Dancing Samba with Ramanujan Partition Congruences

Ralf Hemmecke*

12-Jun-2016

Abstract

The article presents an algorithm to compute a $C[t]$-module basis G for a given subalgebra A over a polynomial ring $R = C[x]$ with a Euclidean domain C as the domain of coefficients and t a given element of A. The reduction modulo G allows a subalgebra membership test. The algorithm also works for more general rings R, in particular for a ring $R \subset C((q))$ with the property that $f \in R$ is zero if and only if the order of f is positive. As an application, we algorithmically derive an explicit identity (in terms of quotients of Dedekind η-functions and Klein's j-invariant) that shows that $p(11n + 6)$ is divisible by 11 for every natural number n where $p(n)$ denotes the number of partitions of n.

Keywords: partition identities, number theoretic algorithm, subalgebra basis

1 Introduction

Ramanujan [Ram21] discovered that

$$p(5n+4) \equiv 0 \pmod 5 \tag{1}$$
$$p(7n+5) \equiv 0 \pmod 7 \tag{2}$$
$$p(11n+6) \equiv 0 \pmod{11} \tag{3}$$

for all natural numbers $n \in \mathbb{N}$ where $p(n)$ denotes the number of partitions of n. In [Ram19] he lists the following identities from which (1) and (2) can be concluded.

$$\sum_{n=0}^{\infty} p(5n+4)q^n = 5\prod_{k=1}^{\infty}\frac{(1-q^{5k})^5}{(1-q^k)^6} \tag{4}$$
$$\sum_{n=0}^{\infty} p(7n+5)q^n = 7\prod_{k=1}^{\infty}\frac{(1-q^{7k})^3}{(1-q^k)^4} + 49q\prod_{k=1}^{\infty}\frac{(1-q^{7k})^7}{(1-q^k)^8} \tag{5}$$

*hemmecke@risc.jku.at

A similar "simple" identity for (3) is not known, although Lehner [Leh43] gave an identity in terms of ad hoc constructed series A and C.

$$q\prod_{k=1}^{\infty}(1-q^{11k})\sum_{n=0}^{\infty}p(11n+6)q^n = 11(11AC^2-11^2C+2AC-32C-2)$$

Radu [Rad15] developed an algorithmic machinery based on modular functions. He first computed generators $M_1,\dots,M_7$ of the monoid of all quotients of Dedekind η-functions of level 22 that only have poles at infinity. For more details see [Rad15]. In terms of q-series, these generators are as follows.

$$\begin{aligned}
M_1 &= q^{-5}\prod_{k=1}^{\infty}\frac{(1-q^k)^7(1-q^{11k})^3}{(1-q^{2k})^3(1-q^{22k})^7}\\
M_2 &= q^{-5}\prod_{k=1}^{\infty}\frac{(1-q^{2k})^8(1-q^{11k})^4}{(1-q^k)^4(1-q^{22k})^8}\\
M_3 &= q^{-6}\prod_{k=1}^{\infty}\frac{(1-q^{2k})^6(1-q^{11k})^6}{(1-q^k)^2(1-q^{22k})^{10}}\\
M_4 &= q^{-5}\prod_{k=1}^{\infty}\frac{(1-q^{2k})(1-q^{11k})^{11}}{(1-q^k)(1-q^{22k})^{11}}\\
M_5 &= q^{-7}\prod_{k=1}^{\infty}\frac{(1-q^{2k})^4(1-q^{11k})^8}{(1-q^{22k})^{12}}\\
M_6 &= q^{-8}\prod_{k=1}^{\infty}\frac{(1-q^k)^2(1-q^{2k})^2(1-q^{11k})^{10}}{(1-q^{22k})^{14}}\\
M_7 &= q^{-9}\prod_{k=1}^{\infty}\frac{(1-q^k)^4(1-q^{11k})^{12}}{(1-q^{22k})^{16}}
\end{aligned}$$

Note that each of these series lives in $\mathbb{Z}((q))$. By his algorithms AB and MW, Radu then computes a relation

$$\begin{aligned}
F = {} & 11(98t^4+1263t^3+2877t^2+1019t-1997)\\
& +11z_1(17t^3+490t^2+54t-871)+11z_2(t^3+251t^2+488t-614)
\end{aligned} \tag{6}$$

where F is defined as on top of page 30 of [Rad15], i. e.,

$$F = q^{-14}\prod_{k=1}^{\infty}\frac{(1-q^k)^{10}(1-q^{2k})^2(1-q^{11k})^{11}}{(1-q^{22k})^{22}}\sum_{n=0}^{\infty}p(11n+6)q^n \tag{7}$$

and t, z_1, z_2 are given by

$$\begin{aligned} t &= \frac{3}{88}M_1 + \frac{1}{11}M_2 - \frac{1}{8}M_4, \\ z_1 &= -\frac{5}{88}M_1 + \frac{2}{11}M_2 - \frac{1}{8}M_4 - 3, \\ z_2 &= \frac{1}{44}M_1 - \frac{3}{11}M_2 + \frac{5}{4}M_4. \end{aligned}$$

Although equation (6) looks promising, its ingredients t, z_1 and z_2 are series that seem to have 11 in the denominators of their coefficients. Radu then shows by the "freshmen's dream" trick that the series for t, z_1, and z_2 have indeed integer coefficients.

In [PR16], Paule and Radu applied Radu's algorithms with

$$\begin{aligned} t &= q^{-5}\prod_{k=1}^{\infty}\frac{(1-q^k)^{12}}{(1-q^{11k})^{12}} \\ f &= t\,q\prod_{k=1}^{\infty}(1-q^{11k})\sum_{n=0}^{\infty}p(11n+6)q^n \end{aligned}$$

and computed a polynomial relation for the generating series of $p(11n+6)$ that witnesses divisibility by 11 directly.

