Disquisitiones Arithmeticae and online sequence A108345

Paul Monsky
Brandeis University, Waltham MA 02454-9110, USA
monsky@brandeis.edu

Abstract

Let $g$ be the element $\sum_{n \geq 0} x^n$ of $A = \mathbb{Z}/2[[x]]$, and $B$ consist of all $n$ for which the coefficient of $x^n$ in $\frac{1}{g}$ is 1. (The elements of $B$ are the entries 0, 1, 2, 3, 5, 7, 8, 9, 13, \ldots in A108345; see [3].) In [1] it is shown that the (upper) density of $B$ is $\leq \frac{1}{4}$, and it is conjectured that $B$ has density 0. This note uses results of Gauss on sums of 3 squares to show that the subset of $B$ consisting of $n \not\equiv 15 \quad (16)$ has density 0. The final section gives some computer calculations, made by Kevin O’Bryant, indicating that, pace [1], $B$ has density $\frac{1}{32}$.

Comments. The note is drawn from my answers, on Mathoverflow, to questions asked by O’Bryant and me.

1 Introduction

I begin with simple derivations of some results from [1]. Let $g$ be the element $1 + x + x^4 + x^9 + \cdots$ of $A = \mathbb{Z}/2[[x]]$. Write $\frac{1}{g}$ as $\sum b_i x^i$ with the $b_i$ in $\mathbb{Z}/2$, and let $B$ consist of all $n$ with $b_n = 1$.

Theorem 1.1. If $n$ is even, $n$ is in $B$ if and only if $\frac{n}{2}$ is a square.

Proof. Let $R \subset A$ be $\mathbb{Z}/2[[x]]$. As $R$-module, $A$ is the direct sum of $R$ and $xR$. Let $pr : A \to R$ be the $R$-linear map which is the identity on $R$ and sends $xR$ to 0. Since $g^2$ is in $R$, so is $\frac{1}{g^2}$. Now $pr(g) = 1 + x^4 + x^{16} + x^{36} + \cdots = g^4$. So $pr \left( \frac{1}{g} \right) = \frac{1}{g^2} pr(g) = g^2$. This is precisely the statement of the theorem.

Theorem 1.2. If $n \equiv 1 \quad (4)$, $n$ is in $B$ if and only if the number of ways of writing $n$ as $(\text{square}) + 4(\text{square})$ is odd.
Proof. \( \frac{1}{g} = g \cdot \frac{1}{g} \). So the coefficient of \( x^n \) in \( \frac{1}{g} \) is the number of ways, modulo 2, of writing \( n \) as \((\text{square}) + 2k\) with \( k \) in \( B \). Since \( n \equiv 1 \pmod{4} \), the square is also \( \equiv 1 \pmod{4} \), and \( k \) is even. Now use Theorem 1.1.

**Theorem 1.3.** The number of \( n \) in \( B \) that are \( \leq x \) and \( \not\equiv 3 \pmod{4} \) is \( O(x/\log(x)) \).

Proof. In view of Theorem 1.1 we may restrict our attention to \( n \) that are \( \equiv 1 \pmod{4} \) (and that are not squares). If such an \( n \) is \( s_1 + 4s_2 \) then \( \sqrt{s_1 + 2i\sqrt{s_2}} \) and \( \sqrt{s_1 - 2i\sqrt{s_2}} \) generate ideals of norm \( n \) in \( \mathbb{Z}[i] \); since \( n \) is not a square, these two ideals are distinct. Since every ideal of norm \( n \) comes from exactly one decomposition of \( n \) as \((\text{square}) + 4(\text{square})\), the number of decompositions of \( n \) is \( \frac{1}{2} \) \( (\text{the number of ideals of norm } n) \). Standard facts about \( \mathbb{Z}[i] \) tell us that this number is odd only when \( n \) is the product of a square by a prime \( \equiv 1 \pmod{4} \). Now use the fact that \( \pi(x) = O(x/\log(x)) \).

**Theorem 1.4.** If \( n \equiv 3 \pmod{8} \), \( n \) is in \( B \) if and only if the number of ways of writing \( n \) as \((\text{square}) + 2(\text{square}) + 8(\text{square})\) is odd.

