

PARITY OF THE PARTITION FUNCTION AND TRACES OF SINGULAR MODULI

PAK-HIN LEE AND ALEXANDR ZAMORZAEV

ABSTRACT. We prove that the parity of the partition function is given by the “trace” of the Hauptmodul $j_6^*(z)$ for $\Gamma_0^*(6)$ at points of complex multiplication. Using Hecke operators, we generalize this to relate the Hecke traces of $j_6^*(z)$ to the partition function modulo 2. We then prove that the generating function for these Hecke traces is equal to the logarithmic derivative of the level 6 Hilbert class polynomial. Finally, we give a procedure involving Hilbert class polynomials for computing the parity of the partition function, and make some speculations about the distribution of these universal polynomials modulo class polynomials.

1. INTRODUCTION AND STATEMENT OF RESULTS

A *partition* of a non-negative integer n is a non-increasing sequence of positive integers whose sum is n . The partition function $p(n)$ is the number of partitions of n . Although there has been much work on the congruence properties of $p(n)$ since Ramanujan, little is known about its parity. For example, Parkin and Shanks [10] conjectured that the partition function is even and odd equally often, i.e.

$$\lim_{X \rightarrow \infty} \frac{\#\{n \leq X : p(n) \text{ is even (resp. odd)}\}}{X} = \frac{1}{2}.$$

However, the best result in the literature (for example, see [1] and [7]) essentially only assures that

$$\#\{n \leq X : p(n) \text{ is even (resp. odd)}\} \gg X^{\frac{1}{2}-\epsilon}.$$

In view of these difficulties, Bringmann and Ono [3] proposed to study the congruence properties of $p(n)$ using the properties of algebraic numbers associated to CM points (imaginary quadratic numbers). In this direction they have success for certain q -series modulo some small primes, but unfortunately $p(n)$ escapes this approach for now. However, they proved that $p(n)$ is the “twisted trace” of a certain Poincaré-Maass series. More precisely, let $I_s(x)$ denote the modified Bessel function of the first kind, $\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$ denote the translations in $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, and $\mathcal{Q}_{d,6}^*$ be the set of positive definite binary quadratic forms $[a, b, c] = aX^2 + bXY + cY^2$ with integer coefficients, a divisible by N , and discriminant $-d = b^2 - 4ac$, equipped with the usual action by the congruence subgroup $\Gamma_0(6)$. They define the Poincaré series $P(z)$ by

$$P(z) := 4\pi \sum_{A \in \Gamma_\infty \backslash \Gamma_0(6)} \mathrm{Im}(Az)^{\frac{1}{2}} I_{\frac{3}{2}}(2\pi \mathrm{Im}(Az)) \exp(-2\pi i \mathrm{Re}(Az))$$

Date: July 22, 2010.

and they showed that

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_{24n-1,6}^*/\Gamma_0(6)} \frac{1}{|\Gamma_{\alpha_Q}|} \chi_{12}(Q) P(\alpha_Q),$$

where $\chi_{12}(Q)$ is defined by $\chi_{12}([a, b, c]) := \left(\frac{12}{b}\right)$. They speculate that $P(\alpha_Q)$ is an algebraic number, but this has remained an open problem.

In this paper, we overcome this difficulty by proving a similar formula for the partition function modulo 2 which indeed involves algebraic integers, namely the singular moduli of the Hauptmodul $j_6^*(z)$ on $\Gamma_0^*(6)$. Before we state our results, we first recall some preliminaries and motivation.

The values of a modular function at CM points, or *singular moduli*, are closely related to half-integral weight modular forms. In [11], Zagier expressed the trace of singular moduli of Klein's j -invariant of discriminant $-d$ as the coefficient of q^d of a certain modular form of weight $3/2$. In Section 8 of [11], he generalized his result by replacing the function $j(z)$ by a modular function of higher level, namely, the Hauptmodul $j_N^*(z)$ associated to the genus zero group $\Gamma_0^*(N)$ (the extension of the congruence subgroup $\Gamma_0(N)$ by the group of all Atkin-Lehner involutions W_p where $p|N$).

We now recall the action of $\Gamma_0^*(N)$ on binary quadratic forms. For all positive integers $d \equiv 0$ or $3 \pmod{4}$, we denote by \mathcal{Q}_d the set of positive definite binary quadratic forms $aX^2 + bXY + cY^2$ with a, b, c integers and discriminant $b^2 - 4ac = -d$, with the usual action by the modular group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. To each $Q \in \mathcal{Q}_d$ we associate its unique root α_Q in the upper half plane. Let $\mathcal{Q}_{d,N}^*$ be the set of forms $aX^2 + bXY + cY^2 \in \mathcal{Q}_d$ with a divisible by N . Then $\Gamma_0^*(N)$ acts on $\mathcal{Q}_{d,N}^*$ naturally and the quotient $\mathcal{Q}_{d,N}^*/\Gamma_0^*(N)$ has a bijection with \mathcal{Q}_d/Γ . More precisely, we can pick a set of representatives of \mathcal{Q}_d/Γ satisfying $N|a$ (see [11] Section 8). For any $\Gamma_0^*(N)$ -invariant function $f(z)$ on the upper half plane, we define its trace to be

$$(1) \quad \mathrm{Tr}(f, N; d) := \sum_{Q \in \mathcal{Q}_{d,N}^*/\Gamma_0^*(N)} \frac{1}{\omega_Q} f(\alpha_Q),$$

where ω_Q is the size of the isotropy subgroup of Q in $\Gamma_0^*(N)$. Note that a positive integer d is a discriminant of $\mathcal{Q}_{d,N}^*$ if and only if $-d$ is a square modulo $4N$.

