CONGRUENT NUMBERS AND CONGRUENCES BETWEEN HALF-INTEGRAL WEIGHT MODULAR FORMS

MATIJA KAZALICKI

ABSTRACT. In this paper we investigate 2-parts of class numbers of quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$ and 2-parts of the algebraic parts of the central L-values associated to the elliptic curves $E_d : y^2 = x^3 - d^2x$ by studying congruences modulo small powers of two between certain half-integral weight modular forms. Assuming the full Birch and Swinnerton-Dyer conjecture for elliptic curves E_d, we prove results about the structure of the 2-part of the Tate-Shafarevich group $Ш(E_d)$. Bruin and Hemenway [2] unconditionally proved some of these results, therefore we verify that for curves E_d Birch and Swinnerton-Dyer conjecture gives correct predictions about the size of 2-part of its Tate-Shafarevich group.

1. INTRODUCTION AND STATEMENT OF RESULTS

A positive integer d is called congruent if it is the area of a right triangle with rational side lengths. The congruent number problem asks for the classification of positive integers which are congruent. It is well known that d is congruent if and only if the elliptic curve $E_d : y^2 = x^3 - d^2x$ has a positive rank over $\mathbb{Q}$. Tunnell [10] constructed weight $3/2$ Hecke eigenform

$$f(\tau) = \eta(8z)\eta(16z)\theta_0(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\frac{3}{2}}(\Gamma_0(128)),$$

whose image under Shimura correspondence $g(z)$ has property that $L(E_1, s) = L(g, s)$. Using Waldspurger's result [11](note that the curves E_d are quadratic twist of E_1), he proved that if d is a positive, odd and square-free integer, then

$$L(E_d, 1) = a(d)^2 \frac{\Omega}{4\sqrt{d}},$$

where $\Omega := \int_1^\infty \frac{dx}{\sqrt{x^3-x}}$. We define the square root of the algebraic part of $L(E_d, 1)$ to be $\sqrt{L^{alg}(E_d, 1)} := a(d)$.

If we assume Birch and Swinnerton-Dyer (BSD) conjecture, we have that d is a noncongruent number if and only if $a(d) \neq 0$. On the other hand, known results

2000 *Mathematics Subject Classification.* 11F52.

Key words and phrases. Congruences between modular forms;Congruent numbers; Class numbers;Birch and Swinnerton-Dyer conjecture.

on BSD conjecture imply unconditionally that if $a(d) \neq 0$, then d is a noncongruent number.

Starting with Gauss, who developed genus theory, many people studied the structure of 2-Sylow subgroup of the class group of the imaginary quadratic fields. For a prime $p \equiv 1 \pmod 4$, denote by $h(-4p)$ the class number of quadratic imaginary field $\mathbb{Q}(\sqrt{-p})$. Cohn and Barrucand [3] discovered that $8|h(-4p)$ if and only if $p = x^2+32y^2$, for some integers x and y. Williams [13] showed that if $\epsilon = T + U\sqrt{p}$ is a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$ then $h(-4p) \equiv T + p - 1 \pmod{16}$, where $8|h(-4p)$. It is not known are there infinitely many primes p for which $16|h(-4p)$.

In the light of the well known analogy between the class group and Tate-Shafarevich group of the elliptic curve, one can ask the similar questions about $Ш(E_p)$, the Tate-Shafarevich group of the elliptic curve E_p. Bruin and Hemenway [2] proved, under the assumption that the primes p for which $E_p(\mathbb{Q})$ has rank 2 have asymptotic density 0 in the set of primes, that at least one of the following is true.

a) There are infinitely many primes p such that $\mathbb{Z}/8\mathbb{Z} \hookrightarrow Ш(E_p)$.
b) There are infinitely many primes p such that $16|h(-4p)$.

We prove the "L-function" analog of this result.

