

p -ADIC AND COMBINATORIAL PROPERTIES OF MODULAR FORM COEFFICIENTS

PO-RU LOH AND ROBERT C. RHOADES

ABSTRACT. For two particular classes of elliptic curves, we establish congruences relating the coefficients of their corresponding modular forms to combinatorial objects. These congruences resemble a supercongruence for the Apéry numbers conjectured by Beukers and proved by Ahlgren and Ono in [AO00]. We also consider the trace $\text{Tr}_{2k}(\Gamma_0(N), n)$ of the Hecke operator T_n acting on the space of cusp forms $S_{2k}(\Gamma_0(N))$. We show that for $(n, N) = 1$, these traces interpolate p -adically in the weight aspect.

1. INTRODUCTION AND STATEMENT OF RESULTS

In 1987, Beukers proved a congruence relating the combinatorially defined Apéry numbers (used in Apéry's proof of the irrationality of $\zeta(3)$) to the coefficients of a weight 4 cusp form over $\Gamma_0(8)$. More precisely, define $a(n)$ for $n \geq 1$ by

$$(1.1) \quad f(z) := \sum_{n=1}^{\infty} a(n)q^n = q \prod_{n=1}^{\infty} (1 - q^{2n})^4 (1 - q^{4n})^4,$$

where $q := e^{2\pi iz}$. For each $n \geq 1$, define the Apéry number

$$A(n) := \sum_{j=0}^n \binom{n+j}{j}^2 \binom{n}{j}^2.$$

Beukers proved that for every odd prime p ,

$$(1.2) \quad A\left(\frac{p-1}{2}\right) \equiv a(p) \pmod{p},$$

and further conjectured that this congruence continues to hold modulo p^2 [Beu87]. This conjecture was proven in 2000 by Ahlgren and Ono by relating the coefficients $a(p)$ to the number of points on a certain Calabi-Yau threefold (over \mathbb{F}_p), expressing this number in terms of a Gaussian hypergeometric series, and applying p -adic analysis to relate this series to the Apéry number $A(\frac{p-1}{2})$ [AO00].

A natural generalization of Beukers' congruence is to begin with coefficients of other modular forms, such as the form

$$(1.3) \quad \sum_{n=1}^{\infty} c(n)q^n := q \prod_{n=1}^{\infty} (1 - q^{4n})^2 (1 - q^{8n})^2 \in S_2(\Gamma_0(32)),$$

and to try to find combinatorial objects $C(n)$ such that

$$c(p) \equiv C\left(\frac{p-1}{2}\right) \pmod{p^2}$$

for all primes $p \geq 3$.

Date: February 1, 2006.

While the q -series in (1.3) may appear rather unexceptional, the coefficients of the modular form so defined are intimately related to the elliptic curve

$$E : y^2 = x^3 - x.$$

Indeed, for primes $p \geq 3$, if we define

$$N(p) := \#\{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 - x\} + 1,$$

so that $N(p)$ counts the number of points on E over \mathbb{F}_p (including the point at infinity), then one can show that

$$c(p) = p + 1 - N(p).$$

Computing the first few coefficients of the q -series,

$$\sum_{n=1}^{\infty} c(n)q^n = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} - 2q^{37} + \dots,$$

we compare with the numbers $N(p)$ in Table 1 below.

TABLE 1. Comparison of $c(p)$ and $N(p)$ for $p < 40$.

p	3	5	7	11	13	17	19	23	29	31	37
$c(p)$	0	-2	0	0	6	2	0	0	-10	0	-2
$N(p)$	4	8	8	12	8	16	20	24	40	32	40

In fact, the above relation is a special case of the following general phenomenon. Define the Legendre family of elliptic curves

$${}_2E_1(\lambda) : y^2 = x(x-1)(x-\lambda)$$

for integers $\lambda \neq 0, 1$. (The curve E considered above corresponds to $\lambda = -1$.) Letting

$${}_2N_1(p; \lambda) := \#\{(x, y) \in \mathbb{F}_p^2 : y^2 = x(x-1)(x-\lambda)\} + 1$$

denote the number of points on the reduction of ${}_2E_1(\lambda)$ modulo p , we define

$${}_2a_1(p; \lambda) := p + 1 - {}_2N_1(p; \lambda).$$

Using the Hecke multiplicative relations, we may extend this definition to ${}_2a_1(n; \lambda)$ for all $n \geq 1$. Then it is a consequence of a theorem of Diamond and Kramer [DK95] that

$$(1.4) \quad f_\lambda(q) := \sum_{n=1}^{\infty} {}_2a_1(n; \lambda)q^n$$

is a modular form. Their result, in turn, is a special case of the modularity of elliptic curves, proven through the combined work of Breuil, Conrad, Diamond, Taylor, and Wiles ([TW95], [Wil95], [BCDT01], [CDT99]).

Now let ϕ denote the Legendre character modulo p , and let

$$(1.5) \quad H_n := 1 + \frac{1}{2} + \dots + \frac{1}{n}$$

denote the n^{th} harmonic number. We will prove the following Beukers-like congruences.

Theorem 1.1. *If $p \geq 5$ is prime and $\lambda \neq 0, 1$ is an integer, then*

$${}_2a_1(p; \lambda) \equiv \phi(-1)(p+1) \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2} + j}{j} \binom{\frac{p-1}{2}}{j} (-\lambda)^{jp} \left(1 + 2jp \left(H_{\frac{p-1}{2}+j} - H_j\right)\right) \pmod{p^2}.$$

Remark. When considered only modulo p , this congruence takes the simpler form

$$(1.6) \quad {}_2a_1(p; \lambda) \equiv \phi(-1) \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2} + j}{j} \binom{\frac{p-1}{2}}{j} (-\lambda)^j \pmod{p}.$$

Compare (1.6) to the congruence (1.2) of Beukers; both relate modular form coefficients to similar binomial sums. However, our congruence holds for a one-parameter family of modular forms. We note that the method that we will use to prove these congruences can be generalized to find congruences modulo p^n for any n . As is to be expected, the calculations become increasingly difficult and result in more and more complicated formulas.

Thus, for the Legendre family of elliptic curves, we obtain congruences very similar to those of Beukers involving the Apéry numbers. Noticing the similarity, one might be led to believe that the coefficients of all modular forms might satisfy similar congruences with sums of products of binomial coefficients. However, this is not the case, as we see when we consider a second family of modular forms associated to the elliptic curves

$$C(\lambda) : \quad y^2 = x^3 + \lambda,$$

for integers $\lambda \neq 0$. As before, we define $M(p; \lambda)$ to be the number of points on the reduction of $C(\lambda)$ modulo p , and define

$$b(p; \lambda) := p + 1 - M(p; \lambda).$$

In the special case $\lambda = 1$, the corresponding modular form is

$$(1.7) \quad \sum_{n=1}^{\infty} b(n)q^n := q \prod_{n=1}^{\infty} (1 - q^{6n})^4 \in S_2(\Gamma_0(36)).$$

It was difficult to obtain congruences mod p^n for $n \geq 3$ for the modular forms (1.4) associated to the Legendre family of elliptic curves, and for the form (1.1) from Beukers' conjecture. For the family of curves $C(\lambda)$, however, we are able to obtain congruences modulo any power of p with little more effort than it takes to establish a congruence modulo p .

Theorem 1.2. *Let p be a prime.*

- (1) *If $p \not\equiv 1 \pmod{6}$, then $b(p; \lambda) = 0$.*
- (2) *If $p \equiv 1 \pmod{6}$, then*

$$b(p; \lambda) \equiv \binom{5(p-1)/6}{(p-1)/3} \lambda^{(p-1)/6} \pmod{p},$$

and for $n \geq 2$,

$$b(p; \lambda) \equiv \frac{\binom{5(p^n-1)/6}{(p^n-1)/3}}{\binom{5(p^{n-1}-1)/6}{(p^{n-1}-1)/3}} \lambda^{\frac{1}{6}(p^n-p^{n-1})} + p \cdot \frac{\binom{(p^{n-2}-1)/2}{(p^{n-2}-1)/6}}{\binom{(p^{n-1}-1)/2}{(p^{n-1}-1)/6}} \lambda^{\frac{5}{6}(p^{n-1}-p^{n-2})} \pmod{p^n}.$$

Remark. As a consequence of (2), we obtain the result that when $p \nmid \lambda$,

$$b(p; \lambda) \not\equiv 0 \pmod{p} \quad \text{for } p \equiv 1 \pmod{6}.$$

The specific examples of modular forms that we have presented thus far, (1.1), (1.3), and (1.7), belong to the spaces of cusp forms

$$S_4(\Gamma_0(8)), \quad S_2(\Gamma_0(32)), \quad \text{and} \quad S_2(\Gamma_0(36)),$$

respectively. Each of these spaces is in fact 1-dimensional. As a result, each of the given forms f is (trivially) an eigenform of the Hecke algebra over its space. For weight $2k$ cusp forms over $\Gamma_0(N)$, this algebra is generated by the operators $T_{p,2k}$, defined by

$$\left(\sum_{n=1}^{\infty} a(n)q^n \right) \Big|_{T_{p,2k}} := \sum_{n=1}^{\infty} (a(pn) + p^{2k-1}a(n/p))q^n,$$

for $p \nmid N$. (In the above formula, $a(r)$ is understood to be zero when $r \notin \mathbb{Z}$.) Thus, when f is normalized to have leading term q , the eigenvalue of the n^{th} Hecke operator equals the coefficient of q^n in the q -series expansion of f .

