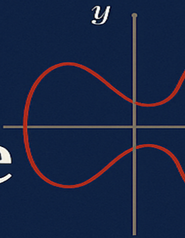
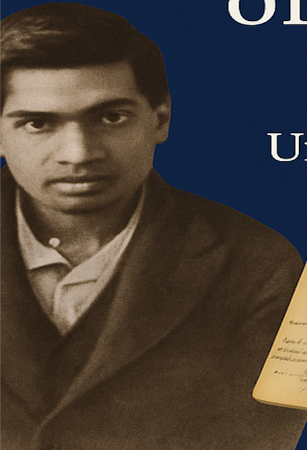
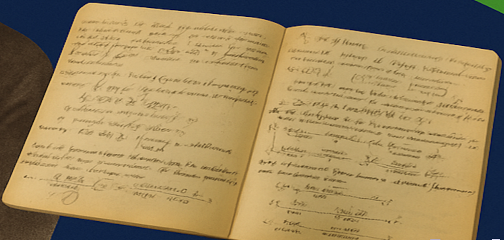
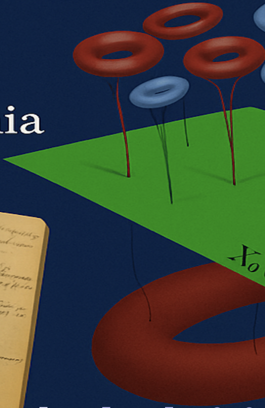


The secret Life of partitions

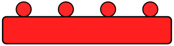
Ken Ono
University of Virginia



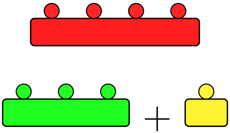




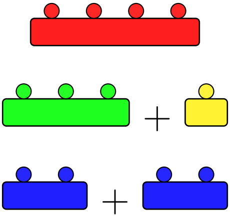
A universe based on **child's play**



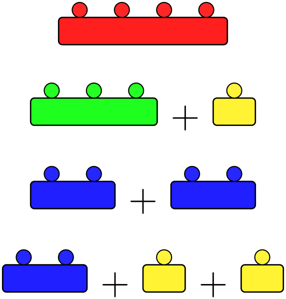
A universe based on **child's play**



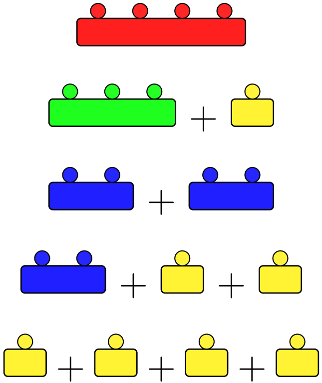
A universe based on **child's play**



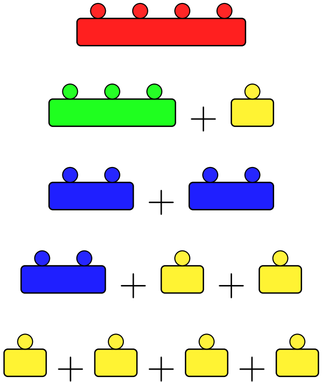
A universe based on child's play



A universe based on child's play



A universe based on child's play



We say that $p(4) = 5$.

A universe based on **child's play**

One easily sees that

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1,$$

A UNIVERSE BASED ON **child's play**

One easily sees that

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1,$$

and so we say that

$$p(5) = 7.$$

Can we count the "uncountable"?

- $p(2) = 2$
- $p(4) = 5$
- $p(8) = 22$
- $p(16) = 231$
- $p(32) = 8349$
- $p(64) = 1741630$
- $p(128) = 4351078600$
- $p(256) = 365749566870782$
- $p(512) = 4453575699570940947378$

Can we count the "uncountable"?

- $p(2) = 2$
- $p(4) = 5$
- $p(8) = 22$
- $p(16) = 231$
- $p(32) = 8349$
- $p(64) = 1741630$
- $p(128) = 4351078600$
- $p(256) = 365749566870782$
- $p(512) = 4453575699570940947378$

I dare you to count $p(200)$!

Why do partitions matter?

Why do partitions matter?

- **Modular & automorphic forms** - generating functions, congruences, Galois representations and the "circle method".
- **Symmetric functions & representation theory** - Young diagrams, Schur/Hall-Littlewood bases, hook-length formula, Frobenius characteristic, S_n characters,...
- ***q*-series & identities** - Rogers-Ramanujan, Andrews-Gordon, Bailey chains, product-sum transformations,...
- **Geometry & physics** - Hilbert schemes of points, Donaldson/Gromov-Witten/BPS state counts, VOA/partition functions in topological strings.
- **Probability & statistical mechanics** - Plancherel measure and limit shapes, plane partitions, Bose-Einstein combinatorics.

