The reciprocals of some characteristic 2 "theta series"

Paul Monsky

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

Abstract

Suppose $l = 2m+1$, $m > 0$. We introduce m "theta-series", $[1], \dots, [m]$, in $\mathbb{Z}/2[[x]]$. It has been conjectured that the n for which the coefficient of x^n in $1/[i]$ is 1 form a set of density 0. This is probably always false, but in certain cases, for n restricted to certain arithmetic progressions, it is true. We prove such zero-density results using the theory of modular forms, and speculate about what may be true in general.

1 Introduction

Throughout L is a field of fractions of $\mathbb{Z}/2[[x]]$, viewed as the field of Laurent series with coefficients in $\mathbb{Z}/2$.

Definition 1.1. For $g \neq 0$ in $\mathbb{Z}/2[[x]]$, $B(g)$ is the set of n in $\mathbb{Z}$ for which the co-efficient of x^n in $1/g$ is 1. Note that only finitely many elements of $B(g)$ can be < 0.

Fix $l = 2m + 1$ with $m > 0$. We define certain "theta series" $[i]$ in $\mathbb{Z}/2[[x]]$.

Definition 1.2. $[i] = \sum x^{n^2}$, the sum extending over all n in $\mathbb{Z}$ with $n \equiv i$ (l). (Note that $[0] = 1$, and that $[i] = [j]$ whenever $i \equiv \pm j \ (l)$. So the ring S generated over $\mathbb{Z}/2$ by all the $[i]$ is just $\mathbb{Z}/2[[1], \dots, [m]]$.)

In this note we study the sets $B([r])$ for fixed l and r with r prime to l. Note that each j in $B([r])$ is $\equiv -r^2 \ (l)$ and that consequently $B([r])$ has (upper) density at most $1/l$ in the positive integers.

In [1], Cooper, Eichhorn and O'Bryant conjectured, in a slightly different language, that each $B([r])$ has density 0. I think this is never true, but we'll show that for certain l and r and in certain congruence classes $\bmod$ a power of 2, $B([r])$ indeed has relative density 0. For example when $l = 3$ the relative density is 0 in the classes $n \equiv 0 \ (2)$, $n \equiv 1 \ (4)$ and $n \equiv 3 \ (8)$. I'll now describe more precisely, what perhaps is true in general, and the small part of it I'm able to prove.

Definition 1.3. Fix l. $k < 0$ is "l-exceptional" if k is in some $B([r])$ with r prime to l. A "basic congruence class" is a congruence class of the form $n \equiv k \ (8q)$, where k is l-exceptional and q is the largest power of 2 dividing k.

Definition 1.4. An integer $n \geq 0$ is in U if it is in some basic congruence class, and in U^* otherwise.

Example 1. Suppose $l = 3$. Then $1/[1] = x^{-1} + \cdots$. So the only 3-exceptional k is -1 and the only basic class is $n \equiv -1 \ (8)$. U^* consists of the integers $n \geq 0$ with $n \equiv 0 \ (2)$, $n \equiv 1 \ (4)$, or $n \equiv 3 \ (8)$.

Example 2. Suppose $l = 9$. The only $[r]$ we need consider are $[1]$, $[2]$ and $[4]$. Now $1/[1] = x^{-1} + \cdots$, $1/[2] = x^{-4} + \cdots$ and $1/[4] = x^{-16} + x^{-7} + \cdots$. So the basic classes are $n \equiv 1$ or $-1 \ (8)$, $n \equiv -4 \ (32)$ and $n \equiv -16 \ (128)$. Then U consists of the integers ≥ 0 lying in $16 + 16 + 4 + 1 = 37$ congruence classes to the modulus 128, and U^* of the integers ≥ 0 in the remaining 91 classes.

It seems to me plausible that when r is prime to l then $B([r])$ has relative density 0 in U^*. I'll show that this holds for $l \leq 11$. When $l = 13$ or 15, then U^* is the union of 83 mod 128 congruence classes, and I'll prove that $B([r])$ has relative density 0 in each of these classes, with the possible exception of the class $n \equiv 48 \ (128)$. Unfortunately the proof is not unified—we have to write U^* as a union of congruence classes and examine each class in turn. To this end we now give the (easily proved) description of U^* as a union of congruence classes for each $l \leq 15$.

l	mod 2	mod 4	mod 8	mod 16	mod 32	mod 64	mod 128
3	0	1	3				
5		1, 2	0, 3	4	12		
7		1	0, 2, 3	4, 6	12		
9		2	3, 5	4, 8	0, 12	16	48
11			1, 3, 6	4, 8, 10	0, 12	16	48
13			2, 3, 5	4, 8, 14	0, 12	16	48
15			1, 2, 3	4, 6, 8	0, 12	16	48

Here's a rough description of how our proofs proceed. Fix l and $[r]$ and a congruence class $j \mod q$ where q is a power of 2. We'll construct a g in $\mathbb{Z}/2[[x]]$, depending on l, r, j and q, with the following properties:

(1) There are integers $c_0, c_1, \ldots$ such that:

  (A) $\sum c_n e^{2\pi i n z}$ converges in $\mathrm{Im}(z) > 0$ to a modular form of integral weight for a congruence group.

  (B) g is the mod 2 reduction of $\sum c_n x^n$

(2) Suppose that $g/[r]^q$ is itself the mod 2 reduction of some $\sum d_n x^n$ where $\sum d_n e^{2\pi i n z}$ converges to a modular form as in 1(A) above. Then $B([r])$ has density 0 in the congruence class $j \mod q$.

g is in fact the image of $[r]^{q-1}$ under a certain projection operator $p_{q,j}$ which we describe in the next section. The fact that g is "the reduction of a modular form" comes from a corresponding result for $[r]$; $[r]$ is the reduction of a weight 1 modular form. (The proof of (2) is deeper, coming from a result of Deligne and Serre on the reduction of modular forms.) Once (1) and (2) are established we still need to show that for each of our choices of l, $[r]$, and the congruence class $j \mod q$ lying in U^*, the power series $g/[r]^q$ satisfies the condition (2) above. This is true, for example, whenever $g/[r]^q$ lies in the ring S of Definition 1.2. In certain cases, extensive computer calculations tell us that $g/[r]^q$ lies in S.

At the end of the paper we'll speculate on the relative density of $B([r])$ in the basic classes. Though we are unable to prove anything, computer calculations suggest that each $B([r])$ has relative density $1/(2l)$ in each basic class.

2 The operators $p_{q,j}$ and the case $l = 3$

If q is a power of 2, let $L^{[q]} \subset L$ consist of all qth powers of elements of L. L is the direct sum of the $L^{[q]}$ vector-spaces $x^j L^{[q]}, 0 \le j < q$.

Definition 2.1. $p_{q,j} L \to x^j L^{[q]}$ is the $L^{[q]}$-linear projection map attached to the above direct sum decomposition.

Note that $p_{q,j}(FG) = \sum p_{q,a}(F) p_{q,b}(G)$, the sum extending over all pairs (a, b) with $a + b \equiv j \ (q)$. Furthermore $p_{2q,2j}(F^2) = (p_{q,j}(F))^2$. We'll use these facts often.