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

By the algorithm that we present in this article, we can compute relations (4), (5), and additionally a relation

$$\begin{aligned} F = {} & 11^2\cdot 3068\,M_7 + 11^2(3\,M_1 + 4236)\,M_6 + 11(285\,M_1 + 11\cdot 5972)\,M_5 \\ & + \frac{11}{8}\,(M_1^2 + 11\cdot 4497\,M_1 + 11^2\cdot 3156)\,M_4 + 11(1867\,M_1 + 11\cdot 2476)\,M_3 \\ & - \frac{11}{8}(M_1^3 + 1011\,M_1^2 + 11\cdot 6588\,M_1 + 11^2\cdot 10880) \end{aligned} \tag{9}$$

that does not require any additional postprocessing, since all q-series involved in (9) already have integer coefficients and there does not appear a denominator that is divisible by 11. In contrast to (8), identity (9) is linear in the generating series for $p(11n+6)$. Note that (9) does not contain M_2.

Our achievement is based on the article [Rad15] by Radu. Since we actually present a generic algorithm for the computation of a subalgebra basis and the identity for $p(11n+6)$ can be seen as a consequence of the application of our

algorithm to the concrete series given by Radu, we refer for all details concerning the theory of modular functions involved to [Rad15].

After some notations and definitions in Section 2, we start in Section 3 with the presentation of the subalgebra basis algorithm. This algorithm is similar to what has already been given by Radu in [Rad15] or by Paule and Radu in [PR15]. However, there are two essential differences.

First, our algorithm works with coefficients in a Euclidean domain C instead of the field $\mathbb{Q}$ of rational numbers. Although we initially demonstrate everything for bases in the ring $R = C[x]$, we show that the essential conditions posed on R allow us to apply our algorithm also to rings different from $C[x]$, in particular to the subset of Laurent series that is used in [Rad15].

Second, we employ a special kind of reduction that can be seen as living somewhat in the middle between ordinary "rational" reduction (i. e., polynomials are kept monic) and pseudo reduction (i. e., before reduction, the polynomial is multiplied by a certain factor to avoid the introduction of denominators). The main idea of our restricted reduction is that we must avoid division and multiplication by a prefactor. In fact, whenever there were an unwanted division or need for a prefactor (for example, division by 11 for the Ramanujan-like identity), we rather declare the element in question to be irreducible.

We turn Radu's AB algorithm into a critical-pair/completion algorithm that is quite similar to Buchberger's algorithm, cf. [BW93]. However, instead of S-polynomials, the critical pairs in our algorithm are products of polynomials and certain special forms of S-polynomials.

In case $C = \mathbb{Q}$, our restricted reduction is the usual "rational" reduction, so that our algorithm produces essentially the same result as Radu's AB algorithm.

In Section 4, we show that for the application to the $p(11n + 6)$ problem, we can choose the Euclidean domain $\mathbb{Z}_{(11)}$ (the ring of integers localized at the prime 11). With our restricted kind of reduction, it leads to a basis for the subalgebra that is "bigger" than what would be obtained by Radu's algorithm over $\mathbb{Q}$. The kind of basis and this restricted reduction then allows to compute relation (9).

In Section 5, we show another identity for the partition function of $p(11n+6)$ in terms of Klein's j-invariant.

2 Definitions and Notations

Let $\mathbb{N}$ denote the natural numbers (including 0). Let C be a computable Euclidean domain and let $\varphi : C \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ be a Euclidean size function (also known as Euclidean degree or simply Euclidean function) on C. At the moment we assume $R = C[x]$. We shall see later, that everything also works in a more general context. Let $R^* = R \setminus \{0\}$. For $f = \sum_{k=0}^{r} c_k x^k \in C[x]$, we denote by $\mathrm{in}(f) = c_r x^r$, $\mathrm{lc}(f) = c_r$, $\deg(f) = r$ the initial, the leading coefficient and the degree of f. In particular, we define $\mathrm{in}(0) = 0$, $\mathrm{lc}(0) = 0$, $\deg(0) = -\infty$.

Definition 2.1. Let $<_{\mathsf{lex}}$ and $\sqsubseteq$ be two relation on $\mathbb{N}^2$ defined by

$$\begin{aligned}(n_1, n_2) <_{\mathsf{lex}} (n_1', n_2') &\iff n_1 < n_1' \vee (n_1 = n_1' \wedge n_2 < n_2') \\ (n_1, n_2) \sqsubseteq (n_1', n_2') &\iff n_1 \leq n_1' \wedge n_2 \leq n_2',\end{aligned}$$

for $n_1, n_2, n_1', n_2' \in \mathbb{N}$. We denote by $\leq_{\mathsf{lex}}$ the reflexive closure of $<_{\mathsf{lex}}$. Let $\psi : R^* \to \mathbb{N}^2$ be defined by $\psi(f) = (\deg(f), \varphi(\operatorname{lc} f))$. Let $d \in \mathbb{N} \setminus \{0\}$, $n, n' \in \mathbb{Z}$. By $n \equiv_d n'$ we denote that n and n' are *congruent modulo* d, i. e., that there exists $a \in \mathbb{Z}$ such that $n = n' + ad$. Let $u, b \in R^*$. We say that u is *reducible by* b *modulo* d (denoted by $b \trianglelefteq_d u$) if and only if

$$\psi(b) \sqsubseteq \psi(u) \wedge \deg u \equiv_d \deg b.$$

In general, from $b \trianglelefteq_d u$ and $u \trianglelefteq_d b$ follows only $\psi(b) = \psi(u)$, but neither $b = u$ nor $\operatorname{in}(b) = \operatorname{in}(u)$.