Our first result relates the parity of the partition function to the trace of singular moduli of the Hauptmodul $j_6^*(z)$ for $\Gamma_0^*(6)$, which is given by the formula

$$j_6^*(z) := \left(\frac{\eta(z)\eta(2z)}{\eta(3z)\eta(6z)} \right)^4 + 4 + 3^4 \left(\frac{\eta(3z)\eta(6z)}{\eta(z)\eta(2z)} \right)^4 = q^{-1} + 79q + 353q^2 + \dots$$

where $\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n)$ is Dedekind's eta-function and $q := e^{2\pi iz}$ throughout.

For notational simplicity, throughout this paper we denote the *trace of $j_6^*(z)$ of discriminant $-d$* to be

$$(2) \quad \mathrm{Tr}_1^*(d) := \mathrm{Tr}(j_6^*, 6; d).$$

For example, we have

$$\mathrm{Tr}_1^*(23) = j_6^* \left(\frac{1 + \sqrt{-23}}{12} \right) + j_6^* \left(\frac{5 + \sqrt{-23}}{12} \right) + j_6^* \left(\frac{-5 + \sqrt{-23}}{12} \right) = -13.$$

We observe that

$$\begin{aligned}
 \sum_{n=1}^{\infty} \text{Tr}_1^*(24n-1)q^n &= -13q - 8q^2 - 29q^3 - q^4 - 53q^5 + 9q^6 - 59q^7 + 22q^8 + \dots \\
 &\equiv q + q^3 + q^4 + q^5 + q^6 + q^7 + q^{12} + q^{13} + q^{14} + q^{16} + q^{17} + q^{18} + q^{20} + \dots \pmod{2}, \\
 \sum_{n=1}^{\infty} p(n)q^n &= q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + 11q^6 + 15q^7 + 22q^8 + \dots \\
 &\equiv q + q^3 + q^4 + q^5 + q^6 + q^7 + q^{12} + q^{13} + q^{14} + q^{16} + q^{17} + q^{18} + q^{20} + \dots \pmod{2},
 \end{aligned}$$

which suggests that $p(n) \equiv \text{Tr}_1^*(24n-1) \pmod{2}$. Indeed this holds for all positive integers n , as follows.

Theorem 1.1. *For any positive integer $N \equiv 23 \pmod{24}$, we have*

$$p\left(\frac{N+1}{24}\right) \equiv \text{Tr}_1^*(N) \pmod{2}.$$

Remark (1). The proof will show that the odd values of $\text{Tr}_1^*(d)$ are supported on $d \equiv -1 \pmod{24}$.

Remark (2). Any positive integer $N \equiv 23 \pmod{24}$ can be uniquely written as $N = dm^2$, where d is a square-free integer with $1 < d \equiv 23 \pmod{24}$ and m is a positive integer coprime to 6. We shall see the important roles of d , which comes from algebraic number theory, and m , which relates to Hecke operators.

In fact this theorem holds in greater generality. Let $J_{6,m}^*(z)$ be the unique weakly holomorphic modular form of weight 0 on $\Gamma_0^*(6)$ of the form $J_{6,m}^*(z) = q^{-m} + O(q)$. Since j_6^* generates the algebra of weakly holomorphic modular functions on $\Gamma_0^*(6)$, it follows that

$$J_{6,m}^*(z) = \mathcal{J}_m(j_6^*(z)) = q^{-m} + O(q)$$

for some monic polynomial \mathcal{J}_m of degree m . Note that \mathcal{J}_m has integer coefficients, since all the Fourier coefficients of $j_6^*(z)$ are integers.

The first few $J_{6,m}^*$ are given by:

$$\begin{aligned}
 J_{6,0}^*(z) &= 1, \\
 J_{6,1}^*(z) &= j_6^*(z) \\
 &= q^{-1} + 79q + 352q^2 + 1431q^3 + 4160q^4 + 13015q^5 + 31968q^6 + \dots, \\
 J_{6,2}^*(z) &= j_6^*(z)^2 - 158 \\
 &= q^{-2} + 704q + 9103q^2 + 63936q^3 + 376032q^4 + 1728640q^5 + 7195095q^6 + \dots, \\
 J_{6,3}^*(z) &= j_6^*(z)^3 - 237j_6^*(z) - 1056 \\
 &= q^{-3} + 4293q + 95904q^2 + 1242943q^3 + 10694592q^4 + 74415105q^5 + \dots.
 \end{aligned}$$

We define the m -th Hecke trace of $j_6^*(z)$ of discriminant $-d$ to be

$$(3) \quad \text{Tr}_m^*(d) := \text{Tr}(J_{6,m}^*, 6; d).$$

Remark. For fundamental discriminants $-d \equiv 1 \pmod{24}$, $\omega_Q = 1$ for all $Q \in \mathcal{Q}_{d,6}^*$, so

$$\mathrm{Tr}_m^*(d) = \sum_{Q \in \mathcal{Q}_{d,6}^*/\Gamma_0^*(6)} J_{6,m}^*(\alpha_Q) = \sum_{Q \in \mathcal{Q}_{d,6}^*/\Gamma_0^*(6)} \mathcal{J}_m(J_6^*(\alpha_Q))$$

is a sum of algebraic integers. In particular, we have that

$$(4) \quad \mathrm{Tr}_0^*(d) = |\mathcal{Q}_{d,6}^*/\Gamma_0^*(6)| = |\mathcal{Q}_d/\Gamma| = H(d)$$

is the usual class number of discriminant $-d$.

Then Theorem 1.1 generalizes to the following.

