Gauss’s $2F_1$ hypergeometric function and the congruent number elliptic curve

by

AHMAD EL-GUINDY (Cairo) and KEN ONO (Madison, WI)

1. Introduction and statement of results. For $\lambda \in \mathbb{C} \setminus \{0, 1\}$, the Legendre normal form elliptic curve $E(\lambda)$ is given by

$$E(\lambda) : y^2 = x(x-1)(x-\lambda).$$

It is well known (for example, see [3]) that $E(\lambda)$ is isomorphic to the complex torus $\mathbb{C}/L_\lambda$, where $L_\lambda = \mathbb{Z} \omega_1(\lambda) + \mathbb{Z} \omega_2(\lambda)$, and the periods $\omega_1(\lambda)$ and $\omega_2(\lambda)$ are given by the integrals

$$\omega_1(\lambda) = \int_{-\infty}^{0} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} \quad \text{and} \quad \omega_2(\lambda) = \int_{1}^{\infty} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}.$$

These integrals can be expressed in terms of Gauss’s hypergeometric function

$$2F_1(x) := 2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; x\right) = \sum_{n=0}^{\infty} \frac{(\frac{1}{2})_n (\frac{1}{2})_n}{(n!)^2} x^n,$$

where $(a)_n = a(a+1) \cdots (a+n-1)$. More precisely, for $\lambda \in \mathbb{C} \setminus \{0, 1\}$ with $|\lambda|, |\lambda-1| < 1$, we have

$$\omega_1(\lambda) = i\pi 2F_1(1-\lambda) \quad \text{and} \quad \omega_2(\lambda) = \pi 2F_1(\lambda).$$

The parameter $\lambda$ is a “modular invariant”. To make this precise, for $z$ in $\mathbb{H}$, the upper half of the complex plane, we define the lattice $\Lambda_z := \mathbb{Z} + \mathbb{Z} z$, and let $\wp$ be the Weierstrass elliptic function associated to $\Lambda_z$. The function $\lambda(z)$ defined by

$$\lambda(z) := \frac{\wp\left(\frac{1}{2}\right) - \wp\left(\frac{z+1}{2}\right)}{\wp\left(\frac{z}{2}\right) - \wp\left(\frac{z+1}{2}\right)} = 16 q^{1/2} \prod_{n=1}^{\infty} \left(\frac{1 + q^n}{1 + q^{n-1/2}}\right)^8,$$

2010 Mathematics Subject Classification: Primary 11F30, 11F11, 11F37, 14H52.

Key words and phrases: Legendre elliptic curves, hypergeometric functions.

DOI: 10.4064/aa144-3-2

© Instytut Matematyczny PAN, 2010
where \( q := e^{2\pi i z} \), is a modular function on \( \Gamma(2) \) that parameterizes the Legendre normal family above. In particular, we have \( \mathbb{C}/\Lambda \cong E(\lambda(z)) \). Furthermore, for any lattice \( \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \) with \( \Im(\omega_1/\omega_2) > 0 \), \( \mathbb{C}/\Lambda \) is isomorphic (over \( \mathbb{C} \)) to \( E(\lambda) \) if and only if \( \lambda \) is in the orbit of \( \lambda(\omega_1/\omega_2) \) under the action of the modular quotient \( \text{SL}_2(\mathbb{Z})/\Gamma(2) \cong \text{SL}_2(\mathbb{Z}/2\mathbb{Z}) \). This quotient is isomorphic to \( S_3 \), and the orbit of \( \lambda \) is
\[
\left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\}.
\]

In view of this structure, it is natural to study expressions like
\[
(5) \quad \omega_2(\lambda) - \omega_2\left( \frac{\lambda}{\lambda-1} \right)
\]
which measures the difference between periods of the isomorphic elliptic curves \( E(\lambda) \) and \( E\left( \frac{\lambda}{\lambda-1} \right) \). Taking into account that \( \lambda(z) \) has level 2, it is natural to consider the modular function
\[
(6) \quad L(z) := \frac{2F_1(\lambda(z)) - 2F_1\left( \frac{\lambda(z)}{\lambda(z)-1} \right)}{2F_1(\lambda(2z)) - 2F_1\left( \frac{\lambda(2z)}{\lambda(2z)-1} \right)} = q^{-1} + 2q^3 - q^7 - 2q^{11} + \cdots.
\]
It turns out that \( L(z) \) is a Hauptmodul for the genus zero congruence group \( \Gamma_0(16) \). Here we study the \( p \)-adic properties of the Fourier expansion of \( L(z) \) using the theory of harmonic Maass forms. To make good use of this theory, we “normalize” \( L(z) \) to obtain a weight 2 modular form whose poles are supported at the cusp \( \infty \) for a modular curve with positive genus. The first case where this occurs is \( \Gamma_0(32) \), where the space of weight 2 cusp forms is generated by the unique normalized cusp form
\[
(7) \quad g(z) := q \prod_{n=1}^{\infty} (1 - q^{4n})^2 (1 - q^{8n})^2 = q - 2q^5 - 3q^9 + 6q^{13} + \cdots.
\]
Our normalization is
\[
(8) \quad \mathcal{F}(z) = \sum_{n=-1}^{\infty} C(n)q^n := -g(z)L(2z) = -q^{-1} + 2q^3 + q^7 - 2q^{11} + 5q^{15} + \cdots.
\]