Proof. \( \frac{1}{g} = g \cdot g^2 \cdot \frac{1}{g^3} \). So the coefficient of \( x^n \) in \( \frac{1}{g} \) is the number of ways, modulo 2, of writing \( n \) as \((\text{square}) + 2(\text{square}) + 4k\) with \( k \) in \( B \). Since \( n \equiv 3 \pmod{8} \), congruences mod 8 show that \( k \) is even, and we use Theorem 1.1.

2 A density result for \( n \equiv 3 \pmod{8} \)

**Lemma 2.1.** Suppose \( n \equiv 3 \pmod{8} \). Let \( R_1 \) and \( R_2 \) be the number of ways of writing \( n \) as \((\text{square}) + (\text{square}) + (\text{square})\) and as \((\text{square}) + 2(\text{square})\). If \( 4 \) divides \( R_1 \) and \( R_2 \), then \( n \) is not in \( B \).

Proof. In view of Theorem 1.4 it suffices to show that \( R_1 + R_2 \) is twice the number of ways of writing \( n \) as \((\text{square}) + 2(\text{square}) + 8(\text{square})\). Suppose \( n = s_1 + s_2 + s_3 \) with the \( s_i \) squares. The \( s_i \) are odd. Let \( r_2 \) and \( r_3 \) be square roots of \( s_2 \) and \( s_3 \) with \( r_2 \equiv r_3 \pmod{4} \). Then \( n = s_1 + 2 \left( \frac{r_2 + r_3}{2} \right)^2 + 8 \left( \frac{r_2 - r_3}{4} \right)^2 = (\text{square}) + 2(\text{square}) + 8(\text{square}) \), and replacing \( r_2 \) and \( r_3 \) by \( -r_2 \) and \( -r_3 \) gives the same decomposition. It’s easy to see that one gets every decomposition \( n = t_1 + 2t_2 + 8t_3 \) with the \( t_i \) squares from some triple \((s_1, s_2, s_3)\) in this way. Furthermore if \((s_1, s_2, s_3) \rightarrow (t_1, t_2, t_3)\), then \((s_1, s_3, s_2) \rightarrow \) the same \((t_1, t_2, t_3)\). It follows that the fiber over a fixed \((t_1, t_2, t_3)\) consists of 2 elements except at those points where \( t_3 = 0 \). But such a point corresponds to a decomposition of \( n \) as \((\text{square}) + 2(\text{square})\).

**Lemma 2.2.** Suppose \( n \equiv 3 \pmod{8} \) and is divisible by 3 or more different primes. Then the number of ways of writing \( n \) primitively as \((\text{square}) + (\text{square}) + \ldots\) (8 times)
(square) is divisible by 4.

Proof. Let $O = \mathbb{Z}[\frac{1 + \sqrt{-n}}{2}]$. A result of Gauss, [2], put into modern language, is that the number of primitive representations of $n$ by the form $x^2 + y^2 + z^2$ is $24 \cdot (\text{the number of invertible ideal classes in } O)$. So the number of ways of writing $n$ primitively as (square) + (square) + (square) is $3 \cdot (\text{the number of invertible ideal classes})$, and it suffices to show that 4 divides this number. Now Gauss developed a genus theory for binary quadratic forms which tells us that the group of invertible ideal classes maps onto a product of $m - 1$ copies of $\mathbb{Z}/2$, where $m$ is the number of different primes dividing $n$. Since $m \geq 3$ we’re done.

Theorem 2.3. If $n \equiv 3 \pmod{8}$ and there are 3 or more primes that occur to odd exponent in the prime factorization of $n$, then $n$ is not in $B$.

Proof. By Lemma 2.2, whenever $a^2$ divides $n$, the number of ways of writing $n/a^2$ primitively as (square) + (square) + (square) is divisible by 4. Summing over $a$ we find that 4 divides $R_1$. Furthermore, by Lemma 3.3, $2R_2$ is the number of ideals of norm $n$ in $\mathbb{Z}[\sqrt{-2}]$. This number is $\sum \left( \frac{-2}{d} \right)$ where $\left( \frac{d}{ } \right)$ is the Jacobi symbol, and $d$ runs over the divisors of $n$. Since $\left( \frac{ }{ } \right)$ is multiplicative, the sum is a product of integer factors, one coming from each prime dividing $n$. Also, a prime having odd exponent in the factorization contributes an even factor. Since there are at least 3 such primes, 8 divides $2R_1$, 4 divides $R_1$, and we use Lemma 2.1.