Lemma 2.2. Fix $l = 2m + 1$. Then:

(1) $p_{2,0}([2i]) = [i]^4$

(2) The subring S of L generated over $\mathbb{Z}/2$ by all the $[i]$ is stabilized by the operators $p_{8,0}, \ldots, p_{8,7}$.

Proof. Since $[2i] = \sum_{n\equiv 2i\ (l)} x^{n^2}$, $p_{2,0}([2i]) = \sum_{k\equiv i\ (l)} x^{4k^2} = [i]^4$.

In view of the formula for $p_{8,j}(FG)$, to prove (2) it suffices to show that $p_{8,0}([i]), \ldots, p_{8,7}([i])$ are all in the subring. Now if $j \neq 0$, 1 or 4, each $p_{8,j}([i])$ is 0. Since every odd square is $\equiv 1\ (8)$, $p_{8,1}([2i]) = p_{2,1}([2i]) = [2i] + [i]^4$. Also $p_{8,0}([4i]) = p_{8,0}p_{2,0}([4i]) = p_{8,0}\left([2i]^4\right) = \left(p_{2,0}([2i])\right)^4 = [i]^{16}$. Similarly, $p_{8,4}([4i]) = \left(p_{2,1}([2i])\right)^4 = [2i]^4 + [i]^{16}$. ☐

Suppose for the rest of this section that $l = 3$. In this case the proofs of zero-density in U^* are much easier than the proofs for $l > 3$, requiring neither modular forms nor computer calculations. Observe that if 3 doesn't divide i, then $[i] = 1$.

Definition 2.3. $a = [1] = [2]$. Note that $p_{2,0}(a) = a^4$.

Theorem 2.4. Suppose $n \equiv 0\ (2)$ and n is in $B(a)$. Then $n/2$ is a square.

Proof. $p_{2,0}\left(\frac{1}{a}\right) = \frac{1}{a^2}p_{2,0}(a) = a^2$. Since n is in $B(a)$ and is even, the coefficient of x^n in a^2 is 1, giving the result. ☐

Theorem 2.5. Suppose $n \equiv 1\ (4)$ and n is in $B(a)$. Then the number of pairs (s_1, s_2) with s_1 and s_2 squares, and $s_1 + 4s_2 = n$ is odd. Furthermore n is the product of a prime and a square.

Proof. $p_{4,1}\left(\frac{1}{a}\right) = \frac{1}{a^4}p_{4,1}(a^3) = \frac{1}{a^4}p_{4,1}(a)p_{4,1}(a^2) = \frac{1}{a^4}\left(a + a^4\right)a^8 = a^5 + a^8$. Since n is in $B(a)$ and is $\equiv 1\ (4)$, the coefficient of x^n in $a^5 + a^8$ is 1, and so the coefficient in $a^5 = a{\cdot}a^4$ is 1. So the number of pairs (r_1, r_2) with $r_1 \equiv r_2 \equiv 1$ (3) and $r_1^2 + 4r_2^2 = n$ is odd. To each such pair attach the pair (s_1, s_2) with s_1 and s_2 squares, $s_1 + 4s_2 = n$, by setting $s_i = r_i^2$. The function from pairs (r_1, r_2) to pairs (s_1, s_2) is 1–1. Since n is in $B(a)$, $n \equiv -1\ (3)$. So whenever we have a pair (s_1, s_2) as above, s_1 and s_2 are $\equiv 1\ (3)$ and have square roots $\equiv 1$ (3). So the function $(r_1, r_2) \to (s_1, s_2)$ is onto, and we get the first assertion of the theorem. A little arithmetic in $\mathbb{Z}[i]$ gives the second assertion. ☐

Lemma 2.6. If $n \equiv 3\ (8)$, n is in $B(a)$ if and only if the number of triples (r_1, r_2, r_3) with $r_1 \equiv r_2 \equiv r_3 \equiv 1\ (3)$ and $r_1^2 + 2r_2^2 + 8r_3^2 = n$ is odd.

Proof. $p_{8,3}\left(\frac{1}{a}\right) = \frac{1}{a^8}p_{8,3}\left(a \cdot a^2 \cdot a^4\right) = \frac{1}{a^8}p_{8,1}(a)p_{8,2}\left(a^2\right)p_{8,0}\left(a^4\right) = \frac{1}{a^8}\left(a + a^4\right)$ $\left(a + a^4\right)^2 a^{16} = a^{11} + a^{14} + a^{17} + a^{20}$. Since $n \equiv 3\ (8)$ the coefficients of x^n in

a^{14}, a^{20}, and $a^{17} = a \cdot a^{16}$ are evidently 0. So n is in $B(a)$ if and only if the coefficient of x^n in $a^{11} = a \cdot a^2 \cdot a^8$ is 1, giving the lemma. □

Lemma 2.7. If $n \equiv 11\ (24)$ the number of triples (s_1, s_2, s_3) where the s_i are squares and $s_1 + s_2 + s_3 = n$ is 3·(the number of triples (r_1, r_2, r_3) as in Lemma 2.6).

Proof. If the s_i are as above, two of them are $\equiv 1\ (3)$ while 3 divides the third. So our lemma states that the number of triples (s_1, s_2, s_3) with the s_i squares, $s_1 + s_2 + s_3 = n$ and $s_3 \equiv 0\ (3)$ is the number of triples (r_1, r_2, r_3) as in Lemma 2.6. If we have a triple (r_1, r_2, r_3) let $s_1 = r_1^2$, $s_2 = (r_2 - 2r_3)^2$, $s_3 = (r_2 + 2r_3)^2$. Then the s_i are squares, $s_3 \equiv 0\ (3)$ and $s_1 + s_2 + s_3 = r_1^2 + 2r_2^2 + 8r_3^2 = n$. That $(r_1, r_2, r_3) \to (s_1, s_2, s_3)$ is 1–1 is easily seen. To prove ontoness suppose we're given (s_1, s_2, s_3). Then s_1 and s_2 are $\equiv 1\ (3)$ and have square roots, $\sqrt{s_1}$ and $\sqrt{s_2}$, that are $\equiv 1\ (3)$. Also, since $n \equiv 3\ (8)$, the s_i are odd. So we can find a square-root, $\sqrt{s_3}$ of s_3 with $\sqrt{s_3} \equiv \sqrt{s_2}\ (4)$. Then the triple $\left(\sqrt{s_1}, \frac{-\sqrt{s_2}-\sqrt{s_3}}{2}, \frac{\sqrt{s_2}-\sqrt{s_3}}{4}\right)$ has its entries $\equiv 1\ (3)$ and maps to (s_1, s_2, s_3). □

Theorem 2.8. Suppose $n \equiv 3\ (8)$ and n is in $B(a)$. Then the number of pairs (s_1, s_2) with s_1 and s_2 squares and $s_1 + 2s_2 = n$ is odd. Furthermore, n is the product of a prime and a square.