**Remark.** It turns out that \( \mathcal{F}(z) \) satisfies the following identities:
\[
\mathcal{F}(z) = \frac{1}{2\pi i} \cdot \frac{d}{dz} L(z) - 4 \frac{g(z)}{L(2z)} = L(z) 2F_1\left( \frac{\lambda(4z)}{\lambda(4z)-1} \right) \cdot 2F_1(\lambda(8z)).
\]

The cusp form \( g(z) \) plays a special role in the context of Legendre normal form elliptic curves. Under the Shimura–Taniyama correspondence, \( g(z) \) is the cusp form which gives the Hasse–Weil \( L \)-function for \( E(-1) \), the congruent number elliptic curve
\[
(9) \quad E(-1) : \quad y^2 = x^3 - x.
\]
By the change of variable $x \mapsto x - 1$, we find that $E(-1)$ is isomorphic to $E(2)$. Since $\lambda = \frac{\lambda}{\lambda - 1}$ when $\lambda = 2$, we see that $g(z)$ is the cusp form corresponding to the “fixed point” of $[5]$. We show that $F(z)$ has some surprising $p$-adic properties which relate the Hauptmodul $L(z)$ to the cusp form $g(z)$. These properties are formulated using Atkin’s $U$-operator

$$\sum a(n)q^n|U(m) := \sum a(mn)q^n.$$  \hspace{1cm} (10)

**Theorem 1.1.** If $p \equiv 3 \pmod{4}$ is a prime for which $p \nmid C(p)$, then as a $p$-adic limit we have

$$g(z) = \lim_{w \to \infty} \frac{\mathfrak{F}(z)|U(p^{2w+1})}{C(p^{2w+1})}.$$  \hspace{1cm} (11)

**Remark.** The $p$-adic limit in Theorem 1.1 means that if we write $g(z) = \sum_{n=1}^{\infty} a_n q^n$, then for all positive integers $n$ the difference

$$C(np^{2w+1})/C(p^{2w+1}) - a_n$$

becomes uniformly divisible by arbitrarily large powers of $p$ as $w \to +\infty$.

**Remark.** A short calculation in MAPLE shows that $p \nmid C(p)$ for every prime $p \equiv 3 \pmod{4}$ less than 25,000. We speculate that there are no primes $p \equiv 3 \pmod{4}$ for which $p | C(p)$.

**Example.** Here we illustrate the phenomenon in Theorem 1.1 for the primes $p = 3$ and 7. For convenience, we let

$$\mathfrak{F}_w(p; z) := \frac{\mathfrak{F}(z)|U(p^{2w+1})}{C(p^{2w+1})}.$$  \hspace{1cm} (12)

If $p = 3$, then

$$\mathfrak{F}_0(3; z) = q + \frac{5}{2}q^5 + 6q^9 - 34q^{17} + \cdots \equiv g(z) \pmod{3},$$

$$\mathfrak{F}_1(3; z) = q + \frac{5}{2}q^5 - \frac{519}{2}q^9 - \frac{39}{4}q^{13} - 1258q^{17} + \cdots \equiv g(z) \pmod{3^2},$$

$$\mathfrak{F}_2(3; z) = q - \frac{665}{346}q^5 + \frac{26923476}{173}q^9 + \cdots \equiv g(z) \pmod{3^3},$$

$$\mathfrak{F}_3(3; z) = q - \frac{150604045}{4487246}q^5 - \frac{3403132854836996346566}{8974492}q^9 + \cdots \equiv g(z) \pmod{3^4}.$$