Theorem 1.2. *Let d be a square-free integer with $1 < d \equiv 23 \pmod{24}$ and m be a positive integer. Then we have*

$$\mathrm{Tr}_m^*(d) \equiv \sum_{\substack{n|m \\ \gcd(n,6)=1 \\ \gcd(m/n,d)=1}} p\left(\frac{dn^2+1}{24}\right) \pmod{2}.$$

As a consequence of Theorem 1.2, we have the following theorem.

Theorem 1.3. *Let d be a square-free integer with $1 < d \equiv 23 \pmod{24}$ and m be a positive integer coprime to 6. If we write $m = ust$ where u is the product of all prime factors (repeated with multiplicity) of m dividing d (so that st is the largest divisor of m that is coprime to d) and $s = \mathrm{rad}(\frac{m}{u})$ is the radical of $\frac{m}{u}$, then we have*

$$(5) \quad p\left(\frac{dm^2+1}{24}\right) \equiv \sum_{w|s} \mathrm{Tr}_{uwt}^*(d) \pmod{2}.$$

Remark. By Remark (2) following Theorem 1.1, every partition number $p(n)$ appears in (5) for a unique pair of d and m satisfying the required conditions.

Remark. Since $-d$ is a fundamental discriminant of $\mathcal{Q}_{d,6}^*$, this theorem expresses the parity of $p(n)$ as a sum of algebraic integers for all positive integers n , which is not directly obvious from Theorem 1.1 in the case when N is not square-free. In Section 4, we shall make use of the fact that $-d$ is fundamental again.

In Section 2 we prove Theorem 1.1 by considering a certain weight $3/2$ modular form. In analogy with Zagier [11], we then consider a sequence of weight $3/2$ modular forms on $\Gamma_0(24)$ and their images under Hecke operators, which will imply Theorem 1.2. Theorem 1.3 will follow as a consequence. The remaining sections will be dedicated to some applications of these results.

In Section 3, we prove a formula for the generating function of the Hecke traces of a fixed discriminant in terms of the level 6 Hilbert class polynomial \mathcal{H}_d , which enables us to give a new proof of Ono's result in [9] without employing the machinery of generalized Borcherds products developed in [5]. More precisely, we prove the following theorem of Ono (see Theorem 1.1 of [9]).

Theorem 1.4. *If d is a square-free integer with $1 < d \equiv 23 \pmod{24}$, then the generating function defined by*

$$\widehat{F}(d; z) := \sum_{\substack{m \geq 1 \\ \gcd(m, 6) = 1}} p\left(\frac{dm^2 + 1}{24}\right) \sum_{\substack{n \geq 1 \\ \gcd(n, d) = 1}} q^{mn}$$

is congruent modulo 2 to a weight 2 meromorphic modular form on $\Gamma_0^(6)$ with integer coefficients whose poles are simple and are supported at CM points of $\mathcal{Q}_{d,6}^*$.*

Remark. Theorem 1.4 extends the mod 2 modularity of $\widehat{F}(d; z)$ on $\Gamma_0(6)$, which was proved in [5], to modularity on $\Gamma_0^*(6)$.

In Section 4, we show that Theorem 1.3 gives rise to a very curious procedure involving Hilbert class polynomials for computing the parity of the partition function; namely, the remainders of the polynomials \mathcal{J}_m modulo \mathcal{H}_d determine the parity of $p(n)$. Finally, we make some speculations about the distribution of the coefficients of this set of polynomials which will shed light on the parity of $p(n)$ from an algebraic viewpoint.

2. TRACES OF SINGULAR MODULI

Motivated by Zagier, we consider the generating function

$$(6) \quad g_1(z) := q^{-1} - 2 + \sum_{d > 0} B(1, d)q^d$$

where

$$B(1, d) := \begin{cases} \text{Tr}_1^*(d) & \text{if } -d \text{ is a square modulo } 24, \\ 0 & \text{otherwise.} \end{cases}$$

The works by Zagier [11] and Kim [6] show that g_1 is a weakly holomorphic modular form of weight $3/2$ on $\Gamma_0(24)$. By definition, g_1 is in the *Kohnen plus space* $M_{3/2}^+(\Gamma_0(24))^\dagger$, the space of weakly holomorphic modular forms of weight $3/2$ on $\Gamma_0(24)$ whose coefficients are supported at n with $-n$ a square modulo 24.

Here we prove that $g_1(z)\eta(24z)$ is a holomorphic modular form equal to 1 modulo 2. This will almost immediately imply the relationship between the parity of $p(n)$ and traces of j_6^* .

Proposition 2.1. *We have that $g_1(z)\eta(24z)$ is a holomorphic modular form of weight 2 on $\Gamma_0(576)$ with Nebentypus χ_{12} , where*

$$\chi_{12}(n) := \left(\frac{12}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 11 \pmod{12}, \\ -1 & \text{if } n \equiv 5, 7 \pmod{12}, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, the q -series expansion of $g_1(z)\eta(24z)$ is equal to 1 modulo 2.

Proof. It is well-known that $\eta(24z) \in S_{1/2}(\Gamma_0(576), \chi_{12})$, hence $g_1(z)\eta(24z)$ is a meromorphic modular form of weight 2 on $\Gamma_0(576)$ with Nebentypus χ_{12} . To show $g_1(z)\eta(24z)$ is holomorphic, it suffices to prove that all the poles of $g_1(z)$ at cusps of $\Gamma_0(24)$ are canceled by the zeros of $\eta(24z)$ there. Following the argument in [4], $g_1(z)$ can be expressed as the image of a Poincaré series under the projection operator onto the Kohnen plus space $M_{3/2}^+(\Gamma_0(24))^\dagger$.

