# Special values of hypergeometric functions over finite fields

June 2007

A senior thesis by Frank Lam written
under the supervision of Ron Evans.

**Acknowledgments**

*This project would not have been possible without the countless hours of kind support and patience from Professor Evans. He defines what it means to be a mentor and his expertise and passion towards math is truly inspirational. I am grateful for this experience and am sure it has already made an enormous impact on my future. Thank you Professor Evans.*

*I would also like to thank my family, without whom I would not be in college today.*

*Finally, I would like to thank Tony Wong, my high school math teacher who was my inspiration to major in math.*

# Special values of hypergeometric functions over finite fields

Frank Lam

June 2007

**Abstract**

Define
$$H(z) = \sum_{x,y \in \mathbb{F}_p} \left( \frac{xy(1-x)(1-y)(1-xyz)}{p} \right)$$
where $p$ is an odd prime, $\left(\frac{a}{p}\right)$ is the Legendre symbol, and $z \in \mathbb{F}_p$. Note that $H(z)$ is a normalized hypergeometric ${}_3F_2$ over $\mathbb{F}_p$. Let $G_n$ and $g_n$ be Ramanujan's class invariants. Let $M_n(x)$ be the minimal polynomial over $\mathbb{Q}$ of $G_n^{-24}$ or $-g_n^{-24}$, according as $n$ is odd or even. Whenever there exists a zero $r$ of $M_n(x)$ mod $p$, we evaluate $H(r)$. This generalizes evaluations of $H(z)$ given by Ono.

## 1 Introduction

In 1984, the systematic study of general hypergeometric series over finite fields was initiated by John Greene in his Ph.D thesis [Gre84]. Prior to that however, work had already been done on specific hypergeometric functions. The main concern of this paper is a function which we shall define as follows.

$$H(z) = \sum_{x,y \in \mathbb{F}_p} \left( \frac{xy(1-x)(1-y)(1-xyz)}{p} \right)$$

where $p$ is an odd prime, $\left(\frac{a}{p}\right)$ is the Legendre symbol, and $z \in \mathbb{F}_p$. In 1981, Ron Evans proved an evaluation of $H(1)$ for all odd primes [Eva81]. In that same year, Evans, Pulham, and Sheehan conjectured a similar evaluation for $H(-1)$ [EPS81] which was proved in 1986 by Stanton and Greene [GS86]. The proofs used ideas analogous to those used to prove evaluations of classical hypergeometric functions over the reals. In 1998, Ono extended these evaluations by using elliptic curves [Ono98] to answer a question posed in 1992 by Koike about $H(\frac{1}{4})$ [Koi92]. In recent years these ideas have been applied in the study of Apéry numbers [AO00], the trace of the Hecke operator [FOP04], and Paley graphs [Wag06].

The primary purpose of this paper is to prove the following new result, which evaluates H(z) for infinitely many $z$, extending the result of Ono.

**Theorem 1.1** *Let $n$ be an integer greater than 1, and $p$ be an odd prime that does not divide $n$. If $r$ is defined to be*

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

*where $G_n$ and $g_n$ are Ramanujan's class invariants, then assuming $r \bmod p$ exists and $r \notin \{0, 1\}$,*

$$H(r) = \begin{cases} (-1)^y(4x^2 - p) & \text{, if } p = x^2 + ny^2 \\ -\left(\frac{1-r}{p}\right) p & \text{, otherwise} \end{cases}$$

*where $x$ and $y$ are taken to be positive integers.*

The existence of $r \bmod p$ will be discussed in Theorem 3.1. Theorem 1.1, our main result, provides evaluations of $H(r)$ for all $n > 1$. Previously $H(r)$ had been evaluated only for $n = 2, 3, 4, 7$; in these cases, $r = -1, 1/4, -1/8, 1/64$, respectively. The proof of this theorem involves a combination of class field theory and elliptic curves which we shall discuss in the following section. Some of the discussion has been motivated by Cohn [Coh85], Miller [Mil98], and Osserman [Oss05].

# 2 Background

The study of class field theory was born in the nineteenth century from two primary motivations. Both Fermat's Last Theorem and Gauss's theory of quadratic forms require the imbedding of fields in larger fields to expand upon ideal theory and the factorization of primes. In relating class field theory to elliptic curves, a new set of tools can be applied to classical problems providing insight on modern problems.

