish the lower bound

$$|N(X)| \gg |\{T^{1/2} < p < T : p \equiv -31 \pmod{28} \text{ is prime}\}|.$$

Theorem 0.2 now follows easily from the Prime Number Theorem in arithmetic progressions. □

Remark 1.3. The proof of Theorem 0.2 explicitly constructs a twist d and a point of infinite order in $A(7)^d(\mathbb{Q})$. In practice, it is possible to take $p(t)$ to be composite. For example, choosing $t = 2$, we find that $p(t) = 5^2$, and direct computation using the same procedure shows us that $A(7)^{4517}$ has the point $(57/16, 119/64)$ of infinite order. Thus $L(1, \chi_{7,4517}) = 0$ and so θ_{4517} vanishes at the Heegner point of $X_0(4 \cdot 4517^2)$ with discriminant -7. Incidentally, the smallest quadratic twist of $A(7)$ to have a point of infinite order is $A(7)^{53}$.

2. Proof of Theorem 0.6

To prove Theorem 0.6, we will bound the number of prime factors of the good integers found in Theorem 0.2. For this purpose we will use a linear weighted sieve inequality for the polynomial $p(x)F(x)$ defined in the previous section.

In particular, we will use a direct application of Theorem 9.3 in [H-R, p. 253]. For completeness, we include the hypotheses and state a particular case of this theorem, which we shall refer to as Theorem T1.

Let $X \gg 1$, and consider a set A of integers in $[1, X]$. We denote $A_d = \{a \in A : d|a\}$. Suppose that for any square-free d we can write

$$|A_d| = X\frac{\omega(d)}{d} + R_d \tag{2.0}$$

for some multiplicative function $\omega(d)$ and a function R_d satisfying the following conditions:

$$(\Omega_1) \qquad 1 \le \frac{1}{1-\omega(p)/p} \le C_1, \text{ for any prime } p,$$

$$(\Omega_2^*(1)) \qquad -C_2 \log\log 3X \le \sum_{v \le p < w} \frac{\omega(p)}{p}\log p - \log\frac{w}{v} \le C_2, \qquad 2 \le v \le w,$$

$$(\Omega_3) \qquad \sum_{z \le p < y} |A_{p^2}| \le C_3\left(\frac{X\log X}{z} + y\right), \qquad 2 \le z \le y,$$

$$(R(1,\alpha)) \qquad \sum_{d < X^{\alpha}/(\log X)^{C_4}} \mu^2(d)3^{\nu(d)}|R_d| \le C_5\frac{X}{\log^2 X}, \qquad X \ge 2,$$

for absolute constants C_1, C_2, C_3, C_4, C_5 and $\alpha > 0$. Then we have

Theorem T1. *Let A be a set satisfying the above conditions* (2.0), (Ω_1), $(\Omega_2^*(1))$, (Ω_3), *and* $(R(1,\alpha))$. *Assume further that $|a| < X^{\alpha(r-1)+\varepsilon}$ for all $a \in A$ and some $\varepsilon > 0$. Then there exists a constant $X_0(r) > 0$ such that*

$$|\{a \in A : a = P_r\}| \ge \frac{1}{7\alpha}\prod_p \frac{1-\omega(p)/p}{1-1/p}\frac{X}{\log X},$$

for $X \ge X_0(r)$. Here $a = P_r$ whenever a has at most r prime factors, counting multiplicity, as in Theorem 0.6.

Let $p(x)$ and $F(x)$ be defined as in the previous section. In order to prove Theorem 0.6 for a given large X, we have to apply Theorem T1 to the sequence $\{p(t)F(t) < X : p(t) \text{ prime}\}$. This can be written as

$$\{pG(p) < X : p \equiv -31 \pmod{28}\}, \tag{2.1}$$

where $G(x) = F((x+31)/28) = x^2 + 84x + 1792$.