Proof. Consider the set of triples (s_1, s_2, s_3) where the s_i are squares and $s_1 + s_2 + s_3 = n$. Since n is in $B(a)$, and $n \equiv 3\ (8)$, $n \equiv 11\ (24)$. Lemmas 2.6 and 2.7 then show that the number of such triples is odd. Now $(s_1, s_2, s_3) \to (s_1, s_3, s_2)$ is an involution on the set of such triples whose fixed points identify with the pairs (s_1, s_2) as in the statement of the theorem. This gives the first assertion of the theorem, and a little arithmetic in $\mathbb{Z}[\sqrt{-2}]$ gives the second. □

Theorem 2.9.

(1) Every element n of $B(a)$ that lies in U^* is the product of a prime and a square.
(2) The number of elements of $B(a)$ that are $\leq x$ and lie in U^* is $O(x/\log x)$.

Proof. The elements of U^* are $\equiv 0\ (2)$, $1\ (4)$, or $3\ (8)$, and we use Theorems 2.4, 2.5 and 2.8 to get (1). (2) is an immediate consequence. □

Remark 1. The proof of Theorem 2.9 is easier than that of a similar result in Monsky [2], which makes use of results of Gauss on representations by sums of 3 squares.

Remark 2. The set $B(a + a^4)$ has been more extensively studied. One sees immediately that $a + a^4 = \sum x^{1+24s}$, where s runs over the generalized pentagonal numbers $0, 1, 2, 5, 7, 12, 15, \ldots$. So the elements of $B(a + a^4)$ are all $\equiv -1$ (24). The mod 2 reduction of a famous identity of Euler tells us that $24k - 1$ is in $B(a + a^4)$ if and only if the number of partitions, $p(k)$, of k is odd. Large-scale computer calculations suggest very strongly that the k for which $p(k)$ is odd have density 1/2, so that $B(a + a^4)$ has relative density 1/2 in the congruence class $n \equiv -1$ (24). It's tempting to believe that $B(a)$ also has relative density 1/2 in this congruence class. This would be in line with the (modest) computer calculations that have been made; see our final section.

3 Enter modular forms. The quintic theta relations

In the proofs of section 2 we expressed $p_{2,0}\left(\frac{1}{a}\right)$, $p_{4,1}\left(\frac{1}{a}\right)$, and $p_{8,3}\left(\frac{1}{a}\right)$ as elements of $\mathbb{Z}/2[a]$, and were able to deduce that $B(a)$ has density 0 in the congruence classes $n \equiv 0$ (2), $n \equiv 1$ (4) and $n \equiv 3$ (8). (Note that $p_{8,7}\left(\frac{1}{a}\right)$ is not in $\mathbb{Z}/2[a]$. Indeed $p_{8,7}\left(\frac{1}{a}\right) = x^{-1} + \cdots$ and is not even in $\mathbb{Z}/2[[x]]$). In our treatment of larger l we'll use a similar idea, but in most cases we'll have to rely on a deep result on modular forms due to Deligne and Serre. My thanks go to David Rohrlich for telling me about this result.

The following is well-known; for a more general theorem on definite quadratic forms in an even number of variables see Schöneberg [4].

Theorem 3.1. $\sum\sum \mathrm{e}^{2\pi i(m^2+n^2)z}$, the sum extending over all pairs (m, n) with m and n in $\mathbb{Z}$ and $n \equiv$ some $j \mod l$, converges in $\mathrm{Im}(z) > 0$ to a weight 1 modular form for a congruence group.

Corollary 3.2. Fix l. Let $u = \sum a_s x^s$ be a product of powers of various $[j]$. Then there are integers $c_0, c_1, \ldots$ such that:

(A) $\sum c_n \mathrm{e}^{2\pi i n z}$ converges in $\mathrm{Im}(z) > 0$ to a modular form of integral weight for a congruence group.
(B) The mod 2 reduction of c_s is a_s.

Proof. It's enough to show this when $u = [j]$. We take our modular form to be that of Theorem 3.1. If we write this form as $\sum c_s \mathrm{e}^{2\pi i s z}$, then (A) is satisfied. Furthermore c_s is the number of pairs (m, n) with $n \equiv j$ (l) and $m^2 + n^2 = s$. $(m, n) \to (-m, n)$ is an involution on this set of pairs. There is one fixed point if s is the square of some $n \equiv j$ (l), and no fixed point otherwise. It follows that the mod 2 reduction of c_s is a_s. ☐

Now fix l. Recall that S is the subring of $\mathbb{Z}/2[[x]]$ generated over $\mathbb{Z}/2$ by all the $[j]$.

Theorem 3.3. If $u = \sum a_n x^n$ is in S, then the set of n for which a_n is 1 has density 0.

Proof. We may assume that u is a product of powers of various $[j]$. As we've seen, there are c_n in $\mathbb{Z}$, with c_n reducing to a_n mod 2, such that $\sum c_n \mathrm{e}^{2\pi i n z}$ converges in $\mathrm{Im}(z) > 0$ to a modular form of integral weight for a congruence group. A theorem of Serre [5], based on results of Deligne attaching Galois representations to Hecke eigenforms, shows that the n for which 2 does not divide c_n form a set of density 0. $\square$

Corollary 3.4. Suppose that $p_{q,j}\,(1/[r])$ is in S, or more generally is in $p_{q,j}(S)$. Then $B([r])$ has relative density 0 in the congruence class $j \mod q$.

Now $p_{q,j}\,(1/[r]) = (1/[r]^q)\, p_{q,j}\,([r]^{q-1})$. But to show that this quotient lies in $p_{q,j}(S)$ for various choices of j and q seems very difficult. There is however a technique for showing that a quotient of two elements of S lies in S that makes use of certain "quintic theta relations".

Lemma 3.5. $p_{2,0}\,([2i][2j]) = [i+j]^2[i-j]^2$.

Proof. It suffices to show that the coefficients of x^{2n} on the two sides are equal. On the left one has the mod 2 reduction of the number of pairs (r,s) with $r \equiv 2i\ (l)$, $s \equiv 2j\ (l)$ and $r^2+s^2 = 2n$. On the right one has the mod 2 reduction of the number of pairs (t,u) with $t \equiv i+j\ (l)$, $u \equiv i-j\ (l)$ and $t^2+u^2 = n$. Clearly $(r,s) \to \left(\frac{r+s}{2}, \frac{r-s}{2}\right)$ gives the desired bijection. $\square$

Theorem 3.6. $[i]^4[2j] + [j]^4[2i] + [2i][2j] + [i+j]^2[i-j]^2 = 0$.

Proof. $p_{2,0}\,([2i][2j]) = p_{2,0}([2i])p_{2,0}([2j]) + p_{2,1}([2i])p_{2,1}([2j]) = [i]^4[j]^4 + ([i]^4+[2i])\,([j]^4+[2j])$. Now use Lemma 3.5. $\square$

Let $x_1, \ldots, x_m$ (where $l = 2m+1$) be indeterminates over $\mathbb{Z}/2$.

Definition 3.7. If r is prime to l, ϕ_r is the homomorphism $\mathbb{Z}/2[x_1, \ldots, x_m] \to S$ taking x_k to $[rk]$.

