A NEW WITNESS IDENTITY FOR $11|p(11n+6)$

PETER PAULE AND CRISTIAN-SILVIU RADU

Dedicated to our friend Krishna Alladi on his 60th birthday

Abstract. Let $p(n)$ be the number of partitions of the positive integer n. A new q-series identity is presented which witnesses Ramanujan's observation that $11|p(11n+6)$ for all $n \geq 0$ at one glance. This identity can be derived in a natural way by applying an algorithm to present subalgebras of the polynomial ring $\mathbb{K}[z]$ as $\mathbb{K}[z]$-modules.

1. Introduction

Recall the celebrated partition congruences observed by Ramanujan [10]:

$$p(5n+4) \equiv 0 \pmod 5, \quad p(7n+5) \equiv 0 \pmod 7, \tag{1}$$

and

$$p(11n+6) \equiv 0 \pmod{11}, \quad n \geq 0, \tag{2}$$

where $p(n)$ counts the number of partitions of the positive integer n.

For the congruences in (1) Ramanujan [10] provided clever elementary proofs based on Euler's pentagonal number theorem and on Jacobi's identity for the third power of Dedekind's eta-function. Also in [10], Ramanujan presented two q-series identities which in explicit fashion witness the stated divisibilities by 5 and 7:

$$\sum_{n=0}^{\infty} p(5n+4)q^n = 5\prod_{n=1}^{\infty}\frac{(1-q^{5n})^5}{(1-q^n)^6}, \tag{3}$$

$$\sum_{n=0}^{\infty} p(7n+5)q^n = 7\prod_{n=1}^{\infty}\frac{(1-q^{7n})^3}{(1-q^n)^4} + 49q\prod_{n=1}^{\infty}\frac{(1-q^{7n})^7}{(1-q^n)^8}. \tag{4}$$

Bruce Berndt's commentary in [5, pp. 372–375] on Ramanujan's paper gives the history of proofs of Ramanujan's congruences. In particular, Berndt points to the fact that (4) in Ramanujan's original paper is stated without any proof and also that Ramanujan only briefly sketches a proof of (3)—an identity greatly admired by Hardy; see Hardy's remark in [5, p. xxxv].

Concerning Ramanujan's congruence (2) a witness identity like (3) or (4), i.e., presenting $\sum_{n\geq 0} p(11n+6)q^n$ as a linear combination of eta-quotients, has been found only recently by Radu [9] with the help of his Ramanujan-Kolberg Algorithm. As the main theorem of this note we present a new and simpler witness identity but built in different fashion:

The research of Radu was supported by the strategic program "Innovatives OÖ 2010 plus" by the Upper Austrian Government in the frame of project W1214-N15-DK6 of the Austrian Science Fund (FWF). Both authors were supported by grant SFB F50-06 of the Austrian Science Fund (FWF).

Theorem 1.1. *Let*

$$t := q^{-5} \prod_{k=1}^{\infty} \left(\frac{1-q^k}{1-q^{11k}} \right)^{12}, \tag{5}$$

and

$$f := q\, t \prod_{k=1}^{\infty} (1-q^{11k}) \sum_{n=0}^{\infty} p(11n+6) q^n. \tag{6}$$

Then

$$\begin{aligned} f^5 &= 5 \cdot 11^4 f^4 + 11^4(-2 \cdot 5 \cdot 11^4 + 251\, t) f^3 \\ &\quad + 11^3(2 \cdot 5 \cdot 11^9 + 2 \cdot 3 \cdot 5 \cdot 11^5 \cdot 31\, t + 4093\, t^2) f^2 \\ &\quad + 11^4(-5 \cdot 11^{12} + 2 \cdot 5 \cdot 11^8 \cdot 17\, t - 2^2 \cdot 3 \cdot 11^3 \cdot 1289\, t^2 + 3 \cdot 41\, t^3) f \\ &\quad + 11^5(11^4 + t)(11^{11} - 3 \cdot 7 \cdot 11^7\, t + 11^2 \cdot 1321\, t^2 + t^3). \end{aligned} \tag{7}$$

The divisibility $11|p(11n+6)$ follows immediately from the fact that all coefficients of powers of q on the right hand side are integers containing 11 as a factor. This property clearly carries over to f since f^5 is an element of an integral domain—regardless whether the q-series/products involved are considered as formal Laurent series or as analytic functions.

The rest of this article is structured as follows. In Section 2 we put the witness identity (7) into the algebraic framework of presenting subalgebras of the polynomial ring $\mathbb{K}[z]$ as finitely generated $\mathbb{K}[z]$-modules. To apply the machinery for deriving the witness identity (7) in algorithmic fashion, basic facts from modular functions are needed; these are provided in Section 3. One of the consequences of this setting is a computational verification of (7). Section 4 describes an algorithm to compute the desired module presentation for the case of polynomials. The analogous algorithm for modular functions is discussed in Section 5, including the algorithmic derivation of the witness identity (7).

