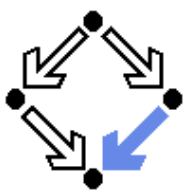
RICAM Special Semester on
Applications of Algebra and Number Theory
Johann Radon Institute (RICAM), Nov 28, 2013

Computer Algebra, Ramanujan Congruences, and Polynomials

Peter Paule
(joint work with Cristian-Silviu Radu)

Johannes Kepler University Linz
Research Institute for Symbolic Computation (RISC)



Introduction

1	1	2	3	5
7	11	15	22	30
42	56	77	101	135
176	231	297	385	490
627	792	1002	1255	1575
1958	2436	3010	3718	4565
5604	6842	8349	10143	12310
14883	17977	21637	26015	31185
37338	44583	53174	63261	75175
89134	105558	124754	147273	173525
204226	239943	281589	329931	386155
451276	526823	614154	715220	831820
966467	1121505	1300156	1505499	1741630
2012558	2323520	2679689	3087735	3554345
4087968	4697205	5392783	6185689	7089500
8118264	9289091	10619863	12132164	13848650

Theorem

Let S be a compact Riemann surface and z a meromorphic function on S having n poles (incl. multiplicity). Let f be any other meromorphic function on S. Then there exist rational functions $c_k(x) \in \mathbb{C}(x)$ such that

$$f^n + c_1(z)f^{n-1} + \cdots + c_{n-1}(z)f + c_n(z) = 0.$$

Theorem

Let S be a compact Riemann surface and z a meromorphic function on S having n poles (incl. multiplicity). Let f be any other meromorphic function on S. Then there exist rational functions $c_k(x) \in \mathbb{C}(x)$ such that

$$f^n + c_1(z)f^{n-1} + \cdots + c_{n-1}(z)f + c_n(z) = 0.$$

Moreover, if

$$\mathrm{PoleSet}(z) \subseteq \mathrm{PoleSet}(f),$$

then the $c_k(x)$ are polynomials; i.e., $c_k(x) \in \mathbb{C}[x]$.

Partition Numbers

Example: $p(4) = 5$: $4,\ 3+1,\ 2+2,\ 2+1+1,\ 1+1+1+1.$

Theorem

$(p(n))_{n\geq 0}$ *is not holonomic.*

Example: $p(4) = 5$: $4,\ 3+1,\ 2+2,\ 2+1+1,\ 1+1+1+1.$

Theorem

$(p(n))_{n\geq 0}$ *is not holonomic.*

Proof. The generating function is

$$\begin{aligned}\sum_{n=0}^{\infty} p(n)q^n &= \prod_{n=1}^{\infty}(1-q^n)^{-1}\\ &= (1+q^1+q^{1+1}+q^{1+1+1}+\dots)\\ &\times (1+q^2+q^{2+2}+q^{2+2+2}+\dots)\\ &\times \text{etc.}\\ &= \dots + q^{1+1+1}q^{2+2}\dots+\dots\end{aligned}$$

This implies non-holonomicity, because holonomic functions have only finitely many singularities.

Growth of $p(n)$

Example [MacMahon 1916]:

$$p(200) = 3,972,999,029,388$$

Growth of $p(n)$

Example [MacMahon 1916]:

$$p(200) = 3,972,999,029,388$$

Theorem

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right) \quad \textit{as} \quad n \to \infty.$$

Back to our table

- 34 of the 80 entries are even; 46 are odd.

Back to our table

- 34 of the 80 entries are even; 46 are odd.
- 4,996 of the first 10,000 entries are even; 5,004 are odd.

Back to our table

- 34 of the 80 entries are even; 46 are odd.
- 4,996 of the first 10,000 entries are even; 5,004 are odd.

Does this pattern continue?

DEEPER INSIGHT: The Subbarao Conjecture (1966)

- `Ono [1996]:` Given integers $0 \leq B < A$:

$$p(An + B) \equiv 0 \pmod{2} \quad \text{for infinitely many } n.$$

DEEPER INSIGHT: The Subbarao Conjecture (1966)

- `Ono [1996]:` Given integers $0 \leq B < A$:

$$p(An + B) \equiv 0 \pmod{2} \quad \text{for infinitely many } n.$$

- `Radu [2012]:` Given integers $0 \leq B < A$:

$$p(An + B) \not\equiv 0 \pmod{2} \quad \text{for infinitely many } n.$$

DEEPER INSIGHT: The Subbarao Conjecture (1966)

- `Ono [1996]:` Given integers $0 \leq B < A$:

$$p(An + B) \equiv 0 \pmod 2 \quad \text{for infinitely many } n.$$

- `Radu [2012]:` Given integers $0 \leq B < A$:

$$p(An + B) \not\equiv 0 \pmod 2 \quad \text{for infinitely many } n.$$

Remark. Radu's algorithmic insight enabled him to invoke a result by Deligne and Rapoport [1979]. The same applies to his proof [2012] of a conjecture of Ahlgren and Ono [2002].