Leonhard Euler's "recurrence"

Theorem (Euler (1700s))

We have that

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - \dots.$$

LEONHARD EULER'S "RECURRENCE"

THEOREM (EULER (1700S))

We have that

$$p(n) = p(n-1)+p(n-2)-p(n-5)-p(n-7)+p(n-12)+p(n-15)-\ldots.$$

REMARK

The first 200 values were famously computed this way in 1915.

$$1, 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, 135, 176, \\ 231, 297, \ldots\ldots\ldots\ldots, p(200) = 3972999029388.$$

Hardy-Ramanujan Theorem (1918)

For large n, we have

$$p(n) \sim \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{2n/3}}.$$

Hardy-Ramanujan Theorem (1918)

For large n, we have

$$p(n) \sim \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{2n/3}}.$$

Remark ("Circle Method")

Based on Cauchy's Integral Formula.

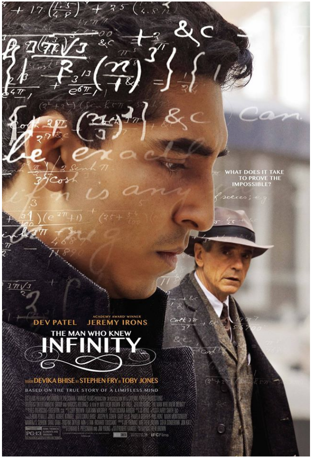
Hardy-Ramanujan Theorem (1918)

For large n, we have

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$

Remark ("Circle Method")

Based on Cauchy's Integral Formula.



This means....

If we let $\text{Approx}(n) := \frac{1}{4n\sqrt{3}} \cdot e^{\pi\sqrt{2n/3}}$, then we have

This means....

If we let $\text{Approx}(n) := \frac{1}{4n\sqrt{3}} \cdot e^{\pi\sqrt{2n/3}}$, then we have

n	$p(n)$	$\text{Approx}(n)$	$\frac{\text{Approx}(n)}{p(n)}$
10	42	48.104...	1.145...
20	627	692.384...	1.104...
30	5604	6080.435...	1.085...
40	37338	40080.080...	1.073...
50	204226	217590.501...	1.065...
$\vdots$	$\vdots$	$\vdots$	$\vdots$
∞	∞	∞	1

Rademacher's "Epiphany"

Theorem (Rademacher (1943))

If n is a positive integer, then

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

Rademacher's "Epiphany"

Theorem (Rademacher (1943))

If n is a positive integer, then

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

Remark

Perfectly good integers expressed as infinite convergent sums.

Example (First 10 approximations for $p(1) = 1$.)

N	$P_N(1)$
1	$1.13355\ldots$
2	$1.00296\ldots$
3	$0.97318\ldots$
$\vdots$	$\vdots$
8	$1.00528\ldots$
9	$1.00633\ldots$
10	$1.00633\ldots$

Example (First 10 approximations for $p(1) = 1$.)

N	$P_N(1)$
1	1.13355 ...
2	1.00296 ...
3	0.97318 ...
$\vdots$	$\vdots$
8	1.00528 ...
9	1.00633 ...
10	1.00633 ...

The 10th approximation is **worse** than the 2nd!

Example (First 10 approximations for $p(1) = 1$.)

N	$P_N(1)$
1	$1.13355\ldots$
2	$1.00296\ldots$
3	$0.97318\ldots$
$\vdots$	$\vdots$
8	$1.00528\ldots$
9	$1.00633\ldots$
10	$1.00633\ldots$

The 10th approximation is **worse** than the 2nd!

Question

But can we actually use this formula to prove new theorems?

A finite algebraic FORMULA

Theorem (Bruinier-O (2011))

There is an explicit **Maass function** $P(\tau)$ *on* $X_0(6)$ *for which*

$$p(n) = \frac{1}{24n-1} \cdot \left(P(\alpha_{n,1}) + P(\alpha_{n,2}) + \cdots + P(\alpha_{n,h_n})\right).$$

The numbers $P(\alpha_{n,m})$ *are* **algebraic**.

A **finite algebraic** FORMULA

THEOREM (BRUINIER-O (2011))

There is an explicit **Maass function** $P(\tau)$ *on* $X_0(6)$ *for which*

$$p(n) = \frac{1}{24n-1} \cdot \left(P(\alpha_{n,1}) + P(\alpha_{n,2}) + \cdots + P(\alpha_{n,h_n})\right).$$

The numbers $P(\alpha_{n,m})$ *are* **algebraic**.

