6-5-2002

The order at 2 of the odd-partition function

Chris Mehelich

The order at 2 of the odd-partition function

Chris Mihelich

Adviser: John Rickert

Mathematical Sciences Technical Report Series
MSTR 02-05

June 5, 2002

Department of Mathematics
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/math

Fax (812)-877-8333 **Phone (812)-877-8193**

The order at 2 of the odd-partition function

Chris Mihelich[1]
Harvard University
mihelich@fas.harvard.edu

June 5, 2002

Abstract. We evaluate the odd-partition function $p_2(n)$ modulo 4 by elementary methods and analyze the asymptotic distribution of $p_2(n)$ modulo 4. We use the theory of modular forms to obtain necessary and sufficient conditions for the order at 2 of $p_2(n)$ to equal any given value between 0 and 4 inclusive.

1 Introduction

A *partition* of an integer n is a nonincreasing sequence of positive integers that sum to n. The *unrestricted partition function* $p(n)$ is the number of partitions of n. The literature also defines a variety of *restricted* partition functions that count only partitions satisfying additional constraints, such as the *odd-partition function* $p_2(n)$, the number of partitions of n into odd parts. Identities involving partition functions have been studied systematically since Euler, who proved, for instance, that the number of partitions of n into odd parts equals the number of partitions into distinct parts. In 1919 Ramanujan initiated a new direction of research in partition theory by proving [16] the congruences

$$\begin{aligned} p(5n+4) &\equiv 0 \pmod 5, \\ p(7n+5) &\equiv 0 \pmod 7, \\ p(11n+6) &\equiv 0 \pmod{11} \end{aligned}$$

valid for all natural numbers n, thus inaugurating the arithmetical study of partition functions. For several decades progress in the field was slow, difficult, and limited. Results similar to Ramanujan's congruences were obtained by Atkin and others (see citations in [14]) for a few more primes, and Rødseth proved [17] an analogue of Ramanujan's modulo-5 congruence for p_2, namely

[1]The author is supported by NSF grant DMS-0097804.

that

$$p_2(125n + 26) \equiv 0 \pmod 5;$$

but the field suffered from a lack of really powerful tools.

More recently, however, advances in the theory of modular forms have provided the ammunition for a more powerful attack on the arithmetic of partition functions. For instance, Ono achieved in 2000 a magnificent generalization of Ramanujan's congruences by proving [14] that for every prime $p \geq 5$, there is an arithmetic progression throughout which $p(n)$ vanishes modulo p. Modern methods are also making clear that restricted partition functions such as $p_2(n)$ have arithmetic properties somewhat different from those of $p(n)$. In particular, a result of Gordon and Ono [5] shows that for each $j \geq 1$, the value of $p_2(n)$ is usually divisible by 2^j in the sense that

$$\frac{1}{L}\#\big\{0 \leq n \leq L : 2^j \mid p_2(n)\big\} = O\left(\frac{1}{\log^\alpha L}\right) \quad \text{for some positive constant } \alpha = \alpha(j).$$

In view of this striking result, it is natural to ask for explicit conditions on n ensuring that $2^j \mid p_2(n)$. Some theorems of this sort have been established already: in particular, Ono and Penniston [15] have evaluated exactly the residue of $p_2(n)$ modulo 8, and Rødseth's paper cited above proves [17, Corollary 2], for instance, that if $p \equiv 23 \pmod{24}$ is a prime whose exponent in $24n + 1$ is odd, then $2^{11} \mid p_2(n)$.

The main result of the present work is the derivation in §4 of necessary and sufficient conditions for the order of $p_2(n)$ at 2 to be exactly ℓ, where ℓ is a nonnegative integer not exceeding 4; these conditions are given in simple terms of the prime-power decomposition of $24n+1$. In §3 we give an exact calculation of the least residue modulo 4 of $p_2(n)$; although the result of [15] is stronger, our proof is interesting for its independence of the theory of modular forms. We also derive in §3 the asymptotic distribution of the residue modulo 4, proving (Theorem 6) that

$$\frac{1}{L}\#\big\{0 \leq n \leq L : p_2(n) \equiv r \pmod 4\big\} \sim \begin{cases} 1, & \text{if } r = 0; \\ \dfrac{\pi^2}{3\log L}, & \text{if } r = 2; \\ \dfrac{1}{3}\sqrt{\dfrac{6}{L}}, & \text{if } r = 1, 3, \end{cases}$$

as $L \to \infty$. In particular, this refines the $O(1/\log^\alpha L)$ of Gordon and Ono's theorem to a precise quantitative result.

2 Preliminaries

In this section we develop or review notation and background material needed in §3 and §4.

We shall perform a fair amount of arithmetic modulo 24, and one should keep in mind that

- the quadratic residues modulo 24 are $1, 4, 9, 12, 16$, and
- the multiplicative group $(\mathbb{Z}/24)^* = \{\pm 1, \pm 5, \pm 7, \pm 11\}$ is isomorphic to $(\mathbb{Z}/2)^3$, a triplet of generators being $5, 7, -1$.

We use the notation $\overline{n}$ for the least residue of n modulo 24.

If P is a logical proposition, we denote by $\big[P\big]$ the value 1 if P is true and 0 if P is false.

For prime p and integer n, the order of n at p will be denoted by $\operatorname{ord}_p n$. We shall also require the *truncated order functions* $\operatorname{ord}_p^{\le k}$, defined by the rule

$$\operatorname{ord}_p^{\le k} n = \min\big\{\operatorname{ord}_p n, k\big\};$$

this function is constructed to have the property that

$$a \equiv b \pmod{p^k} \quad \text{implies} \quad \operatorname{ord}_p^{\le k} a = \operatorname{ord}_p^{\le k} b.$$

We consider $\operatorname{ord}_p^{\le k}$ to take values in the additive semigroup with elements 0, 1, ..., k and addition operation $a, b \rightsquigarrow \min\{a+b, k\}$. This is a precise way of saying that the property

$$\operatorname{ord}_p^{\le k} ab = \operatorname{ord}_p^{\le k} a + \operatorname{ord}_p^{\le k} b \tag{1}$$

is true even when, for instance, we take $p = 2$, $k = 5$, and $a = b = 8$. In this case (1) states that $5 = 3 + 3$, which is true in the semigroup we have defined. We shall write the semigroup element k as k^+ to remind ourselves of the imprecision inherent in the measurement we are taking.

We recall that the generating functions $P(q)$ and $P_2(q)$ of $p(n)$ and $p_2(n)$, respectively, admit the infinite-product representations

$$\begin{aligned} P(q) &= \prod_{n\ge 1} \frac{1}{1-q^n}, \\ P_2(q) &= \prod_{n\ge 1} \frac{1-q^{2n}}{1-q^n}. \end{aligned}$$

2.1 Jacobi's triple product and applications

Jacobi obtained the striking and famous identity

$$\prod_{n\ge 1} \big(1-q^{2n}\big)\big(1+zq^{2n-1}\big)\big(1+z^{-1}q^{2n-1}\big) = \sum_n z^n q^{n^2} \qquad (z \ne 0, |q| < 1), \tag{2}$$

commonly called his *triple-product identity*, in developing his theory of elliptic functions [9]. We review here several special cases of the triple-product identity that figure significantly in the later development. We use the notations

$$n \;= \tfrac{1}{2}n(n+1), \qquad n \;= \tfrac{1}{2}n(3n-1)$$

for the n^{th} triangular and pentagonal numbers respectively.

Lemma 1 *Let* $|q| < 1$.

1. (Euler's pentagonal-number series.) *We have*

$$\frac{1}{P(q)} = \prod_{n\geq 1}\bigl(1-q^n\bigr) = \sum_n (-1)^n q^n \ .$$

2. (Jacobi's triangular-number series.) *We have*

$$\frac{1}{P(q)^3} = \prod_{n\geq 1}\bigl(1-q^n\bigr)^3 = \sum_{n\geq 0}(-1)^n(2n+1)q^n \ .$$

3. (A θ-function series.) *We have*

$$\prod_{n\geq 1}\frac{\bigl(1-q^n\bigr)^2}{1-q^{2n}} = \prod_{n\geq 1}\bigl(1-q^{2n}\bigr)\bigl(1-q^{2n-1}\bigr)^2 = 1+2\sum_{n\geq 1}(-1)^n q^{n^2}.$$

Proof of Lemma 1. In (2) make the replacements $q \leftarrow q^{1/2}$ and $z \leftarrow -q^{-1/2}$. Then we obtain

$$\sum_n (-1)^n q^n \ = \prod_{n\geq 1}\bigl(1-q^{3n}\bigr)\bigl(1-q^{3n-2}\bigr)\bigl(1-q^{3n-1}\bigr) = \prod_{n\geq 1}\bigl(1-q^n\bigr),$$

which is Euler's theorem.

For Jacobi's theorem we make the substitutions $q \leftarrow q^{1/2}$ and $z \leftarrow -q^{1/2}t$, where $t \neq 0, 1$ will be allowed to approach 1 at the end of the argument. We obtain the identity

$$\prod_{n\geq 1}\bigl(1-q^n\bigr)\bigl(1-q^n t\bigr)\bigl(1-q^{n-1}t^{-1}\bigr) = \sum_n (-1)^n t^n q^n \ ,$$

or, on multiplying by $1-t$ and using the fact that $\bigl(-(n+1)\bigr) \ = n$, that

$$\prod_{n\geq 1}\bigl(1-q^n\bigr)\bigl(1-q^n t\bigr)\bigl(1-q^n t^{-1}\bigr) = \sum_n (-1)^n \frac{t^n - t^{-(n+1)}}{1-t} q^n \ . \qquad (3)$$

As $t \to 1$ the left side approaches $\prod_{n\geq 1}\bigl(1-q^n\bigr)^3$, while the fraction on the right side approaches $2n+1$, yielding Jacobi's theorem.