Ahlgren and Ono determined:

- 3,313, 3,325, and 3,362 of the first 10,000 entries are congruent respectively to 0, 1, and 2 modulo 3.

BUT:

Ahlgren and Ono determined:

- 3,313, 3,325, and 3,362 of the first 10,000 entries are congruent respectively to 0, 1, and 2 modulo 3.

BUT:

- 3,611 (many more than the expected one-fifth) of the first 10,000 values of $p(n)$ are divisible by 5.

Ahlgren and Ono determined:

- 3,313, 3,325, and 3,362 of the first 10,000 entries are congruent respectively to 0, 1, and 2 modulo 3.

BUT:

- 3,611 (many more than the expected one-fifth) of the first 10,000 values of $p(n)$ are divisible by 5.

WHY? Let's look again at our table:

1	1	2	3	5
7	11	15	22	30
42	56	77	101	135
176	231	297	385	490
627	792	1002	1255	1575
1958	2436	3010	3718	4565
5604	6842	8349	10143	12310
14883	17977	21637	26015	31185
37338	44583	53174	63261	75175
89134	105558	124754	147273	173525
204226	239943	281589	329931	386155
451276	526823	614154	715220	831820
966467	1121505	1300156	1505499	1741630
2012558	2323520	2679689	3087735	3554345
4087968	4697205	5392783	6185689	7089500
8118264	9289091	10619863	12132164	13848650

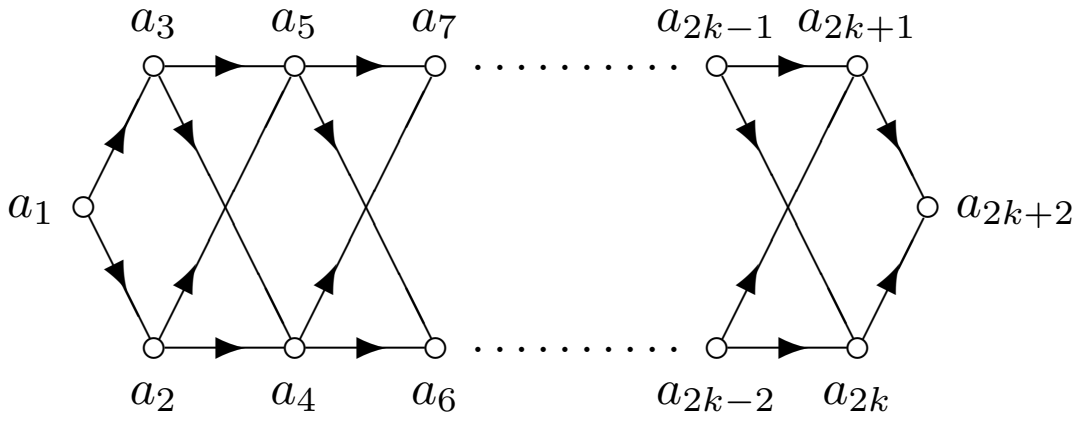
Partition Congruences and Combinatorics

- There is a combinatorial explanation for the divisibility of $p(5n+4)$ by 5 (Dyson's rank statistics). But concerning further connections between combinatorics and modular forms, not too much is known so far.