Definition 2.2. For $u, t, b \in R^*$, $u' \in R$, the relation $u \to_{t,b} u'$ holds (in words: u *reduces in one step modulo* t *and* b to u') if and only if there exist $c \in C$ and $a \in \mathbb{N}$ such that $u = ct^a b + u'$ and either $u' = 0$ or $\psi(u') <_{\mathsf{lex}} \psi(u)$.

If $B = \{b_1, \ldots, b_r\} \subset R^*$, then $u \to_{t,B} u'$ holds (in words: u *can be reduced in one step modulo* t *and* B to u') if and only if there exists $b \in B$ such that $u \to_{t,b} u'$.

Remark 2.3. Clearly, if $u \to_{t,b} u'$, then $b \trianglelefteq_d u$. Conversely, let us assume $b \trianglelefteq_d u$ where $d = \deg t > 0$. Then $a = \frac{\deg u - \deg b}{d} \in \mathbb{N}$ and $\varphi(\operatorname{lc}(b)) \leq \varphi(\operatorname{lc}(u))$. Furthermore, since C is a Euclidean domain, there exists $c \in C$ such that $\operatorname{lc}(u) = c \operatorname{lc}(b) + r$ with either $r = 0$ or $\varphi(r) < \varphi(\operatorname{lc}(b))$. Thus, if the operations in C are computable, we can compute $(a, c) \in \mathbb{N} \times C$ and $u' = u - ct^a b$ such that either $u' = 0$ or $u' \neq 0$ and $lc(u') = r$, i. e., $\psi(u') <_{\mathsf{lex}} \psi(u)$, in other words, we can compute u' with $u \to_{t,b} u'$.

In general, Euclidean division does not necessarily yield unique c and r with the above properties. Consider, for example, the Gaussian integers $C = \mathbb{Z}[i]$ with $\varphi(a + bi) = a^2 + b^2$. Then $3 = (1 - i) \cdot (1 + i) + 1 = (2 - i) \cdot (1 + i) - i$ are two different Euclidean division steps of 3 by $1 + i$.

In order to make the reduction functional, we assume a computable function red such that $\psi(u - ct^a b) <_{\mathsf{lex}} \psi(u)$ for $(a, c) = \operatorname{red}(u, t, b)$ if $u - ct^a b \neq 0$.

Definition 2.4. For $d \in \mathbb{N} \setminus \{0\}$, a set $B \subseteq R^*$ is called *interreduced modulo* d, if for any $b, b' \in B$, $b \neq b'$ neither $b \trianglelefteq_d b'$ nor $b' \trianglelefteq_d b$ holds.

Remark 2.5. Suppose that the set $B \subseteq R^*$ is interreduced modulo d. If C is a field, then $\varphi(c) = 1$ for any $c \in C \setminus \{0\}$. It follows that for any $u \in R^*$ there is at most one $b \in B$ such that $b \trianglelefteq_d u$.

In general, however, for $u \in R^*$ it is still possible that there exist $b, b' \in B$, with $b \neq b'$, $b \trianglelefteq_d u$, and $b' \trianglelefteq_d u$. For example, consider $C = \mathbb{Z}$, $\varphi(z) = |z|$. If $b, b' \in B$, $b \neq b'$ with $\deg b = d + \deg b'$, $\varphi(\operatorname{lc} b) < \varphi(\operatorname{lc} b')$, and $u \in R^*$ is such that $\deg u = \deg b$ and $\varphi(\operatorname{lc} u) = \varphi(\operatorname{lc} b')$. To be more concrete, consider $t = x^2$, i. e., $d = 2$ and $u = 3x^5$, $b = 3x^3$, $b' = 2x^5$. Then $u = tb + 0 = b' + x^5$.

To remove such ambiguity as described in Remark 2.5, we introduce a reduction relation where among possible multiple choices, the element is preferred that has maximal degree in x.

Definition 2.6. Let $t, u \in R^*$, $d = \deg t > 0$, $B \subset R^*$ be interreduced modulo d, and let there exist $b \in B$ with $b \trianglelefteq_d u$. We denote by $\mathrm{select}_{t,B}(u)$ the element $b \in B$ such that $\deg b = \max\{\deg b' \mid b' \in B \wedge b' \trianglelefteq_d u\}$.

We say that the relation $u \mapsto_{t,B} u'$ holds if and only if $u \to_{t,b} u'$ and $u' = u - ct^a b$ for $b = \mathrm{select}_{t,B}(u)$ and $(a, c) = \mathrm{red}(u, t, b)$. By $\mapsto^*_{t,B}$ we denote the reflexive and transitive closure of $\mapsto_{t,B}$. By $\mathrm{reduce}_{t,B}(u)$, we denote the $u' \in R$ such that $u \mapsto^*_{t,B} u'$ and there does not exist $b \in B$ with $b \trianglelefteq_d u'$. If $u' = \mathrm{reduce}_{t,B}(u)$, we say u *reduces modulo* t *and* B to u'.

Remark 2.7. Under the assumption that B is finite, $b \trianglelefteq_d u$ is decidable algorithmically and the function red from Remark 2.3 is computable, also $\mathrm{select}_{t,B}$ and $\mathrm{reduce}_{t,B}$ are computable.