Note that each ϕ_r is onto. We'll use Theorem 3.6 to construct $\frac{m(m-1)}{2}$ elements of $\mathbb{Z}/2[x_1, \ldots, x_m]$ lying in the kernel of each ϕ_r.

Theorem 3.8. Suppose that $m \ge i > j \ge 1$. For $1 \le k \le m$ define x_{l-k} to be x_k, so that we have elements $x_1, \ldots, x_{2m}$ of $\mathbb{Z}/2[x_1, \ldots, x_m]$. Then if we define $R_{i,j}$ to be $x_i^4 x_{2j} + x_j^4 x_{2i} + x_{2i}x_{2j} + x_{i+j}^2 x_{i-j}^2$, each $R_{i,j}$ is in the kernel of each ϕ_r.

Proof. The definition of $x_{m+1},\ldots,x_{2m}$ shows that $\phi_r(x_k) = [rk]$ for $k = 1,\ldots,2m$. The result now follows from Theorem 3.6 on replacing i and j by ri and rj throughout. □

Theorem 3.9. Let u and v be elements of $\mathbb{Z}/2[x_1,\ldots,x_m]$, and N the ideal in this ring generated by the $R_{i,j}$. Suppose that the ideals (N,v) and (N,u,v) are the same. Then the element $\phi_r(u)/\phi_r(v)$ of the field of fractions of S in fact lies in S.

Proof. u is in (N,v). Applying ϕ_r and using Theorem 3.9 we find that in S, $\phi_r(u)$ lies in the principal ideal $\phi_r(v)$. □

Remark. Commutative algebra computer programs such as Macaulay 2 use Gröbner bases to decide whether 2 ideals in a polynomial ring are equal. We shall use such a program to show that in many cases of interest the quotient $\phi_r(u)/\phi_r(v)$ lies in S.

There is one further simple result that we'll use frequently in the calculations to follow.

Lemma 3.10. Suppose that for some a and b, $p_{2,0}(a) = b^4$. Then:

(1) $p_{2,0}\left(\frac{1}{a}\right) = \frac{b^4}{a^2}$
(2) $p_{4,0}\left(\frac{1}{a}\right) = \frac{b^{12}}{a^4}$
(3) $p_{8,0}\left(\frac{1}{a}\right) = \frac{b^8}{a^8}\left(p_{2,0}(ab)\right)^4$

Proof. $p_{2,0}\left(\frac{1}{a}\right) = \frac{1}{a^2}p_{2,0}(a) = \frac{b^4}{a^2}$. Then $p_{4,0}\left(\frac{1}{a}\right) = p_{4,0}p_{2,0}\left(\frac{1}{a}\right) = p_{4,0}\left(\frac{b^4}{a^2}\right) = b^4\left(p_{2,0}\left(\frac{1}{a}\right)\right)^2 = \frac{b^{12}}{a^4}$. Furthermore, $p_{8,0}\left(\frac{1}{a}\right) = p_{8,0}p_{4,0}\left(\frac{1}{a}\right) = p_{8,0}\left(\frac{b^{12}}{a^4}\right) = \frac{b^8}{a^8}p_{8,0}\left(a^4b^4\right)$, giving the last result. □

4 $l = 5$

In this section $l = 5$, so that $m = 2$. Then the ideal N of Theorem 3.9 is generated by the single element $R_{2,1} = x_2^4x_2 + x_1^4x_4 + x_4x_2 + x_3^2x_1^2 = x_1^5 + x_2^5 + x_1x_2 + x_1^2x_2^2$. Now let $r = 1$ or 2 and set $a = [r]$, $b = [2r]$. Then $p_{2,0}(a) = b^4$, $p_{2,0}(b) = a^4$ and we have the quintic relation $a^5 + b^5 + ab + a^2b^2 = 0$.

We'll use the techniques sketched in the last section to show that $p_{4,1}\left(\frac{1}{a}\right)$, $p_{4,2}\left(\frac{1}{a}\right)$, $p_{8,0}\left(\frac{1}{a}\right)$, $p_{8,3}\left(\frac{1}{a}\right)$, $p_{16,4}\left(\frac{1}{a}\right)$ and $p_{32,12}\left(\frac{1}{a}\right)$ are all in S. Corollary 3.4 in conjunction with the description of U^* given in the introduction when $l = 5$ then tells us that $B(a)$ has relative density 0 in U^*.

Theorem 4.1. $p_{8,0}\left(\frac{1}{a}\right) = b^{16}$.

Proof. By Lemma 3.10, $p_{8,0}\left(\frac{1}{a}\right) = \frac{b^8}{a^8}\left(p_{2,0}(ab)\right)^4$. Now $p_{2,0}(ab) = p_{2,0}([4r][2r]) = [3r]^2 \cdot [r]^2 = a^2b^2$. ☐

Theorem 4.2. $p_{4,2}\left(\frac{1}{a}\right)$, $p_{4,1}\left(\frac{1}{a}\right)$ and $p_{8,3}\left(\frac{1}{a}\right)$ are in S.

Proof. We first write these power series as quotients of elements of S.

(1) $p_{4,2}\left(\frac{1}{a}\right) = p_{2,0}\left(\frac{1}{a}\right) + p_{4,0}\left(\frac{1}{a}\right) = \frac{b^4}{a^2} + \frac{b^{12}}{a^4} = \left(\frac{b^4}{a^4}\right)(a^2+b^8)$.

(2) $p_{4,1}\left(\frac{1}{a}\right) = \left(\frac{1}{a^4}\right)p_{4,1}(a)p_{4,0}(a^2) = \left(\frac{1}{a^4}\right)p_{2,1}(a)\left(p_{2,0}(a)\right)^2 = \left(\frac{b^8}{a^4}\right)(a+b^4)$.

(3) $p_{8,3}\left(\frac{1}{a}\right) = \left(\frac{1}{a^8}\right)p_{8,1}(a)p_{8,2}(a^2)p_{8,0}(a^4) = \left(\frac{1}{a^8}\right)p_{2,1}(a)\left(p_{2,1}(a)\right)^2\left(p_{2,0}(a)\right)^4 = \left(\frac{b^{16}}{a^8}\right)(a+b^4)^3$.

In view of (1), (2) and (3) it will suffice to show that $\frac{b^2}{a^2}(a+b^4)$ and $\frac{b^8}{a^4}(a+b^4)$ are each in S. This can be done by hand, but in the mechanized spirit of the paper I'll give a computer argument. First let $u = x_2^2(x_1+x_2^4)$ and $v = x_1^2$. Macaulay 2 tells us that $(N, v) = (N, u, v)$. So by Theorem 3.9, $\phi_r(u)/\phi_r(v)$ is in S. But $\phi_r(u)/\phi_r(v) = \frac{b^2}{a^2}(a+b^4)$. For the second result we argue similarly taking $u = x_2^8(x_1+x_2^4)$ and $v = x_1^4$. ☐

Lemma 4.3. $p_{8,4}\left(\frac{1}{a}\right) + \left(p_{2,1}\left(\frac{1}{b}\right)\right)^4 = a^4 + b^{16}$.