## 2.1 Class Field Theory

For the rest of the paper, we will let $k$ denote the quadratic field $\mathbb{Q}(\sqrt{-n})$ with discriminant $d_k$ where

$$d_k = \begin{cases} -n & \text{, if } n = 3 \bmod 4 \\ -4n & \text{, otherwise.} \end{cases}$$

We will begin our discussion of class field theory with the notion of an *order* of $k$. An *order* $\mathcal{O}$ in a quadratic field $k$ is a subring of the ring of integers of $k$ and a free $\mathbb{Z}$-module of rank 2. Using the notation $[w_1, w_2] = \mathbb{Z}w_1 + \mathbb{Z}w_2$, we can explicitly write

$$\mathcal{O} = \left[1, t\left(\frac{d_k + \sqrt{d_k}}{2}\right)\right]$$

where $t$ denotes the *conductor* of $\mathcal{O}$. Note that when $t = 1$, $\mathcal{O}$ is the ring of integers in $k$, which we shall denote $\mathcal{O}_k$. Furthermore, it is the *maximal order* of $k$, meaning if $\mathcal{O}$ is an order in $k$, then $\mathcal{O} \subseteq \mathcal{O}_k$. We will be primarily concerned with the particular order $\mathbb{Z}[\sqrt{-n}]$. A key invariant of an order is the discriminant, which in our case, can be calculated to be $D = -4n$. From this, we can easily calculate the conductor from $-4n = t^2 d_k$.

A *proper* fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is a $\mathbb{Z}$-module of rank 2 where

$$\mathcal{O} = \{\beta \in k : \beta\mathfrak{a} \subseteq \mathfrak{a}\}.$$

Let $I(\mathcal{O})$ denote the set of all proper fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ denote the set of all principal ideals in $I(\mathcal{O})$, that is, all ideals of the form $\alpha\mathcal{O}, \alpha \in k^*$. Taking the quotient

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

gives us the *ideal class group* of $\mathcal{O}$. When dealing with the maximal order $\mathcal{O}_k$, we will use the notation $I_k = I(\mathcal{O}_k)$ and $P_k = P(\mathcal{O}_k)$.

An ideal $\mathfrak{a}$ is said to be *prime to the conductor* $t$ of $\mathcal{O}$, if $\mathfrak{a} + t\mathcal{O} = \mathcal{O}$. This will allow us to talk about an order $\mathcal{O}$ and its corresponding $\mathcal{O}$-ideals in terms of $\mathcal{O}_k$ and $\mathcal{O}_k$-ideals.

**Proposition 2.1** *Given an order $\mathcal{O}$ of conductor $t$ in $\mathcal{O}_k$,*

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}) \simeq I(\mathcal{O}, t)/P(\mathcal{O}, t) \simeq I_k(t)/P_{k,\mathbb{Z}}(t)$$

*where $I(\mathcal{O}, t)$, $P(\mathcal{O}, t)$, and $I_k(t)$ denote the group of ideals prime to $t$ in $I(\mathcal{O})$, $P(\mathcal{O})$, and $I_k$ respectively and $P_{k,\mathbb{Z}}(t)$ denotes the subgroup of $I_k(t)$ generated by principal ideals of the form $\alpha\mathcal{O}_k$, where $\alpha \in \mathcal{O}_k$ and $\alpha \equiv a \bmod t\mathcal{O}_k$ for some $a \in \mathbb{Z}$ relatively prime to $t$.*

**Proof** See [Cox89, Prop. 7.19, 7.20, 7.22]

□

We can now define $I_k(t)/P_{k,\mathbb{Z}}(t)$ to be the *ring class group* of the order $\mathcal{O}$ of conductor $t$. There is a unique Abelian extension $\Omega_t$ of $k$ such that

$$C(\mathcal{O}) \simeq I_k(t)/P_{k,\mathbb{Z}}(t) \simeq \mathrm{Gal}(\Omega_t/k)$$

which we shall call the *ring class field* modulo $t$ over $k$ [Sch02, p. 328]. Using the *modular j-invariant*, we can generate the ring class field of any order.