Theorem 1.1. *If d is a positive square free integer, then*

$$3H(-4d) \equiv \sqrt{L^{alg}(E_d, 1)} + 8b(d) \pmod{16},$$

where $b(d)$ is dth Fourier coefficient of the certain Eisenstein series (see Proposition 3.1), and $H(-4d)$ is the Hurwitz class number (see Section 2). In particular, if p is a prime, then

$$3h(-4p) \equiv \begin{cases} \sqrt{L^{alg}(E_p, 1)} \pmod{16} & \text{if } p \equiv 1 \pmod{16}, \\ \sqrt{L^{alg}(E_p, 1)} + 8 \pmod{16} & \text{if } p \equiv 9 \pmod{16} \end{cases}$$

Remark. The author [6] proved a similar congruence relation between $h(-4p)$ and algebraic part of the central value of L-function associated to Ramanujan Δ-function and its quadratic twists.

Remark. G. Boxer and P. Diao [1] proved a similar theorem for a certain class of elliptic curves without any rational 2-torsion over $\mathbb{Q}$ (note that E_1 has a full rational 2-torsion over $\mathbb{Q}$).

Assuming the full BSD conjecture, Tunell showed that $\#Ш(E_p) = \frac{1}{4}a(p)^2$ when $a(p) \neq 0$, hence we have the following corollary.

Corollary 1.2. *Let p be a prime. If we assume the full BSD conjecture for the curve E_p, then the following are true:*

a) *If $p \equiv 1 \pmod{16}$ then*

$$16|h(-4p) \iff (\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p) \text{ or } p \text{ is congruent.}$$

b) *If* $p \equiv 9 \pmod{16}$, *then*

$$8||h(-4p) \iff (\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p) \text{ or } p \text{ is congruent.}$$

Chebotarev's density theorem implies that the set S of primes $p \equiv 9 \pmod{16}$ with property that $8|h(-4p)$ has a positive density in the set of primes. For $p \in S$, the sign of functional equation of $L(E_p, s)$ is 1, hence BSD conjecture implies that the rank of E_p is even. If we assume that the set of primes p for which E_p has rank 2 have density 0 in the set of primes, we conclude that there are infinitely many primes $p \in S$ for which p is noncongruent. Corollary 1.2 b) now implies that for $p \in S$ either $16|h(-4p)$ or $(\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p)$.

The following theorem relates the structure of $Ш(E_p)$ to the arithmetic of real quadratic field $\mathbb{Q}(\sqrt{p})$.

Theorem 1.3. *Let* $p \equiv 1 \pmod{8}$ *be a prime. If we assume the full BSD conjecture for the curve* E_p, *then we have*

$$(\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p) \text{ or } p \text{ is congruent} \iff 16|R_2,$$

where $R_2 := \log_2(\epsilon)$ *is* 2*-adic regulator and* ϵ *is a fundamental unit of the real quadratic field* $\mathbb{Q}(\sqrt{p})$.

Remark. In view of the congruences that author proved for Ramanujan Δ-function [6], it is natural to ask whether analogs of the results of this paper (and those of Bruin and Hemenway) hold for Tate-Shafarevich groups of twists of Tate twists of modular motives associated to Δ-function.

2. Preliminaries

2.1. **The theta function.** (See [7], p.12, p.134). A prototypical example of a half-integral weight modular form is the theta function.

Definition 2.1. *The theta function* $\theta_0(z)$ *is given by the Fourier series*

$$\theta_0(z) = 1 + 2\sum_{n=1}^{\infty} q^{n^2} \in M_{\frac{1}{2}}(\Gamma_0(4)).$$

We will be interested in

$$\theta_0(z)^3 = \sum_{n=0}^{\infty} r(n)q^n = 1 + 6q + 12q^2 + 8q^3 + \cdots .$$

A classical result of Gauss states that

$$r(n) = \begin{cases} 12H(-4n) & \text{if } n \equiv 1, 2 \pmod 4 \\ 24H(-n) & \text{if } n \equiv 3 \pmod 8, \\ r(n/4) & \text{if } n \equiv 0 \pmod 4, \\ 0 & \text{if } n \equiv 7 \pmod 8. \end{cases}$$

Here $H(-n)$ is the Hurwitz class number. It is related to the class number $h(-n)$ by the following formula:

$$H(-n) = \frac{h(-D)}{w(-D)} \sum_{d|f} \mu(d) \left(\frac{-D}{d}\right) \sigma_1(f/d),$$

where $-N = -Df^2$ ($-D$ is a negative fundamental discriminant), $w(-D)$ is half the number of units in $\mathbb{Q}(\sqrt{-D})$, and $\mu(d)$ is the Möbius function.