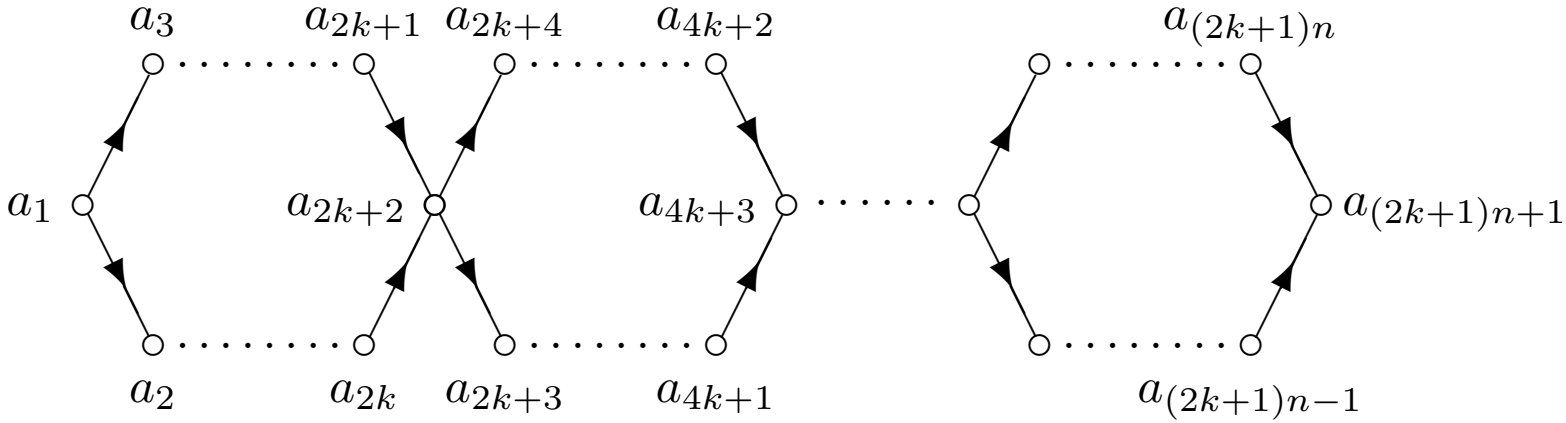
As an example, we present a recent combinatorial construction of modular forms which involves Dedekind's eta function:

$$\eta(\tau) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n) \quad (q = e^{2\pi i\tau}).$$

Partition Diamonds



A k-elongated partition diamond of length 1



A k-elongated partition diamond of length n

Generating function:

$$h_{n,k}(q) = \frac{\prod_{j=0}^{n-1}(1+q^{(2k+1)j+2})(1+q^{(2k+1)j+4})\cdots(1+q^{(2k+1)j+2k})}{\prod_{j=1}^{(2k+1)n+1}(1-q^j)}$$

This generating function is beautiful indeed, but George Andrews wanted more!

Generating function:

$$h_{n,k}(q) = \frac{\prod_{j=0}^{n-1}(1+q^{(2k+1)j+2})(1+q^{(2k+1)j+4})\cdots(1+q^{(2k+1)j+2k})}{\prod_{j=1}^{(2k+1)n+1}(1-q^j)}$$

This generating function is beautiful indeed, but George Andrews wanted more!

From: George E Andrews<andrews@math.psu.edu>
Date: Jan 2005
To: Peter.Paule@risc.uni-linz.ac.at,
Axel.Riese@risc.uni-linz.ac.at

Subject: I had a brainstorm

Dear Axel and Peter,

I have had a BRAINSTORM! (I can almost see the smile on Peter's face ...) To begin with let me draw your attention to Thm.2 in PAXI and Cor.2.1 in PAVIII ... However, THIS IS JUST THE BEGINNING.

Namely, I always had a slight disappointment in both the earlier results because the generating function ... was not a modular form. However, I now know how to produce the appropriate directed graph to provide ... a generating function that is not only a modular form but, in fact, a product of instances of Dedekind's eta-function.

Recall the generating function:

$$h_{n,k}(q) = \frac{\prod_{j=0}^{n-1}(1+q^{(2k+1)j+2})(1+q^{(2k+1)j+4})\cdots(1+q^{(2k+1)j+2k})}{\prod_{j=1}^{(2k+1)n+1}(1-q^j)}$$

The result of Andrews' brainstorm: delete the source:

Recall the generating function:

$$h_{n,k}(q) = \frac{\prod_{j=0}^{n-1}(1+q^{(2k+1)j+2})(1+q^{(2k+1)j+4})\cdots(1+q^{(2k+1)j+2k})}{\prod_{j=1}^{(2k+1)n+1}(1-q^j)}$$

The result of Andrews' brainstorm: delete the source:

$$h^*_{n,k}(q) = \frac{\prod_{j=0}^{n-1}(1+q^{(2k+1)j+1})(1+q^{(2k+1)j+3})\cdots(1+q^{(2k+1)j+2k-1})}{\prod_{j=1}^{(2k+1)n}(1-q^j)}$$

and glue the diamonds together:

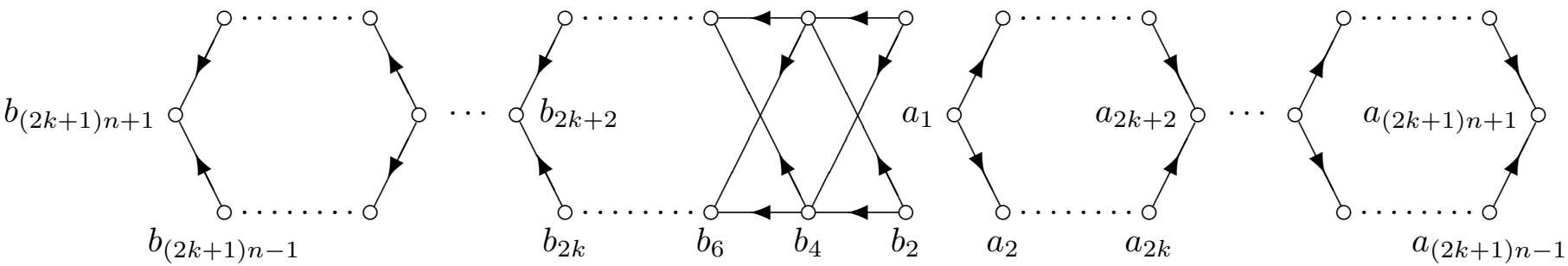
$$\sum_{n=0}^{\infty} \Delta_k(n) q^n := h_{n,k}(q)\, h^*_{n,k}(q)$$

$$= \prod_{n=1}^{\infty} \frac{(1-q^{2n})(1-q^{(2k+1)n})}{(1-q^n)^3(1-q^{(4k+2)n})}$$

$$\sum_{n=0}^{\infty} \Delta_k(n) q^n := h_{n,k}(q)\, h^*_{n,k}(q)$$

$$= \prod_{n=1}^{\infty} \frac{(1-q^{2n})(1-q^{(2k+1)n})}{(1-q^n)^3(1-q^{(4k+2)n})}$$

$$= q^{(k+1)/12} \frac{\eta(2\tau)\eta((2k+1)\tau)}{\eta(\tau)^3\eta((4k+2)\tau)}$$



A broken k-diamond of length $2n$

Numerous Congruences for $\Delta_k(n)$

Example [Sellers & Radu, 2012]

$$\sum_{n=0}^{\infty} \Delta_2(3n+1)q^n \equiv 2q \prod_{n=1}^{\infty} \frac{(1-q^{10n})^4}{(1-q^{5n})^2} \pmod 3$$

Numerous Congruences for $\Delta_k(n)$

Example [Sellers & Radu, 2012]

$$\sum_{n=0}^{\infty} \Delta_2(3n+1)q^n \equiv 2q \prod_{n=1}^{\infty} \frac{(1-q^{10n})^4}{(1-q^{5n})^2} \pmod 3$$

This implies for all $n \geq 0$:

$$\begin{aligned} \Delta_2(15n+1) &\equiv 0 \pmod 3, \\ \Delta_2(27n+16) &\equiv 0 \pmod 3, \\ \Delta_2(147n+58) &\equiv 0 \pmod 3, \end{aligned}$$

etc.

Numerous Congruences for $\Delta_k(n)$

Example [Sellers & Radu, 2012]

$$\sum_{n=0}^{\infty} \Delta_2(3n+1)q^n \equiv 2q \prod_{n=1}^{\infty} \frac{(1-q^{10n})^4}{(1-q^{5n})^2} \pmod 3$$

This implies for all $n \geq 0$:

$$\begin{aligned} \Delta_2(15n+1) &\equiv 0 \pmod 3, \\ \Delta_2(27n+16) &\equiv 0 \pmod 3, \\ \Delta_2(147n+58) &\equiv 0 \pmod 3, \\ &\textit{etc.} \end{aligned}$$

Note. More people became interested in such congruences, e.g., S.H. Chan, W.Y.C. Chen, S. Cui, A.R.B. Fan, S.S. Fu, N. Gu, M.D. Hirschhorn, M. Jameson, E. Mortenson, X. Xiong, R.T. Yu.

Ramanujan's Congruences

Ramanujan's Congruences

$$\begin{aligned} p(5n+4) &\equiv 0 \pmod 5, \\ p(7n+5) &\equiv 0 \pmod 7, \\ p(11n+6) &\equiv 0 \pmod{11} \end{aligned}$$

Ramanujan's Congruences

$$
\begin{aligned}
p(5n+4) &\equiv 0 \pmod 5,\\
p(5^2n+24) &\equiv 0 \pmod{5^2},\\
p(5^3n+99) &\equiv 0 \pmod{5^3},
\end{aligned}
$$

etc.

