SPECIAL VALUES OF HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS

Ron Evans
Department of Mathematics
University of California at San Diego
La Jolla, CA 92093-0112
revans@ucsd.edu

Frank Lam
University of California at San Diego
La Jolla, CA 92093-0112
frlam@ucsd.edu

July, 2007

2000 *Mathematics Subject Classification.* Primary 11T24;
Secondary 33C20, 14H52, 11R37, 11E25, 11R11, 11G15.

Key words and phrases. Hypergeometric functions over finite fields, elliptic curves with complex multiplication, orders in imaginary quadratic fields, ring class fields, genus class fields, Ramanujan class invariants.

Abstract

For an odd prime p, define $H_p(z) = \sum_{u,v (\mathrm{mod}\ p)} \left(\frac{uv(1-u)(1-v)(1-uvz)}{p} \right)$, where z is an integer (mod p) and the summands are Legendre symbols. The function $H_p(z)$ was explicitly evaluated for $z = 1$ by Evans (1981) and for $z = -1$ by Greene and Stanton (1986). Koike (1992) determined $H_p(1/4)(\mathrm{mod}\ p)$, and Ono (1998) evaluated $H_p(z)$ for $z = 1/4, -1/8$, and $1/64$. This paper evaluates $H_p(z)$ for infinitely many new classes of arguments z.

1 Introduction

For an odd prime p, let $\mathbb{F}_p$ denote the field of p elements and let $\phi = \phi_p$ denote the quadratic Dirichlet character (Legendre symbol) on $\mathbb{F}_p$. Define the function $H_p : \mathbb{F}_p \to \mathbb{Z}$ by

$$H_p(z) = \sum_{u,v \in \mathbb{F}_p} \phi_p(uv(1-u)(1-v)(1-uvz)). \tag{1.1}$$

We have [14, Thm. 11.18, p. 193]

$$H_p(z) = p^2 {}_3F_2\left(\begin{matrix} \phi & \phi & \phi \\ & \phi^2 & \phi^2 \end{matrix} \middle| z \right), \quad z \in \mathbb{F}_p, \tag{1.2}$$

where the ${}_3F_2$ is Greene's hypergeometric function [7] over $\mathbb{F}_p$.

In [5, §6], it was shown that

$$H_p(1) = \begin{cases} 4x^2 - 2p, & \text{if } p = x^2 + 4y^2 \quad (x, y \in \mathbb{Z}) \\ 0, & \text{otherwise.} \end{cases}$$

In 1981, Evans, Pulham, and Sheehan [6] conjectured that

$$H_p(-1) = \begin{cases} \phi_p(2)(4x^2 - p), & \text{if } p = x^2 + 2y^2 \\ \phi_p(-1)p, & \text{otherwise.} \end{cases} \tag{1.3}$$

This conjecture was proved in 1986 by Greene and Stanton [8]. In 1992, Koike [10] asked for an evaluation of $H_p(1/4)$. This problem was solved by Ono in 1998 [13]. In fact, using elliptic curves, Ono proved

$$H_p(1/4) = \begin{cases} \phi_p(3)(4x^2 - p), & \text{if } p = x^2 + 3y^2 \\ \phi_p(-1)p, & \text{otherwise,} \end{cases} \tag{1.4}$$

$$H_p(-1/8) = \begin{cases} \phi_p(2)(4x^2 - p), & \text{if } p = x^2 + 4y^2 \\ \phi_p(-2)p, & \text{otherwise,} \end{cases} \tag{1.5}$$

and

$$H_p(1/64) = \begin{cases} \phi_p(7)(4x^2 - p), & \text{if } p = x^2 + 7y^2 \\ \phi_p(-1)p, & \text{otherwise.} \end{cases} \tag{1.6}$$

In this paper, we obtain an infinite class of evaluations of $H_p(z)$ extending those in (1.3)–(1.6).

Our evaluations are formulated in terms of Ramanujan's class invariants

$$G_n = 2^{-\frac{1}{4}} q^{-\frac{1}{24}} \prod_{\text{odd } k \geq 1} (1 + q^k) \tag{1.7}$$

and

$$g_n = 2^{-\frac{1}{4}} q^{-\frac{1}{24}} \prod_{\text{odd } k \geq 1} (1 - q^k), \tag{1.8}$$

where n is a positive integer and

$$q = \exp(\pi i \sqrt{-n}). \tag{1.9}$$

It is well-known that G_n and g_n are algebraic numbers [2, p. 183], and extensive tables of their values may be found in [2, pp. 189–204]. (The formula for G_{505} in [2, p. 198] has misprints; the correct formula is provided in [2, p. 238].) For $n > 1$ define

$$r_n = \begin{cases} G_n^{-24}, & \text{if } n \text{ is odd} \\ -g_n^{-24}, & \text{if } n \text{ is even.} \end{cases} \tag{1.10}$$

