Partitions, singular moduli, and irreducible polynomials

Michael H. Mertens
joint work with Larry Rolen

Emory University

30^{th} Automorphic Forms Workshop
Winston-Salem, March 09, 2016

Partitions

Definition

A partition of a positive integer n is a non-increasing sequence of positive integers summing up to n. The number of partitions of n is denoted by $p(n)$.

Partitions

Definition

A partition of a positive integer n is a non-increasing sequence of positive integers summing up to n. The number of partitions of n is denoted by $p(n)$.

Example

The partitions of 10 are

$(10), (9, 1), (8, 2), (8, 1, 1), (7, 3), (7, 2, 1), (7, 1, 1, 1), (6, 4), (6, 3, 1), (6, 2, 2), (6, 2, 1, 1), (6, 1, 1, 1, 1),$
$(5, 5), (5, 4, 1), (5, 3, 2), (5, 3, 1, 1), (5, 2, 2, 1), (5, 2, 1, 1, 1), (5, 1, 1, 1, 1, 1), (4, 4, 2), (4, 4, 1, 1), (4, 3, 3),$
$(4, 3, 2, 1), (4, 3, 1, 1, 1), (4, 2, 2, 2), (4, 2, 2, 1, 1), (4, 2, 1, 1, 1, 1), (4, 1, 1, 1, 1, 1, 1), (3, 3, 3, 1), (3, 3, 2, 2),$
$(3, 3, 2, 1, 1), (3, 3, 1, 1, 1, 1), (3, 2, 2, 2, 1), (3, 2, 2, 1, 1, 1), (3, 2, 1, 1, 1, 1, 1), (3, 1, 1, 1, 1, 1, 1, 1), (2, 2, 2, 2, 2),$
$(2, 2, 2, 2, 1, 1), (2, 2, 2, 1, 1, 1, 1), (2, 2, 1, 1, 1, 1, 1, 1), (2, 1, 1, 1, 1, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$

Partitions

Definition

A partition of a positive integer n is a non-increasing sequence of positive integers summing up to n. The number of partitions of n is denoted by $p(n)$.

Example

The partitions of 10 are

$(10), (9,1), (8,2), (8,1,1), (7,3), (7,2,1), (7,1,1,1), (6,4), (6,3,1), (6,2,2), (6,2,1,1), (6,1,1,1,1),$
$(5,5), (5,4,1), (5,3,2), (5,3,1,1), (5,2,2,1), (5,2,1,1,1), (5,1,1,1,1,1), (4,4,2), (4,4,1,1), (4,3,3),$
$(4,3,2,1), (4,3,1,1,1), (4,2,2,2), (4,2,2,1,1), (4,2,1,1,1,1), (4,1,1,1,1,1,1), (3,3,3,1), (3,3,2,2),$
$(3,3,2,1,1), (3,3,1,1,1,1), (3,2,2,2,1), (3,2,2,1,1,1), (3,2,1,1,1,1,1), (3,1,1,1,1,1,1,1), (2,2,2,2,2),$
$(2,2,2,2,1,1), (2,2,2,1,1,1,1), (2,2,1,1,1,1,1,1), (2,1,1,1,1,1,1,1,1), (1,1,1,1,1,1,1,1,1,1)$

So $p(10) = \mathbf{42}$.

Formulas for $p(n)$

- L. Euler (1749):

$$p(n) = \sum_{m=1}^{\infty} (-1)^{m+1} \left[p\left(n - \frac{3m^2 - m}{2}\right) + p\left(n - \frac{3m^2 + m}{2}\right)\right],$$

Formulas for $p(n)$

- L. Euler (1749):

$$p(n) = \sum_{m=1}^{\infty} (-1)^{m+1} \left[p\left(n - \frac{3m^2 - m}{2} \right) + p\left(n - \frac{3m^2 + m}{2} \right) \right],$$

- G. H. Hardy – S. Ramanujan (1918):

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}, \quad n \to \infty,$$

Formulas for $p(n)$

- L. Euler (1749):

$$p(n) = \sum_{m=1}^{\infty} (-1)^{m+1} \left[p\left(n - \frac{3m^2 - m}{2}\right) + p\left(n - \frac{3m^2 + m}{2}\right) \right],$$

- G. H. Hardy – S. Ramanujan (1918):

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}, \quad n \to \infty,$$

- H. Rademacher (1937):

$$p(n) = \frac{2\pi}{(24n-1)^{\frac{3}{4}}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_{\frac{3}{2}} \left(\frac{\pi\sqrt{24n-1}}{6k} \right).$$