If $p = 7$, then

$$\mathfrak{F}_0(7; z) = q + 40q^5 + 18q^9 + 104q^{13} + 51q^{17} + \cdots \equiv g(z) \pmod{7},$$

$$\mathfrak{F}_1(7; z) = q + \frac{19167440}{43}q^5 - \frac{93915}{43}q^9 + \frac{215354309456}{43}q^{13} + \cdots \equiv g(z) \pmod{7^2}.$$  

**Theorem 1.1** arises naturally in the theory of harmonic Maass forms. The proof depends on establishing a certain relationship between $F$ and $g$. This is achieved by viewing them as certain derivatives of the holomorphic and non-holomorphic parts of a harmonic weak Maass form that we explicitly construct as a Poincaré series. We then use recent work of Guerzhoy, Kent,
and the second author [2] that explains how to relate such derivatives of a harmonic Maass form \( p \)-adically (cf. Section 2).

2. Proof of Theorem 1.1. Here we prove Theorem 1.1 after recalling crucial facts about harmonic Maass forms.

2.1. Harmonic Maass forms and a certain Poincaré series. We begin by recalling some basic facts about harmonic Maass forms (for example, see Sections 7 and 8 of [6]). Suppose that \( k \geq 2 \) is an even integer. The weight \( k \) hyperbolic Laplacian is defined by

\[
\Delta_k = -y^2 \left( \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right) + iky \left( \frac{\partial}{\partial x} + i \frac{\partial}{\partial y} \right).
\]

A harmonic weak Maass form of weight \( k \) on \( \Gamma_0(N) \) is a smooth function \( f : \mathbb{H} \to \mathbb{C} \) satisfying:

- \( f \) is invariant under the usual \( |k\gamma \) slash operator for every \( \gamma \in \Gamma_0(N) \).
- \( \Delta_k f = 0 \).
- There exists a polynomial

\[
P_f = \sum_{n=0}^{nf} c^n_f (-n)q^{-n} \in \mathbb{C}[q^{-1}]
\]

such that \( f(z) - P_f(z) = O(e^{-\varepsilon y}) \) as \( y \to \infty \) for some \( \varepsilon > 0 \). We require similar growth conditions at all other cusps of \( \Gamma_0(N) \).

The polynomial \( P_f \), for a given cusp, is called the principal part of \( f \) at that cusp. The vector space of all forms satisfying these conditions is denoted by \( H_k(N) \). Note that if \( M^!_k(N) \) denotes the space of weakly holomorphic modular forms on \( \Gamma_0(N) \) then \( M^!_k(N) \subset H_k(N) \).

Any form \( f \in H_{2-k}(N) \) has a natural decomposition as \( f = f^+ + f^- \), where \( f^+ \) is holomorphic on \( \mathbb{H} \) and \( f^- \) is a smooth non-holomorphic function on \( \mathbb{H} \). Let \( D \) be the differential operator \( \frac{1}{2\pi i} \frac{d}{dz} \) and let \( \xi_r := 2iy^r \frac{\partial}{\partial z} \). Then

\[
D^{k-1}(f) = D^{k-1}(f^+) \in M^1_k(N) \quad \text{and} \quad \xi_{2-k}(f) = \xi_{2-k}(f^-) \in S_k(N),
\]

where \( S_k(N) \) is the space of weight \( k \) cusp forms on \( \Gamma_0(N) \). In particular, there is a cusp form \( g_f \) of weight \( k \) attached to any Maass form \( f \) of weight \( 2-k \). Since \( \xi_{2-k}(M^1_{2-k}(N)) = 0 \), it follows that many harmonic Maass forms correspond to \( g_f \). In [1], Bruinier, Rhoades, and the second author narrow down the correspondence by specifying certain additional restrictions on \( f \).

2.2. Specifically, they define a harmonic weak Maass form \( f \in H_{2-k}(N) \) to be good for a normalized newform \( g \in S_k(N) \), whose coefficients lie in a number field \( F_g \), if the following conditions are satisfied:

- The principal part of \( f \) at the cusp \( \infty \) belongs to \( F_g[q^{-1}] \).
- The principal parts of \( f \) at other cusps (if any) are constant.
\[ \xi_{2-k}(f) = g/\|g\|^2, \] where \( \| \cdot \| \) is the Petersson norm.

It is also shown in that paper that every newform has a corresponding good Maass form.

Theorem 1.1 depends on the interplay between the newform \( g(z) \) in (7) and a certain harmonic Maass form which is intimately related to the Hauptmodul \( L(z) \). These forms are constructed using Poincaré series.

