MULTIPLICATIVE SERIES, MODULAR FORMS, AND MANDELBROT POLYNOMIALS

MICHAEL LARSEN

ABSTRACT. We say a power series $\sum_{n=0}^{\infty} a_n q^n$ is *multiplicative* if the sequence $1, a_2/a_1, \ldots, a_n/a_1, \ldots$ is so. In this paper, we consider multiplicative power series f such that f^2 is also multiplicative. We find a number of examples for which f is a rational function or a theta series and prove that the complete set of solutions is the locus of a (probably reducible) affine variety over $\mathbb{C}$. The precise determination of this variety turns out to be a finite computational problem, but it seems to be beyond the reach of current computer algebra systems. The proof of the theorem depends on a bound on the logarithmic capacity of the Mandelbrot set.

1. INTRODUCTION

Let $r_k(n)$ denote the number of representations of n as a sum of k squares. It is classical that $r_1(n)/2$, $r_2(n)/4$, $r_4(n)/8$, and $r_8(n)/16$ are multiplicative functions of n; the first trivially, the second thanks to Fermat, and the third and fourth thanks to Jacobi [Ja, §§42,44]. From the standpoint of generating functions, this can be interpreted as the statement that the theta series $\vartheta_{\mathbb{Z}}(q)$ (see (3.1) for the notation $\vartheta_\Lambda(q)$) and its square, fourth power, and eighth power, all have multiplicative coefficients (after suitable normalization). As a starting point, we prove the converse:

Theorem 1.1. *If $f(q) \in \mathbb{C}[[q]]$, $f(q)^2$, $f(q)^4$, and $f(q)^8$ are all multiplicative, then $f(q)$ is a constant multiple of $\vartheta_{\mathbb{Z}}(\pm q)$.*

This is an immediate consequence of the following more difficult result:

Theorem 1.2. *If $f(q)$, $f(q)^2$, and $f(q)^4$ all have multiplicative coefficients, then $f(q)$ is a constant multiple of $\vartheta_{\mathbb{Z}}(\pm q)$, $\vartheta_{\mathbb{Z}[i]}(\pm q)$, or $\vartheta_{\mathbb{Z}[\zeta_3]}(\pm q)$.*

A much more difficult problem is to characterize all power series $f(q)$ such that $f(q)$ and $f(q)^2$ are multiplicative, without assuming $f(q)^4$ is multiplicative as well. We denote by $\mathcal{X}$ the set of normalized multiplicative power series f such that f^2 is also multiplicative. (See Definition 3.1 for precise definitions.) Since a power series with multiplicative coefficients is determined by its prime power coefficients, and since prime powers form a density-zero subset of the integers, when n is large, the first n coefficients of any $f(q) \in \mathcal{X}$ must satisfy a highly overdetermined system of polynomial

The author was partially supported by the Sloan Foundation and the NSF.

equations. From this point of view, the fact that $\mathcal{X} \neq \emptyset$ is surprising. On the other hand, it is clear that any Hecke eigenform whose square is again a Hecke eigenform belongs to $\mathcal{X}$. The relationship between the action of Hecke operators on the space of modular forms of a fixed weight and the ring structure on the graded vector space of all modular forms is rather mysterious, but, in general, the square of an eigenform is unlikely to be an eigenform unless, for dimension reasons, there is no alternative. Indeed, a number of papers have examined when the product of two eigenforms is again an eigenform (see, e.g., [BJTX, Du, Em, Gh, Jo]), and the moral of these papers seems to be that this phenomenon is a transient one, associated to low levels and weights. A natural place to look for elements of $\mathcal{X}$ is therefore among (noncuspidal) forms of low level and weight. One might reasonably guess that $\mathcal{X}$ consists entirely of modular forms, but this turns out to be wrong; certain rational functions analytic on the open unit disk also belong to $\mathcal{X}$.

Between modular forms and rational functions, the locus $\mathcal{X}$ contains at least nine one-parameter families of solutions and twelve isolated points. There is numerical evidence, based on the search for (mod p) solutions for small primes p, that these solutions constitute all of $\mathcal{X}$, but the results of this paper fall far short of this. Truncating power series at the q^n coefficient, as n varies, one obtains a sequence of complex algebraic varieties $\mathcal{X}_n$ of which $\mathcal{X}$ is the inverse limit. The sequence $\mathcal{X}_n$ does not stabilize. The main theorem of this paper asserts that, nevertheless, $\mathcal{X}$ itself has the structure of a complex affine variety. More precisely, there exists n (in fact, $n = 16$ will do) such that the natural map $\mathcal{X} \to \mathcal{X}_n$ is injective, and its image is a Zariski-closed subset of $\mathcal{X}_n$. In particular, all solutions are determined by their degree 16 truncations.

Remarkably, our proof of this theorem depends, ultimately, on the fact that the logarithmic capacity of the Mandelbrot set $\mathcal{M}$ is less than 2. (In fact, it is known to be 1 [St, §6.2].) Computer algebra computations reduce the problem to the "sparse" case, where the coefficients $a_2 = a_3 = \cdots = a_{n-1} = 0$ and $a_n \neq 0$, for some $n \geq 16$. In this case, one shows first that n is a Mersenne prime and then that the first $\frac{n-1}{2}$ terms of the sequence $a_n, a_{2n-1}, a_{3n-2}, a_{4n-3}, \ldots$ satisfy a certain non-linear recurrence. In fact, there is a universal sequence $M_1, M_2, \ldots \in \mathbb{Q}[y]$ of "Mandelbrot polynomials" such that $a_{i(n-1)+1} = M_i(a_n)$. The multiplicativity of the sequence of coefficients implies that if $i(n-1)+1$ is not a prime power, then $a_{i(n-1)+1} = 0$. Thus, the roots of M_i are highly relevant to the search for sparse solutions. The recurrence formula for the M_i implies that if r_i is a root of $M_i(y)$ for each i and r is a limit point of the sequence r_i, then $-2r$ belongs to the Mandelbrot set. Although the roots of the individual $M_i(y)$ need not be algebraic integers, we have enough p-adic control to guarantee integrality for a simultaneous root of many M_i, like a_n. Since $\mathcal{X}$ is $\mathrm{Aut}(\mathbb{C})$-stable and a set of capacity less than 1 contains only finitely many complete Galois orbits of algebraic integers, there are only finitely many possibilities

for a_n, and in the end we show $a_n = 0$. We actually work not with $\mathcal{M}$ itself but with an open disk containing $\mathcal{M}$ and of radius < 2, thus obviating the need to understand the fine structure of $\mathcal{M}$.

The paper is organized as follows. In §2, we give some preliminaries about inverse systems of varieties. In §3, we present the known elements of $\mathcal{X}$. In §4, we assemble elementary results about the set of prime powers which are needed in the next two sections. In §5, we present results of Maple-assisted computations which reduce the problem to the sparse case. In principle, the results of this section imply that the non-sparse solutions can be determined by a finite computation, but this seems well beyond the reach of currently available computer algebra systems. Sparse solutions are ruled out in §6 by the method discussed above. The last section presents variants and related questions, including proofs of Theorems 1.1 and 1.2. An appendix presents the results of an exhaustive search for non-sparse solutions defined over the finite field $\mathbb{F}_p$ for small primes $p > 2$. I am grateful to Anne Larsen for carrying out this search and identifying almost all of her solutions as modular forms, including a number of "exceptional solutions", that is, examples in which the form involved is not the (mod p) reduction of any known characteristic zero solution. The solutions (x) in Proposition 3.2 and (x') in Corollary 3.4, which did not appear in an earlier draft of this paper, originally appeared as exceptional solutions in her (mod p) tables for $p = 3$, $p = 11$, $p = 17$, and $p = 19$.

I would like to thank the Hebrew University in Jerusalem for its hospitality while much of this work was carried out. I am grateful to Zeév Rudnick for pointing out some relevant literature and to the referee for pointing out several deficiencies in an earlier draft of this paper and suggesting a number of improvements to the exposition.

2. Systems of Affine Varieties

Throughout this paper, an *affine variety* means a scheme $\mathcal{V} = \operatorname{Spec} A$, where A is a finitely generated algebra over $\mathbb{C}$, and a *morphism of varieties* means a morphism over $\operatorname{Spec} \mathbb{C}$. When no confusion seems likely to result, we identify $\mathcal{V}$ with its set $\mathcal{V}(\mathbb{C})$ of closed points.

Let $(\mathcal{Y}_n, \phi_{m,n} \colon \mathcal{Y}_m \to \mathcal{Y}_n)$ denote an inverse system of affine varieties indexed by integers $n \geq 2$. Let $(\mathcal{Y} = \varprojlim \mathcal{Y}_n(\mathbb{C}), \psi_n \colon \mathcal{Y} \to \mathcal{Y}_n(\mathbb{C}))$ denote the set-theoretic inverse limit.

Definition 2.1. *We say the inverse limit $\mathcal{Y}$ is of* affine type *if there exist n and a closed subvariety $\mathcal{V}_n$ of $\mathcal{Y}_n$ such that ψ_n is injective and $\psi_n(\mathcal{Y}) = \mathcal{V}_n(\mathbb{C})$.*

Example 2.2. *If $\mathcal{Y}_n = \operatorname{Spec} \mathbb{C}[x]$ for all n, and every map $\phi_{m,n}$ comes from the $\mathbb{C}$-algebra homomorphism $\mathbb{C}[x] \to \mathbb{C}[x]$ mapping x to 0, then $\mathcal{Y}$ is of affine type (and consists of a single point).*

Example 2.3. *If* $\mathcal{Y}_n = \operatorname{Spec} \mathbb{C}[x, \frac{1}{x-1}, \frac{1}{x-2}, \dots, \frac{1}{x-n}]$ *with the obvious inclusion morphisms, then* $\mathcal{Y} = \mathbb{C} \setminus \mathbb{Z}^{>0}$ *is not of affine type.*

Example 2.4. *If* $\mathcal{Y}_n = \operatorname{Spec} \mathbb{C}[x]/(x^{2^n} - 1)$ *with the obvious morphisms, then* $\mathcal{Y} = \mathbb{Z}_2$ *is not of affine type.*

Proposition 2.5. *Let* $(\mathcal{Y}_n, \phi_{m,n} \colon \mathcal{Y}_m \to \mathcal{Y}_n)$ *be an inverse system,* $n \geq 2$ *an integer, and* $\mathcal{V}$ *a closed subvariety of* $\mathcal{Y}_n$*. Assume the following conditions hold:*

1. *For all* $y \in \mathcal{Y}_n$, $|\psi_n^{-1}(y)| \leq 1$,
2. $\mathcal{V}$ *is contained in* $\psi_n(\mathcal{Y})$,
3. *For all* $y \in \mathcal{Y}_n \setminus \mathcal{V}$ *and all sufficiently large* m, $|\phi_{m,n}^{-1}(y)| \leq 1$.
4. *For all* $y \in \mathcal{Y}_n \setminus \mathcal{V}$*, there exists a neighborhood* U_y *of* y *in the complex topology such that there exist arbitrarily large integers* m *for which* $\phi_{m,n}^{-1}(U_y)$ *is precompact in the complex topology.*

Then $\mathcal{Y}$ *is of affine type.*

Proof. For $m > n$, let $\mathcal{W}_m$ denote the Zariski closure of $\phi_{m,n}(\mathcal{Y}_m)$. Thus,

$$\mathcal{Y}_n \supseteq \mathcal{W}_{n+1} \supseteq \mathcal{W}_{n+2} \supseteq \mathcal{W}_{n+3} \supseteq \cdots,$$

and by the Hilbert basis theorem, this chain must eventually stabilize to some closed subvariety $\mathcal{W}_k \subseteq \mathcal{Y}_n$. We define $\mathcal{V}_n = \mathcal{W}_k$. Thus, $\mathcal{V} \subseteq \psi_n(\mathcal{Y}) \subseteq \mathcal{V}_n$. We need only prove that for all $y \in \mathcal{V}_n \setminus \mathcal{V}$, the inverse image $\psi_n^{-1}(y) \subset \mathcal{Y}$ is non-empty. As $\phi_{m,n}^{-1}(y)$ is finite for all $y \in \mathcal{Y}_n \setminus \mathcal{V}$ and for all m sufficiently large, and since the inverse limit of an inverse system of non-empty finite sets is non-empty, it suffices to prove that $\phi_{m,n}^{-1}(y)$ is non-empty for all $y \in \mathcal{V}_n \setminus \mathcal{V}$ and all m sufficiently large.

As $\phi_{m,n}(\mathcal{Y}_m)$ contains a Zariski dense open subset in $\mathcal{Y}_n$, it contains an open set U_m in the complex topology. Intersecting with the open set U_y and choosing m larger if necessary, we may assume that $\phi_{m,n}^{-1}(U_m)$ is precompact in the complex topology. Now, y is the limit in the complex topology of a sequence of points $y_i \in \phi_{m,n}(\mathcal{Y}_m)$. Choosing $\tilde{y}_i \in \mathcal{Y}_m$ such that $\phi_{m,n}(\tilde{y}_i) = y_i$, the $\tilde{y}_i$ belong to a precompact set, so some subsequence converges to $\tilde{y} \in \mathcal{Y}_m$, and it follows that $\phi_{m,n}(\tilde{y}) = y$. □

3. Solutions

Definition 3.1. *A power series* $f(q) = \frac{1}{2a_0} + \sum_{n=1}^{\infty} a_n q^n$ *is* normalized multiplicative *if* $a_1 = 1$ *and* $a_{mn} = a_m a_n$ *whenever* m *and* n *are relatively prime. We say that* f *is* multiplicative *if some multiple* λf *is normalized multiplicative. The set* $\mathcal{X}$ *consists of all normalized multiplicative power series* $f(q)$ *such that* $f(q)^2$ *is again multiplicative. In this case, we define the multiplicative sequence* b_n *by the equation*

$$a_0 f(q)^2 = \frac{1}{4a_0} + \sum_{n=1}^{\infty} b_n q^n$$

Equivalently, f is multiplicative if and only if the corresponding Dirichlet series has an Euler product

$$\sum_{n=1}^{\infty} a_n n^{-s} = c \prod_p (1 + a_p p^{-s} + a_{p^2} p^{-2s} + \cdots),$$

and normalized if $c = 1$. If $f(q)$ is the q-expansion of a modular form of prime-to-p level and $T_p f = \lambda f$ for some λ, then the Dirichlet series for f is the product of a p-factor $(1 - \lambda p^{-s} + \epsilon(p) p^{2k-1-s})^{-1}$ and a prime-to-p Dirichlet series. In particular, any Hecke eigenform of prime-power level is multiplicative. For general level N, if f is an eigenform also for the Atkin-Lehner operators, then it is again multiplicative.

It is convenient to express the modular solutions as theta-functions. Thus, if Λ is a lattice all of whose elements have integral square-length, we write

$$\vartheta_\Lambda(q) = \frac{1}{|\{\lambda \in \Lambda \mid \|\lambda\| = 1\}|} \sum_{\lambda \in \Lambda} q^{\|\lambda\|^2} \tag{3.1}$$

Proposition 3.2. *Let Φ denote the root lattice of the Lie algebra E_8 normalized so that roots have length 1, H the Hurwitz order in the rational quaternion algebra, and D^* the set $\mathbb{C} \setminus \{-1\}$. Then the following modular forms lie in $\mathcal{X}$:*

(i) $\vartheta_\Phi(q)$,
(ii) $\vartheta^2_{\mathbb{Z}[\zeta_3]}(q)$,
(iii) $\vartheta_H(q) + t\vartheta_H(q^2),\ t \in D^*$,
(iv) $\vartheta_{\mathbb{Z}[\tau]}(q),\ \tau = \frac{1+\sqrt{-7}}{2}$,
(v) $\vartheta_{\mathbb{Z}[i]}(q) + t\vartheta_{\mathbb{Z}[i]}(q^2),\ t \in D^*$,
(vi) $\vartheta_{\mathbb{Z}[\zeta_3]}(q) + t\vartheta_{\mathbb{Z}[\zeta_3]}(q^4),\ t \in D^*$,
(vii) $\vartheta_{\mathbb{Z}}(q) + t\vartheta_{\mathbb{Z}}(q^4),\ t \in D^*$,
(viii) $\vartheta_{\mathbb{Z}[\sqrt{-2}]}(q) + t\vartheta_{\mathbb{Z}[\sqrt{-2}]}(q^2),\ t \in D^*$,
(ix) $\vartheta_{\mathbb{Z}[i]}(q) - \sqrt{-3}\vartheta_{\mathbb{Z}[i]}(q^2) + \sqrt{-3}\vartheta_{\mathbb{Z}[i]}(q^3) + 3\vartheta_{\mathbb{Z}[i]}(q^6) + t(\vartheta_{\mathbb{Z}[i]}(q^2) + \sqrt{-3}\vartheta_{\mathbb{Z}[i]}(q^6)),\ t \in D^*$,
(x) $\vartheta_{\mathbb{Z}[\zeta_3]}(q) + \sqrt{-2}\vartheta_{\mathbb{Z}[\zeta_3]}(q^2)$.