REMARKS

(1) The α'*s are roots of* $h_n \sim \sqrt{n}$ *many* **quadratic equations**.

A finite algebraic FORMULA

THEOREM (BRUINIER-O (2011))

There is an explicit **Maass function** $P(\tau)$ *on* $X_0(6)$ *for which*

$$p(n) = \frac{1}{24n-1} \cdot \left(P(\alpha_{n,1}) + P(\alpha_{n,2}) + \cdots + P(\alpha_{n,h_n})\right).$$

The numbers $P(\alpha_{n,m})$ *are* **algebraic**.

REMARKS

(1) The α'*s are roots of* $h_n \sim \sqrt{n}$ *many* **quadratic equations**.

(2) (Brunier-O-Sutherland) **Efficiently** *compute* $p(n)$.

A finite algebraic FORMULA

THEOREM (BRUINIER-O (2011))

There is an explicit **Maass function** $P(\tau)$ *on* $X_0(6)$ *for which*

$$p(n) = \frac{1}{24n-1} \cdot \left(P(\alpha_{n,1}) + P(\alpha_{n,2}) + \cdots + P(\alpha_{n,h_n})\right).$$

The numbers $P(\alpha_{n,m})$ *are* **algebraic**.

REMARKS

(1) *The* α'*s are roots of* $h_n \sim \sqrt{n}$ *many* **quadratic equations**.

(2) *(Brunier-O-Sutherland)* **Efficiently** *compute* $p(n)$.

(3) *Proved using the method of "theta lifts".*

THE $p(1) = 1$ EXAMPLE.

If $\beta := 161529092 + 18648492\sqrt{69}$, then

$$\frac{1}{23} \cdot P\left(\frac{-1+\sqrt{-23}}{12}\right) = \frac{1}{3} + \frac{\beta^{2/3} + 127972}{6\beta^{1/3}},$$

$$\frac{1}{23} \cdot P\left(\frac{-13+\sqrt{-23}}{24}\right) = \frac{1}{3} - \frac{\beta^{2/3} + 127972}{12\beta^{1/3}} + \frac{\beta^{2/3} - 127972}{4\sqrt{-3}\beta^{1/3}},$$

$$\frac{1}{23} \cdot P\left(\frac{-25+\sqrt{-23}}{36}\right) = \frac{1}{3} - \frac{\beta^{2/3} + 127972}{12\beta^{1/3}} - \frac{\beta^{2/3} - 127972}{4\sqrt{-3}\beta^{1/3}},$$

The $p(1) = 1$ example.

If $\beta := 161529092 + 18648492\sqrt{69}$, then

$$\frac{1}{23} \cdot P\left(\frac{-1+\sqrt{-23}}{12}\right) = \frac{1}{3} + \frac{\beta^{2/3}+127972}{6\beta^{1/3}},$$

$$\frac{1}{23} \cdot P\left(\frac{-13+\sqrt{-23}}{24}\right) = \frac{1}{3} - \frac{\beta^{2/3}+127972}{12\beta^{1/3}} + \frac{\beta^{2/3}-127972}{4\sqrt{-3}\beta^{1/3}},$$

$$\frac{1}{23} \cdot P\left(\frac{-25+\sqrt{-23}}{36}\right) = \frac{1}{3} - \frac{\beta^{2/3}+127972}{12\beta^{1/3}} - \frac{\beta^{2/3}-127972}{4\sqrt{-3}\beta^{1/3}},$$

and we find that

$$p(1) = 1 = \frac{1}{23}\left(P(\alpha_1) + P(\alpha_2) + P(\alpha_3)\right).$$

THE MAASS FUNCTION $P(\tau)$

DEFINITION

In terms of Eisenstein series and Dedekind's eta-function, we let

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

The Maass Function $P(\tau)$

Definition

In terms of Eisenstein series and Dedekind's eta-function, we let

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

Then the **Maass function** $P(\tau)$ is defined by

$$P(\tau) \;=\; -\frac{1}{2\pi i}\,\frac{dF}{d\tau}(\tau) \;-\; \frac{1}{2\pi \mathrm{Im}(\tau)}\,F(\tau).$$

The Maass Function $P(\tau)$

Definition

In terms of Eisenstein series and Dedekind's eta-function, we let

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

Then the **Maass function** $P(\tau)$ is defined by

$$P(\tau) = -\frac{1}{2\pi i}\frac{dF}{d\tau}(\tau) - \frac{1}{2\pi \mathrm{Im}(\tau)}F(\tau).$$

Question

Can we actually use this finite formula to prove new theorems?

Conceptual lens?

Question

A conceptual way to interpret the Bruinier–O formula?

Conceptual lens?

Question

A conceptual way to interpret the Bruinier–O formula?