Finally, for the θ-function series, we note first that

$$\prod_{n\geq 1}\bigl(1-q^{2n}\bigr)\bigl(1-q^{2n-1}\bigr)^2 = \frac{\prod_{n\geq 1}\bigl(\bigl(1-q^{2n}\bigr)\bigl(1-q^{2n-1}\bigr)\bigr)^2}{\prod_{n\geq 1}\bigl(1-q^{2n}\bigr)} = \prod_{n\geq 1}\frac{\bigl(1-q^n\bigr)^2}{1-q^{2n}},$$

so that the two infinite products given in the statement of Lemma 1 are equal. Applying Jacobi's triple-product theorem with $z=-1$ yields

$$\prod_{n\geq 1}\bigl(1-q^{2n}\bigr)\bigl(1-q^{2n-1}\bigr)^2 = \sum_n (-1)^n q^{n^2} \ = 1+2\sum_{n\geq 1}(-1)^n q^{n^2},$$

as desired. □

2.2 Modular forms

We assume knowledge of the essentials of the theory of modular forms as in, for instance, the texts of Apostol [2], Knopp [10], and Koblitz [11]. We shall consistently use the letter τ for the variable with values in the upper half-plane and $q = e^{2\pi i\tau}$ for the associated variable in the unit disc. We recall the definition of Dedekind's η-function

$$\eta(\tau) = e^{\pi i\tau/12} \prod_{n\geq 1} \bigl(1 - q^n\bigr),$$

in terms of which the generating functions P and P_2 are given by the equations

$$\begin{aligned} P(q^{24}) &= \frac{q}{\eta(24\tau)}; \\ P_2(q^{24}) &= \frac{\eta(48\tau)}{q\eta(24\tau)}. \end{aligned}$$

We denote by $M_k(\Gamma, \chi)$ the space of holomorphic modular forms on the subgroup Γ with character χ. The only nontrivial character we shall use is the character χ_2 given by the rule

$$\chi_2(n) = \begin{cases} (-1)^{(n^2-1)/8}, & \text{if } n \text{ is odd;} \\ 0 & \text{otherwise.} \end{cases}$$

We recall the Hecke operators $T(p)$ on $M_k(\Gamma, \chi)$ for prime p, defined on power series by the rule

$$\sum_n a(n)q^n \mid T(p) = \sum_n \bigl(a(pn) + \chi(p)p^{k-1}a(n/p)\bigr)q^n.$$

Here and later we use the standard convention that for any function f whose domain is the integers (for example, the general coefficient in the power series of a holomorphic form), an expression $f(x)$ with x nonintegral denotes zero.

2.3 Representation by binary quadratic forms

In deriving our principal results, we shall have repeated occasion to count representations of an integer n in the form $x^2 + dy^2$ for a fixed positive integer d and variable integers x, y. We denote this count by

$$r_{1,d}(n) := \#\{(x, y) \in \mathbb{Z}^2 : n = x^2 + dy^2\}.$$

For instance $r_{1,1}(5) = 8$ because $5 = (\pm 1)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 1)^2$ for any choices of the signs. For suitable d, including those which concern us here, the evaluation of $r_{1,d}(n)$ is a matter of elementary algebraic number theory. The reader unfamiliar with the rudiments of the arithmetic of imaginary quadratic fields will find [8] a suitable introduction; alternatively, he may take on faith the three theorems asserted below and proceed to §2.2.

The values of d of interest to us are 1, 3, and 6, for which $r_{1,d}$ is evaluable in the following terms.

Lemma 2 *If* $\operatorname{ord}_p n$ *is odd for any prime* $p \equiv 3 \pmod 4$*, then* $r_{1,1}(n) = 0$*. Otherwise*

$$r_{1,1}(n) = \prod_{p \equiv 1(4)} \big(\operatorname{ord}_p n + 1\big).$$

Lemma 3 *If* $\operatorname{ord}_p n$ *is odd for any prime* $p \equiv 2 \pmod 3$*, then* $r_{1,3}(n) = 0$*. Otherwise*

$$r_{1,3}(n) = \left\{ \begin{matrix} 6, & \text{if } 2 \mid n; \\ 2, & \text{if } 2 \mid n \end{matrix} \right\} \prod_{p \equiv 1(3)} \big(\operatorname{ord}_p n + 1\big).$$

Lemma 4 *If* $\operatorname{ord}_p n$ *is odd for any prime* $p \equiv -1, -5, -7, -11 \pmod{24}$*, or*

$$\operatorname{ord}_2 n + \operatorname{ord}_3 n + \sum_{p \equiv 5,11(24)} \operatorname{ord}_p n \qquad \text{is odd,}$$

then $r_{1,6}(n) = 0$*. Otherwise*

$$r_{1,6}(n) = 2 \prod_{p \equiv 1,5,7,11(24)} \big(\operatorname{ord}_p n + 1\big).$$

We prove these in the given order. The result and proof for $d = 1$ are well known, but we give the proof in some detail because the proofs for the two lesser-known theorems follow its outline.

Proof of Lemma 2. We use freely the arithmetic of the Gaussian-rational field $\mathbb{Q}(i)$, whose integer ring $\mathfrak{o} = \mathbb{Z}[i]$ has discriminant -4, class number 1, and four roots of unity, namely $\pm 1, \pm i$.

The equation $n = x^2 + y^2$ is equivalent to the equation

$$(n) = (x + iy)\overline{(x + iy)}$$

of ideals in $\mathfrak{o}$. Conversely, any ideal $\mathfrak{a}$ with $(n) = \mathfrak{a}\overline{\mathfrak{a}}$ corresponds to four representations $n = x^2 + y^2$ because a generator $x + iy$ of $\mathfrak{a}$ has four associates. Thus

$$r_{1,1}(n) = 4\#\big\{\mathfrak{a} : (n) = \mathfrak{a}\overline{\mathfrak{a}}\big\},$$

and we are now counting ideals $\mathfrak{a}$ instead of representations x^2+y^2. Our strategy for counting these will be to decompose (n) into a product of prime ideals and to count the number of ways to partition the prime-ideal factors into two sets such that the products of the sets are conjugate ideals. The decomposition of (n) in $\mathfrak{o}$ may be obtained readily from the factorization of n in $\mathbb{Z}$ once we have analyzed the splitting and ramification of rational primes in $\mathfrak{o}$, which we now do.

In the first place $(2) = \mathfrak{r}_2^2$ with $\mathfrak{r}_2 = (1 + i)$, and no other rational prime ramifies because the discriminant -4 of $\mathbb{Z}[i]$ has no prime factor but 2. Every prime $p > 2$ splits as $\mathfrak{s}_p\overline{\mathfrak{s}_p}$ or remains prime. Now (p) is prime if and only if $\mathfrak{o}/(p)$ is a field; because $\mathfrak{o} \cong \mathbb{Z}[x]/(x^2 + 1)$, this means exactly that $x^2 + 1 \equiv 0$

(mod p) has a solution. But $(-1/p) = 1$ if and only if $p \equiv 1 \pmod 4$. Therefore any $p \equiv 1 \pmod 4$ splits as $\mathfrak{s}_p\overline{\mathfrak{s}_p}$, while any $p \equiv 3 \pmod 4$ remains prime in $\mathfrak{o}$.

Now let

$$n = 2^a \prod_{p\equiv 3(4)} p^{b_p} \prod_{q\equiv 1(4)} q^{c_p},$$

so that

$$(n) = \mathfrak{r}_2^{2a} \prod_{p\equiv 3(4)} p^{b_p} \prod_{q\equiv 1(4)} \mathfrak{s}_q^{c_q}\overline{\mathfrak{s}_q}^{c_q}.$$

Suppose that $(n) = \mathfrak{a}\overline{\mathfrak{a}}$, where

$$\mathfrak{a} = \mathfrak{r}_2^{\alpha} \prod_{p\equiv 3(4)} p^{\beta_p} \prod_{q\equiv 1(4)} \mathfrak{s}_q^{\gamma_q}\overline{\mathfrak{s}_q}^{\gamma'_q}.$$

Clearly $\operatorname{ord}_{\mathfrak{r}_2} \mathfrak{a} = \operatorname{ord}_{\mathfrak{r}_2} \overline{\mathfrak{a}}$ and $\operatorname{ord}_p \mathfrak{a} = \operatorname{ord}_p \overline{\mathfrak{a}}$ for $p \equiv 3 \pmod 4$, whence we must have

$$\alpha = a \qquad \text{and} \qquad \beta_p = b_p/2;$$

in particular, there is no such $\mathfrak{a}$ if $2 \mid b_p$ for any $p \equiv 3 \pmod 4$, and then $r_{1,1}(n) = 0$. In the remaining case, the number of $\mathfrak{a}$ is the number of choices of the γ and γ'. Now $\operatorname{ord}_{\mathfrak{s}_q} \mathfrak{a} = \operatorname{ord}_{\overline{\mathfrak{s}}_q} \overline{\mathfrak{a}}$ and $\operatorname{ord}_{\mathfrak{s}_q} \mathfrak{a} + \operatorname{ord}_{\mathfrak{s}_q} \overline{\mathfrak{a}} = c_q$; the complete set of constraints, then, on the γ and γ' is that

$$0 \le \gamma_q \le \operatorname{ord}_q n \qquad \text{and} \qquad \gamma'_q = c_q - \gamma_q.$$

This gives $\prod(c_q + 1)$ choices of $\mathfrak{a}$. Thus

$$r_{1,1}(n) = 4\prod_q \big(c_q + 1\big) = 4 \prod_{q\equiv 1(4)} \big(\operatorname{ord}_q n + 1\big),$$

as claimed. □

Proof of Lemma 3. Here we use the field $\mathbb{Q}\big(\sqrt{-3}\big)$ of discriminant -3, class number 1, and integer ring $\mathfrak{o} = \mathbb{Z}[\omega]$, where $\omega = \big(1 + \sqrt{-3}\big)/2$. There are six roots of unity, namely ω^i for $0 \le i < 6$. The new complication is that $\mathfrak{o} \ne \mathbb{Z}\big[\sqrt{-3}\big]$, which will shortly be seen to account for the equivocation between 6 and 2 in Lemma 3.

The equation $n = x^2 + 3y^2$ asserts exactly that

$$(n) = \big(x + y\sqrt{-3}\big)\overline{\big(x + y\sqrt{-3}\big)},$$

but a decomposition $(n) = \mathfrak{a}\overline{\mathfrak{a}}$ does not necessarily induce six representations of n because $\mathfrak{a}$ might be generable by an integer not in $\mathbb{Z}\big[\sqrt{-3}\big]$. Fortunately at least one of the six generators of $\mathfrak{a}$ is in $\mathbb{Z}\big[\sqrt{-3}\big]$. For any generator α of $\mathfrak{a}$ not in $\mathbb{Z}\big[\sqrt{-3}\big]$ is of the form $\big(x + y\sqrt{-3}\big)/2$ with $x \equiv y \equiv 1 \pmod 2$, and we have

$$\frac{x + y\sqrt{-3}}{2}\frac{1 \pm \sqrt{-3}}{2} = \frac{(x \mp 3y) + (y \pm x)\sqrt{-3}}{4} \equiv \frac{y \pm x}{4}\big(\pm 1 + \sqrt{-3}\big) \pmod{\mathbb{Z}\big[\sqrt{-3}\big]};$$

for one choice of the sign we have $4 \mid y \pm x$, whence one of $\alpha\omega$ and $\alpha\omega^{-1}$ is in $\mathbb{Z}\big[\sqrt{-3}\big]$.