**Theorem 2.2** *Let $\mathcal{O}$ be an order with conductor $t$ and $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $j(\mathfrak{a})$ is an algebraic integer and $k(j(\mathfrak{a})) = \Omega_t$.*

**Proof** See [Cox89, Thm. 11.1].

□

Of particular interest is when $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$. By definition of the $j$-invariant, we have that $j(\sqrt{-n}) = j(\mathfrak{a})$ where $\mathfrak{a} = [1, \sqrt{-n}]$. Thus, the associated ring class field can be described $\Omega_t = k(j(\sqrt{-n}))$.

**Theorem 2.3** *Let $n$ be a positive integer and $p$ be an odd prime. If $p \nmid n$, then*

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \text{ has an integer solution}$$

*where $f_n(x)$ is the minimal polynomial of an algebraic integer $\alpha$ for which $k(\alpha) = \Omega_t$, the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ with conductor $t$.*

**Proof** See [Cox89, Thm. 9.2].

□

We complete the section on class field theory with the notion of a prime ideal $\mathfrak{p}$ in $k$ *splitting completely* in $\Omega_t$. By this, we mean that if $g = [\Omega_t : k]$, then $\mathfrak{p} = \mathfrak{B}_1 ... \mathfrak{B}_g$ where $\mathfrak{B}_i$ is prime in $\Omega_t$.

**Theorem 2.4** *An ideal* $\mathfrak{p}$ *splits completely in the ring class field* $\Omega_t$ *if and only if it is a principal prime ideal in* $P_{k,\mathbb{Z}}(t)$.

**Proof** See [Cox89, p. 182].

□

## 2.2 Elliptic Curves and Complex Multiplication

We will begin this section with the definition of an *elliptic function*. A function $f(z)$ on $\mathbb{C}$ is an *elliptic function* provided that it is all of the following:

(i) doubly periodic,

(ii) analytic, except at the poles,

(iii) and has no singularities other than poles in the finite part of the complex plane.

A function $f$ is *periodic* if there is some constant $w_1 \in \mathbb{C}^*$ such that $f(z) = f(z + w_1)$. It is *doubly periodic* if $f(z) = f(z + w_1) = f(z + w_2)$ for another constant $w_2 \in \mathbb{C}^*$ assuming that the ratio $\frac{w_1}{w_2}$ is not real. The values $w_1$ and $w_2$ generate a *lattice*

$$L = \{nw_1 + mw_2 : n, m \in \mathbb{Z}\}$$

which stretches across the complex plane $\mathbb{C}$. A lattice corresponding to an elliptic function is called *nondegenerate* because the ratio $\frac{w_1}{w_2}$ is not real. The constants $w_1$ and $w_2$ are called *fundamental* if there is no point $w$ within a parallelogram of $\mathbb{C}$ with corners at $z$, $z + w_1$, $z + w_2$, $z + w_1 + w_2$ such that $f(w) = f(z)$. We will assume that when we mention lattices, they are both nondegenerate and have fundamental periods $w_1$ and $w_2$.

We define the *Weierstrass* $\wp$ *function* to be

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq w \in L} \frac{1}{(z-w)^2} - \frac{1}{w^2}$$

which converges absolutely and uniformly on compact subsets of $\mathbb{C} - L$ so that $\wp$ can be differentiated term by term to get

$$\wp'(z) = -2 \sum_{0 \neq w \in L} \frac{1}{(z-w)^3}$$

which converges on the same compact subsets. Given the *Eisenstein series of weight* $2k$ defined to be

$$G_{2k}(L) = \sum_{0 \neq w \in L} w^{-2k},$$

it can be shown that any elliptic function can be written in terms of $\wp$ and $\wp'$ [Apo97, p. 11], which satisfy

$$\wp'^2(z) = 4\wp^3(z) - 60G_4\wp(z) - 140G_6.$$

Letting $y = \wp'$, $x = \wp$, $g_2 = 60G_4$, and $g_3 = 140G_6$ gives

$$E : y^2 = 4x^3 - g_2x - g_3$$

which is an *elliptic curve* written in *Weierstrass normal form*. The definition of an elliptic curve also requires that the cubic polynomial in $x$ has 3 distinct zeros. Note that this means any lattice has a corresponding elliptic curve. The *discriminant* of $E$ can be written as