Since the Poincaré series in consideration has a simple pole at infinity and is holomorphic at all other cusps of $\Gamma_0(24)$, the poles of its projection cannot be of order greater than 1, hence are canceled by $\eta(24z)$. We refer the reader to [4] for more details of the explicit calculations.

To prove the congruence relation note that the definition of η implies that

$$\eta(24z) \equiv \eta(3z)^8 \pmod{2},$$

hence it suffices to prove it for the q -expansion of $g_1(z)\eta(3z)^8$. We have that $\eta(3z)^8 \in S_4(\Gamma_0(9))$, so by the same argument as before, it follows that $g_1(z)\eta(3z)^8 \in M_{11/2}(\Gamma_0(72))$. If we let $\theta_0(z)$ be the classical theta-function

$$\theta_0(z) := \sum_{n \in \mathbb{Z}} q^{n^2}$$

then we have that $\theta_0(z)^{11}$ is an element of $M_{11/2}(\Gamma_0(4))$ and its q -expansion equals 1 modulo 2. Therefore, by Sturm's Theorem (see Section 2.9 of [8] for the complete statement) applied to $g_1(z)\eta(3z)^8 - \theta_0(z)^{11}$, it suffices to numerically check the first

$$\frac{11}{24}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(72)] = 66$$

coefficients of $g_1(z)\eta(3z)^8$ in order to prove the congruence. □

Proposition 2.2. *The odd values of $B(1, d)$ are supported on d congruent to -1 modulo 24 . Moreover, for all such d we have that*

$$B(1, d) \equiv p \left(\frac{d+1}{24} \right) \pmod{2}.$$

Proof. We have that $g_1(z)\eta(24z) \in M_2(\Gamma_0(576), \chi_{12})$ and the q -expansion of $g_1(z)\eta(24z)$ equals 1 modulo 2. By the identity

$$\frac{1}{\eta(z)} = \sum_{n=0}^{\infty} p(n)q^{n-\frac{1}{24}},$$

we have

$$g_1(z) \equiv \frac{1}{\eta(24z)} \equiv \sum_{n=0}^{\infty} p(n)q^{24n-1} \pmod{2}.$$

□

Proof of Theorem 1.1. Follows immediately from Proposition 2.2. □

Next, we generalize our congruence to higher order traces. Let the *Kohnen plus space* $M_{k+1/2}^+(\Gamma_0(24))^\dagger$ be the space of weakly holomorphic modular forms of weight $k+1/2$ on $\Gamma_0(24)$ whose coefficients are supported at n with $(-1)^k n$ a square modulo 24. It turns out that for every $D > 0$ that is a square modulo 24 there exists a unique element g_D of $M_{3/2}^+(\Gamma_0(24))^\dagger$ of the form

$$g_D(z) = q^{-D} + \sum_{d \geq 0} B(D, d)q^d.$$

Kim [6] has proved the following expression for the traces of J_m^* in terms of Fourier coefficients of g_D 's:

$$(7) \quad \mathrm{Tr}_m^*(d) = - \sum_{u|m} 2^{s(u,6)} u B(u^2, d)$$

where $s(u, n)$ is the number of distinct primes that divide both u and n .

Similarly, for every $d \geq 0$ such that $-d$ is a square modulo 24, there exists a unique element f_d of $M_{1/2}^+(\Gamma_0(24))^\dagger$ of the form

$$f_d(z) = q^{-d} + \sum_{D>0} A(D, d) q^D.$$

Kim [6] has proved the following astonishing symmetry between the coefficients of g_D 's and f_d 's

$$(8) \quad B(D, d) = -A(D, d).$$

Recall that the action of Hecke operators $T(p^2)$ of prime index $p \neq 2, 3$ on $M_{3/2}^+(\Gamma_0(24))^\dagger$ and $M_{3/2}^+(\Gamma_0(24))^\dagger$ is given by

$$(9) \quad g|_{3/2} T(p^2) = \sum_{n \in \mathbb{Z}} \left(b(np^2) + \left(\frac{-n}{p} \right) b(n) + pb(n/p^2) \right) q^n$$

for $f = (\sum_n b(n)q^n) \in M_{3/2}^+(\Gamma_0(24))^\dagger$ and

$$(10) \quad f|_{1/2} T(p^2) = \sum_{n \in \mathbb{Z}} \left(pa(np^2) + \left(\frac{n}{p} \right) a(n) + a(n/p^2) \right) q^n$$

for $f = (\sum_n a(n)q^n) \in M_{1/2}^+(\Gamma_0(24))^\dagger$ with the usual convention that $a(q)$ and $b(q)$ are zero for non-integer q . We can generalize (8) as follows.

Proposition 2.3. *Let \mathcal{A} be the algebra generated by the Hecke operators of prime index not equal to 2 or 3. Given $D > 0$ and $d \geq 0$ such that D and $-d$ are squares modulo 24 and T an element of \mathcal{A} , we have that the coefficient of $g_D|_{3/2} T$ at q^d equals minus the coefficient of $f_d|_{1/2} T$ at q^D .*

Proof. The following proof is based on Zagier's proof of a similar symmetry between the spaces $M_{3/2}^+(\Gamma_0(4))^\dagger$ and $M_{1/2}^+(\Gamma_0(4))^\dagger$ [11].