Proof. $p_{8,4}\left(\frac{1}{a}\right) = p_{4,0}\left(\frac{1}{a}\right) + p_{8,0}\left(\frac{1}{a}\right) = \frac{b^{12}}{a^4} + b^{16}$, by Lemma 3.10 and Theorem 4.1. Furthermore $p_{2,1}\left(\frac{1}{b}\right) = \frac{1}{b} + p_{2,0}\left(\frac{1}{b}\right) = \frac{1}{b} + \frac{a^4}{b^2}$. So the left hand side in the statement of Lemma 4.3 is $b^{16} + \left(\frac{b^3}{a} + \frac{1}{b} + \frac{a^4}{b^2}\right)^4$. But the quintic relation $a^5 + b^5 + ab + a^2b^2 = 0$ tells us that $\frac{b^3}{a} + \frac{1}{b} + \frac{a^4}{b^2} = \frac{1}{ab^2}(b^5 + ab + a^5) = a$. ☐

Theorem 4.4. $p_{16,4}\left(\frac{1}{a}\right)$ and $p_{32,12}\left(\frac{1}{a}\right)$ are in S.

Proof. Applying $p_{16,4}$ to the identity of Lemma 4.3 we find that $p_{16,4}\left(\frac{1}{a}\right) + \left(p_{4,1}\left(\frac{1}{b}\right)\right)^4 = \left(p_{4,1}(a)\right)^4 = a^4 + b^{16}$. But Theorem 4.2 (with r replaced by $2r$) tells us that $p_{4,1}\left(\frac{1}{b}\right)$ is in S. Applying $p_{32,12}$ to the identity of Lemma 4.3 we find that $p_{32,12}\left(\frac{1}{a}\right) + \left(p_{8,3}\left(\frac{1}{b}\right)\right)^4 = \left(p_{8,3}(a)\right)^4 = 0$. And Theorem 4.2 (with r replaced by $2r$) shows that $p_{8,3}\left(\frac{1}{b}\right)$ is in S. ☐

5 $l = 7$

In this section $l = 7$. Then $m = 3$ and the ideal N is generated by $x_1^5 + x_3^4 x_2 + x_1 x_2 + x_2^2 x_3^2$, $x_2^5 + x_1^4 x_3 + x_2 x_3 + x_3^2 x_1^2$ and $x_3^5 + x_2^4 x_1 + x_3 x_1 + x_1^2 x_2^2$. Let r be 1, 2 or 3, $a = [r]$, $b = [4r]$, $c = [2r]$. Then $p_{2,0}$ takes a, b and c to b^4, c^4 and a^4. Lemma 3.5 shows that $p_{2,0}$ takes ab, bc and ac to a^2c^2, a^2b^2 and b^2c^2. We'll prove that $B(a)$ has relative density 0 in U^* by showing that each of $p_{4,1}\left(\frac{1}{a}\right)$, $p_{8,0}\left(\frac{1}{a}\right)$, $p_{8,2}\left(\frac{1}{a}\right)$, $p_{8,3}\left(\frac{1}{a}\right)$, $p_{16,4}\left(\frac{1}{a}\right)$, $p_{16,6}\left(\frac{1}{a}\right)$ and $p_{32,12}\left(\frac{1}{a}\right)$ is in S.

Remark. In this case, as in the case $l = 5$, N is the kernel of each ϕ_r. This is not true when $l = 9$. Whether it holds for all prime l is an interesting question.

Theorem 5.1. $p_{8,0}\left(\frac{1}{a}\right) = b^8 c^8$, and $p_{8,2}\left(\frac{1}{a}\right) = (a^2 + b^8)\, c^8$.

Proof. By Lemma 3.10, $p_{8,0}\left(\frac{1}{a}\right) = \left(\frac{b^8}{a^8}\right)(p_{2,0}(ab))^4 = b^8c^8$. Also, $p_{8,2}\left(\frac{1}{a}\right) = p_{8,2}p_{2,0}\left(\frac{1}{a}\right) = p_{8,2}\left(\frac{b^4}{a^2}\right) = \left(p_{4,1}\left(\frac{b^2}{a}\right)\right)^2$. And $p_{4,1}\left(\frac{b^2}{a}\right) = \frac{1}{a^4}p_{4,1}(a)p_{4,0}(a^2b^2) = \frac{1}{a^4}p_{2,1}(a)\left(p_{2,0}(ab)\right)^2 = (a + b^4)\cdot c^4$. □

Theorem 5.2. $p_{4,1}\left(\frac{1}{a}\right)$, $p_{8,3}\left(\frac{1}{a}\right)$ and $p_{16,6}\left(\frac{1}{a}\right)$ are in S.

Proof. Again we first write these power series as quotients of elements in S.

(1) The proof of Theorem 4.2 shows that $p_{4,1}\left(\frac{1}{a}\right) = \frac{b^8}{a^4}(a + b^4)$, and that $p_{8,3}\left(\frac{1}{a}\right) = \frac{b^{16}}{a^8}\left(a + b^4\right)^3$.

(2) $p_{16,6}\left(\frac{1}{a}\right) = p_{16,6}p_{2,0}\left(\frac{1}{a}\right) = p_{16,6}\left(\frac{b^4}{a^2}\right) = \left(p_{8,3}\left(\frac{b^2}{a}\right)\right)^2$. Now $p_{8,3}\left(\frac{b^2}{a}\right) = \frac{1}{a^8}p_{8,1}(a)p_{8,0}(a^4)p_{8,2}(a^2b^2) = \frac{1}{a^8}p_{2,1}(a)\left(p_{2,0}(a)\right)^4\cdot\left(p_{4,1}(ab)\right)^2$. Now $p_{4,3}(ab) = 0$, and it follows that $p_{4,1}(ab) = p_{2,1}(ab) = ab + p_{2,0}(ab) = ab + a^2c^2$. So $p_{8,3}\left(\frac{b^2}{a}\right) = \left(\frac{b^{16}}{a^8}\right)(a + b^4)(a^2b^2 + a^4c^4)$.

We can now use the technique of the last section to prove the theorem. It suffices to show that $\left(\frac{b^8}{a^4}\right)(a + b^4)$ and $\left(\frac{b^{16}}{a^8}\right)(a + b^4)(a^2b^2 + a^4c^4)$ are in S. To prove the second result we take u to be $x_3^{16}(x_1 + x_3^4)(x_1^2x_3^2 + x_1^4x_2^4)$, and v to be x_1^8. Macaulay 2 verifies that $(N, v) = (N, u, v)$. So $\phi_r(u)/\phi_r(v)$ is in S, as desired. The first result is proved similarly. □

Lemma 5.3. $p_{8,4}\left(\frac{1}{a}\right) + \left(p_{4,2}\left(\frac{1}{c}\right)\right)^2 = u^4$ for some u in S.