An algebraic formula for $p(n)$

Theorem (Bruinier-Ono, 2013)

We have

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_D} P(\tau_Q),$$

where

An algebraic formula for $p(n)$

Theorem (Bruinier-Ono, 2013)

We have

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_D} P(\tau_Q),$$

where

- $\mathcal{Q}_D$: representatives of positive definite binary quadratic forms $Q(x,y) = ax^2 + bxy + cy^2$ of discriminant $D = 1 - 24n$ modulo $\Gamma_0(6)$, where $6|a$ and $b \equiv 1 \pmod{12}$,

An algebraic formula for $p(n)$

Theorem (Bruinier-Ono, 2013)

We have

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_D} P(\tau_Q),$$

where

- $\mathcal{Q}_D$: representatives of positive definite binary quadratic forms $Q(x,y) = ax^2 + bxy + cy^2$ of discriminant $D = 1 - 24n$ modulo $\Gamma_0(6)$, where $6|a$ and $b \equiv 1 \pmod{12}$,
- $P(\tau)$ is a certain Maaß form for $\Gamma_0(6)$ of weight 0,

An algebraic formula for $p(n)$

Theorem (Bruinier-Ono, 2013)

We have

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_D} P(\tau_Q),$$

where

- $\mathcal{Q}_D$: representatives of positive definite binary quadratic forms $Q(x,y) = ax^2 + bxy + cy^2$ of discriminant $D = 1 - 24n$ modulo $\Gamma_0(6)$, where $6|a$ and $b \equiv 1 \pmod{12}$,
- $P(\tau)$ is a certain Maaß form for $\Gamma_0(6)$ of weight 0,
- $\tau_Q \in \mathbb{H}$ such that $Q(\tau_Q, 1) = 0$.

An algebraic formula for $p(n)$

Theorem (Bruinier-Ono, 2013)

We have

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_D} P(\tau_Q),$$

where

- $\mathcal{Q}_D$: representatives of positive definite binary quadratic forms $Q(x,y) = ax^2 + bxy + cy^2$ of discriminant $D = 1 - 24n$ modulo $\Gamma_0(6)$, where $6|a$ and $b \equiv 1 \pmod{12}$,
- $P(\tau)$ is a certain Maaß form for $\Gamma_0(6)$ of weight 0,
- $\tau_Q \in \mathbb{H}$ such that $Q(\tau_Q, 1) = 0$.

Remark

The numbers $P(\tau_Q)$ above are algebraic numbers with denominators dividing D (Larsson-Rolen, 2013).

A polynomial related to partitions

Consider the polynomial

$$H_D(x) := \prod_{Q \in \mathcal{Q}_D} (x - P(\tau_Q)) \in \mathbb{Q}[x].$$

A polynomial related to partitions

Consider the polynomial

$$H_D(x) := \prod_{Q \in \mathcal{Q}_D} (x - P(\tau_Q)) \in \mathbb{Q}[x].$$

Question: Is this polynomial irreducible over $\mathbb{Q}$?

A polynomial related to partitions

Consider the polynomial

$$H_D(x) := \prod_{Q \in \mathcal{Q}_D} (x - P(\tau_Q)) \in \mathbb{Q}[x].$$

Question: Is this polynomial irreducible over $\mathbb{Q}$?
Answer: Usually not,

$$H_D(x) = \prod_{\substack{f>0 \\ f^2 | D}} \varepsilon(f)^{h\left(\frac{D}{f^2}\right)} \widehat{H}_{\frac{D}{f^2}}(\varepsilon(f)x),$$

- $h(d)$ denotes the class number of discriminant d,
- $\varepsilon(f) = 1$ if $f \equiv \pm 1 \pmod{12}$ and $\varepsilon(f) = -1$ otherwise,

Another polynomial related to partitions

Letting $\mathcal{P}_D$ denote the set of primitive forms in $\mathcal{Q}_D$ (i.e., $\gcd(a,b,c)=1$), define

$$\widehat{H}_D(x) := \prod_{Q\in\mathcal{P}_D} (x - P(\tau_Q)) \in \mathbb{Q}[x].$$

Another polynomial related to partitions

Letting $\mathcal{P}_D$ denote the set of primitive forms in $\mathcal{Q}_D$ (i.e., $\gcd(a,b,c)=1$), define

$$\widehat{H}_D(x) := \prod_{Q\in\mathcal{P}_D} (x - P(\tau_Q)) \in \mathbb{Q}[x].$$

Question (Bruinier-Ono-Sutherland): Is this irreducible over $\mathbb{Q}$?