We will deduce Theorem 0.6 from the application of Theorem T1 to the general sequence of polynomials evaluated at primes,

$$A = A(f,k,l) = \{f(p) : p \le x \text{ prime}, p \equiv l \pmod{k}\}, \tag{2.2}$$

for a pair of fixed integers $(k,l) = 1$ and an irreducible polynomial $f(x) \in \mathbb{Z}[x]$. Hence, our first goal is to verify that (2.2) satisfies the hypotheses of Theorem T1.

The sequence in (2.2), given as Example 6 in [H-R, p. 22], is a generalization of that in Theorem 9.8 [H-R, p. 261] with the additional condition that the primes are in a certain congruence class. As in [H-R], to verify that the sequence (2.2) satisfies the conditions in Theorem T1, we first prove a series of technical lemmas.

For any given integer q, let

$$E(x,q) = \max_{2 \le y \le x} \max_{\substack{1 \le h \le q \\ (h,q)=1}} \left|\pi(y;h,q) - \frac{\mathrm{li}(y)}{\varphi(q)}\right|,$$

where $\pi(y;h,q)$ is the number of primes congruent to h modulo q and less than y, and

$$\mathrm{li}(y) = \int_2^y \frac{dt}{\log t}$$

is the usual logarithmic integral function li, which is asymptotic to $\frac{y}{\log y}$ as y goes to infinity.

Lemma 2.1. *Let h, k be positive integers, and suppose $k \leq \log^c x$. Given any positive constant U_1, there exists a positive constant $C_1 = C_1(h,c,U_1)$ such that*

$$\sum_{d<x^{1/2}/k\log^{C_1} x} \mu^2(d) h^{\nu(d)} E(x,[k,d]) = O_{h,c,U_1}\left(\frac{x}{\varphi(k)\log^{U_1} x}\right),$$

where $\mu(d)$ is the Möbius function, $\varphi(d)$ is the Euler function and $\nu(d)$ counts the number of prime factors of d.

Proof. The proof is the argument of Lemma 3.5 of [H-R, p. 115], replacing $E(x,kd)$ by $E(x,[k,d])$ and noting that since $[k,d] \leq kd$, we have

$$\sum_{d<x^{1/2}/k\log^{C_1} x} E(x,[k,d]) \leq \sum_{d<x^{1/2}/\log^{C_1} x} E(x,d).$$

□

We now introduce some notation. Let $f(x)$, k and l be as in (2.2). For a square-free integer d, let $D=(d,k)$, and

$$\rho_{k,l}(d) = \begin{cases} |\{1 \leq m \leq d/D\,,\ (m,d/D)=1\,, f(m) \equiv 0 \pmod{d/D}\}| & \text{if } D | f(l), \\ 0 & \text{if } D \nmid f(l). \end{cases}$$

It is easy to check that, as in Example 6 in [H-R], $\rho_{k,l}(d)$ is a multiplicative function.

Lemma 2.2. *Let l and k be relatively prime integers. Let $f(x)$ be an irreducible polynomial of degree g with integer coefficients such that $(f(l),k)=1$. Consider the set $A = \{f(p) : p \leq x \text{ prime}, p \equiv l \pmod{k}\}$. Suppose that the function given by $\rho(d) = |\{1 \leq m \leq d\,, f(m) \equiv 0 \pmod{d}\}|$ satisfies*

$$\rho(p) \leq p-1 \quad \text{and} \quad \rho(p) < p-1 \quad \text{if} \quad p \leq g+1\,, p \nmid f(l). \tag{2.3}$$

Then for any square-free d, we have the following relations.

a) *For $X = \frac{\mathrm{li}(x)}{\varphi(k)}$, we have*

$$|A_d| = X\frac{\omega(d)}{d} + R_d,$$

where $\omega(d) = \rho_{k,l}(d)\varphi(D)\frac{d}{\varphi(d)}$ is multiplicative and

$$|R_d| \leq \rho(d)\left(E(x,[k,d])+1\right).$$

b) *The functions $\omega(d)$ and R_d satisfy conditions (Ω_1), $(\Omega_2^*(1))$, (Ω_3) and $(R(1,\alpha))$.*

Proof. a) The proof is the argument in Examples 5 and 6 in [H-R]. Note that $\omega(\cdot)$ is multiplicative, since $\rho_{k,l}(\cdot)$ is multiplicative as remarked above.

b) We take the four conditions in order.