Proof. We begin with a few general remarks. If $f(q)$ is multiplicative and n is a prime power, then $f(q) + tf(q^n)$ is multiplicative for all $t \in D^*$. By [He, p. 792], if R is the ring of integers in an imaginary quadratic field, then $\vartheta_R(q)$ is a modular form of weight 1, level $\mathrm{Disc}(R)$, and nebentypus of order 2. If, in addition, R is a PID, then the corresponding theta-series is multiplicative. This remark applies to $\mathbb{Z}[\zeta_3]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, and $\mathbb{Z}[\sqrt{-2}]$. The modular curves $X_0(N)$ for $N \in \{1, 3, 4, 7, 8, 12, 16\}$ are all of genus 0, so every $\Gamma_0(N)$ modular form of weight 2 with N in this set is a linear combination of Eisenstein series.

We now consider the individual cases. By [Se2, VII, §6.6], ϑ_Φ is the Eisenstein series $\frac{1}{240}E_4$, and since there is only one normalized form of level

1 and weight 8, ϑ_Φ^2 is an eigenform. The space of forms of weight 4 and level 3 (resp. 4) has dimension 2 (resp. 3) and therefore consists entirely of linear combinations of Eisenstein series (since the number of divisors of the level equals the dimension of the space). This finishes (ii). For (iii), we observe that $\vartheta_H(q)$ is of level 2. We can see this from the formula $\vartheta_H(q) = -\frac{1}{24}E_2(q) + \frac{1}{12}E_2(q^2)$ expressing the theta series of the Hurwitz order in terms of the not-quite-modular Eisenstein series E_2 (cf. [Ma, II §5]). Thus, the forms in question are all of level 4. Case (vi) requires extra care since unlike the cases (iv), (v), and (viii), the level is no longer a prime power; we can write the Dirichlet series for $f(q)^2$ as a product of p-factors for all $p \notin \{2,3\}$ together with a factor involving all terms of the form 2^m3^n. As $b_{3n} = b_n$ for all n, this final term is actually the product of $(1-3^{-s})^{-1}$ and a power series in 2^{-s}. For (vii), the form f is of weight $1/2$ and is multiplicative by inspection. By the two-squares theorem, its square is of the form

$$\frac{1}{4}\sum_{n=0}^{\infty} p(n)r_2(n)q^n, \quad p(n) = \begin{cases} 1+t & \text{if } n \equiv 0 \pmod 4, \\ 1 & \text{if } n \equiv 1 \pmod 4, \\ (1+t)^{-1} & \text{if } n \equiv 2 \pmod 4, \\ 0 & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

For (ix),

$$\vartheta_{\mathbb{Z}[i](q)} + u\vartheta_{\mathbb{Z}[i](q^2)} + v\vartheta_{\mathbb{Z}[i](q^3)} + uv\vartheta_{\mathbb{Z}[i](q^6)}$$

is multiplicative for all $u, v \in \mathbb{C}$. As $X_0(24)$ has genus 1, the condition that $f(q)^2$ be a linear combination of Eisenstein series imposes a single equation, which happens to be $v^2 + 3 = 0$. We check that when v is a square root of -3, $b_{3n} = b_n$ for all n. For (x), we verify

$$\begin{aligned}(1-\sqrt{-2})&(\vartheta_{\mathbb{Z}[\zeta_3]}(q) + \sqrt{-2}\vartheta_{\mathbb{Z}[\zeta_3]}(q^2))^2 \\ &= E_2(q) - 2E_2(q^2) + (1+2\sqrt{-2})E_2(q^3) - (2+4\sqrt{-2})E_2(q^6),\end{aligned}$$

which is again multiplicative. □

We remark that (i)–(viii) above each have at least one representative which is the theta-series of an order in a (possibly non-commutative, possibly even non-associative) algebra. This is obvious except for (i), which corresponds to the ring of octavian integers in the Cayley numbers ([CS, §9.3]) and (ii), which corresponds to a maximal order in the rational quaternion algebra ramified only at 3 and ∞. We remark also that (i), (ii), (iii), (v), (vi), and (vii) each contain at least one representative which is the theta-series of a root lattice.

Lemma 3.3. *If $f(q) \in \mathcal{X}$, so is $-f(-q)$.*

Proof. We have $(-(-1)^m)(-(-1)^n) = (-(-1)^{mn})$ whenever m and n are not both even. When they are both even, of course, they are not relatively prime. □

Corollary 3.4. *The following modular forms belong to $\mathcal{X}$:*

(i') $-\vartheta_{\Phi}(-q)$,
(ii') $-\vartheta^2_{\mathbb{Z}[\zeta_3]}(-q)$,
(iv') $-\vartheta_{\mathbb{Z}[\tau]}(-q)$,
(ix') $\vartheta_{\mathbb{Z}[i]}(q) - \sqrt{-3}\vartheta_{\mathbb{Z}[i]}(q^2) - \sqrt{-3}\vartheta_{\mathbb{Z}[i]}(-q^3) + 3\vartheta_{\mathbb{Z}[i]}(q^6) + t(\vartheta_{\mathbb{Z}[i]}(q^2) + \sqrt{-3}\vartheta_{\mathbb{Z}[i]}(q^6))$, $t \in D^*$,
(x') $-\vartheta_{\mathbb{Z}[\zeta_3]}(-q) - \sqrt{-2}\vartheta_{\mathbb{Z}[\zeta_3]}(q^2)$.

Next, we present some rational solutions. Clearly,

(xi) $\frac{1}{2a_0} + q$, $a_0 \neq 0$

belongs to $\mathcal{X}$. It is easy to see that these are the only polynomial solutions. In addition, one readily checks the following proposition:

Proposition 3.5. *The following rational functions all belong to $\mathcal{X}$:*

(xii) $t\frac{1+q^2}{1-q^2} + \frac{q}{1-q^2} = t + q + 2tq^2 + q^3 + 2tq^4 + q^5 + 2tq^6 + \cdots, t \neq 0$;
(xiii) $\frac{q^2+7q+1}{6q^2+6q+6} = \frac{1}{6} + q - q^2 + q^4 - q^5 + q^7 - q^8 + \cdots$;
(xiii') $\frac{-q^2+7q-1}{6q^2-6q+6} = -\frac{1}{6} + q + q^2 - q^4 - q^5 + q^7 + q^8 - \cdots$;
(xiv) $\frac{q^2+10q+1}{12(q-1)^2} = \frac{1}{12} + q + 2q^2 + 3q^3 + 4q^4 + \cdots$;
(xiv') $\frac{-q^2+10q-1}{12(q+1)^2} = -\frac{1}{12} + q - 2q^2 + 3q^3 - 4q^4 + \cdots$.

The form of the above solutions suggests the following elementary proposition whose proof we leave to the reader:

Proposition 3.6. *If $f(q)$ is a multiplicative power series which is a rational function but not a polynomial, then there exists a constant a_0, a non-negative integer d, a positive integer N, and an N-periodic sequence of constants $a_1, a_2, a_3, \ldots$ such that*

$$f(q) = \frac{1}{2a_0} + \sum_{n=1}^{\infty} a_n n^d q^n.$$

The appendix presents the results of a comprehensive search for normalized multiplicative series $f(q) \in \mathbb{F}_p[[q]]$, $3 \leq p \leq 31$, such that $f(q)^2$ is again multiplicative. The majority arise from (mod p) reduction of solutions (i)–(xiv') above (with $t \in \mathbb{Q}$ in the case of parametric solutions). The exceptions appear to be (mod p) reductions of q-expansions of modular forms with coefficients in $\mathbb{Q}$ and in most cases can be written in the form $f(q) = \sum_{d|N} c_d g(q^d)$, where g is either a theta series or an Eisenstein series. However, somewhat unexpectedly, cusp forms also make an appearance. The following proposition gives an illustrative example:

Proposition 3.7. *Let $\bar{\Delta}$ denote the (mod 13) reduction of the normalized cusp form of level 1 and weight 12. Then $\bar{f}(q) = 2 + \bar{\Delta}$ is a normalized multiplicative series in $\mathbb{F}_{13}[[t]]$ whose square is again multiplicative.*

Proof. It is well known (see, for instance, [Se2, VII, Corollary 2]) that the ring of complex modular forms of level 1 is $\mathbb{C}[E_4, E_6]$. As E_{2k} is normalized to have constant term 1, $E_{10} = E_4 E_6$, and

$$\Delta = \frac{E_4^3 - E_6^2}{1728},$$

$E_4\Delta$, $E_6\Delta$, and $E_4^2\Delta$ are the unique normalized cusp forms of weight 12, 16, 18, and 20 respectively. An easy calculation shows

$$E_{12} = \frac{441E_4^3 + 250E_6^2}{691} \tag{3.2}$$

(see, for instance, [Se, §1.1]).

By a theorem of Serre and Swinnerton-Dyer $\bar{f}(q) \in \mathbb{F}_p[[q]]$ is the (mod p) reduction of a modular form of level 1 and weight k, then $q\frac{d\bar{f}}{dq}$ is the reduction (mod p) of a cusp form of weight $k+p+1$ [Se, §1.4, Corollaire 2]. In particular, for $p = 13$, we have

$$q\frac{\partial \bar{E}_4}{\partial q} = 240\bar{E}_6\bar{\Delta}$$

and

$$q\frac{d\bar{E}_6}{dq} = -504\bar{E}_4^2\bar{\Delta}.$$

By the Leibniz rule,

$$q\frac{d\bar{E}_{10}}{dq} = (240\bar{E}_6^2 - 504\bar{E}_4^3)\bar{\Delta}.$$

By the von Staudt-Clausen theorem, $\bar{E}_{12} = 1$, which together with (3.2) implies

$$\bar{E}_6^2 = 5 + 9\bar{E}_4^3,\ \bar{\Delta} = 8\bar{E}_4^3 + 5,\ q\frac{d\bar{E}_{10}}{dq} = (5\bar{E}_4^3 + 4)\bar{\Delta}.$$

Thus,

$$\frac{1}{4}\overline{2E_{12} + \Delta}^2 = \frac{1}{4}(2 + \bar{\Delta})^2 = 1 + \bar{\Delta} + \frac{1}{4}(8\bar{E}_4^3 + 5)\bar{\Delta} = 1 + 3q\frac{d\bar{E}_{10}}{dq},$$

which is multiplicative. The proposition follows. □

4. Prime Powers

A normalized multiplicative power series $f(q) = \frac{1}{2a_0} + \sum_{n=2}^{\infty} a_n q^n$ is determined by a_0 and the coefficients a_n as n ranges over the set $\mathbb{P}$ of positive integral powers of primes. If it is also multiplicative, the normalization of $f(q)^2$ is

$$a_0 f(q)^2 = \frac{1}{4a_0} + q + \sum_{n=2}^{\infty} b_n q^n.$$

Each $n = p_1^{e_1} \cdots p_k^{e_k}$ which is not in $\mathbb{P}$ determines an equation

$$b_{p_1^{e_1} \cdots p_k^{e_k}} = b_{p_1^{e_1}} \cdots b_{p_k^{e_k}}.$$

Writing b_i formally as a polynomial $B_i(a_0, a_2, a_3, \ldots)$ with integer coefficients in the variables a_0 and $\{a_i \mid i \in \mathbb{P}\}$, we obtain the polynomial equation

$$P_{p_1^{e_1}\cdots p_k^{e_k}} = B_{p_1^{e_1}\cdots p_k^{e_k}} - B_{p_1^{e_1}} \cdots B_{p_k^{e_k}} = 0. \tag{4.1}$$

For $n \geq 2$, let k (resp. l) denote the largest element of $\mathbb{P}$ (resp. $\mathbb{N} \setminus \mathbb{P}$) in $[1, n]$, and let $\mathcal{X}_n$ denote the affine variety

$$\operatorname{Spec} \mathbb{C}[a_0, a_2, a_3, a_4, a_5, a_7, a_8, a_9, a_{11}, \ldots, a_k]/(P_6, P_{10}, \ldots, P_l).$$

We identify points on $\mathcal{X}_n$ with polynomials of degree $\leq n$ in $\mathbb{C}$. For $m \geq n$ we have projection morphisms $\phi_{m,n} \colon \mathcal{X}_m \to \mathcal{X}_n$, and for $n \geq 2$, we have the projection $\psi_n \colon \mathcal{X} \to \mathcal{X}_n$.

If $f(q)$ is a power series in q, we denote by $\mathbb{E}(f)$ the set of $n \geq 2$ such that the q^n coefficient of f is non-zero.

Lemma 4.1. *If $f, g \in \mathcal{X}_m$ satisfy $\phi_{m,n}(f) = \phi_{m,n}(g)$, then $\mathbb{E}(f-g) \cap [1, 2n]$ and*

$$\mathbb{E}(f(f-g)) \cap [1, \min(2n, m)]$$

are contained in $\mathbb{P}$. If $\mathbb{E}(f-g)$ contains any element other than m, its smallest element satisfies $k, k+1 \in \mathbb{P}$.

Proof. If $k \leq 2n$ is not in $\mathbb{P}$, then $k = k_1 k_2$, where k_1 and k_2 are relatively prime and $\leq n$. The q^{k_1} and q^{k_2} coefficients of f and g coincide, so $f, g \in \mathcal{X}_m$ and $k \leq m$ implies that the q^k coefficients of f and g are the same, giving the first claim. As $\mathbb{E}((f-g)^2) \subset [2n+2, \infty)$, we have

$$\mathbb{E}(f(f-g)) \cap [1, \min(2n, m)] = \mathbb{E}(f^2 - g^2) \cap [1, \min(2n, m)].$$

If $k \leq 2n$ is not in $\mathbb{P}$, we factor as before, and if $k \leq m$, the $k_1 k_2$ coefficients of f^2 and g^2 are determined by the k_1 and k_2 coefficients and are therefore the same. For the last claim, we note that if $k \leq m-1$ is the smallest element of $\mathbb{E}(f-g)$ and $k+1 \notin \mathbb{P}$, then $k+1 \notin \mathbb{E}(f-g)$ and $k+1 \notin \mathbb{E}(f(f-g))$. Writing $f = \frac{1}{2a_0} + q + \cdots$ and $f - g = c_k q^k + c_{k+1} q^{k+1} + \cdots$, we have $c_k \neq 0$ and $c_{k+1} = 0$, so

$$f(f-g) = \frac{c_k}{2a_0} q^k + c_k q^{k+1} + \cdots,$$

which implies $k+1 \in \mathbb{E}(f(f-g))$, giving a contradiction. □

Corollary 4.2. *If $k > 0$ is the minimal element of $\mathbb{E}(f-g)$ for $f, g \in \mathcal{X}$, then $k, k+1 \in \mathbb{P}$.*

Proof. Without loss of generality, we may assume $k \geq 5$. The corollary follows by applying Lemma 4.1 to $\psi_m(f)$ and $\psi_m(g)$ for $m = k+1$ and $n = k-1$. □

The condition $k, k+1 \in \mathbb{P}$ is very restrictive:

Lemma 4.3. *If k and $k+1$ both belong to $\mathbb{P}$ and $k > 8$, then k is a Mersenne prime or $k+1$ is a Fermat prime.*

Proof. Either k or $k+1$ is even and therefore a power of 2. The highest power of 2 dividing $p^{2^r(2s+1)} \pm 1$ is at most 2^{r+1} times the highest power of 2 dividing $p \pm 1$. Therefore, the only solutions of $2^m - p^n = \pm 1$ in integers $m, n, p > 1$ is $(3, 2, 3)$. If we allow $n = 1$ but insist that p is prime, we obtain precisely the solutions of Mersenne and Fermat type. □

For use in the next two sections, we prove a number of facts about $\mathbb{P}$ with special reference to Mersenne and Fermat primes.