Remark 2.8. By keeping track of the individual reduction steps, it is clear that if $u' = \mathrm{reduce}_{t,B}(u)$, then for every $b \in B$ there exists $p_b \in C[x]$ such that

$$u = u' + \sum_{b \in B} p_b(t) b \tag{10}$$

and $\psi(u) = \max_{<_{\mathsf{lex}}}(\{\psi(u')\} \cup \{\psi(p_b(t)b) \mid b \in B, p_b \neq 0\})$. In particular, we want to emphasize that there is no summand s on the right-hand side of (10) with $\psi(u) <_{\mathsf{lex}} \psi(s)$.

3 The SubAlgebra Module Basis Algorithm: samba

In this section we present an algorithm that computes a $C[t]$-module basis for a subalgebra of $C[x]$ and prove its termination and correctness. The algorithm samba is presented in a form that allows for relatively simple proofs.

Input: $t, f_1, \ldots, f_r \in R^*$, $\deg t > 0$, $\mathrm{lc}\, t = 1$.
Output: $B = \{g_0, g_1, \ldots, g_s\} \subset A = C[t, f_1, \ldots, f_r]$ such that for $f \in R$ holds $\mathrm{reduce}_{t,B}(f) = 0$ iff $f \in A$.

```
1  B := {1}
2  B_crit := {f_1, ..., f_r}
3  d := deg t
4  P := ∅
5  S := ∅
6  while B_crit ∪ P ∪ S ≠ ∅ do
7        u := "take one element from B_crit ∪ P ∪ S and remove it from B_crit, P, and S"
8        u' := reduce_{t,B}(u)
9        if u' ≠ 0 then
10             B_crit := B_crit ∪ {b ∈ B | u' ⊴_d b}
11             B := (B \ B_crit) ∪ {u'}
12             P := {b1 b2 | b1, b2 ∈ B \ {1}}
13             S := {t^a b | ∀a ∈ ℕ, b ∈ B ∃b' ∈ B : deg(t^a b) = deg(b')}
14 return B
```

Theorem 3.1. *Algorithm* samba *terminates.*

Proof. Let $U = (u_i)_{i\in I} \subset R^*$ with $I \subseteq \mathbb{N} \setminus \{0\}$ be the sequence of elements that are added to the set B in line 11 such that u_i is added earlier than u_j if $i < j$. Note that then $\neg(u_i \trianglelefteq_d u_j)$, i. e., "later" elements are not reducible by "earlier" elements. For each k, $0 \le k < d = \deg t$ a subsequence of U is defined by $U^{[k]} = (u_i)_{i\in I^{[k]}}$, $I^{[k]} \subseteq I$ consisting only of those elements u of U for which $\deg u \equiv_d k$ and $\neg(u_i \trianglelefteq_d u_j)$ if $i < j$. $U^{[k]}$ corresponds to a sequence $(\psi(u_i))_{i\in I^{[k]}}$ in $\mathbb{N}^2$ with $\neg(\psi(u_i) \sqsubseteq \psi(u_j))$, which must be finite by Dickson's Lemma, [BW93, p. 163]. Taking the union of all those finite sets $I^{[k]}$, we conclude that there is an index m such that $I \subseteq \{1, \dots, m\}$. In other words, all the finitely many elements from $B_{\text{crit}} \cup P \cup S$ reduce to zero in line 8 after the m-th iteration of the while loop. Thus the algorithm terminates.

Note that when elements are removed from B in line 11, these elements are "reducible". More precisely, if u_i is removed from B then there is some $u_j \in B$ with $i < j$ and $u_j \trianglelefteq_d u_i$. Since the relation $\trianglelefteq_d$ is transitive, we can still conclude by Dickson's Lemma the finiteness of the sequence U (with all the "reducible" elements removed). □

Note that we do not simply require that $f \in A$ can be expressed as a $C[t]$-linear combination of elements of B, but rather our algorithm yields a basis by which every element of A can be reduced to zero in the sense of our "restriced" reduction. This is a slightly stronger condition. In fact, without the treatment of the set S in the algorithm, $\text{reduce}_{t,B}(f) = 0$ can not be concluded for every $f \in A$.

As a counterexample choose the Euclidean domain $C = \mathbb{Z}_{(3)}$, i. e., rational numbers with no denominator divisible by 3. Each $c \in C \setminus \{0\}$ can be written as $3^n \frac{a}{b}$ with $\gcd(3, a) = \gcd(3, b) = 1$, $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. The Euclidean size function φ is defined by $\varphi(3^n \frac{a}{b}) = n$. Then take $t = x^2$, $f_1 = 3^2x^3$, $f_2 = 3x^7 - x^3$ and apply the above algorithm without considering the set S. Neither $f_1 \trianglelefteq_2 f_2$ nor $f_2 \trianglelefteq_2 f_1$ holds. Thus there are only the products f_1^2, f_1f_2, and f_2^2 to consider. All of those products have only even powers of x and thus reduce to 0 modulo t. So we get $\{1, f_1, f_2\}$ as the final basis although, $x^3 = t^4f_1 - (3t^2 + 1)f_2$ and x^3 cannot be reduced modulo t and $\{1, f_1, f_2\}$. Therefore, the treatment of S is essential.

We have split the proof of the correctness of algorithm samba into two Theorems. While Theorem 3.2 even holds if the set S is not considered in the algorithm, the treatment of S is essential for Theorem 3.4.

Theorem 3.2. *Let $t, f_1, \dots, f_r \in R^*$, $d = \deg t > 0$, and $A = C[t, f_1, \dots, f_r] \subseteq R$ with $\operatorname{lc} t = 1$. Let $G = \{g_0, \dots, g_s\}$ be the output of Algorithm* samba *applied to $t, f_1, \dots, f_r$. Then for every $f \in A$ there exist $p_0, \dots, p_s \in C[x]$ such that*

$$f = \sum_{i=0}^{s} p_i(t)g_i, \tag{11}$$

i. e., $A = \langle g_0, \dots, g_s\rangle_{C[t]}$ as $C[t]$-modules.