• We first verify condition (Ω_1). If $p|k$, then $p\nmid f(l)$ and $\omega(p)=0$. Otherwise,

$$\omega(p)=\begin{cases}\frac{\rho(p)-1}{p-1}p & \text{if } p|f(l),\\ \frac{\rho(p)}{p-1}p & \text{if } p\nmid f(l).\end{cases}$$

By (2.3) we have $\omega(p)\le(1-1/g)p$ whenever $p\le g+1$. Meanwhile if $p\ge g+2$, then by Lagrange's Theorem and (2.3) we have $\rho(p)\le g$, and so $\omega(p)\le\frac{g}{p-1}p\le(1-1/(g+1))p$. Therefore Ω_1 is satisfied with $C_1=g+1$.

• Condition $(\Omega_2^*(1))$ is a trivial consequence of Nagel's result [N] (see [H-R, p. 18]), $\sum_{p<x}\rho(p)\log p/p=\log x+O(1)$, and partial summation.

• Now we explain how to guarantee condition (Ω_3). If $\mathcal{D}$ is the discriminant of f, then it is well known that $\rho(p^2)\le g\mathcal{D}^2$ (see [H-W]). Hence,

$$|A_{p^2}|\le|\{n\le x\,:\,f(n)\equiv 0\pmod{p^2}\}|\ll\frac{x}{p^2}+1\ll\frac{X\log X}{p^2}+1,$$

which trivially gives (Ω_3).

• Now we verify condition $(R(1,\alpha))$. We have, by Lagrange's Theorem, that $\rho(p)\le g$, and so $\rho(d)\le g^{\nu(d)}$. Therefore, by a) we have

$$|R_d|<g^{\nu(d)}(E(x,[k,d])+1). \tag{2.4}$$

□

Lemma 2.3. *Under the hypotheses of Lemma* 2.2*, for* $x\gg 1$ *we have*

$$\begin{aligned}&|\{p\le x\ \textit{prime}: p\equiv l\,(\mathrm{mod}\ k)\,:\,f(p)=P_{2g+1}\}|\\ &\quad\ge\frac{2}{7}\prod_{p|k}\frac{p}{p-1}\prod_{p|f(l)}\frac{1-(\rho(p)-1)/(p-1)}{1-1/p}\prod_{p\nmid f(l),p\nmid k}\frac{1-\rho(p)/(p-1)}{1-1/p}\frac{x}{\log^2 x}.\end{aligned}$$

Proof. Apply Theorem T1 with $\alpha=1/2$ and $r=2g+1$. The result then follows from

$$\frac{\mathrm{li}(x)}{\varphi(k)\log(\mathrm{li}(x)/\varphi(k))}\ge\frac{\mathrm{li}(x)}{\varphi(k)\log\mathrm{li}(x)}\ge\frac{x}{\varphi(k)\log^2 x}.$$

□

Proof of Theorem 0.6. Let $G(x)$ be as in (2.1). In this case we have $G(-31)=149$, and so (2.3) is trivial for this polynomial. Hence we can apply Lemma 2.3 to the polynomial $G(x)$, $k=28$, $l=-31$ and $x=X^{1/3}$ to deduce Theorem 0.6. □

3. The case $D=15$

Let $K=\mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field with discriminant $-D$, and let H be the Hilbert class field of K. Gross showed, using the theory of complex multiplication ([G1, Theorem 9.1]), that producing an elliptic curve over H with CM by $\mathcal{O}_K$ is the same as giving its j-invariant together with an algebraic Hecke character of H with values in K such that

$$\chi(\alpha\mathcal{O}_H)=N_{H/K}\alpha \tag{3.1}$$

for all $\alpha\equiv 1\ (\mathrm{mod}\ {}^*\mathfrak{M})$, where $\mathfrak{M}$ is some integral ideal of H. The relation between χ and the elliptic curve A is that