2. Presenting Subalgebras of the polynomial ring $\mathbb{K}[z]$

By $\mathbb{K}[z]$ we denote the ring of univariate polynomials in z with coefficients from a field $\mathbb{K}$. In our context it is useful to keep in mind that $\mathbb{K}[z]$ is also a vector space over $\mathbb{K}$; sometimes we emphasize this fact by saying that $\mathbb{K}[z]$ is a $\mathbb{K}$-algebra[1] For example, we can consider the $\mathbb{K}$-algebra generated by given polynomials $f_0, \dots, f_n \in \mathbb{K}[z]$,

$$\mathbb{K}[f_0, f_1, \dots, f_n] := \Big\{ \sum_{j_0, j_1, \dots, j_n \geq 0} c_{j_0, j_1, \dots, j_n} f_0^{j_0} f_1^{j_1} \dots f_n^{j_n} \Big\};$$

i.e., the elements are polynomials in the f_j with coefficients $c_{j_0, j_1, \dots, j_n} \in \mathbb{K}$.

We will consider also slight variations of this setting. For example, the right hand side of (7) can be considered as an element of the $\mathbb{Q}$-algebra $\mathbb{Q}[t, f]$. Here t and f are not polynomials but Laurent series in q. More precisely, the right hand side of (7) has a particular structure; namely, it is an element of

$$\mathbb{Q}[t] + \mathbb{Q}[t]f + \dots + \mathbb{Q}[t]f^4 := \{p_0(t) + p_1(t)f + \dots + p_4(t)f^4 : p_j(t) \in \mathbb{Q}[t]\}.$$

[1] For us a $\mathbb{K}$-algebra R is a commutative ring R with 1 which is also a vector space over $\mathbb{K}$.

Obviously this is a subalgebra of $\mathbb{Q}[t,f]$. Vice versa, the relation (7) guarantees that all the elements of $\mathbb{Q}[t,f]$ are contained in this subalgebra. As a consequence, the witness identity (7) has also an *algebraic* meaning; namely,

$$\mathbb{Q}[t,f]=\mathbb{Q}[t]+\mathbb{Q}[t]f+\cdots+\mathbb{Q}[t]f^4. \tag{8}$$

In other words, (8) tells us that the algebra $\mathbb{Q}[t,f]$ can be presented as a module over the polynomial ring $\mathbb{Q}[t]$ with module generators $1,f,\dots,f^4$.

We note that this module is freely generated[2] owing to fact that the orders $\mathrm{ord}(f^j)$ are pairwise different. As usual, for a formal Laurent series, resp. meromorphic function, $F(q)=\sum_{n=\ell}^{\infty}F_nq^n$ with $F_\ell\neq 0$, its order is defined as $\mathrm{ord}(F(q)):=\ell$.

It is well-known that subalgebras of $\mathbb{K}[z]$ are finitely generated:

Theorem 2.1 ([4]). *Let $A\neq\mathbb{K}$ be a subalgebra of $\mathbb{K}[z]$ and let n be the degree of the polynomial of smallest positive degree in A. Then A can generated by a set of not more than $n+1$ elements.*

Gale's proof is elegant and short, but non-constructive. Nevertheless, its underlying idea bases on presenting a subalgebra as a finitely generated $\mathbb{K}[t]$-module as in (8). Almost 60 years after Gale's paper, Radu [3] in [9] introduced a constructive version of this approach.

Remark 2.2. Presentations like (8) also solve the problem to decide subalgebra membership. In computer algebra usually such problems are solved by constructing a convenient basis. To this end, for *multivariate* polynomial rings, SAGBI ("Subalgebra Analogs to Gröbner Bases for Ideals") bases are considered. This concept was introduced by Kapur and Madlener [7] and independently by Robbiano and Sweedler [11]. They also present a method for computing such bases given a set of generators for a subalgebra of a multivariate polynomial ring. In general this method is not algorithmic, but in the *univariate* case $\mathbb{K}[z]$ it can be shown to terminate after a finite number of steps. In this context, Anna Torstensson [12] gave a careful algorithm analysis for the case when the subalgebra is generated by two polynomials. Radu's algorithm works completely different to the SAGBI mechanism. The algorithm computes a Noether normalization (e.g., [3, Theorem 30]) of a finitely generated $\mathbb{K}$-subalgebra of $\mathbb{K}[z]$ to solve the subalgebra membership problem in the case of *univariate* polynomial rings.

In Section 4 we explain the main algorithmic ideas used to establish (7), resp. (8). Before doing so, we set up the required algebraic/analytic frame for these equalities.

3. Modular Functions Background

Modular functions provide a convenient mathematical environment for the objects t and f in Theorem 1.1. In this context we view $q=q(\tau)$ as a function on the upper half complex plane $\mathbb{H}:=\{\tau\in\mathbb{C}:\mathrm{Im}(\tau)>0\}$ defined by $q(\tau):=\exp(2\pi i\tau)$. The congruence subgroup $\Gamma_0(N)$ of the modular group is defined as

$$\Gamma_0(N):=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}):N|c\right\}.$$

[2] I.e., every element $p_0(t)+p_1(t)f+\cdots+p_4(t)f^4$ in the module has uniquely determined coefficients $p_j(t)\in\mathbb{Q}[t]$.

[3] Not knowing about Gale's paper at that time.

A holomorphic function g defined on $\mathbb{H}$ is called a modular function for $\Gamma_0(N)$ if (i) for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$,

$$g\left(\frac{a\tau+b}{c\tau+d}\right) = g(\tau), \;\; \tau \in \mathbb{H}, \tag{9}$$

and (ii) if for each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ there exists a Laurent series expansion with *finite principal part* such that for all $\tau \in \mathbb{H}$ sufficiently close to $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$:

$$g(\tau) = \sum_{n=-\infty}^{\infty} c_n(\gamma) e^{2\pi i n(\gamma^{-1}\tau)/w_\gamma} \tag{10}$$

where

$$w_\gamma := \min\left\{ h \in \mathbb{N} \setminus \{0\} : \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \gamma^{-1}\Gamma_0(N)\gamma \right\}.$$

Note. $\mathrm{SL}_2(\mathbb{Z})$ and $\Gamma_0(N)$ act on $\mathbb{H}$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau := \frac{a\tau+b}{c\tau+d}$, and also on $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ by defining $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\infty := \frac{a}{c}$ and $\frac{a}{0} := \infty$.