Proof. Let $G = \{g_0, \ldots, g_s\}$ be the set B at the end of the algorithm. Note that $1 \in G$. It is clear that $A = C[t][G]$, because at the beginning of the while loop, it holds $A = C[t][B \cup B_{\text{crit}}]$ and this equation is an invariant of the while loop. For any u that is removed from B_{crit}, there is a $u' = \text{reduce}_{t,B}(u)$ (line 8) and thus a representation in terms of the respective B at that time in the algorithm, i. e.,

$$u = u' + \sum_{b \in B} p_b^{(u)}(t) b$$

for some polynomials $p_b^{(u)} \in C[x]$. Then either $u' = 0$, or $u' \in A$ and u' is added to B in line 11.

By keeping track of the reductions that happen during the algorithm, it follows that for every f_j there exists a representation

$$f_j = \sum_{i=0}^{s} p_i^{(j)}(t) g_i. \tag{12}$$

Since $\text{reduce}_{t,G}(g_j g_k) = 0$ for every pair $0 \leq j, k \leq s$, there is a representation

$$g_j g_k = \sum_{i=0}^{s} p_i^{(j,k)}(t) g_i. \tag{13}$$

By combining (12) and (13), we conclude that for every pair $1 \leq j, k \leq r$ there is a representation

$$f_j f_k = \sum_{i=0}^{s} \bar{p}_i^{(j,k)}(t) g_i.$$

By induction, and by $C[t]$-linearity of A, we can conclude that for every $f \in A$ there exists a representation (11). □

Remark 3.3. In general such a representation (11) is not unique, because there might be $i_1, i_2 \in \{0, \ldots, s\}$ with $i_1 < i_2$, $\text{lc}(g_{i_2}) = 1$, $\varphi(\text{lc}(g_{i_1})) > \varphi(\text{lc}(g_{i_2}))$, $tg_{i_1} = \text{lc}(g_{i_1}) g_{i_2}$, $p_{i_1} = x$, $p_{i_2} = \text{lc}(g_{i_1})$, and $\deg f < \deg(tg_{i_1}) = \deg(\text{lc}(g_{i_1}) g_{i_2})$. In other words, (11) does not correspond to a reduction sequence with respect to $\mapsto_{t,G}$. More concretely, consider $C = \mathbb{Z}$ with the absolute value as the Euclidean size function. Let $t = x^2$, $g_0 = 1$, $g_1 = 5x^3$, $g_2 = x^5$. Then $f = x^4 = t^2 g_0 = t^2 g_0 + t g_1 + (-5) g_2$ are two representations for f of the form (11).

For $f \in R$ it is obvious that from $\text{reduce}_{t,B}(f) = 0$ follows $f \in A$. Thus we only need to prove the following theorem in order to show correctness of algorithm samba.

Theorem 3.4. *Let $t, f_1, \ldots, f_r \in R^*$, $d = \deg t > 0$, and $A = C[t, f_1, \ldots, f_r] \subseteq R$ with $\text{lc}\, t = 1$. Let $G = \{g_0, \ldots, g_s\}$ be the output of Algorithm* samba *applied to $t, f_1, \ldots, f_r$. Then $\text{reduce}_{t,G}(f) = 0$ for every $f \in A$, i. e., representation (11) can be found algorithmically.*

Proof. In order to show that $\mathrm{reduce}_{t,G}(f) = 0$ holds for every $f \in A$, it is sufficient to show that every $f \in A \setminus \{0\}$ is reducible, i. e., that there exists $g \in G$ such that $g \trianglelefteq_d f$.

From the algorithm it is clear that all elements of G have different degree. Namely, if an element u' is added to B in line 11 of the algorithm, then all the elements of degree equal to $\deg(u')$ will be removed from B. Without loss of generality, we can assume that $\deg(g_i) < \deg(g_j)$ for $i < j$.

Let $f \in A \setminus \{0\}$. From Theorem 3.2 follows that there is a representation (11). Among all such representations (11) for f, we choose one such that

$$m = \max\{\deg(p_i(t)g_i) \mid i \in \{0, \dots s\}, p_i(x) \neq 0\}$$

is minimal and for the set

$$I = \{i \in \{0, \dots s\} \mid p_i(x) \neq 0, \deg(p_i(t)g_i) = m\} \tag{14}$$

the value of $\iota = \min I$ is maximal and the value of $\psi(p_\iota)$ is $<_{\mathsf{lex}}$-minimal. Note that $\deg f \leq m$.

The set I contains exactly one element, because otherwise we can construct another representation that contradicts the minimality/maximality properties in the choice of the original representation.

Assume for a contradiction that I contains a second element k. Then $\iota < k$ and $\deg(g_\iota) \equiv_d \deg(g_k)$. Let

$$j = \min\{i \in \mathbb{N} \mid \iota < i \leq k, \deg(g_\iota) \equiv_d \deg(g_i)\}.$$

Let $e = \deg(p_\iota)$, $c = \mathrm{lc}(p_\iota)$. Note that $e > 0$, because $\deg g_\iota < \deg g_j$. Furthermore, according to line 13 of algorithm samba, there exists $a \in \mathbb{N}$ such that $\deg(t^a g_\iota) = \deg(g_j)$ and $t^a g_\iota$ has been added to S and eventually reduced to zero. This reduction starts by using g_j, i. e., $\mathrm{select}_{t,G}(t^a g_\iota) = g_j$, $(1, c') = \mathrm{red}(u, t, g_j)$, and $u = t^a g_\iota - c' g_j$. Either $u = 0$ or $u \neq 0$ and $\psi(u) <_{\mathsf{lex}} \psi(t^a g_\iota)$. Thus, this reduction gives rise to a representation

$$t^a g_\iota = c' g_j + u = c' g_j + \sum_{i=0}^{s} \hat{p}_i(t) g_i \tag{15}$$

where $\psi(\hat{p}_i(t)g_i) \leq_{\mathsf{lex}} \psi(u)$ for every i with $\hat{p}_i \neq 0$, because the $\hat{p}_i$ come from an application of $\mathrm{reduce}_{t,G}$ to u.