Thus every representation $n = x^2+3y^2$ is induced by a factorization $(n) = \mathfrak{a}\overline{\mathfrak{a}}$ after all; the question is now how many representations proceed from each choice of $\mathfrak{a}$. Let $\mathfrak{a} = (\alpha)$ with $\alpha = x + y\sqrt{-3}$ for $x, y \in \mathbb{Z}$, and note that

$$\alpha\omega^{\pm 1} = \frac{(x \mp 3y) + (y \pm x)\sqrt{-3}}{2}$$

is in $\mathbb{Z}\big[\sqrt{-3}\big]$ if and only if $x + y$ is even. Now because

$$x + y \equiv x^2 + 3y^2 = n \pmod 2,$$

we see that all six associates of α induce representations of n if n is even, while only the two associates $\pm\alpha$ are admissible when n is odd. This accounts for the variable factor of 6 or 2 in the result.

The remainder of the proof proceeds by analogy with Lemma 2. The ideal $(3) = \mathfrak{r}_3^2$, where $\mathfrak{r}_3 = \big(\sqrt{-3}\big)$, is the only ramified prime. Because $\mathfrak{o} \cong \mathbb{Z}[x]/(x^2+x+1)$, a prime $p \neq 3$ splits if and only if $x^2+x+1 \equiv 0 \pmod p$, or $(2x+1)^2 \equiv -3 \pmod p$, is soluble. But $1 = (-3/p) = (p/3)$ exactly when $p \equiv 1 \pmod 3$.

Repeating arguments from Lemma 2, we find that $r_{1,3}(n) = 0$ unless $\operatorname{ord}_p n$ is even for each $p \equiv 2 \pmod 3$, in which case

$$r_{1,3}(n) = \left\{ \begin{matrix} 6, & \text{if } 2 \mid n; \\ 2, & \text{if } 2 \mid n \end{matrix} \right\} \prod_{p \equiv 1 (3)} \big(\operatorname{ord}_p n + 1\big),$$

as claimed. □

Proof of Lemma 4. The operative field is now $\mathbb{Q}\big(\sqrt{-6}\big)$. The integer ring $\mathfrak{o}$ is once more $\mathbb{Z}\big[\sqrt{-d}\big]$, but now unique factorization fails, the class number of $\mathbb{Z}\big[\sqrt{-6}\big]$ being 2. The discriminant is -24 and there are no roots of unity but ± 1. This time representations $n = x^2 + 6y^2$ correspond to factorizations $(n) = \mathfrak{a}\overline{\mathfrak{a}}$ *with* $\mathfrak{a}$ *principal*, which has become a nontrivial condition. We first analyze the behavior of rational primes in $\mathfrak{o}$, then count the number of admissible factorizations of (n).

The ramified primes are $(2) = \mathfrak{r}_2^2$ and $(3) = \mathfrak{r}_3^2$, where $\mathfrak{r}_2 = (2, \sqrt{-6})$ and $\mathfrak{r}_3 = (3, \sqrt{-6})$ are nonprincipal. The condition for $p > 3$ to remain prime is that

$$-1 = \left(\frac{-6}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{2}{p}\right),$$

which means that $p \equiv 13, 17, 19, 23 \pmod{24}$. The other primes split, but we now need to know whether they split into a product of principal ideals $\mathfrak{s}\overline{\mathfrak{s}}$ or of nonprincipal ideals $\mathfrak{n}\overline{\mathfrak{n}}$. The answer is that $p \equiv 1, 7 \pmod{24}$ is necessary and sufficient for the factors to be principal; we prove this now by induction on p. During the proof we let χ be the function

$$\chi(l) = \left\{ \begin{matrix} 1, & \text{if } l \equiv 1 \pmod 6; \\ 0, & \text{if } l \equiv 5 \pmod 6 \end{matrix} \right.$$

on integers relatively prime to 6 with values in $\mathbb{Z}/2$. We identify the ideal class group with $\mathbb{Z}/2$ and let $\widetilde{\mathfrak{a}}$ denote the class of the ideal $\mathfrak{a}$ in $\mathbb{Z}/2$.

Fix a prime $p \equiv 1, 5, 7, 11 \pmod{24}$ and assume the claim proven for all smaller such p. The induction assumption easily implies the following statement, which will be more useful:

> Let m be a number such that $(6, m) = 1$, all prime factors of m are strictly less than p, and $\operatorname{ord}_q m$ is even for all primes $q \equiv 13, 17, 19, 23 \pmod{24}$. If $m = \mu\overline{\mu}$, then $\widetilde{\mu} = \chi(m)$.

A decomposition $m = \mu\overline{\mu}$ always exists because the prime factors of m all split. Writing similarly $p = \pi\overline{\pi}$, we are to prove that $\widetilde{\pi} = \chi(p)$.

Let $|x| < p/2$ and $x^2 + 6 \equiv 0 \pmod{p}$; then $x^2 + 6 = p2^a3^bm$, where $0 < m < p$. Moreover a and b can take no values other than 0 and 1. We can write $m = \mu\overline{\mu}$ in such a way that

$$\left(x + y\sqrt{-6}\right) = \pi\mathfrak{r}_2^a\mathfrak{r}_3^b\mu,$$

whence

$$0 = \widetilde{\pi} + a + b + \widetilde{\mu}. \tag{4}$$

We distinguish four cases.

1. Suppose $a = b = 0$. Then $(6, x) = 1$, whence $x^2 + 6 \equiv 7 \pmod{24}$ and $0 = \chi(7) = \chi(pm) = \chi(p) + \chi(m)$, or $\chi(p) = \chi(m)$. By (4) we have $\widetilde{\pi} = \widetilde{\mu} = \chi(m) = \chi(p)$, as desired.

2. Suppose $a = 1$ and $b = 0$. Then $x = 2y$ with $3 \mid y$, whence $pm = 2y^2 + 3 \equiv 5 \pmod{6}$ and $\chi(p) + \chi(m) = 1$. By (4) we have $\widetilde{\pi} + 1 + \widetilde{\mu} = 0$, whence $\widetilde{\pi} = \chi(m) + 1 = \chi(p)$.

3. Suppose $a = 0$ and $b = 1$. Then $x = 3y$ with $2 \mid y$, whence $pm = 3y^2 + 2 \equiv 5 \pmod{6}$, and the argument is completed as in case 2.

4. Suppose finally that $a = b = 1$, so that $x = 6y$ and $pm = 6y^2 + 1 \equiv 1 \pmod{6}$. Then $\chi(m) + \chi(p) = 0$ and $\widetilde{\pi} + 2 + \widetilde{\mu} = 0$, whence $\widetilde{\pi} = \chi(p)$.

We have now completely analyzed the splitting of primes. Resuming the approach of Lemma 2, we factor n as

$$n = 2^a3^b \prod_{p \equiv 13,17,19,23 (24)} p^{c_p} \prod_{q \equiv 1,7 (24)} q^{d_q} \prod_{r \equiv 5,11 (24)} r^{e_r}$$

and find that

$$(n) = \mathfrak{r}_2^{2a}\mathfrak{r}_3^{2b} \prod_{p \equiv 13,17,19,23 (24)} p^{c_p} \prod_{q \equiv 1,7 (24)} \mathfrak{s}_q^{d_q}\overline{\mathfrak{s}_q}^{d_q} \prod_{r \equiv 5,11 (24)} \mathfrak{n}_r^{e_r}\overline{\mathfrak{n}_r}^{e_r},$$

where the $\mathfrak{s}_q$ are principal, while the $\mathfrak{r}_i$ and $\mathfrak{n}_r$ are not. We wish to count principal ideals

$$\mathfrak{a} = \mathfrak{r}_2^\alpha\mathfrak{r}_3^\beta \prod_p p^{\gamma_p} \prod_q \mathfrak{s}_q^{\delta_q}\overline{\mathfrak{s}_q}^{\delta'_q} \prod_r \mathfrak{n}_r^{\epsilon_r}\overline{\mathfrak{n}_r}^{\epsilon'_r}$$

such that $(n) = \mathfrak{a}\overline{\mathfrak{a}}$. We find easily that

$$\alpha = a, \quad \beta = b, \quad \gamma_p = c_p/2, \quad \delta'_q = d_q - \delta_q, \quad \epsilon'_r = e_r - \epsilon_r.$$

In particular there is no such $\mathfrak{a}$ unless $\operatorname{ord}_p n$ is even for all $p \equiv 13, 17, 19, 23 \pmod{24}$. Moreover $\mathfrak{a}$ is principal if and only if

$$\alpha + \beta + \sum_r e_r = \operatorname{ord}_2 n + \operatorname{ord}_3 n + \sum_{r \equiv 5,11 (24)} \operatorname{ord}_r n \qquad \text{is even,} \tag{5}$$

whence $r_{1,6}(n) = 0$ if the sum in (5) is odd. In the remaining case there are

$$\prod_q (d_q + 1) \prod_r (e_r + 1) = \prod_{t \equiv 1,5,7,11 (24)} \big(\operatorname{ord}_t n + 1\big)$$

choices of $\mathfrak{a}$. Because there are only the two roots of unity ± 1, the claim of Lemma 4 follows at once. $\square$

3 Elementary determination of p_2 modulo 4

The residue of $p_2(n)$ modulo 8 has been evaluated by Ono and Penniston [15] by methods of the theory of modular forms. In this section we give a more elementary evaluation of $p_2(n)$ modulo 4 and use this to obtain a quantitative refinement of the abstract result that $p_2(n)$ is usually divisible by 4, as well as an equidistribution result for the odd values of $p_2(n)$.

3.1 Formula for the residue

We begin with a recurrence for p_2 obtained by Ewell [4]. Namely, equating coefficients on the extremes of the identity

$$\Big(1 + 2\sum_{n \geq 1} (-1)^n q^n\Big) P_2(q) = \prod_{n \geq 1} \frac{\big(1 - q^n\big)^2}{1 - q^{2n}} \prod_{n \geq 1} \frac{1 - q^{2n}}{1 - q^n} = \prod_{n \geq 1} \big(1 - q^n\big) = \sum_n (-1)^n q^n$$

yields the recurrence

$$p_2(n) = \big\{(-1)^a\big\}_{n=a} + 2\sum_{k \geq 1} (-1)^{k+1} p_2(n - k^2), \tag{6}$$

where $\big\{(-1)^a\big\}_{l\ =a} = (-1)^l$ and $\big\{(-1)^a\big\}_{n=a} = 0$ if n is not pentagonal. It is evident from Ewell's recurrence that $p_2(n)$ is odd if and only if n is pentagonal. Applying this observation to the terms $p_2(n - k^2)$ in (6), we find that

$$p_2(n) \equiv \big\{(-1)^a\big\}_{n=a} + 2\#\{k \geq 1 : n - k^2 = \ \ \} \pmod 4. \tag{7}$$

Thus we need only count representations $n = k^2 + l$ with $k \geq 1$.