If $m = m(\gamma)$ is the smallest index such that $c_m(\gamma) \neq 0$ in (10), then we call m the γ-order of g at $\tau = \frac{a}{c}$; notation: $m = \mathrm{ord}^{\gamma}_{a/c}(g)$. If $\frac{a}{c} = \gamma_1\infty = \gamma_2\infty$ for $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$, then $\mathrm{ord}^{\gamma_1}_{a/c}(g) = \mathrm{ord}^{\gamma_2}_{a/c}(g)$. This leads to define the order of a modular function g at a point $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$, called a "cusp of g", by

$$\mathrm{ord}_{a/c}(g) := \mathrm{ord}^{\gamma}_{a/c}(g)$$

for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma\infty = \frac{a}{c}$.

The action of $\Gamma_0(N)$ maps cusps onto cusps, and it turns out that for each $N \in \mathbb{N} \setminus \{0\}$ the set of cusps $\mathbb{Q} \cup \{\infty\}$ splits only into finitely many orbits. A cusp $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ is called a critical point of a modular function g if $\mathrm{ord}_{a/c}(g) < 0$. This property is invariant under the action of $\Gamma_0(N)$ owing to the fact that for two cusps $\frac{a}{c}$ and $\frac{a'}{c'}$ from the same orbit, i.e., $\frac{a'}{c'} = \gamma\frac{a}{c}$ for some $\gamma \in \Gamma_0(N)$, one has

$$\mathrm{ord}_{a'/c'}(g) = \mathrm{ord}_{a/c}(g).$$

The $\Gamma_0(N)$-orbit of the cusp $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ is denoted by $[\frac{a}{c}]$. An orbit $[\frac{a}{c}]$ where $\frac{a}{c}$ is a critical point of g is called critical orbit of g.

The set of modular functions for $\Gamma_0(N)$ forms a $\mathbb{C}$-algebra denoted by $M(N)$. An important subalgebra is

$$M^{\infty}(N) := \{g \in M(N) : g \text{ is constant, or } [\infty] \text{ is the only critical orbit of } g\}.$$

This, in view of (10), gives a normal form presentation for any modular function $g \in M^{\infty}(N)$. Namely, we take the Laurent series expansion at the cusp ∞ using $\gamma := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \mathrm{Id}$:

$$g(\tau) = \sum_{n=\mathrm{ord}_{\infty}(g)}^{\infty} c_n q^n. \tag{11}$$

Note that $q = q(\tau) = \exp(2\pi i\tau)$, $c_n := c_n(\mathrm{Id})$, and $w_\gamma = w_{\mathrm{Id}} = 1$; if g is a constant then $\mathrm{ord}_{\infty}(g) = 0$ and $c_n = 0$ for all $n \geq 1$. We call this unique Laurent series the *q-series presentation* of g.

This setting provides a convenient mathematical environment for the objects t and f in Theorem 1.1.

Lemma 3.1. *Let t and f be defined as in* (5) *and* (6) *of Theorem 1.1 where $q = q(\tau) := \exp(2\pi i\tau), \tau \in \mathbb{H}$. Then*

$$t, f \in M^{\infty}(11),$$

and the q-series/products in (5) *and* (6) *correspond to the Laurent series expansions of t and f at the cusp ∞ as in* (11). *Consequently,*

$$\mathrm{ord}_{\infty}(t) = -5 \ \ \textit{and} \ \ \mathrm{ord}_{\infty}(f) = -4.$$

Proof. The statement follows immediately from

$$q^{-5}\prod_{k=1}^{\infty}\left(\frac{1-q^{k}}{1-q^{11k}}\right)^{12} \in M^{\infty}(11) \text{ and } q\prod_{k=1}^{\infty}(1-q^{11k})\sum_{n=0}^{\infty}p(11n+6)q^{n} \in M^{\infty}(11),$$

which, for instance, is proven in [9]. □

Despite the analytic setting, to decide equality of two functions in $M^{\infty}(N)$ can be done in purely algebraic and finitary fashion.

Lemma 3.2. *Let g and h be in $M^{\infty}(N)$ with q-series presentations*

$$g(\tau) = \sum_{n=\mathrm{ord}_{\infty}(g)}^{\infty} a_n q^n \ \ \textit{and} \ \ h(\tau) = \sum_{n=\mathrm{ord}_{\infty}(h)}^{\infty} b_n q^n.$$

Then $g = h$ if and only if $\mathrm{ord}_{\infty}(g) = \mathrm{ord}_{\infty}(h) =: \ell$ *and*

$$(a_{\ell}, \dots, a_{-1}, a_0) = (b_{\ell}, \dots, b_{-1}, b_0).$$

Proof. See [8, Sect. 6], or any introductory text on modular functions. □

In other words, if $g(\tau) = \sum_{n=\mathrm{ord}_{\infty}(g)}^{\infty} a_n q^n \in M^{\infty}(N)$, the coefficients a_n, $n \geq 1$, are uniquely determined by those of the principal part and a_0. Algebraically this corresponds to an isomorphic embedding of $\mathbb{C}$-vector spaces:

$$\begin{aligned} &\varphi : M^{\infty}(N) \to \mathbb{C}[z], \\ &\sum_{n=\mathrm{ord}_{\infty}(g)}^{\infty} a_n q^n \mapsto a_{\mathrm{ord}_{\infty}(g)} z^{-\mathrm{ord}_{\infty}(g)} + \cdots + a_{-1}z + a_0. \end{aligned} \tag{12}$$

In computationally feasible cases the zero test for $g - h \overset{?}{=} 0$ of Lemma 3.2 trivializes the task of proving identities between modular functions.

