COMPUTING AN ORDER COMPLETE BASIS FOR $M^\infty(N)$ AND APPLICATIONS

MARK VAN HOEIJ† AND CRISTIAN-SILVIU RADU†

Abstract. This paper gives a quick way to construct all modular functions for the group $\Gamma_0(N)$ having only a pole at $\tau = i\infty$. We assume that we are given two modular functions f, g for $\Gamma_0(N)$ with poles only at $i\infty$ and coprime pole orders. As an application we obtain two new identities from which one can derive that $p(11n+6) \equiv 0 \pmod{11}$, here $p(n)$ is the usual partition function.

1. Description of the Problem

For basic notions about modular functions used in this paper we refer to [14]. In this paper we show how to obtain an order complete basis for $M^\infty(N)$ with an application to the case $N = 11$. We use this basis to obtain two new Ramanujan type identities for $\sum_{n=0}^{\infty} p(11n+6)q^n$. Such bases have also been constructed by other authors [1, 2, 4, 7, 8, 9, 11, 12] by using various tricks to produce sufficiently many new modular functions $f_1, f_2, \ldots \in M^\infty(N)$ until $\mathbb{C}[f_1, f_2, \ldots]$ becomes equal to $M^\infty(N)$. The advantage of our approach is that we need only two functions in $t, f \in M^\infty(N)$. Then $\mathbb{C}[t, f]$ will generally be a proper subset of $M^\infty(N)$, but instead of searching for more modular functions, we fill this gap with a *normalized integral basis*.

Let t and f be modular functions for the group $\Gamma_0(N)$ with poles only at $\tau = i\infty$, in other words, let $t, f \in M^\infty(N)$. Suppose that the pole orders are n and m respectively, and that $\gcd(n, m) = 1$, such functions always exist [13, Example 2.3]. Then there exists an irreducible polynomial $p = p(x, y) \in \mathbb{C}[x, y]$ with $p(t, f) = 0$, $\deg_x(p) = m$, and $\deg_y(p) = n$ by [21, Lemma 1]. One can compute p from the q-expansions of t and f by making an Ansatz for the unknown coefficients of p and solving a system of equations where each equation is a coefficient in the q-expansion of $p(t, f)$. We use p to compute in the function field $\mathbb{C}(t, f) \cong \mathbb{C}(x)[y]/(p)$.

The function field $\mathbb{C}(t, f)$ contains $M^\infty(N)$ see [13, Prop 4.3], here $M^\infty(N)$ is the set of all modular functions for the group $\Gamma_0(N)$ with a pole only at $i\infty$. Obtaining all modular functions for the group $\Gamma_0(N)$ having a pole only at $i\infty$ is equivalent to finding all modular functions $h \in \mathbb{C}(t, f)$ that are *integral* over $\mathbb{C}[t]$ (which means there is a *monic* polynomial $g(X) \in \mathbb{C}[t][X]$ for which $g(h) = 0$). Thus, one starts by computing an *integral basis*, which is a basis $b_1, \ldots, b_n \in \mathbb{C}(t, f)$ of the $\mathbb{C}[t]$-module of all $h \in \mathbb{C}(t, f)$ that are integral over $\mathbb{C}[t]$. There are several algorithms to compute an integral basis [5, 20] and implementations in several computer algebra systems. Then every h that is integral over $\mathbb{C}[t]$ can be written as $h = p_1(t)b_1 + \cdots + p_n(t)b_n$ for some polynomials $p_1, \ldots, p_n$. Given the q-expansions of h and $b_1, \ldots, b_n$ the algorithm described in [16, Alg. MW] can find $p_1, \ldots, p_n$ provided that $\mathrm{ord}_{i\infty}(b_1) < \mathrm{ord}_{i\infty}(b_2) < \cdots < \mathrm{ord}_{i\infty}(b_n)$. We call such an integral basis *order complete.*

† Supported by NSF 1618657.
† Supported by grant SFB F50-06 of the Austrian Science Fund (FWF)..

After computing an integral basis, we can find an order complete basis by using *normalization at infinity* from Trager's PhD thesis [19, Chapter 2, Section 3], see Section 1.2 for details.