Now $n = k^2 + l$ means precisely that $24n+1 = (6l-1)^2 + 6(2k)^2$, suggesting a connection between $r_{1,6}(24n+1)$ and the cardinality in (7). In fact we prove that

$$\#\{k \geq 1 : n - k^2 = \quad\} = \begin{cases} \frac{1}{4} r_{1,6}(24n+1), & \text{if } n \neq \quad ; \\ \frac{1}{4}\big(r_{1,6}(24n+1) - 2\big), & \text{if } n = \quad . \end{cases} \tag{8}$$

Assume first that n is not pentagonal (equivalently, that $24n+1$ is not square), and consider an arbitrary representation

$$24n + 1 = \lambda^2 + 6\kappa^2.$$

By considering this equation modulo 24 and performing a finite verification, we see that necessarily $2 \mid \kappa$ and $\lambda \equiv \pm 1 \pmod 6$; moreover, we have $\kappa \neq 0$ because $24n+1$ is not square. Thus exactly one of $\pm\kappa$ is of the form $2k$ for $k \geq 1$, and exactly one of $\pm\lambda$ is congruent to -1 modulo 6. We have shown that the set appearing in (8) contains exactly one out of every four representations $(\pm\kappa, \pm\lambda)$, and (8) follows when n is not pentagonal. When $n = l$ is pentagonal the only difference is that the two trivial representations $24n + 1 = \big(\pm(6l-1)\big)^2 + 0^2$ must be counted out, as is done in (8).

We can now apply Lemma 4 to evaluate the residue of $p_2(n)$ modulo 4. We put $N := 24n+1$ for brevity and assume first that n is not pentagonal (N is not square); then $4 \mid p_2(n)$ unless $\frac{1}{4} r_{1,6}(N)$ is odd, in which case $p_2(n) \equiv 2 \pmod 4$. From Lemma 4 we know that $r_{1,6}(N) = 0$ unless $\operatorname{ord}_p N$ is even for all primes $p \equiv -1, -5, -7, -11 \pmod{24}$. If N does have even order at all such p, then also

$$2 \mid \sum_{p \equiv 5, 11 (24)} \operatorname{ord}_p N,$$

for N represents the identity class $\overline{1}$ of $(\mathbb{Z}/24)^*$, and its powers of $\overline{5}$ and $\overline{11}$ must be canceled in $(\mathbb{Z}/24)^*$ by a power of $\overline{7} = \overline{5} \cdot \overline{11}$. Thus the formula

$$r_{1,6}(N) = 2 \prod_{p \equiv 1,5,7,11 (24)} \big(\operatorname{ord}_p N + 1\big)$$

of Lemma 4 is applicable, and we see from (7) and (8) that

$$p_2(n) \equiv \prod_{p \equiv 1,5,7,11 (24)} \big(\operatorname{ord}_p N + 1\big) \pmod 4.$$

Now $\operatorname{ord}_p N$ is odd for at least one $p \equiv 1, 5, 7, 11 \pmod{24}$, for N has even order at all other primes but is not square. If $\operatorname{ord}_p N$ is odd for at least two p, or $\operatorname{ord}_p N \equiv 3 \pmod 4$ for some p, then $4 \mid p_2(n)$. In the remaining case we have $N = p^{4m+1} a^2$ for some $m \geq 0$, some prime $p \equiv 1 \pmod{24}$, and some a indivisible by p. Thus we have proven the second and third clauses of

Theorem 5 *Given n, let $N = 24n + 1$. Then*

- *if* $N = (6l-1)^2$ (i.e., if $n = l$), *then*

$$p_2(n) \equiv (-1)^{l+r} \pmod 4, \quad \text{where } r = \sum_{p \equiv 1,5,7,11 (24)} \operatorname{ord}_p(6l-1);$$

- *if* $N = p_1^{4m+1} a^2$ *with* $p_1 \mid a$, *then* $p_2(n) \equiv 2 \pmod 4$;
- *otherwise* $p_2(n) \equiv 0 \pmod 4$.

For the remaining clause, let $n = l$, and compute from (7) and (8) that

$$\begin{aligned} p_2(n) &\equiv (-1)^l - 1 + \prod_{p \equiv 1,5,7,11 (24)} \big(\operatorname{ord}_p N + 1\big) \\ &= (-1)^l - 1 + \prod_{p \equiv 1,5,7,11 (24)} \big(2 \operatorname{ord}_p(6l-1) + 1\big) \\ &\equiv (-1)^l - 1 + (-1)^r, \quad \text{where } r = \sum_{p \equiv 1,5,7,11 (24)} \operatorname{ord}_p(6l-1) \\ &\equiv (-1)^{l+r} \pmod 4. \end{aligned}$$

3.2 Asymptotic distribution of the residue

From the results of [5] mentioned above, we know that

$$\frac{1}{L} \#\big\{0 \le n \le L : 4 \mid p_2(n)\big\} = O\left(\frac{1}{\log^\alpha L}\right)$$

for some $\alpha > 0$. We can now use Theorem 5 to refine this qualitative result.

Theorem 6 *As* $L \to \infty$ *we have*

$$\frac{1}{L} \#\big\{0 \le n \le L : p_2(n) \equiv r \pmod 4\big\} \sim \begin{cases} 1, & \text{if } r = 0; \\ \dfrac{\pi^2}{3 \log L}, & \text{if } r = 2; \\ \dfrac{1}{3}\sqrt{\dfrac{6}{L}}, & \text{if } r = 1, 3. \end{cases}$$

Proof. The statement about $r = 0$ is a trivial consequence of the statements for $r = 1, 2, 3$. We consider first $r = 2$, for which, by Theorem 5, we are to prove that

$$\sum_{n \le L} \big[24n + 1 = p^{4m+1} a^2, (a, p) = 1\big] \sim \frac{\pi^2 L}{3 \log L}. \tag{9}$$

First we prove that the simpler sum

$$\sum_{n \le L} \big[24n + 1 = p a^2\big] \tag{10}$$

differs negligibly from the sum in (9). Indeed, the difference between the sums (10) and (9) is precisely

$$\begin{aligned}\sum_{n\le L}\big[24n+1=p^{4m+3}a^2,(a,p)=1\big] &\le \sum_{n\le L}\big[24n+1=p^3a^2\big]\\ &= \sum_{p\equiv 1(24)}\ \sum_{1\le a\le\sqrt{(24L+1)/p^3}}\big[a\equiv\pm1\ (\mathrm{mod}\ 6)\big]\\ &\le 5\sqrt{L}\sum_{p\equiv 1(24)}p^{-3/2}\\ &= O\big(\sqrt{L}\big).\end{aligned}$$

We now recall Dirichlet's theorem on primes in arithmetic progressions, namely, that

$$\#\{p\le x: p\equiv r\ (\mathrm{mod}\ m)\}\sim\frac{1}{\phi(m)}\frac{x}{\log x}\quad\text{if } (r,m)=1,$$

where ϕ denotes Euler's totient function. In particular, for $(24,r)=1$ we have

$$\#\{p\le x: p\equiv r\ (\mathrm{mod}\ m)\}\sim\frac{1}{8}\frac{x}{\log x}.$$

Using Dirichlet's theorem we now deduce that

$$\begin{aligned}\sum_{n\le L}\big[24n+1=pa^2\big] &= \sum_{\substack{a\ge1\\ a\equiv\pm1(6)}}\#\{p\le(24L+1)/a^2: p\equiv1\ (\mathrm{mod}\ 24)\}\\ &= \sum_{\substack{1\le a\le5\sqrt{L}\\ a\equiv\pm1(6)}}\frac{1}{8}\frac{(24L+1)/a^2}{\log\big((24L+1)/a^2\big)}+o\left(\frac{L}{\log L}\right)+O\big(\sqrt{L}\big)\\ &= \frac{3L}{\log L}\sum_{\substack{a\ge1\\ a\equiv\pm1(6)}}\frac{1}{a^2}\left(1+O\left(\frac{\log a}{\log L}\right)\right)+o\left(\frac{L}{\log L}\right)\\ &\sim \frac{3L}{\log L}\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\sum_{a\ge1}\frac{1}{a^2}\\ &= \frac{\pi^2L}{3\log L},\end{aligned}$$

the result desired.

Now it is trivial that

$$\#\{n\le L: p_2(n)\equiv1\ (\mathrm{mod}\ 2)\}=\#\{l: l\ \ \le L\}\sim\frac{2}{3}\sqrt{6L},$$

so the assertion of Theorem 6 about $r=1,3$ is equivalent to the statement that

$$\#\{n\le L: p_2(n)\equiv1\ (\mathrm{mod}\ 4)\}-\#\{n\le L: p_2(n)\equiv3\ (\mathrm{mod}\ 4)\}=o\big(\sqrt{L}\big).\quad(11)$$

If we introduce the temporary notation

$$\chi(l) = \begin{cases} 1, & \text{if } p_2\big(l\ \big) \equiv 1 \pmod 4; \\ -1, & \text{if } p_2\big(l\ \big) \equiv 3 \pmod 4, \end{cases}$$

then (11) can be stated in the form

$$\sum_{l\ \le L} \chi(l) = o\big(\sqrt{L}\big). \tag{12}$$

We shall prove (12) in §3.3. □

3.3 Proof of the equidistribution of odd values

In this section we require several of the special functions of elementary number theory: the *von Mangoldt function*

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^a; \\ 0 & \text{otherwise;} \end{cases}$$

the ω-function

$$\omega(n) = \sum_p \operatorname{ord}_p n$$

that counts the prime factors of n with multiplicities, and the *Möbius function*

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{if } n \text{ is squarefree;} \\ 0 & \text{otherwise.} \end{cases}$$

We define a variant ω_S of ω, where S is a collection of residue classes modulo 24, by the rule

$$\omega_S(n) = \sum_{p \equiv S(24)} \operatorname{ord}_p n.$$

In terms of this function, we can write χ as

$$\chi(l) = (-1)^{l + \omega_{1,5,7,11}(6l-1)}. \tag{13}$$

We recall the important properties [7]

$$\begin{aligned} \sum_{d|n} \mu(d) &= \big[n = 1\big], \\ \sum_{d|n} \mu\left(\frac{n}{d}\right) \Lambda(d) &= -\mu(n) \log n, \end{aligned}$$

both valid for positive integers n.