1. *What do the CM points* $\alpha_{n,1}, \alpha_{n,2}, \ldots, \alpha_{n,h_n}$ *represent?*

Conceptual lens?

Question

A conceptual way to interpret the Bruinier–O formula?

1. *What do the CM points* $\alpha_{n,1}, \alpha_{n,2}, \ldots, \alpha_{n,h_n}$ *represent?*
2. *What is the "meaning" of the summands in the formula*

$$p(n) = \frac{1}{24n-1}\left(P(\alpha_{n,1}) + P(\alpha_{n,2}) + \cdots + P(\alpha_{n,h_n})\right) ?$$

Conceptual lens?

Question

A conceptual way to interpret the Bruinier–O formula?

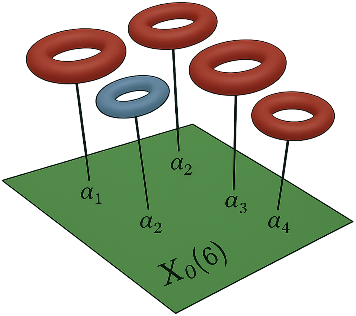
1. *What do the CM points* $\alpha_{n,1}, \alpha_{n,2}, \ldots, \alpha_{n,h_n}$ *represent?*
2. *What is the "meaning" of the summands in the formula*

$$p(n) = \frac{1}{24n-1}\left(P(\alpha_{n,1}) + P(\alpha_{n,2}) + \cdots + P(\alpha_{n,h_n})\right) \text{ ?}$$

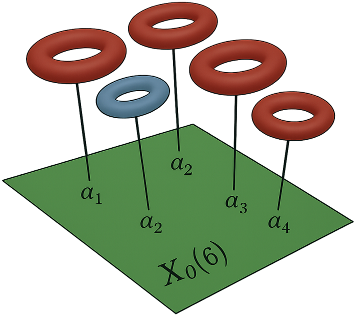
Answer

Elliptic curve moduli.

A CARTOON



A CARTOON



$$\mathbb{T}^2 \cong E(\mathbb{C})$$

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots\} \subset X_0(6)$$

What are $P(\alpha_{n,1}), P(\alpha_{n,2}), \ldots$?

What is $X_0(6)$? (Moduli viewpoint)

- **Elliptic curve over** $\mathbb{C} \cong$ a torus $\mathbb{C}/\Lambda$ (a lattice $\Lambda \subset \mathbb{C}$).

WHAT IS $X_0(6)$? (MODULI VIEWPOINT)

- **Elliptic curve over** $\mathbb{C} \cong$ a torus $\mathbb{C}/\Lambda$ (a lattice $\Lambda \subset \mathbb{C}$).
- **Level-6 structures**: These are pairs (E, C) with *cyclic subgroup*

$$C \leq E[6] \text{ cyclic of order 6.}$$

What is $X_0(6)$? (Moduli viewpoint)

- **Elliptic curve over** $\mathbb{C} \cong$ a torus $\mathbb{C}/\Lambda$ (a lattice $\Lambda \subset \mathbb{C}$).
- **Level-6 structures**: These are pairs (E, C) with *cyclic subgroup*

$$C \leq E[6] \text{ cyclic of order } 6.$$

- **Isomorphism rule:** $(E, C) \sim (E', C')$ if there is an isomorphism $\phi : E \to E'$ with $\phi(C) = C'$.

What is $X_0(6)$? (Moduli viewpoint)

- **Elliptic curve over** $\mathbb{C} \;\cong\;$ a torus $\mathbb{C}/\Lambda$ (a lattice $\Lambda \subset \mathbb{C}$).
- **Level-6 structures**: These are pairs (E, C) with *cyclic subgroup*

$$C \leq E[6] \text{ cyclic of order 6.}$$

- **Isomorphism rule:** $(E, C) \sim (E', C')$ if there is an isomorphism $\phi : E \to E'$ with $\phi(C) = C'$.
- **Moduli Space.**

$$\{\; X_0(6)(\mathbb{C}) \;\longleftrightarrow\; \{\text{isomorphism classes of pairs } (E, C)\}.$$

WHAT IS $X_0(6)$? (MODULI VIEWPOINT)

- **Elliptic curve over** $\mathbb{C} \cong$ a torus $\mathbb{C}/\Lambda$ (a lattice $\Lambda \subset \mathbb{C}$).
- **Level-6 structures**: These are pairs (E, C) with *cyclic subgroup*

$$C \leq E[6] \text{ cyclic of order } 6.$$

- **Isomorphism rule:** $(E, C) \sim (E', C')$ if there is an isomorphism $\phi : E \to E'$ with $\phi(C) = C'$.
- **Moduli Space.**

$$\{ \ X_0(6)(\mathbb{C}) \ \longleftrightarrow \ \{\text{isomorphism classes of pairs } (E, C)\}.$$

- **Forgetting the level:** Forgetting C, we have the map

$$j : \ X_0(6) \longrightarrow X(1) \qquad (E, C) \longmapsto j(E).$$

What do the CM points α represent?