Lemma 4.4. *If $p > 7$ is a Mersenne prime, then*

$$p + n \notin \mathbb{P} \quad \forall n \in \{2, 3, 5, 7, 8, 9, 11, 13, 14, 15\}.$$

Moreover, either $p + 4 \notin \mathbb{P}$ or $p + 6 \notin \mathbb{P}$.

Proof. Every Mersenne prime is of the form $2^\ell - 1$ for ℓ prime, and we may assume $\ell > 3$. For n odd between 3 and 15, $p + n$ is even and lies strictly between 2^ℓ and $2^{\ell+1}$. For $n = 2$, $p + n \notin \mathbb{P}$ by Lemma 4.3. For $n \in \{8, 14\}$, $p + n$ cannot be in $\mathbb{P}$ since it is divisible by 3 but is either 5 or 7 (mod 8) and therefore not a power of 3. Finally, one of $p + 4$ and $p + 6$ is divisible by 7 but cannot be a power of 7 since neither 3 nor 5 is a power of 7 (mod 8). □

Lemma 4.5. *If $p > 17$ is a Fermat prime, then*

$$p + n \notin \mathbb{P} \quad \forall n \in \{1, 3, 4, 5, 7, 8, 9, 10, 11\}.$$

Proof. For $n \leq 11$ odd, $p + n$ is an even number strictly between two consecutive powers of 2. For $n = 4$, $p + n$ is divisible by 3 but is not congruent to 3 (mod 8). If it is a power of 3, it is therefore a perfect square, which is impossible since

$$\left(2^{2^{k-1}}\right)^2 < 2^{2^k} + 1 + n < \left(2^{2^{k-1}} + 1\right)^2.$$

For $n = 8$, $p + n$ is not a square and therefore cannot be in $\mathbb{P}$ by a (mod 40) argument. Finally, $p + 10$ is divisible by 3. If $p + 10 = 3^r$, the congruences $3^r \equiv 12 \pmod{17}$ and $3^r \equiv 12 \pmod{257}$ would imply the inconsistent congruences $r \equiv 13 \pmod{16}$ and $r \equiv 97 \pmod{256}$. This rules out the case $p > 257$, and for $p = 257$, $267 \notin \mathbb{P}$. □

Lemma 4.6. *If $p > 5$ is a Fermat prime, then $2p \pm 1 \notin \mathbb{P}$.*

Proof. As $p = 2^{2^k} + 1$ and $k \geq 2$, we have $3|2p - 1$ and $5|2p + 1$. By Lemma 4.3, $2p - 1$ cannot be a power of 3. As for $2p + 1$, it is congruent to 3 (mod 8), so it cannot be a power of 5. □

Lemma 4.7. *If $p > 7$ is a Mersenne prime and $2p + 3 \in \mathbb{P}$, then $3p + 4 \notin \mathbb{P}$.*

Proof. Assuming $p = 2^n - 1$ is Mersenne, if $2p + 3$ is prime, it is a Fermat prime ≥ 5 and therefore 2 (mod 5). It follows that $p \equiv 2 \pmod{5}$, and

therefore that 5 divides $3p+4$. If $3p+4$ is of the form 5^m, then $5^m \equiv 1 \pmod{2^n}$. The highest power of 2 dividing $5^m - 1$ is 2^{m+2},

$$3 \geq \frac{5^m - 1}{2^{m+2}} > 2^{m-2}.$$

This implies $m \leq 3$. Now, $5^3 - 1$ is not divisible by 3 at all, and while $(5^2-4)/3$ is a Mersenne prime, it is not greater than 7. □

Lemma 4.8. *If $p_1, p_2 > 3$ are Mersenne primes, then $p_1 + p_2 + 1 \notin \mathbb{P}$.*

Proof. Mersenne primes greater than 3 are always congruent to 1 (mod 3). Thus, 3 divides $p_1 + p_2 + 1$. However, $3^n + 1$ is never divisible by 8, so $p_1 + p_2 + 1$ cannot be a power of 3. □

Lemma 4.9. *If $3 < p_1 < p_2$, p_1 is a Mersenne prime, and p_2 is a Fermat prime, then $2p_1 + p_2 + 2 \notin \mathbb{P}$.*

Proof. As p_1 and p_2 are Mersenne and Fermat respectively, they are 1 and 2 (mod 3) respectively, so $2p_1 + p_2 + 2$ is divisible by 3. As $2p_1 + p_2 + 2 \equiv 1 \pmod 8$, if $2p_1 + p_2 + 2 \in \mathbb{P}$, there exists n such that $2p_1 + p_2 + 2 = 3^{2n}$. If $n = 2^r s$, where s is odd, then the highest power of 2 dividing $3^{2n} - 1$ is 2^{r+3}. If $p_1 = 2^m - 1$, then $r + 3 \geq m + 1$. As $p_2 - 1$ is a perfect square, it is less than or equal to $(3^n - 1)^2$, so

$$2 \cdot 3^n - 1 \leq 2p_1 + 3 = 2^{m+1} + 1 \leq 2^{r+3} + 1,$$

i.e.,

$$3^{2^r s} = 3^n \leq 2^{r+2} + 1 < 3^{r+2}.$$

Thus, $2^r s < r + 2$, so $s = 1$ and $r \in \{0, 1\}$. This is impossible since $p_1 \geq 7$. □

Lemma 4.10. *For every odd prime ℓ, every positive integer d not divisible by ℓ, and every residue class (mod d), there exists an integer $n \leq (2d^2)^{9\log(2d)}$ such that n belongs to the specified residue class and $\binom{2n}{n}$ is not divisible by ℓ.*

Proof. Let $\ell = 2k + 1$. If the digits in the base ℓ expansion of n are all $\leq k$, then the second condition is satisfied. In particular, if $k \geq d$, then the theorem is certainly true since then the integers in $[1, k]$ represent every residue class (mod d). We therefore assume that $\ell < 2d$.

Let

$$F_r(x) = \prod_{i=0}^{r-1} \Big(1 + x^{\ell^i} + x^{2\ell^i} + \cdots + x^{k\ell^i}\Big).$$

Then $F_r(x)$ is a sum of distinct terms x^n where $\ell \nmid \binom{2n}{n}$. We would like to show that for a suitable value of r, all residue classes of d are represented among the exponents of $F_r(x)$. As $F_r(1) = (k+1)^r$, it suffices to prove that

$$|F_r(\zeta^i)| < \frac{(k+1)^r}{d},\ \zeta = e^{2\pi i/d},\ 1 \leq i < d.$$

If m is not congruent (mod d) to an integer in the interval $[-3d/4\ell, 3d/4\ell]$, then

$$\Big| \sum_{j=0}^{k} \zeta^{jm} \Big| = \frac{\big| 1 - \zeta^{(k+1)m} \big|}{\big| 1 - \zeta^m \big|} \le \frac{2}{|2 \sin(\pi m/d)|} \le \frac{1}{|\sin(3\pi/4\ell)|}.$$

For $0 \le x \le \pi/6$, $\sin x \ge 3x/\pi$. Therefore, if $\ell > 3$, then

$$\Big| \sum_{j=0}^{k} \zeta^{jm} \Big| \le \frac{4\ell}{9} < \frac{8(k+1)}{9}.$$

On the other hand, if $\ell = 3$, then $|1 + \zeta^m| \le \sqrt{2} < \frac{8(k+1)}{9}$.

If m is not congruent to 0 (mod d) and $\ell^s > d$, then m, $m\ell$, $m\ell^2$, $\dots$, $m\ell^{s-1}$ cannot all be congruent (mod d) to integers in $[-3d/4\ell, 3d/4\ell]$. Therefore, the product of any s consecutive multiplicands in $F_r(\zeta)$ is less than $\frac{8}{9}(k+1)^s$. If $t > \frac{\log d}{\log 9 - \log 8}$, then

$$|F_{st}(\zeta^m)| < F_{st}(1)/d.$$

We may therefore take n to be less than

$$\ell^{st} < \ell^{\left(\frac{\log d}{\log \ell} + 1\right) t} < (2d^2)^{9 \log(2d)}.$$

The proposition follows. □

Lemma 4.11. *For all integers $k > 1$, there exists a prime $\ell \le 4k + 1$ such that ℓ does not divide $2^k - 2$.*

Proof. For any $s \in \mathbb{N}$,

$$\frac{2^{2s}}{2s} = \frac{2 + \sum_{i=1}^{2s-1} \binom{2s}{i}}{2s} \le \binom{2s}{s} = \frac{(2s)!}{s!^2} = \prod_p p^{k_p},$$

where $p^{k_p} \le 2s$ for all p. As $\pi(n) \le \frac{n+1}{2}$ and $\prod_{p \le n} p \ge n$,

$$\prod_{p \le 2s} p \ge \frac{2^{2s}}{2s \prod_{p \le \sqrt{2s}} p^{k_p - 1}} \ge \frac{2^{2s}}{2s \prod_{p \le \sqrt{2s}} \frac{2s}{p}} \ge 2^{2s} (2s)^{-1 - \sqrt{2s}/2}.$$

For $s \ge 16$, we have $1 - \sqrt{2}/2 < s^{-1/2}$ and $\log 2s < \frac{3}{2}\sqrt{s} \log 2$, so

$$\sum_{p \le 2s} \log p \ge 2s \log 2 - \left(\frac{\sqrt{2s}}{2} + 1 \right) \log 2s \ge 2s \log 2 - \sqrt{s} \log 2s \ge \frac{s \log 2}{2}.$$

If ℓ is the smallest prime not dividing $2^k - 2$ and $\ell > 31$ then $s = \frac{\ell - 1}{2} \ge 16$, so

$$\frac{s \log 2}{2} \le \sum_{p \le 2s} \log p \le \log(2^k - 2) < k \log 2.$$

Thus, $\ell \le 4k + 1$. This proves the existence of the desired prime ℓ when $k \ge 8$. For $k \le 7$, we can set $\ell = 5$ except for $k = 5$, for which we can set $\ell = 7$. □

Lemma 4.12. *For $k \geq 5$, an arithmetic progression of integers with initial term, $a \in [1, 2^{2k+1}]$, common difference $2^k - 2$, and length 2^{k-2} contains an integer not in $\mathbb{P}$, except when $(k, a) = (5, 19)$.*

Proof. For $k \geq 6$, there exists a prime $\ell < 2^{k-3}$ such that $\ell \nmid 2^k - 2$. Then any such progression contains at least two terms divisible by ℓ, differing by $(2^k - 2)\ell$. At least one is not divisible by ℓ^2, so if they are both powers of ℓ, then $2^k - 1 = \ell^{r-1}$. By Lemma 4.3, this means $r = 2$ which is impossible since $\ell \leq 2^{k-3}$. Thus, the progression contains an integer not in $\mathbb{P}$. For $k = 5$, it is easy to check that $a = 19$ is the only initial term which gives an 8-term progression consisting only of elements of $\mathbb{P}$. □

5. Reduction to the Sparse Case

The polynomial equations P_n, $n \notin \mathbb{P}$, defined in (4.1) are of weighted degree n where each variable a_m has degree m. They are therefore linear in a_m for $m > n/2$. In this section we systematically exploit this linearity.

Proposition 5.1. *Let $n \leq 15$ be an integer. Let*

$$F = \begin{pmatrix} a_2 & a_4 & a_5 & a_6 & a_8 & a_9 & a_{10} & a_{11} & a_{12} \\ 1 & a_3 & a_4 & a_5 & a_7 & a_8 & a_9 & a_{10} & a_{11} \\ 0 & 1 & a_2 & a_3 & a_5 & a_6 & a_7 & a_8 & a_9 \\ 0 & 0 & 0 & 0 & 1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix},$$

$$M' = \begin{pmatrix} a_2 & a_3 & a_4 & a_5 & a_7 & a_8 & a_9 & a_{11} & a_{13} & a_{14} \\ 1 & a_2 & a_3 & a_4 & a_6 & a_7 & a_8 & a_{10} & a_{12} & a_{13} \\ 0 & 0 & 0 & 0 & 1 & a_2 & a_3 & a_5 & a_7 & a_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a_3 & a_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a_2 \end{pmatrix},$$

$$M'' = \begin{pmatrix} a_2 & a_3 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{11} & a_{13} & a_{14} & a_{15} \\ 1 & a_2 & a_4 & a_5 & a_6 & a_7 & a_8 & a_{10} & a_{12} & a_{13} & a_{14} \\ 0 & 0 & 1 & a_2 & a_3 & a_4 & a_5 & a_7 & a_9 & a_{10} & a_{11} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a_3 & a_4 & a_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a_2 & a_3 \end{pmatrix}.$$

If every point in

(5.1)

$$\{f \in \mathcal{X}_n \mid \mathrm{rk}(F) \leq 3\} \cup \{f \in \mathcal{X}_n \mid \mathrm{rk}(M') \leq 4\} \cup \{f \in \mathcal{X}_n \mid \mathrm{rk}(M'') \leq 4\}$$

is the image of one and only one point of $\mathcal{X}$, then $\mathcal{X}$ is of affine type.

Proof. We apply Proposition 2.5, where $\mathcal{V} \subset \mathcal{X}_n$ is the union of the three closed subvarieties defined by the conditions that one of F, M', or M'' is not of full rank. The hypothesis guarantees condition (2) and condition (1) for elements of $\mathcal{X}_n$ in which at least one of the matrices is not of full rank. In verifying the remaining conditions, we may therefore assume that all three matrices are of full rank.

Suppose $f, g \in \mathcal{X}$ map to the same element in $\mathcal{X}_n$, and let $k = \inf \mathbb{E}(f-g)$. By Corollary 4.2 and Lemma 4.3, either $k+1$ is a Fermat prime or k is a Mersenne prime.

Suppose $k+1$ is Fermat. By Lemma 4.1 and Lemma 4.5,

$$\mathbb{E}(f(f-g)) \cap [k, k+12] \subseteq \{k, k+1, k+3, k+7\}.$$

Defining x_i to be the q^{k+i} coefficient of $f-g$ for $i = 0, 1, \dots, 12$, we have $x_i = 0$ for $i \in \{2, 4, 5, 6, 8, 9, 10, 11, 12\}$, so we obtain

$$(x_0\, x_1\, x_3\, x_7)F = 0,$$

which by the rank condition implies that $x_0 = x_1 = x_3 = x_7 = 0$, contrary to the definition of k.

If k is Mersenne, then by Lemma 4.1 and Lemma 4.4, either

$$\mathbb{E}(f(f-g)) \cap [k, k+15] \subseteq \{k, k+1, k+4, k+10, k+12\}$$

or

$$\mathbb{E}(f(f-g)) \cap [k, k+15] \subseteq \{k, k+1, k+6, k+10, k+12\}.$$

Defining x_i to be the q^{k+i} coefficient of $f-g$ for $i = 0, 1, \dots, 15$, we have $x_i = 0$ for $i \in \{2, 3, 4, 5, 7, 8, 9, 11, 13, 14, 15\}$ or $i \in \{2, 3, 5, 6, 7, 8, 9, 11, 13, 14, 15\}$ respectively, and we therefore have

$$(x_0\, x_1\, x_4\, x_{10}\, x_{12})M'' = 0$$

or

$$(x_0\, x_1\, x_6\, x_{10}\, x_{12})M' = 0$$

respectively. Either way, we get a contradiction, implying that $f = g$, as claimed. This gives condition (1) for $y \in \mathcal{X}_n \setminus \mathcal{V}$.