1.1. Notations.

$K = \mathbb{C}(x)[y]/(p)$ where $p \in \mathbb{C}[x, y]$ is irreducible.
O_K is ring of all elements of K that are integral over $\mathbb{C}[x]$.
R_∞ is the ring of all $h \in \mathbb{C}(x)$ that have no pole at $x = \infty$.
O_∞ is ring of all elements of K that are integral over R_∞.

To compute a basis of O_∞ as R_∞-module, first substitute $x \mapsto 1/\tilde{x}$, then compute a *local integral basis* at $\tilde{x} = 0$ (most integral basis implementations allow the option of computing a local integral basis). After that, replace $\tilde{x}$ by $1/x$.

1.2. Normalize an integral basis at infinity.

The process of normalizing an integral basis at infinity was introduced in [19] in order to compute a Riemann-Roch space that was needed for integrating algebraic functions. For completeness we will describe this process:

Algorithm: Normalize an integral basis at infinity.

(1) Let $b_1, \ldots, b_n$ be a basis of O_K as $\mathbb{C}[x]$-module.
(2) Let $b'_1, \ldots, b'_n$ be a basis of O_∞ as R_∞-module.
(3) Write $b_i = \sum_{j=1}^{n} r_{ij} b'_i$ with $r_{ij} \in \mathbb{C}(x)$.
(4) Let $D \in \mathbb{C}[x]$ be a non-zero polynomial for which $a_{ij} := Dr_{ij} \in \mathbb{C}[x]$ for all i, j. Now $Db_i = \sum_{j=1}^{n} a_{ij} b'_i$.
(5) For each $i \in \{1, \ldots, n\}$, let m_i be the maximum of the degrees of $a_{i1}, \ldots, a_{in}$. Now let $V_i \in \mathbb{C}^n$ be the vector whose j'th entry is the x^{m_i}-coefficient of a_{ij}. Let $d_i := m_i - \deg_x(D)$.
(6) If $V_1, \ldots, V_n$ are linearly independent, then return $b_1, \ldots, b_n$ and $d_1, \ldots, d_n$ and stop.
Otherwise, take $c_1, \ldots, c_n \in \mathbb{C}$, not all 0, for which $c_1V_1 + \cdots c_nV_n = 0$.
(7) Among those $i \in \{1, \ldots, n\}$ for which $c_i \neq 0$, choose one for which d_i is maximal. For this i, do the following
  (a) Replace b_i by $\sum_{k=1}^{n} c_k x^{d_i - d_k} b_k$.
  (b) Replace a_{ij} by $\sum_{k=1}^{n} c_k x^{d_i - d_k} a_{kj}$ for all $j \in \{1, \ldots, n\}$.
(8) Go back to step 5.

The $b_1, \ldots, b_n$ remain a basis of O_K throughout the algorithm because the new b_i in step 7a can be written as a nonzero constant times the old b_i plus a $\mathbb{C}[x]$-linear combination of the b_j, $j \neq i$. When we go back to step 5 the non-negative integer d_i decreases while the d_j, $j \neq i$ stay the same. Hence the algorithm must terminate.

Let $b_1, \ldots, b_n$ and $d_1, \ldots, d_n$ be the output of the algorithm. By construction, the number d_i in the algorithm is the smallest integer for which $b_i \in x^{d_i} O_\infty$. If $\beta \in O_K$ with $\beta \neq 0$ then we can write $\beta = c_1b_1 + \cdots + c_nb_n$ for some $c_1, \ldots, c_n \in \mathbb{C}[x]$. Denote d_β as the maximum of $\deg_x(c_j) + d_j$ taken over all j for which $c_j \neq 0$. Then $\beta \in x^{d_\beta} O_\infty$ by construction. Since the vectors $V_1, \ldots, V_n$ in the algorithm are linearly independent when the algorithm terminates, there can not be any cancellation, which means that d_β is the smallest integer for which $\beta \in x^{d_\beta} O_\infty$. Because of this, we get the following:

If d is a positive integer, then the set $B_d := \{x^j b_i \mid 0 \leq j \leq d - d_i,\ 1 \leq i \leq n\}$ is a basis of $O_K \bigcap x^d O_\infty$ as $\mathbb{C}$-vector space.

Note that B_d is a basis of the Riemann-Roch space of the pole-divisor of x^d. So computing B_d can be interpreted as (i): a direct application of a normalized integral basis, or (ii): a special case of algorithms [3, 6] for Riemann-Roch spaces. The two interpretations are equivalent because the first step in computing Riemann-Roch spaces is to compute a normalized integral basis.