$$\Delta_E = g_2^3 - 27g_3^2.$$

This allows us to define the *$j$-invariant* of an elliptic curve to be

$$j_E = \frac{(12g_2)^3}{\Delta_E}.$$

Recall that Theorem 2.2 required the argument of $j$ to be a proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$ that can be written $[\alpha, \beta]$ where $\alpha, \beta \in \mathcal{O}$. A central notion in complex multiplication is that $\alpha$ and $\beta$ correspond directly to $w_1$ and $w_2$, the underlying generators of a lattice $L$ for a class of elliptic curves. Explicitly speaking, if $j_E = j(\mathfrak{a})$, then we say that $E$ has complex multiplication by the order $\mathcal{O}$. This implies that if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class, then $j(\mathfrak{a}) = j(\mathfrak{b})$.

We are interested in elliptic curves over a finite field $\mathbb{F}_p$ where $p$ is prime. We will write $\bar{E}$ to denote the *nondegenerate reduction* of $E$ by $p$, that is $\bar{E}$ remains an elliptic curve. There are two types of elliptic curves over a finite field, namely *ordinary* and *supersingular*. For our purposes, we will use the following result as our distinguishing criterion.

**Theorem 2.5** *Let $E$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field $k$. Let $\bar{E}$ be a nondegenerate reduction of $E$ by a prime $p$. The curve $\bar{E}$ is supersingular if and only if $p$ has only one prime above it in $k$, that is, either $p$ is inert or ramified in $k$. Furthermore, $\bar{E}$ has $p+1$ points mod $p$*

**Proof** See [Lan73, Sec. 13.4, Thm. 12].

□

By a point on $E$, we mean a solution $(x, y) \in (\mathbb{F}_p, \mathbb{F}_p) \cup (\infty, \infty)$. We may now look at the other case, when $E$ is ordinary.

**Theorem 2.6** *Let $E$ be an elliptic curve over a finite field $\mathbb{F}_p$ with complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field $k$. That is, $E$ is ordinary. If $p = \pi\bar{\pi}$ where $\pi \in \mathcal{O}$, then there are $p + 1 - (\pi + \bar{\pi})$ points on $E$.*

**Proof** See [Sil94, Chapter V, Exercise 5.10] and [Cox89, Thm. 14.16].

□

## 3 Proof of Theorem 1.1

We will begin this section by looking at the existence of $r \bmod p$. Following, we will relate the parity of $y$ and value of the Legendre symbol $\left(\frac{1-r}{p}\right)$. Along with the results of §2.2, we will be able to prove our main result.

Our first theorem examines the relationship between $r$ and $p$.

**Theorem 3.1** *Let $p$ be an odd prime and $x$, $y$, and $n$ be positive integers. Define*

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

*where $G_n$ and $g_n$ are Ramanujan's class invariants. Then $r$ generates the ring class field $k(j(\sqrt{-n}))$. Additionally, the following hold:*

*(i) If $p = x^2 + ny^2$, then $r \bmod p$ exists.*

*(ii) If $\left(\frac{-n}{p}\right) = 1$ but $p \neq x^2 + ny^2$, then $r \bmod p$ does not exist.*

*(iii) If $p$ is inert from $\mathbb{Q}$ to $k$, then $r \bmod p$ conditionally exists.*

We provide a conjecture about the existence of $r$ in the third case.

**Conjecture 3.2** *If $p$ is inert from $\mathbb{Q}$ to $k$, then $r \bmod p$ exists if and only if $-p$ is a square mod $n$.*

**Proof** *(Theorem 3.1)* We may write the Ramanujan class invariants raised to the $-24^{\text{th}}$ power in terms of Weber functions so that we can conclude that $r$ generates the ring class field $k(j(\sqrt{-n}))$ [Sch02]. By Theorem 2.2, we know that $k(j(\sqrt{-n}))$ corresponds to the order $\mathbb{Z}[\sqrt{-n}]$ so that $r$ generates the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$.