A slight variant gives (3). In the Fermat case, we assume $m \geq n + 12$, and let $f, g \in \mathcal{X}_m$ map to the same element in $\mathcal{X}_n$ but different elements in $\mathcal{X}_{n+1}$. By Lemma 4.1 and Lemma 4.3, either $k+1$ is a Fermat prime or k is a Mersenne prime, and the argument proceeds as before. In the Mersenne case, we assume $m \geq n + 15$, and otherwise the argument is the same.

Now consider a bounded open neighborhood $U \subseteq \mathcal{X}_n$ of polynomials such that the full rank condition for F, M', and M'' and the condition $a_0 \neq 0$ hold on the closure $\bar{U}$ in the complex topology. For (4), it is enough to show that for each such U there exists $m > n$ such that $\phi_{m,n}^{-1}(U)$ is bounded. If $n+1 \notin \mathbb{P}$, then factoring $n+1 = k_1 k_2$, where the $k_i > 1$ are relatively prime, we can take $m = n+1$, since $a_{n+1} = a_{k_1} a_{k_2}$ is bounded on U. If $n+2 \notin \mathbb{P}$, we can take $m = n+2$. Factoring $n+2 = k_1 k_2$, $a_{n+2} = a_{k_1} a_{k_2}$ is bounded on U, and the same is true for a_{n+1}, since (in the notation of Definition 3.1)

$$a_{k_1} a_{k_2} + 2a_0 a_{n+1} + a_0(a_2 a_n + a_3 a_{n-1} + \cdots + a_n a_2) = b_{n+2} = b_{k_1} b_{k_2}$$

can be regarded as a linear equation in a_{n+1} whose coefficients are polynomial in $a_0, a_2, \dots, a_n$. Thus, it suffices to consider the cases that n is Mersenne or that $n+1$ is Fermat.

If $n+1$ is Fermat, we take $m = n+12$. Each of $n+2, n+4, n+5, \dots, n+12$ can be written as a product of two relatively prime integers $\leq n$,

so $a_{n+2}, \dots, a_{n+12}$ are bounded on U. To prove that $a_n, a_{n+1}, a_{n+3}, a_{n+7}$ are likewise bounded on U, we note that a_k and b_k are bounded on U for $k - n \in \{2, 4, 5, 6, 8, 9, 10, 11, 12\}$, so

$$(a_0\, a_1\, a_3\, a_7)F$$

is bounded on U. As F is of full rank on $\bar{U}$, this implies a_0, a_1, a_3, a_7 are bounded on U. The same argument applies to Mersenne primes, taking $m = n + 15$ and using M' or M'' in place of F.

□

Lemma 5.2. *If* $\mathrm{rk}(F) \le 3$, $\mathrm{rk}(M') \le 4$, *or* $\mathrm{rk}(M'') \le 4$, *then either* $a_2 = a_3 = a_4 = 0$ *or* $a_3 = 1$ *and* $a_0 = a_2 = a_4 = \pm 1$.

Proof. This follows by solving the equations P_6, P_{10}, P_{12}, P_{14}, P_{15} of (4.1) together with the equations expressing any of the three rank conditions in (5.1). □

Proposition 5.3. *If* $\epsilon \in \{1, -1\}$, $f \in \mathcal{X}$, *and*

$$f = \frac{\epsilon}{2} + q + \epsilon q^2 + q^3 + \epsilon q^4 + a_5 q^5 + a_6 q^6 + \cdots,$$

then $a_n = \epsilon^{n+1}$ *for all* $n \ge 1$.

Proof. By Lemma 3.3, we may assume $\epsilon = 1$. Solving the equations P_n, $6 \le n \le 72$, we obtain the unique solution $a_n = 1$ for $2 \le n \le 15$. Thus any solution f maps to the same element of $\mathcal{X}_{15}$ as $\frac{1}{2} + \sum_{i=1}^{\infty} q^i$, which is a special case of solution (xii). By Corollary 4.2 and Lemma 4.3, the smallest value m for which $a_m \ne 1$ is either a Mersenne prime or one less than a Fermat prime. Either way, comparing f with

$$g = \frac{1}{2} + (a_m - 1)q^m + (a_{m+1} - 1)q^{m+1} + \sum_{i=1}^{2m-1} q^i \in \mathcal{X}_{2m-1}$$

either $\psi_{2m-1}(f) = g$ or $k = \inf \mathbb{E}(\psi_{2m-1}(f) - g)$ satisfies $k, k+1 \in \mathbb{P}$.

If $m + 1$ is a Fermat prime, then this is possible if and only if $k = 2m - 1$ (in which case k is a Mersenne prime). Whether $a_{2m-1} = 1$ or not, $2m+1, 2m+3 \notin \mathbb{P}$ by Lemma 4.6, so the equations P_{m+2}, P_{2m+1}, and P_{2m+3} read:

$$\begin{aligned} m + 2 &= 2a_m + 2a_{m+1} + m - 2, \\ 2m + 1 &= 2a_m a_{m+1} + 2a_{2m-1} + 2a_m + 2m - 5, \\ 2m + 3 &= 2a_{2m-1} + 2a_m + 2m - 1. \end{aligned}$$

Solving, we obtain $a_m = a_{m+1} = 1$, giving a contradiction.

We may therefore assume that $m > 7$ is Mersenne. In this case, $a_i = 1$ for $i \le 2m - 1$, and also $m + 2, 2m \notin \mathbb{P}$, so $a_{m+2} = 1$, $a_{2m} = a_m$, $b_{m+2} = m + 2$, and $b_{2m} = 2b_m = 2m + 2a_m - 2$. Solving P_{m+2} and P_{2m}, we obtain

$(a_m, a_{m+1}) \in \{(1,1),(2,0)\}$. By hypothesis, the latter alternative must be true. We now define

$$g = \frac{1}{2} + \sum_{i=1}^{m^2+m-1} c_i q^i$$

where

$$c_i = \begin{cases} 2 & \text{if } m|i, \\ 0 & \text{if } m+1|i, \\ 1 & \text{otherwise.} \end{cases}$$

It is impossible that $g = \psi_{m^2+m-1}(f)$, since g does not lift to an element of $\mathcal{X}_{m^2+m}$. Let $k = \inf \mathbb{E}(f-g)$.

If $k \leq 4m$, then $k = 2m+2$, $k+1$ is Fermat, and $a_k \neq c_k = 0$. The multiplicativity of f^2 implies $a_{3m+2} = 2a_{2m+2} + 1$ and $a_{3m+4} = -2a_{2m+2} + 1$. Now by Lemma 4.7, $3m+4 \notin \mathbb{P}$. Therefore, $a_{3m+4} = 1$, contrary to assumption. Thus, we may assume $k \geq 4m$.

We define c_i as above. If k is Mersenne, we define

$$g = \frac{1}{2} + \sum_{i=1}^{k+m+1} c_i q^i + (a_k - 1)(q^k - q^{k+1} - q^{m+k-1}).$$

Then $\psi_{m+k-2}(g) \in \mathcal{X}_{m+k-2}$, so it coincides with $\psi_{m+k-2}(f)$ If $m+k-1 \notin \mathbb{P}$, then P_{m+k-1} shows there is no way of lifting $\psi_{m+k-2}(f)$ to $\mathcal{X}_{m+k-1}$, which is absurd. Thus, $m+k-1 \in \mathbb{P}$, and $\psi_{m+k}(g) \in \mathcal{X}_{k+m}$ must coincide with $\psi_{m+k}(f)$. By Lemma 4.8, $k+m+1 \notin \mathbb{P}$, so P_{m+k+1} shows there is no way of lifting $\psi_{m+k}(f)$ to $\mathcal{X}_{m+k+1}$, which is absurd.

If $k+1$ is Fermat, we define

$$g = \frac{1}{2} + \sum_{i=1}^{k+2m+3} c_i q^i + a_k(q^k(1-q) + 2q^{m+k}(1-q^2) - 3q^{2m+k-1}(1-q^2)^2).$$

Now, $\psi_{m+k-1}(g) \in \mathcal{X}_{m+k-1}$ coincides with $\psi_{m+k-1}(f)$. If $m+k \notin \mathbb{P}$, then P_{m+k} shows there is no way of lifting $\pi_{m+k-1}(f)$ to $\mathcal{X}_{m+k}$, which is absurd. We repeat the argument, replacing $m+k-1$ successively by $m+k+1$, $m+2k-2$, $m+2k$, $m+2k+2$. We conclude that $m+2k+2 \in \mathbb{P}$, which is impossible by Lemma 4.9.

The only remaining possibility is $k = m^2+m-1$, and $k \in \mathbb{P}$. In this case, we set

$$g = \frac{1}{2} + \sum_{i=1}^{m^2+2m-2} c_i q^i$$

where

$$c_i = \begin{cases} 2 & \text{if } i = m^2+m-1, \\ 2 & \text{if } i \leq m^2 \text{ and } m|i, \\ 0 & \text{if } i = m^2+2m-2 \text{ or } m+1|i, \\ 1 & \text{otherwise.} \end{cases}$$

It is impossible that $m^2+m \le \mathbb{E}(f-g) \le m^2+2m-2$ since there is no Mersenne or Fermat prime in that interval. However, g does not lift to an element of $\mathcal{X}_{m^2+2m-1}$, which gives a contradiction. □

Lemma 5.4. *Suppose $a_2 = 0$ and $\mathrm{rk}(F) \le 3$, $\mathrm{rk}(M') \le 4$, or $\mathrm{rk}(M'') \le 4$. Let*

$$m = \inf\{i \ge 2 \mid a_i \ne 0\} \tag{5.2}$$

either m is undefined (in which case $f(q)$ is linear in q), m is a Mersenne prime ≥ 31, or $m+1$ is a Fermat prime ≥ 257.

Proof. As $a_2 = 0$, we have $a_3 = a_4 = 0$, and also $a_6 = 0$. Equation P_6 implies $a_5 = 0$, and P_{15} implies $a_7 a_8 = 0$. If $a_7 \ne 0$, the equations P_i as i runs through all positive integers ≤ 92 not in $\mathbb{P}$ are inconsistent; if $a_7 = 0$, the equations up through $i = 34$ imply $a_8 = a_9 = \cdots = a_{16} = 0$. The multiplicativity of f implies $m \in \mathbb{P}$; the multiplicativity of f^2 implies $m+1 \in \mathbb{P}$. The result now follows from Lemma 4.3. □

Definition 5.5. *We say f is* sparse *if the* index *m of (5.2) is ≥ 16.*

Proposition 5.6. *If $f, g \in \mathcal{X}$ are not sparse and $f \equiv g \pmod{x^{17}}$, then $f = g$. In other words, a non-sparse element of $\mathcal{X}$ is determined by its first 17 coefficients.*

Proof. By Lemma 5.2 and Proposition 5.3, if F, M', or M'' has less than full rank then either f is a solution of type (xi) or $a_2 = 0$. In the latter case, f is sparse by Lemma 5.4. Thus, we may assume full rank. By Proposition 5.1, this implies that all higher coefficients are determined from the first 17 coefficients. □

6. Sparse Solutions and Mandelbrot Polynomials

Lemma 6.1. *Let S be a set of positive integers such that if $s, t \in S$ are relatively prime, then $st \in S$. Let n be a positive integer and $c_1, c_2, \ldots$ a multiplicative sequence such that if $m \in (1, n)$ is an integer and $c_m \ne 0$, then $m \in S$. Then for all integers $m \in [n, 2n)$ with $c_m \ne 0$, either $m \in S$ or $m \in \mathbb{P}$.*

Proof. If for some $m \in [n, 2n) \setminus \mathbb{P}$ we have $c_m \ne 0$, then m can be factored $m = m_1 m_2$, where m_1 and m_2 are relatively prime and greater than 1. Thus $m_1, m_2 \in (1, n)$, and by multiplicativity, both c_{m_1} and c_{m_2} are non-zero. Therefore $m_1, m_2 \in S$, so $m \in S$. □

It will be useful to note that the same argument gives the same result for odd values of m in $[n, 3n)$.

Lemma 6.2. *Let S be a set of positive integers, $f \in \mathcal{X}$, and m the smallest integer in $\mathbb{E}(f) \setminus S$. If $m+1$ cannot be written as a sum of two elements of S, either $a_{m+1} \ne 0$ or $b_{m+1} \ne 0$.*

Proof. For $2 \leq i \leq m-1$, $a_i \neq 0$ only if $i \in S$. As $m+1$ is not the sum of any pair of elements in S,

$$b_{m+1} = a_{m+1} + 2a_0a_m + a_0 \sum_{i=2}^{m-1} a_i a_{m+1-i} \tag{6.1}$$

simplifies to $a_{m+1} + 2a_0a_m$. Since $a_m \neq 0$, either $a_{m+1} \neq 0$ or $b_{m+1} \neq 0$. □

Lemma 6.3. *If $f \in \mathcal{X}$ is sparse, then $\mathbb{E}(f) \subset 1 + 6\mathbb{N}$, that is, for $n > 1$, $a_n = 0$ except when $n \equiv 1 \pmod 6$.*

Proof. Suppose that n is such that for all positive integers $1 < m < n$, $a_m \neq 0$ implies $m \equiv 1 \pmod 6$. Applying Lemma 6.1 to $S_1 = 1 + 6\mathbb{N}$ and the sequence a_i, we see that for $m \in [n, 2n)$, $a_m \neq 0$ implies $m \in S_1$ or $m \in \mathbb{P}$. Also, for $1 < m < n$, $b_m \neq 0$ implies m is congruent to 1 or 2 (mod 6). Applying Lemma 6.1 to $S_{1,2} = 1 + 6\mathbb{N} \cup 2 + 6\mathbb{N}$, for $m \in [n, 2n)$, $b_m \neq 0$ implies $m \in S_{1,2}$ or $m \in \mathbb{P}$.

If the lemma does not hold, we can define n to be the smallest integer in $\mathbb{E}(f) \setminus S_1$. As n is a prime power not in S_1, it is not divisible by 6, so $n+1$ is not in $S_{1,2}$ and therefore cannot be written as a sum of two elements of S_1. Applying Lemma 6.2 to $S = S_1$, either $a_{n+1} \neq 0$ or $b_{n+1} \neq 0$, and as $n+1$ belongs to neither S_1 nor $S_{1,2}$, either condition implies $n+1 \in \mathbb{P}$. As $n \geq 16$, either n is a Mersenne prime or $n+1$ is a Fermat prime. All Mersenne primes ≥ 7 lie in S_1, so only the latter case is possible.

Now suppose that there is another value $m \in E(f) \setminus S_1$ which lies in $(n, 2n)$. As before, $m \in \mathbb{P}$, and $m+1$ is not in S_1 or $S_{1,2}$, so $a_{m+1} = 0$, and by Lemma 6.2, $b_{m+1} = 0$. Note that $n < m < 2n$ implies that m is an odd prime power, so $m+1$ is 4 or 0 (mod 6) and can be written as a product m_1m_2 with $1 < m_1, m_2 < n$ and m_1 and m_2 relatively prime. Therefore, m_1 and m_2 cannot both belong to $S_{1,2}$, and if either is 2, the other cannot belong to $S_{1,2}$. Therefore, $b_{m+1} = b_{m_1}b_{m_2} = 0$, which is a contradiction. Thus $\mathbb{E}(f) \setminus (S_1 \cup \{n\})$ contains no element smaller than $2n$. In particular, it does not contain $n+1$, so $a_{n+1} = 0$, and so $b_{n+1} \neq 0$, by Lemma 6.2.