We can take q-expansions for each of the elements of B_d, and then make a change of basis so that the new basis B_d^{REF} will have q-expansions in Reduced Echelon Form. This means that if $b \in B_d^{\mathrm{REF}}$ and $b = a_r q^r + a_{r+1} q^{r+1} + \cdots$ with $a_r \neq 0$ then $a_r = 1$ and all other basis elements have a zero coefficient at q^r. Then B_d^{REF}, for suitable d, is an order complete basis. For an implementation and two examples see:
www.math.fsu.edu/∼hoeij/files/OrderComplete

2. New Identities

We will give two identities of Ramanujan type found using our algorithm (the second one is only on our website). Let $p(n)$ be the partition function. Define

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

and

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

and

$$f := (dt/dq) \prod_{n=1}^{\infty} (1-q^n)^{-2} (1-q^{11n})^{-2}.$$

Both h and t are modular functions in $M^\infty(11)$, see [14, Lemma 3.1].

To prove that f is in $M^\infty(11)$ as well, first note that by [10, Prop. 3.1.1]

$$b(\tau) := q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2, \quad q = e^{2\pi i \tau}$$

satisfies

$$b\Big(\frac{a\tau+b}{c\tau+d}\Big) = (c\tau+d)^2 b(\tau) \tag{1}$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$. Since $t \in M^\infty(11)$, we have

$$t\Big(\frac{a\tau+b}{c\tau+d}\Big) = t(\tau).$$

The derivative with respect to τ is:

$$(c\tau+d)^{-2} t'\Big(\frac{a\tau+b}{c\tau+d}\Big) = t'(\tau) \tag{2}$$

Multiplying (2) by $(c\tau+d)^2$ and dividing by (1) gives

$$(t'/b)\Big(\frac{a\tau+b}{c\tau+d}\Big) = (t'/b)(\tau).$$

Since $\frac{d}{d\tau} = 2\pi i q \frac{d}{dq}$, it follows that $t'/b = 2\pi i f$. Therefore

$$f\Big(\frac{a\tau+b}{c\tau+d}\Big) = f(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$. Furthermore, since $b(\tau)$ has no zeros in the upper half plane and $t(\tau)$ is holomorphic in the upper half plane it follows that f is holomorphic in the upper half plane. Hence the first condition of being a modular function for $\Gamma_0(11)$ according to the definition in [14] is satisfied. The second condition is equivalent to showing that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we have an expansion of the form

$$f\Big(\frac{a\tau+b}{c\tau+d}\Big) = \sum_{n=m(\gamma)}^{\infty} a_\gamma(n) q^{\frac{\gcd(c^2,n)n}{N}}. \tag{3}$$

As seen in [14], if this property hold for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then it also holds for $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, if there exists $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_0(11)$ such that $\frac{A\frac{a}{c}+B}{C\frac{a}{c}+D} = \frac{a'}{c'}$. So we need to find representatives of the orbits of the action of $\Gamma_0(11)$ on $\mathbb{Q}\cup\{i\infty\}$, that is, the cusps of $\Gamma_0(N)$. From [17] we find that these representatives are 0 and $i\infty$. Then it suffices to show (3) for two cases: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The first case holds because f is a q-series. For the second case we need to show that $f(-1/\tau)$ is a Laurent series in $q^{1/11}$ with finite principal part. By [15] we have

$$\eta(-1/\tau) = (-i\tau)^{1/2}\eta(\tau).$$

This implies

$$t(-1/\tau) = t^{-1}\Big(\frac{\tau}{11}\Big) \tag{4}$$

and

$$b(-1/\tau) = -\frac{1}{11}b(\frac{\tau}{11})\tau^2.$$

The derivative of (4) is

$$\tau^{-2}t'(-1/\tau) = \frac{1}{11}t^{-2}(\frac{\tau}{11})t'(\frac{\tau}{11})$$

which is equivalent to

$$t'(-1/\tau) = \frac{1}{11}\tau^2 t^{-2}(\frac{\tau}{11})t'(\frac{\tau}{11}).$$

This implies

$$(t'/b)(-1/\tau) = -(t'/b)(\frac{\tau}{11})t^{-2}(\frac{\tau}{11}).$$

Hence

$$f(-1/\tau) = -f(\tau/11)t^{-2}(\tau/11) = 5q^{4/11} + O(q^{5/11}).$$

So the last condition for f being a modular function for $\Gamma_0(11)$ is verified. In order for f to be in $M^\infty(11)$ we need the order of f to be nonnegative at all cusps except $i\infty$. That only leaves the cusp 0 where the order is 4. This shows $f \in M^\infty(11)$.