Over a 1-dimensional space, these considerations may seem like much ado about nothing. (Or perhaps that would be so over a 0-dimensional space.) For general spaces $S_{2k}(\Gamma_0(N))$ of cusp forms of weight $2k$ and level N , however, the machinery of the Hecke operators becomes a valuable tool. Indeed, for fixed N , the dimension of $S_{2k}(\Gamma_0(N))$ grows approximately linearly as $k \rightarrow \infty$. On the other hand, it is not clear at the outset how to find, in the general case, even a single form in $S_{2k}(\Gamma_0(N))$ with integer coefficients.

In our prior examples, we obtained congruences for modular form coefficients by counting points on elliptic curves (or in the proof of the Beukers supercongruence, by counting points on a variety over a higher-dimensional space). Thus, our forms had integer coefficients by construction. One might ask, then, whether it is possible to find integer-coefficient modular forms without an explicit relation to points on a variety.

The Hecke operators provide one way to produce such forms. One can define the Petersson scalar product on $S_{2k}(\Gamma_0(N))$, under which the Hecke operators form a commutative algebra of hermitian operators. It follows that the space $S_{2k}(\Gamma_0(N))$ has a basis of normalized forms f_1, \dots, f_d , each of which is a simultaneous eigenform of $T_{2k}(n)$ for all n [Lan95, Ch. I].

In the second half of this paper, we consider the trace form

$$F_{\text{Tr}(2k,N)} := f_1 + \dots + f_d.$$

Then, defining $\text{Tr}_{2k}(\Gamma_0(N), n)$ to be the trace of the n^{th} Hecke operator $T_{2k}(n)$ on $S_{2k}(\Gamma_0(N))$, we have

$$F_{\text{Tr}(2k,N)}(z) = \sum_{n=1}^{\infty} \text{Tr}_{2k}(\Gamma_0(N), n)q^n.$$

One can show that each eigenvalue of the Hecke operators $T_{2k}(n)$ is an algebraic integer, and furthermore, the simultaneous eigenforms f_1, \dots, f_d can be partitioned into sets of Galois conjugates. It follows that the trace form $F_{\text{Tr}(2k,N)}$ has integer coefficients, for any choice of k and N .

It will be more convenient, however, for us to consider the similar form

$$(1.8) \quad F_{2k,N} := \sum_{(n,N)=1} \text{Tr}_{2k}(\Gamma_0(N), n)q^n$$

which has nonzero coefficients only at n coprime to the level N . While this form is no longer modular over $S_{2k}(\Gamma_0(N))$, it is obtained from $F_{\text{Tr}(2k,N)}$ via twisting by the trivial character with conductor N ; hence, it is still modular over at least $\Gamma_0(N^3)$ [Kob93, Prop III.17(b)].

Having found a family of modular forms with integer coefficients, we now ask whether it is possible to find congruences among their coefficients. As an example, recall that for $k \geq 2$, the Eisenstein series E_{2k} is a modular form of weight $2k$ over $\mathrm{SL}(2, \mathbb{Z})$, given by

$$E_{2k}(z) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n,$$

where B_{2k} are the Bernoulli numbers and $\sigma_{m-1}(n) := \sum_{d|n} d^{m-1}$ for $m \geq 1$. Recall that an odd prime p is defined to be *regular* if p does not divide the numerator of any of B_2, B_4, \dots, B_{p-3} . For regular primes p , it follows from the Kummer congruences [IR90, §15.2] that E_{2k} is p -integral for all k , and if

$$2k \equiv 2k' \pmod{(p-1)p^r},$$

then

$$(1.9) \quad E_{2k} \equiv E_{2k'} \pmod{p^{r+1}}.$$

In other words, the E_{2k} are a natural family of modular forms that can be p -adically interpolated in the weight aspect.

Motivated by the above congruences, we find the following theorem.

Theorem 1.3. *Let $p \geq 5$ be a prime, and let r be a nonnegative integer. If $k, k' > r$ and*

$$(1.10) \quad 2k \equiv 2k' \pmod{(p^2-1)p^r},$$

then

$$(1.11) \quad F_{2k,N} \equiv F_{2k',N} \pmod{p^r}.$$

Furthermore, if $(n, N) = 1$ and n is not a quadratic residue mod p , then

$$(1.12) \quad \mathrm{Tr}_{2k}(\Gamma_0(N), n) \equiv \mathrm{Tr}_{2k'}(\Gamma_0(N), n) \pmod{p^{r+1}}.$$

The two key ingredients in the proof of the p -adic interpolation of E_{2k} are the Kummer congruences and Euler's theorem. In our proof of Theorem 1.3, the Eichler-Selberg trace formula takes the place of the Kummer congruences, and we extend Euler-type arguments to p -adically consider powers of algebraic integers.

Remark. For $N = 1$, Theorem 1.3 shows that the trace forms on $\mathrm{SL}(2, \mathbb{Z})$ interpolate p -adically (no twisting is necessary in this case, because $(n, 1) = 1$ for all n). We also know that the Eisenstein series of weight $(p^2 - 1)p^r$ satisfies

$$E_{(p^2-1)p^r} \equiv 1 \pmod{p^r}$$

by (1.9), with $2k = (p^2 - 1)p^r$ and $2k' = 0$. It follows that the map

$$\psi : S_{2k} \rightarrow S_{2k+(p^2-1)p^r}, \quad f \mapsto E_{(p^2-1)p^r} f$$

is an injection that preserves coefficients mod p^r . While ψ does not take eigenforms of S_{2k} to eigenforms of $S_{2k+(p^2-1)p^r}$ —the images are only “eigenforms mod p^r ”—it is nonetheless true that the eigenvalues of each Hecke operator T_n in weight $2k$ are reproduced in weight $2k + (p^2 - 1)p^r$. In this context, our theorem tells us that the complementary eigenvalues not obtained in this manner “cancel out” mod p^r when summed to obtain the trace.

Remark. At first glance, Theorem 1.3 may seem rather divorced from our previous theorems that proved congruences involving “combinatorial numbers.” But in fact, it is possible to reformulate Theorem 1.3 in such a way, using expressions for the trace formula proven in [FOP04]. For example, [FOP04, Thm 1.1] shows

$$(1.13) \quad \mathrm{Tr}_{2k}(\Gamma_0(7), 2) = -2 - \sum_{r=0}^{k-1} \binom{k+r-1}{2r} (-2)^{k-r-1}.$$

In general, these expressions will be more complicated, however, and will involve ${}_2F_1$ classical hypergeometric functions, defined by

$$(1.14) \quad {}_2F_1 \left(\begin{matrix} a & b \\ & c \end{matrix} \middle| x \right) := \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \cdot \frac{x^n}{n!},$$

where

$$(s)_n := s(s+1) \cdots (s+n-1).$$

Note that in the specific cases that we consider, these series are actually finite, and hence are polynomials.

For brevity, we content ourselves with the special case (1.13), which provides a nice illustration of our result. Taking $p = 5$, Table 2 gives $\mathrm{Tr}_{2k}(\Gamma_0(7), 2) \pmod{25}$ for $2k = 24t + 6$, $t = 1, \dots, 15$. Observe that because 2 is not a quadratic residue mod 5, congruence of $2k$ and $2k' \pmod{p^2 - 1 = 24}$ is enough to obtain agreement of traces mod 5, as claimed in the second statement of Theorem 1.3; congruence mod 120 gives agreement mod 25. It is worth pointing out that *a priori*, it is not at all clear that the binomial sum on the right side of (1.13) should satisfy such congruences!

TABLE 2. Traces of T_2 on $S_{2k}(\Gamma_0(7))$.

$2k$	30	54	78	102	126	150	174	198	222	246	270	294
Tr_{2k}	14	4	19	9	24	14	4	19	9	24	14	4

Finally, note that this example also illustrates that our result is tight—that is, in general, the congruence condition (1.10) cannot be weakened if (1.12) is to hold, and likewise with (1.11).

We pause now to give a brief outline of the remainder of the paper. In section 2, we introduce the p -adic Gamma function, Gauss and Jacobi sums, and Gaussian hypergeometric series, ending the section by evaluating one such series mod p^2 . Section 3 contains the proofs of Theorems 1.1 and 1.2. In section 4 we state the Eichler-Selberg trace formula and perform a few calculations, which we use in Section 5 to prove Theorem 1.3.