First consider the case where $\left(\frac{-n}{p}\right) = 1$ and $p = x^2 + ny^2$. By Theorems 2.2 and 2.3, it is clear that $M_n(z) = 0$, where $M_n$ is taken to be the minimal polynomial of $r$, has integer solutions mod $p$ so that $r$ exists mod $p$.

Now we consider the case that $\left(\frac{-n}{p}\right) = 1$ but $p \neq x^2 + ny^2$. By Theorem 2.3, it follows that $M_n(z) = 0$ has no integer solutions mod $p$ so $r$ does not exist mod $p$ in this case.

Finally, we consider the case that $p$ is inert from $\mathbb{Q}$ to $k$. It follows that $p\mathcal{O}$ is a prime ideal which splits completely in $k(r)$ by Theorem 2.4. This implies that $M_n$ splits completely over $\mathcal{O}/(p) \simeq \mathbb{F}_{p^2}$ [Nar73, p. 161]. Since $r$ is real, it follows that $M_n$ is defined over $\mathbb{Q}$ so it implies that $M_n$ splits into linear factors in $\mathbb{F}_{p^2}$. Therefore, $r \bmod p$ exists when there are zeros of $M_n$ in $\mathbb{F}_p \subset \mathbb{F}_{p^2}$.

$\square$

**Lemma 3.3** *$j(\sqrt{1-r})$ generates $\Omega_{2t}$, the ring class field of conductor $2t$.*

**Proof** Consider $k(j(\sqrt{-n}))$ which we know by Theorem 3.1 is generated by $r = -g_n^{-24}$ in the case that $n$ is even. Replacing $n$ by $4n$ implies that $k(j(\sqrt{-4n}))$

is generated by $-g_{4n}^{-24}$ for all $n$. By identities of Ramanujan class invariants [Ber97, p.187], we have that

$$g_{4n} = \begin{cases} 2^{1/8} g_n \left( g_n^8 + \sqrt{g_n^{16} + g_n^{-8}} \right)^{\frac{1}{8}} & \text{, if } n \text{ is even} \\ 2^{1/8} G_n \left( G_n^8 + \sqrt{G_n^{16} - G_n^{-8}} \right)^{\frac{1}{8}} & \text{, if } n \text{ is odd} \end{cases}$$

$$\text{so } g_{4n}^{24} = \frac{8}{r^2}(4 - 3r + (4 - r)\sqrt{1 - r})$$

Thus, we have that $k(j(\sqrt{-4n})) = k(\sqrt{1 - r})$. Applying Theorem 2.2, it is clear that $k(\sqrt{1 - r}) = \Omega_{2t}$.

□

**Theorem 3.4** *If* $p = x^2 + ny^2$*, then* $\left(\frac{1-r}{p}\right) = (-1)^y$.

**Proof** Write $\pi = x + y\sqrt{-n}$. We will prove the following equivalences where $\mathfrak{p}$ is a prime ideal above $\pi$ in $k(r)$ and $\Omega_{2t}$ is the ring class field of conductor $2t$.

$$\begin{aligned} \left(\frac{1-r}{p}\right) = 1 &\Leftrightarrow 1 - r \bmod \mathfrak{p} \text{ is a square in } k(r) && (1) \\ &\Leftrightarrow x^2 - (1 - r) \bmod \mathfrak{p} \text{ splits into linear factors} && (2) \\ &\Leftrightarrow \mathfrak{p} \text{ splits in } \Omega_{2t} && (3) \\ &\Leftrightarrow y \text{ even} && (4) \\ &\Leftrightarrow (-1)^y = 1 && (5) \end{aligned}$$

For the first equivalence, since $\mathfrak{p} \mid p$ in $k(r)$, it is clear that $\left(\frac{1-r}{p}\right) = 1$ implies that $1 - r$ is a square mod $\mathfrak{p}$. It remains to show that when $1 - r$ is a square mod $\mathfrak{p}$, then it is a square mod $p$. In order to do this, it suffices to show $\mathbb{Z}/(p) \simeq \{\text{integers in } \Omega_t\}/(\mathfrak{p})$. Since $p$ splits completely, $\mathfrak{p}$ has degree 1 over $p$ so that the previous statement holds and the first equivalence follows.

The second and last equivalences are clear.