Proof. $p_{8,4}\left(\frac{1}{a}\right) = p_{4,0}\left(\frac{1}{a}\right) + p_{8,0}\left(\frac{1}{a}\right)$. By Lemma 3.10 and Theorem 5.1, this is $\frac{b^{12}}{a^4} + b^8c^8$. And $p_{4,2}\left(\frac{1}{c}\right) = p_{2,0}\left(\frac{1}{c}\right) + p_{4,0}\left(\frac{1}{c}\right) = \frac{a^4}{c^2} + \frac{a^{12}}{c^4}$. So the left-hand side in the statement of the lemma is the fourth power of $\frac{b^3}{a} + b^2c^2 + \frac{a^2}{c} + \frac{a^6}{c^2}$. To show that $\frac{b^3}{a}+\frac{a^2}{c}+\frac{a^6}{c^2}$ is in S, we write it as a quotient, $\frac{b^3c^2+a^3c+a^7}{ac^2}$, and use our Macaulay 2 technique. □

Theorem 5.4. $p_{16,4}\left(\frac{1}{a}\right)$ and $p_{32,12}\left(\frac{1}{a}\right)$ are in S.

Proof. Applying $p_{16,4}$ to the identity of Lemma 5.3 we find that $p_{16,4}\left(\frac{1}{a}\right)+\left(p_{8,2}\left(\frac{1}{c}\right)\right)^2=(p_{4,1}(u))^4$. Now Theorem 5.1 (with r replaced by $2r$) shows that $p_{8,2}\left(\frac{1}{c}\right)$ is in S. Since S is stable under $p_{4,1}$, $p_{16,4}\left(\frac{1}{a}\right)$ is in S. Similarly, applying $p_{32,12}$ to the identity, we find that $p_{32,12}\left(\frac{1}{a}\right)+\left(p_{16,6}\left(\frac{1}{c}\right)\right)^2=(p_{8,3}(u))^4$. Theorem 5.2 shows that $p_{16,6}\left(\frac{1}{c}\right)$ is in S, and we use the fact that $p_{8,3}$ stabilizes S. □

6 $l=9$

Now $l=9$. Then $m=4$ and N is generated by $x_1^5+x_4^4x_2+x_1x_2+x_3^2x_4^2$, $x_2^5+x_1^4x_4+x_2x_4+x_3^2x_1^2$, $x_4^5+x_2^4x_1+x_4x_1+x_3^2x_2^2$, $x_1^4x_3+x_3^4x_2+x_2x_3+x_2^2x_4^2$, $x_2^4x_3+x_3^4x_4+x_4x_3+x_4^2x_1^2$, and $x_4^4x_3+x_3^4x_1+x_1x_3+x_1^2x_2^2$. Let r be 1, 2 or 4, $a=[r]$, $b=[4r]$, $c=[2r]$ and $d=[3r]=[6r]$. Then $p_{2,0}(d)=d^4$, and $p_{2,0}$ takes a, b and c to b^4, c^4 and a^4. Lemma 3.5 shows that $p_{2,0}$ takes ab, bc and ac to c^2d^2, a^2d^2 and b^2d^2, and that it takes ad, bd and cd to a^2c^2, a^2b^2 and b^2c^2. We'll prove that $B(a)$ has relative density 0 in U^* by showing that each of $p_{4,2}\left(\frac{1}{a}\right)$, $p_{8,3}\left(\frac{1}{a}\right)$, $p_{8,5}\left(\frac{1}{a}\right)$, $p_{16,4}\left(\frac{1}{a}\right)$, $p_{16,8}\left(\frac{1}{a}\right)$, $p_{32,0}\left(\frac{1}{a}\right)$, $p_{64,16}\left(\frac{1}{a}\right)$ and $p_{128,48}\left(\frac{1}{a}\right)$ is in S.

Theorem 6.1. $p_{4,2}\left(\frac{1}{a}\right)$, $p_{8,3}\left(\frac{1}{a}\right)$, $p_{8,5}\left(\frac{1}{a}\right)$, $p_{16,4}\left(\frac{1}{a}\right)$ and $p_{16,8}\left(\frac{1}{a}\right)$ are in S.

Proof. Again we first write these power series as quotients of elements in S.

(1) The proof of Theorem 4.2 shows that $p_{4,2}\left(\frac{1}{a}\right)=\left(\frac{b^4}{a^4}\right)(a^2+b^8)$ while $p_{8,3}\left(\frac{1}{a}\right)=\left(\frac{b^{16}}{a^8}\right)(a+b^4)^3$.

(2) $p_{8,5}\left(\frac{1}{a}\right)=\left(\frac{1}{a^8}\right)p_{8,1}(a)p_{8,0}(a^2)p_{8,4}(a^4)=\left(\frac{1}{a^8}\right)p_{2,1}(a)\left(p_{4,0}(a)\right)^2\left(p_{2,1}(a)\right)^4=\frac{b^8}{a^8}(a+b^4)^5$.

(3) $p_{16,4}\left(\frac{1}{a}\right)=p_{16,4}p_{4,0}\left(\frac{1}{a}\right)=\left(p_{4,1}\left(\frac{b^3}{a}\right)\right)^4$. And $p_{4,1}\left(\frac{b^3}{a}\right)=\left(\frac{1}{a^4}\right)p_{4,1}(ab)p_{4,0}(a^2b^2)$ $=\left(\frac{1}{a^4}\right)p_{2,1}(ab)\left(p_{2,0}(ab)\right)^2=\frac{c^4d^4}{a^4}(ab+c^2d^2)$.

(4) $p_{8,0}\left(\frac{1}{a}\right)=\left(\frac{b^8}{a^8}\right)\left(p_{2,0}(ab)\right)^4=\left(\frac{bcd}{a}\right)^8$. If follows that $p_{16,8}\left(\frac{1}{a}\right)=p_{16,8}p_{8,0}\left(\frac{1}{a}\right)=\left(p_{2,1}\left(\frac{bcd}{a}\right)\right)^8$. Now $p_{2,1}\left(\frac{bcd}{a}\right)=\left(\frac{1}{a^2}\right)p_{2,1}((ab)(cd))=\left(\frac{1}{a^2}\right)$ $((c^2d^2)(cd+b^2c^2)+(ab+c^2d^2)(b^2c^2))=\left(\frac{1}{a^2}\right)(ab^3c^2+c^3d^3)$.

We conclude with our by now standard computer procedure. For example to show that $\left(\frac{1}{a^2}\right)(ab^3c^2 + c^3d^3)$ is in S we set $u = x_1x_4^3x_2^2 + x_2^3x_3^3$, $v = x_1^2$ and use Macaulay 2 to verify that $(N, v) = (N, u, v)$. $\square$

Lemma 6.2. $p_{16,0}\left(\frac{1}{a}\right)$ is the sixteenth power of $\frac{d(ab^2+bc^2+ca^2)}{a}$.

Proof. Arguing as in the above calculation of $p_{16,8}\left(\frac{1}{a}\right)$ we find that $p_{16,0}\left(\frac{1}{a}\right)$ is the eighth power of $p_{2,0}\left(\frac{bcd}{a}\right) = \frac{abcd}{a^2} + \frac{ab^3c^2+c^3d^3}{a^2}$. So it suffices to show that $(abcd + ab^3c^2 + c^3d^3) + d^2(a^2b^4 + b^2c^4 + c^2a^4) = 0$. To do this, set $u = (x_1x_4x_2x_3 + x_1x_4^3x_2^2 + x_2^3x_3^3) + x_3^2(x_1^2x_4^4 + x_4^2x_2^4 + x_2^2x_1^4)$. Macaulay 2 shows that $(N, u) = N$. So u is in N and applying ϕ_r gives the result. $\square$

Lemma 6.3. $p_{16,0}\left(\frac{1}{a}\right) + \left(p_{8,4}\left(\frac{1}{b}\right)\right)^4 = u^{16}$ for some u in S.