2. PRELIMINARIES

In this section we develop the background material that will be needed to prove Theorems 1.1 and 1.2. Our plan of attack is analogous to that of [AO00]. First, we relate the number of points on each elliptic curve under consideration to a character sum. Second, we express the character sums in terms of the p -adic Gamma function, via the Gross-Koblitz formula. Finally, we use the methods of p -adic analysis to evaluate these expressions modulo powers of p , producing combinatorial objects similar to the Apéry numbers.

It turns out that the expressions involving character sums that we obtain in the case of the Legendre family of elliptic curves belong to the broader class of Gaussian hypergeometric series (not to be confused with the classical ${}_2F_1$ functions defined earlier in (1.14)). We therefore end this

section by introducing that formalism and evaluating one such series modulo p^2 ; we will use this evaluation in the section 3.

2.1. The p -adic gamma function. For an introduction to p -adic analysis, the reader can consult [Kob84]. Here we will outline the properties of the p -adic gamma function, Γ_p , which will be useful in the proofs of Theorems 1.1 and 1.2. Let $\mathbb{Z}_p, \mathbb{Q}_p$ and \mathbb{C}_p be as usual. Then Γ_p is defined on \mathbb{Z}_p by

$$\Gamma_p(n) := (-1)^n \prod_{j < n, p \nmid j} j, \quad \text{for } n \in \mathbb{N},$$

and

$$\Gamma_p(x) := \lim_{n \rightarrow x} \Gamma_p(n), \quad \text{for } x \in \mathbb{Z}_p.$$

In the limit above we may choose any sequence of integers n that approaches x p -adically. We note in particular that

$$(2.1) \quad \Gamma_p(n+1) = (-1)^{n+1} n!, \quad \text{for } 0 \leq n \leq p-1.$$

We have the following properties of Γ_p for all $x \in \mathbb{Z}_p$:

$$\begin{aligned} \Gamma_p(0) &= 1; \\ \frac{\Gamma_p(-x+1)}{\Gamma_p(-x)} &= \begin{cases} x & \text{if } x \in \mathbb{Z}_p^\times \\ -1 & \text{if } x \in p\mathbb{Z}_p; \end{cases} \\ \Gamma_p(x) &\in \mathbb{Z}_p^\times. \end{aligned}$$

From the above two statements, it is easy to see that for positive integers n ,

$$(2.2) \quad \Gamma_p(-n) = \frac{(-p)^{\lfloor n/p \rfloor} \cdot \lfloor n/p \rfloor!}{n!}.$$

Additionally, Γ_p satisfies the functional equation

$$(2.3) \quad \Gamma_p(x)\Gamma_p(1-x) = (-1)^{x_0}, \quad \text{for } x \in \mathbb{Z}_p,$$

where $x_0 \in \{1, 2, \dots, p\}$ satisfies $x_0 \equiv x \pmod{p}$. In particular, it follows that

$$(2.4) \quad \Gamma_p\left(\frac{1}{2}\right)^2 = (-1)^{(p+1)/2} = -\phi(-1).$$

It is also known that for $x, y \in \mathbb{Z}_p$ and $n \geq 1$,

$$(2.5) \quad x \equiv y \pmod{p^n} \implies \Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^n}.$$

We will find this property to be especially useful.

We turn now to the derivative of the p -adic gamma function. In [AO00] Ahlgren and Ono deduce several properties of Γ_p' and the logarithmic derivative

$$G(x) := \frac{\Gamma_p'(x)}{\Gamma_p(x)}.$$

We summarize the results we will use below.

Proposition 2.1. *Let $p \geq 5$ be a prime. If $x_0 \in \mathbb{Z}_p$ and $z \in p\mathbb{Z}_p$, we have*

$$(2.6) \quad \Gamma_p'(x_0 + z) \equiv \Gamma_p'(x_0) \pmod{p}$$

and

$$(2.7) \quad \Gamma_p(x_0 + z) \equiv \Gamma_p(x_0) + z\Gamma_p'(x_0) \pmod{p^2}.$$

Also,

$$G(x) \in \mathbb{Z}_p, \quad \text{for } x \in \mathbb{Z}_p,$$

and if $x \in \mathbb{Z}_p^\times$,

$$(2.8) \quad G(x+1) - G(x) = \frac{1}{x}.$$

2.2. Gauss and Jacobi Sums. Let p be an odd prime. We extend multiplicative characters χ of \mathbb{F}_p^\times to \mathbb{F}_p by setting $\chi(0) := 0$. Thus, by “a character of \mathbb{F}_p ,” we mean “the extension to \mathbb{F}_p of a character of \mathbb{F}_p^\times .” As before, let ϕ denote the quadratic character. Also, let ϵ denote the trivial character. Of course, these characters depend on the prime p , but since the prime will always be clear from context, we suppress the p -dependence for notational convenience.

Let $\pi \in \mathbb{C}_p$ be a fixed root of

$$(2.9) \quad x^{p-1} + p = 0,$$

and let ζ_p be the unique p -th root of unity in \mathbb{C}_p such that $\zeta_p = 1 + \pi \pmod{\pi^2}$. Then for any character $\chi : \mathbb{F}_p \rightarrow \mathbb{C}_p$, we define the Gauss sum

$$g(\chi) := \sum_{x=0}^{p-1} \chi(x) \zeta_p^x.$$

The Jacobi sum for a pair of characters χ_1, χ_2 is defined by

$$J(\chi_1, \chi_2) := \sum_{x=0}^{p-1} \chi_1(x) \chi_2(1-x).$$

In the following proposition, we list a few well-known properties of Gauss and Jacobi sums that will be of use.

Proposition 2.2. *Let χ, χ_1 , and χ_2 be characters of \mathbb{F}_p , and let ϵ denote the trivial character. Then*

- (1) $g(\chi)g(\bar{\chi}) = \chi(-1)p$.
- (2) *If χ_1 and χ_2 are not both trivial, but $\chi_1\chi_2 = \epsilon$, then $J(\chi_1, \chi_2) = -\chi_1(-1)$.*
- (3) *If $\chi_1\chi_2 \neq \epsilon$, then $J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$.*

Using properties (1) and (2), it is easy to deduce that

$$(2.10) \quad g(\phi)^2 = \phi(-1)p \quad \text{and} \quad J(\phi, \phi)^2 = 1.$$

Recall that \mathbb{Z}_p contains all $(p-1)^{\text{st}}$ roots of unity. Thus, there exists a primitive (multiplicative) character $\omega : \mathbb{F}_p \rightarrow \mathbb{Z}_p$ satisfying $\omega(x) \equiv x \pmod{p}$ for all $x = 0, 1, \dots, p-1$; ω is called the Teichmüller character. It is not hard to show that

$$(2.11) \quad \omega(x) \equiv x^{p^{n-1}} \pmod{p^n}$$

for all $n \geq 1$.

Finally, the vehicle that we will use to convert Gauss sums to expressions in Γ_p is the celebrated Gross-Koblitz formula [GK79].

Theorem 2.3 (Gross-Koblitz).

$$(2.12) \quad g(\bar{\omega}^j) = -\pi^j \Gamma_p \left(\frac{j}{p-1} \right), \quad \text{for } 0 \leq j \leq p-2.$$

2.3. Gaussian hypergeometric series. If A and B are two characters of \mathbb{F}_p , then we define the normalized Jacobi sum $\binom{A}{B}$ by

$$\binom{A}{B} := \frac{B(-1)}{p} J(A, \bar{B}) = \frac{B(-1)}{p} \sum_{x=0}^{p-1} A(x) \bar{B}(1-x).$$

As in Greene [Gre87], for characters A_0, A_1, \dots, A_n and B_1, \dots, B_n we define the Gaussian hypergeometric series over \mathbb{F}_p by

$${}_{n+1}F_n \left(\begin{matrix} A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \mid x \right) := \frac{p}{p-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x),$$

where the sum runs over all characters χ of \mathbb{F}_p .

We will only consider the case in which $A_i = \phi$ for all i and $B_j = \epsilon$ for all j , so we ease notation by writing

$${}_{n+1}F_n(x) := {}_{n+1}F_n \left(\begin{matrix} \phi, & \phi, & \dots, & \phi \\ & \epsilon, & \dots, & \epsilon \end{matrix} \mid x \right).$$

Recall that we defined H_n to be partial sums of the harmonic series (1.5). With this notation, we prove the following congruence for ${}_{n+1}F_n(x)$.

Theorem 2.4. *Let n be odd, $l = (n+1)/2$, and p prime with $p \geq 5$. Then*

$$\begin{aligned} & -\phi(x) p^n {}_{n+1}F_n(x) \\ & \equiv (p+1) \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2} + j}{j}^l \binom{\frac{p-1}{2}}{j}^l (-1)^{jl} x^{-jp} \left(1 + (n+1)jp \left(H_{\frac{p-1}{2}+j} - H_j \right) \right) \pmod{p^2}. \end{aligned}$$

We begin with a useful lemma.