Then [4, p. 256]

$$r_n = \begin{cases} -64\eta(\sqrt{-n})^{24}/\eta\left(\frac{1+\sqrt{-n}}{2}\right)^{24}, & \text{if } n \text{ is odd} \\ -64\eta(\sqrt{-n})^{24}/\eta\left(\frac{\sqrt{-n}}{2}\right)^{24}, & \text{if } n \text{ is even,} \end{cases} \tag{1.11}$$

where η is the Dedekind eta function. Let $M_n(w) \in \mathbb{Z}[w]$ denote the minimal polynomial of r_n over $\mathbb{Q}$. Equivalently, since r_n is real, $M_n(w)$ is the minimal polynomial of r_n over $\mathbb{Q}(\sqrt{-n})$. Denote the discriminant of $M_n(w)$ by $\mathrm{disc}(M_n)$.

We will say "$r_n (\mathrm{mod}\ p)$ exists" if r_n is congruent to some $z \in \mathbb{F}_p$ modulo some prime ideal P of $\mathbb{Q}(r_n)$ above p. When $r_n (\mathrm{mod}\ p)$ exists, we identify $r_n (\mathrm{mod}\ p)$ with z. Note that $r_n (\mathrm{mod}\ p)$ exists if and only if $\overline{M}_n(w)$ has a linear factor $w - z$ over $\mathbb{F}_p$, where $\overline{M}_n(w)$ denotes the reduction of $M_n(w)$ $(\mathrm{mod}\ p)$. For example, when $n = 5$, we have $r_5 = 9 - 4\sqrt{5}$, and $z = r_5 (\mathrm{mod}\ p)$ exists if and only if $p \equiv \pm 1 (\mathrm{mod}\ 5)$. The choice of $z \in \mathbb{F}_p$ may depend on the choice of P; for example, when $n = 5$ and $p = 31$, one has the choices $z = 2$ and $z = 16$.

Our main result is the following theorem.

Theorem. *Let n be an integer > 1 and let p be a prime which does not divide $2n\,\mathrm{disc}(M_n)$.*
(A) *If $p = x^2 + ny^2$ for integers x, y, then $z = r_n (\mathrm{mod}\ p)$ exists and*

$$H_p(z) = (-1)^y (4x^2 - p), \quad \textit{when } z \neq 1. \tag{1.12}$$

In all of the other cases with $\phi_p(-n) = 1$, $r_n (\mathrm{mod}\ p)$ does not exist.
(B) *If $\phi_p(-n) = -1$ and $-p$ is a square $(\mathrm{mod}\ n)$, then $z = r_n (\mathrm{mod}\ p)$ exists and*

$$H_p(z) = -\phi_p(1 - z)p, \quad \textit{when } z \neq 1. \tag{1.13}$$

In all of the other cases with $\phi_p(-n) = -1$, $r_n (\mathrm{mod}\ p)$ does not exist.

The proof of the Theorem is given in Section 4. The needed background in ring class field theory is summarized in Section 2. Our proof depends on properties of certain elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-n}]$. These curves, defined in terms of Ramanujan's class invariants, are introduced in Section 3.

Examples. If $p = x^2 + 5y^2$, then by (1.12),

$$H_p(9 - 4\sqrt{5}\ (\mathrm{mod}\ p)) = H_p(z) = (-1)^y (4x^2 - p).$$

For example, when $p = 41$, we have $z \in \{20, 39\}$, so that

$$H_p(20) = H_p(39) = -(144 - 41) = -103.$$

In contrast with (1.12), the left side of (1.13) may depend on the choice of $z = r_n (\mathrm{mod}\ p)$ for given n, p. For example, when $n = 5$, $p = 31$, we have $z \in \{2, 16\}$ and

$$H_p(2) = p, \quad H_p(16) = -p.$$

Remark 1. We conjecture that when $p > n$, the condition $z \neq 1$ in the Theorem holds as well as the condition $p \nmid \mathrm{disc}(M_n)$ (cf. [9]).

Remark 2. Assume that $p \mid \mathrm{disc}(M_n)$. Then $r_n (\mathrm{mod}\ p)$ need not exist. For example, when $n = 98$ so that $\mathrm{disc}(M_n)$ is divisible by primes 5, 13, 29, 37, et al., we have $r_n (\mathrm{mod}\ 5) = 4$ and $r_n (\mathrm{mod}\ 13) = 12$, but $r_n (\mathrm{mod}\ 29)$ and $r_n (\mathrm{mod}\ 37)$ do not exist. Our proof of the Theorem will show that $\phi_p(-n) = -1$ and that $H_p(z)$ is given by (1.13) when $z = r_n (\mathrm{mod}\ p)$ exists.

