Reduction of CM elliptic curves and modular function congruences

REDUCTION OF CM ELLIPTIC CURVES AND MODULAR FUNCTION CONGRUENCES

NOAM ELKIES, KEN ONO AND TONGHAI YANG

1. Introduction and Statement of Results

Let $j(z)$ be the modular function for $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$j(z) := \sum_{n=1}^{\infty} c(n)q^n = \frac{\left(1 + 240\sum_{n=1}^{\infty}\sum_{v|n} v^3 q^n\right)^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}} = q^{-1} + 744 + 196884q + \cdots,$$

where $q = e^{2\pi iz}$. The coefficients $c(n)$ possess some striking properties. By "Monstrous Moonshine", these integers occur as degrees of a special graded representation of the Monster group, and they satisfy some classical Ramanujan-type congruences. In particular, Lehner proved [Le] that if $p \leq 7$ is prime and m is a positive integer, then for every $n \geq 1$ we have

$$c(p^m n) \equiv \begin{cases} 0 \pmod{2^{3m+8}} & \text{if } p = 2, \\ 0 \pmod{3^{2m+3}} & \text{if } p = 3, \\ 0 \pmod{5^{m+1}} & \text{if } p = 5, \\ 0 \pmod{7^m} & \text{if } p = 7. \end{cases}$$

Modulo 11, it also turns out that $c(11n) \equiv 0 \pmod{11}$ for every positive integer n.

As usual, if $U(p)$ denotes the formal power series operator

$$\left(\sum_{n=-\infty}^{\infty} a(n)q^n\right) \Big| U(p) := \sum_{n=-\infty}^{\infty} a(pn)q^n, \tag{1.1}$$

then these congruences imply that

$$j(z) \mid U(p) \equiv 744 \pmod{p}$$

for every prime $p \leq 11$. It is natural to ask whether such congruences hold for any primes $p \geq 13$.

Date: February 2, 2008.

2000 *Mathematics Subject Classification.* 11F30, 11G05.

The authors thank the National Science Foundation for its support. The second author is grateful for the support of the David and Lucile Packard, H. I. Romnes and John S. Guggenheim Fellowships.

Remark. Since the Hecke operator $T(p)$ acts like $U(p)$ on spaces of holomorphic integer weight modular forms modulo p, this problem is somewhat analogous to that of determining whether there are infinitely many non-ordinary primes for the generic integer weight newform without complex multiplication. Apart from those newforms associated to modular elliptic curves, for which the existence of infinitely many non-ordinary primes was shown in [El], little is known.

Serre showed [Se] that the answer to this question for $j(z)$ is negative, an observation which has been generalized by the second author and Ahlgren [AO]. In particular, if $F(x) \in \mathbb{Z}[x]$ is a polynomial of degree $m \geq 1$ and $p > 12m+1$ is a prime which does not divide the leading coefficient of $F(x)$, then (see Corollary 5 of [AO])

$$F(j(z)) \mid U(p) \not\equiv a(0) \pmod{p},$$

where $a(0)$ is the constant term in the Fourier expansion of $F(j(z))$.

Remark. In the cuspidal case where $(m, p) = (1, 13)$, it is interesting to note that (for example, see Section (6.16) or [Se])

$$(j(z) - 744) \mid U(13) \equiv -\Delta(z) \pmod{13},$$

where $\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ is the usual Delta-function.

Here we investigate the more general question concerning the existence of congruences of the form

$$F(j(z)) \mid U(p) \equiv G_p(j(z)) \pmod{p}, \tag{1.2}$$

where $G_p(x) \in \mathbb{Z}[x]$. The result quoted above implies that congruences of the form (1.2) do not hold for any primes $p > 12m + 1$. This follows from the simple fact that the only polynomials in $j(z)$ whose Fourier expansions do not contain negative powers of q are constant.