Lemma 2.5. For primes $p \geq 5$, for $0 \leq j \leq \frac{p-1}{2}$ we have

$$\frac{\Gamma_p(\frac{1}{2} + j)^2}{\Gamma_p(1 + j)^2} \equiv \binom{\frac{p-1}{2} + j}{j} \binom{\frac{p-1}{2}}{j} (-1)^{j+1} \phi(-1) \pmod{p^2}.$$

Proof. Following the proof of [AO00, Lemma 7.2], we apply (2.1) to write

$$\binom{\frac{p-1}{2} + j}{j} \binom{\frac{p-1}{2}}{j} = \frac{(\frac{p-1}{2} + j)!}{j! 2^{(\frac{p-1}{2} - j)!}} = \frac{\Gamma_p(\frac{1}{2} + j + \frac{p}{2})}{\Gamma_p(1 + j)^2 \Gamma_p(\frac{1}{2} - j + \frac{p}{2})}.$$

We now apply the functional equation (2.3) to write

$$\frac{\Gamma_p(\frac{1}{2} + j + \frac{p}{2})}{\Gamma_p(1 + j)^2 \Gamma_p(\frac{1}{2} - j + \frac{p}{2})} = \frac{\Gamma_p(\frac{1}{2} + j + \frac{p}{2}) \Gamma_p(\frac{1}{2} + j - \frac{p}{2})}{\Gamma_p(1 + j)^2} (-1)^{\frac{1}{2} + j + \frac{p}{2}}.$$

Applying the Taylor expansion (2.7),

$$\begin{aligned} \Gamma_p(\frac{1}{2} + j + \frac{p}{2}) \Gamma_p(\frac{1}{2} + j - \frac{p}{2}) & \equiv \left(\Gamma_p(\frac{1}{2} + j) + \frac{p}{2} \Gamma'_p(\frac{1}{2} + j) \right) \left(\Gamma_p(\frac{1}{2} + j) - \frac{p}{2} \Gamma'_p(\frac{1}{2} + j) \right) \\ & \equiv \Gamma_p(\frac{1}{2} + j)^2 \pmod{p^2}, \end{aligned}$$

and substituting $\phi(-1) = (-1)^{(p-1)/2}$ gives the desired congruence. \square

Proof of Theorem 2.4. Using the relation

$$\binom{\phi\chi}{\chi} \chi(-1) = \binom{\phi}{\chi}$$

derived from properties of Jacobi sums, we obtain

$$\frac{p-1}{p} {}_{n+1}F_n(x)_p = \sum_{\chi} \binom{\phi\chi}{\chi}^{n+1} \chi(x) = \sum_{\chi} \binom{\phi}{\chi}^{n+1} \chi((-1)^{n+1}x) = \sum_{\chi} \binom{\phi}{\chi}^{n+1} \chi(x),$$

where we use the fact that $n+1$ is even in the final equality. Using the definition of the normalized Jacobi sum and parts (2) and (3) of Proposition 2.2, we have

$$\begin{aligned} {}_{n+1}F_n(x) &= \frac{p}{p-1} \sum_{\chi} \frac{1}{p^{n+1}} J(\phi, \bar{\chi})^{n+1} \chi((-1)^{n+1}x) \\ &= \frac{1}{p^n(p-1)} \sum_{\chi} J(\phi, \chi)^{n+1} \bar{\chi}(x) \\ &= \frac{1}{p^n(p-1)} \left(\phi(x) J(\phi, \phi)^{n+1} + \sum_{\chi \neq \phi} \frac{g(\phi)^{n+1} g(\chi)^{n+1}}{g(\phi\chi)^{n+1}} \bar{\chi}(x) \right) \\ &= \frac{1}{p^n(p-1)} \left(\phi(x) (-\phi(-1))^{n+1} + \sum_{\chi \neq \phi} \frac{g(\phi)^{n+1} g(\chi)^{n+1}}{g(\phi\chi)^{n+1}} \bar{\chi}(x) \right) \\ &= \frac{1}{p^n(p-1)} \left(\phi(x) + \sum_{\chi \neq \phi} \frac{g(\phi)^{n+1} g(\bar{\chi})^{n+1}}{g(\phi\bar{\chi})^{n+1}} \chi(x) \right) \\ &= \frac{1}{p^n(p-1)} \left(\phi(x) + (\phi(-1)p)^{\frac{n+1}{2}} \sum_{\chi \neq \phi} \frac{g(\bar{\chi})^{n+1}}{g(\phi\bar{\chi})^{n+1}} \chi(x) \right), \end{aligned}$$

where we used (2.10) to replace $g(\phi)^2$ in the last equation. The next step in the proof is to represent the characters in terms of the Teichmüller character and then apply the Gross-Koblitz formula (2.12) to introduce the p -adic gamma function. We have:

$$\begin{aligned} &p^n(p-1) \cdot {}_{n+1}F_n(x) \\ &= \phi(x) + (\phi(-1)p)^{\frac{n+1}{2}} \sum_{j=0}^{\frac{p-3}{2}} \frac{g(\bar{\omega}^j)^{n+1}}{g(\bar{\omega}^{j+\frac{p-1}{2}})^{n+1}} \omega^j(x) + (\phi(-1)p)^{\frac{n+1}{2}} \sum_{j=\frac{p+1}{2}}^{p-2} \frac{g(\bar{\omega}^j)^{n+1}}{g(\bar{\omega}^{j-\frac{p-1}{2}})^{n+1}} \omega^j(x) \\ &= \phi(x) + \frac{(\phi(-1)p)^{\frac{n+1}{2}}}{(-\pi^{\frac{p-1}{2}})^{n+1}} \sum_{j=0}^{\frac{p-3}{2}} \frac{\Gamma_p(\frac{j}{p-1})^{n+1}}{\Gamma_p(\frac{j}{p-1} + \frac{1}{2})^{n+1}} \omega^j(x) \\ &\quad + (\phi(-1)p)^{\frac{n+1}{2}} (-\pi^{\frac{p-1}{2}})^{n+1} \sum_{j=\frac{p+1}{2}}^{p-2} \frac{\Gamma_p(\frac{j}{p-1})^{n+1}}{\Gamma_p(\frac{j}{p-1} - \frac{1}{2})^{n+1}} \omega^j(x) \\ &= \phi(x) + (-\phi(-1))^{\frac{n+1}{2}} \left(\sum_{j=0}^{\frac{p-3}{2}} \frac{\Gamma_p(\frac{j}{p-1})^{n+1}}{\Gamma_p(\frac{j}{p-1} + \frac{1}{2})^{n+1}} \omega^j(x) + p^{n+1} \sum_{j=\frac{p+1}{2}}^{p-2} \frac{\Gamma_p(\frac{j}{p-1})^{n+1}}{\Gamma_p(\frac{j}{p-1} - \frac{1}{2})^{n+1}} \omega^j(x) \right), \end{aligned}$$

where the last statement was obtained by substituting $\pi^{p-1} = -p$ from (2.9). Notice that we broke the sum into two pieces. In the first sum we wrote $\phi = \bar{\omega}^{(p-1)/2}$, while in the second sum we used $\phi = \bar{\omega}^{-(p-1)/2}$. This was necessary because the Gross-Koblitz formula (2.12) only holds for $0 \leq j \leq p-2$.

Now recalling that $\Gamma_p(x) \in \mathbb{Z}_p^\times$ for all $x \in \mathbb{Z}_p$, we see that the second term vanishes modulo p^2 , leaving

$$\begin{aligned} p^n(p-1) \cdot {}_{n+1}F_n(x) &\equiv \phi(x) + (-\phi(-1))^{\frac{n+1}{2}} \sum_{j=0}^{\frac{p-3}{2}} \frac{\Gamma_p(\frac{j}{p-1})^{n+1}}{\Gamma_p(\frac{j}{p-1} + \frac{1}{2})^{n+1}} \omega^j(x) \pmod{p^2} \\ &\equiv \phi(x) + (-\phi(-1))^{\frac{n+1}{2}} \sum_{j=1}^{\frac{p-1}{2}} \frac{\Gamma_p(\frac{1}{2} - \frac{j}{p-1})^{n+1}}{\Gamma_p(1 - \frac{j}{p-1})^{n+1}} \omega^{\frac{p-1}{2}-j}(x), \end{aligned}$$

replacing j by $(p-1)/2 - j$. By (2.5), $\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^2}$ if $x \equiv y \pmod{p^2}$; thus, since $\frac{-1}{p-1} \equiv p+1 \pmod{p^2}$,

$$p^n(p-1) \cdot {}_{n+1}F_n(x) \equiv \phi(x) + (-\phi(-1))^{\frac{n+1}{2}} \phi(x) \sum_{j=1}^{\frac{p-1}{2}} \frac{\Gamma_p(\frac{1}{2} + j + jp)^{n+1}}{\Gamma_p(1 + j + jp)^{n+1}} \omega^{-j}(x) \pmod{p^2}.$$