We first recall the definition of (holomorphic) Poincaré series. Denote by \( \Gamma_0(N)_{\infty} \) the stabilizer of \( \infty \) in \( \Gamma_0(N) \) and set \( e(z) := e^{2\pi i z} \). For integers \( m, k > 2 \) and positive \( N \), the classical holomorphic Poincaré series is defined by

\[ P(m, k, N; z) := \sum_{\gamma \in \Gamma_0(N)_{\infty} \setminus \Gamma_0(N)} e(tz) |_{k} \gamma = q^m + \sum_{n=1}^{\infty} a(m, k, N; n) q^n. \]

We extend the definition to the case \( k = 2 \) using “Hecke’s trick”. For a positive integer \( m \), we have

\[ P(m, k, N; z) \in S_k(N) \quad \text{and} \quad P(-m, k, N; z) \in M_k^!(N). \]

The Poincaré series \( P(-m, k, N; z) \) is holomorphic at all cusps except \( \infty \) where the principal part is \( q^{-m} \).

The coefficients of these functions are infinite sums of Kloosterman sums multiplied with the \( I_n \) and \( J_n \) Bessel functions. The modulus \( c \) Kloosterman sum \( K_c(a, b) \) is

\[ K_c(a, b) := \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} e\left(\frac{av + bv^{-1}}{c}\right). \]

It is well known (for example, see [4] or Proposition 6.1 of [1]) that for positive integers \( m \) we have

\[ a(m, k, N; n) = 2\pi (-1)^{k/2} \left(\frac{n}{m}\right)^{(k-1)/2} \cdot \sum_{c=1}^{\infty} \frac{K_{nc}(m, n)}{Nc} \cdot J_{k-1} \left(\frac{4\pi \sqrt{mn}}{Nc}\right), \]

\[ a(-m, k, N; n) = 2\pi (-1)^{k/2} \left(\frac{n}{m}\right)^{(k-1)/2} \cdot \sum_{c=1}^{\infty} \frac{K_{nc}(-m, n)}{Nc} \cdot I_{k-1} \left(\frac{4\pi \sqrt{mn}}{Nc}\right). \]

Furthermore, the Petersson norm of the cusp form \( P(m, k, N; z) \) for positive \( m \) is given by

\[ \| P(m, k, N; z) \|^2 = \frac{(k-2)!}{(4\pi m)^{k-1}} (1 + a(m, k, N; m)). \]

These Poincaré series are related to the Maass–Poincaré series which we now briefly recall. Let \( M_{\nu, \mu}(z) \) be the usual Whittaker function given by

\[ M_{\nu, \mu}(z) = e^{-z/2} z^{\nu+1/2} \, 1F1(\mu - \nu + 1/2, 1 + 2\nu; z), \]

where \( 1F1(a, b; z) = \sum_{n=0}^{\infty} \frac{(a)_n z^n}{(b)_n n!} \). For \( y > 0 \) set

\[ M_{-m, k}^*(x + iy) := e(-mx)(4\pi my)^{-k/2} M_{-k/2,(1-k)/2}(4\pi my). \]
Then, for $k > 2$ the Poincaré series

$$Q(-m, k, N; z) := \sum_{\gamma \in \Gamma_0(N) \setminus \Gamma_0(N)}^\infty M^*_{-m,k}(z)|_{k\gamma}$$

is in $H_{2-k}(N)$ (for example, see [1]). This series converges normally for $k > 2$, and we can extend its definition to the case $k = 2$ using analytic continuation to get a form in $H_0(N)$. These different Poincaré series are connected via the differential operators $D$ and $\xi_{2-k}$ as follows (see §6.2 of [1]):

$$D^{k-1}(Q(-m, k, N; z)) = -m^{k-1}P(-m, k, N; z),$$

(14)

$$\xi_{2-k}(Q(-m, k, N; z)) = \left(\frac{4\pi m}{k-1}\right)^{k-1} \cdot P(m, k, N; z).$$

(15)

The following lemma relates $\mathcal{F}$ and $g$ using these Poincaré series.

**Lemma 2.1.** The following are true:

1. We have $g(z) = P(1, 2, 32; z) \left(1 + a(1, 2, 32; 1)\right)$ and $\mathcal{F}(z) = -P(-1, 2, 32; z)$.
2. $Q(-1, 2, 32; z)$ is good for $g$.
3. $D(Q(-1, 2, 32; z)) = \mathcal{F}(z)$.