Proof. $p_{8,4}\left(\frac{1}{b}\right) = p_{8,0}\left(\frac{1}{b}\right) + p_{4,0}\left(\frac{1}{b}\right)$. Using Lemma 3.10 we find that this is $\left(\frac{acd}{b}\right)^8 + \left(\frac{c^3}{b}\right)^4$. So the left-hand side in the statement of the lemma is the sixteenth power of $u = \frac{d(ab^2+bc^2+ca^2)}{a} + \frac{a^2c^2d^2}{b^2} + \frac{c^3}{b}$. It remains to show that this u is in S. This is established using Macaulay 2 in the usual way. $\square$

Theorem 6.4. $p_{32,0}\left(\frac{1}{a}\right)$ and $p_{64,16}\left(\frac{1}{a}\right)$ are in S.

Proof. Applying $p_{32,0}$ to the identity of Lemma 6.3 we find that $p_{32,0}\left(\frac{1}{a}\right) = (p_{2,0}(u))^{16}$ with u in S. Applying $p_{64,16}$ to the identity we find that $p_{64,16}\left(\frac{1}{a}\right) + \left(p_{16,4}\left(\frac{1}{b}\right)\right)^4 = (p_{4,1}(u))^{16}$. But Theorem 6.1 shows that $p_{16,4}\left(\frac{1}{b}\right)$ is in S. $\square$

Theorem 6.5. $p_{32,12}\left(\frac{1}{a}\right)$ and $p_{128,48}\left(\frac{1}{a}\right)$ are in S.

Proof. We show how the second result follows from the first. Applying $p_{128,48}$ to the identity of Lemma 6.3 we find that $p_{128,48}\left(\frac{1}{a}\right) + \left(p_{32,12}\left(\frac{1}{b}\right)\right)^4 = (p_{8,3}(u))^{16}$. Since $p_{32,12}\left(\frac{1}{b}\right)$ is in S and $p_{8,3}$ stabilizes S we get the second result. To prove the first result we once again express our element as a quotient of two elements of S. $p_{32,12}\left(\frac{1}{a}\right) = p_{32,12}p_{4,0}\left(\frac{1}{a}\right) = p_{32,12}\left(\frac{b^{12}}{a^4}\right) = \left(p_{8,3}\left(\frac{b^3}{a}\right)\right)^4$. So it's enough to show that $p_{8,3}\left(\frac{b^3}{a}\right)$ is in S. Now $p_{8,3}\left(\frac{b^3}{a}\right) = \left(\frac{1}{a^8}\right)p_{8,3}\left((a^2b^2)(ab)(a^4)\right) = \left(\frac{1}{a^8}\right)p_{8,2}(a^2b^2)\left(p_{8,1}(ab)p_{8,0}(a^4) + p_{8,5}(ab)p_{8,4}(a^4)\right)$. Now modulo a^8, $p_{8,1}(ab) = p_{8,0}(a)p_{8,1}(b) = c^{16}(b + c^4)$. Also $p_{4,1}(ab) = p_{2,1}(ab) = ab + c^2d^2$. So modulo a^8, $p_{8,5}(ab) = p_{4,1}(ab) + c^{16}(b + c^4) = ab + c^2d^2 + c^{16}(b + c^4)$. We conclude that $p_{8,3}\left(\frac{b^3}{a}\right)$ is the sum of an element of S and $\frac{1}{a^8}(a^2b^2 + c^4d^4)$ $(c^{16}(b + c^4)b^{16} + (ab + c^2d^2 + c^{16}(b + c^4))(a^4 + b^{16}))$. A Macaulay 2 calculation shows that this last element is in S. $\square$

7 $l = 11$, 13 and 15

We state the results for these l with very brief indications of proofs.

Lemma 7.1. Let $a = [r]$ with r prime to l. Then $p_{8,k}\left(\frac{1}{a}\right)$, $p_{16,2k}\left(\frac{1}{a}\right)$, $p_{32,4k}\left(\frac{1}{a}\right)$ and $p_{64,8k}\left(\frac{1}{a}\right)$ are all quotients of elements of S by powers of a.

Proof. $p_{8,k}\left(\frac{1}{a}\right) = \frac{1}{a^8}p_{8,k}(a^7)$, and we use Lemma 2.2. For the remaining results we may assume that $r = 4s$. Let $b = [2s]$, $c = [s]$, $e = [3s]$ so that $p_{2,0}(a) = b^4$, $p_{2,0}(ab) = c^2e^2$. Then $p_{64,8k}\left(\frac{1}{a}\right) = p_{64,8k}p_{8,0}\left(\frac{1}{a}\right)$. By Lemma 3.10 this is the eighth power of $p_{8,k}\left(\frac{bce}{a}\right)$, and we use the fact that $p_{8,k}(a^7bce)$ is in S. $p_{16,2k}\left(\frac{1}{a}\right)$ and $p_{32,4k}\left(\frac{1}{a}\right)$ are treated similarly. □

Theorem 7.2. Let $a = [r]$ with r prime to l.

(1) When $l = 11$, $p_{8,1}$, $p_{8,3}$, $p_{8,6}$, $p_{16,4}$, $p_{16,8}$, $p_{16,10}$, $p_{32,0}$, $p_{32,12}$ and $p_{64,16}$ all take $\frac{1}{a}$ to an element of S.
(2) When $l = 13$, $p_{8,2}$, $p_{8,3}$, $p_{8,5}$, $p_{16,4}$, $p_{16,8}$, $p_{16,14}$, $p_{32,0}$, $p_{32,12}$ and $p_{64,16}$ all take $\frac{1}{a}$ to an element of S.
(3) When $l = 15$, $p_{8,1}$, $p_{8,2}$, $p_{8,3}$, $p_{16,4}$, $p_{16,6}$, $p_{16,8}$, $p_{32,0}$, $p_{32,12}$ and $p_{64,16}$ all take $\frac{1}{a}$ to an element of S.

Idea of proof. By Lemma 7.1 each $p_{q,j}\left(\frac{1}{a}\right)$ is the quotient of an element of S by a power of a. It's clear that one can write down such a representation explicitly. In each case the Macaulay 2 argument using the ideal N of quintic relations shows that $p_{q,j}\left(\frac{1}{a}\right)$ is in fact in S.

Corollary 7.3. Suppose $l = 11$, 13, or 15. Then in each of the mod 128 congruence classes constituting U^*, with the possible exception of the congruence class $n \equiv 48 \ (128)$, $B(a)$ has relative density 0

Proof. This follows from Theorem 7.2, Corollary 3.4 and the explicit description of U^* as a union of congruence classes. □

I'll now show that when $l = 11$ each $B(a)$ in fact has relative density 0 in the congruence class 48 mod 128.