Note that $x^2 - (1 - r)$ is the minimal polynomial of $\sqrt{1 - r}$ which generates $\Omega_{2t}$ from $k$ by Lemma 3.3. Since this polynomial splits mod $\mathfrak{p}$, $\mathfrak{p}$ will split in $\Omega_{2t}$ [Nar73, p. 161] so that (2)⇔(3).

Finally, since $\mathfrak{p}$ splits completely in $\Omega_{2t}$, it is in the principal ring class $P_{k,\mathbb{Z}}(2t)$ by Theorem 2.4 so that (3)⇔(4) follows. Therefore, the theorem holds.

□

We are now ready to prove our main result.

**Proof** *(Theorem 1.1)*

Let $E$ be the following elliptic curve.

$$y^2 = (x - 1)\left(x^2 - \frac{1}{1 - s}\right)$$

By mapping $(x, y) \to (x + \frac{1}{3}, \frac{y}{2})$, we can write $E$ in Weierstrass form,

$$y^2 = 4x^3 - g_2 x - g_3$$

which we will denote as $E'$ where $g_2 = \frac{4}{3} + \frac{4}{1-s}$ and $g_3 = \frac{8}{27} - \frac{8}{3(1-s)}$. We can calculate the discriminant and $j$-invariant as follows.

$$\Delta_{E'} = \frac{64s^2}{(1-s)^3}$$

$$j_{E'} = \frac{(12g_2)^3}{\Delta_{E'}} = \frac{64(4-s)^3}{s^2}$$

Setting $j_{E'} = j(\sqrt{-n})$ gives $E$ complex multiplication by $\mathbb{Z}[\sqrt{-n}]$. This gives the cubic equation

$$64s^3 + (j(\sqrt{-n}) - 768)s^2 + 3072s - 4096 = 0$$

and substituting the well-known equality

$$j(\sqrt{-n}) = \frac{256(1-k_n^2+k_n^4)^3}{(k_n^2-k_n^4)^2}$$

where $k_n$ is an elliptic modulus [BB98, Thm. 4.4] and solving for $s$ gives three solutions, namely

$$\begin{aligned} s_1 &= 4k_n^2(1-k_n^2) = G_n^{-24} \\ s_2 &= -\frac{4k_n^2}{(1-k_n^2)^2} = -g_n^{-24} \\ s_3 &= -\frac{4(1-k_n^2)}{k_n^4} = -g_{4n}^{-24}. \end{aligned}$$

The rightmost equalities result from [Ber97, p. 185] where $G_n$ and $g_n$ are called Ramanujan class invariants. We can thus define $E$ such that $s = s_1$ when $n$ is odd and $s = s_2$ when $n$ is even so that we may replace $s$ with $r$.

When $p$ is inert, $\bar{E}$ is supersingular by Theorem 2.5, so $\bar{E}$ has $p+1$ points over $\mathbb{F}_p$. Suppose now that $p$ splits, so $p = x^2 + ny^2 = \pi\bar{\pi}$ with $\pi = x + y\sqrt{-n} \in \mathbb{Z}[\sqrt{-n}]$. Then by Theorem 2.6, $\bar{E}$ has $p + 1 \pm 2x$ points.

Now consider the transformation of $E$ by $(x, y) \to (\frac{x}{\lambda^2}, \frac{y}{\lambda^3})$ where $\lambda = \frac{4(r-1)}{r}$ which gives the curve

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

In [Ono03, p. 190], Ono calculates that if the above curve has $p + 1 - a(p)$ points over $\mathbb{F}_p$, then

$$H\left(\frac{4}{4-\lambda}\right) = \left(\frac{\lambda^2 - 4\lambda}{p}\right)(a(p)^2 - p)$$

This new curve is isomorphic to $E$ so it has $p+1$ or $p+1 \pm 2x$ according as $E$ is supersingular or not.

By substituting $\lambda = \frac{4(r-1)}{r}$ in the above, we can see that when $E$ is supersingular and $r$ exists mod $p$, $a(p) = 0$ so

$$H(r) = -\left(\frac{1-r}{p}\right)p.$$

When $E$ is ordinary, $a(p) = \pm 2x$ so

$$H(r) = (-1)^y (4x^2 - p.)$$

Therefore, using Theorem 3.4, the main result is proven.