Using (9) and (10) we can show by induction that the action of T on $M_{3/2}^+(\Gamma_0(24))^\dagger$ and $M_{3/2}^+(\Gamma_0(24))^\dagger$ can be described as follows

$$(11) \quad g|_{3/2} T = \sum_{n \in \mathbb{Z}} \sum_{r \in \mathbb{Q}^+} \alpha_r(-nr) b(nr^2) q^n$$

for $g = (\sum_n b(n)q^n) \in M_{3/2}^+(\Gamma_0(24))^\dagger$ and

$$(12) \quad f|_{1/2} T = \sum_{n \in \mathbb{Z}} \sum_{r \in \mathbb{Q}^+} \alpha_r(n/r) a(n/r^2) q^n$$

for $f = (\sum_n a(n)q^n) \in M_{1/2}^+(\Gamma_0(24))^\dagger$, where $\alpha_r(n)$ are some linear combinations of products of quadratic characters of the form $\left(\frac{u^2 n/v^2}{w} \right)$ and all but finitely many α_r are identically zero.

Since the principal part of g_D is q^{-D} we have that the principal part of $g_D|T$ is given by

$$\sum_{n < 0} \sum_{r \in \mathbb{Q}^+} \alpha_r(-nr) \delta_{nr^2, -D} q^n = \sum_{r \in \mathbb{Q}^+} \alpha_r(D/r) q^{-D/r^2}$$

where δ is the Kronecker δ -function and the non-integer exponents of q are omitted. By the uniqueness of g_D 's we have that

$$(13) \quad g_D|T = \sum_{r \in \mathbb{Q}^+} \alpha_r(D/r) g_{D/r^2}$$

where, again, g_{D/r^2} is zero whenever it is not well-defined. Note that coefficient at q^d of the right hand side equals

$$\sum_{n \in \mathbb{Z}} \sum_{r \in \mathbb{Q}^+} \alpha_r(D/r) B(D/r^2, d)$$

which by (8) and (12) equals minus the coefficient of $f_d|T$ at q^D . Thus, (13) gives us the desired identity. \square

Proof of Theorem 1.2. Reducing (7) modulo 2 gives us

$$(14) \quad \text{Tr}_m^*(d) \equiv \sum_{\substack{u|m \\ \gcd(u,6)=1}} B(u^2, d) \pmod{2}.$$

Let M be largest divisor of m that is coprime to 6. We are going to express the right hand side as the d -th coefficient the image of g_1 under an element $\beta(M)$ of the Hecke algebra which we will define recursively. Set $\beta(1) = \text{id}$ and $\beta(p) = T(p^2)$ for primes p that are not 2 or 3. We define β for powers of primes recursively by

$$\beta(p^k) = \beta(p^{k-1})T(p^2) + \beta(p^{k-2})$$

for $k \geq 2$. Finally, if $n = \prod p_i^{n_i}$ is coprime to 6 then $\beta(n)$ is defined multiplicatively as follows

$$\beta(n) = \prod \beta(p_i^{n_i}).$$

Note that the order of the prime factors of n does not matter because the Hecke algebra is commutative.

By looking at the principal part, it is easy to see that

$$g_n|_{3/2} T(p^2) \equiv g_{np^2} + \left(\frac{-n}{p}\right) g_n + g_{n/p^2} \pmod{2}$$

and

$$f_n|_{1/2} T(p^2) \equiv f_{np^2} + \left(\frac{n}{p}\right) f_n + f_{n/p^2} \pmod{2}$$

for a prime p that is not 2 or 3, where, as before, f_r and g_r are omitted whenever they are not defined. Using the congruences above and the fact that

$$\beta(np^2) = \beta(np)T(p^2) + \beta(n)$$

for every positive n we show inductively that

$$(15) \quad g_1|_{3/2} \beta(M) \equiv \sum_{u|M} g_{u^2} \pmod{2}$$

and

$$(16) \quad f_d|_{1/2}\beta(M) \equiv \sum_{u|M} \left(\frac{d}{M/u} \right) f_{du^2} \pmod{2}$$

for a square-free $d \equiv -1 \pmod{24}$. Comparing the coefficient at q^d of (15) and the coefficient at q of (16) and applying Proposition 2.3 we get the following congruence

$$\sum_{u|M} \left(\frac{d}{M/u} \right) B(1, u^2d) \equiv \sum_{u|M} uB(u^2, d) \pmod{2}$$

which together with Theorem 1.1 and congruence (14) gives us the desired result. \square

Proof of Theorem 1.3. Assuming the notations defined in the statement of the theorem, we see that Theorem 1.2 gives

$$\mathrm{Tr}_{ust}^*(d) \equiv \sum_{n|st} p \left(\frac{du^2n^2 + 1}{24} \right) \pmod{2}.$$

An application of the Möbius inversion formula yields

$$p \left(\frac{dm^2 + 1}{24} \right) \equiv \sum_{n|st} \mu \left(\frac{st}{n} \right) \mathrm{Tr}_{un}^*(d) \pmod{2}.$$

Since μ takes the value ± 1 at square-free integers and 0 elsewhere, the term $\mu \left(\frac{st}{n} \right)$ vanishes unless $\frac{st}{n}$ divides $\mathrm{rad}(st) = s$, i.e. n is divisible by t . Letting $n = wt$, we get

$$p \left(\frac{dm^2 + 1}{24} \right) \equiv \sum_{w|s} \mathrm{Tr}_{uwt}^*(d) \pmod{2}$$

as desired. \square

3. HILBERT CLASS POLYNOMIAL AND THE GENERATING FUNCTION FOR Tr_m^*

First we derive a formula for the generating function for $\mathcal{J}_m(x)$. Recall the definition of Ramanujan's Theta-operator:

$$\Theta \left(\sum_{n=n_0}^{\infty} a_n q^n \right) := \sum_{n=n_0}^{\infty} n a_n q^n.$$

It is clear that $\Theta = q \frac{d}{dq} = \frac{1}{2\pi i} \frac{d}{dz}$.