Moduli meaning on $X_0(6)$

(1) We have that

$$\alpha \in X_0(6)(\mathbb{C}) \iff [(E, C)] \text{ with } C \subset E[6] \text{ cyclic of order 6.}$$

What do the CM points α represent?

Moduli meaning on $X_0(6)$

(1) We have that

$$\alpha \in X_0(6)(\mathbb{C}) \iff [(E, C)] \text{ with } C \subset E[6] \text{ cyclic of order } 6.$$

(2) We have that

$$\alpha \text{ is } CM \iff \mathrm{End}(E) \cong \mathcal{O}_D \text{ (an imaginary quadratic order).}$$

What do the CM points α represent?

Moduli meaning on $X_0(6)$

(1) We have that

$$\alpha \in X_0(6)(\mathbb{C}) \iff [(E, C)] \text{ with } C \subset E[6] \text{ cyclic of order } 6.$$

(2) We have that

$$\alpha \text{ is } CM \iff \mathrm{End}(E) \cong \mathcal{O}_D \text{ (an imaginary quadratic order).}$$

Remarks ($D := 1 - 24n$)

(1) For $D < 0$, the CM points form a Heegner packet on $X_0(6)$.

What do the CM points α represent?

Moduli meaning on $X_0(6)$

(1) We have that

$$\alpha \in X_0(6)(\mathbb{C}) \iff [(E, C)] \text{ with } C \subset E[6] \text{ cyclic of order 6.}$$

(2) We have that

$$\alpha \text{ is } CM \iff \mathrm{End}(E) \cong \mathcal{O}_D \text{ (an imaginary quadratic order).}$$

Remarks ($D := 1 - 24n$)

(1) For $D < 0$, the CM points form a Heegner packet on $X_0(6)$.

(2) The α's are those moduli points $[(E, C)]$ where E has complex multiplication by $\mathcal{O}_D$.

What's the deal with $P(\tau)$?

What's the deal with $P(\tau)$?

Problem

Is it a problem that $P(\tau)$ is a Maass function which **does not** *arise in arithmetic geometry?*

What's the deal with $P(\tau)$?

Problem

Is it a problem that $P(\tau)$ is a Maass function which **does not** *arise in arithmetic geometry?*

Theorem (O, 2025)

For each n, there is a modular function $F_n(\tau)$ on $X_0(6)$ such that, for the CM points $\{\alpha_{n,1}, \ldots, \alpha_{n,h_n}\}$, we have

$$F_n(\alpha_{n,j}) = P(\alpha_{n,j}) \qquad \textit{for all } j.$$

Sketch of the Proof.

1. Work on $X_0(6)$, which has genus zero, so modular functions are just rational functions in a single Hauptmodul.

Sketch of the Proof.

1. Work on $X_0(6)$, which has genus zero, so modular functions are just rational functions in a single Hauptmodul.
2. Prescribe the cusp behavior to match the growth of the Maass function P (after the standard scaling).

Sketch of the Proof.

1. Work on $X_0(6)$, which has genus zero, so modular functions are just rational functions in a single Hauptmodul.
2. Prescribe the cusp behavior to match the growth of the Maass function P (after the standard scaling).
3. The CM values of P are determined by holomorphic data its values on each CM packet are algebraic and Galois-stable.

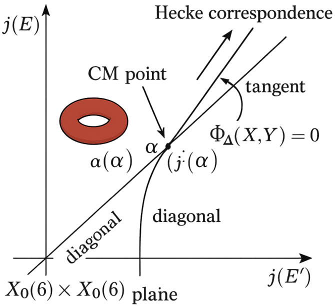
Sketch of the Proof.

1. Work on $X_0(6)$, which has genus zero, so modular functions are just rational functions in a single Hauptmodul.
2. Prescribe the cusp behavior to match the growth of the Maass function P (after the standard scaling).
3. The CM values of P are determined by holomorphic data its values on each CM packet are algebraic and Galois-stable.
4. Interpolate: A unique rational function with the chosen cusp divisor hits those CM values.

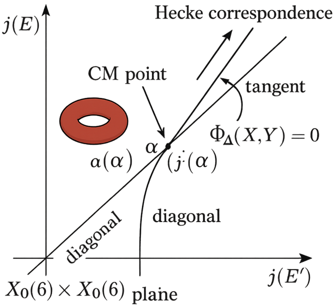
Sketch of the Proof.