Now, by Lemma 4.6, $2n+1 \notin \mathbb{P}$. By the remark following Lemma 6.1, $a_{2n+1} = 0$. Likewise $a_2 = 0$ and $a_{n+1} = 0$. Let $m = 2n+1$. As $m+1 = 2n+2 \notin S_{1,2}$, (6.1) simplifies to $b_{2n+2} = a_{2n+2} = 0$, which is absurd since $b_{2n+2} = b_2b_{n+1} \neq 0$.

□

Corollary 6.4. *If $f \in \mathcal{X}$ is a nonlinear sparse power series, its index is a Mersenne prime.*

Lemma 6.5. *If $f \in \mathcal{X}$ is a sparse series of index p, then for all $n \in \mathbb{E}(f)$, there exists r such that $n \equiv r \pmod{p-1}$, and $1 \leq r \leq \frac{2n}{p-1} - 1$.*

Proof. We proceed by induction. We say $n \geq p$ is *a-typical* (resp. *b-typical*) if it is congruent (mod $p-1$) to a positive integer $r \leq \frac{2n}{p-1} - 1$ (resp $r \leq$

$\frac{2(n-1)}{p-1}$.) The sum of two a-typical integers is a-typical, and the same is true for products since for $n_1, n_2 \geq p$, we have

$$\Big(\frac{2n_1}{p-1}-1\Big)\Big(\frac{2n_2}{p-1}-1\Big) = \frac{4}{(p-1)^2}n_1n_2 - \left(\frac{2n_1+2n_2}{p-1}-1\right) \leq \frac{2}{p-1}n_1n_2 - 1.$$

Likewise, the set of b-typical integers is closed under addition and multiplication since

$$\frac{2(n_1-1)}{p-1}\frac{2(n_2-1)}{p-1} = \frac{4}{(p-1)^2}(n_1n_2-(n_1+n_2-1)) \leq \frac{2}{p-1}(n_1n_2-1).$$

The lemma asserts that every element $n \in \mathbb{E}(f)$ is a-typical. If n is the smallest exception, then $a_n \neq 0$, so $n \notin \mathbb{P}$ implies we can factor $n = n_1n_2$ where $n_1, n_2 > 1$ and $a_{n_i} \neq 0$ for $i = 1, 2$. As f has index p, we have $n_i \geq p$ for $i = 1, 2$, so n_1 and n_2 are a-typical, implying n is a-typical, contrary to assumption. Moreover, if $b_k \neq 0$ for $2 < k < n$, then there exist non-negative integers i, j such that $i + j = k$, $a_i \neq 0$, and $a_j \neq 0$. Thus, i and j are either ≤ 1 or are a-typical. It follows that k is a-typical, one greater than an integer which is a-typical, or the sum of two a-typical integers, and in each case, k is b-typical.

Suppose that $n+1 \notin \mathbb{P}$. In general, subtracting 1 from a b-typical integer leaves either an a-typical integer or a multiple of $p-1$. As n is a prime power, it is not divisible by $p-1$, so $n+1$ is not b-typical and therefore not a-typical. Writing $n+1 = n_1n_2$ for $n_1, n_2 > 1$ relatively prime, it is impossible that n_1 and n_2 are both b-typical and therefore impossible they are both are a-typical, so $a_{n+1} = 0$. Applying Lemma 6.2 with S equal to the set of a-typical integers, we deduce $b_{n+1} \neq 0$. As n_1 and n_2 are not both b-typical, this gives a contradiction. We conclude that since $n \geq p \geq 17$, either n is a Mersenne prime or $n+1$ is a Fermat prime. By Corollary 6.4, n is in fact a Mersenne prime. Writing $p = 2^a - 1$ and $n = 2^b - 1$ we have $2^a \equiv 2 \pmod{p-1}$, so

$$n \equiv 2^{1+b-a} - 1 \pmod{p-1}.$$

Setting $r = 2^{1+b-a} - 1$, we have

$$(p-1)(r+1) = 2^{1+b} - 2^{2+b-a} < 2^{1+b} - 2 = 2n,$$

so n is a-typical, which gives a contradiction. □

Proposition 6.6. *If $f \in \mathfrak{X}$ is sparse of index p, then $a_p \neq 1$.*

Proof. If $a_p = 1$, then the polynomial condition P_{2p} defined in (4.1) implies $a_{2p-1} = 0$. By Lemma 6.5, if a_i and a_j are non-zero, $i + j \equiv 2 \pmod{p-1}$, and $i + j < p^2/2$, then either $i = 0$, $j = 0$, or $i \equiv j \equiv 1 \pmod{p-1}$. The first two possibilities are ruled out by Lemma 6.3 (note that $p \equiv 1 \pmod 6$), so $p-1$ must divide $i-1$ and $j-1$. Thus

$$b_{k(p-1)+2} = \frac{a_{k(p-1)+1}}{a_0}$$

for $1 \le k < \frac{p+1}{2}$. For $2 \le k < \frac{p+1}{2}$, the highest power of 2 dividing $k(p-1)+2$ is less than $p+1$, so $a_{k(p-1)+1} = 0$.

Equation $P_{p(p+1)}$ guarantees that there is some $n > p$ for which $a_n \neq 0$. Suppose that the smallest such n satisfies $n < p^2/2$. We have just proved that $n \not\equiv 1 \pmod{p-1}$. For $r, s > 1$, $a_r a_s \neq 0$ implies $rs \ge p^2$; thus $n \in \mathbb{P}$. Likewise, $b_{n+1} = 2a_0 a_n \neq 0$ so $n+1 \in \mathbb{P}$. By Lemma 6.3, $n+1$ cannot be a Fermat prime, so n is a Mersenne prime. If n reduces to $s \pmod{p-1}$, $1 < s < p-1$, an easy induction shows that for every residue class r, $1 < r < s$, and every $m < p^2/2$, $m \equiv r \pmod{p-1}$, we have $a_m = 0$. Therefore,

$$0 = b_{n+p} = \frac{a_{n+p-1} + a_n}{a_0},\ 0 = b_{n+2p-1} = \frac{a_{n+2p-1} + a_{n+p-1}}{a_0},\ \dots$$

In particular, if $n \le m < p^2/2$, and $m \equiv n \pmod{p-1}$, then $a_m \neq 0$. Since the largest possible Mersenne prime less than $p^2/2$ is $\le \frac{(p+1)^2}{4}$, we have an arithmetic progression of at least $(p+1)/4$ terms with common difference $p-1$ and every term in $\mathbb{P}$.

If the smallest element n of the set $\{n > p \mid a_n \neq 0\}$ exceeds $p^2/2$, then proceeding as before, either n is Mersenne (necessarily $\frac{p^2+2p-1}{2}$) or $n = p^2 + p - 1$. In either case, by induction

$$a_n = -a_{n+(p-1)} = a_{n+2(p-1)} = -a_{n+3(p-1)} = \cdots = -a_{n+\frac{p-3}{4}(p-1)}.$$

Thus, the proposition follows from Lemma 4.12. □

Definition 6.7. *We define the* Mandelbrot polynomials $M_i(y)$ *by the recursive formula*

$$M_n(y) = \begin{cases} y & \text{if } n = 1, \\ -\frac{1}{2}\sum_{i=1}^{n-1} M_i(y) M_{n-i}(y) & \text{if } n > 1 \text{ odd}, \\ \frac{1}{2} M_{n/2}(y) - \frac{1}{2}\sum_{i=1}^{n-1} M_i(y) M_{n-i}(y) & \text{if } n > 1 \text{ even}. \end{cases}$$

Thus,

$$M_2(y) = \frac{-y^2 + y}{2},\ M_3(y) = \frac{y^3 - y^2}{2},$$
$$M_4(y) = \frac{-5y^4 + 6y^3 - 3y^2 + 2y}{8},\ M_5(y) = \frac{7y^5 - 10y^4 + 5y^3 - 2y^2}{8},$$
$$M_6(y) = \frac{-21y^6 + 35y^5 - 21y^4 + 13y^3 - 6y^2}{16}, \dots$$

The definition is motivated by the following proposition:

Proposition 6.8. *If $f \in \mathcal{X}$ is sparse of index p, then for $1 \le i \le \frac{p-1}{2}$, $M_i(a_p) = 0$ whenever $i(p-1)+1 \notin \mathbb{P}$.*

Proof. Let $c_i = a_{i(p-1)+1}$. We have seen that

$$b_{k(p-1)+2} = \frac{1}{2a_0} \sum_{i=0}^{k} c_i c_{k-i}.$$

For $2 \leq k \leq \frac{p-1}{2}$, $k(p-1)+2$ is even, but the highest power of 2 dividing it is $< p+1$. Therefore,

$$b_{k(p-1)+2} = \begin{cases} 0 & \text{if } k \geq 3 \text{ is odd,} \\ \frac{b_2 b_{k(p-1)+2}}{2} & \text{if } k \geq 2 \text{ is even.} \end{cases}$$

As $b_2 = 1/2a_0$, we have

$$\sum_{i=0}^{k} c_i c_{k-i} = \begin{cases} 0 & \text{if } k \geq 3 \text{ is odd,} \\ \frac{b_{k(p-1)+2}}{2} = c_{k/2} & \text{if } k \geq 2 \text{ is even.} \end{cases}$$

As $c_0 = 1$ and $c_1 = a_p$, the proposition follows by induction. □

Corollary 6.9. *If $f \in \mathcal{X}$ is sparse, then its index must be greater than 2^{2000}.*

Proof. No two polynomials $M_i(y)$ for $i \leq 11$ have a common root other than 0 and 1. By machine computation, for every prime $q < 2000$ there exist positive integers $i < j \leq 11$ such that $i(2^q - 2) + 1, j(2^q - 2) + 1 \notin \mathbb{P}$. (In every case, this can be witnessed by a prime divisor less than 1000.) □

Proposition 6.10. *The roots of $M_n(y)$ are always 2-adically integral. Moreover, if p does not divide the binomial coefficient $\binom{2n}{n}$, then the roots are p-adically integral.*

Proof. Let v denote the valuation on $\bar{\mathbb{Q}}_2$ normalized so that $v(2) = 1$, and let γ be an element of $\bar{\mathbb{Q}}_2$ with $v(\gamma) < 0$. We claim that for any sequence γ_i with $\gamma_1 = \gamma$, such that

$$\beta_n = 2\gamma_n + \sum_{i=1}^{n-1} \gamma_i \gamma_{n-i}$$

is zero when n is odd and has valuation at least $v(\gamma_{n/2})$ when n is even, the valuation of γ_n does not depend on the β_i. In fact, if γ_i and δ_i are two such sequences, then $v(\delta_n - \gamma_n) > v(\gamma_n) = v(\delta_n)$ for all n.

It suffices to treat the case that

$$2\delta_n + \sum_{i=1}^{n-1} \delta_i \delta_{n-i} = 0$$

for all $n \geq 2$, i.e.,

$$\Big(1 + \sum_{i=1}^{\infty} \delta_i x^i\Big)^2 = 1 + 2\gamma x.$$

By the binomial theorem

$$\delta_n = (-1)^{n-1} \frac{(2n-3)!!}{n!} \gamma^n,$$

where, as usual, $k!!$ is the product of all odd numbers up to k. In other words, if $d(n)$ denotes the sum of the digits in the binary expansion of n,

$$v(\delta_n) = nv(\gamma) + d(n) - n.$$

As $d(i+j) \le d(i) + d(j)$

$$v(\delta_i \delta_{n-i}) \ge v(\delta_n)$$

for $0 < i < n$, and if n is even,

$$v(\delta_{n/2}^2) \ge v(2\delta_n).$$

We prove by induction that $v(\gamma_i - \delta_i) > v(\gamma_i) = v(\delta_i)$ for all i. Assume it holds all $i < n$. Defining $\gamma_{n/2} = \delta_{n/2} = 0$ if n is odd,

$$\begin{aligned} \delta_n - \gamma_n = -\frac{1}{2}\beta_n - \sum_{1 \le i < n/2} (\delta_i - \gamma_i)\gamma_j - \sum_{1 \le i < n/2} \delta_i(\delta_j - \gamma_j) \\ - \frac{1}{2}(\delta_{n/2} - \gamma_{n/2})(\delta_{n/2} + \gamma_{n/2}). \end{aligned} \tag{6.2}$$

If n is even,

$$v(\beta_n/2) \ge v(\gamma_{n/2}/2) = v(\delta_{n/2}/2) \ge v(\delta_n) - v(\delta_{n/2}) > v(\delta_n)$$

since $v(\delta_i) < 0$ for all $i \ge 1$. The right hand side of (6.2) is therefore a sum of terms with valuation strictly larger than $v(\delta_n)$, as claimed.

For p odd, we note that by induction $M_n(y) \in \mathbb{Z}_p[y]$ for all n. The leading coefficient of $M_n(y)$ is again $(-1)^{n-1}(2n-3)!!/n!$ and is therefore not divisible by p if $\binom{2n}{n}$ is not. □

Proposition 6.11. *If $f \in \mathcal{X}$ is sparse of index m, then a_m is an algebraic integer.*

Proof. By Corollary 6.4, $m = 2^k - 1$, and by Corollary 6.9, we may assume $k > 2000$. Let ℓ be any odd prime and let p be a prime not dividing $m - 1$. By Lemma 4.11, we may take $p \le 4k + 1$; if $k < 27720$, we take $p = 29$. An integer congruent to $-p \pmod{p^2}$ cannot be in $\mathbb{P}$, so we apply Lemma 4.10, with $d = p^2$, and a residue class a such that $a(m-1) + 1 \equiv -p \pmod{p^2}$. If $2000 < k < 27720$ and $d = 841$ or $k \ge 27720$ and $d \le (4k+1)^2$, then $m/2 > (2d^2)^{9\log(2d)}$, so there exists $n < m/2$ such that $n(m-1) + 1 \notin \mathbb{P}$ and $\ell \nmid \binom{2n}{n}$. By Proposition 6.8, $M_n(a_p) = 0$, but by Lemma 6.10, all the roots of M_n are ℓ-adically integral. □

We next consider the generating function

$$g_c(z) = 1 + \sum_{n=1}^{\infty} M_n(c) z^n.$$

By construction, $g_c(z)$ satisfies the formal functional equation

$$g_c(z)^2 = g_c(z^2) + 2cz.$$

This motivates the recursive definition

$$g_{n,c}(z) = \begin{cases} 1 & \text{if } n = 0, \\ \sqrt{g_{n-1,c}(z^2) + 2cz} & \text{if } n > 0. \end{cases} \tag{6.3}$$

Explicitly,

$$g_{1,c}(z) = \sqrt{1+2cz},$$
$$g_{2,c}(z) = \sqrt{\sqrt{1+2cz^2}+2cz},$$
$$g_{3,c}(z) = \sqrt{\sqrt{\sqrt{1+2cz^4}+2cz^2}+2cz},$$

and so forth. This sequence of power series in z converges coefficientwise to $g_c(z)$; in fact the first 2^n coefficients of $g_{n,c}(z)$ coincide with those of $g_c(z)$.

So far, we have regarded $g_c(z)$ as a formal power series parametrized by c, but each series $g_{n,c}(z)$ converges, for each value c, in a disk around 0. The algebraic function $g_{n,c}(z)$ can have branch points only for z in the set

$$\{z \mid g_{n,c}(z) = 0\} \cup \{z \mid g_{n-1,c}(z^2) = 0\} \cup \cdots \cup \{z \mid g_{1,c}(z^{2^{n-1}}) = 0\}.$$

For each n, let $K_{n,0} = \mathbb{C}(\sqrt{z})$ and define $K_{n,k}$ recursively for $1 \le k \le n$ by setting

$$K_{n,k} = K_{n,k-1}(g_{k,c}(z^{2^{n-k}})),$$

so $g_{n,c}(z) \in K_{n,n}$. Let $I_{n,c}(z_0)$ denote the nth iterate of the function $z^2 + c$ with initial value z_0.