Example 3.3. Knowing from Lemma 3.1 that t and f are in $M^{\infty}(11)$ the proof of the witness identity (7) can be left to a computer algebra package: First one specifies the input for t and f as, for instance, in `In[16]` and `In[17]` of Section 5. Then applying a simplification command as, for instance, `Simplify` in Mathematica reduces the difference of the expressions on the left and on the right hand side of (7) to `O[q]^2`; this means, to 0 in view of Lemma 3.2.

4. Algorithm "MODULE GENERATORS" for Polynomials

In view of the isomorphic vector space embedding φ defined in (12), we present an algorithm to compute a suitable module presentation as in (8).

ALGORITHM 4.1 ("MODULE GENERATORS: polynomial case")**.**
Given non-constant polynomials $t := f_0, f_1, \dots, f_n \in \mathbb{K}[z]$*, the algorithm computes* $g_1, \dots, g_k \in \mathbb{K}[z]$ *such that*

$$\mathbb{K}[t, f_1, \dots, f_n] = \mathbb{K}[t] + \mathbb{K}[t]\, g_1 + \cdots + \mathbb{K}[t]\, g_k. \tag{13}$$

To explain a basic ingredient of the algorithm, we first consider the problem of finding convenient presentations of finitely generated additive submonoids of $\mathbb{N} = \{0, 1, \dots\}$.

Example 4.2. Consider the submonoid M generated by 6, 9, and 20; i.e.,

$$M = \{6a + 9b + 20c : a, b, c \in \mathbb{N}\}.$$

The presentation of M which is most relevant for our purpose is a set partition of M into residue classes modulo t:

$$[M]_i := \{x \in M : x \equiv i \pmod{t}\}.$$

For example, choosing $t := 6$ we have that M is the disjoint union of $[M]_0, \dots, [M]_5$ where $[M]_0 = 0 + 6\mathbb{N} = \{0 + 6m : m \in \mathbb{N}\}$, and

$$[M]_1 = 49 + 6\mathbb{N}, [M]_2 = 20 + 6\mathbb{N}, [M]_3 = 9 + 6\mathbb{N}, [M]_4 = 40 + 6\mathbb{N}, [M]_5 = 29 + 6\mathbb{N}.$$

Example 4.3. How does one compute the elements $49, 20$, etc.? For example, 49 is the smallest element of the form $1 + 6a$ that can be represented in the form $9b + 20c$, $a, b, c \in \mathbb{N}$. There are various tools to solve such linear Diophantine problems; e.g., the Omega package [1, 2] written in Mathematica:

```
In[1]:= << RISC`Omega.m`
        Omega Package version 2.49 written by Axel Riese (in cooperation
        with George E. Andrews and Peter Paule) © RISC-JKU

In[2]:= OEqR[OEqSum[x^a y^b z^c, −6a + 9b + 20c == 1, λ]]
                  x^8 y z^2
Out[2]= ─────────────────────────────
        (1 − x^3 y^2)(1 − x^10 z^3)
```

Out[2] gives the rational form of the generating function $\sum x^a y^b z^c$ of all non-negative integer triples (a, b, c) satisfying $-6a + 9b + 20c = 1$; $(8, 1, 2)$ corresponds to $9 \cdot 1 + 20 \cdot 2 = 1 + 6 \cdot 8 = 49$.

Next we consider what happens when to a given submonoid of $\mathbb{N}$ another generator is added[4].

Example 4.4. Consider the submonoid M^+ generated by 4, 6, 9, and 20; i.e.,

$$M = \{4a + 6b + 9c + 20d : a, b, c, d \in \mathbb{N}\} := \langle 4, 6, 9, 20 \rangle. \tag{14}$$

Note. Subsequently it will be convenient to use a short hand notation for the monoid which lists its generators as on the right side of (14).

Keeping the choice $t := 6$, we need to update the residue classes. Doing so, we obtain $M^+ = [M^+]_0 \cup \cdots \cup [M^+]_5$ where $[M^+]_0 = 0 + 6\mathbb{N}$, and

$$[M^+]_1 = 13 + 6\mathbb{N}, [M^+]_2 = 8 + 6\mathbb{N}, [M^+]_3 = 9 + 6\mathbb{N}, [M^+]_4 = 4 + 6\mathbb{N}, [M^+]_5 = 17 + 6\mathbb{N}.$$

A simple but relevant observation is that for each j the smallest element in $[M^+]_j$ is less or equal to smallest element in $[M]_j$.

[4] An entertaining application of this situation is shown in the Numberphile video "How to order 43 Chicken McNuggets": `www.youtube.com/watch?v=vNTSugyS038`

These elementary facts about monoids are used to compute the desired module presentations.