1. Work on $X_0(6)$, which has genus zero, so modular functions are just rational functions in a single Hauptmodul.
2. Prescribe the cusp behavior to match the growth of the Maass function P (after the standard scaling).
3. The CM values of P are determined by holomorphic data its values on each CM packet are algebraic and Galois-stable.
4. Interpolate: A unique rational function with the chosen cusp divisor hits those CM values.
5. This gives F_n. $\square$

CM values as tangents



CM values as tangents

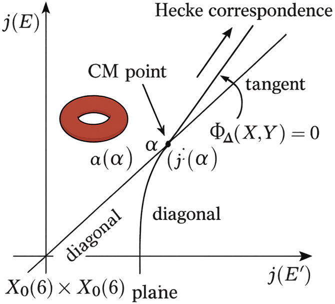


Theorem (CM tangent (O))

If $J = j(\alpha_Q)$ and $\Phi_{\Delta_n}(X,Y)$ is the modular polynomial, then

$$P(\alpha_Q) = -D_{-2}F(\alpha_Q) + \frac{1}{6}F(\alpha_Q)\left.\frac{\Phi_{YY}-\Phi_{XY}}{\Phi_Y}\right|_{(J,J)}.$$

CM values as tangents



Theorem (CM tangent (O))

If $J = j(\alpha_Q)$ and $\Phi_{\Delta_n}(X,Y)$ is the modular polynomial, then

$$P(\alpha_Q) \;=\; -D_{-2}F(\alpha_Q) + \frac{1}{6}F(\alpha_Q)\left.\frac{\Phi_{YY}-\Phi_{XY}}{\Phi_Y}\right|_{(J,J)}.$$

Remark

The Maass value $P(\alpha_Q)$ is essentially the tangent of the Hecke correspondence along the diagonal at (J,J) in $X_0(1)\times X_0(1)$.

New arithmetic formula for $p(n)$

Theorem (O (2025))

If $\Delta = 1 - 24n < 0$ *and* $\mathcal{A}_\Delta$ *is the CM packet on* $X_0(6)$*, then*

$$p(n) \;=\; \frac{1}{24n-1} \sum_{\alpha \in \mathcal{A}_\Delta} \text{“Diagonal tangent slopes”.}$$

New arithmetic formula for $p(n)$

Theorem (O (2025))

If $\Delta = 1 - 24n < 0$ *and* $\mathcal{A}_\Delta$ *is the CM packet on* $X_0(6)$*, then*

$$p(n) = \frac{1}{24n-1} \sum_{\alpha \in \mathcal{A}_\Delta} \text{“Diagonal tangent slopes”}.$$

Remark

We can and will use this formula to prove new theorems!

Yin and Yang

That was the "Yin" part of the story of $p(n)$.

Yin and Yang

That was the "Yin" part of the story of $p(n)$.

Turning to the "Yang"...

How often is $p(n)$ even?

How often is $p(n)$ even?

Let $\text{Prop}_2(N) :=$ proportion of the first N values that are even.

N	$\text{Prop}_2(N)$
200,000	0.5012...
600,000	0.5000...
1,000,000	0.5004...
∞	$\frac{1}{2}$?

How often is $p(n)$ even?

Let $\text{Prop}_2(N)$:= proportion of the first N values that are even.

N	$\text{Prop}_2(N)$
200,000	0.5012...
600,000	0.5000...
1,000,000	0.5004...
∞	$\frac{1}{2}$?

Conjecture

Half of the partition numbers are even.

How often is $p(n)$ a multiple of 3?

N	$\text{Prop}_3(N)$
800	0.334...
1,600	0.314...
2,400	0.319...
3,200	0.331...
$\vdots$	$\vdots$

How often is $p(n)$ a multiple of 3?

N	$\mathrm{Prop}_3(N)$
800	$0.334\ldots$
1,600	$0.314\ldots$
2,400	$0.319\ldots$
3,200	$0.331\ldots$
$\vdots$	$\vdots$

Conjecture

One third of the partition numbers are multiples of 3.

How often is $p(n)$ a multiple of 5?

How often is $p(n)$ a multiple of 5?

N	$\mathrm{Prop}_5(N)$
500	0.336...
1,000	0.342...
1,500	0.348...
2,000	0.346...
$\vdots$	$\vdots$

How often is $p(n)$ a multiple of 5?

N	$\text{Prop}_5(N)$
500	0.336...
1,000	0.342...
1,500	0.348...
2,000	0.346...
$\vdots$	$\vdots$

Question

What the heck?