Remark 3. By [2, pp. 187, 189, 200], we have

$$r_2 = -1, \quad r_3 = 1/4, \quad r_4 = -1/8, \quad r_7 = 1/64,$$

and so the cases $n = 2, 3, 4, 7$ of the Theorem are easily seen to be equivalent to (1.3)–(1.6), respectively. Some additional simple values of r_n of small degree (with $n < 100$) are given in the table below. As an example, consider the case $n = 30$ with $p > 30$. We see quickly from the table that $z = r_n (\mathrm{mod}\ p)$ exists if and only if 2 and 5 are both squares (mod p). Then by the Theorem, $H_p(z)$ is determined by (1.12) when p is congruent to 1, 31, 49, or 79 (mod 120), and $H_p(z)$ is determined by (1.13) when p is congruent to 41, 71, 89, or 119 (mod 120). For all other $p > 30$, $r_n (\mathrm{mod}\ p)$ does not exist.

n	r_n
2	-1
3	$1/4$
4	-1/8
5	$9-4\sqrt{5}$
6	$-17+12\sqrt{2}$
7	$1/64$
8	$(7-5\sqrt{2})/8$
9	$97-56\sqrt{3}$
10	$-161+72\sqrt{5}$
12	$(-26+15\sqrt{3})/16$
13	$649-180\sqrt{13}$
15	$(47-21\sqrt{5})/128$
16	$(140-99\sqrt{2})/32$
18	$-4801+1960\sqrt{6}$
21	$4032\sqrt{3}-1524\sqrt{21}-2640\sqrt{7}+6985$
22	$-19601+13860\sqrt{2}$
25	$51841-23184\sqrt{5}$
27	$(-80\cdot 4^{1/3}+100\cdot 2^{1/3}+1)/4$
28	$(-2024+765\sqrt{7})/64$
30	$-82080\sqrt{2}+36708\sqrt{10}+51912\sqrt{5}-116081$
33	$-155220\sqrt{3}+46800\sqrt{33}-81060\sqrt{11}+268849$
37	$1555849-255780\sqrt{37}$
40	$(-450\sqrt{2}-207\sqrt{10}+288\sqrt{5}+647)/8$
42	$-1108800\sqrt{6}+725880\sqrt{14}+592680\sqrt{21}-2716001$
45	$3204160\sqrt{3}-1432944\sqrt{15}-2481932\sqrt{5}+5549769$
48	$(-9405\sqrt{2}-5445\sqrt{6}+7680\sqrt{3}+13336)/64$
49	$-6033996\cdot 7^{\frac{1}{4}}2^{\frac{1}{2}}-2280636\cdot 7^{\frac{3}{4}}2^{\frac{1}{2}}+5246208\cdot 7^{\frac{1}{2}}+13880161$
57	$-45083220\sqrt{3}+10342800\sqrt{57}-17914260\sqrt{19}+78086449$
58	$-192119201+35675640\sqrt{29}$
70	$718516260\sqrt{2}-321330240\sqrt{10}+454429584\sqrt{5}-1016135441$
72	$(-13615\sqrt{2}+7840\sqrt{6}-11060\sqrt{3}+19207)/8$
75	$(-33870\cdot 10^{\frac{1}{3}}+15720\cdot 10^{\frac{2}{3}}-15150\cdot 10^{\frac{1}{3}}5^{\frac{1}{2}}+7032\cdot 10^{\frac{2}{3}}5^{\frac{1}{2}}+5)/20$
78	$-3098066400\cdot 2^{\frac{1}{2}}+859249020\sqrt{26}+1215161640\sqrt{13}-4381327601$
85	$-6625268496\sqrt{5}-1606863636\sqrt{85}+3593056320\sqrt{17}+14814550729$
88	$(55440\sqrt{2}-16695\sqrt{22}-23670\sqrt{11}+78407)/8$
93	$32416675200\sqrt{3}-5822206740\sqrt{93}-10084357920\sqrt{31}+56147328649$

2 Ring class field theory

We collect here some results on ring class field theory that will be used in proving the Theorem of Section 1.

For any integer $n > 1$, consider the imaginary quadratic field

$$k = \mathbb{Q}(\sqrt{-n}), \text{ with ring of integers } \mathcal{O}_k. \tag{2.1}$$