Theorem 2.4. The number of $n$ in $B$ that are $\leq x$ and $\equiv 3 \pmod{8}$ is $O \left( x \log \log(x) / \log(x) \right)$.

Proof. Let $\pi_2(x)$ be the number of $n \leq x$ that are a product of 2 primes. It’s well-known that $\pi_2(x)$ is $O \left( x \log \log(x) / \log(x) \right)$. By Theorem 2.3 an element of $B$ that is $\equiv 3 \pmod{8}$ is either the product of a single prime and a square, or of two primes and a square. The result follows easily.

3 A density result for $n \equiv 7 \pmod{16}$

For $n \equiv 7 \pmod{16}$ we show that $n$ is in $B$ if and only if the number of ways to write $2n$ as (square) + (square) + (square) is $\equiv 2 \pmod{4}$, and arguing as in the last section, prove the analogue to Theorem 2.4.

Lemma 3.1. If $n \equiv 1 \pmod{8}$ then the number of ideals $U$ of norm $n$ in $\mathbb{Z}[\sqrt{-2}]$ is congruent mod 4 to the number of ideals $V$ of norm $n$ in $\mathbb{Z}[i]$ unless $n = A^2$ with $A \equiv \pm 3 \pmod{8}$. 

3
Proof. $U = \sum \left( \frac{\,\cdot\,}{d} \right)$ and $V = \sum \left( \frac{\,\cdot\,}{d} \right)$ where the sums are over the divisors of $n$. Since $\left( \frac{\,\cdot\,}{d} \right)$ is multiplicative, $U$ (resp. $V$) is a product of contributions, one for each prime dividing $n$. A contribution is even if the prime occurs to odd exponent in the factorization of $n$, and is odd otherwise. In particular if 2 or more $p$ appear to odd exponent, then 4 divides $U$ and $V$. Next suppose there is exactly one prime $p$ occurring with odd exponent and that the exponent is $c$. Since $n \equiv 1 \pmod{8}$, $p \equiv 1 \pmod{8}$, and $\left( \frac{\,\cdot\,}{p} \right) = \left( \frac{\,\cdot\,}{p} \right) = 1$. So $p$ makes a contribution of $c + 1$ both to $U$ and to $V$. Since all the other contribution are odd, $U \equiv V \equiv 0 \pmod{4}$ when $c \equiv 3 \pmod{4}$, and $U \equiv V \equiv 2 \pmod{4}$ when $c \equiv 1 \pmod{4}$.

It remains to analyze the case $n = A^2$. In this case $U$ and $V$ are odd, and we are reduced to showing: if $A \equiv \pm 1 \pmod{8}$ then $UV \equiv 1 \pmod{4}$, while if $A \equiv \pm 3 \pmod{8}$, then $UV \equiv 3 \pmod{4}$. Consider $UV$ as an element of the multiplicative group $\{1, 3\}$ of $\mathbb{Z}/4$. $UV$ is a product of contributions, one for each prime dividing $A$. A $p \equiv \pm 1 \pmod{8}$ makes the same contribution to $U$ as to $V$ and so does not contribute to the product. If on the other hand $p \equiv \pm 3 \pmod{8}$ and has exponent $c$ in the factorization of $A$ then the contribution it makes to $UV$ is $(2c + 1) \cdot 1$ when $p \equiv 3 \pmod{8}$ and $1 \cdot (2c + 1)$ when $p \equiv -3 \pmod{8}$. In other words the contribution is $-1$ precisely when $c$ is odd. This tells us that $UV \equiv 1 \pmod{4}$ when the number of primes $\equiv \pm 3 \pmod{8}$ with odd exponent in the factorization of $A$ is even, and that $UV \equiv 3 \pmod{4}$ when this number is odd. But in the first case $A \equiv \pm 1 \pmod{8}$, while in the second $A \equiv \pm 3 \pmod{8}$.

**Definition 3.2.** Suppose $n$ is odd. $U_1$ is the number of ways of writing $n$ as $(\text{square}) + 2(\text{square})$ while $U_2$ is the number of ways of writing $n$ as $(\text{square}) + 4(\text{square})$.