Ramanujan's Conjecture (1919)

For $\ell \in \{5, 7, 11\}$ and $\alpha \in \{1, 2, 3, \dots\}$:

$$p(\ell^\alpha n + \mu_{\alpha,\ell}) \equiv 0 \pmod{\ell^\alpha},$$

where $\mu_{\alpha,\ell} \in \{0, \dots, \ell^\alpha - 1\}$ is uniquely defined by

$$24\,\mu_{\alpha,\ell} \equiv 1 \pmod{\ell^\alpha}.$$

A Bit of History

- Ramanujan [1917-1919]: proof sketches for $\ell = 5$ and $\ell = 7$; see Berndt and Ono [1999].

A Bit of History

- Ramanujan [1917-1919]: proof sketches for $\ell = 5$ and $\ell = 7$; see Berndt and Ono [1999].
- Watson [1938]: $\ell = 5$ and $\ell = 7$ *(corrected version)*

A Bit of History

- Ramanujan [1917-1919]: proof sketches for $\ell = 5$ and $\ell = 7$; see Berndt and Ono [1999].
- Watson [1938]: $\ell = 5$ and $\ell = 7$ *(corrected version)*
- Atkin [1967]: $\ell = 11$

A Bit of History

- Ramanujan [1917-1919]: proof sketches for $\ell = 5$ and $\ell = 7$; see Berndt and Ono [1999].
- Watson [1938]: $\ell = 5$ and $\ell = 7$ *(corrected version)*
- Atkin [1967]: $\ell = 11$
- Gordon [1983]:

$$p(11^{\alpha} n + \mu_{\alpha,11}) \equiv 0 \pmod{11^{\alpha+\epsilon}},$$

where ϵ is a fixed non-positive integer to be determined. Following Gordon's proof one can easily determine $\epsilon = 0$.

Our proof for $\ell = 11$ and $\ell = 5, 7$:

- In his generalization of Watson's method, Gordon needs to compute the structure constants of a certain algebra.
  Although this is not needed in the case $\ell = 5, 7$.

Our proof for $\ell = 11$ and $\ell = 5, 7$:

- In his generalization of Watson's method, Gordon needs to compute the structure constants of a certain algebra. Although this is not needed in the case $\ell = 5, 7$.

- For $\ell = 11$ we succeeded to do without structure constants, (i.e., we stay with the module structure), so the ingredients here are the same as in the original proof of Watson.

Our proof for $\ell = 11$ and $\ell = 5, 7$:

- In his generalization of Watson's method, Gordon needs to compute the structure constants of a certain algebra. Although this is not needed in the case $\ell = 5, 7$.
- For $\ell = 11$ we succeeded to do without structure constants, (i.e., we stay with the module structure), so the ingredients here are the same as in the original proof of Watson.
- This way we obtain a unified framework for all three cases $\ell = 5, 7, 11$.

Our proof for $\ell = 11$ and $\ell = 5, 7$:

- In his generalization of Watson's method, Gordon needs to compute the structure constants of a certain algebra. Although this is not needed in the case $\ell = 5, 7$.
- For $\ell = 11$ we succeeded to do without structure constants, (i.e., we stay with the module structure), so the ingredients here are the same as in the original proof of Watson.
- This way we obtain a unified framework for all three cases $\ell = 5, 7, 11$.
- The price to pay: our approach is more expensive computationally.

The Modular Function Setting

Basic Notions

The level ℓ congruence subgroup

$$\Gamma_0(\ell) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{\ell} \right\}$$

acts on $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$ (extended upper half plane) via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\tau) \mapsto \frac{a\tau + b}{c\tau + d}.$$

Basic Notions

The level ℓ congruence subgroup

$$\Gamma_0(\ell) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{\ell} \right\}$$

acts on $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$ (extended upper half plane) via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\tau) \mapsto \frac{a\tau + b}{c\tau + d}.$$

This induces an action on functions $f : \mathbb{H}^* \to \mathbb{C} \cup \{i\infty\}$ by

$$(f|\gamma)(\tau) := f\left(\frac{a\tau + b}{c\tau + d}\right) \quad \text{where} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Compact Riemann Surfaces $X_0(\ell)$

$$X_0(\ell) := \text{orbit space of the action of } \Gamma_0(\ell) \text{ on } \mathbb{H}^*$$
$$= \{[\tau] : \tau \in \mathbb{H}^*\}$$