$\square$

# 4 Example

For $n = 58$ and $p = 67$, $p = x^2 + 58y^2 = 67$ so we have $x = 3$ and $y = 1$. At $n = 58$,

$$\begin{aligned} r &= -g_{58}^{-24} \\ &= -\left[2^{-\frac{1}{4}} e^{\pi\sqrt{58}/24} \prod_{k=1,3,5,..}^{\infty} \left(1 - e^{-k\pi\sqrt{58}/24}\right)\right]^{-24} \quad \text{[Ber97, p. 183]} \\ &= -\left(\frac{\sqrt{29}-5}{2}\right)^{12} \quad \text{[Ber97, p. 201]} \end{aligned}$$

which evaluates to $r = 5$ or 27 mod 67. Taking $r = 5$ (arbitrarily), this gives the elliptic curve

$$y^2 = (x-1)\left(x^2 - \frac{1}{1-5}\right) \mod 67$$

which has $67 + 1 \pm 6$ points mod 67. It follows that $H(5) = (-1)^1(4(3)^2 - 67) = 31$.

# References


[AO00] Scott Ahlgren and Ken Ono. A Gaussian hypergeometric series evaluation and Apéry numbers congruences. *J. reine agnew. Math*, 518:187–212, 2000.

[Apo97] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory (Graduate Texts in Mathematics)*. Springer, 1997.

[BB98] Jonathan M. Borwein and Peter B. Borwein. *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity*. Wiley-Interscience, 1998.

[Ber97] Bruce C. Berndt. *Ramanujan's Notebooks, Part V*. Springer, 1997.

[Coh85] Harvey Cohn. *Introduction to the construction of class fields (Cambridge studies in advanced mathematics)*. Cambridge University Press, 1985.

[Cox89] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Wiley-Interscience, 1989.

[EPS81] R. Evans, J. R. Pulham, and J. Sheehan. On the number of complete subgraphs contained in certain graphs. *Journal of Combinatorial Theory*, 30:364–371, 1981.

[Eva81] Ron Evans. Identities for products of Gauss sums over finite fields. *Enseignement Math*, 27:197–209, 1981.

[FOP04] Sharon Frechette, Ken Ono, and Matthew Papanikolas. Gaussian hypergeometric functions and Hecke operators. *International Mathematics Research Notices*, 60:3233–3262, 2004.

[Gre84] John Greene. *Character Sum Analogues for Hypergeometric and Generalized Hypergeometric Functions over Finite Fields*. PhD thesis, University of Minnesota, Minneapolis, 1984.

[GS86] John Greene and Dennis Stanton. A character sum evaluation and Gaussian hypergeometric series. *Journal of Number Theory*, 23:136–148, 1986.

[Koi92] Masao Koike. Hypergeometric series over finite fields and Apéry numbers. *Hiroshima Mathematical Journal*, 22:461–467, 1992.

[Lan73] Serge Lang. *Elliptic Functions*. Addison-Wesley Publishing Company, Inc., 1973.

[Mil98] Wendy Miller. *Counting Points on Certain CM Elliptic Curves Modulo Primes*. PhD thesis, University of California, San Diego, 1998.

[Nar73] Wladyslaw Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Polish Scientific Publishers PWN, 1973.

[Ono98] Ken Ono. Values of Gaussian hypergeometric series. *Transactions of the American Mathematical Society*, 350:1205–1223, 1998.

[Ono03] Ken Ono. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and Q-Series (Cbms Regional Conference Series in Mathematics)*, volume 102. American Mathematical Society, 2003.

[Oss05] Brian Osserman. Math 254a: Number theory lectures notes. University of California, Berkeley, 2005.

[Sch02] Reinhard Schertz. Weber's class invariants revisited. *Journal de Théorie des Nombres de Bordeaux*, 14(325-343), 2002.

[Sil94] Joseph H. Silverman. *The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics)*. Springer, 1994.

[Wag06] Nicholas Wage. Character sums and Ramsey properties of generalized Paley graphs. *INTEGERS: Electronic Journal of Combinatorial Number Theory*, 2006.