We want to express h as an element of $\mathbb{C}(t,f)$. The pole orders of t and f are 5 and 6 so $p(x,y) = \sum_{i=0}^{6}\sum_{j=0}^{5} a_{ij}x^i y^j$ is an Ansatz for the algebraic relation $p(t,f) = 0$. Solving linear equations coming from q-expansions gives

$$p(x,y) = y^5 + 170xy^4 + 9345x^2y^3 + 167320x^3y^2 + (5^5x^2 - 7903458x + 5^5 11^6)x^4.$$

We use $p(x,y)$ to compute in $\mathbb{C}(t,f) \cong \mathbb{C}(x)[y]/(p)$. We compute B_d^{REF} from the previous section with $d = 1$ and obtain b_0, b_2, b_3, b_4, b_5 where $b_0 = 1$ and $b_i =$

$q^{-i} + c_i q^{-1} + O(q^1)$ for $i = 2, \ldots, 5$ for some constants c_i. Since h has a pole of order 4, we can write it as a linear combination of b_0, b_2, b_3, b_4. We have $b_0 = 1$ and

$$\begin{aligned}
b_2 &= 12 + \tfrac{5t}{22}\left(\tfrac{t-11^3}{f+47t} - \tfrac{(42t+f)(t+11^3)}{f^2+89ft+1424t^2}\right) &&= q^{-2} + 2q^{-1} + 5q + 8q^2 + O(q^3)\\
b_3 &= 12 + \tfrac{5t}{22}\left(3\tfrac{t-11^3}{f+47t} - \tfrac{(16t+3f)(t+11^3)}{f^2+89ft+1424t^2}\right) &&= q^{-3} + q^{-1} + 2q + 2q^2 + O(q^3)\\
b_4 &= 12 + \tfrac{5t}{22}\left(-3\tfrac{t-11^3}{f+47t} - \tfrac{(28t+19f)(t+11^3)}{f^2+89ft+1424t^2}\right) &&= q^{-4} - 2q^{-1} + 6q + 3q^2 + O(q^3).
\end{aligned}$$

Like in [16, Alg. MW], we use

$$h = 11q^{-4} + 165q^{-3} + 748q^{-2} + 1639q^{-1} + 3553 + O(q)$$

to find

$$h - 11b_4 - 165b_3 - 748b_2 - 3553b_0 = O(q).$$

This expression in $M^\infty(11)$ has no poles and a root at $\tau = i\infty$ (at $q = 0$) hence it is the zero function. Therefore

$$h = 11b_4 + 165b_3 + 748b_2 + 3553b_0.$$

Replacing b_0, b_2, b_3, b_4 with their corresponding expressions in terms of t and f gives

$$h = qt\prod_{n=1}^{\infty}(1-q^{11k})\sum_{n=0}^{\infty}p(11n+6)q^n = 11^4 + 55t\left(5\frac{t-11^3}{f+47t} - \frac{2(71t+3f)(t+11^3)}{f^2+89ft+1424t^2}\right).$$

This implies $p(11n + 6) \equiv 0 \pmod{11}$. Other expressions for h that prove this congruence were already in [1, 9], however, our expression in terms of t, f is novel.

For our second example, take t and h be as before and let

$$E_4 := 1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}$$

be the usual Eisenstein series. Let

$$\Delta := q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Let $J := E_4^3/\Delta = q^{-1} + \cdots$ and

$$f := Jt^3.$$

Next we show that $f \in M^\infty(11)$. From the last chapter of [18] we find

$$E_4\Big(\frac{a\tau+b}{c\tau+d}\Big) = (c\tau+d)^4E_4(\tau)$$

and

$$\Delta\Big(\frac{a\tau+b}{c\tau+d}\Big) = (c\tau+d)^{12}\Delta(\tau)$$

for all $\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. These two identities imply

$$J\Big(\frac{a\tau+b}{c\tau+d}\Big) = J(\tau)$$

for all $\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Since $\mathrm{SL}_2(\mathbb{Z})$ has only one cusp, $i\infty$, and since J is a q-series it follows that J is a modular function on $\mathrm{SL}_2(\mathbb{Z})$ and thus on $\Gamma_0(11)$.