By the theory of the Theta-operator, the derivative of $j_6^*(z)$ is a weakly holomorphic modular form of weight 2 on $\Gamma_0^*(6)$. A direct calculation gives the formula

$$\begin{aligned} \Theta(j_6^*(z)) &= \frac{1}{6} \left(\left(\frac{\eta(z)\eta(2z)}{\eta(3z)\eta(6z)} \right)^4 - 3^4 \left(\frac{\eta(3z)\eta(6z)}{\eta(z)\eta(2z)} \right)^4 \right) (E_2(z) + 2E_2(2z) - 3E_2(3z) - 6E_2(6z)) \\ &= -\frac{1}{q} + 79q + 704q^2 + \dots, \end{aligned}$$

where $E_2(z) := 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n)q^n$ is the classical nearly holomorphic Eisenstein series.

Proposition 3.1. *The generating function for $\mathcal{J}_m(x)$ is equal to*

$$-\frac{\Theta j_6^*(z)}{j_6^*(z) - x} = \sum_{m=0}^{\infty} \mathcal{J}_m(x)q^m = 1 + xq + (x^2 - 158)q^2 + (x^3 - 237x - 1056)q^3 + \cdots.$$

Proof. The following is motivated by Asai, Kaneko and Ninomiya's [2] proof of the analogous formula for $j(z)$ on $\mathrm{SL}_2(\mathbb{Z})$.

Since j_6^* is surjective onto the Riemann sphere $\mathbb{C} \cup \{\infty\}$, it is equivalent to prove the following:

$$-\frac{\Theta j_6^*(z)}{j_6^*(z) - j_6^*(x)} = \sum_{m=0}^{\infty} J_{6,m}^*(x)q^m.$$

Let $j_6^*(x) = p^{-1} + \sum_{n \geq 1} c_n p^n$ where $p = e^{2\pi i x}$. By the definition of the Theta-operator, we have

$$(17) \quad \Theta j_6^*(x) = -p^{-1} + \sum_{n=1}^{\infty} n c_n p^n.$$

On the other hand, for any non-negative integer m , $(\Theta j_6^*(x))J_{6,m}^*(x) = (\Theta j_6^*(x))\mathcal{J}_m(j_6^*(x))$ is the derivative of a polynomial (namely, the antiderivative of \mathcal{J}_m) in $j_6^*(x)$, and hence has zero constant term in its Fourier expansion (recall that $\frac{1}{2\pi i} \frac{d}{dx} = p \frac{d}{dp}$). Denoting $J_{6,m}^*(x) = p^{-m} + a_m p + \cdots$, we have $m c_m - a_m = 0$.

Since $j_6^*(x)J_{6,m}^*(x)$ is a weakly holomorphic modular function on $\Gamma_0^*(6)$, it is uniquely determined by its principal part. By comparing coefficients and using the relation $a_m = m c_m$, we obtain

$$j_6^*(x)J_{6,m}^*(x) = J_{6,m+1}^*(x) + \sum_{n=0}^m c_{m-n} J_{6,n}^*(x) + m c_m$$

for non-negative integers m .

Multiplying both sides of the above equation by q^m and summing over all non-negative integers m , we get

$$j_6^*(x) \sum_{m=0}^{\infty} J_{6,m}^*(x)q^m = \sum_{m=0}^{\infty} J_{6,m+1}^*(x)q^m + \left(\sum_{m=0}^{\infty} c_m q^m \right) \left(\sum_{m=0}^{\infty} J_{6,m}^*(x)q^m \right) + \sum_{m=0}^{\infty} m c_m q^m.$$

Using $j_6^*(z) = q^{-1} + \sum_{m \geq 1} c_m q^m$ and (17), this simplifies to

$$\sum_{m=0}^{\infty} J_{6,m}^*(x)q^m = -\frac{\Theta j_6^*(z)}{j_6^*(z) - j_6^*(x)}.$$

□

For any discriminant $-d$ of $\mathcal{Q}_{d,6}^*$, we define the *level 6 Hilbert class polynomial* to be

$$(18) \quad \mathcal{H}_d(x) := \prod_{Q \in \mathcal{Q}_{d,6}^*/\Gamma_0^*(6)} (x - j_6^*(\alpha_Q))^{\frac{1}{\omega_Q}}.$$

Remark. For fundamental discriminants $-d \equiv 1 \pmod{24}$, the factor $\frac{1}{\omega_Q}$ is always 1 and \mathcal{H}_d is a polynomial of degree $H(d)$, the class number of discriminant $-d$ (see (4)). For example, we have

$$\mathcal{H}_{23}(x) = x^3 + 13x^2 - 274x - 4265.$$

It is well-known that the Hauptmodul j_6^* takes on algebraic integer values at CM points in the upper half plane, and in the case when $-d \equiv 1 \pmod{24}$ is a fundamental discriminant of $\mathcal{Q}_{d,6}^*$ we have that $\mathcal{H}_d(x)$ is the minimal polynomial for all the $j_6^*(\alpha_Q)$, where Q runs through a set of $\Gamma_0^*(6)$ -representatives of $\mathcal{Q}_{d,6}^*$. Hence \mathcal{H}_d has integer coefficients. Moreover, $\mathcal{H}_d(j_6^*(z))$ is a modular function on $\Gamma_0^*(6)$ whose zeros are supported at CM points of $\mathcal{Q}_{d,6}^*$. In analogy with Theorem 5 in [11], we have the following