We show first that (12) follows from the result that

$$\sum_{0 \le k < N} (-1)^{\omega(24k+r)} = o(N) \quad \text{if } (r, 24) = 1, \tag{14}$$

whose proof we defer. We note that

$$\omega(n) = \omega_{1,5,7,11}(n) + \omega_{13,17,19,23}(n) \quad \text{for } (24,n)=1$$

and that

$$\omega_{13,17,19,23}(n) \equiv \big[n \equiv 13,17,19,23 \pmod{24}\big] \pmod 2 \quad \text{for } n>0,$$

for $\{13,17,19,23\}$ is the nontrivial coset in $(\mathbb{Z}/24)^*$ of the subgroup $\{1,5,7,11\}$. Consequently (13) may be put in the form

$$\begin{aligned}
\chi(l) &= (-1)^l \left\{ \begin{matrix} +1, & \text{if } |6l-1| \equiv 13,17,19,23 \pmod{24}; \\ -1, & \text{if } |6l-1| \equiv 1,5,7,11 \pmod{24} \end{matrix} \right\} (-1)^{\omega(|6l-1|)} \\
&= \left\{ \begin{matrix} +1, & \text{if } 2 \mid l; \\ -1, & \text{if } 2 \mid l \end{matrix} \right\} \left\{ \begin{matrix} +1, & \text{if } l \equiv 1,2 \pmod 4; \\ -1, & \text{if } l \equiv 0,3 \pmod 4 \end{matrix} \right\} \left\{ \begin{matrix} +1, & \text{if } l>0; \\ -1, & \text{if } l \le 0 \end{matrix} \right\} (-1)^{\omega(|6l-1|)} \\
&= \left\{ \begin{matrix} +1, & \text{if } l \equiv 2,3 \pmod 4; \\ -1, & \text{if } l \equiv 0,1 \pmod 4 \end{matrix} \right\} \left\{ \begin{matrix} +1, & \text{if } l>0; \\ -1, & \text{if } l \le 0 \end{matrix} \right\} (-1)^{\omega(|6l-1|)}. \qquad (15)
\end{aligned}$$

Therefore the sum (12) can be evaluated as

$$\begin{aligned}
\sum_{l\ \le L} \chi(l) &= \sum_{1 \le l \le O(\sqrt{L})} \chi(l) + \sum_{O(\sqrt{L}) \le l \le 0} \chi(l) \\
&= \sum_{0<j\le 4} \left\{ \begin{matrix} +1, & \text{if } j=2,3; \\ -1, & \text{if } j=1,4 \end{matrix} \right\} \sum_{0 \le k \le O(\sqrt{L})} (-1)^{\omega(24k+6j-1)} \\
&\quad + \sum_{0 \le j < 4} \left\{ \begin{matrix} +1, & \text{if } j=0,1; \\ -1, & \text{if } j=2,3 \end{matrix} \right\} \sum_{0 \le k \le O(\sqrt{L})} (-1)^{\omega(24k+6j+1)} \\
&= \sum_{\substack{0<r<24 \\ (r,24)=1}} \left\{ \begin{matrix} +1, & \text{if } r=1,7,11,17; \\ -1, & \text{if } r=5,13,19,23 \end{matrix} \right\} \sum_{0 \le k \le O(\sqrt{L})} (-1)^{\omega(24k+r)},
\end{aligned}$$

a linear combination of eight sums as in (14) with $N=\sqrt{L}$. Thus we need only prove (14).

Proof of (14). We define the auxiliary function

$$M_r(x) := \sum_{\substack{1 \le k \le x \\ k \equiv r (24)}} \mu(k).$$

For $r>0$ with $(24,r)=1$ we have

$$\begin{aligned}
\sum_{0 \le l \le N} (-1)^{\omega(24l+1)} &= \sum_{a \ge 1} \sum_{k \le N/a^2} \mu(k) \big[ka^2 \equiv r \pmod{24}\big] \\
&= \sum_{\substack{a \ge 1 \\ a \equiv \pm 1 (6)}} \sum_{\substack{k \le N/a^2 \\ k \equiv r (24)}} \mu(k) \\
&= \sum_{\substack{a \ge 1 \\ a \equiv \pm 1 (6)}} M_r\left(\frac{N}{a^2}\right).
\end{aligned}$$

Because $\sum_{a\geq 1} 1/a^2$ converges, it is easily seen to be sufficient to show that $M_r(N) = o(N)$ for each admissible r, which we do now by arguments patterned after those in [7, ch. XXII].

By Stirling's approximation we have $\sum_{1\leq n\leq x} \log(x/n) = O(x)$, whence *a fortiori*

$$\sum_{\substack{1\leq n\leq x\\ n\equiv r(24)}} \mu(n)\log(x/n) = O(x).$$

Consequently we have

$$\begin{aligned} M_r(x)\log x &= -\sum_{\substack{1\leq n\leq x\\ n\equiv r(24)}} \mu(n)\log n + O(x) \\ &= \sum_{\substack{1\leq n\leq x\\ n\equiv r(24)}} \sum_{d\mid n} \mu\left(\frac{n}{d}\right)\Lambda(d) + O(x) \\ &= \sum_{\substack{dk\leq x\\ dk\equiv r(24)}} \mu(k)\Lambda(d) + O(x) \\ &= \sum_{1\leq k\leq x} \mu(k) \sum_{\substack{1\leq d\leq x/k\\ dk\equiv r(24)}} \Lambda(d) + O(x), \end{aligned} \tag{16}$$

which suggests that we analyze the function

$$L_s(x) := \sum_{\substack{1\leq k\leq x\\ k\equiv s(24)}} \Lambda(k).$$

Now we have

$$\begin{aligned} L_s(x) &= \sum_{\substack{p^a\leq x\\ p^a\equiv s(24)}} \log p \\ &= \sum_{\substack{p\leq x\\ p\equiv s(24)}} \log p + \sum_{\substack{p^a\leq x\\ a\geq 2\\ p\equiv s(24)}} \log p \\ &= \sum_{\substack{p\leq x\\ p\equiv s(24)}} \log p + O\big(x^{1/2}\log^2 x\big); \end{aligned}$$

moreover, for each $\epsilon > 0$ we have

$$\begin{aligned} \sum_{\substack{p\leq x\\ p\equiv s(24)}} &= \sum_{\substack{x^{1-\epsilon}<p\leq x\\ p\equiv s(24)}} \log p + O\big(x^{1-\epsilon}\log x\big) \\ &= \big(1+L(\epsilon)\big) \sum_{\substack{p\leq x\\ p\equiv s(24)}} \log x + O\big(x^{1-\epsilon}\log x\big), \end{aligned}$$

whence by Dirichlet's theorem we have

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv s(24)}} &\sim \#\{p\le x : p\equiv s \pmod{24}\}\log x\\ &= \frac{1}{8}\big[(24,s)=1\big]\,\lfloor x\rfloor + o(x).\end{aligned}$$

Substitution into (16) now yields

$$\begin{aligned}M_r(x)\log x &= \sum_{k\le x}\mu(k)L_{rk^{-1}}\left(\frac{x}{k}\right)\\ &= \frac{1}{8}\sum_{\substack{k\le x\\ k\equiv\pm1(6)}}\mu(k)\left\lfloor\frac{x}{k}\right\rfloor + o(x\log x)\\ &= \frac{1}{8}\sum_{n\le x}\sum_{\substack{d\mid n\\ (6,d)=1}}\mu(d) + o(x\log x).\end{aligned}$$

But the sum on d vanishes except when n has no prime factors but 2 and 3, when it equals unity. Thus

$$\begin{aligned}M_r(x)\log x &= \frac{1}{8}\sum_{n\le x}\big[n=2^a3^b\big] + o(x\log x)\\ &= O\big(\log^2 x\big) + o(x\log x)\\ &= o(x\log x).\end{aligned}$$

In other terms $M_r(x) = o(x)$, as was desired. This completes the proof of Theorem 6. □

4 The order of p_2 at 2

After the results of §3, it is natural to ask for a description of the behavior of p_2 modulo higher powers of 2. The exact formula for the residue of p_2 modulo 8 given in [15] being fairly cumbersome and much harder to obtain than Theorem 5, it seems unlikely that the residue of p_2 modulo higher powers of 2 can be evaluated in a reasonably clean and compact form. In this section we study instead the order at 2 of $p_2(n)$, whose analysis can be pushed somewhat further without excessive complications of detail. We shall find that if $0\le\ell\le 4$, there is an exact characterization of the n such that

$$\operatorname{ord}_2 p_2(n) = \ell$$

in terms of the prime-power decomposition of $24n+1$.

We shall have use of a modification of the generating function $P_2(q)$, namely

$$\frac{\eta(48\tau)}{\eta(24\tau)} = \sum_n p_2(n) q^{24n+1}; \tag{17}$$

by the usual results on η-products (see, for instance, [15, p. 144]), this is a form on $\Gamma_0(1152)$ of weight 0 and character χ_2. The appearance of $24n+1$ as the exponent of q in the series in (17) is why our result depends on the factorization of $24n+1$.

4.1 A useful Hecke eigenform

Lovejoy's investigation [12] of the order at 5 of p_2 turns heavily on the properties of a particular Hecke eigenform in $M_4(\Gamma_0(1152), \chi_2)$ constructed from eight pieces, each resembling the function (17). The same form is also essential to our investigation, and we recall its definition here. Define the function

$$g(q) := \left(\frac{\eta(24\tau)^2}{\eta(48\tau)}\right)^8 = \left(1 + 2\sum_{n\geq 1} (-1)^n q^{24n^2}\right)^8, \tag{18}$$

and for $0 \leq i < 24$ with $(24, i) = 1$ let

$$f_i(q) = \sum_n a_i(n) q^n := g(q) \left(\frac{\eta(48\tau)}{\eta(24\tau)}\right)^i. \tag{19}$$

Of course $a_i(n) = 0$ unless $n \equiv i \pmod{24}$. Because

$$g(q) \equiv 1 \pmod{16} \tag{20}$$

we have

$$a_1(24n+1) \equiv p_2(n) \pmod{16}. \tag{21}$$

For this reason, the form f_1 will be of especial interest.

Now each f_i is a form in $M_4(\Gamma_0(1152), \chi_2)$, as is any $\mathbb{C}$-linear combination

$$h = \sum_i \alpha_i f_i.$$

If, as in[2] [12], we choose

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_{13} &= -8i\sqrt{77}, \\
\alpha_5 &= -2i\sqrt{35}, & \alpha_{17} &= 16\sqrt{55}, \\
\alpha_7 &= 2\sqrt{110}, & \alpha_{19} &= 16i\sqrt{70}, \\
\alpha_{11} &= 4i\sqrt{154}, & \alpha_{23} &= 32\sqrt{2},
\end{aligned}$$

[2]That this choice yields an eigenform was proven in [6], but the α_i were unfortunately misprinted there. The corrected values given here appear in [12].

then work of Gordon and Sinor [6] shows that h is a simultaneous eigenform of the Hecke operators on $M_4(\Gamma_0(1152), \chi_2)$. From this property we can deduce the action of each $T(p)$ (where $p \geq 5$) on the individual f_i. Indeed, because $p^2 \equiv 1 \pmod{24}$ for such p, we have $pn \equiv n/p \pmod{24}$ for all n divisible by p, and the coefficients of

$$f_i \mid T(p) = \sum_n \left(a_i(pn) + \chi_2(p)p^3 a_i(n/p)\right) q^n$$

are supported on the indices n with $pn \equiv i \pmod{24}$. Thus the $f_i \mid T(p)$ have coefficients supported on distinct arithmetic progressions, and equating coefficients in the eigenform property

$$h \mid T(p) = \sum_i \alpha_i f_i \mid T(p) = \lambda_p \sum_i \alpha_i f_i$$

shows that

$$f_i \mid T(p) = \mu_{ip} f_{\overline{ip}} \tag{22}$$

for suitable constants μ_{ip}. By comparing leading terms in (22), we find more precisely that

$$f_i \mid T(p) = \frac{\alpha_{\overline{p}}\alpha_{\overline{ip}}a_{\overline{p}}(p)}{\alpha_i} f_{\overline{ip}}. \tag{23}$$

Equating coefficients in (23) yields the equations

$$a_i(pn) + \chi_2(p)p^3 a_i(n/p) = \frac{\alpha_{\overline{p}}\alpha_{\overline{ip}}a_{\overline{p}}(p)}{\alpha_i} a_{\overline{ip}}(n), \quad n \text{ integral.} \tag{24}$$

These are essentially linear recurrences for $a_i(n)$ with $\operatorname{ord}_p n$ as the recursion variables. After we have solved them, we shall be able to determine $\operatorname{ord}_2 a_i(n)$ by induction over the prime-power decomposition of n.