$$\chi(\mathfrak{A})+\overline{\chi(\mathfrak{A})}=\#k+1-\#A(k)$$

for every integral ideal $\mathfrak{A}$ of H prime to $\mathfrak{M}$ (conductor of A), where k is the residue field at $\mathfrak{A}$. When $D \equiv 3 \pmod 4$, let ϵ be the quadratic character $\epsilon : (\mathcal{O}_K/\sqrt{-D})^* \cong (\mathbb{Z}/D)^* \longrightarrow \{\pm 1\}$, where the last map is the Dirichlet character $(\frac{-D}{\cdot})$. So

$$\epsilon_D(\alpha\mathcal{O}_K) = \epsilon(\alpha)\alpha \tag{3.2}$$

is a well-defined homomorphism from the group of principal ideals of K to K^*. Since the norms of ideals of H to K are always principal by class field theory, this gives rise to a unique Hecke character $\chi_H = \epsilon_D \circ N_{H/K}$ of H satisfying the condition (3.1). So there is a unique elliptic curve $A(D)$ over H with associated Hecke character χ_H and j-invariant $j(A(D)) = j(\frac{1+\sqrt{-D}}{2})$. Furthermore, [G1, Theorem 10.2] asserts that $A(D)$ descends to two isogenous elliptic curves over $F = \mathbb{Q}(j)$, which we still denote by $A(D)$. One can distinguish the two elliptic curves by their minimal discriminants, as Gross did in the case where D is a prime. On the other hand, ϵ_D extends to h_D the so-called canonical Hecke characters of K, denoted by χ_D. Here h_D is the ideal class number of K. Canonical Hecke characters differ from each other by ideal class characters. By the theory of complex multiplication, one sees that

$$L(s, A(D)/F) = L(s, \chi_H) = \prod L(s, \chi_D), \quad L(s, A(D)^d/F) = \prod L(s, \chi_{D,d}),$$

where the product runs over all canonical Hecke characters of K, and $\chi_{D,d} = \chi_D(\frac{d}{\cdot}) \circ N_{K/\mathbb{Q}}$ is the quadratic twist of χ_D. We remark that all sides in the above identities are independent of the choices of $A(D)$ or χ_D.

The arithmetic and the L-functions of $A(D)$ and its quadratic twists have been extensively studied by Gross, Rorhlich, Rodriguez-Villegas, and the second author, among others. For example, it is now known ([G1], [M-R], [M-Y]) that $A(D)(F)$ has Mordell-Weil rank 0 or h_D, depending on whether $D \equiv 7 \pmod 8$ or $3 \pmod 8$, and that the Tate-Shafarevich group is finite. When D is a prime number, Gross also determined its torsion group ([G1]) and its minimal model ([G2]). It seems to be of independent interest to extend Gross's work to general D. In this section we deal with the special case $D = 15$, and answer Questions 0.3 and 0.4 affirmatively in this case. From now on, let $K = \mathbb{Q}(\sqrt{-15})$, and let

$$j = j\left(\frac{1+\sqrt{-15}}{2}\right) = -\frac{191025 + 85995\sqrt{5}}{2}. \tag{3.3}$$

So $F = \mathbb{Q}(j) = \mathbb{Q}(\sqrt{5})$, and $H = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ is the Hilbert class field of K. Let $\epsilon = \frac{1+\sqrt{5}}{2}$ be a fundamental unit of F. Then there are algebraic integers $m, n \in \mathcal{O}_F$ such that ([B, p. 57])

$$m^3 = -\epsilon j \quad \text{and} \quad -3n^2 = j - 1728.$$

Similarly to [G1, p. 80], for any nonzero number $c \in F^*$ we set

$$E_c : y^2 = x^3 - 9\epsilon m c^2 x + 18\epsilon^2 n c^3. \tag{3.4}$$

Then $j(E_c) = j$ and $\Delta(E_c) = -2^{12}3^9\epsilon^4 c^6$. Let

$$E = E_{\frac{1}{12\epsilon}} : \quad y^2 = x^3 - \frac{1}{16}(15 + 12\sqrt{5})x + \frac{7}{64}(6 + 4\sqrt{5}). \tag{3.5}$$

Then $\Delta(E) = -3^3\epsilon^{-2}$, and E_c is just the quadratic twist $E^{12\epsilon c}$ of E. We mention in passing that the denominators in equation (3.5) are for the purpose of getting the minimal discriminant $3^3\mathcal{O}_F$ (see Proposition 3.1 below) and can be easily cleared. Indeed, E is isomorphic to

$$E = E^4: \quad y^2 = x^3 - (15+12\sqrt{5})x + 7(6+4\sqrt{5}), \tag{3.5′}$$

which has integral coefficients.