Note that if $u \neq 0$, it does not necessarily hold $\deg(u) < \deg(t^a g_\iota)$. All we need here is that $\psi(u) <_{\mathsf{lex}} \psi(t^a g_\iota)$. Furthermore, since $\mathrm{select}_{t,G}$ always selects elements with highest possible degree, there is no $i < \iota$ such that $\hat{p}_i \neq 0$ and $\deg(\hat{p}_i(t)g_i) = \deg(t^a g_\iota)$.

We have $a \leq e$ by the minimal choice of j. Thus, in the representation (11) for f, we can use (15) to replace $ct^e g_\iota$, leading to a new representation

$$f = \sum_{i=0}^{s} p'_i(t) g_i \tag{16}$$

where either $\max\{\deg(p'_i(t)g_i) \mid i \in \{0,\dots s\}, p'_i(x) \neq 0\} < m$ or $p'_\iota = 0$ or $\psi(p'_\iota) <_{\mathsf{lex}} \psi(p_\iota)$. Therefore, either m could not have been minimal or ι could not have been maximal or $\psi(p_\iota)$ could not have been $<_{\mathsf{lex}}$-minimal in contrast to our choice of the representation.

We conclude that $I = \{\iota\}$ and, thus, $\mathrm{in}(p_\iota(t)g_\iota) = \mathrm{in}(f)$, i. e., $m = \deg f$ and $g\iota \trianglelefteq_d f$. □

Remark 3.5. From the above proof it follows that the set S that is computed in line 13 of algorithm samba need only contain $t^a b$ where a is minimal with the respective property.

In case C is a field, the set S need not be computed at all, because then there exists no pair $b, b' \in B$ with $b \neq b'$ and $\deg(b) \equiv_d \deg(b')$ and thus the corresponding set I (see (14)) can only contain one element.

4 Generalized Application of samba

Up to now samba applies to the ring $R = C[x]$. Of course, all operations that are performed by samba must be computable, in particular all ring operations of R and also taking the degree of an element of R or computing the Euclidean size of a coefficient from C.

The ring R can be generalized to a situation that fits into the context of Radu's article [Rad15]. In fact, Radu considers Laurent series in q with the property that an element is zero if and only if its order in q is greater than 0.

The ring R does not really matter. Looking at the operations performed by the algorithm samba, it is sufficient if the operations in the C-algebra $A = C[t, f_1, \dots, f_r]$ (i. e., in the algebra generated by the input elements) are computable, since the algorithm never deals with an element from $R \setminus A$. In particular, it is not necessary that we require a computable zero test for every element of R, it is sufficient that the zero test in A is computable.

For the application to Ramanujan's partition congruence modulo 11, it is sufficient to consider input series from $C((q))$. For $f = \sum_{k=r}^{\infty} c_k q^k \in C((q))$, we denote by $\mathrm{in}(f) = c_r q^r$, $\mathrm{lc}(f) = c_r$, $\deg(f) = -r$ the initial, the leading coefficient and the degree of f. In particular, we define $\mathrm{in}(0) = 0$, $\mathrm{lc}(0) = 0$, $\deg(0) = -\infty$. Note that in order to keep things similar to what we have done above for $C[x]$, we define the degree of a Laurent series as the negative value of what is commonly known as its order.

If we assume that the input to algorithm samba is such that for every element $f \in A$ it holds

$$f = 0 \iff \deg(f) < 0, \tag{17}$$

then the zero test in A is computable. When computing with elements of $A \subset C((q))$, we can postpone any "infinite" ring operation until a test for zero occurs in the algorithm. For this test only a finite number of coefficients must be computed.

In fact, Laurent series can be represented in a finitary way on a computer by storing the first few coefficients and a function that computes the "next"

coefficient if it is needed, i. e., the ring operations can be computed in a lazy fashion in finitely many steps.

The algorithm samba can effectively be applied to a subalgebra of Laurent series $C((q))$ with the property (17) where C is a computable Euclidean domain. The (input) series used by Radu generate such a subalgebra of $C((q))$.

In order to compute the relation (9), we choose $C = \mathbb{Z}_{(11)}$, i. e., the rational numbers with no denominator divisible by 11 with the Euclidean size function defined by $\varphi(c) = n$ for $c = 11^n \frac{a}{b} \in \mathbb{Z}_{(11)}$ and $\gcd(a, 11) = \gcd(b, 11) = 1$.