In Section 2 we give a general criterion (Theorem 2.3) that proves such congruences, and we apply it to Hilbert class polynomials. For a discriminant $-D < 0$, let $\mathcal{H}_D(x) \in \mathbb{Z}[x]$ be the associated Hilbert class polynomial. More precisely, $\mathcal{H}_D(x)$ is the polynomial of degree $h(-D)$ whose roots are the singular moduli of discriminant $-D$, where $h(-D)$ is the class number of the ring of integers $\mathcal{O}_D$ of $\mathbb{Q}(\sqrt{-D})$. By the theory of complex multiplication, these singular moduli are the j-invariants of those elliptic curves that have complex multiplication by $\mathcal{O}_D$, the ring of integers of $\mathbb{Q}(\sqrt{-D})$.

Although there are no congruences of the form (1.2) for $F(x) = \mathcal{H}_D(x)$ involving primes $p > 12h(-D)+1$, we show that such congruences are quite common for smaller primes, as Lehner demonstrated for $F(x) = \mathcal{H}_3(x) = x$.

Theorem 1.1. *Suppose that $-D < 0$ is a fundamental discriminant, and that integers $c_D(n)$ are defined by*

$$\mathcal{H}_D(j(z)) = \sum_{n=-h(-D)}^{\infty} c_D(n) q^n.$$

(1) *If $p \leq 11$ is prime and $h(-D) < p$, then*

$$\mathcal{H}_D(j(z)) \mid U(p) \equiv c_D(0) \pmod{p}.$$

(2) *For every prime p there is a non-positive integer N_p such that*

$$\mathcal{H}_D(j(z)) \mid U(p) \equiv G_p(j(z)) \pmod{p},$$

for some $G_p(x) \in \mathbb{Z}[x]$, provided that $-D < N_p$ and $\left(\frac{-D}{p}\right) \neq 1$. This polynomial $G_p(x)$ has degree $\leq h(-D)/p$. In particular, $G_p(x)$ is constant if $h(-D) < p$, or more generally if $c_D(-pn) \equiv 0 \pmod{p}$ for every integer $n > 0$.

Proving Theorem 1.1 (2) depends heavily on the interplay between singular moduli and supersingular j-invariants. For a prime $p \geq 5$, define the supersingular loci $S_p(x)$ and $\widetilde{S}_p(x)$ in $\mathbb{F}_p[x]$ by

$$\begin{aligned} S_p(x) &:= \prod_{E/\overline{\mathbb{F}}_p \text{ supersingular}} (x - j(E)), \\ \widetilde{S}_p(x) &:= \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular} \\ j(E) \notin \{0, 1728\}}} (x - j(E)). \end{aligned} \tag{1.3}$$

These products are over isomorphism classes of supersingular elliptic curves. It is a classical fact (for example, see [Si1]) that the degree of $\widetilde{S}_p(x)$ is $\lfloor p/12 \rfloor$.

The criterion for proving congruences of the form (1.2) is stated in terms of the divisibility of $F(x)$ by $\widetilde{S}_p(x)^2$ in $\mathbb{F}_p[x]$. For Hilbert class polynomials, this criterion is quite natural since a classical theorem of Deuring asserts that the reduction of every discriminant $-D$ singular modulus modulo p is a supersingular j-invariant when p does not split in $\mathbb{Q}(\sqrt{-D})$.

Therefore, to prove Theorem 1.1 we are forced to consider the surjectivity of Deuring's reduction map of singular moduli onto supersingular j-invariants, a question which is already of significant interest. Using classical facts about elliptic curves with CM and certain quaternion algebras, we reinterpret this problem in terms of the vanishing of Fourier coefficients of specific weight 3/2 theta functions constructed by Gross. Then, using deep results of Duke and Iwaniec which bound coefficients of half-integral weight cusp forms, we obtain the following theorem.

Theorem 1.2. *If p is an odd prime and $t \geq 1$, then there is a non-positive integer $N_p(t)$ such that $S_p(x)^t \mid \mathcal{H}_D(x)$ in $\mathbb{F}_p[x]$ for every fundamental discriminant $-D < N_p(t)$ for which $\left(\frac{-D}{p}\right) \neq 1$.*

Three Remarks. 1. After this paper was submitted for publication, Bill Duke and the referee informed us of earlier work of P. Michel [Mi]. In this recent paper, Michel obtains equidistribution results which imply Theorem 1.2 for discriminants for which p is inert. His proof, which is different from ours, is based on subconvexity bounds for L-functions. Our proof, which also includes the ramified cases, is based on non-trivial estimates of Fourier coefficients of half-integral weight cusp forms. Both proofs are somewhat related via Waldspurger's formulas connecting values of L-functions to Fourier coefficients.