Proposition 3.2. *For all fundamental discriminants $-d \equiv 1 \pmod{24}$ of $\mathcal{Q}_{d,6}^*$, we have*

$$(19) \quad \mathcal{H}_d(j_6^*(z)) = q^{-H(d)} \exp \left(- \sum_{m=1}^{\infty} \text{Tr}_m^*(d) \frac{q^m}{m} \right).$$

Proof. Proposition 3.1 easily implies that

$$j_6^*(z) - j_6^*(x) = q^{-1} \exp \left(- \sum_{m=1}^{\infty} J_{6,m}^*(x) \frac{q^m}{m} \right).$$

Substituting into the formula

$$\mathcal{H}_d(j_6^*(z)) = \prod_{Q \in \mathcal{Q}_{d,6}^*/\Gamma_0^*(6)} (j_6^*(z) - j_6^*(\alpha_Q))^{\frac{1}{\omega_Q}},$$

we obtain the desired identity. \square

Now we show that $\mathcal{H}_d(j_6^*(z))$ is closely related to the generating function for the Hecke traces of j_6^* . More precisely, we have

Theorem 3.3. *The generating function for the m -th Hecke traces Tr_m^* of j_6^* of a fixed fundamental discriminant $-d \equiv 1 \pmod{24}$ of $\mathcal{Q}_{d,6}^*$ is a weight 2 meromorphic modular form on $\Gamma_0^*(6)$ with integer coefficients whose poles are simple and are supported at CM points of $\mathcal{Q}_{d,6}^*$. Furthermore, we have*

$$\sum_{m=0}^{\infty} \text{Tr}_m^*(d) q^m = - \frac{\Theta(\mathcal{H}_d(j_6^*(z)))}{\mathcal{H}_d(j_6^*(z))}.$$

Proof. The given identity follows by taking logarithmic derivatives on both sides of (19). The first statement is then clear since $\mathcal{H}_d(j_6^*(z))$ is a weight 0 modular form on $\Gamma_0^*(6)$ whose zeros are supported at CM points of $\mathcal{Q}_{d,6}^*$ and whose only pole is at infinity. \square

In [9], Ono proved that if $1 < d \equiv 23 \pmod{24}$ is square-free, then the generating function

$$\widehat{F}(d; z) = \sum_{\substack{m \geq 1 \\ \gcd(m,6)=1}} p \left(\frac{dm^2 + 1}{24} \right) \sum_{\substack{n \geq 1 \\ \gcd(n,d)=1}} q^{mn}$$

is congruent modulo 2 to a weight 2 meromorphic modular form on $\Gamma_0(6)$ with integer coefficients, namely, the logarithmic derivative of a certain generalized Borcherds product. The mod 2 modularity of $\widehat{F}(d; z)$ is then used to prove results about the parity of $p\left(\frac{dm^2+1}{24}\right)$.

In view of our results above, we offer a new proof of Ono's result (see Theorem 1.1 of [9]).

Proof of Theorem 1.4. For $d \equiv 23 \pmod{24}$ positive and square-free, Theorem 1.2 and Theorem 3.3 together imply that

$$\widehat{F}(d; z) \equiv \frac{\Theta(\mathcal{H}_d(j_6^*(z)))}{\mathcal{H}_d(j_6^*(z))} \pmod{2}.$$

□

4. UNIVERSAL POLYNOMIALS MODULO \mathcal{H}_d

Throughout this section d will denote a square-free integer d with $1 < d \equiv 23 \pmod{24}$ (so that $-d$ is a fundamental discriminant of $\mathcal{Q}_{d,6}^*$) and m will denote a positive integer. We define the polynomial $\mathcal{R}_{d,m}$ to be the remainder of \mathcal{J}_m upon division by \mathcal{H}_d . Thus $\mathcal{R}_{d,m}$ is a polynomial with integer coefficients of degree at most $H(d) - 1$, where $H(d)$ is the class number of discriminant $-d$.

Since \mathcal{J}_k are monic polynomials of degree k , $\mathcal{R}_{d,m}$ can be expressed as a unique linear combination of \mathcal{J}_k over the integers, where $0 \leq k \leq H(d) - 1$, i.e. there exist unique integers $a_{d,m,k}$ such that

$$(20) \quad \mathcal{R}_{d,m}(x) = \sum_{k=0}^{H(d)-1} a_{d,m,k} \mathcal{J}_k(x).$$

We relate the residues of $a_{d,m,k}$ modulo 2 to the partition function. Since $j_6^*(\alpha_Q)$ is a root of \mathcal{H}_d for any $Q \in \mathcal{Q}_{d,6}^*$, we have

$$J_{6,m}^*(\alpha_Q) = \mathcal{J}_m(j_6^*(\alpha_Q)) = \mathcal{R}_{d,m}(j_6^*(\alpha_Q)).$$

Summing the above identity over all Q in $\mathcal{Q}_{d,6}^*$ and applying (20) gives

$$(21) \quad \mathrm{Tr}_m^*(d) = \sum_{k=0}^{H(d)-1} a_{d,m,k} \mathrm{Tr}_k^*(d)$$

for every positive integer m . This gives a procedure for computing $\mathrm{Tr}_m^*(d)$ for all positive integers m , given the first $H(d)$ such values and the universal polynomials \mathcal{J}_m modulo \mathcal{H}_d . By Theorem 1.3, we then have the following.