Starting samba with $t = M_1$ and $f_i = M_i$ for $i \in \{1, 2, \ldots, 7\}$ gives the basis $G = \{g_0, g_1, \ldots, g_5\}$ where

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= \frac{8M_7 - 40M_6 + 168M_5 + (2343 - M_1)M_4 - 680M_3 + M_1^2 + 505M_1}{1024} \\
&= 11\,q^{-3} + 11\,q^{-1} - \frac{11^2}{32} + O\left(q\right), \\
g_2 &= \frac{M_4 - M_1}{8} = q^{-4} - 2\,q^{-3} + 2\,q^{-2} + 3 + O(q), \\
g_3 &= M_3 = q^{-6} + 2\,q^{-5} - q^{-4} - 2\,q^{-3} - q^{-2} - 6\,q^{-1} + O\left(q\right), \\
g_4 &= M_5 = q^{-7} - 4\,q^{-5} + 2\,q^{-3} + 8\,q^{-1} + O\left(q\right) \\
g_5 &= M_6 = q^{-8} - 2\,q^{-7} - 3\,q^{-6} + 6\,q^{-5} + 2\,q^{-4} - q^{-2} - 10\,q^{-1} + O\left(q^3\right)
\end{aligned}
$$

Computing $\text{reduce}_{t,G}(F)$ with the F given by (7) returns 0 where (by collecting the cofactors of that reduction) relation (9) is obtained. See Section 1 for the definition of the M_i.

5 Ramanujan's Partition Congruence in Terms of Klein's j-invariant

Historically, we first implemented Radu's original algorithms in FriCAS [fri] with $\mathbb{Q}$ as the coefficient domain. Peter Paule then asked whether Ramanujan's partition congruence modulo 11 can be witnessed by an identity involving Klein's j-invariant.

Klein's j-invariant (also called modular invariant or absolute invariant) is a modular function of weight zero for $SL_2(\mathbb{Z})$. In the theory of modular functions, the j-invariant is interesting because every modular function can be expressed as a rational function in j. For a definition see, for example, Chapter VII of [Ser73]. It follows from there that in terms of q-series ($q = \exp(2\pi i\tau)$), the j-invariant is given by

$$j(\tau) = 1728\frac{g_2^3}{\Delta}$$

where

$$\Delta = g_2^3 - 27g_3^2 = (2\pi)^{12} q \prod_{k=1}^{\infty} (1-q^k)^{24}$$
$$g_2 = \frac{(2\pi)^4}{12}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)$$
$$g_3 = \frac{(2\pi)^6}{216}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right)$$

and $\sigma_k(n) = \sum_{d|n} d^k$ is the sum of k-th powers of positive divisors of n. From the definition it is obvious that the q-series for j has integer coefficients.

$$\begin{aligned} j(\tau) = q^{-1} &+ 744 + 196884\,q + 21493760\,q^2 + 864299970\,q^3 + 20245856256\,q^4 \\ &+ 333202640600\,q^5 + 4252023300096\,q^6 + 44656994071935\,q^7 \\ &+ 401490886656000\,q^8 + 3176440229784420\,q^9 + O(q^{10}). \end{aligned}$$

Application of algorithm AB (or algorithm samba with $C = \mathbb{Q}$) to

$$\begin{aligned} t &= q^{-5}\prod_{k=1}^{\infty}\frac{(1-q^k)^{12}}{(1-q^{11k})^{12}} \\ &= q^{-5} - 12\,q^{-4} + 54\,q^{-3} - 88\,q^{-2} - 99\,q^{-1} + 540 + O(q), \end{aligned}$$

$t^3 \cdot j(\tau)$, and $t \cdot j_p$ where $j_p = j(11\tau)$ results in a $\mathbb{Q}[t]$-module basis with 5 elements.[1] By keeping track of the cofactors during that computation, each basis element can be expressed as a polynomial in t, j, and j_p with rational coefficients. For

$$F = q\prod_{k=1}^{\infty}(1-q^{11k})\sum_{n=0}^{\infty}p(11n+6)q^n$$

the element t^3F reduces modulo the above basis to 0, i. e., $t^3F \in \mathbb{Q}[t, t^3j, tj_p]$. However, that reduction only gives rise to a representation of t^3F as a polynomial in t, j, and j_p with coefficients having a denominator divisible by 11^{40}. In other words, Radu's algorithm cannot be used in its original form to derive a witness for Ramanujan's partition congruence modulo 11. Also modifying Radu's algorithm to work over $\mathbb{Z}$ instead of $\mathbb{Q}$ by using pseudo-reduction did not help. It resulted in an annoying prefactor for t^3F of 11^{40}. The problem of such a high power of 11 then led to develop the algorithm samba. The crucial idea to overcome the problem was to trade division by 11 against growing the size of the resulting basis.

The algorithm samba can be called with input t, t^3j, and tj_p and coefficients living in $\mathbb{Z}_{(11)}$. Instead of 5 elements, it yields a basis of $G = \{g_0 = 1, g_1, \ldots, g_{12}\}$ where the ψ-values (cf. Def. 2.1) of the 12 non-constant elements are

$$(7,18), (8,8), (9,4), (11,3), (12,3), (13,3), (14,0), (16,0), (17,2), (18,1), (22,0), (23,0).$$

[1] Note that t, $t^3 \cdot j(\tau)$, and $t \cdot j_p$ can be proven to have poles only at infinity. Let A be the algebra generated by the respective q-series. Then for every $f \in A$ property (17) holds. Thus, these series can be used as input in algorithm samba.

Note that the basis elements of degree 14, 16, 22, and 23 have no factor of 11 in their leading coefficient.

We have $0 = \mathrm{reduce}_{t,G}(t^7 F)$ which gives a representation

$$t^7 F = t^7 q \prod_{k=1}^{\infty} (1 - q^{11k}) \sum_{n=0}^{\infty} p(11n+6) q^n = 11\, t^2 h(t, j, j_p). \tag{18}$$

The expression $h(t, j, j_p)$ is a $Z_{(11)}$-linear combination of powerproducts $t^u j^v j_p^w$ i. e., with coefficients of the form $\frac{a}{b}$ such that $\gcd(b, 11) = 1$, where each a and b has about 2400 decimal digits and the 161 exponent triples (u, v, w) are given by the following list. Note that $u \leq 16$, $v \leq 4$, $w \leq 4$.