Another polynomial related to partitions

Letting $\mathcal{P}_D$ denote the set of primitive forms in $\mathcal{Q}_D$ (i.e., $\gcd(a,b,c)=1$), define

$$\widehat{H}_D(x) := \prod_{Q\in\mathcal{P}_D} (x - P(\tau_Q)) \in \mathbb{Q}[x].$$

Question (Bruinier-Ono-Sutherland): Is this irreducible over $\mathbb{Q}$?

Theorem (M.-Rolen, 2015)

The polynomial $\widehat{H}_D(x)$ is irreducible over $\mathbb{Q}$. Moreover we have that Ω_t, the ring class field of the order of conductor t in $K := \mathbb{Q}(\sqrt{d})$, is exactly the splitting field of $\widehat{H}_D(x)$ over K.

Table of Contents

Non-holomorphic modular functions

Define

$$F(\tau) := \frac{E_2(\tau) - 2E_2(2\tau) - 3E_2(3\tau) + 6E_2(6\tau)}{2\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2}$$

$$= q^{-1} - 10 - 29q - 104q^2 - \ldots \in M^!_{-2}(\Gamma_0(6))$$

and

$$P(\tau) := R_{-2}(F)(\tau) = \left(\frac{1}{2\pi i}\frac{\partial}{\partial\tau} - \frac{(-2)}{4\pi\,\mathrm{Im}(\tau)}\right)F(\tau).$$

Non-holomorphic modular functions

Define

$$F(\tau) := \frac{E_2(\tau) - 2E_2(2\tau) - 3E_2(3\tau) + 6E_2(6\tau)}{2\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2}$$

$$= q^{-1} - 10 - 29q - 104q^2 - \ldots \in M^!_{-2}(\Gamma_0(6))$$

and

$$P(\tau) := R_{-2}(F)(\tau) = \left(\frac{1}{2\pi i}\frac{\partial}{\partial\tau} - \frac{(-2)}{4\pi\,\mathrm{Im}(\tau)}\right) F(\tau).$$

Write $P = A + B \cdot C$ with

- $A(\tau)$, $B(\tau)$ explicit meromorphic modular functions for $\Gamma_0(6)$,
- $C(\tau)$ is an explicit real-analytic modular function for $\mathrm{SL}_2(\mathbb{Z})$.

Singular moduli

Lemma

For every non-special discriminant $D < 0$ (i.e., $D \neq -3 \cdot \square$), there exists a (meromorphic) modular function M_D for $\Gamma_0(6)$ such that

$$P(\tau_Q) = M_D(\tau_Q)$$

for all quadratic forms Q of discriminant D.

Singular moduli

Lemma

For every non-special discriminant $D < 0$ (i.e., $D \neq -3 \cdot \square$), there exists a (meromorphic) modular function M_D for $\Gamma_0(6)$ such that

$$P(\tau_Q) = M_D(\tau_Q)$$

for all quadratic forms Q of discriminant D.

Proof.

- Consider the modular polynomial $\Phi_{-D}(x, y) \in \mathbb{Z}[x, y]$ defined by $\Phi_{-D}(j(\tau), y) := \prod_{M \in \mathcal{V}_{-\mathcal{D}}} (y - j(M\tau))$.

$\square$

Singular moduli

Lemma

For every non-special discriminant $D < 0$ (i.e., $D \neq -3 \cdot \square$), there exists a (meromorphic) modular function M_D for $\Gamma_0(6)$ such that

$$P(\tau_Q) = M_D(\tau_Q)$$

for all quadratic forms Q of discriminant D.

Proof.

- Consider the modular polynomial $\Phi_{-D}(x, y) \in \mathbb{Z}[x, y]$ defined by $\Phi_{-D}(j(\tau), y) := \prod_{M \in \mathcal{V}_{-D}} (y - j(M\tau))$.
- Write

$$\Phi_{-D}(x, y) =: \sum_{\mu,\nu} \beta_{\mu,\nu}(\tau_Q)(x - j(\tau_Q))^{\mu}(y - j(\tau_Q))^{\nu}.$$

$\square$

Singular moduli

Lemma

For every non-special discriminant $D < 0$ (i.e., $D \neq -3 \cdot \square$), there exists a (meromorphic) modular function M_D for $\Gamma_0(6)$ such that

$$P(\tau_Q) = M_D(\tau_Q)$$

for all quadratic forms Q of discriminant D.

Proof.