2. Theorem 1.2 is ineffective due to the ineffectivity of Siegel's lower bound for class numbers. It is possible to obtain effective results by employing various Riemann hypotheses (for example, see work [OS] by the second author and Soundararajan concerning Ramanujan's ternary quadratic form), or by assuming the non-existence of Landau-Siegel zeros.

3. Theorem 1.2 is closely related to the work of Gross and Zagier [GZ] which provides the prime factorization of norms of differences of singular moduli in many cases.

In Section 2 we use a result of Koike (arising in his study of "p-adic rigidity of $j(z)$") to prove Theorem 2.3. In Section 3 we recall preliminary facts regarding endomorphism rings of elliptic curves with complex multiplication and quaternion algebras, and we prove Theorem 1.2 using facts about weight 3/2 Eisenstein series combined with the Duke-Iwaniec bounds for coefficients of weight 3/2 cusp forms. Then we combine these results with Theorem 2.3 to prove Theorem 1.1. In Section 4 we conclude with some remarks on numerical calculations related to Theorems 1.1 and 1.2.

2. A congruence criterion and supersingular j-invariants

Here we give a simple criterion which implies congruences of the form (1.2). This criterion is a simple generalization of Theorem 2 of [AO]. The following result of Koike (see Proposition 1 of [Koi]), which is a special case of work of Dwork and Deligne [Dw], describes the Fourier expansion of $j(pz) \pmod{p^2}$ in terms of $j(z)$ and the collection of supersingular j-invariants. Since clearly $j(pz) \equiv j(z)^p \bmod p$, we can describe the Fourier expansion of $j(pz) \pmod{p^2}$ via the reduction modulo p of the expansion of $(j(pz) - j(z)^p)/p$.

Theorem 2.1. *For each prime p there is a rational function $\delta_p(x) = N_p(x)/\widetilde{S}_p(x)$, with $N_p \in \mathbb{F}_p[x]$, such that*

$$j(pz) \equiv j(z)^p + p\delta_p(j(z)) \pmod{p^2}. \tag{2.1}$$

Corollary 2.2. *For all $F \in \mathbb{Z}[x]$ we have*

$$F(j(pz)) \equiv F(j(z)^p) + pF'(j(z)^p)\delta_p(j(z)) \pmod{p^2}, \tag{2.2}$$

where F' denotes the derivative of F.

Proof. By linearity it suffices to prove this for $F = x^k$ ($k = 0, 1, 2, \ldots$). The case $k = 0$ is trivial; $k = 1$ is Theorem 2.1; and for $k > 1$ we may either raise the congruence in Theorem 2.1 to the power k and reduce mod p^2, or argue by induction from the case $k - 1$ and the same congruence, obtaining

$$j(pz)^k \equiv j(z)^{pk} + pj(z)^{(k-1)p}\delta_p(j(z)) \pmod{p^2} \tag{2.3}$$

as claimed. □

We can now deduce our congruence criterion using little more than the theory of Hecke operators.

Theorem 2.3. *Let $F(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree m, and let*

$$F(j(z)) = \sum_{n=-m}^{\infty} a(n)q^n.$$

(1) *If p is prime and $\widetilde{S}_p(x)^2$ divides $F(x)$ in $\mathbb{F}_p[x]$, then*

$$F(j(z)) \mid U(p) \equiv G_p(j(z)) \pmod{p},$$

for some $G_p(x) \in \mathbb{Z}[x]$ with degree $\leq m/p$.

(2) *If $p \leq 11$ is prime and $m < p$, then*

$$F(j(z)) \mid U(p) \equiv a(0) \pmod{p},$$

where $a(0)$ is the constant term in the Fourier expansion of $F(j(z))$.