2.2. **Cohen-Eisenstein series.** (See [7], p.14). To study special values of Dirichlet L-functions at negative integers we define Cohen-Eisenstein series.

Definition 2.2. *If $r \geq 2$ is an integer, then the weight $r + \frac{1}{2}$ Cohen-Eisenstein series is defined by*

$$H_r(z) = \sum_{N=0}^{\infty} H(r, N) q^N.$$

Here $H(r, N)$ is defined by

$$H(r, N) = L(1 - r, \chi_D) \sum_{d|n} \mu(d) \chi_D(d) d^{r-1} \sigma_{2r-1}(n/d),$$

where $\chi_D(d) = \left(\frac{D}{d}\right)$. In particular, $H(r, N) = L(1 - r, \chi_D)$ if $D = (-1)^r N$ is a fundamental discriminant.

Cohen [4] proved the following important result.

Theorem 2.3. *If $r \geq 2$ is an integer, then $H_r(z) \in M_{r+\frac{1}{2}}(\Gamma_0(4))$.*

2.3. **Sturm's Theorem.** (See [9], p.171). In order to prove congruences between modular forms it is enough to check congruences between a finite number of their initial Fourier coefficients.

Let $f(z) = \sum_{n=0}^{\infty} a(n) q^n \in M_k(\Gamma)$, be a modular form of weight $k \in \mathbb{Z}$ for a congruence group $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ with $a(n) \in \mathcal{O}_K$, and let $\mathfrak{m} \subset \mathcal{O}_K$ be an ideal. Define

$$ord_{\mathfrak{m}}(f) = min\{n : a(n) \notin \mathfrak{m}\}.$$

Theorem 2.4 (Sturm)**.** *If we have*

$$ord_{\mathfrak{m}}(f) > \frac{k}{12} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma],$$

then it follows that $ord_{\mathfrak{m}}(f) = \infty$.

We will apply this result to half-integral weight modular forms. We call the quantity in the theorem the Sturm bound for $M_k(\Gamma)$.

Let N,M and $2k$ be integers. Assume $4|N$ and $N|M$. We define

$$M_k(M, N) = \bigoplus_{\chi} M_k(\Gamma_0(M), \chi),$$

where the sum is over all Dirichlet characters of conductor dividing N. We have the following proposition (for the proof see Section 3.2. of [6]).

Proposition 2.5. *Let k be an integer and $f(z) \in M_{k+\frac{1}{2}}(M, N)$. If we have*

$$ord_{\mathfrak{m}}(f) > \frac{2k+1}{24} M\phi(N) \prod_{p|M}(1+\frac{1}{p}),$$

then we have $ord_{\mathfrak{m}}(f) = \infty$.

For a power series $f(z) = \sum c(n)q^n$, and positive integers $a < b$, with $\gcd(a, b) = 1$, denote by $f(z)_{a,b}$ a power series $\sum_{n \equiv a \pmod b} c(n)q^n$. It follows that if $f(z) \in M_{k+\frac{1}{2}}(M, 2^N)$, then $f(z)_{a,2^b} \in M_{k+\frac{1}{2}}(M \cdot 2^{2b}, \max(2^N, 2^{b-1}))$. Denote by $f^+(z) := f(z)_{1,8}$.

2.4. **Weight 1 Eisenstein series.** Let $n \geq 2$ be a positive integer. In this subsection, we recall the construction of weight one Eisenstein series $W_n(z)$ with the property that $W_n(z) \equiv 1 \pmod{2^n}$(for more details see Section 3.3. of [6]).