We will be working with the order

$$\mathcal{O} = \mathbb{Z}[\sqrt{-n}] \subset \mathcal{O}_k. \tag{2.2}$$

Letting d_k denote the discriminant of k, we see that the discriminant of $\mathcal{O}$ is

$$-4n = t^2 d_k, \tag{2.3}$$

where t is the conductor of $\mathcal{O}$ [4, p. 134]. Let $I_k(t)$ denote the group of (nonzero) fractional ideals of k prime to t, and let $P_{k,\mathbb{Z}}(t)$ denote the subgroup consisting of the ideals $(\mathcal{O}_k\alpha/\beta)$, where α and β run through the nonzero elements of $\mathcal{O}_k$ that are congruent (mod $t\mathcal{O}_k$) to rational integers prime to t. The ring class group $I_k(t)/P_{k,\mathbb{Z}}(t)$ of the order $\mathcal{O}$ is isomorphic to the ideal class group $C(\mathcal{O})$ of the order $\mathcal{O}$ [4, p. 145], and $C(\mathcal{O})$ is isomorphic via the Artin map to $\mathrm{Gal}(\Omega_t/k)$, where Ω_t is the ring class field of k (mod t) [4, p. 180]. Each prime ideal $\mathfrak{p} \in I_k(t)$ is unramified in Ω_t, and $\mathfrak{p}$ splits completely in Ω_t if and only if $\mathfrak{p} \in P_{k,\mathbb{Z}}(t)$ [4, pp. 180–182].

For each $n > 1$, let

$$j_n = j(\sqrt{-n}) \tag{2.4}$$

denote the j-invariant for $\mathcal{O}$. Then [4, p. 220] j_n is a real algebraic integer such that

$$\Omega_t = k(j_n). \tag{2.5}$$

By (1.11) and [15, pp. 329, 337], one also has the interesting formula

$$\Omega_t = k(r_n). \tag{2.6}$$

Write

$$G = \mathrm{Gal}(\Omega_t/k). \tag{2.7}$$

Then clearly,

$$\mathrm{Gal}(\Omega_t/\mathbb{Q}) = G \cup G\tau, \tag{2.8}$$

where $\tau \in \mathrm{Gal}(\Omega_t/\mathbb{Q})$ is complex conjugation. Each of the $|G|$ elements in the coset $G\tau$ has order 2 [4, p. 190].

The genus class field K_t of $k \pmod t$ is the abelian extension of k defined by [16, p. 1592]

$$\mathrm{Gal}(\Omega_t/K_t) = \mathrm{Gal}(\Omega_t/k)^2. \tag{2.9}$$

Letting s denote the 2-rank of the group $C(\mathcal{O})$, we have

$$|\mathrm{Gal}(K_t/k)| = |C(\mathcal{O})/C(\mathcal{O})^2| = 2^s. \tag{2.10}$$

For an odd prime p, define $p^* = \phi_p(-1)p$. Let $p_1, \ldots, p_m$ denote the odd prime factors of n. It can be shown (see [16, p. 1592]) that

$$K_t = \begin{cases} k(\sqrt{p_1{}^*}, \ldots, \sqrt{p_m{}^*}, \sqrt{2}, i), & \text{if } 8 \mid n \\ k(\sqrt{p_1{}^*}, \ldots, \sqrt{p_m{}^*}, i), & \text{if } 4 \parallel n \\ k(\sqrt{p_1{}^*}, \ldots, \sqrt{p_m{}^*}), & \text{if } 4 \nmid n. \end{cases} \tag{2.11}$$

By (2.1) and (2.10)–(2.11), s is determined by

$$s = \begin{cases} m+1, & \text{if } 8 \mid n \\ m-1, & \text{if } n \equiv 3 \pmod 4 \\ m, & \text{otherwise.} \end{cases} \tag{2.12}$$

3 Class invariants and elliptic curves

For complex $r \notin \{0, 1\}$, consider the elliptic curves E defined by

$$y^2 = 4x^3 - g_2 x - g_3, \tag{3.1}$$

where

$$g_2 = \frac{4}{3} + \frac{4}{1-r}, \quad g_3 = \frac{8}{27} - \frac{8}{3-3r}. \tag{3.2}$$

The curve E has nonzero discriminant

$$\Delta_E = {g_2}^3 - 27{g_3}^2 = 64r^2/(1-r)^3 \tag{3.3}$$

and j-invariant

$$j_E = (12g_2)^3/\Delta_E = 64(4-r)^3/r^2. \tag{3.4}$$

Write $j_n = j(\sqrt{-n})$ as in (2.4), for fixed $n > 1$. The cubic equation in r over $k(j_n) = \Omega_t$ given by

$$64(4-r)^3 = j_n r^2 \tag{3.5}$$

has three solutions, and for any one of these three values of r, it follows from (3.4) that E has complex multiplication by $\mathcal{O}$. (Note that $r = 1$ cannot satisfy (3.5), otherwise $j_n = 12^3$, which happens only for $n = 1$ [4, p. 212].) To explicitly find the three solutions r of (3.5), we use the formula [3, (5.3.17), p. 73]

$$j_n = 256(1 - \kappa_n^2 + \kappa_n^4)^3/(\kappa_n^2 - \kappa_n^4)^2, \tag{3.6}$$

where κ_n is the singular modulus defined in terms of the classical theta functions

$$\theta_2(q) = \sum_{-\infty}^{\infty} q^{(n+1/2)^2}, \quad \theta_3(q) = \sum_{-\infty}^{\infty} q^{n^2} \tag{3.7}$$

by

$$\kappa_n = \theta_2(q)^2/\theta_3(q)^2, \quad q = \exp(i\pi\sqrt{-n}). \tag{3.8}$$