Proposition 3.1. (1) *The CM elliptic curve E has minimal discriminant $3^3\mathcal{O}_F$ and conductor $3^2\mathcal{O}_F$. In particular, it has good reduction everywhere outside $3\mathcal{O}_F$.*

(2) *E is F-isogenous to its Galois conjugate,*

$$E': \quad y^2 = x^3 - \frac{1}{16}(15-12\sqrt{5})x + \frac{7}{64}(6-4\sqrt{5}).$$

(3) *The elliptic curve E is F-isogenous to the quadratic twist E^{-3}. In particular, E^{-3} has minimal discriminant $3^9\mathcal{O}_F$ and has good reduction everywhere outside* 3.

Proof. Direct calculation gives $j(E_c) = j$ and $\Delta(E_c) = -2^{12}3^9\epsilon^4c^6$. In particular, $\Delta(E) = -3^3\epsilon^{-2}$, and so E has good reduction everywhere outside $6\mathcal{O}_F$. The substitution

$$x = x_1 - \frac{1}{4}, \quad y = y_1 + \frac{1}{2}x_1 + \frac{\epsilon}{2}$$

gives an integral model of E with the same Δ:

$$E: y_1^2 + x_1y_1 + \epsilon y_1 = x_1^3 - x_1^2 - 2\epsilon x_1 + \epsilon.$$

This implies that E has good reduction at 2. So E has good reduction everywhere outside $3\mathcal{O}_F$. Notice that E has CM, and thus its conductor is a square that divides Δ. So its conductor is $3^2\mathcal{O}_F$. This proves (1).

To prove (2), we compute the 5th division polynomial of E using the equation (3.5′) and MAGMA. It has a quadratic factor $x^2 - 2\sqrt{5}x + \frac{6\sqrt{5}}{5} - 1$. Using the algorithm in [C, p. 99], one then finds that E is 5-isogenous to the elliptic curve

$$y^2 = x^3 - 5^2(15-12\sqrt{5})x + 5^3 7(6-4\sqrt{5})$$

over F, which is isomorphic to E'. The same procedure shows that E' is 3-isogenous to E^{-3}. This, combined with (2), shows that E is 15-isogenous to E^{-3}, proving (3). Incidentally, this isogeny becomes the complex multiplication by $\sqrt{-15}$ over $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$. □

Theorem 3.2. (1) *The two elliptic curves $A(15)$ over F are $A(15)_1 = E^{-\sqrt{5}(2+\sqrt{5})}$ and $A(15)_2 = A(15)_1^{-3}$.*

(2) *There are infinitely many square-free integers d such that $A(15)^d(F)$ is infinite and such that the functional equation of $L(s, \chi_{15}^d)$ has positive sign. Here $A(15) = A(15)_i$ with $i = 1, 2$.*

It is interesting to note that the functional equation for $L(s, A(15)^d)$ has positive sign. However, it is trivially zero at $s = 1$ if the root number of χ_{15}^d is -1. It is also interesting to note that $A(15)$ has a quadratic twist that has good reduction everywhere outside 3, including the prime $\sqrt{5}$ of $\mathbb{Q}(\sqrt{5})$.