Definition 2.6. *For primitive Dirichlet characters ψ and ϕ, such that $(\psi\phi)(-1) = -1$, we define an Eisenstein series*

$$E_1^{\psi,\phi}(z) = \delta(\phi)L(0,\psi) + \delta(\psi)L(0,\phi) + 2\sum_{n=1}^{\infty} \sigma_0^{\psi,\phi}(n)q^n.$$

Here $\delta(\psi) = 1$ if $\psi = \mathbf{1}$, and 0 otherwise, and the generalized divisor sum is

$$\sigma_0^{\psi,\phi}(n) = \sum_{m|n} \psi\left(\frac{n}{m}\right)\phi(m).$$

Also for a positive integer t, we define

$$E_1^{\psi,\phi,t}(z) = E_1^{\psi,\phi}(tz).$$

The following well known result gives a basis for the Eisenstein subspace of weight 1 (for the proof see [5], p.141).

Theorem 2.7. *Let N be a positive integer. Let A_N be a set of pairs $(\{\psi, \phi\}, t)$ where ψ and ϕ are primitive Dirichlet characters of modulus u and v, such that $(\psi\phi)(-1) = -1$, and t is a positive integer such that $tuv|N$. Then the set*

$$\{E_1^{\psi,\phi,t}(z) : (\{\psi, \phi\}, t) \in A_N\}$$

represents a basis of the Eisenstein subspace of $M_1(\Gamma_1(N))$.

Recall that the group of Dirichlet characters of modulus 2^n is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$. Also, if ψ is an odd Dirichlet character of conductor f, we have

$$L(0,\psi) \quad = -B_{1,\psi} = -\frac{1}{f}\sum_{i=0}^{f-1} \psi(i)i,$$

where $B_{1,\psi}$ is a generalized Bernoulli number.

Theorem 2.8. *Let $n \geq 2$ be a positive integer, and let ψ and ϕ be the generators of the group of Dirichet characters of modulus 2^n of order 2 and 2^{n-2}. Then the Eisenstein series*

$$W_n = \sum_{i=0}^{\infty} a_i q^i = -2 \sum_{i=0}^{2^{n-2}} (-1)^i E_1^{\mathbf{1},\psi\phi^i}(z) \in M_1(\Gamma_1(2^n))$$

satisfies $W_n \equiv 1 \pmod{2^n}$.

3. Proofs

The following proposition was proved in [6].

Proposition 3.1. *The following congruences hold.*
We have

$$2\theta_0(z)^{3+} \equiv 59\theta_0(z)^+ + 64F_1(z) - 8H_4(z)^+ \pmod{128},$$

where $F_1(z) = \sum_{n=0}^{\infty} b(n)q^n \in M_1(\Gamma_1(128))$ is an Eisenstein series such that for prime number p we have

$$\begin{aligned} b(p) &\equiv 0 \pmod 2 \quad \text{if } p \equiv 1 \pmod{16}, \\ b(p) &\equiv 1 \pmod 2 \quad \text{if } p \equiv 9 \pmod{16}. \end{aligned}$$

The following result relates Fourier coefficients $a(d)$ to the special values of Dirichlet L-function.

Proposition 3.2. *We have that*

$$16f^+(z) \equiv 240H_4^+(z) + 14 \sum_{d>0 \text{ odd}} d^4 q^{d^2} - 8 \sum_{d>0 \text{ odd}} d^2 q^{d^2} + 8 \sum_{d>0 \text{ odd}} q^{d^2} \pmod{2^8}$$

Proof. Sturm bound for the modular form

$$\begin{aligned} h(z) = 16f^+(z)W_7(z)^3 - 240H_4^+(z) - 7W_7(z)^4 \sum_{\substack{i \equiv 1 \pmod 8 \\ 0<i<2^6}} i^2\theta_0(z)_{i,2^6} \\ - 4W_7(z)^4 \sum_{\substack{i \equiv 1 \pmod 8 \\ 0<i<2^5}} i\theta_0(z)_{i,2^5} + 4W_7(z)^4\theta_0(z)_{1,2} \in M_{4+\frac{1}{2}}(2^{14}, 2^7) \end{aligned}$$

is 589824. A computer check verifies that $h(z) \equiv 0 \pmod{2^8}$, which completes the proof since $h(z)$ is congruent modulo 2^8 to the expression from the statement of the proposition. □

Combining these two propositions, we obtain proofs of the results from the introduction.