4.2 Analysis of the recurrences

We begin by solving a general system of recurrences including those in the a_i as special cases.

Lemma 7 *Given a positive integer n and two sequences u_i and v_i such that*

$$\begin{aligned} u_i &= \alpha v_{i+1} + \gamma u_{i+2}, \\ v_i &= \beta u_{i+1} + \gamma v_{i+2} \end{aligned} \tag{25}$$

for certain constants α, β, γ and all $0 \leq i < n$, we have

$$u_0 = r_n \begin{Bmatrix} u_n, & \text{if } 2 \mid n; \\ v_n, & \text{if } 2 \mid n \end{Bmatrix} + \gamma r_{n-1} \begin{Bmatrix} v_{n+1}, & \text{if } 2 \mid n; \\ u_{n+1}, & \text{if } 2 \mid n \end{Bmatrix},$$

where

$$r_k = \sum_{i \leq k} \binom{k-i}{i} \alpha^{\lceil k/2 \rceil - i} \beta^{\lfloor k/2 \rfloor - i} \gamma^i.$$

Proof. Induction on n. $\square$

For each prime $p \neq 2, 3$ and all positive integers n, m with $(p, m) = 1$, the eigenform recurrences

$$\begin{aligned} a_1(pn) &= \alpha_{\overline{p}}^2 a_{\overline{p}}(p) a_{\overline{p}}(n) - \chi_2(p) p^3 a_1(n/p), \\ a_{\overline{p}}(pn) &= a_{\overline{p}}(p) a_1(n) - \chi_2(p) p^3 a_{\overline{p}}(n/p) \end{aligned}$$

give rise to sequences

$$u_i := a_1(p^{n-i}m), \qquad v_i := a_{\overline{p}}(p^{n-i}m)$$

satisfying the premise (25) of Lemma 7 with

$$\alpha = \alpha_{\overline{p}}^2 a_{\overline{p}}(p), \quad \beta = a_{\overline{p}}(p), \quad \gamma = -\chi_2(p)p^3.$$

Because $u_{n+1} = v_{n+1} = 0$ for these sequences, the result of Lemma 7 is that

$$a_1(p^n m) = \sum_{i \leq n} \binom{n-i}{i} \left(\alpha_{\overline{p}}^2\right)^{\ell - i} a_{\overline{p}}(p)^{n-2i} \left(-\chi_2(p)p^3\right)^i \times \begin{cases} a_1(m), & \text{if } n = 2\ell; \\ \alpha_{\overline{p}}^2 a_{\overline{p}}(m), & \text{if } n = 2\ell + 1; \end{cases} \tag{26}$$

interchanging u_i, α with v_i, β respectively and applying Lemma 7 again, we have analogously that

$$a_{\overline{p}}(p^n m) = \sum_{i \leq n} \binom{n-i}{i} \left(\alpha_{\overline{p}}^2\right)^{\ell - i} a_{\overline{p}}(p)^{n-2i} \left(-\chi_2(p)p^3\right)^i \times \begin{cases} a_1(m), & \text{if } n = 2\ell; \\ a_{\overline{p}}(m), & \text{if } n = 2\ell + 1. \end{cases} \tag{27}$$

We aim ultimately to evaluate $\operatorname{ord}_2^{\leq 5} p_2(n)$ and consequently will now evaluate not $\operatorname{ord}_2 a_1(N)$ but $\operatorname{ord}_2^{\leq 5} a_1(N)$, which contains all the information we can utilize. In the first place, we note that $a_1\left(p^{2\ell+1}m\right)$ is divisible by $\alpha_{\overline{p}}^2$ because each term of the sum in (26) is so divisible. For $p \equiv 11, 13, 17, 19, 23 \pmod{24}$ the quantity $\alpha_{\overline{p}}^2$ is a multiple of 32. Therefore

$$\operatorname{ord}_2^{\leq 5} a_1(N) = 5^+ \quad \text{if } \operatorname{ord}_p N \text{ is odd for any } p \equiv 11, 13, 17, 19, 23 \pmod{24}. \tag{28}$$

We now need analyze the effects on $\operatorname{ord}_2^{\leq 5} a_1(N)$ only of even powers of primes and odd powers of primes congruent to 1, 5, or 7 modulo 24. We assume henceforth, as we may by (28), that $\operatorname{ord}_p N$ is even for all $p \equiv 11, 13, 17, 19, 23 \pmod{24}$.

Making progress at this point is synonymous with evaluating $\operatorname{ord}_2^{\leq 5}$ of the binomial sum in (26) and (27). We begin with a more general evaluation of this sort.

Lemma 8 *Let η be rational with $\operatorname{ord}_2 \eta = d \geq 2$. Let n be a nonnegative integer, and let $\ell = \lfloor n/2 \rfloor$. Then*

$$\operatorname{ord}_2 \sum_{i \leq n} \binom{n-i}{i} \eta^{-i} = \begin{cases} -d\ell, & \text{if } n \text{ is even;} \\ -d\ell + \operatorname{ord}_2(\ell + 1), & \text{if } n \text{ is odd.} \end{cases}$$

Proof. The last nonvanishing term in the sum is

$$\binom{n-\ell}{\ell}\eta^{-\ell} = \begin{cases} \eta^{-\ell}, & \text{if } n \text{ is even;} \\ (\ell+1)\eta^{-\ell}, & \text{if } n \text{ is odd.} \end{cases}$$

The order asserted in Lemma 8 is precisely the order of this final term, so it is sufficient to prove that the other nonvanishing terms in the sum have order strictly greater than the final term. Because the binomial coefficients are integers, this is a triviality if n is even or if n is odd and ℓ is even. In the remaining case, when $\ell+1$ is even, we consider for $k \geq 1$ the term ratio

$$\frac{\binom{n-\ell+k}{\ell-k}\eta^{-\ell+k}}{\binom{n-\ell}{\ell}\eta^{-\ell}} = \frac{(\ell+1+k)\cdots(\ell+2)\ell\cdots(\ell+1-k)}{(2k+1)!}\eta^k. \tag{29}$$

Of course $\operatorname{ord}_2 \eta^k = kd$. To handle the fraction, note that at least $\lfloor k/2^j \rfloor$ of the numbers $\ell+2, \ldots, \ell+1+k$ are divisible by 2^j for each $j \geq 1$, and the same is true of the numbers $\ell+1-k, \ldots, \ell$. Of the numbers $1, \ldots, 2k+1$ *exactly* $\lfloor (2k+1)/2^j \rfloor$ are divisible by 2^j. Consequently the order at 2 of the ratio (29) is at least

$$\begin{aligned} 2\sum_{j\geq 1}\left\lfloor \frac{k}{2^j}\right\rfloor - \sum_{j\geq 1}\left\lfloor \frac{2k+1}{2^j}\right\rfloor + kd &= 2\sum_{j\geq 1}\left\lfloor \frac{k}{2^j}\right\rfloor - \sum_{j\geq 0}\left\lfloor \frac{k}{2^j}\right\rfloor + kd \\ &= \sum_{j\geq 1}\left\lfloor \frac{k}{2^j}\right\rfloor - k + kd \\ &\geq k(d-1), \end{aligned}$$

which is positive, as desired. □

The binomial sum in (26) and (27) can be rewritten as

$$\left(\alpha_{\overline{p}}^2\right)^{\ell} a_{\overline{p}}(p)^n \sum_{i\leq n}\binom{n-i}{i}\left(\frac{\alpha_{\overline{p}}^2 a_{\overline{p}}(p)^2}{-\chi_2(p)p^3}\right)^{-i}, \tag{30}$$

which makes Lemma 8 applicable provided that the order at 2 of $\alpha_{\overline{p}}^2 a_{\overline{p}}(p)^2$ can be calculated exactly and is at least 2. We accomplish this in

Lemma 9 *If* $p \equiv 1 \pmod{24}$ *then* $\operatorname{ord}_2 a_1(p) = 1$. *If* $p \equiv 5, 7 \pmod{24}$ *then* $a_{\overline{p}}(p)$ *is odd.*

Proof. Because $a_1(24n+1) \equiv p_2(n) \pmod{16}$, the statement for $p \equiv 1 \pmod{24}$ follows from Theorem 5.

Let $p \equiv 5 \pmod{24}$. Working modulo 2, we recall that

$$\frac{\eta^2(24\tau)}{\eta(48\tau)} \equiv 1$$

and deduce that

$$f_5 \equiv \frac{\eta^5(48\tau)}{\eta^5(24\tau)} = \frac{\eta^4(48\tau)}{\eta^8(24\tau)}\frac{\eta(48\tau)}{\eta^{-3}(24\tau)} \equiv \eta(48\tau)\eta^3(24\tau) \equiv q^5 \sum_l \sum_{k\geq 0} q^{48l\ +24k}\ ,$$

where we have used Euler and Jacobi's polygonal-number series. Extracting coefficients, we find that

$$a_5(p) \equiv \#\{(k,l) : k \geq 0, p = 5 + 48l\ \ + 24k\ \} \pmod 2.$$

Now $p = 5 + 48l\ \ + 24k\ \ $ means exactly that

$$2p = 6(2k+1)^2 + \big(2(6l-1)\big)^2. \tag{31}$$

By Lemma 4 the equation

$$2p = \lambda^2 + 6\kappa^2 \tag{32}$$

has exactly four solutions, which differ from each other only in the signs of κ and λ. Considering (32) modulo 24, we find that κ is odd and $\lambda^2 \equiv 4 \pmod{24}$, whence $\frac{1}{2}\lambda \equiv \pm 1 \pmod 6$. For exactly one choice of the signs, the solution is of the stricter form in (31). Therefore we have proven that $a_5(p) \equiv 1 \pmod 2$, as desired.