Observe that from (2.4), $\Gamma_p(\frac{1}{2})^2 = -\phi(-1)$, and clearly $\Gamma_p(1)^2 = 1$. It follows that the ‘‘extra’’ term $\phi(x)$ corresponds to the summand $j = 0$ and can be assimilated into the sum:

$$(2.13) \quad p^n(p-1) \cdot {}_{n+1}F_n(x) \equiv \phi(x) (-\phi(-1))^{\frac{n+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} \frac{\Gamma_p(\frac{1}{2} + j + jp)^{n+1}}{\Gamma_p(1 + j + jp)^{n+1}} \omega^{-j}(x) \pmod{p^2}.$$

We now apply p -adic analysis to the Γ_p -quotient in the summand, using (2.7) from Proposition 2.1:

$$\begin{aligned} \frac{\Gamma_p(\frac{1}{2} + j + jp)^{n+1}}{\Gamma_p(1 + j + jp)^{n+1}} &\equiv \frac{(\Gamma_p(\frac{1}{2} + j) + jp\Gamma'_p(\frac{1}{2} + j))^{n+1}}{(\Gamma_p(1 + j) + jp\Gamma'_p(1 + j))^{n+1}} \pmod{p^2} \\ &\equiv \frac{\Gamma_p(\frac{1}{2} + j)^{n+1} (1 + (n+1)jpG(\frac{1}{2} + j))}{\Gamma_p(1 + j)^{n+1} (1 + (n+1)jpG(1 + j))} \\ &\equiv \frac{\Gamma_p(\frac{1}{2} + j)^{n+1}}{\Gamma_p(1 + j)^{n+1}} (1 + (n+1)jp\{G(\frac{1}{2} + j) - G(1 + j)\}), \end{aligned}$$

where $G(x)$ is the logarithmic derivative of $\Gamma_p(x)$. Using the equation (2.8) along with the congruence (2.6), it is not hard to show that

$$G(\frac{1}{2} + j) - G(1 + j) \equiv H_{\frac{p-1}{2}+j} - H_j \pmod{p},$$

which is [AO00, Eq. 7.3]. Hence,

$$\begin{aligned} \frac{\Gamma_p(\frac{1}{2} + j + jp)^{n+1}}{\Gamma_p(1 + j + jp)^{n+1}} &\equiv \frac{\Gamma_p(\frac{1}{2} + j)^{n+1}}{\Gamma_p(1 + j)^{n+1}} \left(1 + (n+1)jp \left(H_{\frac{p-1}{2}+j} - H_j\right)\right) \pmod{p^2} \\ &\equiv \left[\binom{\frac{p-1}{2} + j}{j} \binom{\frac{p-1}{2}}{j} (-1)^{j+1} \phi(-1) \right]^{\frac{n+1}{2}} \left(1 + (n+1)jp \left(H_{\frac{p-1}{2}+j} - H_j\right)\right) \end{aligned}$$

from Lemma 2.5. Applying this in (2.13), we have, after some cancellation,

$$\begin{aligned} p^n(p-1) \cdot {}_{n+1}F_n(x) &\equiv \phi(x) \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2} + j}{j}^l \binom{\frac{p-1}{2}}{j}^l (-1)^{jl} \left(1 + (n+1)jp \left(H_{\frac{p-1}{2}+j} - H_j\right)\right) \omega^{-j}(x) \pmod{p^2}, \end{aligned}$$

where we have written $l = (n + 1)/2$.

Finally, applying (2.11) to obtain

$$\omega^{-j}(x) \equiv x^{-j} \pmod{p} \quad \text{and} \quad \omega^{-j}(x) \equiv x^{-jp} \pmod{p^2},$$

and multiplying through by $\phi(x)(p + 1)$, we obtain the claimed congruence. \square

3. PROOFS OF THEOREMS 1.1 AND 1.2

Proof of Theorem 1.1. We have

$$\begin{aligned} {}_2a_1(p; \lambda) &= p + 1 - {}_2N_1(p; \lambda) \\ &= p - \sum_{x \in \mathbb{F}_p} (1 + \phi(x(x-1)(x-\lambda))) \\ &= -\phi(\lambda) \sum_x \phi(x)\phi(1-x)\phi(1-\lambda^{-1}x). \end{aligned}$$

By [Gre87, §3], this sum can be converted into a hypergeometric sum:

$$\begin{aligned} {}_2a_1(p; \lambda) &= -\phi(-\lambda)p \cdot {}_2F_1(\lambda^{-1}) \\ &\equiv \phi(-1)(p+1) \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}+j}{j} \binom{\frac{p-1}{2}}{j} (-\lambda)^{jp} \left(1 + 2jp \left(H_{\frac{p-1}{2}+j} - H_j\right)\right) \pmod{p^2}, \end{aligned}$$

where the second equivalence follows from Theorem 2.4. \square

Turning to the proof of Theorem 1.2, we first give a simple lemma.

Lemma 3.1. Let a and b be positive integers such that

$$\lfloor a/p \rfloor + \lfloor b/p \rfloor = \lfloor (a+b)/p \rfloor.$$

Then

$$\frac{\Gamma_p(-a)\Gamma_p(-b)}{\Gamma_p(-a-b)} = \frac{\binom{a+b}{a}}{\binom{\lfloor (a+b)/p \rfloor}{\lfloor a/p \rfloor}}.$$

Proof. The lemma follows immediately by substituting (2.2) in each Γ_p term and cancelling powers of $-p$. \square

Proof of Theorem 1.2. We first deal with the case $p \not\equiv 1 \pmod{6}$. In this case, it suffices to observe that the map $x \mapsto x^3$ is a bijection on \mathbb{F}_p . Hence, as x runs through a complete system of residues modulo p , $x^3 + \lambda$ does the same. Because there are an equal number of quadratic residues and nonresidues modulo p , it follows that $M(p; \lambda) = p + 1$ and $b(p; \lambda) = 0$.

Now assume $p \equiv 1 \pmod{6}$. As before, let ω denote the Teichmüller character. Let $\chi_3 = \omega^{(p-1)/3}$ denote one of the characters of order 3; note that such a character exists because of the condition

on p . Then we may express $M(p; \lambda)$ as follows:

$$\begin{aligned}
 M(p; \lambda) - 1 &= \#\{y^2 \equiv x^3 + \lambda\} \\
 &= \sum_{r \in \mathbb{F}_p} \#\{y^2 \equiv r\} \cdot \#\{x^3 \equiv r - \lambda\} \\
 &= \sum_r (\phi(r) + 1)(\chi_3(r - \lambda) + \bar{\chi}_3(r - \lambda) + 1) \\
 &= \sum_r (\phi(r) + 1)(\chi_3(\lambda - r) + \bar{\chi}_3(\lambda - r) + 1) \\
 &= p + \phi(\lambda)\chi_3(\lambda) \sum_r \phi(r\lambda^{-1})\chi_3(1 - r\lambda^{-1}) + \phi(\lambda)\bar{\chi}_3(\lambda) \sum_r \phi(r\lambda^{-1})\bar{\chi}_3(1 - r\lambda^{-1}) \\
 &= p + \phi\chi_3(\lambda)J(\phi, \chi_3) + \phi\bar{\chi}_3(\lambda)J(\phi, \bar{\chi}_3).
 \end{aligned}$$

Therefore,

$$\begin{aligned}
 b(p; \lambda) &= p + 1 - M(p; \lambda) \\
 &= -\phi\bar{\chi}_3(\lambda)J(\phi, \bar{\chi}_3) - \phi\chi_3(\lambda)J(\phi, \chi_3) \\
 &= -\phi\bar{\chi}_3(\lambda) \frac{g(\phi)g(\bar{\chi}_3)}{g(\phi\bar{\chi}_3)} - \phi\chi_3(\lambda) \frac{g(\phi)g(\chi_3)}{g(\phi\chi_3)} \\
 &= -\phi\bar{\chi}_3(\lambda) \frac{g(\bar{\omega}^{(p-1)/2})g(\bar{\omega}^{(p-1)/3})}{g(\bar{\omega}^{5(p-1)/6})} - \phi\chi_3(\lambda) \frac{g(\bar{\omega}^{(p-1)/2})g(\bar{\omega}^{2(p-1)/3})}{g(\bar{\omega}^{(p-1)/6})} \\
 &= \phi\bar{\chi}_3(\lambda) \frac{\Gamma_p(\frac{1}{2})\Gamma_p(\frac{1}{3})}{\Gamma_p(\frac{5}{6})} - \phi\chi_3(\lambda)p \cdot \frac{\Gamma_p(\frac{1}{2})\Gamma_p(\frac{2}{3})}{\Gamma_p(\frac{1}{6})}
 \end{aligned}$$

by the Gross-Koblitz formula (2.12). Using the functional equation (2.3) on the factor $\Gamma_p(\frac{2}{3})$ in the second term, we obtain

$$b(p; \lambda) = \phi\bar{\chi}_3(\lambda) \frac{\Gamma_p(\frac{1}{2})\Gamma_p(\frac{1}{3})}{\Gamma_p(\frac{5}{6})} + \phi\chi_3(\lambda)p \cdot \frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{1}{3})\Gamma_p(\frac{1}{6})}.$$