Example 4.5. As specified in the input/output description of Algorithm 4.1 we compute a module presentation of the subalgebra $\mathbb{Q}[t, f_1, f_2]$ of $\mathbb{Q}[z]$ where

```
In[3]:= t = z^6 - 1; f1 = z^9 + 2; f2 = z^20 + 1;
```

Obviously the monoid $\langle 6, 9, 20\rangle$ generated by the degrees of t, f_1, and f_2 is a subset of the set of all possible degrees arising from the polynomials in $\mathbb{Q}[t, f_1, f_2]$. Consequently, in view of Example 4.2, it is a natural idea to choose as monoid generators $g_j \in \mathbb{Q}[t, f_1, f_2]$ such that

$$\textit{(T1)} \qquad (\deg(g_1), \deg(g_2), \deg(g_3), \deg(g_4), \deg(g_5)) \equiv (1, 2, 3, 4, 5) \pmod{6}.$$

Note that here, as in Example 4.2, we decided to go modulo 6 which is the smallest degree of the given polynomials t, f_1, and f_2. For setting up presentations of monoids in general, this choice is free and can be adapted to the context.

To establish

$$\mathbb{Q}[t, f_1, f_2] = \mathbb{Q}[t] + \mathbb{Q}[t]\, g_1 + \cdots + \mathbb{Q}[t]\, g_5 \tag{15}$$

we need to show:

$$\textit{(T2a)} \qquad \mathbb{Q}[t] + \mathbb{Q}[t]\, g_1 + \cdots + \mathbb{Q}[t]\, g_5 \text{ is a subalgebra of } \mathbb{Q}[t, f_1, f_2]; \text{ and}$$

$$\textit{(T2b)} \qquad f_1, f_2 \in \mathbb{Q}[t] + \mathbb{Q}[t]\, g_1 + \cdots + \mathbb{Q}[t]\, g_5.$$

Task (T1). By Examples 4.2 and 4.3 we know that $49 = 1 \cdot 9 + 2 \cdot 20$ is the smallest element in the monoid $\langle 6, 9, 20\rangle$ which is congruent to 1 modulo 6. This suggests to take

```
In[4]:= g1 = f1 f2^2.
```

With the same reasoning we choose also the remaining elements:

```
In[5]:= g2 = f2; g3 = f1; g4 = f2^2; g5 = f1 f2;
```

This choice satisfies *(T1)*:

$$\begin{aligned}(\deg(g_1), \deg(g_2), \deg(g_3), \deg(g_4), \deg(g_5)) &= (49, 20, 9, 40, 29)\\ &\equiv (1, 2, 3, 4, 5) \pmod{6},\end{aligned}$$

and settles also *Task (T2b)*.

In view of In[4] and In[5] *Task (T2a)* amounts to show

$$g_i g_j \in \mathbb{Q}[t] + \mathbb{Q}[t]\, g_1 + \cdots + \mathbb{Q}[t]\, g_5 \text{ for all } i, j \in \{1, \ldots, 5\}.$$

This is checked computationally. For example,

```
 In[6]:= {g3^2, g3^2 - t^3}//Expand
Out[6]=  {4 + 4z^9 + z^18, 5 - 3z^6 + 4z^9 + 3z^12}
 In[7]:= {g3^2 - t^3, g3^2 - t^3 - 3t^2}//Expand
Out[7]=  {5 - 3z^6 + 4z^9 + 3z^12, 2 + 3z^6 + 4z^9}
 In[8]:= {g3^2 - t^3 - 3t^2, g3^2 - t^3 - 3t^2 - 4g3}//Expand
Out[8]=  {2 + 3z^6 + 4z^9, -6 + 3z^6}
 In[9]:= {g3^2 - t^3 - 3t^2 - 4g3, g3^2 - t^3 - 3t^2 - 4g3 - 3(t - 1)}//Expand
Out[9]=  {-6 + 3z^6, 0}
```

In other words, we obtained

$$g_3^2 = t^3 + 3t^2 + 3(t-1) + 4g_3 \in \mathbb{Q}[t] + \mathbb{Q}[t]\, g_1 + \cdots + \mathbb{Q}[t]\, g_5.$$

Such reductions work for all $g_i g_j$. To give another example,

$$g_2 g_4 = p - 3g_2 + 3g_4$$

for

$$p = t^{10} + 10t^9 + 45t^8 + 120t^7 + 210t^6 + 252t^5 + 210t^4 + 120t^3 + 45t^2 + 10t + 2.$$

In contrast to Example 4.5, in general it is not true that

$$\{\deg g(z) : g(z) \in \mathbb{K}[t, f_1, \ldots, f_n]\} = \langle \deg t(z), \deg f_1(z), \ldots, \deg f_n(z)\rangle;$$

see the next example.