Proof. Let $E1 = E^{-\sqrt{5}(2+\sqrt{5})}$. Since $-\sqrt{5}(2+\sqrt{5}) \equiv 1 \pmod 4$, the quadratic twist does not induce bad reduction at 2, and so the conductor of $E1$ is $(3\sqrt{5}\mathcal{O}_F)^2$. The same proof as in Proposition 3.1 shows that $E1$ is a CM $\mathbb{Q}$-curve, and thus that the scalar restriction $B = \mathrm{Res}_{F/\mathbb{Q}}E1$ is a CM abelian variety over $\mathbb{Q}$ with CM by H such that all its complex multiplications are defined over K. This implies, by the theory of complex multiplication, that there is an algebraic Hecke character χ of K with values in H such that

$$L(s, E1) = L(s, B) = L(s, \chi)L(s, \chi^\sigma),$$

where $\sigma \in \mathrm{Gal}(H/K)$ is nontrivial. Looking at the functional equation of both sides, one sees that the conductor of χ is $\sqrt{-15}\mathcal{O}_K$, the same as that of χ_{15}. So $\phi = \chi\chi_{15}^{-1}$ is a Hecke character of K of finite order and with good reduction everywhere. This means that ϕ is an ideal class character of K. Replacing χ_{15} by $\chi_{15}\phi$ if necessary, we obtain $\chi = \chi_{15}$. Recall that $j(E1) = j$; so $E1$ is one of $A(15)$ over F, the other one is $E1^{-3}$. This proves (1).

To prove (2), we take $A(15)$ to be $E1$. A substitution $x \mapsto x + \frac{1}{4}(35 + 16\sqrt{5})$ gives

$$E1 : y^2 = \frac{x}{4} f(x),$$

where

$$f(x) = 4x^2 + 105x + 1410 + (48x + 630)\sqrt{5}.$$

Assume that x is a rational number and that

$$f(x) = d_1(a + \sqrt{5})^2 \tag{3.6}$$

with $a, d_1 \in \mathbb{Q}$. Then $(x, \frac{1}{2}(a+\sqrt{5}))$ is a nontrivial F-rational point of the quadratic twist $E1^d$ with $d = xd_1$. Since a, d_1, and x are rational numbers, (3.6) implies that

$$\frac{4x^2 + 105x + 1410}{a^2 + 5} = \frac{48x + 630}{2a} = d_1.$$

Substituting $a = \frac{8x+105}{z}$, one has

$$A : -15z^2 + (1410 + 105x + 4x^2)z - 192x^2 - 5040x - 33075 = 0 \tag{3.7}$$

and the following fact: If (x, z) is a rational solution of (3.7), then $E1^d$ with

$$d = 3xz \tag{3.8}$$

has an F-rational point that is of infinite order for all but finitely many d ([Go, Proposition 1]). Now part (2) of the theorem follows from the following steps.

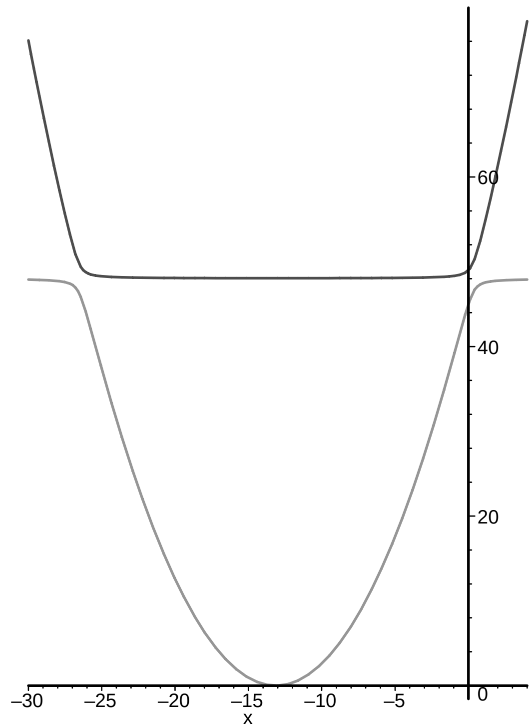
1. The equation (3.7) defines an elliptic curve A over $\mathbb{Q}$. It has two "infinite" points, the horizontal one $O = [0, 1, 0]$ and the vertical one $[1, 0, 0]$ in terms of homogeneous coordinates $[x, z, y]$. We choose O to be the identity. One can check that $Q_0 = (17/28, 2307/49)$ is of infinite order. The graph below is the real locus of A in the (x, z)-plane.