Expressing all characters in terms of the Teichmüller character,

$$\phi\bar{\chi}_3 = \omega^{(p-1)/6} \quad \text{and} \quad \phi\chi_3 = \omega^{5(p-1)/6}.$$

We may now use (2.11) to obtain the congruence

$$(3.1) \quad b(p; \lambda) \equiv \frac{\Gamma_p(\frac{1}{2})\Gamma_p(\frac{1}{3})}{\Gamma_p(\frac{5}{6})} \lambda^{\frac{1}{6}(p^n - p^{n-1})} + p \cdot \frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{1}{3})\Gamma_p(\frac{1}{6})} \lambda^{\frac{5}{6}(p^{n-1} - p^{n-2})} \pmod{p^n}.$$

Observe that

$$\Gamma_p\left(\frac{1}{2}\right) \equiv \Gamma_p\left(\frac{1 - p^n}{2}\right) \pmod{p^n}$$

and likewise for the other $\Gamma_p(x)$ in (3.1). It is then easy to verify that Lemma 3.1 applies with $a = (p^n - 1)/2$, $b = (p^n - 1)/3$ in the first term, and $a = (p^{n-1} - 1)/3$, $b = (p^{n-1} - 1)/6$ in the second term, completing the proof of the theorem. \square

4. THE EICHLER-SELBERG TRACE FORMULA

We give the version of the Eichler-Selberg trace formula for $\mathrm{Tr}_{2k}(\Gamma_0(N), n)$ due to Hijikata [HPS89, Thm 2.2] and reformulated in [FOP04] and [Rou]. Fix k, N , and n . Let

$$\begin{aligned} E &:= \{s \in \mathbb{Z} \mid s^2 - 4n < 0\}, \\ H &:= \{s \in \mathbb{Z} \mid \exists t \in \mathbb{Z}^+, s^2 - 4n = t^2\}. \end{aligned}$$

For $s \in E \cup H$, let t_0 be the largest positive integer such that $t_0^2 \mid (s^2 - 4n)$. Define $t = t(s)$ according to

$$t := \begin{cases} t_0 & \text{if } (s^2 - 4n)/t_0^2 \equiv 1 \pmod{4}, \\ t_0/2 & \text{if } (s^2 - 4n)/t_0^2 \equiv 2, 3 \pmod{4}. \end{cases}$$

Next, for $s \in E \cup H$, let y and \bar{y} be the roots of the quadratic $x^2 - sx + n = 0$, and set

$$(4.1) \quad a(s, k, n) := \begin{cases} \frac{1}{2} \cdot \frac{y^{2k-1} - \bar{y}^{2k-1}}{y - \bar{y}} & \text{if } s \in E, \\ \frac{\min\{|y|, |\bar{y}|\}^{2k-1}}{|y - \bar{y}|} & \text{if } s \in H. \end{cases}$$

Assume now that N and n are coprime. If n is a perfect square, let

$$(4.2) \quad \tilde{\sigma}(k, N, n) := n^{k-1} \frac{2k-1}{12} N \prod_{\ell \mid N} (1 + 1/\ell) - n^{k-1} \frac{\sqrt{n}}{2} \prod_{\ell \mid N} \mathrm{par}(\ell, N),$$

where the products are taken over primes ℓ dividing N , and $\mathrm{par}(\ell, N)$ are integers given explicitly in [HPS89, §2]. If n is not a perfect square, let $\tilde{\sigma}(k, N, n) := 0$.

Theorem 4.1. *If N and n are positive coprime integers, and $k > 1$, then*

$$\mathrm{Tr}_{2k}(\Gamma_0(N), n) = \tilde{\sigma}(k, N, n) - \sum_{s \in E \cup H} a(s, k, n) \sum_{f \mid t(s)} b(s, f, n) \prod_{\ell \mid N} c(s, f, N, n, \ell)$$

where $b(s, f, n)$ are rational numbers and $c(s, f, N, n, \ell)$ are integers independent of k . The product is taken over primes ℓ dividing N , as usual.

The numbers $b(s, f, n)$ and $c(s, f, N, n, \ell)$ are given explicitly in [HPS89, §2]. In the following lemma, we record the properties of these numbers that we will need.

Lemma 4.2.

- (1) If $s \in E$, then $b(s, f, n)$ has denominator at most 3.
- (2) If $s \in H$, then $t(s) = \sqrt{s^2 - 4n}$ and

$$(4.3) \quad b(s, f, n) = \frac{1}{2} \varphi(t/f),$$

where φ denotes the Euler φ -function.

- (3) Suppose $s \in H$ and $\ell \mid N$ is a fixed odd prime. Let $\nu := \mathrm{ord}_\ell(N)$, $a := \mathrm{ord}_\ell(t)$, and $d := \mathrm{ord}_\ell(t/f)$.

- (a) If ν is odd, $\nu = 2\rho + 1$, then

$$c(s, f, N, n, \ell) = \begin{cases} 2 & \text{if } d = 0, \\ 2\ell^d + 2\ell^{d-1} & \text{if } 1 \leq d \leq \rho, \\ 2\ell^\rho & \text{if } d \geq \rho + 1. \end{cases}$$

(b) If ν is even, $\nu = 2\rho$, then

$$c(s, f, N, n, \ell) = \begin{cases} 2 & \text{if } d = 0, \\ 2\ell^d + 2\ell^{d-1} & \text{if } 1 \leq d \leq \rho - 1, \\ \ell^\rho + 2\ell^{\rho-1} & \text{if } d = \rho, \\ \ell^\rho + \ell^{\rho-1} & \text{if } d \geq \rho + 1. \end{cases}$$

Proof. [HPS89] proves part (2) of our lemma and shows that the denominator of $b(s, f, n)$ is either 2 or half the order of the unit group of an imaginary quadratic field. The only possible orders are 2, 4, and 6, which proves (1). Part (3) of our lemma follows from Case A of [HPS89, Lemma 2.5]. \square

Although the trace formula is complicated, we must keep in mind that we seek only to prove a p -adic statement about $\text{Tr}_{2k}(\Gamma_0(N), n)$ as k varies, with N and n remaining fixed. In particular, Lemma 4.2 implies the following corollary.

Corollary 4.3. For $p \geq 5$, the term

$$(4.4) \quad D(s, N, n) := \sum_{f|t(s)} b(s, f, n) \prod_{\ell|N} c(s, f, N, n, \ell)$$

is a p -adic integer, independent of k .

We will therefore be able to ignore this factor, provided that we can show that $a(s, k, n)$ can be p -adically interpolated in the way we want. It turns out that we will be able to do so in the case $s \in E$. For $s \in H$, however, the denominator $|y - \bar{y}|$ of $a(s, k, n)$ poses a problem, and we must be more careful.

For the remainder of this section, assume k, N, n , and $s \in H$ are all fixed, with $t = \sqrt{s^2 - 4n}$. Then (4.4) takes the form

$$D(s) = \sum_{f|t} b(f) \prod_{\ell|N} c(f, \ell),$$

which, upon using (4.3) to rewrite $b(f)$, gives

$$2D(s) = \sum_{f|t} \varphi(t/f) \prod_{\ell|N} c(f, \ell).$$

Now, observe that in Lemma 4.2, the values of $c(f, \ell)$ depend only on $\text{ord}_\ell(f)$. Hence, by the multiplicativity of φ , we have the decomposition

$$(4.5) \quad 2D(s) = \prod_{\ell|tN} D'(a(\ell), \ell),$$

where

$$(4.6) \quad D'(a, \ell) := \begin{cases} \sum_{d=0}^a \varphi(\ell^d) c(\ell^{a-d}, \ell) & \text{if } \ell | N, \\ \sum_{d=0}^a \varphi(\ell^d) & \text{if } \ell \nmid N, \end{cases}$$

with $a := \text{ord}_\ell(t)$ as in the statement of the lemma.

We make use of this result to prove the following lemma.

Lemma 4.4. Let $s \in H$. Then for odd primes ℓ ,

$$\frac{D(s, N, n)}{|y - \bar{y}|} \in \mathbb{Z}_\ell.$$

Proof. By definition, $|y - \bar{y}|$ is the difference of the roots of the quadratic $x^2 - sx + n = 0$, so we have

$$|y - \bar{y}| = \sqrt{s^2 - 4n} = t.$$

Thus, we are to prove $\text{ord}_\ell(D(s, N, n)) \geq \text{ord}_\ell(t)$.

In the case $\ell \nmid t$, this is trivial. Assume then that $a := \text{ord}_\ell(t) \geq 1$. By the decomposition (4.5), it suffices to show that $\text{ord}_\ell(D'(a, \ell)) \geq a$. If $\ell \nmid N$, we are in the second case of (4.6), and we easily obtain

$$D'(a, \ell) = \sum_{d=0}^a \varphi(\ell^d) = \ell^a,$$

precisely as wanted. Otherwise,

$$D'(a, \ell) = \sum_{d=0}^a \varphi(\ell^d) c(\ell^{a-d}, \ell),$$

and we must use the formulas for $c(f, \ell)$ given in Lemma 4.2, considering a few cases.