**Proof.** Since $g$ and $P(1, 2, 32; z)$ are both non-zero cusp forms in the one-dimensional space $S_2(32)$, the first equality follows easily. For the second equality, note that $\mathcal{F}$ and $-P(-1, 2, 32; z)$ have the same principal part at $\infty$ and no constant term, hence their difference must be in $S_2(32)$, hence a multiple of $g$. Further, since $K_{32c}(-1, 1) = 0$ for all $c \geq 1$, we see that the coefficient of $q$ in both $\mathcal{F}$ and $-P(-1, 2, 32; z)$ is zero, and it follows that they must be equal. The proof of the “goodness” of $Q$ follows from the properties of $Q$ listed above and from (13) and (15). Claim (3) now follows from (14).

2.2. **Proof of Theorem 1.1.** Theorem 1.1 is a consequence of the following theorem which was recently proved by Guerzhoy, Kent, and the second author.

**Theorem 2.2 (Theorem 1.2(2) of [2]).** Let $g \in S_k(N)$ be a normalized CM newform. Suppose that $f \in H_{2-k}(N)$ is good for $g$ and set

$$F := D^{k-1}f = \sum_{n \gg -\infty} c(n)q^n.$$

If $p$ is an inert prime in the CM field of $g$ such that $p^{k-1} \nmid c(p)$, and if

$$\lim_{w \to \infty} p^{-w(k-1)} F|_{U(p^{2w+1})} \neq 0,$$

(16)
then as a $p$-adic limit we have
\[
g = \lim_{w \to \infty} \frac{F | U(p^{2w+1})}{c(p^{2w+1})}.
\]

We require a lemma regarding the existence of certain modular functions with integral coefficients that are holomorphic away from the cusp $\infty$.

**Lemma 2.3.** Let $\mathbb{Z}((q))$ denote the ring of Laurent series in $q$ over $\mathbb{Z}$.

1. For each positive integer $n \not\equiv 1 \pmod{4}$ there exists a modular function
   \[
   \phi_n = q^{-n} + O(q) \in M_0^!(32) \cap \mathbb{Z}((q))
   \]
   such that $\phi_n$ is holomorphic at all cusps except $\infty$.
2. For each $n \geq 5$ with $n \equiv 1 \pmod{4}$ there exists a modular function
   \[
   \phi_n = q^{-n} + a_{n-1}^{-1} + O(q) \in M_0^!(32) \cap \mathbb{Z}((q))
   \]
   such that $\phi_n$ is holomorphic at all cusps except $\infty$.
3. In both cases, the coefficients of $\phi_n(z)$ vanish for all indices not congruent to $-n \pmod{4}$.

**Proof.** This follows by induction. Specifically, let $L(z)$ be as in (6) and set
\[
\phi_2(z) := L(2z) = q^{-2} + 2q^6 - q^{14} + \cdots,
\]
\[
\phi_3(z) := L(z)L(2z) = q^{-3} + 2q + q^5 + 2q^9 + \cdots.
\]
Both $\phi_2$ and $\phi_3$ are modular functions of level 32 with integer coefficients. It is clear that one can inductively construct polynomials
\[
\Psi_n(x, y) = \sum t_n(i, j)x^iy^j \in \mathbb{Z}[x, y]
\]
such that $\Psi_n(\phi_2(z), \phi_3(z))$ satisfies the conditions on the principal parts in Lemma [2.3]. For example
\[
\phi_7(z) = \phi_3(7)\phi_2(z)^2 - 2\phi_3(7) = q^{-7} + q + 8q^5 + 2q^9 + \cdots.
\]
Furthermore, if $n$ is even (resp. $n \equiv 3 \pmod{4}$, resp. $n \equiv 1 \pmod{4}$) then one sees that $\Psi_n(x, y) = \Psi_n(x, 1)$ (i.e. it is purely a polynomial in $x$) (resp. $\Psi_n(x, y)$ equals $y$ multiplied by a polynomial in $x^2$, resp. $\Psi_n(x, y)$ equals $xy$ multiplied by a polynomial in $x^2$). This remark establishes the last assertion. ■

This sequence of modular functions turns out to be closely related to $\mathfrak{F}$ as follows.