Proof. For (1), let

$$F(j(z)) = \sum_{n=-\infty}^{\infty} a(n)q^n.$$

Denote by $T_0(p)$ the operator $pT(p)$, that is, p times the usual weight zero pth Hecke operator. Then we have

$$pF(j(z)) \mid U(p) = F(j(z)) \mid T_0(p) - F(j(pz)) = p\sum_{n=-\infty}^{\infty} a(pn)q^n. \tag{2.4}$$

The modular function $F(j(z)) \mid T_0(p)$ is in $\mathbb{Z}[j(z)]$ since it has integer Fourier coefficients and is holomorphic on $\mathbb{H}$. Since $\widetilde{S}_p(x)^2 | F(x)$ we have $\widetilde{S}_p(x) | F'(x)$, whence also $\widetilde{S}_p(x) | F'(x^p)$. By Corollary 2.2 it follows that $F(j(pz)) \pmod{p^2}$ is congruent modulo p^2 to an integer polynomial in $j(z)$, namely $F(j(z))^p + pF'(j(z)^p)\delta_p(j(z))$. Thus (2.4) yields the desired congruence modulo p between $F(j(z)) \mid U(p)$ and a

polynomial in $j(z)$. Moreover, this polynomial must have degree $\leq m/p$ because $F(j(z)) \mid U(p)$ has valuation $\geq -m/p$ at the cusp.

For (2), we observe that the condition $\widetilde{S}_p(x)^2|F(x)$ of (1) is vacuous for $p \leq 11$, because $\widetilde{S}_p(x) = 1$ for those p. Thus $F(j(z)) \mid U(p)$ is always congruent mod p to a polynomial in j of degree at most m/p. In particular, if $m < p$ then this polynomial reduces to a constant, which must equal $a(0)$ by the definition of $U(p)$.

□

3. Gross' theta functions and the proofs of Theorems 1.1 and 1.2

Throughout, p shall denote a prime. We begin by recalling certain facts about elliptic curves with complex multiplication (for example, see Chapter II of [Si2]). Let B be the unique quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞. For $x \in B$, let $Q(x) = x\bar{x} = -x^2$, the reduced norm of x; the map $Q : B \to \mathbb{Q}$ is a quadratic form on B, which is positive-definite because B is ramified at ∞. Fix a maximal order $R \subset B$. Then Q takes integer values on R, and since B is ramified at p, the subset

$$\pi := \{x \in R \mid p|Q(x)\}$$

of R is a two-sided ideal with R/π a finite field of p^2 elements and $\pi^2 = pR$.

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field with ring of integers $\mathcal{O}_D$. More generally, for a positive integer m congruent to 0 or 3 mod 4, let

$$\mathcal{O}_m = \mathbb{Z} + \frac{1}{2}(m + \sqrt{-m})\mathbb{Z},$$

the order of discriminant $-m$ in $\mathbb{Q}(\sqrt{-m})$. An *optimal embedding* of $\mathcal{O}_m$ into R is an embedding in $i : \mathbb{Q}(\sqrt{-m}) \hookrightarrow B$ for which $i^{-1}(R) = \mathcal{O}_m$. Such an embedding is determined by the image of $\sqrt{-m}$ in

$$V = \{x \in B \mid \operatorname{tr} x = 0\},$$

a 3-dimensional subspace of B. This image must be an element of norm m in the lattice

$$L := V \cap (\mathbb{Z} + 2R)$$

in V, and conversely every $v \in L$ of norm m comes from an embedding $\mathbb{Q}(\sqrt{-m}) \hookrightarrow B$, which is optimal if and only if v is a primitive vector of L (that is, $v \notin fL$ for any $f > 1$).