**Lemma 3.3.** The number of ideals $U$ of $\mathbb{Z} \left[ \sqrt{-2} \right]$ of norm $n$ is $2U_1 - 1$ when $n$ is a square and $2U_1$ otherwise. The number of ideals $V$ of $\mathbb{Z}[i]$ of norm $n$ is $2V_1 - 1$ when $n$ is a square and $2V_1$ otherwise.

Proof. Suppose $n = s_1 + 2s_2$ with $s_1$ and $s_2$ squares. Then $\sqrt{s_1} + \sqrt{-2} \sqrt{s_2}$ and $\sqrt{s_1} - \sqrt{-2} \sqrt{s_2}$ generate ideals of norm $n$ in $\mathbb{Z} \left[ \sqrt{-2} \right]$. These 2 ideals are distinct except when $n$ is a square and $s_2 = 0$. Also every ideal of norm $n$ comes from exactly one such decomposition of $n$. This gives the first result and the proof of the second is similar.

Lemmas 3.1 and 3.3 immediately give:

**Lemma 3.4.** If $n \equiv 1 \pmod{16}$, then $U_1 \equiv V_1 \pmod{2}$.

**Lemma 3.5.** If $n \equiv 1 \pmod{16}$, then the coefficient of $x^n$ in $\frac{1}{y^n}$ is 1 if and only if $n$ is a square.
Proof. Since \( n \equiv 1 \pmod{8} \), the number of ways \( U_1 \) of writing \( n \) as \((\text{square}) + 2(\text{square})\) is the number of ways of writing \( n \) as \((\text{square}) + 8(\text{square})\). So the image of \( U_1 \) in \( \mathbb{Z}/2 \) is the coefficient of \( x^n \) in \( g \cdot g^8 = g^9 \). Similarly, the image of \( V_1 \) in \( \mathbb{Z}/2 \) is the coefficient of \( x^n \) in \( g \cdot g^{16} = g^{17} \). Lemma 3.4 then tells us that for \( n \equiv 1 \pmod{16} \) the coefficients of \( x^n \) in \( g^9 \) and in \( g^{17} \) are equal.

Now let \( S \subseteq A \) be \( \mathbb{Z}/2[[x^{16}]] \). As \( S \)-module \( A \) is the direct sum of the \( x^j S \) for \( j \leq 15 \). Let \( pr : A \to xS \) be the \( S \)-linear map that is the identity on \( xS \) and 0 on the other summands. The last paragraph tells us that \( pr(g^9) = pr(g^{17}) \).

Since \( \frac{1}{g^r} \) is in \( S \), \( pr \left( \frac{1}{g^r} \right) = pr(g) \). But as \( n \equiv 1 \pmod{16} \), the coefficient of \( x^n \) in \( pr(g) \) is the coefficient of \( x^n \) in \( g \), giving the result.

\[ \square \]

Theorem 3.6. If \( n \equiv 7 \pmod{16} \) then \( n \) is in \( B \) if and only if the number of ways of writing \( n \) as \((\text{square}) + 2(\text{square}) + 4(\text{square})\) is odd.

Proof. \( \frac{1}{g} = g^2 \cdot g^4 \cdot \frac{1}{g} \). So the coefficient of \( x^n \) in \( \frac{1}{g} \) is the number of ways, modulo 2, of writing \( n \) as \( 2(\text{square}) + 4(\text{square}) + k \) with the coefficient of \( x^k \) in \( \frac{1}{g} \) equal to 1. Suppose we have such a representation of \( n \). Then \( k \) is odd. Since \( \frac{1}{g^r} = \frac{1}{g} \), it follows that \( k \equiv 1 \pmod{8} \). A congruence mod 16 argument using the fact that \( n \equiv 7 \pmod{16} \) shows that \( k \equiv 1 \pmod{16} \), and Lemma 3.5 tells us that \( k \) is a square. Conversely suppose \( n = 2(\text{square}) + 4(\text{square}) + k \), where \( k \) is a square. Then \( k \equiv 1 \pmod{8} \) and our congruence mod 16 argument tells us that \( k \equiv 1 \pmod{16} \). By Lemma 3.5, the coefficient of \( x^k \) in \( \frac{1}{g^r} \) is 1, and this completes the proof.

\[ \square \]

Lemma 3.7. Let \( R_3 \) be the number of ways of writing \( 2n \) as \((\text{square}) + (\text{square}) + (\text{square})\). Then if \( n \equiv 7 \pmod{8} \), \( R_3 = 6 \cdot \text{(the number of ways of writing } n \text{ as } (\text{square}) + 2(\text{square}) + 4(\text{square})\).)