Then (3.5) becomes

$$(4-r)^3/r^2 = 4(1-\kappa_n^2+\kappa_n^4)^3/(\kappa_n^2-\kappa_n^4)^2. \tag{3.9}$$

Solving (3.9) for r, we get the following three solutions (whose product is 64):

$$4\kappa_n^2(1-\kappa_n^2), \quad -4\kappa_n^2/(1-\kappa_n^2)^2, \quad -4(1-\kappa_n^2)/\kappa_n^4. \tag{3.10}$$

By [2, eq. (1.6), p. 185; Entry 2.1, p. 187] the three values of r in (3.10) are respectively

$$G_n^{-24}, \quad -g_n^{-24}, \quad -g_{4n}^{24}. \tag{3.11}$$

In view of (2.3), replacing n by $4n$ is equivalent to replacing t by $2t$. The "odd" elements of $P_{k,\mathbb{Z}}(t)$ form a group generated by ideals of the form $\mathcal{O}_k(a+b\sqrt{-n})$, where $a, b \in \mathbb{Z}$, $(a^2+nb^2, 2t) = 1$. The subgroup of index 2 generated by those ideals for which b is even is $P_{k,\mathbb{Z}}(2t)$. Thus

$$|\Omega_{2t} : \Omega_t| = 2. \tag{3.12}$$

Moreover, by (2.6),

$$\Omega_t = k(r_n), \quad \Omega_{2t} = k(r_{4n}). \tag{3.13}$$

Since $r_{4n} = -g_{4n}^{-24}$ by (1.10), it follows from (3.12)–(3.13) that g_{4n}^{24} has degree 2 over Ω_t. Thus two of the three entries in (3.11) generate Ω_{2t} over k, while the remaining entry lies in $k(j_n) = \Omega_t$. More precisely, by (1.10) and (3.13),

$$\Omega_t = k(G_n^{-24}), \quad \Omega_{2t} = k(g_{4n}^{24}) = k(g_n^{-24}), \quad \text{if } 2 \nmid n \tag{3.14}$$

and

$$\Omega_t = k(g_n^{-24}), \quad \Omega_{2t} = k(g_{4n}^{24}) = k(G_n^{-24}), \quad \text{if } 2 \mid n. \tag{3.15}$$

By [2, Entries 2.1 and 2.2, p. 187],

$$
\begin{aligned}
g_{4n}^{24} &= \frac{8}{r_n}(r_n^{-1/3} + (r_n^{-2/3} - r_n^{1/3})^{1/2})^3 \\
&= \frac{8}{r_n^2}(4 - 3r_n + (4 - r_n)(1 - r_n)^{1/2}).
\end{aligned} \tag{3.16}
$$

Since $k(g_{4n}^{24}) = \Omega_{2t}$ by (3.14)–(3.15), it follows from (3.16) that

$$\Omega_{2t} = k(\ (1 - r_n)^{1/2}\ ). \tag{3.17}$$

We now choose r from the list in (3.11) by taking $r = G_n^{-24}$ or $r = -g_n^{-24}$ according as n is odd or even. In other words, we specify $r = r_n$. In view of (3.14)–(3.15), this choice of r makes the degree of r over $\mathbb{Q}$ smaller than the degree of any other choice from (3.11) For example, $r_5 = G_5^{-24} = 9 - 4\sqrt{5}$ has degree 2, while g_5^{-24} and g_{20}^{24} each have degree 4.

We shall write $E = E_n$ to emphasize the dependence of the curve E on $r = r_n$. As was indicated after (3.5), E_n has complex multiplication by $\mathcal{O}$.

4 Proof of the Theorem

Throughout this section, n is an integer > 1 and p is a prime with $p \nmid 2n$. Recall that the elliptic curve E_n over $\mathbb{Q}(r_n)$ defined by

$$y^2 = 4x^3 - g_2x - g_3 \tag{4.1}$$

with

$$g_2 = \frac{4}{3} + \frac{4}{1 - r_n}, \quad g_3 = \frac{8}{27} - \frac{8}{3 - 3r_n} \tag{4.2}$$

has complex multiplication by $\mathcal{O}$.