Finally, let $p \equiv 7 \pmod{24}$, and note that

$$f_7 \equiv \frac{\eta^7(48\tau)}{\eta^7(24\tau)} = \frac{\eta^4(48\tau)}{\eta^8(24\tau)}\frac{\eta^3(48\tau)}{\eta^{-1}(24\tau)} \equiv \eta^3(48\tau)\eta(24\tau) \equiv q^7 \sum_{k\geq 0} \sum_l q^{48k\ +24l}\ ,$$

whence

$$a_7(p) \equiv \#\{(k,l) : k \geq 0, p = 7 + 48k\ \ + 24l\ \} \pmod 2.$$

The equation on p, k, l is that

$$p = 6(2k+1)^2 + (6l-1)^2. \tag{33}$$

By Lemma 4 the equation $p = \lambda^2 + 6\kappa^2$ has four solutions, and by considering residues modulo 24 again, we find that exactly one has the strict form of (33). Thus $a_7(p) \equiv 1 \pmod 2$. $\square$

By virtue of Lemma 9 we have

$$\operatorname{ord}_2^{\leq 5}\big(\alpha_{\overline{p}}^2 a_{\overline{p}}(p)^2\big) = \begin{cases} 2, & \text{if } p \equiv 1, 5 \pmod{24}; \\ 3, & \text{if } p \equiv 7 \pmod{24}. \end{cases}$$

We can therefore apply Lemma 8 to find $\operatorname{ord}_2^{\leq 5}$ of (30) when $p \equiv 1, 5, 7 \pmod{24}$, obtaining, after a little manipulation, the result

$$\operatorname{ord}_2^{\leq 5}\big(\alpha_{\overline{p}}^2\big)^\ell a_{\overline{p}}(p)^n \sum_{i\leq n} \binom{n-i}{i} \left(\frac{\alpha_{\overline{p}}^2 a_{\overline{p}}(p)^2}{-\chi_2(p)p^3}\right)^{-i} = \begin{cases} 0, & \text{if } n \text{ is even;} \\ 1 + \operatorname{ord}_2^{\leq 5}(\ell+1), & \text{if } n = 2\ell+1 \text{ and } p \equiv 1 \pmod{24}; \\ \operatorname{ord}_2^{\leq 5}(\ell+1), & \text{if } n = 2\ell+1 \text{ and } p \equiv 5, 7 \pmod{24}. \end{cases} \tag{34}$$

Using (34) in (26) and (27), we find that

$$\operatorname{ord}_2^{\le 5} a_1(p^n m) = \begin{cases} \operatorname{ord}_2^{\le 5} a_1(m), & \text{if } n \text{ is even;} \\ \operatorname{ord}_2^{\le 5} a_1(m) + 1 + \operatorname{ord}_2^{\le 5}(\ell+1), & \text{if } n = 2\ell+1 \text{ and } p \equiv 1 \pmod{24}; \\ \operatorname{ord}_2^{\le 5} a_5(m) + 2 + \operatorname{ord}_2^{\le 5}(\ell+1), & \text{if } n = 2\ell+1 \text{ and } p \equiv 5 \pmod{24}; \\ \operatorname{ord}_2^{\le 5} a_7(m) + 3 + \operatorname{ord}_2^{\le 5}(\ell+1), & \text{if } n = 2\ell+1 \text{ and } p \equiv 7 \pmod{24}; \end{cases} \tag{35}$$

$$\operatorname{ord}_2^{\le 5} a_{\overline{p}}(p^n m) = \begin{cases} \operatorname{ord}_2^{\le 5} a_{\overline{p}}(m), & \text{if } n \text{ is even;} \\ \operatorname{ord}_2^{\le 5} a_1(m) + 1 + \operatorname{ord}_2^{\le 5}(\ell+1), & \text{if } n = 2\ell+1 \text{ and } p \equiv 1 \pmod{24}; \\ \operatorname{ord}_2^{\le 5} a_1(m) + \operatorname{ord}_2^{\le 5}(\ell+1), & \text{if } n = 2\ell+1 \text{ and } p \equiv 5, 7 \pmod{24}. \end{cases} \tag{36}$$

It is now easy to deduce

Theorem 10 *Let $M \equiv 1 \pmod{24}$ be a positive integer. If $\operatorname{ord}_p M$ is odd for any $p \equiv 11, 13, 17, 19, 23 \pmod{24}$, then $\operatorname{ord}_2^{\le 5} a_1(M) = 5^+$. Otherwise let r_1, $2h_5$, $2h_7$ be the numbers of primes congruent to 1, 5, 7 respectively at which M has odd order. Then*

$$\operatorname{ord}_2^{\le 5} a_1(M) = r_1 + 2h_5 + 3h_7 + \sum_{\operatorname{ord}_p M \equiv 1 (2)} \operatorname{ord}_2^{\le 5} \frac{1 + \operatorname{ord}_p M}{2}. \tag{37}$$

Proof. If M has odd order only at $p \equiv 1, 5, 7 \pmod{24}$, the number of primes congruent modulo 24 to 5 at which M has odd order is necessarily even because $M \equiv 1 \pmod{24}$, and similarly for primes congruent to 7. Thus we can verify (37) by induction by evaluating

$$\operatorname{ord}_2^{\le 5} a_1(p_1^{2l+1} m), \quad \operatorname{ord}_2^{\le 5} a_1(p_5^{2l+1} q_5^{2k+1} m), \quad \operatorname{ord}_2^{\le 5} a_1(p_7^{2l+1} q_7^{2k+1} m),$$

where $p_r, q_r \equiv r \pmod{24}$ do not divide m, in terms of $\operatorname{ord}_2^{\le 5} a_1(m)$. These evaluations are trivial applications of (35) and (36). □

4.3 From a_1 to p_2

If we could prove that $a_1(24m+1) \equiv p_2(m) \pmod{32}$ for all $m \ge 0$, we could immediately deduce

Theorem 11 *Given $m \ge 0$, let $M = 24m + 1$. If $\operatorname{ord}_p M$ is odd for some $p \equiv 11, 13, 17, 19, 23 \pmod{24}$, then $\operatorname{ord}_2^{\le 5} p_2(m) = 5^+$. Otherwise let r_1, $2h_5$, $2h_7$ be the numbers of primes congruent to 1, 5, 7 respectively at which M has odd order. Then*

$$\operatorname{ord}_2^{\le 5} p_2(m) = r_1 + 2h_5 + 3h_7 + \sum_{\operatorname{ord}_p M \equiv 1 (2)} \operatorname{ord}_2^{\le 5} \frac{1 + \operatorname{ord}_p M}{2}. \tag{38}$$

Because $f_1(q) = g(q)\eta(48\tau)/\eta(24\tau)$ with $g \equiv 1 (\text{mod } 16)$, we do have $a_1(24m+1) \equiv p_2(m) (\text{mod } 16)$. The truth modulo 32 is not as clean, but it is good enough for our purposes:

Lemma 12 *Given $m \geq 0$, let $M = 24m + 1$. Then*

$$p_2(m) \equiv \begin{cases} a_1(M) + 16, & \text{if } M = \mu^2 \text{ for some } \mu \equiv 5, 11, 13, 19 \pmod{24}; \\ a_1(M) & \text{otherwise.} \end{cases} \tag{39}$$

Proving Lemma 12 will establish Theorem 11, for in the exceptional case of (39), the number $p_2(m)$, whence also $a_1(M)$, is odd by Theorem 5, whence $\operatorname{ord}_2^{\leq 5}\big(a_1(M)+16\big) = \operatorname{ord}_2^{\leq 5} a_1(M)$ trivially.

Proof of Lemma 12. We recall the generating function

$$\theta_8(q) := \left(1 + 2\sum_{n\geq 1} q^{n^2}\right)^8$$

of the number $r_8(n)$ of representations of an integer n as the sum of eight squares. In terms of this function, we have $g(q) = \theta_8\big(-q^{24}\big)$. Because $\theta_8(q) \equiv 1 \pmod{16}$ we have $\theta_8(-q) \equiv \theta_8(q) \pmod{32}$, whence

$$g(q) \equiv \theta_8(q^{24}) \pmod{32}.$$

Multiplying by $\eta(48\tau)/\eta(24\tau)$ and equating coefficients yields the congruence

$$a_1(24m+1) \equiv \sum_{0\leq j\leq m} r_8(j) p_2(m-j). \tag{40}$$

A result of [13] implies that for $j \geq 1$ we have modulo 32 that

$$r_8(j) \equiv 16\#\{d \mid j : d \text{ odd}\} \equiv \begin{cases} 16, & \text{if } j \text{ is square or twice a square;} \\ 0 & \text{otherwise.} \end{cases}$$

Moreover $p_2(m-j)$ is even unless $24(m-j)+1$ is square; consequently, (40) involves

$$\begin{aligned} a_1(M) - p_2(m) &\equiv 16\#\{(j,k) : j \geq 1, k \geq 0,\ j \text{ or } j/2 \text{ square}, M = 24j + k^2\} \\ &\equiv 16\left(\#\{(k,l) : l \geq 1, k \geq 0, M = 24l^2 + k^2\} + \#\{(k,l) : l \geq 1, k \geq 0, M = 48l^2 + k^2\}\right). \end{aligned} \tag{41}$$

Now $\kappa^2 + 6\lambda^2 \equiv 1 \pmod{24}$ implies $2 \mid \kappa$, and $\kappa^2 + 3\lambda^2 \equiv 1 \pmod{24}$ implies $4 \mid \kappa$, as a finite verification will show. Thus we have

$$a_1(M) - p_2(m) \equiv 4\big(r_{1,3}(M) + r_{1,6}(M)\big) \pmod{32} \quad \text{for nonsquare } M, \tag{42}$$

for if M is not square, there is no representation with $l = 0$, and exactly one-fourth of the representations of M appear in the sets in (41).

We assume first that M is in fact nonsquare. Recalling the results of Lemma 3 and Lemma 4, we rewrite (42) as the modulo-4 congruence

$$\begin{aligned} \frac{1}{8}\big(a_1(M) - p_2(m)\big) &\equiv \big[\operatorname{ord}_p M \text{ even at all } p \equiv 5, 11, 17, 23 \pmod{24}\big] \prod_{p\equiv 1,7,13,19(24)} \big(\operatorname{ord}_p M + 1\big) \\ &\quad + \big[\operatorname{ord}_p M \text{ even at all } p \equiv 13, 17, 19, 23 \pmod{24}\big] \prod_{p\equiv 1,5,7,11(24)} \big(\operatorname{ord}_p M + 1\big). \end{aligned} \tag{43}$$

We shall show that the right-hand side of (43) is divisible by 4. For brevity we let $\#_3$ and $\#_6$ denote the first and second indexed products in (43) respectively, and we refer to the right-hand side of (43) as R. We distinguish several cases.