Two optimal embeddings i_1, i_2 are *equivalent* if they are conjugate to each other by a unit in R; In other words, if there is $u \in R^\times$ such that $i_1(x) = ui_2(x)u^{-1}$ for all $x \in \mathcal{O}_m$. Let $h(\mathcal{O}_m, R)$ be the number of equivalence classes of optimal embeddings of $\mathcal{O}_m$ into R. Using the connection between embeddings and lattice vectors, Gross proved [Gr] that these numbers generate the theta series of L as follows:

Lemma 3.1. ([Gr], Proposition 12.9) *The theta function*

$$\theta_L(z) := \sum_{x \in L} e(Q(x))$$

is given by

$$\theta_L(z) = 1 + \sum_{m \geq 1} a_R(m) q^m,$$

where

$$a_R(m) = w_R \sum_{m = f^2 D} \frac{h(\mathcal{O}_D, R)}{u(d)},$$

in which $u(D) = \frac{1}{2}\#\mathcal{O}_d^\times$ *and* $w_R = \#R^\times$. *Moreover,* θ_L *is a holomorphic modular form of weight* $3/2$ *and level* $4p$.

Remark. This $\theta_L(z)$ is a modular form of half-integral weight in the sense of Shimura [Sh]. Moreover, it lies in Kohnen's plus-space [Koh].

Now recall that every maximal order of B is isomorphic with the endomorphism ring of some supersingular elliptic curve E_0 over $\overline{k} = \overline{\mathbb{F}}_p$, say $R = \mathrm{End}(E_0)$, with the ideal π comprising the inseparable endomorphisms of E_0. Let $\mathbb{C}_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$. The residue field of the unramified quadratic extension of $\mathbb{Q}_p$ in $\mathbb{C}_p$ is a finite field of p^2 elements; call it k. There is then a canonical map $R \to k$, $x \mapsto \widetilde{x}$, defined as follows: any $x \in R = \mathrm{End}(E_0)$ induces multiplication by $\widetilde{x}$ on the invariant differentials of E_0. The kernel $\{x \mid \widetilde{x} = 0\}$ is our ideal π, so this map $x \mapsto \widetilde{x}$ identifies k with R/π.

Suppose that (E, i) is a CM elliptic curve over $\mathbb{C}_p$ with complex multiplication by $\mathcal{O}_D$. We may then choose a map

$$i : \mathcal{O}_D \xrightarrow{\sim} \mathrm{End}(E)$$

which is *normalized* in the sense that any $a \in \mathcal{O}_D$ acts on the invariant differentials of E by multiplication by a. (There are two choices of i, related by conjugation in $\mathrm{Gal}(K/\mathbb{Q})$, and one of them is normalized.) If p is inert or ramified in K, then a classical result of Deuring states that $\widetilde{E} := E \mod \mathfrak{p}$ is a supersingular elliptic curve over $\overline{k}$, and if $\widetilde{E} \cong E_0$, then we obtain an optimal embedding

$$f : \mathcal{O}_D \cong \mathrm{End}(E) \to \mathrm{End}(\widetilde{E}) \cong \mathrm{End}(E_0) = R,$$

and moreover the embedding is *normalized*: if $x = f(a)$ then $\widetilde{x}$ is the residue of a in k. Any embedding equivalent to a normalized one is again normalized, because conjugation by a unit in $R^\times$ commutes with our map $x \mapsto \widetilde{x}$. Since any two isomorphisms $\widetilde{E} \cong E_0$ differ by multiplication by a unit in $R^\times$, one sees that the equivalence class of f is uniquely determined by (E, i). Conversely, given a normalized optimal embedding $f : \mathcal{O}_D \to R$, Deuring's lifting theorem (see [GZ, Proposition 2.7]) asserts

that there is a CM elliptic curve (E, i), unique up to isomorphism, such that $\widetilde{E} \cong E_0$, and its associated optimal embedding is normalized and equivalent to f.

Note now that embeddings of $\mathcal{O}_K$ into R come in conjugate pairs $\{i, \bar{\imath}\}$, where $\bar{\imath}(a) = i(\bar{a}) = \overline{i(a)}$. If p is inert in K, then in each pair $\{i, \bar{\imath}\}$ exactly one of $i, \bar{\imath}$ is normalized, whereas if p is ramified in K then every embedding is normalized. We have thus proved the following lemma.