- Consider the modular polynomial $\Phi_{-D}(x, y) \in \mathbb{Z}[x, y]$ defined by $\Phi_{-D}(j(\tau), y) := \prod_{M \in \mathcal{V}_{-D}} (y - j(M\tau))$.
- Write

$$\Phi_{-D}(x, y) =: \sum_{\mu,\nu} \beta_{\mu,\nu}(\tau_Q)(x - j(\tau_Q))^{\mu}(y - j(\tau_Q))^{\nu}.$$

- Write $C(\tau_Q)$ in terms of $\beta_{\mu,\nu}(\tau_Q)$ (Masser's formula). $\square$

Table of Contents

Definition

Let $N \in \mathbb{N}$ and $D = t^2 d < 0$ be a discriminant, with $t \in \mathbb{N}$ and d a fundamental discriminant. Moreover, let $\{Q_1, ..., Q_r\}$ $(Q_j(x, y) = a_j x^2 + b_j xy + c_j y^2)$ be a system of representatives of primitive quadratic forms modulo $\mathrm{SL}_2(\mathbb{Z})$. We call the set $\{Q_1, ..., Q_r\}$ an N-system mod t if the conditions

$$\gcd(c_j, N) = 1 \quad \text{and} \quad b_j \equiv b_\ell \pmod{N},\ 1 \leq j, \ell \leq r$$

are satisfied.

N-systems and Galois orbits

Theorem (Schertz, 2002)

Let g be a modular function for $\Gamma_0(N)$ for some $N \in \mathbb{N}$ whose Fourier coefficients at all cusps lie in the Nth cyclotomic field. Suppose furthermore that $g(\tau)$ and $g(-\frac{1}{\tau})$ have rational Fourier coefficients, and let $Q(x,y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant $D = t^2 d$, d a fundamental discriminant, with $\gcd(c, N) = 1$ and $N|a$. Then we have that $g(\tau_Q) \in \Omega_t$ unless g has a pole at τ_Q.
Moreover, if $\{Q = Q_1, ..., Q_h\}$ is an N-system mod t, then

$$\{g(\tau_{Q_1}), ..., g(\tau_{Q_h}\} = \{\sigma(g(\tau_{Q_1})) \, : \, \sigma \in \mathrm{Gal}_D\}$$

where Gal_D denotes the Galois group of $\Omega_t/\mathbb{Q}(\sqrt{d})$.

$\widehat{H}_D(x)$ is a perfect power

Proposition

Let P be as in as in the introduction, $D = -24n + 1 = t^2 d$ with d a fundamental discriminant. Then $P(\tau_{Q_0}) \in \Omega_t$ and

$$\{P(\tau_Q) \,:\, Q \in \mathcal{P}_D\} = \{\sigma(P(\tau_{Q_0})) \,:\, \sigma \in \mathrm{Gal}_D\}$$

for all $Q_0 \in \mathcal{P}_D$. In particular, the values $P(\tau_Q)$ for $Q \in \mathcal{P}_D$ generate the ring class field Ω_t over $\mathbb{Q}(\sqrt{d})$ and $\widehat{H}_D(x)$ is a perfect power of an irreducible polynomial.

$\widehat{H}_D(x)$ has only simple zeros I

Lemma

Let γ be a one of 12 representatives of $\Gamma_0(6)/\operatorname{SL}_2(\mathbb{Z})$ and assume that

$$F|_{-2}\gamma(\tau) = h\zeta q^{-\frac{1}{h}} + a_0 + a_1 q^{\frac{1}{h}} + ...,$$

where h is the width of the cusp $\gamma\infty$ and ζ is a certain 6th root of unity. Then, for every γ and $\tau \in \mathcal{F}$ (usual fundamental domain of $\operatorname{SL}_2(\mathbb{Z})$), we have

$$P|_0\gamma(\tau) = \zeta\left(1 - \frac{h}{2\pi \operatorname{Im}(\tau)}\right)e^{-\frac{2\pi i\tau}{h}} + E_\gamma(\tau),$$

where the error E_γ satisfies the uniform bound $|E_\gamma(\tau)| \leq \kappa := 1334.42$.

$\widehat{H}_D(x)$ has only simple zeros II

- $Q(x,y) = ax^2 + bxy + cy^2 =: [a,b,c]$ $\mathrm{SL}_2(\mathbb{Z})$-reduced quadratic form of discriminant $D = 1 - 24n$.