Proof. Suppose \( 2n = s_1 + s_2 + s_3 \) with the \( s_i \) squares. A congruence mod 16 argument shows that the \( s_i \), in some order, are \( 1, 4 \) and \( 9 \) mod 16. So \( R_3 = 6 \cdot \text{(the number of ways of writing } 2n \text{ as } s_1 + s_2 + s_3 \text{ with the } s_i \text{ squares, } s_1 \equiv 1 \pmod{16}, s_2 \equiv 4 \pmod{16}, s_3 \equiv 9 \pmod{16} \)). Suppose we have such a representation. Then we can choose square roots of \( s_1 \) and \( s_3 \) congruent to \( 1 \) and \( 5 \) respectively mod 8. Then \( n = \left( \frac{\sqrt{s_1} + \sqrt{s_3}}{2} \right)^2 + 2 \left( \frac{s_2}{4} \right) + 4 \left( \frac{\sqrt{s_1} - \sqrt{s_3}}{4} \right)^2 = (\text{square}) + 2(\text{square}) + 4(\text{square}) \). Conversely suppose \( n = t_1 + 2t_2 + 4t_3 \) with the \( t_i \) squares. Then the \( t_i \) are odd. Choose square roots of \( t_1 \) and \( t_3 \) that are \( 1 \) (4). Then \( 2n = \left( 2\sqrt{t_3} - \sqrt{t_1} \right)^2 + 4t_2 + \left( 2\sqrt{t_3} + \sqrt{t_1} \right)^2 \), and the three squares appearing in this decomposition are, in order, congruent mod 16 to 1, 4 and 9. In this way we get a 1–1 correspondence that establishes the result.

\[ \square \]

Combining Theorem 3.6 and Lemma 3.7 we get:
Theorem 3.8. An \( n \equiv 7 \ (16) \) is in \( B \) if and only if the \( R_3 \) of Lemma 3.7 is \( \equiv 2 \ (4) \).

Lemma 3.9. Suppose \( n \equiv 7 \ (8) \) and is divisible by 3 or more different primes. Then the number of ways of writing \( 2n \) primitively as \((\text{square})+(\text{square})+(\text{square})\) is divisible by 4.

Proof. Let \( \mathcal{O} = \mathbb{Z}[\sqrt{-2n}] \). When we write \( 2n \) as \((\text{square})+(\text{square})+(\text{square})\), the summands, being \( \equiv 1, 4 \) and 9 mod 16 are non-zero and distinct. So the number we’re talking about is \( \frac{1}{8} \cdot (\text{the number of primitive representations of } 2n \text{ by the form } x^2 + y^2 + z^2). \) In [2] Gauss showed that this (in modern language) is \( \frac{1}{8} \cdot 12 \cdot (\text{the number of invertible ideal classes in } \mathcal{O}). \) Let \( m \) be the number of different primes dividing \( 2n \). Gauss’ genus theory tells us that the group of invertible ideal classes maps onto a product of \( m - 1 \) copies of \( \mathbb{Z}/2 \). Since \( m \geq 4 \) we’re done.

Corollary 3.10. If \( n \equiv 7 \ (8) \) and 3 or more different primes occur to odd exponent in the factorization of \( n \), then the \( R_3 \) of Lemma 3.7 is divisible by 4.

Proof. For \( a^2 \) dividing \( 2n \), Lemma 3.9 shows that the number of ways of writing \( 2n/a^2 \) primitively as \((\text{square})+(\text{square})+(\text{square})\) is a multiple of 4. Summing over \( a \) gives the result.

Theorem 3.11. If \( n \equiv 7 \ (16) \) and 3 or more primes occur to odd exponent in the factorization of \( n \) then \( n \) is not in \( B \). Furthermore the number of \( n \) in \( B \) that are \( \leq x \) and \( \equiv 7 \ (16) \) is \( O(x \log \log(x)/\log(x)) \).