$(0,0,0), (0,0,1), (0,0,2), (1,0,0), (1,0,1), (1,0,2), (1,0,3), (2,0,0), (2,0,1), (2,0,2),$
$(2,0,3), (2,0,4), (2,1,0), (2,1,1), (3,0,0), (3,0,1), (3,0,2), (3,0,3), (3,0,4), (3,1,0),$
$(3,1,1), (3,1,2), (4,0,0), (4,0,1), (4,0,2), (4,0,3), (4,0,4), (4,1,0), (4,1,1), (4,1,2),$
$(4,1,3), (4,2,0), (5,0,0), (5,0,1), (5,0,2), (5,0,3), (5,0,4), (5,1,0), (5,1,1), (5,1,2),$
$(5,1,3), (5,2,0), (5,2,1), (6,0,0), (6,0,1), (6,0,2), (6,0,3), (6,0,4), (6,1,0), (6,1,1),$
$(6,1,2), (6,1,3), (6,2,0), (6,2,1), (6,2,2), (7,0,0), (7,0,1), (7,0,2), (7,0,3), (7,0,4),$
$(7,1,0), (7,1,1), (7,1,2), (7,1,3), (7,2,0), (7,2,1), (7,2,2), (7,3,0), (8,0,0), (8,0,1),$
$(8,0,2), (8,0,3), (8,0,4), (8,1,0), (8,1,1), (8,1,2), (8,1,3), (8,2,0), (8,2,1), (8,2,2),$
$(8,3,0), (8,3,1), (9,0,0), (9,0,1), (9,0,2), (9,0,3), (9,1,0), (9,1,1), (9,1,2), (9,1,3),$
$(9,2,0), (9,2,1), (9,2,2), (9,3,0), (9,3,1), (10,0,0), (10,0,1), (10,0,2), (10,0,3),$
$(10,1,0), (10,1,1), (10,1,2), (10,1,3), (10,2,0), (10,2,1), (10,2,2), (10,3,0), (10,3,1),$
$(10,4,0), (11,0,0), (11,0,1), (11,0,2), (11,1,0), (11,1,1), (11,1,2), (11,2,0), (11,2,1),$
$(11,2,2), (11,3,0), (11,3,1), (11,4,0), (12,0,0), (12,0,1), (12,0,2), (12,1,0), (12,1,1),$
$(12,1,2), (12,2,0), (12,2,1), (12,2,2), (12,3,0), (12,3,1), (12,4,0), (13,0,0), (13,0,1),$
$(13,1,0), (13,1,1), (13,2,0), (13,2,1), (13,3,0), (13,3,1), (13,4,0), (14,0,0), (14,0,1),$
$(14,1,0), (14,1,1), (14,2,0), (14,2,1), (14,3,0), (14,3,1), (14,4,0), (15,0,0), (15,1,0),$
$(15,2,0), (15,3,0), (15,4,0), (16,0,0), (16,1,0), (16,2,0), (16,3,0), (16,4,0)$

6 Conclusion

In this article we have presented the algorithm samba that, for some set of polynomials $\{t, f_1, \ldots, f_r\} \subset C[x]$ computes a $C[t]$-module basis G for $A = C[t, f_1, \ldots, f_r]$ by which then it can be algorithmically tested whether a given polynomial $f \in C[x]$ belongs to A.

In a generalized context, this algorithm has then successfully been applied to find an identity witnessing Ramanujan's partition congruence $p(11n + 6) \equiv 0 \pmod{11}$ for every $n \in \mathbb{N}$.

7 Acknowledgement

We would like to thank Peter Paule who made us aware of the problem of finding an identity for the partition function of $p(11n + 6)$ in terms of Klein's modular j-invariant that would witness divisibility by 11. Special thanks go to Silviu Radu who helped with the theory of modular functions and also with getting the details right while implementing his algorithms. Due to its mathematical type hierarchy, the computer algebra system FriCAS allowed us to easily implement samba and to experiment with different coefficient domains (and equally apply it in $C[x]$ and subalgebras of Laurent series with the property (17)) without changing any line in the underlying algorithm. Thanks to all the designers and developers of that system.

References

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[fri] FriCAS—an advanced computer algebra system. Available at `http://fricas.sf.net`.

[Leh43] Joseph Lehner. Ramanujan identities involving the partition function for the moduli 11^a. *American Journal of Mathematics*, 65(3):492–520, 1943.

[PR15] Peter Paule and Silviu Radu. Partition analysis, modular functions, and computer algebra. In Andrew Beveridge, Jerrold R. Griggs, Leslie Hogben, Gregg Musiker, and Prasad Tetali, editors, *Recent Trends in Combinatorics*, The IMA Volumes in Mathematics and its Applications, pages 511–544. Springer-Verlag, 2015.

[PR16] Peter Paule and Silviu Radu. A new witness identity for $11|p(11n + 6)$. Available at `http://www.risc.jku.at/publications/download/risc_5329/a60_submission.pdf`, 2016.

[Rad15] Cristian-Silviu Radu. An algorithmic approach to Ramanujan-Kolberg identities. *Journal of Symbolic Computation*, 68, Part 1:225–253, 2015.

[Ram19] S. Ramanujan. Some properties of $p(n)$, the number of partitions of n. In *Proceedings of the Cambridge Philosophical Society*, volume 19, pages 207–210, 1919.

[Ram21] S. Ramanujan. Congruence properties of partitions. *Mathematische Zeitschrift*, 9(1-2):147–153, 1921.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer-Verlag, New York, 1973.