2. For each rational point $P = (x, z) \in A(\mathbb{Q})$, let $d(P)$ be the square-free part of $3x(P)z(P)$. Then for every square-free integer $d \neq 0$, there are only finitely many $P \in A(\mathbb{Q})$ such that $d = d(P)$. Indeed, for a fixed d, if $3xz = dy^2$, then (3.7) gives rise to

$$C : -15d^2y^4 + 3d(1410 + 105x + 4x^2)xy^2 - 27(8x + 105)^2x^2 = 0.$$

This defines an algebraic curve C that has 2 double points $(0, 0)$ and $(-\frac{105}{8}, 0)$ and is nonsingular everywhere. So the normalization of C has genus $6 - 2 = 4 > 1$ generically, and thus has finitely many rational points. This implies that A produces infinitely many square-free $d(P)$'s.

3. It is known that the root number of χ_{15}^d is the sign of d when $(15, d) = 1$. Since 5 is a square in F, we can replace d by $d/5$ without affecting the curve or the



root number. So we only need to make sure that $3 \nmid d$. Let $Q_0^0 = (\frac{17}{28}, \frac{2307}{49}) \in A(\mathbb{Q})$, and for each integer $r > 0$, let $Q_r^j = (-1)^j 2Q_{r-1}^0$ for $j = 0, 1$. For example,

$$Q_1^0 = \left(-\frac{671}{112}, \frac{867}{64}\right), \quad Q_1^1 = \left(-\frac{2269}{112}, \frac{867}{64}\right),$$

and

$$Q_2^0 = \left(\frac{-8520616668059}{290795014496}, \frac{126353913920688}{2639880802441}\right),$$

$$Q_2^1 = \left(\frac{887247537539}{290795014496}, \frac{126353913920688}{2639880802441}\right).$$

Claim. Let $x_r^j = x(Q_r^j)$ and $z_r = z(Q_r^j)$. Then the x-coordinates x_r^j are relatively prime to 3 (i.e., in $\mathbb{Z}_3^*$), and

$$z_r \equiv -6 \mod 9, \quad \text{but} \quad z_r \not\equiv -6 \mod 27. \tag{3.9}$$

First notice that by rewriting (3.7) as a polynomial equation of x, one sees that

$$x_r^0 x_r^1 = -\frac{15}{4}\frac{(z_r - 45)(z_r - 49)}{z_r - 48}, \quad x_r^0 + x_r^1 = -\frac{105}{4}. \tag{3.10}$$

So (3.9) would imply that $x_r^0 x_r^1$ is prime to 3. This implies in turn by (3.10) that x_r^j is prime to 3. We prove (3.9) by induction. Direct computation using MAPLE gives

$$z(2Q) = \frac{3}{4}\frac{f(x,z)}{g(x,z)},$$

where $x = x(Q), z = z(Q)$, and

$$\begin{aligned} f(x,z) &= 64x^6z - 2048x^6 - 80640x^5 + 2800x^5z + 6200zx^4 + 208080x^4 \\ &+ 80z^2x^4 + 47565000x^3 + 12600z^2x^3 - 1604400zx^3 - 2400z^3x^2 + 876121425x^2 \\ &- 42374700zx^2 + 617700z^2x^2 - 420336000zx + 6604510500x + 8914500z^2x \\ &- 63000z^3x + 4500z^4 + 59625000z^2 + 21918802500 - 846000z^3 - 1867122000z, \end{aligned}$$

and

$$g(x,z) = x^2(-30z + 1410 + 105x + 4x^2)^2.$$

When $3 \nmid x$ and z satisfies (3.9), one sees immediately from the formulas that $\mathrm{ord}_3 z(2Q) = 1$. By (3.9), one has $z \equiv 3 \pmod 9$, and so

$$z(2Q)/3 + 2 \equiv \frac{3}{x^2+3x+3} \mod 9.$$

This proves that $z(2Q)$ also satisfies (3.9), and thus the claim.