Suppose first that $r_n \pmod p$ exists, i.e.,

$$r_n \equiv z \pmod{P} \tag{4.3}$$

for some $z \in \mathbb{F}_p$ and some prime ideal P of $\mathbb{Q}(r_n)$ above p. Note that z is nonzero, as $r = r_n$ satisfies (3.5). Suppose further that $z \neq 1$. Then by (3.3), E_n has good reduction (mod P) to a curve $\overline{E_n}$ over $\mathbb{F}_p$ defined by

$$y^2 = 4x^3 - \overline{g}_2 x - \overline{g}_3. \tag{4.4}$$

For $\lambda \in \mathbb{F}_p,\ \lambda \notin \{0, 4\}$, consider the elliptic curve $E(\lambda)$ defined over $\mathbb{F}_p$ by

$$y^2 = x^3 - \lambda^2 x^2 + (4\lambda^3 - \lambda^4)x + (\lambda^6 - 4\lambda^5). \tag{4.5}$$

Ono [14, Thm 11.15, p. 190] proved that

$$H_p\left(\frac{4}{4-\lambda}\right) = \phi_p(\lambda^2 - 4\lambda)(a(p)^2 - p), \tag{4.6}$$

where $p + 1 - a(p)$ is the number of points on $E(\lambda)$ over $\mathbb{F}_p$, including the point at infinity. (See also [1, Theorem 2.1] for an equivalent version of (4.6) over general fields $\mathbb{F}_q$.) In the notation of (4.3), take

$$\lambda = 4(z-1)/z, \quad \text{i.e.,} \quad z = 4/(4-\lambda). \tag{4.7}$$

Then the map

$$x \to -1/3 + x/\lambda^2, \quad y \to 2y/\lambda^3 \tag{4.8}$$

gives an isomorphism from $\overline{E}_n$ to $E(\lambda)$. Thus $\overline{E}_n$ has $p+1-a(p)$ points over $\mathbb{F}_p$, and, under the assumption (4.3), it follows from (4.6)–(4.7) that

$$H_p(z) = \phi_p(1-z)(a(p)^2 - p), \text{ if } z \neq 1. \tag{4.9}$$

We proceed to prove (1.12). Suppose that $p = x^2 + ny^2$. Then

$$p\mathcal{O}_k = (\pi)(\overline{\pi}), \quad \text{with } \pi = x + y\sqrt{-n}. \tag{4.10}$$

Since $(\pi) \in P_{k,\mathbb{Z}}(t)$, it follows from (4.10) that p splits completely into first degree prime ideals of $\Omega_t = k(r_n)$. Therefore $z = r_n (\text{mod } p)$ exists, i.e., (4.3) holds, so we can apply (4.9). A theorem of Deuring [4, Thm. 14.16, p. 317] applied to $\overline{E}_n$ shows that $a(p) = \pi + \overline{\pi} = 2x$, so that by (4.9),

$$H_p(z) = \phi_p(1-z)(4x^2 - p), \text{ if } z \neq 1. \tag{4.11}$$

To complete the proof of (1.12), it remains to show that

$$\phi_p(1-z) = (-1)^y, \quad z \neq 1. \tag{4.12}$$

For this, we will again need to invoke ring class field theory.

As we noted above (3.12), the integral ideals in $P_{k,\mathbb{Z}}(2t)$ are the ideals of the form $\mathcal{O}_k(a + b\sqrt{-n})$ where $(a^2 + nb^2, 2t) = 1$ and b is even. Thus by (4.10),

$$y \text{ is even } \Leftrightarrow (\pi) \in P_{k,\mathbb{Z}}(2t). \tag{4.13}$$

Now,

$$(\pi) \in P_{k,\mathbb{Z}}(2t) \Leftrightarrow p \text{ splits completely in } \Omega_{2t}. \tag{4.14}$$

Since $x^2 - (1 - r_n)$ is the minimal polynomial of $(1 - r_n)^{1/2}$ over Ω_t, it follows from (3.17) and Kummer's Theorem [12, Thm. 4.33, p. 168] that

(4.15) p splits completely in $\Omega_{2t} \Leftrightarrow x^2 - (1 - z)$ has linear factors in $\mathbb{F}_p[x]$.

Thus (4.12) follows from (4.13)–(4.15). This completes the proof of (1.12).

Suppose next that $\phi_p(-n) = 1$ but p does not have the form $x^2 + ny^2$. We must show that $r_n (\text{mod } p)$ does not exist. Since $\phi_p(-n) = 1$, $p\mathcal{O}_k = \mathfrak{p}\overline{\mathfrak{p}}$ for

a first degree prime ideal $\mathfrak{p}$ of k. Since $\mathfrak{p} \notin P_{k,\mathbb{Z}}(t)$, $\mathfrak{p}$ splits into prime ideals of Ω_t having degree $f > 1$. Thus $\overline{M}_n = M_n(w) (\mathrm{mod}\ p)$ splits into irreducible factors of degree f in view of Kummer's theorem, which is applicable here since [4, p. 299] $p \nmid \mathrm{disc}(M_n)$ when $\phi_p(-n) = 1$. Since $\overline{M}_n$ has no linear factors in $\mathbb{F}_p[x]$, $r_n (\mathrm{mod}\ p)$ does not exist. This completes the proof of part (A) of the Theorem.