(1) ν is odd, $\nu = 2\rho + 1$.

(a) $1 \leq a \leq \rho$. Then

$$D'(a, \ell) = \varphi(1) \cdot 2 + \sum_{d=1}^a \varphi(\ell^d) (2\ell^d + 2\ell^{d-1}) = 2 + \sum_{d=1}^a 2(\ell^{2d} - \ell^{2d-2}) = 2\ell^{2a},$$

giving $\text{ord}_\ell(D'(a, \ell)) = 2a \geq a$.

(b) $\rho + 1 \leq a$. Then

$$\begin{aligned} D'(a, \ell) &= D'(\rho, \ell) + \sum_{d=\rho+1}^a \varphi(\ell^d) \cdot 2\ell^\rho \\ &= 2\ell^{2\rho} + \sum_{d=\rho+1}^a 2(\ell^{d+\rho} - \ell^{d+\rho-1}) = 2\ell^{a+\rho}, \end{aligned}$$

giving $\text{ord}_\ell(D'(a, \ell)) = a + \rho \geq a$.

(2) ν is even, $\nu = 2\rho$.

(a) $1 \leq a \leq \rho - 1$. Then the situation is the same as case (i) above.

(b) $a = \rho$. Then

$$\begin{aligned} D'(a, \ell) &= D'(\rho - 1, \ell) + \varphi(\ell^\rho) (\ell^\rho + 2\ell^{\rho-1}) \\ &= 2\ell^{2\rho-2} + \ell^{2\rho} + \ell^{2\rho-1} - 2\ell^{2\rho-2} = \ell^{2\rho} + \ell^{2\rho-1}, \end{aligned}$$

giving $\text{ord}_\ell(D'(a, \ell)) = 2\rho - 1 \geq \rho = a$.

(c) $\rho + 1 \leq a$. Then

$$\begin{aligned} D'(a, \ell) &= D'(\rho, \ell) + \sum_{d=\rho+1}^a \varphi(\ell^d) (\ell^\rho + \ell^{\rho-1}) \\ &= \ell^{2\rho} + \ell^{2\rho-1} + \sum_{d=\rho+1}^a (\ell^{d+\rho} - \ell^{d+\rho-2}) = \ell^{a+\rho} + \ell^{a+\rho-1}, \end{aligned}$$

giving $\text{ord}_\ell(D'(a, \ell)) = a + \rho - 1 \geq a$.

□

5. PROOF OF THEOREM 1.3

In order to proceed systematically, it is useful to begin by introducing some terminology.

Definition 5.1. Let p be an odd prime and $f : \mathbb{N} \rightarrow \overline{\mathbb{Q}}_p$. We say that f *interpolates* (p -adically) if for all positive integers r , and $k, k' > r$,

$$(5.1) \quad k \equiv k' \pmod{\frac{1}{2}(p^2 - 1)p^r} \implies \text{ord}_p(f(k) - f(k')) \geq r.$$

Under this definition, it is easy to see that the following two propositions hold.

Proposition 5.2. *The set of functions f that interpolate p -adically form a ring \mathcal{R}_p (under the usual pointwise addition and multiplication).*

Proposition 5.3. *The polynomial ring $\mathbb{Z}_p[k]$ is a subring of \mathcal{R}_p .*

With a little more work, we next show that certain exponential functions also interpolate.

Lemma 5.4. For $b \in \mathbb{Z}_p$, the function

$$f(k) := b^{k-1}$$

belongs to \mathcal{R}_p .

Proof. Fix $r \geq 1$. Suppose first that $\text{ord}_p(b) \geq 1$. Then for all $k > r$, we have $\text{ord}_p(f(k)) \geq r$, and the claim holds trivially.

Otherwise, $\text{ord}_p(b) = 0$. Abusing notation slightly by writing b also for the projection of b in $\mathbb{Z}_p/p^r\mathbb{Z}_p$, we have

$$b \in (\mathbb{Z}_p/p^r\mathbb{Z}_p)^\times \cong (\mathbb{Z}/p^r\mathbb{Z})^\times,$$

which has order $\varphi(p^r)$; hence,

$$b^{\varphi(p^r)} \equiv 1 \pmod{p^r}.$$

Since $\varphi(p^r) = (p-1)p^{r-1}$ divides the desired period $\frac{1}{2}(p^2 - 1)p^r$, the result follows. \square

Lemma 5.5. For α a root of a monic quadratic with coefficients in \mathbb{Z}_p , the function

$$f(k) := \alpha^{2k-1}$$

belongs to \mathcal{R}_p .

Proof. Fix $r \geq 1$. If $\alpha \in \mathbb{Z}_p$, then $f(k) = \alpha^{k-1} \cdot \alpha^{k-1} \cdot \alpha \in \mathcal{R}_p$ by applying Lemma 5.4. Otherwise, $L := \mathbb{Q}_p[\alpha]$ is a quadratic extension of \mathbb{Q}_p . Arguing along the same lines as in the proof of the previous lemma, we first consider the case $\text{ord}_p(\alpha) \geq \frac{1}{2}$. Again, for all $k > r$, we have $\text{ord}_p(f(k)) > r$, and the claim holds trivially.

We are left with the case $\text{ord}_p(\alpha) = 0$, so L is an unramified extension of \mathbb{Z}_p . Denote by \mathcal{O}_L its ring of integers, and let $\mathfrak{p} = p\mathcal{O}_L$ denote the unique maximal ideal of \mathcal{O}_L . Then the residue field $\mathcal{O}_L/\mathfrak{p} \cong \mathbb{F}_{p^2}$, and hence (abusing notation again)

$$\alpha \in (\mathcal{O}_L/\mathfrak{p})^\times \cong \mathbb{F}_{p^2}^\times,$$

which has order $p^2 - 1$. It follows that

$$\alpha^{p^2-1} \in 1 + \mathfrak{p}.$$

We claim that for $n \geq 1$,

$$(5.2) \quad x \in 1 + \mathfrak{p}^n \implies x^p \in 1 + \mathfrak{p}^{n+1}.$$

Indeed, it suffices to write $x = 1 + x'p^n$ for some $x' \in \mathcal{O}_L$ and then apply the binomial expansion to x^p . By successive application of (5.2), we thus obtain

$$(5.3) \quad \alpha^{(p^2-1)p^{r-1}} \in 1 + \mathfrak{p}^r,$$

and the result follows since

$$k \equiv k' \pmod{\frac{1}{2}(p^2-1)p^r} \implies (p^2-1)p^{r-1} \mid 2(k-k').$$

□

We are now prepared to prove that the trace formula interpolates.

Theorem 5.6. *Fix positive coprime integers N and n . Then (as a function of k), $\mathrm{Tr}_{2k}(\Gamma_0(N), n) \in \mathcal{R}_p$ for all primes $p \geq 5$.*

Proof. The trace formula (Theorem 4.1) gives

$$\mathrm{Tr}_{2k}(\Gamma_0(N), n) = \tilde{\sigma}(k, N, n) - \sum_{s \in E \cup H} a(s, k, n)D(s, N, n),$$

with $D(s, N, n)$ defined in (4.4). Note that the sets E and H are independent of k , so it suffices to show that $\tilde{\sigma}$ and all terms of the sum interpolate.

Proving that $\tilde{\sigma} \in \mathcal{R}_p$ requires nothing more than looking back at its definition and applying the lemmas we have already proven. In the case that n is not a perfect square, $\tilde{\sigma}$ is identically zero and there is nothing to prove. Otherwise, $\tilde{\sigma}$ is given by (4.2). Then each of the terms

$$\frac{1}{12}N \prod_{\ell \mid N} (1 + 1/\ell), \quad \frac{\sqrt{n}}{2} \prod_{\ell \mid N} \mathrm{par}(\ell, N), \quad 2k-1, \quad \text{and} \quad n^{k-1}$$

interpolate. The first two are constants (with respect to k) in \mathbb{Z}_p because $p \nmid 12$. The third belongs to \mathcal{R}_p by Proposition 5.3, and the fourth by Lemma 5.4. Therefore, $\tilde{\sigma} \in \mathcal{R}_p$.

We now consider the terms $a(s, k, n)D(s, N, n)$. Recalling the definition (4.1) of $a(s, k, n)$, we see that there are two cases to consider, depending on whether s falls in E or H . The case $s \in H$ is easier. The key here is that Lemma 4.4 ensures that any powers of p dividing the denominator $|y - \bar{y}|$ of $a(s, k, n)$ are cancelled by $D(s, N, n)$. Thus, it is enough to prove that the remaining term $\min\{|y|, |\bar{y}|\}^{2k-1} \in \mathcal{R}_p$. Noting that $y, \bar{y} \in \mathbb{Z}$ for $s \in H$, so that $\min\{|y|, |\bar{y}|\}$ is a fixed positive integer, this is given to us by Lemma 5.5.