Since $t(\tau)$ is already a modular function on $\Gamma_0(11)$, it follows that f is a modular function on $\Gamma_0(11)$. To show that f is in $M^\infty(11)$ it suffices to show that the order of f at the cusp 0 is nonnegative. Since $J(-1/\tau) = (q^{-1/11})^{11} + O(1)$ the order of J at 0 is -11. The order of t at 0 is 5, so the order of f at the cusp 0 is $-11 + 3 \cdot 5 = 4 \geq 0$. This shows $f \in M^{\infty}(11)$.

The only pole of f is at $i\infty$, it has order 16. We compute the algebraic relation $p(t, f) = 0$ with the Ansatz method, and use p to compute B_d^{REF}. Then we express h in terms of the t and the new f. This relation, and the Maple file that computes it, are given at www.math.fsu.edu/~hoeij/files/OrderComplete.

References

[1] A. O. L. Atkin. Proof of a Conjecture of Ramanujan. *Glasgow Mathematical Journal*, 8:14–32, 1967.

[2] F. G. Garvan. Some Congruences for Partitions that are p-Cores. *Proceedings of the London Mathematical Society*, 66:449–478, 1993.

[3] F. Hess. Computing riemannroch spaces in algebraic function fields and related topics. *Journal of Symbolic Computation*, 33:425–445, 2002.

[4] K. Hughes. Ramanujan Congruences for $p_{-k}(n)$ Modulo Powers of 17. *Canadian Journal of Mathematics*, 43:506–525, 1991.

[5] E. Nart J. Guàrdia, J. Montes. Higher newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. Théor. Nombres Bordeaux*, 23:667–696, 2011.

[6] K. Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Mathematics of Computation*, 73:333–357, 2004.

[7] O. Kolberg. An Elementary discussion of Certain Modular Forms. *UNIVERSITET I BERGEN ÅRBOK Naturvitenskapelig rekke*, 16, 1959.

[8] O. Kolberg. Congruences Involving the Partition Function for the Moduli 17, 19, and 23. *UNIVERSITET I BERGEN ÅRBOK Naturvitenskapelig rekke*, 15, 1959.

[9] J. Lehner. Ramanujan Identities Involving the Partition Function for the Moduli 11^{α}. *American Journal of Mathematics*, 65:492–520, 1943.

[10] G. Ligozat. Courbes modulaires de genre 1. *Mémoires de la S.M.F*, 43:5–80, 1975.

[11] M. Newman. Construction and Application of a Class of Modular Functions. *Proceedings London Mathematical Society*, 3(7), 1957.

[12] M. Newman. Construction and Application of a Class of Modular Functions 2. *Proceedings London Mathematical Society*, 3(9), 1959.

[13] P. Paule and C.-S. Radu. A Proof of the Weierstrass Gap Theorem not using the Riemann-Roch Formula. Available from `http://www3.risc.jku.at/publications/download/risc_5928/corrections_to_pp_final_Jan31.pdf`.

[14] P. Paule and C.-S. Radu Radu. A new witness identity for $11 \mid p(11n+6)$. In *Analytic number theory, modular forms and q-hypergeometric series*, volume 221 of *Springer Proc. Math. Stat.*, pages 625–639. Springer, Cham, 2017.

[15] H. Rademacher. The Ramanujan Identities Under Modular Substitutions. *Transactions of the American Mathematical Society*, 51(3):609–636, 1942.

[16] C.-S. Radu. An Algorithmic Approach to Ramanujan-Kolberg Identities. *Journal of Symbolic Computations*, 68:225–253, 2015.

[17] C.-S. Radu. An algorithm to prove algebraic relations involving eta quotients. *Annals of Combinatorics*, 22:377–391, 2018.

[18] J. P. Serre. *A Course in Arithmetic*. Springer, 1996.

[19] B. Trager. *Integration of algebraic functions*. PhD thesis, Dept. of EECS, MIT, 1984.

[20] M. van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *J. Symbolic Comput.*, 18(4):353–363, 1994.

[21] Y. Yang. Defining Equations of Modular Curves. *Advances in Mathematics*, 204:481–508, 2006.