So we see that $d(Q_r^j)$ is always relative prime to 3. To show that there are infinitely many $d(Q_r^j) > 0$, it is enough to make the following observation: If $x(Q)$ and $x(-Q)$ are both negative, then at least one of the four numbers $x(\pm 2Q)$ and $x(\pm 4Q)$ is positive. This can be easily seen from MAPLE. To be brief, we can assume that $-105/8 < x(Q) < 0$. If Q is in the upper branch, then one of the two numbers $x(\pm 2Q$ is positive. Let $x_0 = -.768...$ be the reflective point of the lower branch of $A(\mathbb{R})$ on the right of $x = -105/8$. When $-105/8 < x(Q) < x_0$, the tangent line at Q is below the curve (concave up) and hits the curve at $-2Q$ with $x(-2Q) > 0$. When $x_0 < x < 0$, the same consideration gives $x(2Q) < x_0$. So either $x(4Q)$ or $x(-4Q)$ is positive. Since x_0 is not a rational number, we do not need to worry about $x = x_0$. This completes the proof of Theorem 3.2. □

References

[B] W. E. H. Berwick, *Modular invariants expressible in terms of quadratic and cubic irrationals*, Math. Ann. **96** (1927), 53–69.

[B-K-O] J. Bruinier, W. Kohnen, and K. Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Compositio Math., accepted for publication.

[C] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1997. MR **99e:**11068

[G1] B. Gross, *Arithmetic of elliptic curves vith complex multiplication*, Lecture Notes in Mathematics 776, Springer-Verlag, Berlin, 1980. MR **81f:**10041

[G2] ———, *Minimal models for elliptic curves with complex multiplication*, Compositio Math. **45** (1982), 155–164. MR **84j:**14044

[Go] F. Gouvêa, *The square-free sieve over number fields*, J. Number Theory **43** (1993), 109-122. MR **93m:**11045

[G-M] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23. MR **92b:**11039

[H-R] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, No. 4, Academic Press, London, 1974. MR **54:**12689

[H-W] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edition, The Clarendon Press, Oxford Univ. Press, 1979. MR **81i:**10002

[J] J. Jiménez Urroz, *Non-trivial zeroes for quadratic twists of Hasse-Weil L-Functions*, J. Number Theory **77** (1999), 331–335. MR **2000d:**11088

[K-L] V. A. Kolyvagin and D. Yu. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties* (Russian), Algebra i Analiz **1** (1989), no. 5, 171–196. Translation in Leningrad Math. J. **1** (1990), 1229-1253. MR **91c:**11032

[M-R] H. Montgomery and D. Rohrlich, *On the L-functions of canonical Hecke characters of imaginary quadratic fields*, Duke Math. J. **49** (1982), 937–942. MR **84e:**12014

[M-Y] S. Miller and T. H. Yang, *Non-vanishing of the central derivative of canonical Hecke L-functions*, Math. Res. Letters **7** (2000), 263–277. MR **2001i:**11058

[N] T. Nagel, *Généralisation d'un théorème de Tchebycheff*, J. Math. Pures. Appl. (8) **4** (1921), 343–356.

[R] D. E. Rohrlich, *A modular version of Jensen's formula*, Math. Proc. Cambridge Philos. Soc. **95** (1984), 15–20. MR **85d:**11043

[RV-Y] F. Rodriguez Villegas and T. H. Yang, *Central values of Hecke L-functions of CM number fields*, Duke Math. J. **98** (1999), 541–564. MR **2000j:**11074

[S-T] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973. MR **95m:**11055

[Y] T. H. Yang, *Nonvanishing of central Hecke L-values and rank of certain elliptic curves*, Compositio Math. **117** (1999), 337–359. MR **2001a:**11093

Departamento de Matemática Aplicada IV, ETSETB, Universidad Politecnica de Catalunya, 08034 Barcelona, España

E-mail address: jjimenez@mat.upc.es

Department of Mathematics, University of Wisconsin Madison, Madison, Wisconsin 53717

E-mail address: thyang@math.wisc.edu