We are left with $s \in E$, which requires more work. Here, we simply discard the constant factor $D(s, N, n) \in \mathbb{Z}_p$, leaving us to prove

$$(5.4) \quad a'(k) := \frac{y^{2k-1} - \bar{y}^{2k-1}}{y - \bar{y}} \in \mathcal{R}_p.$$

First, suppose $\mu := \min\{\mathrm{ord}_p(y), \mathrm{ord}_p(\bar{y})\} \geq 1$. Then $z := y/p$ and $\bar{z} := \bar{y}/p$ are the roots of the monic quadratic $x^2 - \frac{s}{p}x + \frac{n}{p^2} \in \mathbb{Z}[x]$, so

$$a'(k) = p^{2k-2} \cdot \frac{z^{2k-1} - \bar{z}^{2k-1}}{z - \bar{z}}.$$

But the latter fraction is a symmetric polynomial in z and \bar{z} , hence is an integer. It follows that $\mathrm{ord}_p(a'(k)) \geq 2k-2 \geq r$ for all k , giving $a' \in \mathcal{R}_p$ trivially.

Now, note that 2μ is a nonnegative integer because y and \bar{y} belong to a quadratic extension of \mathbb{Z}_p . Thus, we are left to consider the cases $\mu = \frac{1}{2}$ and $\mu = 0$.

In the case $\mu = \frac{1}{2}$, we must have $\text{ord}_p(y) = \text{ord}_p(\bar{y}) = \frac{1}{2}$, because y and \bar{y} are Galois conjugates. From $s = y + \bar{y}$, $n = y\bar{y}$, we obtain $\text{ord}_p(s) \geq 1$, $\text{ord}_p(n) = 1$. Hence,

$$\text{ord}_p(y - \bar{y}) = \frac{1}{2}\text{ord}_p((y - \bar{y})^2) = \frac{1}{2}\text{ord}_p(s^2 - 4n) = \frac{1}{2}.$$

Therefore, $\text{ord}_p(a'(k)) \geq \frac{1}{2}(2k - 2) \geq r$ for all k , and again $a' \in \mathcal{R}_p$ trivially.

We are left with the case $\mu = 0$. Without loss of generality, let $\text{ord}_p(y) = 0$. If $\text{ord}_p(y - \bar{y}) = 0$ as well, then we may ignore the denominator of $a'(k)$ and apply Lemma 5.5 to show that $y^{2k-1}, \bar{y}^{2k-1} \in \mathcal{R}_p$, from which $a' \in \mathcal{R}_p$ follows immediately.

Suppose finally that $\nu := \text{ord}_p(y - \bar{y}) > 0$. Then $\text{ord}_p(\bar{y}) = 0$ as well. Also, $\nu \in \mathbb{Z}$ as the extension $L := \mathbb{Q}_p[y]$ is unramified. (Note: it is possible that the ‘‘extension’’ L is in fact just \mathbb{Q}_p , but we need not distinguish the two cases.) Letting \mathcal{O}_L denote the integer ring of L and \mathfrak{p} denote its maximal ideal as before, we have

$$y + \mathfrak{p}^\nu = \bar{y} + \mathfrak{p}^\nu \implies \bar{y}/y \in 1 + \mathfrak{p}^\nu.$$

Applying (5.2) repeatedly, we obtain

$$\bar{y}^{p^r}/y^{p^r} \in 1 + \mathfrak{p}^{\nu+r}.$$

It follows that for $2k \equiv 2k' \pmod{(p^2 - 1)p^r}$,

$$\begin{aligned} (5.5) \quad \frac{y^{2k-1} - \bar{y}^{2k-1}}{y - \bar{y}} &\equiv \frac{y^{2k-1} - \bar{y}^{2k-1} \cdot \left(\bar{y}^{-2k'-2k}/y^{2k'-2k}\right)}{y - \bar{y}} \pmod{\mathfrak{p}^r} \\ &\equiv y^{2k-2k'} \cdot \frac{y^{2k'-1} - \bar{y}^{2k'-1}}{y - \bar{y}} \pmod{\mathfrak{p}^r} \\ &\equiv \frac{y^{2k'-1} - \bar{y}^{2k'-1}}{y - \bar{y}} \pmod{\mathfrak{p}^r}, \end{aligned}$$

the last congruence holding because

$$y^{2k-2k'} \in 1 + \mathfrak{p}^r$$

by (5.3) from Lemma 5.5. We have thus shown that (5.4) holds in all cases, completing the proof of the theorem. \square

Proof of Theorem 1.3. The first claim of the theorem is simply a rewording of the interpolation theorem we have just proven. The second claim is that for values of n coprime to the level N , n not a quadratic residue mod p , the interpolation holds with one additional factor of p in the result. The reason is that the full strength of the condition $2k \equiv 2k' \pmod{(p^2 - 1)p^r}$ is rarely used; for most of our arguments, p^{r-1} is enough. In fact, the only place in which the congruence mod p^r is needed is in (5.5).

This occurs in the context of analyzing the term $a(s, k, n)$ for $s \in E$ such that $\text{ord}_p(y) = \text{ord}_p(\bar{y}) = 0$, $\text{ord}_p(y - \bar{y}) > 0$. Then we have

$$\text{ord}_p(n) = \text{ord}_p(y\bar{y}) = 0 \quad \text{and} \quad \text{ord}_p(s^2 - 4n) = \text{ord}_p((y - \bar{y})^2) > 0,$$

i.e., $s^2 - 4n \equiv 0 \pmod{p}$. Since p is odd, it follows that $n \equiv \left(\frac{s}{2}\right)^2 \pmod{p}$ is a quadratic residue mod p if (5.5) is ever applied. \square

Remark. Although we stated and proved Theorem 1.3 for primes $p \geq 5$, a similar result holds for $p = 3$, and we expect the same is true of $p = 2$. For $p = 3$, the results of Theorem 1.3 hold if we require an extra factor of 3 in the congruence condition on $2k$ and $2k'$. The reason is not hard to see: from Lemma 4.2, the numbers $b(s, f, n)$ are allowed to have a single factor of 3 in their denominators,

and likewise we must take into account the 12 in the denominator of the first term of $\tilde{\sigma}(k, N, n)$. These are the only changes that occur, however.

The case $p = 2$ is somewhat different. In this case, the formulas for $c(s, f, N, n, \ell)$ given in Lemma 4.2 change, and hence more casework would be required to obtain an analogue of Corollary 4.3. Because proving such a result would not substantially increase our understanding, we opt not to carry out the additional computations.

ACKNOWLEDGMENTS

The authors were supported by the University of Wisconsin–Madison NSF VIGRE REU program. We thank Ken Ono for his guidance, and Jeremy Rouse for providing GP/PARI code for computing traces of Hecke operators. We also thank them and Karl Mahlburg for carefully proofreading drafts of this manuscript. We are grateful to the referee for making several helpful suggestions and corrections.

REFERENCES

- [AO00] Scott Ahlgren and Ken Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, J. Reine Angew. Math. **518** (2000), 187–212. MR MR1739404 (2001c:11057)
- [BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over \mathbf{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR MR1839918 (2002d:11058)
- [Beu87] F. Beukers, *Another congruence for the Apéry numbers*, J. Number Theory **25** (1987), no. 2, 201–210. MR MR873877 (88b:11002)
- [CDT99] Brian Conrad, Fred Diamond, and Richard Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567. MR MR1639612 (99i:11037)
- [DK95] Fred Diamond and Kenneth Kramer, *Modularity of a family of elliptic curves*, Math. Res. Lett. **2** (1995), no. 3, 299–304. MR MR1338788 (96h:11050)
- [FOP04] Sharon Frechette, Ken Ono, and Matthew Papanikolas, *Combinatorics of traces of Hecke operators*, Proc. Natl. Acad. Sci. USA **101** (2004), no. 49, 17016–17020 (electronic). MR MR2114776 (2005h:11090)
- [GK79] Benedict H. Gross and Neal Koblitz, *Gauss sums and the p -adic Γ -function*, Ann. of Math. (2) **109** (1979), no. 3, 569–581. MR MR534763 (80g:12015)
- [Gre87] John Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77–101. MR MR879564 (88e:11122)
- [HPS89] Hiroaki Hijikata, Arnold K. Pizer, and Thomas R. Shemanske, *The basis problem for modular forms on $\Gamma_0(N)$* , Mem. Amer. Math. Soc. **82** (1989), no. 418, vi+159. MR MR960090 (90d:11056)
- [IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR MR1070716 (92e:11001)
- [Kob84] Neal Koblitz, *p -adic numbers, p -adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR MR754003 (86c:11086)
- [Kob93] ———, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR MR1216136 (94a:11078)
- [Lan95] Serge Lang, *Introduction to modular forms*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 222, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original. MR MR1363488 (96g:11037)
- [Rou] Jeremy Rouse, *Vanishing and non-vanishing of traces of Hecke operators*, To appear in Trans. Amer. Math. Soc.
- [TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR MR1333036 (96d:11072)
- [Wil95] Andrew Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR MR1333035 (96d:11071)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WI 53706

E-mail address: ploh@caltech.edu

E-mail address: rhoades@math.wisc.edu