Example 4.6. Consider the subalgebra $\mathbb{Q}[t, f_1, f_2, f_3]$ of $\mathbb{Q}[z]$ where

```
In[10]:= t = z^6 − 1; f1 = z^9 + 2; f2 = z^20 + 1; f3 = z^18 + z^4;
```

Observe that

$$\begin{aligned}\langle \deg t(z), \deg f_1(z), \deg f_2(z), \deg f_3(z)\rangle &= \langle 6, 9, 20, 18\rangle = \langle 6, 9, 20\rangle \\ &\neq \{\deg h(z) : g(z) \in \mathbb{Q}[t, f_1, f_2, f_3]\};\end{aligned}$$

for instance,

$$h(z) := f_3 - (t^3 + 3t^2 + 3t) = z^4 + 1 \in \mathbb{Q}[t, f_1, f_2, f_3] \tag{16}$$

and therefore, $\deg(h) = \deg(z^4 + 1) = 4 \neq \langle 6, 9, 20\rangle$. Consequently, to obtain a general algorithm as specified in Algorithm 4.1, we need to modify the procedure from Example 4.5 as follows: we update the given data by considering $\mathbb{Q}[t, f_1, f_2, f_3, f_4]$ instead of $\mathbb{Q}[t, f_1, f_2, f_3]$ by adding explicitly the "new" element from (16):

```
In[11]:= f4 = z^4 + 1;
```

Recall Example 4.4 where the element 4 was added to the monoid $\langle 6, 9, 20\rangle$; this had the effect that for the resulting monoid $\langle 4, 6, 9, 20\rangle$ the smallest elements in the representing residue classes modulo 6 changed from $(49, 20, 9, 40, 29)$ to $(13, 8, 9, 4, 17)$. For termination reasons of the algorithm it is important to note that by adding a new element to the monoid the new smallest elements are less or equal than their predecessors in the respective residue classes.

To obtain a module representation for $\mathbb{Q}[t, f_1, f_2, f_3, f_4]$ we utilize this observation when updating the generators g_j accordingly. This means, we now choose $G_j \in \mathbb{Q}[t, f_1, f_2, f_3, f_4]$ such that

```
In[12]:= G1 = f1f4; G2 = f4^2; G3 = f1; G4 := f4; G5 = f1f4^2;
```

This choice satisfies condition *(T1)* from above:

$$\begin{aligned}(\deg(G_1), \deg(G_2), \deg(G_3), \deg(G_4), \deg(G_5)) &= (13, 8, 9, 4, 17) \\ &\equiv (1, 2, 3, 4, 5) \pmod 6.\end{aligned}$$

Because of

```
In[13]:= f2 − G4^5 + 5G2^2 − 10G4^3 + 10G2 − 5G4//Expand
Out[13]= 0
```

and (16) it also satisfies condition *(T2b)*. Again a computational check verifies condition *(T2a)*; for example:

```
In[14]:= G1^2 − (t^3 + 3t^2 + 3t − 3)G2 − 4G5//Expand
Out[14]= 0
```

From Example 4.6 we can obtain a complete picture of the Algorithm 4.1, namely: Out of the subalgebra generators $f_0, \dots, f_n \in \mathbb{K}[z]$ we choose a non-constant element $t := f_0$ which fixes the modulus $\deg(t)$ for all the steps of the algorithm. It also determines the module structure

$$\mathbb{K}[t] + \mathbb{K}[t]\, g_1 + \cdots + \mathbb{K}[t]\, g_k$$

for the first step of the algorithm, where $k = \deg(t) - 1$ is the number of non-constant module generators $g_1, \dots, g_k \in \mathbb{K}[z]$. Whenever it happens, as in Example 4.6, that during the module-reduction with respect to $g_1, \dots, g_k$ multiplied by powers of t an element $h \in \mathbb{K}[t, f_1, \dots, f_n]$ arises with

$$\deg(h) \not\in \langle \deg(t), \deg(f_1), \dots, \deg(f_n) \rangle,$$

then we update to new generators $G_1, \dots, G_k$ as in Example 4.6. Since in each such update-step the degrees of the G_j are less or equal to those of the corresponding g_j (at least one degree has to be smaller in case of an update!), the algorithm terminates after a finite number of steps.

5. Algorithm "MODULE GENERATORS" for Modular Functions

Algorithm 4.1 carries over from polynomials to modular functions by the linear embedding φ defined in (12). We present the version given in [8].

ALGORITHM 5.1 ("MODULE GENERATORS: modular function case"). *Given non-constant modular functions* $t := f_0, f_1, \dots, f_n \in M^\infty(N)$ *with* $m := -\operatorname{ord}_\infty(t)$ *and*

$$\gcd\left(\operatorname{ord}_\infty(t), \operatorname{ord}_\infty(f_2), \dots, \operatorname{ord}_\infty(f_n)\right) = 1,$$

the algorithm computes $g_1, \dots, g_{m-1} \in M^\infty(N)$ *such that*

$$\mathbb{C}[t, f_1, \dots, f_n] = \mathbb{C}[t] + \mathbb{C}[t]\, g_1 + \cdots + \mathbb{C}[t]\, g_{m-1}. \tag{17}$$

The gcd-condition and also the steps of the algorithm are explained in detail in [8]. In fact, exchanging the polynomial degrees with negative orders, the algorithm works completely analogous to the case of polynomials.

As an illustration we sketch the derivation of our 11-witness identity (7).

Example 5.2. Consider $\mathbb{C}[t, f]$ with $t, f \in M^\infty(N)$ as in (5) and (6) of our main Theorem (1.1). We have $m = -\operatorname{ord}_\infty(t) = 5$, hence we expect $m - 1 = 4$ module generators in addition to the constant function 1. Observing that

$$\begin{aligned}(-\deg(f), -\deg(f^2), -\deg(f^3), -\deg(f^4)) &= (4, 8, 12, 16) \\ &\equiv (4, 3, 2, 1) \pmod 5,\end{aligned}$$

we choose

$$(g_1, g_2, g_3, g_4) := (f, f^2, f^3, f^4).$$

This matches condition *(T1)* above; condition *(T2b)* is trivially satisfied. Owing to the fact that $g_i g_j = f^{i+j}$, to verify condition *(T2a)* reduces to showing that

$$f^5 \in \mathbb{C}[t] + \mathbb{C}[t]\, f + \mathbb{C}[t]\, f^2 + \mathbb{C}[t]\, f^3 + \mathbb{C}[t]\, f^4.$$

But this is a *straightforward* computational exercise. In fact, anyone being familiar with Example 4.5 can easily accomplish this task; in other words, can easily "discover" herself/himself the witness identity (7) just by applying the reduction process to f^5 with respect to the given t and f.