Lemma 6.12. *For all $n \ge 1$ and all $c \in \mathbb{C}$ such that 0 is not a periodic point of $z^2 - 2c$ with period $\le n$, we have $[K_{n,n} : K_{n,0}] = 2^n$ and*

$$N_{K_{n,n}/K_{n,0}} g_{n,c}(z) = N_{K_{n,n}/\mathbb{C}(\sqrt{z})} g_{n,c}(z) = I_{n,-2c}(0) z^{2^{n-1}} - 1.$$

Proof. We prove the following pair of claims by induction on $k \ge 1$.

(1) $[K_{n,k} : K_{n,0}] = 2^k$,
(2) $N_{K_{n,k}/K_{n,0}}(g_{k,c}(z^{2^{n-k}}) + z_0 z^{2^{n-1-k}}) = -1 + I_{k,-2c}(z_0) z^{2^{n-1}}$.

For $k = n$, combining (1) and (2) for $z_0 = 0$, we obtain the claim of the lemma,

$$N_{K_{n,n}/K_{n,0}} g_{n,c}(z) = N_{K_{n,n}/K_{n,0}}(-g_{n,c}(z)) = I_{n,-2c}(0) z^{2^{n-1}} - 1.$$

For $k = 1$, Claim (1) is obvious, while (2) is the identity

$$(\sqrt{1+2cz^{2^{n-1}}} + z_0 z^{2^{n-2}})(-\sqrt{1+2cz^{2^{n-1}}} + z_0 z^{2^{n-2}}) = -1 + (z_0^2 - 2c) z^{2^{n-1}}.$$

The relation

$$-g_{k+1,c}(z^{2^{n-k-1}})^2 = -g_{k,c}(z^{2^{n-k}}) - 2cz^{2^{n-k-1}}$$

implies $[K_{n,k+1} : K_{n,k}] \ge 2$. By the induction hypothesis,

(6.4)

$$\begin{aligned} N_{K_{n,k}/K_{n,0}}(-g_{k+1,c}(z^{2^{n-k-1}})^2) &= N_{K_{n,k}/K_{n,0}}(-g_{k,c}(z^{2^{n-k}}) - 2cz^{2^{n-k-1}}) \\ &= -1 + I_{k,-2c}(-2c) z^{2^{n-1}} \\ &= -1 + I_{k+1,-2c}(0) z^{2^{n-1}}. \end{aligned}$$

As $I_{k+1,-2c}(0) \neq 0$, the right hand side of (6.4) has only non-zero simple zeroes, so it is not the square of a rational function in $\sqrt{z}$. This implies $-g_{k+1,c}(z^{2^{n-k-1}})^2$ is not the square of an element in $K_{n,k}$, therefore that $g_{k+1,c}(z^{2^{n-k-1}}) \notin K_{n,k}$, and finally that $[K_{n,k+1} : K_{n,k}] \geq 2$, giving Claim (1) for $k+1$. Therefore

$$\begin{aligned}
&N_{K_{n,k+1}/K_{n,0}}(g_{k+1,c}(z^{2^{n-1-k}}) + z_0 z^{2^{n-2-k}}) \\
&\qquad = N_{K_{n,k}/K_{n,0}} N_{K_{n,k+1}/K_{n,k}}(g_{k+1,c}(z^{2^{n-1-k}}) + z_0 z^{2^{n-2-k}}) \\
&\qquad = N_{K_{n,k}/K_{n,0}}(-g_{k+1,c}(z^{2^{n-1-k}})^2 + (z_0 z^{2^{n-2-k}})^2) \\
&\qquad = N_{K_{n,k}/K_{n,0}}(-g_{k,c}(z^{2^{n-k}}) - 2cz^{2^{n-1-k}} + z_0^2 z^{2^{n-1-k}}) \\
&\qquad = N_{K_{n,k}/K_{n,0}}(-g_{k,c}(z^{2^{n-k}}) + (z_0^2 - 2c) z^{2^{n-1-k}}) \\
&\qquad = -1 + I_{k,-2c}(z_0^2 - 2c)) z^{2^{n-1}} \\
&\qquad = -1 + I_{k+1,-2c}(z_0) z^{2^{n-1}},
\end{aligned}$$

giving Claim (2) for $k+1$. □

Therefore the power series for $g_{n,c}(z)$ converges in an open disk around 0 of radius

$$R_{n,c} = \inf_{1 \leq k \leq n} |I_{k,-2c}(0)|^{-2^{1-n}} = \Big(\sup_{1 \leq k \leq n} |I_{k,-2c}(0)| \Big)^{-2^{1-n}}.$$

Lemma 6.13. *Let U be a connected neighborhood of ∞ in the Riemann sphere such that for all finite $c \in U$, the absolute value of $I_{n,-2c}(0)$ is strictly greater than the absolute values $|I_{k,-2c}(0)|$ for $k < n$. Then for each $c \in U$, $g_{n,c}(z)^2$ has exactly one zero, denoted $z_{n,c}$, in the disk $|z| < R_{n-1,c}^{1/2}$. Moreover,*

$$z_{n,c}^{-2^{n-1}} = I_{n,-2c}(0),$$

and the zero at $z_{n,c}$ is simple.

Proof. First we observe that $g_{n,c}(z)^2 = g_{n-1,c}(z^2) + 2cz$ is really defined in the disk $|z| < R_{n-1,c}^{1/2}$. In particular it is defined at every 2^{n-1}st root of $I_{n,-2c}(0)^{-1}$. Since the product of $g_{n,c}(z)^2$ and its conjugates over the field of rational functions has only simple zeroes, we need only show that $g_{n,c}(z)^2$ itself accounts for exactly one of those zeroes. We prove this by analytic continuation, using the fact that in a continuously varying family of analytic functions, the number of zeroes inside a continuously varying disk never changes as long as there is never a zero on the boundary of the disk. As U is connected, it suffices to prove the claim when $|c| \gg 0$. But in this case it is clear that each conjugate of $g_{n-1,c}(z^2) + 2cz$ accounts for exactly one of the 2^{n-1} roots in question, each according to the constant term in its power series expansion, which is a different 2^{n-1}st root of unity for each conjugate. □

Lemma 6.14. *If $c \in \mathbb{C}$, $r > 0$, and $n \in \mathbb{N}$ are such that $g_{n,c}(z)$, $g_{n+1,c}(z)$, $g_{n+2,c}(z)$, ... all have radius of convergence greater than $r < 1$, then $g_c(z)$ has radius of convergence greater than r and the sequence $\{g_{k,c}(z)\}_{k\geq n}$ converges to $g_c(z)$ on the closed disk of radius r centered at the origin.*

Proof. As $\left| \frac{d}{dz}\sqrt{1+z} \right| \leq 1$ for all $|z| \leq 3/4$, by induction on k, $|w_1| + \cdots + |w_k| \leq 3/4$ implies

$$\left| \frac{\partial}{\partial w_i} \sqrt{\sqrt{\cdots \sqrt{\sqrt{1+w_1} + w_2} + \cdots + w_{k-1}} + w_k} \right| \leq 1$$

for $1 \leq i \leq k$. Thus,

$$\left| \sqrt{\sqrt{\cdots \sqrt{\sqrt{1+w} + 2cz^{2^{n-1}}} + \cdots + 2cz^2} + 2cz} - g_{n,c}(z) \right| \leq |w|,$$

whenever $|w| + |2cz^{2^{n-1}}| + \cdots + |2cz| \leq 3/4$. In particular,

$$|g_{n+1,c} - g_n(c)| \leq |2cz^{2^n}|$$

provided

$$2|c|(|z| + |z|^2 + |z|^4 + \cdots + |z|^{2^n}).$$

It follows that the sequence

$$\{g_{k,c}(z)\}_{k=1,2,3,\ldots} \tag{6.5}$$

converges whenever

$$|z| < \inf(1, \frac{3}{14|c|}).$$

By the recursive definition (6.3) of $g_{n,c}(z)$, the sequence (6.5) converges for z whenever $|z| \leq r$ and it converges for z^2. The convergence of (6.5) in $\{z\colon |z| \leq r\}$ follows by a bootstrapping argument. □

Let R_c denote the minimum of $\lim_{n\to\infty} R_{n,c}$ and 1. We have the following immediate corollary:

Lemma 6.15. *The series $g_c(z)$ converges for all $|z| < R_c$.*

In the next two results, we sketch a proof that there is an upper limit to the index of sparseness for any element of $\mathfrak{X}$.

Lemma 6.16. *Let X be a compact set and $b_i\colon X \to \mathbb{C}$ a collection of continuous functions indexed by integers $i \geq 0$. Let $f_x(z) = \sum_{k=0}^{\infty} b_k(x)z^k$. We suppose that for each $x \in X$ there exists $r_x > 0$, depending continuously on x, such that $f_x(z)^2$ converges in a disk of radius greater than r_x and has exactly one zero, counting multiplicity, in the disk of radius r_x. Then there exists N such that for all $k > N$ and for all $x \in X$, $b_k(x) \neq 0$.*

Proof. By compactness we may assume without loss of generality that a single $r = r_x$ works for all $x \in X$. Choose $s > r$ such that all $f_x(z)^2$ have radius of convergence $> s$. As f_x is continuous in x, the unique zero z_x of $f_x(z)^2$ in the closed disk D_r of radius r varies continuously with x. Therefore $\frac{f_x(z)^2}{z-z_x}$ is continuous on $X \times D_r$ and nowhere vanishing on that set. Therefore its absolute value is always greater than some $\epsilon > 0$. We make a branch cut from z_x to $z_x\infty$ to make $f_x(z)$ single valued and then estimate $b_k(x)$ by computing the contour integral $\oint_{Q_x} \frac{f_x(z)}{z^{k+1}} dz$, where Q_x denotes a contour consisting of an outward segment from z_x to $s\frac{z_x}{|z_x|}$, a counterclockwise circle of radius s, and an inward segment from $s\frac{z_x}{|z_x|}$ to z_x. For large values of k, only the two segments matter, and their contributions are equal since $f_x(z)$ changes sign over the circle of radius s. If $f_x(z)^2 = c_1(z - z_x) + c_2(z - z_x)^2 + \cdots$, the integral over one of the segments of Q_x is

$$\Gamma(3/2)c_1^{1/2} z_x^{3/2} k^{-3/2} z_x^{-k} + O(k^{-5/2} z_x^{-k}).$$

Since $|c_1| > \epsilon$ and the implicit constant above is uniform in X, $b_k(x) \neq 0$ for all $k \gg 0$ uniformly in X. □

Theorem 6.17. *For all open neighborhoods U of the Mandelbrot set $\mathcal{M}$ there exists an integer N such that for all $n > N$ and for all $c \notin U$, $M_n(-c/2) \neq 0$.*

Proof. Making U smaller if necessary, we may assume that it is bounded. Let U_1 and U_2 be disjoint open sets in $\mathbb{CP}^1$ such that U_1 contains the complement of U and U_2 contains $\mathcal{M}$. By construction the set $-\frac{1}{2}U_1$ satisfies the hypotheses of Lemma 6.13 for all n greater than some fixed C. Let K denote a compact subset of U_1 containing the complement of U, and let X denote the product of the one-point compactification $\mathbb{Z}^{\geq C} \cup \{\infty\}$ and $-\frac{1}{2}K$. We define

$$f_{n,c}(z) = \begin{cases} \sqrt{1-z} & \text{if } c = \infty, \\ g_c(z/c) & \text{if } n = \infty, \\ g_{n,c}(z/c) & \text{otherwise.} \end{cases}$$

By Lemma 6.14, $f_x(z)$ is continuous in x and is analytic in a neighborhood of 0 for each fixed x. (Note that we have renormalized the $g_{n,c}$ and g_c to prevent the radius of convergence from going to zero as $c \to \infty$.) The conclusion of Lemma 6.13 implies that $f_x(z)$ satisfies the hypotheses of Lemma 6.16, and the theorem follows. □

By Proposition 6.11, if f is sparse of index m, then a_m is an algebraic integer. On the other hand, $\mathcal{X}$ is rational over $\mathbb{Q}$, so all conjugates of a_m must also give rise to sparse solutions. In particular, if $m \gg 0$, a_m and its conjugates all lie in any specified open set containing $-\frac{1}{2}\mathcal{M}$. Since $\mathcal{M}$ is a closed subset of the disk of radius 2 meeting the boundary of the disk only at the point -2, this open set can be taken to have capacity less than 1, and therefore to contain finitely many conjugacy classes of algebraic integers

[Fe]. In fact, it is easy to see that it can be chosen small enough that 0 and 1 are the only possible values for a_m. The first is ruled out by definition, the second by Proposition 6.6.

However, to prove the main theorem, it is necessary to make the above estimates effective. We do this by choosing a particular open neighborhood of $-\frac{1}{2}\mathcal{M}$, namely the disk of radius 7/8 centered at 1/4. We begin by finding the orbits of algebraic integers belonging to this disk.

Proposition 6.18. *If α is an algebraic integer all of whose conjugates satisfy $|z - 1/4| \leq 7/8$, then α is 0 or 1.*

Proof. According to the maximum principle, for elements $\alpha_1, \ldots, \alpha_n$ of a closed disk of radius r, the product $\prod_{i \neq j} |\alpha_i - \alpha_j|$ can achieve its maximum only if all α_i lie on the boundary of the disk. By the concavity of $\log |1 - e^{i\theta}|$, the product is achieved when the α_i form the vertices of an inscribed regular n-gon. In this case, the product is

$$\left(\prod_{i=1}^{n-1} \left| \, r - r\zeta_n^i \, \right| \right)^n = r^{n^2-n} \left| \, 1 + x + x^2 + \cdots + x^{n-1}|_{x=1} \, \right|^n = n^n r^{n^2-n}.$$

For $r = 7/8$, this expression is < 1 for $n \geq 26$. For $6 \leq n \leq 25$, we still have that $g(n)$ is less than the Minkowski bound $\frac{n^{2n}\pi^n}{(n!)^2 4^n}$. For $3 \leq n \leq 5$, $g(n)$ remains less than the smallest actual discriminant absolute value, as tabulated in [Po]. Finally, for $n = 2$, two conjugate algebraic integers lie in the same disk of radius 7/8 if and only if the integers are of the form $n + e^{\frac{\pm 2\pi i}{3}}$ for some $n \in \mathbb{Z}$. In particular, no such pair lie in a disk centered at 1/4. □

Proposition 6.19. *If $n \geq 2$ and $|d + 1/2| > 7/4$, then*

$$(|d + 1/2| - 1/4)^{2^{n-1}} < |I_{n,d}(0)| < (|d + 1/2| + 1/4)^{2^{n-1}}. \tag{6.6}$$

Proof. As $I_2(d) = d^2 + d = (d + 1/2)^2 - 1/4$, setting $r = |d + 1/2| > 7/4$, we have

$$\begin{aligned} (r - \frac{1}{4})^2 + \frac{3}{4}(r - \frac{1}{4})^{-1} < r^2 - \frac{1}{4} &\leq |I_2(d)| \\ &\leq r^2 + \frac{1}{4} < (r + \frac{1}{4})^2 - \frac{3}{4}(r + \frac{1}{4})^{-1} \end{aligned}$$

We prove by induction that for all $n \geq 2$, we have

(6.7)

$$\begin{aligned} (r - \frac{1}{4})^{2^{n-1}} + \frac{3}{4}(r - \frac{1}{4})^{1-2^{n-1}} < r^2 - \frac{1}{4} &\leq |I_{n,d}(0)| \\ &\leq r^2 + \frac{1}{4} < (r + \frac{1}{4})^{2^{n-1}} - \frac{3}{4}(r + \frac{1}{4})^{1-2^{n-1}} \end{aligned}$$

For the induction step, we apply

$$|w|^2 - r - \frac{1}{2} \leq |w^2 + d| \leq |w|^2 + r + \frac{1}{2},$$

to $w = I_{n,d}(0)$ in (6.7), using the inequalities

$$\frac{3}{2}(r \pm \frac{1}{4}) > r + \frac{1}{4},\ \frac{3}{4}(r \pm \frac{1}{4}) > 1.$$

The inequalities (6.6) follow immediately. □

Corollary 6.20. *If $n \geq 2$, $|c - 1/4| > 7/8$, then*

$$\frac{1}{2|c-1/4| + 1/4} < R_{n,c} < \frac{1}{2|c-1/4| - 1/4} < \frac{2}{3}.$$

In particular,

$$\frac{5}{16|c|} \leq R_c \leq \frac{3}{4|c|}.$$

Proof. The proposition implies that $|I_{n,-2c}(0)|$ is monotonically increasing for $n \geq 2$. Thus $R_{n,c} = |I_{n,-2c}(0)|^{2^{1-n}}$. The first claim follows immediately, the second from the inequality

$$\frac{5}{16} < \frac{|c|}{|2|c-1/4| \pm 1/4|} < \frac{3}{4},$$

which holds for $|c - 1/4| > 7/8$. □

Corollary 6.21. *The sequence $z_{1,c}, z_{2,c}, \ldots$ converges to z_c, and $|z_c| = R_c$.*

Proof. By Lemma 6.13 and Corollary 6.20, $|z_{n,c}| = R_{n,c}$ for all $n \geq 1$. As $g_{n,c}^2(z)$ converges for $|z| < R_{n-1,c}^{1/2}$, choosing

$$r \in ((2|c-1/4| - 1/4)^{-1}, (2|c-1/4| + 1/4)^{-1/2}),$$

the sequence $g_{n,c}^2(z)$ converges to $g_c(z)^2$ uniformly on the disc $|z| \leq r$, and $z_{n,c}$ is the unique zero of $g_{n,c}^2(z)$ in that disk and is moreover simple. It follows that $z_c = \lim_{n\to\infty} z_c$.