Theorem 4.1. *There exists an algorithm for computing the parity of $p(n)$ for any positive integer n which involves the values of $\mathrm{Tr}_k^*(d)$ for $0 \leq k \leq H(d) - 1$ and the polynomials $\overline{\mathcal{R}}_{d,m}(x) \in \mathbb{F}_2[x]$ (the reduction of $\mathcal{R}_{d,m}$ modulo 2) for $m \in \mathbb{N}$, where d is the square-free part of $24n - 1$.*

By (21), if $\mathrm{Tr}_m^*(d) \equiv 0 \pmod{2}$ for all m between 0 and $H(d) - 1$, then $\mathrm{Tr}_m^*(d) \equiv 0 \pmod{2}$ for all non-negative integers m . In this case, moreover, Theorem 1.3 would imply that $p\left(\frac{dm^2+1}{24}\right)$ is even for all positive integers m coprime to 6. However, this scenario seems to be inconsistent with the numerical evidence that the parity of $p(n)$ behaves randomly. For

example, Ono [9] proved that for all $d < 25000$, $p\left(\frac{dm^2+1}{24}\right)$ is even (resp. odd) for infinitely many m coprime to 6. We make the following conjecture.

Conjecture 4.2. *If d is a square-free integer with $1 < d \equiv 23 \pmod{24}$, then $\text{Tr}_m^*(d)$ is odd for some $0 \leq m \leq H(d) - 1$.*

The distribution of the polynomials $\overline{\mathcal{R}}_{d,m}$ has number-theoretic significance related to the partition function. There are exactly $2^{H(d)}$ possibilities for $\overline{\mathcal{R}}_{d,m}(x)$, namely, all polynomials in $\mathbb{F}_2[x]$ of degree strictly smaller than $H(d)$. When $d = 23$, there are $2^{H(23)} = 8$ polynomials in $\mathbb{F}_2[x]$ of degree smaller than 3. The frequency of each of their occurrence in the set $\{\overline{\mathcal{R}}_{23,m}(x) : 0 \leq m \leq M\}$, where M ranges from 1000 to 10000, is listed as follows:

M	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
1000	11.70%	11.70%	12.30%	12.70%	12.30%	14.00%	13.60%	11.80%
2000	13.00%	11.45%	12.15%	13.15%	12.15%	12.70%	13.40%	12.05%
3000	13.80%	11.40%	11.83%	13.03%	11.83%	13.07%	12.70%	12.37%
4000	13.45%	11.73%	12.28%	12.78%	12.13%	13.18%	12.50%	12.00%
5000	13.52%	11.68%	12.42%	12.48%	11.96%	13.14%	12.78%	12.04%
6000	13.63%	11.68%	12.18%	12.47%	11.88%	12.95%	13.10%	12.12%
7000	13.37%	12.01%	12.11%	12.31%	12.09%	12.69%	13.11%	12.31%
8000	13.23%	11.96%	11.98%	12.45%	12.28%	12.91%	13.06%	12.15%
9000	13.20%	11.88%	12.06%	12.54%	12.28%	12.84%	12.93%	12.28%
10000	13.21%	11.94%	12.22%	12.50%	12.39%	12.60%	12.91%	12.24%

We note that each of the 8 polynomials occurs roughly $\frac{1}{8}$ of the time. This leads us to the following speculation.

Speculation 4.3. *Fix a square-free positive integer $d \equiv 23 \pmod{24}$. As m goes to infinity, the polynomial $\overline{\mathcal{R}}_{d,m}(x)$ equals each of the $2^{H(d)}$ polynomials in $\mathbb{F}_2[x]$ of degree smaller than $H(d)$ equally often.*

If Conjecture 4.2 is true (i.e. $\text{Tr}_m^*(d)$ is odd for some m), then Speculation 4.3 and (21) together imply, loosely speaking, that $\text{Tr}_m^*(d) \pmod{2}$ behaves randomly as m goes to infinity. In view of Theorem 1.3, the random distribution of the coefficients $a_{d,m,k}$ modulo 2 will shed light on the parity of the partition function. We leave this as an open question.

REFERENCES

- [1] Scott Ahlgren. Distribution of parity of the partition function in arithmetic progressions. *Indag. Math. (N.S.)*, 10(2):173–181, 1999.
- [2] Tetsuya Asai, Masanobu Kaneko, and Hirohito Ninomiya. Zeros of certain modular functions and an application. *Comment. Math. Univ. St. Paul.*, 46(1):93–101, 1997.
- [3] Kathrin Bringmann and Ken Ono. An arithmetic formula for the partition function. *Proc. Amer. Math. Soc.*, 135(11):3507–3514 (electronic), 2007.
- [4] Jan Hendrik Bruinier, Paul Jenkins, and Ken Ono. Hilbert class polynomials and traces of singular moduli. *Math. Ann.*, 334(2):373–393, 2006.
- [5] Jan Hendrik Bruinier and Ken Ono. Heegner divisors, L -functions and harmonic weak maass forms. *Ann. of Math.*, in press.

- [6] Chang Heon Kim. Borcherds products associated with certain Thompson series. *Compos. Math.*, 140(3):541–551, 2004.
- [7] J.-L. Nicolas, I. Z. Ruzsa, and A. Sárközy. On the parity of additive representation functions. *J. Number Theory*, 73(2):292–317, 1998. With an appendix in French by J.-P. Serre.
- [8] Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q -series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.
- [9] Ken Ono. Parity of the partition function. *Adv. Math.*, 225:349–366, 2010.
- [10] Thomas R. Parkin and Daniel Shanks. On the distribution of parity in the partition function. *Math. Comp.*, 21:466–480, 1967.
- [11] Don Zagier. Traces of singular moduli. In *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, volume 3 of *Int. Press Lect. Ser.*, pages 211–244. Int. Press, Somerville, MA, 2002.

P.O. BOX 14039, STANFORD, CA 94309-4039, USA

E-mail address: pakhinlee@stanford.edu

70 AMHERST STR., CAMBRIDGE, MA 02142, USA

E-mail address: alex.z@mit.edu