Compact Riemann Surfaces $X_0(\ell)$

$$X_0(\ell) := \text{orbit space of the action of } \Gamma_0(\ell) \text{ on } \mathbb{H}^*$$
$$= \{[\tau] : \tau \in \mathbb{H}^*\}$$

Note.

$$\frac{a\tau + b}{c\tau + d} \longrightarrow \frac{a}{c} \quad \text{when} \quad \tau \longrightarrow i\infty.$$

and

$$\frac{a}{0} = i\infty.$$

Compact Riemann Surfaces $X_0(\ell)$

$$X_0(\ell) := \text{orbit space of the action of } \Gamma_0(\ell) \text{ on } \mathbb{H}^*$$
$$= \{[\tau] : \tau \in \mathbb{H}^*\}$$

Note.

$$\frac{a\tau + b}{c\tau + d} \longrightarrow \frac{a}{c} \quad \text{when} \quad \tau \longrightarrow i\infty.$$

and

$$\frac{a}{0} = i\infty.$$

Set of cusps: For any prime ℓ,

$$\{[x] \in X_0(\ell) : x \in \mathbb{Q} \cup \{i\infty\}\} = \{[0], [i\infty]\}.$$

Modular Functions (MF) on Compact Riemann Surfaces $X_0(\ell)$

$f : \mathbb{H}^* \to \mathbb{C} \cup \{i\infty\}$ induces a MF $f^* : X_0(\ell) \to \mathbb{C} \cup \{i\infty\}$ if

Modular Functions (MF) on Compact Riemann Surfaces $X_0(\ell)$

$f : \mathbb{H}^* \to \mathbb{C} \cup \{i\infty\}$ induces a MF $f^* : X_0(\ell) \to \mathbb{C} \cup \{i\infty\}$ if

- f is holomorphic on $\mathbb{H}$;
- f is constant on the orbits $[\tau]$, $\tau \in \mathbb{H}^*$;
- f is meromorphic at points in $\mathbb{Q} \cup \{i\infty\}$.

Fourier expansions of f^* *at* cusps $[a/c] \in X_0(\ell)$

For $\tau \in \text{neighborhood}(i\infty)$:

$$f^*\left(\left[\frac{a\tau+b}{c\tau+d}\right]\right)) = (f|\gamma)(\tau) = \sum_{n \geq \text{ord}_{[a/c]}(f^*)} a_{[a/c]}(n) q_{[a/c]}^n.$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$, $q_{[a/c]} = \left(e^{2\pi i \tau}\right)^{\frac{\gcd(c^2,\ell)}{\ell}}$.

Fourier expansions of f^* *at* cusps $[a/c] \in X_0(\ell)$

For $\tau \in \text{neighborhood}(i\infty)$:

$$f^*\left(\left[\frac{a\tau+b}{c\tau+d}\right]\right)) = (f|\gamma)(\tau) = \sum_{n \geq \text{ord}_{[a/c]}(f^*)} a_{[a/c]}(n) q_{[a/c]}^n.$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$, $q_{[a/c]} = \left(e^{2\pi i \tau}\right)^{\frac{\gcd(c^2,\ell)}{\ell}}$.

Note. If $[a/c] = [a/0] = [i\infty]$ then $q_{[a/c]} = q$.

Back to Ramanujan's congruences

$$L_{2\beta-1,\ell} := q\prod_{n=1}^{\infty}(1-q^{\ell n})\sum_{n=0}^{\infty}p(\ell^{2\beta-1}n+\mu_{2\beta-1,\ell})q^n,$$

and

$$L_{2\beta,\ell} := q\prod_{n=1}^{\infty}(1-q^{n})\sum_{n=0}^{\infty}p(\ell^{2\beta}n+\mu_{2\beta,\ell})q^n.$$

We consider these series as Fourier expansions at $[i\infty]$ of modular functions $f^* : X_0(\ell) \to \mathbb{C} \cup \{i\infty\}$ from a suitable subring $R(\ell)$.