We restrict to present only the first steps of this computational "discovery" of (7).

$$\text{In[15]:=}\quad \mathbf{Tquot[k\_] := \frac{1-q^{k}}{1-q^{11k}};}$$

$$\text{In[16]:=}\quad \mathbf{t = \frac{1}{q^{5}}Product[Series[Tquot[k]^{12}, q, 0, 26], k, 1, 26]}$$

$$\text{Out[16]=}\quad \frac{1}{q^{5}} - \frac{12}{q^{4}} + \frac{54}{q^{3}} - \frac{88}{q^{2}} - \frac{99}{q} + 540 - 418q - 648q^{2} + \cdots - 22176q^{20} + 61656q^{21} + O[q]^{22}$$

$$\text{In[17]:=}\quad \mathbf{f = qtSeries[(1-q^{11})(1-q^{22}), q, 0, 21] * Sum[PartitionsP[11n+6]q^{n}, n, 0, 21]}$$

$$\text{Out[17]=}\quad \frac{11}{q^{4}} + \frac{165}{q^{3}} + \frac{748}{q^{2}} + \frac{1639}{q} + 3553 + 4136q + 6347q^{2} + \cdots + 12738q^{16} - 51216q^{17} + O[q]^{18}$$

$$\text{In[18]:=}\quad \mathbf{F = \frac{f}{11};}$$

$$\text{In[19]:=}\quad \mathbf{F^{5}}$$

$$\text{Out[19]=}\quad \frac{1}{q^{20}} + \frac{75}{q^{19}} + \frac{2590}{q^{18}} + \cdots + \frac{298958660282220}{q} + 530018316923711 + 877706745683995q + O[q]^{2}$$

$$\text{In[20]:=}\quad \mathbf{F^{5} - t^{4}}$$

$$\text{Out[20]=}\quad \frac{123}{q^{19}} + \frac{1510}{q^{18}} + \frac{69935}{q^{17}} + \cdots + 530018316923711 + 877706745683995q + O[q]^{2}$$

$$\text{In[21]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41 * t^{3}F}$$

$$\text{Out[21]=}\quad \frac{4093}{q^{18}} + \frac{54929}{q^{17}} + \frac{570947}{q^{16}} + \cdots + 530565611750339 + 877363195058527q + O[q]^{2}$$

$$\text{In[22]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41t^{3}F - 4093t^{2}F^{2}}$$

$$\text{Out[22]=}\quad \frac{30371}{q^{17}} + \frac{1008898}{q^{16}} + \frac{12509585}{q^{15}} + \cdots + 536556550241327 + 873666097417069q + O[q]^{2}$$

$$\text{In[23]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41t^{3}F - 4093t^{2}F^{2} - 11^{2} * 251 * tF^{3}}$$

$$\text{Out[23]=}\quad \frac{6655}{q^{16}} + \frac{573782}{q^{15}} - \frac{16074850}{q^{14}} + \cdots + 552225581222579 + 867953372178310q + O[q]^{2}$$

$$\text{In[24]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41t^{3}F - 4093t^{2}F^{2} - 11^{2} * 251 * tF^{3} - 11^{3} * 5 * F^{4}}$$

$$\text{Out[24]=}\quad \frac{174482}{q^{15}} - \frac{26869260}{q^{14}} + \frac{438710910}{q^{13}} + \cdots - 2294272165605596 - 3831090632203670q + O[q]^{2}$$

$$\text{In[25]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41t^{3}F - 4093t^{2}F^{2} - 11^{2} * 251 * tF^{3} - 11^{3} * 5 * F^{4} -}$$
$$\mathbf{11^{2} * 2 * 7 * 103 * t^{3}}$$

$$\text{Out[25]=}\quad \frac{20587908}{q^{14}} + \frac{335068602}{q^{13}} + \frac{3501794450}{q^{12}} - \cdots - 3781753922516174q + O[q]^{2}$$

$$\text{In[26]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41t^{3}F - 4093t^{2}F^{2} - 11^{2} * 251 * tF^{3} - 11^{3} * 5 * F^{4} -}$$
$$\mathbf{11^{2} * 2 * 7 * 103 * t^{3} + 11^{3} * 2^{2} * 3 * 1289 * t^{2}F}$$

$$\text{Out[26]=}\quad \frac{149777430}{q^{13}} + \frac{2678278130}{q^{12}} + \frac{7440556200}{q^{11}} - \cdots - 3884781928756850q + O[q]^{2}$$

$$\text{In[27]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41t^{3}F - 4093t^{2}F^{2} - 11^{2} * 251 * tF^{3} - 11^{3} * 5 * F^{4} -}$$
$$\mathbf{11^{2} * 2 * 7 * 103 * t^{3} + 11^{3} * 2^{2} * 3 * 1289 * t^{2}F - 11^{5} * 2 * 3 * 5 * 31 * tF^{2}}$$