Proof. Theorem 3.8 and Corollary 3.10 give the first result, and we argue as in Theorem 2.4 to get the second.

Combining Theorems 1.3, 2.4 and 3.11 we get:

Theorem 3.12. The number of \( n \) in \( B \) that are \( \leq x \) and \( \not\equiv 15 \ (16) \) is \( O(x \log \log(x)/\log(x)) \). In particular the upper density of \( B \) is \( \leq \frac{1}{16} \).

Can one go further? A hope would be to find extensions of Theorems 1.1, 1.2 and 1.4 of this note that hold for \( n \equiv 7 \ (16) \), \( n \equiv 15 \ (32) \), \( n \equiv 31 \ (64) \), . . . . The authors of [1] claim that such extensions exist, but apart from \( n \equiv 7 \ (16) \), treated in this section, this seems unlikely. (The formulas they propose are incorrect.) There seems to be no theoretical evidence supporting the proposition that the \( n \equiv 15 \ (16) \) that lie in \( B \) form a set of density 0. As we’ll see in the next section the empirical evidence supports a quite different proposition.
Suppose \( x \) is in \( N \). There evidently are \( x \) positive integers that are \( \leq 16x \) and \( \equiv 15 \pmod{16} \). Let \( \beta = \beta(x) \) be the number of these integers that are in \( B \). Virtually nothing is known about the asymptotic growth of \( \beta \). But Kevin O’Bryant has calculated \( \beta \) for \( x \leq 2^{19} \), and his calculations show, for example:

(1) If \( x = 2^{16} \), the numbers of elements of \( B \) that are \( \equiv 15 \pmod{16} \) and lie in \([0, 16x], [16x, 32x], \ldots, [112x, 128x]\), are given respectively by \( \frac{x}{2} + 13, \frac{x}{2} + 94, \frac{x}{2} - 231, \frac{x}{2} + 207, \frac{x}{2} - 120, \frac{x}{2} + 14, \frac{x}{2} - 270 \) and \( \frac{x}{2} + 7 \).

(2) Suppose \( x \leq 2^{19} \) and is divisible by \( 2^{10} \). Then \( \beta = \frac{x}{2} + \alpha \sqrt{x} \) with \(-1.1 < \alpha < 0.58\). (The minimum of \( \alpha \) is attained at \( 5 \cdot 2^{10} \), and the maximum at \( 37 \cdot 2^{10} \).)

This provides evidence for the following “15 mod 16 conjecture”: For every \( \rho > \frac{1}{2} \), \( \beta = \frac{x}{2} + O(x^\rho) \).

Note that if the conjecture holds then Theorem 3.12 shows that \( B \) has density \( \frac{1}{32} \).

**Remark 4.1.** There is a related much studied problem. Let \( g^* \) in \( \mathbb{Z}/2[[x]] \) be \( 1 + x + x^3 + x^5 + x^7 + \cdots \) where the exponents are the generalized pentagonal numbers. Just as we used \( \frac{1}{g} \) to define \( B \) we can use \( \frac{1}{g^*} \) to define a set \( B^* \). (A famous result of Euler says that \( B^* \) consists of all \( n \) for which the number of partitions, \( p(n) \), of \( n \) is odd.) Let \( \beta^* = \beta^*(x) \) be the number of elements of \( B^* \) that are \( \leq x \). Despite extensive study only very weak results about the asymptotic growth of \( \beta^* \) have been proved. But Parkin and Shanks \[4\], on the basis of computer calculations, conjectured that for every \( \rho > \frac{1}{2} \), \( \beta = \frac{x}{2} + O(x^\rho) \). The resistance of this conjecture to attack suggests however that any proof of our 15 mod 16 conjecture is far off.

**References**

[1] Cooper J.N., Eichhorn D., O’Bryant K., Reciprocals of binary series, Int. J. Number Theory 2 (2006), 499–522.

[2] Gauss C.F., Disquisitiones Arithmeticæ(1801)—translated by Arthur A. Clarke, S.J., Yale University Press, New Haven, U.S. (1966).

[3] The On-Line Encyclopedia of Integer Sequences (OEIS).

[4] Parkin T.R., Shanks D., On the distribution of parity in the partition function, Math. Comp. 21 (1967), 466–480.