$\widehat{H}_D(x)$ has only simple zeros II

- $Q(x,y) = ax^2 + bxy + cy^2 =: [a,b,c]$ $\mathrm{SL}_2(\mathbb{Z})$-reduced quadratic form of discriminant $D = 1 - 24n$.
- Exactly one γ_Q as in Lemma satisfies $Q \circ \gamma_Q^{-1} \in \mathcal{P}_D$.

$\widehat{H}_D(x)$ has only simple zeros II

- $Q(x,y) = ax^2 + bxy + cy^2 =: [a,b,c]$ $\mathrm{SL}_2(\mathbb{Z})$-reduced quadratic form of discriminant $D = 1 - 24n$.
- Exactly one γ_Q as in Lemma satisfies $Q \circ \gamma_Q^{-1} \in \mathcal{P}_D$.
- Define $h_Q \in \{1,2,3,6\}$ and ζ_Q a 6^{th} root of unity by

$$F|_{-2}\gamma_Q(\tau) = h_Q \zeta_Q q^{-\frac{1}{h_Q}} + O(1).$$

$\widehat{H}_D(x)$ has only simple zeros II

- $Q(x,y) = ax^2 + bxy + cy^2 =: [a,b,c]$ $\mathrm{SL}_2(\mathbb{Z})$-reduced quadratic form of discriminant $D = 1 - 24n$.
- Exactly one γ_Q as in Lemma satisfies $Q \circ \gamma_Q^{-1} \in \mathcal{P}_D$.
- Define $h_Q \in \{1,2,3,6\}$ and ζ_Q a 6^{th} root of unity by

$$F|_{-2}\gamma_Q(\tau) = h_Q \zeta_Q q^{-\frac{1}{h_Q}} + O(1).$$

- Notice that $a \cdot h_Q \equiv 0 \pmod 6$, focus on $a \cdot h_Q = 12$.

$\widehat{H}_D(x)$ has only simple zeros II

- $Q(x,y) = ax^2 + bxy + cy^2 =: [a,b,c]$ $\mathrm{SL}_2(\mathbb{Z})$-reduced quadratic form of discriminant $D = 1 - 24n$.
- Exactly one γ_Q as in Lemma satisfies $Q \circ \gamma_Q^{-1} \in \mathcal{P}_D$.
- Define $h_Q \in \{1,2,3,6\}$ and ζ_Q a 6^{th} root of unity by

$$F|_{-2}\gamma_Q(\tau) = h_Q \zeta_Q q^{-\frac{1}{h_Q}} + O(1).$$

- Notice that $a \cdot h_Q \equiv 0 \pmod 6$, focus on $a \cdot h_Q = 12$.

Q	γ_Q	h_Q	ζ_Q	φ_Q
$[2,-1,3n]$	$\gamma_{0,0}$	6	1	$-\frac{\pi}{12}$
$[4,1,\frac{3n}{2}]$	$\gamma_{\frac{1}{2},1}$	3	ζ_6	$\frac{5\pi}{12}$
$[6,-5,n+1]$	$\gamma_{\frac{1}{3},0}$	2	1	$-\frac{5\pi}{12}$
$[12,1,\frac{n}{2}]$	γ_∞	1	1	$\frac{\pi}{12}$

Table: Quadratic forms with $a \cdot h_Q = 12$ for n even

$\widehat{H}_D(x)$ has only simple zeros III

- From estimates in Lemma: For $n \geq 54$ we have

$$|P|\gamma_{Q_1}(\tau_{Q_1})| \neq |P|\gamma_{Q_2}(\tau_{Q_2})|$$

for $h_{Q_1}a_1 = 12 \neq h_{Q_2}a_2$ and

$$\arg(P|\gamma_{Q_1}(\tau_{Q_1})) \neq \arg(P|\gamma_{Q_2}(\tau_{Q_2}))$$

for $h_{Q_1}a_1 = 12 = h_{Q_2}a_2$.

General theorem

Theorem (Braun-Buck-Girsch, 2015)

Let $F \in M^!_{-2k}(\mathrm{SL}_2(\mathbb{Z}))$ with rational Fourier coefficients and define the non-holomorphic modular function P by applying the Maaß raising operator k times to F and define for each fundamental discriminant $D < 0$ the polynomial

$$\widehat{H}_{D,F} := \prod_{Q \in \mathcal{P}_D} (x - P(\tau_Q)) \in \mathbb{Q}[x].$$

Then $\widehat{H}_{D,F}(x)$ is irreducible over $\mathbb{Q}$ for sufficiently large D (bound explicit, depends on the principal part of F).

Thank you for your attention.