The Rings $R(5), R(7)$, and $R(11)$

Recall $$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n) \quad (q = e^{2\pi i\tau}).$$

From the literature it is well known that we can take

The Rings $R(5), R(7)$, and $R(11)$

Recall $$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n) \quad (q = e^{2\pi i\tau}).$$

From the literature it is well known that we can take

$$R(5) = \mathbb{Z}[z_5], \quad R(7) = \mathbb{Z}[z_7],$$

and

$$R(11) = \langle J_0, J_1, \ldots, J_4 \rangle_{\mathbb{Z}[z_{11}]}$$

where

$$z_5 := \frac{\eta^6(5\tau)}{\eta^6(\tau)}, \quad z_7 := \frac{\eta^4(7\tau)}{\eta^4(\tau)}, \quad z_{11} := \frac{\eta^{12}(11\tau)}{\eta^{12}(\tau)},$$

and with the J_k such that $\mathrm{ord}_{[i\infty]}(J_k^*) = k$ as in Atkin (1967).

The U-operator

$$U_\ell(f^*) := \sum_n a(\ell n) q^n$$

where $f^*([\tau]) = \sum_n a(n) q^n$ is the Fourier expansion of f^* at $[i\infty]$.

The U-operator

$$U_\ell(f^*) := \sum_n a(\ell n) q^n$$

where $f^*([\tau]) = \sum_n a(n) q^n$ is the Fourier expansion of f^* at $[i\infty]$.

Definition. For prime ℓ,

$$U_\ell^{(1)}(f^*) := U_\ell\left(\frac{\eta(\ell^2\tau)}{\eta(\tau)} f^*\right) \quad \text{and} \quad U_\ell^{(2)}(f^*) := U_\ell(f^*).$$

The U-operator

$$U_\ell(f^*) := \sum_n a(\ell n) q^n$$

where $f^*([\tau]) = \sum_n a(n) q^n$ is the Fourier expansion of f^* at $[i\infty]$.

Definition. For prime ℓ,

$$U_\ell^{(1)}(f^*) := U_\ell\left(\frac{\eta(\ell^2\tau)}{\eta(\tau)} f^*\right) \quad \text{and} \quad U_\ell^{(2)}(f^*) := U_\ell(f^*).$$

Lemma.

$$f^* \in R(\ell) \Rightarrow U_\ell^{(i)}(f^*) \in R(\ell).$$

Recursive representation of $L_{\alpha,\ell}$ in $R(\ell)$

Lemma. For $\ell \in \{5, 7, 11\}$,

$$L_{\alpha,\ell} \in R(\ell);$$

the $L_{\alpha,\ell}$ satisfy a recursion in $R(\ell)$ as follows:

$$L_{0,\ell} = 1,$$

$$L_{2\beta-1,\ell} = U_\ell^{(1)}(L_{2\beta-2,\ell}) \text{ and } L_{2\beta,\ell} = U_\ell^{(2)}(L_{2\beta-1,\ell}).$$

This recursion is used in the induction proof of our "Main Theorem":

Main Theorem

For suitably defined subsets $X_{s,\ell}$ of $R(\ell)$ we have:

Theorem. For $\ell \in \{5, 7, 11\}$ and all positive integers β there exist $f_{\beta,\ell} \in X_{1,\ell}$ if β is odd, and $f_{\beta,\ell} \in X_{2,\ell}$ if β is even, such that

$$L_{\beta,\ell} = \ell^{\beta} f_{\beta,\ell} \qquad \text{for} \quad \ell = 5, 11,$$

and

$$L_{\beta,\ell} = \ell^{\lceil \frac{\beta+1}{2} \rceil} f_{\beta,\ell} \qquad \text{for} \quad \ell = 7.$$

Note. Ramanujan's congruences are obtained as an immediate corollary.

The $R(\ell)$-subsets $X_{s,\ell}$ ($\ell = 11$: Atkin)

Set

$$A_\ell := \frac{12}{\gcd(\ell-1,12)}\frac{\ell}{\ell+1} \quad \text{and} \quad z_\ell := \left(\frac{\eta_\ell}{\eta}\right)^{\frac{24}{\gcd(\ell-1,12)}}.$$

Definition. For $\ell \in \{5,7,11\}$ and $s = 1, 2$:

$$X_{s,\ell} := \left\{ \sum_{i=0}^{n_\ell - 1} J_{i,\ell} \sum_{j=0}^{\infty} a_i(j) \ell^{\lceil \frac{A_\ell}{\ell}(\ell j + \xi_i^{(s,\ell)})\rceil} z_\ell^j \;:\; a_0(0) = 0 \text{ and } \right.$$
$$\left. \text{with } a_i(j) \in \mathbb{Z} \text{ nonzero for only finitely many } j \right\}$$

The integer exponents $\xi_i^{(s,\ell)}$ are defined as follows:

The Exponents $\xi_i^{(s,\ell)}$

Definition. For $\ell \in \{5, 7, 11\}$ and $s = 1, 2$ define

$$\xi^{(s,\ell)} : \{0, \ldots, n_\ell - 1\} \to \mathbb{Z},\ i \mapsto \xi_i^{(s,\ell)}$$

by

$$\begin{aligned}(\xi_0^{(1,11)}, \ldots, \xi_4^{(1,11)}) &:= (-5, -1, 1, 2, 6),\\ (\xi_0^{(2,11)}, \ldots, \xi_4^{(2,11)}) &:= (-4, 0, 2, 3, 7);\end{aligned}$$

and

$$\xi_0^{(1,7)} := -7 \text{ and } \xi_0^{(2,7)} := -10;$$

and

$$\xi_0^{(1,5)} := -6 \text{ and } \xi_0^{(2,5)} := -5.$$

Main Tool: The Fundamental Lemma

Fundamental Lemma. Let $\ell \in \{5, 7, 11\}$. For any analytic $w : \mathbb{H} \to \mathbb{C}$ and $j \in \mathbb{Z}$:

$$U_\ell(w z_\ell^j) = -\sum_{i=0}^{d_\ell - 1} a_i^{(\ell)}(z_\ell) U_\ell(w z_\ell^{j+i-d_\ell}).$$

Setting w to the generators of the module $R(\ell)$, we obtain the $U_\ell^{(i)}$ actions on all the module elements — provided

we know the $2 \cdot d_\ell \cdot n_\ell$ $(2 \cdot 5 \cdot 1, 2 \cdot 7 \cdot 1, 2 \cdot 55 \cdot 5)$ initial actions.

This action then serves to express $L_{\beta,\ell}$ in terms of the generators which reveal the divisibilty properties of these elements.

Proof of the Main Theorem

The Fundamental Polynomial for any prime $\ell \geq 5$

The main ingredient in our induction proof is

Theorem. For any prime $\ell \geq 5$ there exists a monic irreducible polynomial $F_\ell(X, Y) \in \mathbb{Q}[Y][X]$ of degree $d_\ell := \frac{\ell(\ell-1)}{\gcd(\ell-1,12)}$ in X (and Y) such that

$$F_\ell(z_\ell(\tau), z_\ell(\ell\tau)) = 0.$$

Recall that

$$z_\ell(\tau) = \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{\frac{24}{\gcd(\ell-1,12)}}.$$

Proving the Existence of the Fundamental Polynomial

Proof.

The proof uses a variant of a classical fact from Riemann surfaces; namely, that on a compact Riemann surface two meromorphic functions are connected by an algebraic relation. □

The Fundamental Polynomial for $\ell \in \{5, 7, 11\}$

Theorem. For $\ell \in \{5, 7, 11\}$ the fundamental polynomial

$$F_\ell(X, Y) = X^{d_\ell} + \sum_{i=0}^{d_\ell - 1} a_i^{(\ell)}(Y) X^i$$

has coefficient polynomials $a_i^{(\ell)}(Y) \in \mathbb{Q}[Y]$ of the form

$$a_i^{(\ell)}(Y) = \sum_{j=\lceil \frac{d_\ell - i}{\ell} \rceil}^{d_\ell} s_\ell(i, j) \ell^{\lceil \frac{A_\ell}{\ell}(\ell j + i - d_\ell) \rceil} Y^j$$

with $s_\ell(i, j) \in \mathbb{Z}$ (determined using computer algebra).

Corollary: The Fundamental Lemma

Fundamental Lemma. Let $\ell \in \{5, 7, 11\}$. For any $w : \mathbb{H} \to \mathbb{C}$ and $j \in \mathbb{Z}$:

$$U_\ell(w z_\ell^j) = -\sum_{i=0}^{d_\ell - 1} a_i^{(\ell)}(z_\ell) U_\ell(w z_\ell^{j+i-d_\ell}).$$

Corollary: The Fundamental Lemma

Fundamental Lemma. Let $\ell \in \{5, 7, 11\}$. For any $w : \mathbb{H} \to \mathbb{C}$ and $j \in \mathbb{Z}$:

$$U_\ell(wz_\ell^j) = -\sum_{i=0}^{d_\ell - 1} a_i^{(\ell)}(z_\ell) U_\ell(wz_\ell^{j+i-d_\ell}).$$

Proof.

Applying U_ℓ to $wz_\ell^{j-d_\ell} F_\ell(z_\ell(\tau), z_\ell(\ell\tau)) = 0$ gives the desired result. □