Suppose from now on that $\phi_p(-n) = -1$, so that p is inert in the extension $k/\mathbb{Q}$. Under the assumption (4.3), we may apply a theorem of Deuring [11, Thm. 12, p. 182] to the curve $\overline{E}_n$ to deduce that $a(p) = 0$ (the supersingular case). Thus, when $r_n (\mathrm{mod}\ p)$ exists, (1.13) follows from (4.9). In particular, this proves the last assertion in Remark 2.

Assume from now on that $p \nmid \mathrm{disc}(M_n)$. To complete the proof of part (B) of the Theorem, we must show that

$$r_n (\mathrm{mod}\ p) \text{ exists } \Leftrightarrow -p \text{ is a square } (\mathrm{mod}\ n). \tag{4.16}$$

For this we will need to invoke genus class field theory.

Since $p \nmid \mathrm{disc}(M_n)$, Kummer's theorem [12, p. 168] implies that $r_n (\mathrm{mod}\ p)$ exists if and only if there is a first degree prime ideal of $\mathbb{Q}(r_n)$ above p. The principal prime ideal $p\mathcal{O}_k \in P_{k,\mathbb{Z}}(t)$ splits completely in Ω_t into a product of $|G|$ distinct primes (where $G = \mathrm{Gal}(\Omega_t/k)$), namely the product

$$\prod_{\sigma \in G} \sigma(\mathfrak{P}), \tag{4.17}$$

where $\mathfrak{P}$ is a second degree prime of Ω_t. Thus there exists a first degree prime of $\mathbb{Q}(r_n)$ above p if and only if some factor $\sigma(\mathfrak{P})$ in (4.17) is fixed by complex conjugation $\tau \in \mathrm{Gal}(\Omega_t/\mathbb{Q})$. Equivalently,

$$r_n (\mathrm{mod}\ p) \text{ exists } \Leftrightarrow \sigma^{-1}\tau\sigma(\mathfrak{P}) = \mathfrak{P} \text{ for some } \sigma \in G. \tag{4.18}$$

In the notation of (2.11), $-p$ is a square $(\mathrm{mod}\ n)$ if and only if both

$$\phi_p(p_i^*) = \mathrm{sgn}(p_i^*), \quad 1 \le i \le m \tag{4.19}$$

and

$$\begin{cases} \phi_p(-1) = -1, & \text{if } 4 \| n \\ \phi_p(-1) = -1 \text{ and } \phi_p(2) = 1, & \text{if } 8 \mid n \end{cases} \tag{4.20}$$

hold. Thus by (2.11), $-p$ is a square (mod n) if and only if p splits in every real quadratic subfield of K_t (and p is inert in every nonreal quadratic subfield of K_t). Therefore

$$-p \text{ is a square (mod } n) \Leftrightarrow p \text{ splits completely in } K_t \cap \mathbb{R}. \tag{4.21}$$

We proceed to prove (4.16). Suppose that $r_n (\text{mod } p)$ exists. Then as we noted below (4.16), there is a first degree prime of $\mathbb{Q}(r_n)$ above p. Thus there is a first degree prime of L above p for every quadratic subfield L of $\mathbb{Q}(r_n)$. Therefore p splits completely in $K_t \cap \mathbb{R}$, so $-p$ is a square (mod n) by (4.21). This proves one direction of (4.16). Now assume that $-p$ is a square (mod n). To complete the proof of (4.16), it remains to show that $\sigma^{-1}\tau\sigma(\mathfrak{P}) = \mathfrak{P}$ for some $\sigma \in G$, in view of (4.18).

Let H denote the abelian group $\text{Gal}((K_t \cap \mathbb{R})/\mathbb{Q})$. Then by (4.21), p splits completely in $K_t \cap \mathbb{R}$ into a product of $|H|$ distinct primes, namely the product

$$\prod_{\gamma \in H} \gamma(\mathfrak{p}), \tag{4.22}$$

where $\mathfrak{p} = \mathfrak{P} \cap (K_t \cap \mathbb{R})$.

Since $\mathfrak{P}$ is a second degree prime of Ω_t, $\mathfrak{P}$ is fixed by a Frobenius automorphism $\nu \in \text{Gal}(\Omega_t/\mathbb{Q})$ of order 2. Note that $\nu \notin G$, by (4.17). Define $S \subset \text{Gal}(\Omega_t/\mathbb{Q})$ by

$$S := \{\sigma^{-1}\tau\sigma : \sigma \in G\}. \tag{4.23}$$

Our ultimate goal is to show that $\nu \in S$.