Proof of Theorem 1.1. From Proposition 3.1 it follows that $3H(-4d) \equiv 8b(d) - H(4,d) \pmod{16}$, while Proposition 3.2 implies $a(d) \equiv -H(4,d) \pmod{16}$. Putting this together we get $a(d) \equiv 3H(-4d) - 8b(d) \pmod{16}$. The rest follows from Proposition 3.1. □

Proof of Corollary 1.2. Let $p \equiv 1 \pmod{16}$ be a prime. If $16|h(-4p)$, then Proposition 3.2 implies that $16|a(p)$. If $a(p) \neq 0$, then p is noncongruent and $\#Ш(E_p) = \frac{1}{4}a(p)^2$ implies that $(\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow \#Ш(E_p)$. The rest follows similarly. □

Theorem 1.3. We recall the 2-adic class number formula ([12], p.71). Let ϵ be a fundamental unit of $\mathbb{Q}(\sqrt{p})$. Then we have (up to the sign)

$$\frac{2h(p)\log_2 \epsilon}{\sqrt{p}} = \left(1 - \frac{\chi_p(2)}{2}\right)^{-1} L_2(1, \chi_p).$$

Since $h(p)$ is odd, we have $16|\log_2 \epsilon$ if and only if $16|L_2(1,\chi_p)$. On the other hand, by definition $L_2(1-2^n,\chi_p) = (1-\chi_p(2)2^{2^n-1})L(1-2^n,\chi_p)$ and $L_2(1,\chi_p) \equiv L_2(1-2^2,\chi_p) \pmod{32}$ (Shiratani [8]), hence $16|L_2(1,\chi_p)$ if and only if $16|L(-3,\chi_p)$. Proposition 3.2 implies that $a(p) \equiv 15L(-3,\chi_p) \pmod{16}$, hence $16|\log_2 \epsilon$ if and only $16|a(p)$. If p is noncongruent, then $\#Ш(E_p) = \frac{1}{4}a(p)^2$ so $16|a(p)$ is equivalent to $(\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p)$. □

4. Acknowledgements

I would like to thank referee for his helpful comments.

References

[1] G. Boxer, P. Diao, *2-Selmer groups of quadratic twists of elliptic curves* Proc. Amer. Math. Soc. **138** (2010), no. 6, 1969–1978.
[2] N. Bruin, B. Hemenway, *On congruent primes and class numbers of imaginary quadratic fields*, arXiv:1110.5959 (2011)
[3] P. Barrucand, H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity,* J. Reine Angew. Math. **238** (1969), 67–70.
[4] H.Cohen, *Sums Involving the Values at Negative Integers of L-functions of Quadratic Characters*, Math.Ann. **217** (1975), 271–285.
[5] F. Diamond, J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, Springer-Verlag, **228**, (2005)
[6] M. Kazalicki. *2-adic and 3-adic part of class numbers and properties of central values of L-functions*, Acta Arith. **147** (2011), no. 1, 51–72.
[7] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Regional Conference Series in Mathematics, AMS, **102**, (2003)
[8] K. Shiratani, *On certain values of p-adic L-functions,* Mem. Fac. Sci. Kyushu Univ. **28** (1974), 59–82.
[9] W. Stein, *Modular forms, a computational approach,* GSM **79** (2007).
[10] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. **72** (1983), no. 2, 323–334.

[11] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. (9) **60** (1981), no. 4, 375–484.
[12] L. C. Washington, *Introduction to Cyclotomic Fields,* Graduate Texts in Mathematics, Springer-Verlag **83** (1997).
[13] K. Williams, *On the class number of* $Q(\sqrt{-p})$ *modulo* 16, *for* $p \equiv 1 \pmod 8$ *a prime,* Acta Arith. **39** (1981), no. 4, 381–398.

Department of Mathematics, University of Zagreb, Croatia, Zagreb, Bijenička cesta 30
E-mail address: mkazal@math.hr