□

Theorem 6.22. *The only sparse elements in $\mathcal{X}$ are the linear solutions (xi).*

Proof. Suppose $f \in \mathcal{X}$ is sparse of index p. Setting $c = a_p$, we have $c \neq 0$ by definition and $c \neq 1$ by Proposition 6.6. Therefore, by Proposition 6.11 and Proposition 6.18, we have $|c - 1/2| > 7/4$.

We want to estimate the constant N of Lemma 6.16. Our first task is to estimate the derivative of $h_c(z) = g_c(z)^2$ at its unique zero z_c in the disk $|z| < \lim_{n\to\infty} R_{n-1,c}^{1/2}$. This is the same as the limit of the derivative of $g_{n,c}(z)^2$ at its unique zero $z_{n,c}$ satisfying $|z_{n,c}| \leq R_{n-1,c}^{1/2}$. By induction on k, we have

$$g_{n-k,c}(z_{n,c}^{2^k}) = I_{k,-2c}(0) z_{n,c}^{2^{k-1}}$$

for $0 \leq k \leq n$. Differentiating (6.3), we obtain

$$g'_{n-k,c}(z) = \frac{c + z g'_{n-k-1,c}(z^2)}{g_{n-k,c}(z)}$$

for all $i \geq 1$, and substituting $z = z_{n,c}^{2^k}$, we get

$$g'_{n-k,c}(z_{n,c}^{2^k}) = \frac{c}{I_{k,-2c}(0) z_{n,c}^{2^{k-1}}} + \frac{z_{n,c}^{2^{k-1}} g'_{n-k-1,c}(z_{n,c}^{2^{k+1}})}{I_{k,-2c}(0)}.$$

Therefore, the value of the derivative of $g_{n,c}(z)^2 = 2cz + g_{n-1,c}(z^2)$ at $z_{n,c}$ is

$$\begin{aligned} 2c + 2z_{n,c} g'_{n-1,c}(z_{n,c}^2) &= 2c + \frac{2c}{I_1(-2c)} + \frac{2z_{n,c}^2 g'_{n-2,c}(z_{n,c}^4)}{I_1(-2c)} \\ &= 2c + \frac{2c}{I_1(-2c)} + \frac{2c}{I_1(-2c) I_2(-2c)} + \frac{2z_{n,c}^4 g'_{n-3,c}(z_{n,c}^8)}{I_2(-2c)} \\ &= \cdots . \end{aligned}$$

Expanding completely (and using the fact that $g'_{0,c}$ is identically zero), we obtain

$$2c \left(1 + \frac{1}{I_1(-2c)} + \frac{1}{I_1(-2c) I_2(-2c)} + \cdots + \frac{1}{I_1(-2c) I_2(-2c) \cdots I_{n-1}(-2c)} \right).$$

As $I_1(-2c) = -2c$ lies on a circle of radius $7/4$ centered at $-1/2$, its inverse lies on the circle with diameter the real interval $[-4/9, 4/5]$. It follows that $|1 + I_1(-2c)^{-1}| \geq 5/9$. On the other hand, $|I_1(-2c)| \geq 5/4$, and by (6.6), $|I_2(-2c)| \geq 9/4$, and $|I_{n,-2c}(0)| \geq 5$ for $n \geq 3$, so

$$\left| 1 + \frac{1}{I_1(-2c)} + \cdots + \frac{1}{I_1(-2c) \cdots I_{n-1}(-2c)} \right| \geq 5/9 - \frac{1 + 5^{-1} + 5^{-2} + \cdots}{|I_1(-2c) I_2(-2c)|} \geq \frac{1}{9}.$$

Thus,

$$|h'_c(z_c)| \geq \frac{|c|}{9} > \frac{1}{30 R_c}. \tag{6.8}$$

Next, we need to estimate the second derivative of $h_c(z)$ near $z = z_c$. By Cauchy's integral formula for derivatives,

$$|f''(z)| \leq 2 \frac{\sup_\theta |f(z + re^{i\theta})|}{r^2}.$$

By Lemma 6.15, $h_c(z)$ converges for $|z| < \sqrt{R_c}$ and therefore, by Corollary 6.20, for $|z| < 1.2 R_c$. For $|z| < 1.1 R_c$, we may take $r = R_c/10$ and still have $|c(z + re^{i\theta})| < 1$ by Corollary 6.20. As $|c| > 1$, the inequality $|\sqrt{1+z}| \leq 1 + |z|/2$ implies

$$|g_{n,c}(z + re^{i\theta})| \leq 1 + |c(z + re^{i\theta})| + \frac{|c(z + re^{i\theta})^2|}{2} + \frac{|c(z + re^{i\theta})^4|}{4} + \cdots \leq 3. \tag{6.9}$$

Thus, $|z| < 1.1 R_c$ implies

$$|h''_c(z)| \leq \frac{1800}{R_c^2}.$$

By (6.8), $|z - z_c| \leq R_c/120$ implies

$$\left| \frac{h_c'(z)}{h_c'(z_c)} - 1 \right| \leq \frac{1}{2},$$

so integrating $h_c'(z)$ along the directed line segment from z_c to z, we obtain

$$\left| \frac{h_c(z)}{h_c'(z_c)(z - z_c)} - 1 \right| = \left| \frac{\int_{z_c}^{z} h_c'(w)dw}{h_c'(z_c)(z - z_c)} - 1 \right| \leq \frac{1}{2}.$$

As $|(x + iy)^2 - 1| \leq 1/2$ implies

$$(x^2 + y^2)^2 + 2y^2 + 1 - 2x^2 = (x^2 - y^2 - 1)^2 + (2xy)^2 \leq \frac{1}{4},$$

it follows that

$$\Re \sqrt{\frac{h_c(z)}{h_c'(z_c)(z - z_c)}} > \frac{1}{2}$$

in the ball $|z - z_c| \leq R_c/120$.

We integrate $\sqrt{h_c(z)}z^{-k-1}$ over the contour consisting of a straight line from z_c to $\frac{121}{120}z_c$, a counterclockwise circle C of radius $\frac{121R_c}{120}$, and a straight line returning to z_c. As $\sqrt{h_c(z)}$ changes sign over the contour, the integral is twice the original segment plus the circle. We will show that the integral is non-zero by showing that

(6.10)

$$\Re \left(h_c'(z_c)^{-1/2} z_c^{k+1/2} \int_{z_c}^{\frac{121 z_c}{120}} \frac{\sqrt{h_c(z)}}{z^{k+1}} dz \right) > \left| h_c'(z_c)^{-1/2} z_c^{k+1/2} \int_C \frac{\sqrt{h_c(z)}}{z^{k+1}} dz \right|.$$

The left hand side of (6.10) is the integral of

$$\left(\frac{z_c}{z}\right)^k \sqrt{\frac{z_c(z - z_c)}{z^2}} \Re \sqrt{\frac{h_c(z)}{h_c'(z_c)(z - z_c)}} > \frac{1}{2}\left(\frac{z_c}{z}\right)^k \sqrt{\frac{z_c(z - z_c)}{z^2}}. \tag{6.11}$$

It is therefore greater than the integral of the right hand side of (6.11) from $z_c(1 + 1/480)$ to $z_c(1 + 1/240)$, and so is at least

$$\frac{\sqrt{480}(1 + 1/240)^{-k} R_c}{2 \cdot 480 \cdot 481}. \tag{6.12}$$

The right hand side of (6.10) is no larger than

$$2\pi \frac{121R_c}{120} \frac{1}{\sqrt{|h_c'(z_c)R_c|}} \frac{\sup_{z \in C} \sqrt{|h_c(z)|}}{(1 + 1/120)^{k+1}} \leq 2\pi \frac{121R_c}{120} \frac{1}{\sqrt{30}} \frac{3}{(1 + 1/120)^{k+1}},$$

by (6.8) and (6.9). Comparing this to the lower bound (6.12), for $k \geq 2773$, we have

$$\left(\frac{242}{241}\right)^k > 48 \cdot 481\pi,$$

implying (6.10).

If $p \geq 2^{13} - 1$, then by Lemma 4.12, there exists k satisfying $p - 1 \geq k \geq (p - 1)/2 \geq 2773$ such that $k(p - 1) + 1 \notin \mathbb{P}$ and the z^k coefficient of $g_c(z)$,

i.e., $M_k(c) = M_k(a_p)$ is non-zero. This contradicts Proposition 6.8, and we are done.

This leaves two cases: $p = 31$ and $p = 127$. For the former, $3 \cdot 30 + 1 \notin \mathbb{P}$ and for the latter, $2 \cdot 126 + 1 \notin \mathbb{P}$. Now, either $M_2(c) = 0$ or $M_3(c) = 0$ implies $c \in \{0, 1\}$, which is impossible. This again contradicts Proposition 6.8, which proves the theorem.

□

7. Some Variants

In this section, we consider some variants of the problem of classifying normalized multiplicative power series whose squares are multiplicative.

We begin by proving Theorem 1.2, or more precisely:

Proposition 7.1. *The set of normalized multiplicative power series $f(q)$ such that $f(q)^2$ and $f(q)^4$ are both multiplicative is as follows:*

$$\{\vartheta_{\mathbb{Z}}(q), \vartheta_{\mathbb{Z}[i]}(q), \vartheta_{\mathbb{Z}[\zeta_3]}(q), -\vartheta_{\mathbb{Z}}(-q), -\vartheta_{\mathbb{Z}[i]}(-q), -\vartheta_{\mathbb{Z}[\zeta_3]}(-q)\}. \tag{7.1}$$

Proof. First, we claim that each series $f(q)$ in (7.1) is a solution. It suffices to prove that $f(q)$ and some multiple of $f(q)^2$ lie in $\mathcal{X}$, and by Lemma 3.3, it suffices to prove this for $\vartheta_{\mathbb{Z}}(q)$, $\vartheta_{\mathbb{Z}[i]}(q)$, and $\vartheta_{\mathbb{Z}[\zeta_3]}(q)$. By Proposition 3.2, these are of type (vii), (v), and (vi) respectively. As $\vartheta_{\mathbb{Z}}(q)^2 = \vartheta_{\mathbb{Z}[i]}(q)$ and $2\vartheta^2_{\mathbb{Z}[i]}(q) = \vartheta_H(q) + 2\vartheta_H(q^2)$, the squares of the theta series, suitably normalized, are elements of $\mathcal{X}$ of type (v), (iii), and (ii) respectively.

Let the polynomials P_n be defined as in (4.1). We define polynomials Q_n which play the role for f^4 which the P_n play for f^2; namely, if $2a_0^3 f(q)^4 = \sum_n d_n q^n$, and D_n denotes the polynomial expression in $a_0, a_2, \ldots$, for the coefficient d_n, we set

$$Q_{p_1^{e_1} \cdots p_k^{e_k}} = D_{p_1^{e_1} \cdots p_k^{e_k}} - D_{p_1^{e_1}} \cdots D_{p_k^{e_k}}.$$

We consider the system of 14 polynomial equations in the 13 variables $a_0, a_2, \ldots, a_{19}$ given by P_n and Q_n for $n \in [6, 20] \cap \mathbb{Z} \setminus \mathbb{P}$.

A Maple computation shows that there are exactly six solutions, corresponding to the initial coefficients of the six modular forms listed above. Since performing this calculation reasonably efficiently is not straightforward, we describe our steps in more detail. We begin by solving for the variables a_4, a_5, a_8, a_9, a_{11}, a_{13}, a_{16}, a_{17}, a_{19} using the polynomial equations Q_6, P_6, Q_{10}, P_{10}, P_{12}, P_{14}, Q_{18}, P_{18}, and P_{20} respectively and substituting the resulting expressions into the equations Q_{12}, Q_{14}, P_{15}, Q_{15}, Q_{20}. The resulting polynomials in a_0, a_2, a_3, and a_7 have degrees 11, 11, 13, 13, and 17 respectively. We reduce to equations in a_0 and a_2 by using Q_{12} to eliminate a_7 and Q_{14} to eliminate a_3 from P_{15}, Q_{15}, Q_{20}. These three equations have a degree 24 common factor, $A(a_0, a_2)^2$, but pulling out this factor and using the first of the three remaining factors to eliminate a_0 from the second and third, we can take the g.c.d. to solve for a_2. The possible solutions, 0, ± 1, $\pm\frac{1}{2}$ can then be substituted back into the original equations Q_{12},

Q_{14}, P_{15}, Q_{15}, Q_{20}, at which point Maple is capable of solving directly for all triples (a_0, a_3, a_7). To deal with solutions of $A(a_0, a_2) = 0$, we eliminate a_7 and a_3 from Q_{15} and Q_{20} using Q_{14} and P_{15} respectively. The resulting polynomials in a_0 and a_2 again have a common factor, $B(a_0, a_2)^4$, of degree 92. Removing this factor from Q_{15} and Q_{20} and eliminating a_0 using A, we see again that $a_2 \in \{0, \pm 1, \pm\frac{1}{2}\}$. Thus, we need only consider the case $A(a_0, a_2) = B(a_0, a_2) = 0$. Eliminating a_7 and a_3 from Q_{20} using P_{15} and Q_{15} respectively, we obtain an equation in a_0 and a_2, and eliminating a_2 from this equation and B using A, we get $a_0 = 0$, which is impossible.

By Proposition 5.6, there is at most one solution $f(q)$ with each of these initial coefficient sequences.

□

Note that Theorem 1.1, or more precisely, the following statement, is an immediate corollary:

Corollary 7.2. *The set of normalized multiplicative power series $f(q)$ such that $f(q)^2$, $f(q)^4$, and $f(q)^8$ are all multiplicative consists of*

$$\{\vartheta_{\mathbb{Z}}(q), -\vartheta_{\mathbb{Z}}(-q)\}.$$

Next we consider the following question: What can be said about $f(q)$ if f and f^2 both belong to the vector space V of *finite linear combinations* of multiplicative power series, or more generally, if all powers of f belong to V? The following proposition proves that this question is not vacuous.

Proposition 7.3. *The vector space V is a proper subspace of the complex power series in q.*

Proof. We prove the following stronger claim: There exists a function $F(x)$ such that if $|a_{n+1}| \geq F(|a_n|)$ for all $n \geq 0$, then $f(q) = \sum_{n=0}^{\infty} a_n q^n$ does not belong to V.