$$\text{Out[27]=}\quad -\frac{17715610}{q^{12}} - \frac{797202450}{q^{11}} - \frac{13641019700}{q^{10}} - \cdots - 3863023611723320q + O[q]^{2}$$

$$\text{In[28]:=}\quad \mathbf{F^{5} - t^{4} - 3 * 41t^{3}F - 4093t^{2}F^{2} - 11^{2} * 251 * tF^{3} - 11^{3} * 5 * F^{4} -}$$
$$\mathbf{11^{2} * 2 * 7 * 103 * t^{3} + 11^{3} * 2^{2} * 3 * 1289t^{2}F - 11^{5} * 2 * 3 * 5 * 31 * tF^{2} +}$$
$$\mathbf{11^{6} * 2 * 5 * F^{3}}$$

$$\text{Out[28]=}\quad \frac{1931001490}{q^{10}} - \frac{9903025990}{q^{9}} + \frac{619514881700}{q^{8}} - \cdots + 6359340881620540q + O[q]^{2}$$

Some remarks are in place. As input for t and f we take their truncated q-series expansions with one more term than needed to decide equality; i.e., up to $O(q^2)$. In order to keep coefficient growth within bounds we work with $F := f/11$ instead of f. Starting with the reduction of F^5 each reduction step works with respect to a uniquely determined power product $t^a F^b$. The last reduction displayed shows a jump from order -12 to order -10. By looking at the monoid $\langle 5, 4, 8, 12, 16\rangle$ this can be explained by the fact that 11 is the largest integer not contained in this monoid[5]. The reduction process stops when the witness identity (7) is fully revealed.

6. Conclusion

The algorithm we applied to derive the witness identity (7) is a powerful tool also in much more general situations when dealing with q-series identities in the context of

[5] Such a number is called Frobenius number. Note that $1, 2, 3, 6$, and 7 are the other integers not contained in the monoid.

modular functions. For example, it plays an essential role in Radu's algorithmic approach to Ramanujan-Kolberg type identities [9]. There, among other things, this algorithm was used to derive a witness identity for $11|p(11n+6)$ of completely different character than (7); namely, where $\sum_{n\geq 0} p(11n+6)q^n$ is expressed as a $\mathbb{Q}$-linear combination of eta-quotients. In order to conclude $11|p(11n+6)$ from this presentation, additional "massage" like "freshman's dream relations" is needed. However, Ralf Hemmecke [6] obtained an identity which presents $\sum_{n\geq 0} p(11n+6)q^n$ as a essentially *integer*-linear combination which in direct fashion shows the divisibility by 11. This was done by generalizing the algorithm for deciding membership in a $\mathbb{Q}$-subalgebra of $\mathbb{Q}[z]$ to an algorithm that decides membership in a $\mathbb{Z}$-subalgebra of $\mathbb{Z}[z]$. Such kind of results indicate additional potential for using variants of this algorithm to obtain suitable identities which witness divisibility.

References

[1] George E. Andrews, Peter Paule, and Axel Riese. MacMahon's Partition Analysis III: The Omega package. *European Journal of Combinatorics*, 22:887–904, 2001.

[2] George E. Andrews, Peter Paule, and Axel Riese. MacMahon's Partition Analysis VI: A New reduction algorithm. *Annals of Combinatorics*, 5:251–270, 2001.

[3] David S. Dummit and Richard M. Foote. *Abstract Algebra, third ed.* John Wiley & Sons, 2005.

[4] David Gale. Subalgebras of an algebra with a single generator are finitely generated. *Proc. Amer. Math. Soc.*, 8:929–930, 1957.

[5] G.H. Hardy, P.V.S. Aiyar, and B.M. Wilson (eds.). *Collected Papers of Srinivasa Ramanujan.* Originally: Cambridge University Press, 1927. Reprint: AMS Chelsea Publishing, 2000.

[6] Ralf Hemmecke. Dancing Samba with Ramanujan Partition Congruences. *preprint*, page 14 pages, 2016.

[7] Deepak Kapur and Klaus Madlener. *A completion procedure for computing a canonical basis for a k-subalgebra*, pages 1–11. Computers and Mathematics (Cambridge, MA, 1989). Springer, 1989.

[8] Peter Paule and Cristian-Silviu Radu. *Partition Analysis, Modular Functions, and Computer Algebra*, pages 511–544. Recent Trends in Combinatorics, The IMA Volumes in Mathematics. Springer, 2016.

[9] Cristian-Silviu Radu. An algorithmic approach to Ramanujan-Kolberg identities. *Journal of Symbolic Computation*, 68:1–33, 2014.

[10] Srinivasa Ramanujan. Some properties of $p(n)$, the number of partitions of n. *Proceedings Cambridge Philosophical Society*, 19:207–210, 1919.

[11] Lorenzo Robbiano and Moss Sweedler. *Subalgebra bases*, pages 61–87. Commutative Algebra (Salvador 1988), Lecture Notes in Math. 1430. Springer, 1990.

[12] Anna Torstensson. Canonical bases for subalgebras on two generators in the univariate polynomial ring. *Beiträge Algebra Geom.*, 43(2):565–577, 2002.

Research Institute for Symbolic Computation (RISC), Johannes Kepler University, A-4040 Linz, Austria

Research Institute for Symbolic Computation (RISC), Johannes Kepler University, A-4040 Linz, Austria