Lemma 7.4. When $l = 11$, $p_{8,0}\left(\frac{1}{a}\right) + \left(p_{8,4}\left(\frac{1}{b}\right)\right)^4 = u^8$ for some u in S.

Idea of proof. As we noted in the proof of Lemma 7.1, $p_{8,0}\left(\frac{1}{a}\right) = \left(\frac{bce}{a}\right)^8$. Furthermore $p_{8,4}\left(\frac{1}{b}\right) = p_{8,4}p_{2,0}\left(\frac{1}{b}\right) = \left(\frac{1}{b^8}\right)p_{8,4}(b^6c^4)$. This is the quotient of a square in S by b^8. It follows that the left-hand side in the statement of Lemma 7.4 is the eighth power of $\frac{v}{ab^4}$ for some v in S. Our usual Macaulay 2 technique shows that $\frac{v}{ab^4}$ is in fact in S.

Theorem 7.5. When $l = 11$, $p_{128,48}\left(\frac{1}{a}\right)$ is in $p_{128,48}(S)$. In fact it's the eighth power of an element of $p_{16,6}(S)$. Corollary 3.4 then shows that $B(a)$ has relative density 0 in the congruence class 48 mod 128, and consequently in U^*.

Proof. Applying $p_{128,48}$ to the identity of Lemma 7.4 we find that $p_{128,48}\left(\frac{1}{a}\right) + \left(p_{32,12}\left(\frac{1}{b}\right)\right)^4 = (p_{16,6}(u))^8$. Now $p_{32,12}\left(\frac{1}{b}\right) = p_{32,12}p_{4,0}\left(\frac{1}{b}\right) = p_{32,12}\left(\frac{c^{12}}{b^4}\right)$, which is the square of $p_{16,6}\left(\frac{c^6}{b^2}\right)$. So $p_{128,48}\left(\frac{1}{a}\right)$ is the eighth power of $p_{16,6}\left(\frac{c^6}{b^2}\right) + p_{16,6}(u)$, and it will suffice to show that $p_{16,6}\left(\frac{c^6}{b^2}\right)$ is in S. In fact, $p_{8,3}\left(\frac{c^3}{b}\right)$ is in S; the Macaulay 2 calculations going into the proof of Theorem 7.2 show this. □

Remarks. We've established various zero-density results when $l \leq 15$. If we take $l > 15$, computer trouble arises. Suppose for example we restrict ourselves to congruence classes to the modulus 8 that lie in U^*. Then necessarily $l \leq 21$ or $l = 25$. When $l = 17$, the classes $n \equiv 5\ (8)$ and $n \equiv 6\ (8)$ are in U^*. But the ideal N in $\mathbb{Z}/2[x_1, \ldots, x_8]$ has 28 generators, and attempts, using Macaulay 2, to show that $p_{8,5}\left(\frac{1}{a}\right)$ (or $p_{8,6}\left(\frac{1}{a}\right)$) is in S cause a computer crash. Indeed the computer seemed at its limit in handling the congruence class $n \equiv 16\ (64)$ when $l = 15$; it was an all-day calculation.

For $l = 11$ I don't know whether Theorem 7.5 can be strengthened to show that $p_{128,48}\left(\frac{1}{a}\right)$ is in S. When $l = 13$ or 15 it's possible that, as in the case $l = 11$, $p_{128,48}\left(\frac{1}{a}\right)$ is the eighth power of an element of $p_{16,6}(S)$. But there's no analogue of Lemma 7.4 that could be used to prove this.

8 The basic classes — a little computer evidence

Fix l together with r prime to l and a basic congruence class C. All the elements of $B([r])$ are $\geq -r^2$ and are congruent to $-r^2$ mod l. There is some evidence that $B([r])$ has density $\frac{1}{2l}$ in C, so that "half the elements of C that are $\geq -r^2$ and are congruent to $-r^2$ mod l lie in $B([r])$."

Suppose for example that $l \leq 9$ and we are looking at the basic classes to the modulus 8. These are:

(1) $l = 3 \quad n \equiv 7 \ (8)$

(2) $l = 5 \quad n \equiv 7 \ (8)$

(3) $l = 7 \quad n \equiv 7 \ (8)$

(4) $l = 9 \quad n \equiv 1$ or $7 \ (8)$

Consider the first $2^{17} = 131,072$ elements of C that are $\geq -r^2$ and congruent to $-r^2$ mod l. The number of these lying in $B([r])$ has been calculated by O'Bryant [3]. Here are his results.

(1) $l = 3$	$n \equiv 7 \ (8)$,	$r = 1$	$65,411$					
(2) $l = 5$	$n \equiv 7 \ (8)$,	$r = 1$	$65,397$	$r = 2$	$65,713$			
(3) $l = 7$	$n \equiv 7 \ (8)$,	$r = 1$	$65,185$	$r = 2$	$65,474$	$r = 3$	$65,622$	
(4) $l = 9$	$n \equiv 1 \ (8)$,	$r = 1$	$65,495$	$r = 2$	$65,666$	$r = 4$	$65,367$	
	$n \equiv 7 \ (8)$,	$r = 1$	$65,877$	$r = 2$	$65,579$	$r = 4$	$65,813$	

We may also consider the basic congruence class $n \equiv 14 \ (16)$ when $l = 7$. Now if we consider the first 65,536 elements of the class that are $\equiv -r^2$ mod 7 and $\geq -r^2$, the number in $B([r])$ is 32,673 when $r = 1$. It is 32,716 when $r = 2$ and 32,981 when $r = 3$. All this suggests the following:

Speculation. Suppose that $\rho > \frac{1}{2}$. Consider a basic class C and the first X elements in the class that are $\geq -r^2$ and congruent to $-r^2$ mod l. Of these elements, the number in $B([r])$ is $\frac{X}{2} + O(X^\rho)$.

We might go even further, speculating that this is true not only for the basic classes, but for any congruence class contained in a a basic class.

It would be interesting to test these speculations further experimentally. But some caution is in order. Suppose for example that $l = 9$. Then the congruence class $n \equiv 2 \ (4)$ is contained in U^*, and as we've seen, $B([1])$, $B([2])$ and $B([4])$ all have relative density 0 in this class. Consider now the first $2^{18} = 262,144$ elements of this class that are $\geq -r^2$ and congruent to $-r^2$ mod 9. The number of these elements that lie in $B([r])$ is 102,284 when $r = 1$, and 110,034 when $r = 2$. This is in good accord with our zero-density result. But when $r = 4$ more than half of the elements are in $B([r])$! (The number is 137,657.) So we are advised not to place too much predictive power in such computer counts unless the range over which we're counting is considerably extended.

References

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

[2] Monsky P., Disquistiones arithmeticæ and online sequence A108345, arXiv (NT) 1009.3985.

[3] O'Bryant K., personal communication.

[4] Schöneberg B., Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen, Math. Ann. 116 (1939), 511–523.

[5] Serre J.-P., Divisibilité des coefficients des formes modulaires de poids entier, C. R. Acad. Sci. Paris Sér. A 279 (1974), 679–682.