- If $\operatorname{ord}_p M$ is odd for some $p \equiv 17, 23 \pmod{24}$, then both terms in R vanish, and the claim is trivially true.
- Suppose $\operatorname{ord}_p M$ is odd for some $p \equiv 13, 19$. If $\operatorname{ord}_q M$ is odd for any $q \equiv 5, 11, 17, 23$, then $R = 0$. Otherwise $R = \#_3$, and $\operatorname{ord}_{p'} M$ must be odd for some $p' \neq p$ with $p' \equiv 7, 13, 19$, or M would not have residue 1 modulo 24. Thus $\#_3$ contains at least two even factors.
- Suppose $\operatorname{ord}_p M$ is odd for some $p \equiv 5, 11$. Then $R = 0$ if $\operatorname{ord}_q M$ is odd for any $q \equiv 13, 17, 19, 23$. Otherwise $R = \#_6$, and M has odd order at some $p' \equiv 5, 7, 11$ other than p, whence $4 \mid \#_6$.
- We henceforth assume $\operatorname{ord}_p M$ even except possibly at $p \equiv 1, 7$, the other cases having been settled. We have $R = \#_3 + \#_6$. If $\operatorname{ord}_p M$ is odd at some $p \equiv 7$, it is odd at another such prime, and both $\#_3$ and $\#_6$ are divisible by 4. We have $4 \mid \#_3, \#_6$ also if $\operatorname{ord}_p M$ is odd for two primes congruent to 1 or if $\operatorname{ord}_p M \equiv 3 \pmod 4$ for some $p \equiv 1$.
- In the remaining case $M = p^{4m+1}k^2$ for $p \equiv 1$ not dividing k. In this case $\#_3 \equiv \#_6 \equiv 2 \pmod 4$, whence $\#_3 + \#_6 \equiv 0 \pmod 4$, as desired.

In the remaining case M is a square μ^2. In this case we have

$$a_1(M) - p_2(m) \equiv 4\big(\big(r_{1,3}(M) - 2\big) + \big(r_{1,6}(M) - 2\big)\big)$$

(the subtraction of 2 eliminates the representations $M = \kappa^2 + \{3 \text{ or } 6\}\lambda^2$ with $\lambda = 0$). In other terms, if we let n_i denote the sum of the orders of μ at primes $p \equiv i \pmod{24}$, we have modulo 4 that

$$\begin{aligned}
\frac{a_1(M) - p_2(m)}{8} &\equiv \prod_{p \equiv 1,7,13,19(24)} \big(2 \operatorname{ord}_p \mu + 1\big) + \prod_{p \equiv 1,5,7,11(24)} \big(2 \operatorname{ord}_p \mu + 1\big) - 2 \\
&\equiv (-1)^{n_1+n_7+n_{13}+n_{19}} + (-1)^{n_1+n_5+n_7+n_{11}} - 2 \\
&\equiv 2 + (-1)^{n_1+n_7+n_{13}+n_{19}}\big(1 + (-1)^{n_5+n_{11}+n_{13}+n_{19}}\big) \\
&\equiv \begin{cases} 0, & \text{if } (-1)^{n_5+n_{11}+n_{13}+n_{19}} = 1; \\ 2 & \text{otherwise.} \end{cases}
\end{aligned}$$

Now $\{5, 11, 13, 19\}$ is the nontrivial coset of the subgroup $\{\pm 1, \pm 7\} \subset (\mathbb{Z}/24)^*$; therefore

$$(-1)^{n_5+n_{11}+n_{13}+n_{19}} = (-1)^{[\mu \equiv 5,11,13,19(24)]},$$

which completes the proof. $\square$

4.4 Explicit criteria

In view of Theorem 11, we can easily obtain necessary and sufficient conditions that $\operatorname{ord}_2 p_2(n) = \ell$, where $0 \le \ell \le 4$, in terms of the factorization of $N := 24n + 1$. To keep the answer concise and clear, we introduce the notation

$$x_1^{r_1(m_1)} \cdots x_s^{r_s(m_s)} \tag{44}$$

for the class of numbers of the form

$$k^2 \prod_{1 \le i \le s} p_i^{e_i},$$

where the p_i are distinct primes not dividing k such that $p_i \equiv x_i \pmod{24}$ for each i, and $e_i \equiv r_i \pmod{m_i}$ for each i. For instance, the prime 13 is a $13^{1(4)}$ but not a $13^{3(4)}$, and the product $5 \cdot 29 \cdot 73^2$ is a $5^{1(16)}5^{1(8)}$. In the special case when $s = 0$ (the class of square numbers), we write $\square$ instead of the empty string.

If $\operatorname{ord}_2 p_2(n) < 5$ then N has even order at all primes congruent to 11, 13, 17, 19, or 23 modulo 24. In this circumstance $\operatorname{ord}_2 p_2(n)$ is given by the expression in (38), all of whose terms take nonnegative values determined solely by the orders of N at the remaining primes. Consequently, the set of N for which $\operatorname{ord}_2 p_2(n) = \ell$, for given $0 \le \ell \le 4$, is the union of finitely many of the classes (44), and these classes can be enumerated by finite trial. For instance, the sum in (38) vanishes only for $r_1 = h_5 = h_7 = 0$, i.e., when N has even order at every prime, and we recover the result that

$$\operatorname{ord}_2 p_2(n) = 0 \quad \text{if and only if} \quad N \in \square.$$

Similarly we have $\operatorname{ord}_2 p_2(n) = 1$ only when $r_1 = 1$, $h_5 = h_7 = 0$, and the sum in (38) is empty. That means that N has even order at all primes except for one prime $p \equiv 1 \pmod{24}$ at which $\big(\operatorname{ord}_p N + 1\big)/2$ is odd. We thus recover the result of Theorem 5 that

$$\operatorname{ord}_2 p_2(n) = 1 \quad \text{if and only if} \quad N \in 1^{1(4)}.$$

Like methods work as well for $\ell = 2, 3, 4$, when Theorem 5 is inapplicable; and one easily verifies

Theorem 13 *Given $n \ge 0$, let $N = 24n + 1$.*

- *We have* $\operatorname{ord}_2 p_2(n) = 2$ *if and only if*

$$N \in 1^{1(4)}1^{1(4)} \text{ or } 1^{3(8)} \text{ or } 5^{1(4)}5^{1(4)}.$$

- *We have* $\operatorname{ord}_2 p_2(n) = 3$ *if and only if*

$$N \in 1^{1(4)}1^{1(4)}1^{1(4)} \text{ or } 1^{3(8)}1^{1(4)} \text{ or } 1^{7(16)} \text{ or } 1^{1(4)}5^{1(4)}5^{1(4)} \text{ or } 5^{3(8)}5^{1(4)} \text{ or } 7^{1(4)}7^{1(4)}.$$

- *We have* $\operatorname{ord}_2 p_2(n) = 4$ *if and only if*

$$\begin{aligned} N \in\ & 1^{1(4)}1^{1(4)}1^{1(4)}1^{1(4)} \text{ or } 1^{3(8)}1^{1(4)}1^{1(4)} \\ & \text{or } 1^{3(8)}1^{3(8)} \text{ or } 1^{7(16)}1^{1(4)} \text{ or } 1^{15(32)} \\ & \text{or } 1^{1(4)}1^{1(4)}5^{1(4)}5^{1(4)} \text{ or } 1^{3(8)}5^{1(4)}5^{1(4)} \\ & \text{or } 1^{1(4)}5^{3(8)}5^{1(4)} \text{ or } 5^{1(4)}5^{1(4)}5^{1(4)}5^{1(4)} \\ & \text{or } 5^{3(8)}5^{3(8)} \text{ or } 5^{7(16)}5^{1(4)} \\ & \text{or } 1^{1(4)}7^{1(4)}7^{1(4)} \text{ or } 7^{3(8)}7^{1(4)}. \end{aligned}$$

4.5 Beyond the fifth power

Theorem 13 leaves open the question of when $\operatorname{ord}_2 p_2(n)$ takes a specified value ≥ 5. A result in this direction may be found in [17], where Rødseth proves that whenever $N = 24n + 1$ has odd order at a prime p, we must have $\operatorname{ord}_2 p_2(n) \geq (r-1)/2$, where r denotes the least residue of p modulo 24. For $p \equiv 1 \pmod{24}$ this is vacuous, and for $p \equiv 5, 7, 11 \pmod{24}$ we have proven the assertion. Our methods, however, do not appear to extend readily to handle the cases in which $r > 5$. In light of Rødseth's theorem, it is natural to suspect that the circumstances under which $\operatorname{ord}_2 p_2(n) = \ell$ may be completely analyzable for some $\ell \geq 5$. But the answer, if there is one, cannot depend only on the orders and residue classes modulo 24 of the primes dividing N, for there are small ($n \leq 2000000$) examples of $N \in 11^{1(2)}11^{1(2)}$ for which $\operatorname{ord}_2 p_2(n)$ is any number between 5 and 18 inclusive. What form a correct necessary and sufficient condition like those in Theorem 13 might assume is not evident.

Acknowledgments

The author thanks Professor John Rickert of Rose-Hulman Institute of Technology for his helpful advice and the National Science Foundation for its generous support.

References

[1] G. E. Andrews, *The Theory of Partitions*, New York, Cambridge University Press, 1998.

[2] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, 2nd ed., New York, Springer-Verlag, 1997.

[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, New York, John Wiley and Sons, 1989.

[4] J. A. Ewell, Recurrences for Two Restricted Partition Functions, Fib. Quart. **18** (1980), 1–2.

[5] B. Gordon and K. Ono, Divisibility of certain partition functions by powers of primes, Ramanujan J. **1** (1997), 25–34.

[6] B. Gordon and D. Sinor, Multiplicative properties of η-products, *Number Theory, Madras 1987* (Lecture Notes in Math. **1395**), New York, Springer-Verlag, 1989, pp. 173–200.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (5th ed.), New York, Oxford University Press, 1993.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, New York, Springer-Verlag, 1998.

[9] C. G. J. Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, Königsberg, Bornträger, 1829.

[10] M. I. Knopp, *Modular Functions in Analytic Number Theory*, Chicago, Markham, 1970.

[11] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2^{nd} ed., New York, Springer-Verlag, 1993.

[12] J. Lovejoy, The number of partitions into distinct parts modulo powers of 5, preprint (`www.math.wisc.edu/~lovejoy/5powersQ.ps`, June 21, 2001).

[13] M. B. Nathanson, *Elementary Methods in Number Theory*, New York, Springer-Verlag, 2000.

[14] K. Ono, Distribution of the partition function modulo m, Ann. Math. **151** (2000), 293–307.

[15] K. Ono and D. Penniston, The 2-adic behavior of the number of partitions into distinct parts, J. Comb. Theory Ser. A **92** (2000), 138–157.

[16] S. Ramanujan, Congruence properties of partitions, Proc. London Math. Soc. **19** (1919), 207–10.

[17] Øystein Rødseth, Congruence properties of the partition functions $q(n)$ and $q_0(n)$, Arbok Univ. Bergen Mat.-Naturv. Ser. **13**, 1970.

[18] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge, Cambridge University Press, 1996.