Ramanujan's Theorem

Theorem (Ramanujan (1915))

For every n we have

$$\begin{aligned} p(5n+4) &\text{ is a multiple of } 5,\\ p(7n+5) &\text{ is a multiple of } 7,\\ p(11n+6) &\text{ is a multiple of } 11. \end{aligned}$$

A tantalyzing and enigmatic quote

"I have proved... that

$$p(5n+4) \equiv 0 \pmod{5},$$
$$p(7n+5) \equiv 0 \pmod{7},$$
$$p(11n+6) \equiv 0 \pmod{11}.$$

There appear to be **corresponding properties** *in which the moduli are powers of 5, 7, or 11..., and* **no simple properties** *for any moduli involving primes other than these three."*

Ramanujan (1919)

"Corresponding properties"

Ramanujan, Watson (1938), and Atkin (1967) proved:

Theorem (Ramanujan's Congruences)

If $1 \leq \delta_\ell(m) < \ell^m$ *satisfies* $24\delta_\ell(m) \equiv 1 \pmod{\ell^m}$, *then*

$$p(5^m n + \delta_5(m)) \equiv 0 \pmod{5^m},$$
$$p(7^m n + \delta_7(m)) \equiv 0 \pmod{7^{\lfloor \frac{m+2}{2} \rfloor}},$$
$$p(11^m n + \delta_{11}(m)) \equiv 0 \pmod{11^m}.$$

Mystery

Question

What did Ramanujan mean when he said

"...and no simple properties for any moduli involving primes other than these three (5,7,11)" ?

Mystery

Question

What did Ramanujan mean when he said

"...and no simple properties for any moduli involving primes other than these three (5,7,11)" ?

Theorem (Radu, 2011)

There are no arithmetic progressions $An + B$ for which

$$p(An + B) \equiv 0 \pmod 2 \quad \text{or} \quad p(An + B) \equiv 0 \pmod 3.$$

More on the mystery

Theorem (Ahlgren and Boylan, 2005)

The only (ℓ, a) *for which*

$$p(\ell n + a) \equiv 0 \pmod{\ell},$$

are $(5, 4), (7, 5),$ *and* $(11, 6)$.

Not so **simple** properties

Theorem (O, 2000)

For primes $Q \geq 5$, there are **infinitely many** *progressions $An + B$ for which*

$$p(An+B) \equiv 0 \pmod{Q}.$$

NOT SO **simple** PROPERTIES

THEOREM (O, 2000)

For primes $Q \geq 5$, there are **infinitely many** *progressions $An + B$ for which*

$$p(An + B) \equiv 0 \pmod{Q}.$$

Examples. For example, we have:

$$p(48037937n + 1122838) \equiv 0 \pmod{17},$$
$$p(1977147619n + 815655) \equiv 0 \pmod{19},$$
$$p(14375n + 3474) \equiv 0 \pmod{23},$$
$$p(348104768909n + 43819835) \equiv 0 \pmod{29},$$
$$p(4063467631n + 30064597) \equiv 0 \pmod{31}.$$

Supersingular (E, C)

Definition (Supersingularity)

Let k be a field of char $p > 0$. An elliptic curve E/k is *supersingular* if $E[p](\overline{k}) = \{0\}$.

Supersingular (E, C)

Definition (Supersingularity)

Let k be a field of char $p > 0$. An elliptic curve E/k is *supersingular* if $E[p](\overline{k}) = \{0\}$.

Deuring reduction for CM

If $E/\mathbb{C}$ have CM by a $\mathcal{O}_{-D}$ and $\left(\frac{-D}{p}\right) \in \{0, -1\}$, then $\overline{E}$ is supersingular.

Supersingular (E, C)

Definition (Supersingularity)

Let k be a field of char $p > 0$. An elliptic curve E/k is *supersingular* if $E[p](\overline{k}) = \{0\}$.

Deuring reduction for CM

If $E/\mathbb{C}$ have CM by a $\mathcal{O}_{-D}$ and $\left(\frac{-D}{p}\right) \in \{0, -1\}$, then $\overline{E}$ is supersingular.

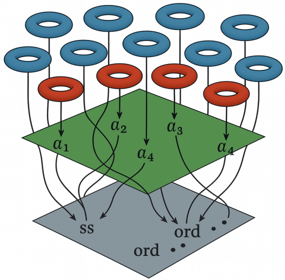


Illustration of CM points descending to the ordinary/supersingular layers.