We have $|S| = |G|/c$, where c is the number of $\sigma \in G$ which commute with τ in $\mathrm{Gal}(\Omega_t/\mathbb{Q})$. By the remark following (2.8), $(\sigma\tau)^2$ is trivial for each $\sigma \in G$. Let ℓ denote the order of a given $\sigma \in G$. Then

$$\tau\sigma = \sigma^\ell \tau\sigma = \sigma^{\ell-1}(\sigma\tau)^2\tau = \sigma^{\ell-1}\tau.$$

Thus σ commutes with τ if and only if σ^2 is trivial. With notation as in (2.10), there are 2^s elements of G of order ≤ 2. Thus $c = 2^s$, so that by (2.10),

$$|S| = |G|/c = |G|/2^s = |\mathrm{Gal}(\Omega_t/K_t)|. \tag{4.24}$$

In the notation of (4.22), $\nu(\mathfrak{p}) = \mathfrak{p}$, since ν fixes $\mathfrak{P}$. Thus by (4.22), the restriction of ν to $K_t \cap \mathbb{R}$ is the identity element of H, that is, ν is trivial on $K_t \cap \mathbb{R}$. Every $\mu \in S$ is clearly also trivial on $K_t \cap \mathbb{R}$. Moreover, $\mu(\sqrt{-n}) = -\sqrt{-n}$, and also $\nu(\sqrt{-n}) = -\sqrt{-n}$, since $\nu \notin G$. This proves that ν agrees with every $\mu \in S$ on K_t. There are exactly $|\mathrm{Gal}(\Omega_t/K_t)|$ automorphisms in $\mathrm{Gal}(\Omega_t/\mathbb{Q})$ that agree with ν on K_t. Thus (4.24) shows that S consists precisely of those automorphisms in $\mathrm{Gal}(\Omega_t/\mathbb{Q})$ that agree with ν on K_t. Therefore $\nu \in S$. □

Remark. This proof shows that exactly 2^s of the $|G|$ algebraic conjugates of j_n in Ω_t are real. To see this, note that for $\sigma \in G$, $\sigma\tau(\sqrt{-n}) = -\sqrt{-n} = \tau\sigma(\sqrt{-n})$, so σ commutes with τ in $\mathrm{Gal}(\Omega_t/\mathbb{Q})$ if and only if $\sigma\tau(j_n) = \tau\sigma(j_n)$. Therefore σ commutes with τ if and only if $\sigma(j_n)$ is real. Thus j_n has $c = 2^s$ real conjugates.

Acknowledgment: The authors are grateful to H. M. Stark for helpful conversations.

References

[1] S. Ahlgren, K. Ono, and D. Penniston, Zeta functions of an infinite family of $K3$ surfaces, Amer. J. Math. **124** (2002), 353–368.

[2] B. C. Berndt, Ramanujan's Notebooks, Part V, Springer-Verlag, New York, 1998.

[3] H. Cohn, Introduction to the construction of class fields, Cambridge University Press, Cambridge, 1985.

[4] D. A. Cox, Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, Wiley, New York, 1989.

[5] R. Evans, Identities for products of Gauss sums over finite fields, Enseignment Math. **27** (1981), 197–209.

[6] R. Evans, J. Pulham, and J. Sheehan, On the number of complete subgraphs contained in certain graphs, J. Combin. Theory Ser. B **30** (1981), 364–371.

[7] J. Greene, Hypergeometric series over finite fields, Trans. Amer. Math. Soc. **301** (1987), 77–101.

[8] J. Greene and D. Stanton, A character sum evaluation and Gaussian hypergeometric series, J. Number Theory **23** (1986), 136–148.

[9] T. Hutchinson, A conjectural extension of the Gross-Zagier formula on singular moduli, Tokyo J. Math. **21** (1998), 255–265.

[10] M. Koike, Hypergeometric series over finite fields and Apéry numbers, Hiroshima Math. J. **22** (1992), 461–467.

[11] S. Lang, Elliptic Functions, Springer-Verlag, New York, 1987.

[12] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, 3rd ed., Springer-Verlag, Berlin, 2004.

[13] K. Ono, Values of Gaussian hypergeometric series, Trans. Amer. Math. Soc. **350** (1998), 1205–1223.

[14] K. Ono, The web of modularity: Arithmetic of the coefficients of modular forms and q-series, CBMS No. 102, Amer. Math. Soc., Providence, R. I., 2004.

[15] R. Schertz, Weber's class invariants revisited, Journal de Théorie de Nombres de Bordeaux **14** (2002), 325–343.

[16] J. Voight, Quadratic forms that represent almost the same primes, Math. Comp. **76** (2007), 1589–1617.