Suppose

$$f(q) = a_0 + \sum_{i=1}^{n} c_i f_i(q),$$

where the f_i are normalized multiplicative :

$$f_i(q) = a_{i,0} + q + a_{i,2}q^2 + a_{i,3}q^3 + a_{i,4}q^4 + a_{i,5}q^5 + a_{i,2}a_{i,3}q^6 + \cdots .$$

Let $C_k(x_i, y_{i,j})$ denote the polynomial representing the q^k coefficient of f in terms of $x_i = c_i$ and $y_{i,j} = a_{i,j}$ ($j \in \mathbb{P} \cup \{0\}$). Thus C_k is a sum of distinct products of subsets of the variables

$$\{x_i \mid 1 \leq i \leq n\} \cup \{y_{i,j} \mid 1 \leq i \leq n,\ j \leq k,\ j \in \mathbb{P} \cup \{0\}\}.$$

By the prime number theorem, the number of variables in the set grows like $nk/\log k$. Therefore, for $N \gg 0$, the polynomials C_{N+1}, C_{N+2}, $\ldots$, C_{2N} involve among them fewer than N variables. The proposition now follows from the following two lemmas: □

Lemma 7.4. *For $x = (x_1, \dots, x_m)$ and $I = (i_1, \dots, i_m)$, we denote by x^I the monomial $x_1^{i_1} \cdots x_m^{i_m}$. There exist functions $G, H \colon \mathbb{N} \to \mathbb{N}$ such that if*

$$Q_i(x_1, \dots, x_m) = \sum_{I \in \{0,1\}^m} a_{i,I} x^I, \ i = 1, \dots, m+1,$$

with $a_{i,I} \in \{0, 1\}$, then there exists a polynomial $R(y_1, \dots, y_{m+1})$ of degree $\le G(m)$ and integer coefficients of absolute value $\le H(m)$ such that

$$R(Q_1(x), \dots Q_{m+1}(x)) \equiv 0.$$

Proof. For any positive integer N, there are $\binom{N+m+1}{m+1}$ monomials in $Q_1, \dots, Q_{m+1}$ of degree $\le N$; all are of degree $\le mN$ as polynomials in $x_1, \dots, x_m$ and have all coefficients $\le (2^m)^N$. The total number of monomials of degree $\le mN$ in the x_i is $\binom{mN+m}{m}$. If $N = G(m)$ is sufficiently large, the former number is larger, so there must be some linear relation between the monomials. The coefficients of the relation can be bounded by $H(m)$ depending only on N and m, and therefore only on m.

□

Lemma 7.5. *Given functions $G, H \colon \mathbb{N} \to \mathbb{N}$ there exists a function $F \colon \mathbb{R} \to \mathbb{R}$ such that for all $m \ge 2$, all sequences $z_1, \dots, z_{2m} \in \mathbb{C}$ satisfying $|z_{i+1}| \ge F(|z_i|)$ for $1 \le i \le 2m-1$, and all non-zero polynomials $R \in \mathbb{C}[x_1, \dots, x_m]$ with degree $\le G(m)$ and coefficients with absolute value $\le H(m)$, we have*

$$R(z_{m+1}, \dots, z_{2m}) \neq 0.$$

Proof. Replacing $G(x)$ and $H(x)$ by $x + \sup_{n \le x} G(n)$ and $\sup_{n \le x} H(n)$ respectively, we may regard both as non-decreasing functions defined on $[0, \infty)$, where, moreover, $G(x+1) \ge G(x) + 1$ and $G(x) \ge x$ for all $x \ge 0$. For $x \ge 0$, let

$$F(x) = (1 + H(x))e^{(1+G(x))x} + 3.$$

Then we have $F(x) \ge e^x + 3 > \max(3, x+3)$. By induction on r, we have $|z_{r+1}| \ge 3r \ge r+2$ for all $r \ge 1$, so

$$\begin{aligned} |z_{r+2}| > F(|z_{r+1}|) &= (1 + H(|z_{r+1}|)e^{(1+G(|z_{r+1}|)|z_{r+1}|} \\ &> (1 + H(r+2))e^{(1+G(r+2))|z_{r+1}|}. \end{aligned}$$

As $\frac{\log x}{x}$ is increasing on $(0, e)$ and decreasing on (e, ∞), for $e \le x \le y$, we have $x^y \ge y^x$, and for $x, a \ge 0$, we have

$$e^{ax} = (e^x)^a \ge (x^e)^a = x^{ea}.$$

Thus,

$$\begin{aligned} |z_{r+2}| > H(r+2)|z_{r+1}|^{e(1+G(r+2))} &> H(r+2)(r+2)^{1+G(r+2)}|z_{r+1}|^{1+G(r+2)} \\ &> (1 + G(r+2))^{r+2} H(r+2)|z_{r+1}|^{1+G(r+2)}. \end{aligned}$$

In particular, for $1 \leq j \leq m$,

$$\begin{aligned}|z_{m+j}| &> |z_{m+j-1}|(1+G(m+j))^{m+j}H(m+j)|z_{m+j-1}|^{G(m+j)} \\ &> \cdots > |z_m| \prod_{k=1}^{j} (1+G(m+k))^{m+k} H(m+k) |z_{m+k-1}|^{G(m+k)} \\ &> (1+G(m))^m H(m) \prod_{i=1}^{j-1} |z_{m+i}|^{G(m)}.\end{aligned}$$

Thus, given m-tuples of non-negative integers $\leq G(m)$ such that

$$(k_1, \ldots, k_m) > (k'_1, \ldots, k'_m)$$

in lexicographic order, we have

$$|z_{2m}|^{k_1} \cdots |z_{m+2}|^{k_{m-1}} |z_{m+1}|^{k_m} > (1+G(m))^m H(m) |z_{2m}|^{k'_1} \cdots |z_{m+2}|^{k'_{m-1}} |z_{m+1}|^{k'_m}$$

which in turn implies that any non-trivial integer linear combination of monomials $z_{2m}^{k_1} \cdots z_{m+1}^{k_m}$ with $k_i \leq G(m)$ and coefficient absolute values $\leq H(m)$ is non-zero. □

If a_n and b_n are multiplicative sequences, then the sequences $n \mapsto a_n b_n$ and $n \mapsto \sum_{ij=n} a_i b_j$ are multiplicative. The polynomial

$$S_n(q) = \sum_{d|n} q^d$$

has multiplicative coefficients, and every polynomial, in particular, every monomial in q is a finite linear combination of the polynomials S_i. It follows that $f(q^n) \in V$ whenever $f(q) \in V$.

If $M_*(N)$ denotes the graded ring of modular forms of integral weight for $\Gamma_1(N)$, then it is clear by reduction to the case of newforms that $\bigcup_N M_*(N) \subset V$. As the union of the $M_*(N)$ is a ring, the same is true for all powers of f. Certain power series, such as $24E_2(q)$, though not modular forms themselves, are congruent to elements of $M_*(N)$ modulo every prime [Se]. Naturally, any integer power of such a series has the same property.

Question 7.6. *Is $E_2(q)^2 \in V$?*

In a different direction, we have the following:

Proposition 7.7. *If $f(q)$ is the q-expansion of a modular form of weight $1/2$, then f and f^2 are both in V.*

Proof. Obviously $f^2 \in M_*(N)$ for some N, so $f^2 \in V$. As for f, by [SS], it is a finite linear combination of series of the form

$$\sum_{n=-\infty}^{\infty} \psi(n) q^{kn^2},$$

where k is a positive integer and ψ is periodic. Equivalently, f is a linear combination of series

$$f_{k,m,a} = \sum_{n \in a+m\mathbb{Z}} q^{kn^2} = \begin{cases} \frac{1}{2} \displaystyle\sum_{n \equiv \pm a \pmod m} q^{kn^2} & \text{if } m \neq 2, \\ \displaystyle\sum_{n \equiv a \pmod 2} q^{kn^2} & \text{if m=2,} \end{cases}$$

where $(a, m) = 1$.

It therefore suffices to prove that $f_{1,m,a} \in V$ whenever a and m are relatively prime, but this is clear since $f_{1,m,a}$ is a linear combination of the multiplicative power series $\sum_{n \in \mathbb{Z}} \chi(n) q^{n^2}$, as χ ranges over the even characters of $(\mathbb{Z}/m\mathbb{Z})^*$. □

Question 7.8. *Are forms of half-integral weight $k \geq 3/2$ finite linear combinations of multiplicative power series?*

References

[BJTX] Jeffrey Beyerl; Kevin James; Catherine Trentacoste; Hui Xue: Products of nearly holomorphic eigenforms. *Ramanujan J.* **27** (2012), no. 3, 377–386.

[CS] John H. Conway, Derek A. Sloane: On quaternions and octonions, AK Peters, 2003.

[Du] W. Duke: When is the product of two Hecke eigenforms an eigenform? Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), 737–741, de Gruyter, Berlin, 1999.

[Em] Brad A. Emmons: Products of Hecke eigenforms. *J. Number Theory* **115** (2005), no. 2, 381–393.

[Fe] Michael Fekete: Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Math. Z.* **17** (1923), 228–249.

[Gh] Eknath Ghate: On products of eigenforms. *Acta Arith.* **102** (2002), no. 1, 27–44.

[He] Erich Hecke: Mathematische Werke, Vandenhoeck und Ruprecht, Göttingen, 1959.

[Ja] Carl G. J. Jacobi: Fundamenta Nova Theoriae Functionum Ellipticarum, 1829.

[Jo] Matthew Leander Johnson: Hecke eigenforms as products of eigenforms. *J. Number Theory* **133** (2013), no. 7, 2339–2362.

[Li] Wen Ch'ing Winnie Li: Newforms and functional equations, *Math. Ann.* **212** (1975), 285–315.

[Ma] Barry Mazur: Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 133–186.

[Po] G. Poitou: Minorations de discriminants (d'après A. Odlyzko), Séminaire Bourbaki 1975/76, 136–153.

[Se] Jean-Pierre Serre: Formes modulaires et fonctions zêta p-adiques, Modular Functions of one Variable III, Lecture Notes in Mathematics 350, Springer-Verlag (1973), 191–268.

[Se2] Jean-Pierre Serre: A Course in Arithmetic, Springer-Verlag, 1973.

[SS] Jean-Pierre Serre, Harold Stark: Modular forms of weight 1/2, Modular Functions of one Variable VI, Lecture Notes in Mathematics 627, Springer-Verlag (1977), 29–68.

[St] Norbert Steinmetz, Rational Iteration: Complex Analytic Dynamical Systems, De Gruyter Studies in Mathematics, 16. Walter de Gruyter & Co., Berlin, 1993.

TABLE 1. Exceptional solutions (mod 3)

$1/2a_0$	a_2	a_3	a_4	a_5	a_7	a_8	a_9	a_{11}	a_{13}	a_{16}	Comments
1	0	0	0	0	2	0	0	0	2	0	E_2
1	0	1	0	0	2	0	1	0	2	0	E_2
1	0	1	1	0	1	0	1	0	2	1	E_2
1	0	2	2	2	0	0	0	1	0	2	$\vartheta_{\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]}$
1	1	1	0	0	1	1	1	0	2	0	E_2
1	1	1	0	0	2	0	1	0	2	0	E_2
1	1	1	1	2	2	1	1	0	2	1	E_2
1	1	1	2	1	2	1	1	0	2	2	E_2
1	1	2	1	1	0	0	1	2	1	1	15.2.1.a
1	1	2	2	0	0	2	0	2	0	2	$\vartheta_{\mathbb{Z}[\sqrt{2}]}$
1	2	1	0	2	2	2	1	0	2	0	E_2
1	2	1	1	0	0	0	1	2	2	1	75.2.1.a or 75.2.1.b
1	2	1	2	1	2	0	1	1	1	2	21.2.1.a
1	2	2	0	1	1	2	1	1	1	2	
1	2	2	2	0	1	2	1	0	1	2	50.2.1.b

8. Appendix, by Anne Larsen

A computer was used to find all multiplicative series whose squares are also multiplicative (when multiplied by a suitable scalar), mod small primes. The series found, excluding mod p versions of the general types listed before and "sparse" solutions, are listed in the tables below. However, for each solution, the same series with even coefficients multiplied by -1 will also be a solution; only one solution in each pair is exhibited in the tables.

Note that there is no table of mod 2 solutions because

$$(1 + a_1 q + a_2 q^2 + \ldots)^2 = 1 + (a_1)^2 q^2 + (a_2)^2 q^4 + \ldots \pmod 2,$$

which has no q term and is therefore not strictly a multiplicative series.

For all but one (mod 3) solution, the comments column gives a possible match for the series as some modular form. Usually, the series is identified as a modified Eisenstein or θ-series. (The modification consists of taking some finite linear combination of $f(q^k)$, so, for example, the mod 19 solution listed as E_6 is actually $E_6(q) - E_6(q^2) + 7E_6(q^4)$.) However, there are also some cusp forms (plus a scalar term, which is interpreted as E_{p-1}), which are identified by their label on the online LMFDB database of holomorphic cusp forms. Proposition 3.7 provides a proof that the mod 13 series identified as 1.12.1.a in the tables is indeed multiplicative; presumably, proofs for the other cusp forms should be similar.

There were no exceptional solutions mod 23, 29, or 31.

TABLE 2. Exceptional solutions (mod 5)

$1/2a_0$	a_2	a_3	a_4	a_5	a_7	a_8	a_9	a_{11}	a_{13}	a_{16}	Comments
1	1	2	2	1	4	0	4	2	3	4	E_4
1	1	2	3	0	1	0	2	2	2	1	5.4.1.a
1	2	3	3	1	3	0	3	2	4	4	E_2
1	2	4	4	1	3	4	3	2	4	4	E_2
1	3	4	2	1	3	0	3	2	4	1	E_2
2	3	3	4	1	4	2	2	2	3	1	E_4

TABLE 3. Exceptional solutions (mod 7)

$1/2a_0$	a_2	a_3	a_4	a_5	a_7	a_8	a_9	a_{11}	a_{13}	a_{16}	Comments
1	6	2	3	6	2	0	4	3	1	2	3.6.1.a
2	5	2	5	2	0	5	1	0	2	5	$\vartheta_{\mathbb{Z}[i]}$
3	2	4	1	1	1	6	6	5	0	2	E_2
3	2	5	2	2	0	2	1	0	2	2	$\vartheta_{\mathbb{Z}[i]}$
3	3	0	2	0	0	3	2	1	0	4	7.6.1.a
3	3	6	5	4	1	6	3	3	0	3	E_6

TABLE 4. Exceptional solutions (mod 11)

4	3	1	10	0	2	3	1	0	2	10	$\vartheta_{\mathbb{Z}[\zeta_3]}$
5	6	9	8	1	5	7	0	7	4	2	2.10.1.a

TABLE 5. Exceptional solutions (mod 13)

$1/2a_0$	a_2	a_3	a_4	a_5	a_7	a_8	a_9	a_{11}	a_{13}	a_{16}	Comments
2	2	5	10	7	0	6	3	0	8	7	1.12.1.a
2	5	11	10	9	6	11	8	6	1	6	E_4
4	6	10	9	6	12	1	0	8	1	5	E_6

TABLE 6. Exceptional solutions (mod 17)

$1/2a_0$	a_2	a_3	a_4	a_5	a_7	a_8	a_9	a_{11}	a_{13}	a_{16}	Comments
3	12	1	16	5	14	16	12	5	7	14	1.16.1.a
4	7	12	11	11	13	13	14	4	5	14	E_8

TABLE 7. Exceptional solutions (mod 19)

$1/2a_0$	a_2	a_3	a_4	a_5	a_7	a_8	a_9	a_{11}	a_{13}	a_{16}	Comments
1	5	15	5	2	0	5	1	0	2	5	$\vartheta_{\mathbb{Z}[i]}$
5	6	15	6	2	0	6	1	0	2	6	$\vartheta_{\mathbb{Z}[i]}$
5	13	16	5	10	12	15	13	8	15	12	E_6
9	7	15	7	2	0	7	1	0	2	7	$\vartheta_{\mathbb{Z}[i]}$

Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A.
E-mail address: mjlarsen@indiana.edu