**Corollary 2.4.** If $n \geq 2$ and $\phi_n(z) = \sum_{l=-n}^{\infty} A_n(l)q^l$, then $C(n) = -A_n(1)$.

**Proof.** Since $C(n) = 0$ whenever $n \not\equiv 3 \pmod{4}$, then the corollary follows trivially for such $n$ by Lemma [2.3]. For $n \equiv 3 \pmod{4}$, the
meromorphic differential \( F(z) \phi_n(z)dz \) is holomorphic everywhere except at the cusp \( \infty \). Recall that the sum of residues of a meromorphic differential is zero. Furthermore, the residue at \( \infty \) of the differential \( h(z)dz \) (for any weight 2 form \( h \)) is a multiple of the constant term in its \( q \)-expansion. Since \( \mathfrak{F}(z) = DQ(-1, 2, 32; z) \) we see that \( \mathfrak{F} \) has no constant term at any cusp, and hence \( \mathfrak{F} \phi_n \) vanishes at all cusps except \( \infty \). It follows that the residue at \( \infty \) must be zero, and the result follows since the constant term of the \( q \)-expansion of \( \mathfrak{F}(z) \phi_n(z) \) is \( C(n) + A_n(1) \).

**Proof of Theorem 1.1.** By Theorem 2.2, Lemma 2.1, and the fact that the primes inert in \( \mathbb{Q}(i) \), the CM field for \( g \), are the primes \( p \equiv 3 \pmod{4} \), it suffices to prove (16) under the assumption that \( p \nmid C(p) \).

Recall that the weight \( k \) \( m \)th Hecke operator \( T(m) \) (see [5, 6]) acts on \( M_k^!(N) \) by

\[
(17) \quad f|T(m)(z) = f|U(p)(z) + p^{k-1}f(pz).
\]

It is obvious from the definition that integrality of the coefficients is preserved for forms of positive weight. In particular, for

\[
\mathfrak{F} = -q^{-1} + 2q^3 + q^7 - 2q^{11} + \cdots,
\]

we get

\[
\mathfrak{F}|_2T(p) = -pq^{-p} + C(p)q + O(q^2),
\]

and \( \mathfrak{F}|_2T(p) \) is holomorphic at all cusps except \( \infty \). For \( p \equiv 3 \pmod{4} \) Lemma 2.3 and Corollary 2.4 give

\[
(18) \quad \mathfrak{F}|_2T(p)(z) = \phi_p'(z) = \sum_{n=-p}^{\infty} a_{\phi_p'}(n)q^n = \sum_{n=-p}^{\infty} nA_p(n)q^n.
\]

From (17) we get

\[
\mathfrak{F}|U(p) = \phi_p'(z) - p\mathfrak{F}(pz).
\]

Acting by \( U(p^2) \) gives

\[
\mathfrak{F}|U(p^2) = \phi_p'|U(p^2) - p\mathfrak{F}(z)|U(p),
\]

and it follows by induction that

\[
(19) \quad p^{-w} \mathfrak{F}|U(p^{2w+1}) = \sum_{l=1}^{w} p^{-l} \phi_p'|U(p^{2l}) - \mathfrak{F}|U(p).
\]

If

\[
\lim_{w \to \infty} p^{-w} \mathfrak{F}|U(p^{2w+1}) = 0,
\]

then

\[
\mathfrak{F}|U(p) = \sum_{l=1}^{\infty} p^{-l} \phi_p'|U(p^{2l}).
\]
Gauss’s \( \binom{2}{1} \) and the congruent number elliptic curve

(The convergence here is \( p \)-adic.) Focusing on the coefficient of \( q \) gives

\[
C(p) = \sum_{l=1}^{\infty} p^{-l} a_{\phi'}(p^{2l}) = \sum_{l=1}^{\infty} p^{-l} p^{2l}(A_p(p^{2l})).
\]

Hence

\[
C(p) = p \sum_{l=1}^{\infty} p^{l-1}(A_p(p^{2l})),
\]

which contradicts the hypothesis that \( p \nmid C(p) \). Thus hypothesis (16) is satisfied, thereby proving the theorem. ■

**Acknowledgements.** The authors would like to thank the referee for his useful suggestions.

The second author thanks for the support of the NSF, the Hilldale Foundation and the Manasse family.

**References**


Ahmad El-Guindy
Department of Mathematics
Faculty of Science
Cairo University
Giza, Egypt 12613
E-mail: a.elguindy@gmail.com

Ken Ono
Department of Mathematics
University of Wisconsin-Madison
Madison, WI 53703, U.S.A.
E-mail: ono@math.wisc.edu

Received on 7.8.2009
and in revised form on 31.1.2010 (6111)