Lemma 3.2. *Let J_D be the set of j-invariants of CM elliptic curves with endomorphism ring $\mathcal{O}_D$. If we set*

$$J_D(E_0) = \{j \in J_D \mid j \bmod \mathfrak{p} = j(E_0)\},$$

then

$$\#J_D(E_0) = \varepsilon h(\mathcal{O}_D, R),$$

where $R = \mathrm{End}(E_0)$ and $\varepsilon = 1/2$ or 1 according as p is inert or ramified in K.

Proof of Theorem 1.2. For every prime p, there are finitely many supersingular elliptic curves E_0 over $\overline{\mathbb{F}}_p$. So to prove the theorem it suffices to show, for each supersingular curve E_0 with $R = \mathrm{End}(E_0)$ and each positive integer t, that there is a non-positive integer $N_p(t)$ such that every fundamental discriminant $-D < N_p(t)$ with $\left(\frac{-D}{p}\right) \neq 1$ has the property that $\mathrm{ord}_{x=j(E_0)}(\mathcal{H}_D(x) \bmod \mathfrak{p}) \geq t$. By Lemmas 3.1 and 3.2, this is equivalent to

$$a_R(D) \geq \frac{w_R t}{\varepsilon u(d)}. \tag{3.1}$$

This turns out to be a simple consequence of well-known deep results of Siegel [Si], Duke [Du], and Iwaniec [Iw]. Indeed, one has by [Si]

$$\theta_L(z) = \frac{12}{p-1} E_{\mathrm{gen}(L)}(z) + C_L(z), \tag{3.2}$$

where $E_{\mathrm{gen}(L)}(z)$ is the Eisenstein series associated to the genus of the lattice L and $C_L(z)$ is a cusp form of weight $3/2$ and level $4p$. Although Siegel's result is not stated for forms of half-integral weight forms, the proof follows *mutatis mutandis*, with the constant $12/(p-1)$ coming from Gross' explicit calculation of these Eisenstein series. More precisely, he shows in [Gr, (12.11)] (this is $2G$ in his notation, see also [KRY, §8]) that

$$E_{\mathrm{gen}(L)}(z) = \frac{p-1}{12} + 2\sum_{m>0} H_p(m) q^m, \tag{3.3}$$

where $H_p(m)$ is a slight modification of Kronecker-Hurwitz class number $H(m)$ defined in [Gr, (1.8)]. In particular, when $-D$ is a fundamental discriminant, one has

$$H_p(D) = \frac{1}{2}\left(1 - \left(\frac{-D}{p}\right)\right)\frac{h(-D)}{u(D)},$$

where $h(-D)$ is the ideal class number of K.

By Siegel's theorem [Si], one has

$$H_p(D) \gg D^{\frac{1}{2}-\epsilon}$$

for every $\epsilon > 0$ when $(\frac{-D}{p}) \neq 1$. On the other hand, a theorem of Duke [Du], which extended earlier work of Iwaniec [Iw], implies that the coefficients of the cusp form

$$C_L(z) = \sum_{m \geq 1} c_L(m) q^m$$

satisfy

$$|c_L(D)| \ll D^{\frac{3}{7}+\epsilon}.$$

Since $3/7 < 1/2$, we get

$$a_R(D) = \frac{24}{p-1} H_p(D) + c_L(D) \gg D^{\frac{1}{2}-\epsilon}.$$

This proves (3.1), and consequently completes the proof of the theorem. □

Proof of Theorem 1.1. Theorem 1.1 (1) follows immediately from Theorem 2.3 (1). Theorem 1.1 (2) follows from Theorem 2.3 (2) and Theorem 1.2 by letting $N_p = N_p(2)$. □

4. Concluding Remarks

Numerical computations reveal many nearly uniform sets of examples of congruences of the form (1.2). Here we comment on those cases where

$$\mathcal{H}_D(j(z)) \mid U(p) \equiv c_D(0) \pmod{p}.$$

In view of Theorem 2.3, it is natural to investigate those fundamental discriminants $-D < 0$ for which

$$p/6 < h(-D) < p. \tag{4.1}$$

The lower bound of this inequality is dictated by the fact that the degree of $\widetilde{S}_p(x)$ is $\lfloor p/12 \rfloor$, and the upper bound is chosen so that the $U(p)$ operator does not produce a Fourier expansion with negative powers of q.

Computations reveal that if $-239 < -D < 0$ and p is an odd prime satisfying (4.1) for which $\left(\frac{-D}{p}\right) \neq 1$, then $S_p(x)^2$ divides $\mathcal{H}_D(x)$ in $\mathbb{F}_p[x]$, which, by Theorem 2.3, in turn implies that

$$\mathcal{H}_D(j(z)) \mid U(p) \equiv c_D(0) \pmod{p}.$$

This uniformity suggests that this phenomenon might hold in generality. However, this is not true; when $-D = -239$, we have

$$\mathcal{H}_{-239}(j(z)) \mid U(79) \equiv 44 + 2q + 62q^2 + \cdots \pmod{79},$$

although 79 is inert in $\mathbb{Q}(\sqrt{-239})$ and $h(-239) = 15$. In this case $S_{79}(x)$ divides $\mathcal{H}_{239}(x)$ in $\mathbb{F}_{79}[x]$, but the supersingular j-invariant $j = -15$ is a root of multiplicity only 1. This raises the following natural question.

Question. If p is an odd prime, then define Ω_p by

$$\Omega_p := \left\{ -D \text{ fundamental} \;\middle|\; p/6 < h(-D) < p \text{ and } \left(\frac{-D}{p}\right) \neq 1 \right\}.$$

In general, what "proportion" of $-D \in \Omega_p$ have the property that

$$\mathcal{H}_D(j(z)) \mid U(p) \equiv c_D(0) \pmod{p}?$$

References

[AO] S. Ahlgren and K. Ono, *Arithmetic of singular moduli and class equations*, Compositio Mathematica **141** (2005), pages 293–312.

[Du] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), pages 73–90.

[Dw] B. Dwork, *p-adic cycles*, Inst. Hautes Études Sci. Publ. Math. **37** (1969), pages 27–115.

[El] Elkies, N.D.: *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (1987), pages 561–567.

[Gr] B. Gross, *Heights and the special values of L-series*, Number Theory (Montreal, Quebec, 1985) CMS Conference Proc. **7**, Amer. Math. Soc. (1987), pages 115–187.

[GZ] B. Gross and D. Zagier, *On singular moduli*, J. reine angew. Math. **355** (1985), pages 191–220.

[Iw] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. **87** (1987), pages 385–401.

[Koh] W. Kohnen, *Newforms of half-integral weight*, J. reine angew. Math. **333** (1982), pages 32–72.

[Koi] M. Koike, *Congruences between modular forms and functions and applications to the conjecture of Atkin*, J. Fac. Sc. Univ. Tokyo, Sect. IA Math. **20** (1973), pages 129–169.

[KRY] S. Kudla, M. Rapoport, and T.H. Yang, *The derivative of Eisenstein series and the Faltings's heights*, Compos. Math. **140** (2004), pages 887–951.

[Le] J. Lehner, *Further congruence properties of the Fourier coefficients of the modular invariant* $j(\tau)$, Amer. J. Math. **71** (1949), pages 373–386.

[Mi] P. Michel, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points*, Annals of Math. **160** (2004), pages 185–236.

[OS] K. Ono and K. Soundararajan, *Ramanujan's ternary quadratic form,* Invent. Math. **130** (1997), pages 415–454.

[Se] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Enseign. Math. **22** (1976), pages 227–260.

[Sh] G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), pages 440–481.

[Si] C.L. Siegel, *Über die analytische Theorie der quadratischen Formen I, II, III*, Ann. of Math. **36** (1935), pages 527–606; **37** (1936), pages 230–263; **38** (1937), pages 212–291.

[Si1] J. Silverman, *The Arithmetic of Elliptic curves*, Springer-Verlag, New York, 1986.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138
E-mail address: elkies@math.harvard.edu

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: thyang@math.wisc.edu
E-mail address: ono@math.wisc.edu