UNIVERSAL MOD ℓ CONGRUENCE ($\ell \geq 5$)

THEOREM (O (2025))

If $\ell \geq 5$ is prime and $\left(\frac{\Delta_n}{\ell}\right) = -1$, then

$$p(n) \equiv -\frac{1}{\Delta_n} \sum_{(E,C) \in SS_\ell(6)} h_{\Delta_n}(E,C) \cdot P^{(\ell)}(E,C) \pmod{\ell},$$

Universal mod ℓ congruence ($\ell \geq 5$)

Theorem (O (2025))

If $\ell \geq 5$ is prime and $\left(\frac{\Delta_n}{\ell}\right) = -1$, then

$$p(n) \equiv -\frac{1}{\Delta_n} \sum_{(E,C) \in SS_\ell(6)} h_{\Delta_n}(E,C) \cdot P^{(\ell)}(E,C) \pmod{\ell},$$

where $SS_\ell(6)$ is the supersingular locus of $X_0(6)$ in char ℓ and

$h_{\Delta_n}(E,C) := \#\{$oriented optimal embeddings of $\mathcal{O}_{\Delta_n} \mapsto \mathrm{End}(E,C).\}$

Congruences via CM tangents

Theorem (Ramanjan's Congruences)

For each integer $j \geq 1$ there exist residue classes $\beta_m(j)$ such that

$$p(5^j n + \beta_5(j)) \equiv 0 \pmod{5^j},$$
$$p(7^j n + \beta_7(j)) \equiv 0 \pmod{7^{\lfloor j/2 \rfloor + 1}},$$
$$p(11^j n + \beta_{11}(j)) \equiv 0 \pmod{11^j}.$$

Here each $\beta_m(j)$ is characterized by $24\,\beta_m(j) \equiv 1 \pmod{m^j}$.

Sketch of Proof Ramanujan's congruences

1. **Replace P by a modular function.** For each n, there is a modular function F_n on $X_0(6)$ with $F_n(\alpha) = P(\alpha)$ for every CM point α in the packet.

Sketch of Proof Ramanujan's congruences

1. **Replace P by a modular function.** For each n, there is a modular function F_n on $X_0(6)$ with $F_n(\alpha) = P(\alpha)$ for every CM point α in the packet.
2. **Potential issue.** A modular function can behave badly modulo ℓ (poles collide with the supersingular fiber, denominators vanish, etc.).

Sketch of Proof Ramanujan's congruences

1. **Replace P by a modular function.** For each n, there is a modular function F_n on $X_0(6)$ with $F_n(\alpha) = P(\alpha)$ for every CM point α in the packet.
2. **Potential issue.** A modular function can behave badly modulo ℓ (poles collide with the supersingular fiber, denominators vanish, etc.).
3. **Lucky primes $5, 7, 11$.** In characteristics $\ell = 5, 7, 11$ the supersingular j-invariants are *only* 0 and 1728. Therefore, we can normalize F_n so its reduction is well behaved on the supersingular fiber (i.e. $E_4(\rho) = E_6(i) = 0$.).

Sketch of Proof Ramanujan's congruences

1. **Replace P by a modular function.** For each n, there is a modular function F_n on $X_0(6)$ with $F_n(\alpha) = P(\alpha)$ for every CM point α in the packet.
2. **Potential issue.** A modular function can behave badly modulo ℓ (poles collide with the supersingular fiber, denominators vanish, etc.).
3. **Lucky primes $5, 7, 11$.** In characteristics $\ell = 5, 7, 11$ the supersingular j-invariants are *only* 0 and 1728. Therefore, we can normalize F_n so its reduction is well behaved on the supersingular fiber (i.e. $E_4(\rho) = E_6(i) = 0$.).
4. **Consequence.** We study F_n (hence P) modulo ℓ *entirely on the supersingular locus* of $X_0(6)$ without pathologies.

Sketch of Proof (continued)

5. Ramanujan's congruences have $\ell \mid \Delta_n$ which is ramification.

Sketch of Proof (continued)

5. Ramanujan's congruences have $\ell \mid \Delta_n$ which is ramification.
6. Then $P(\alpha_{n,j})$ correspond to supersingular $(E, C) \in X_0(6)$.

Sketch of Proof (continued)

5. Ramanujan's congruences have $\ell \mid \Delta_n$ which is ramification.
6. Then $P(\alpha_{n,j})$ correspond to supersingular $(E, C) \in X_0(6)$.
7. **CM $\rightarrow$ supersingular reduction.** The CM sum giving $-\Delta_n\, p(n)$ specializes to a sum over supersingular points

$$-\Delta_n\, p(n) = \sum_i \underbrace{h_{\Delta_n}(E_i, C_i)}_{\#\ \textbf{optimal embeddings}} \cdot \underbrace{P^{(\ell)}(E_i, C_i)}_{\text{reduced CM invariant}}$$

Sketch of Proof (continued)

5. Ramanujan's congruences have $\ell \mid \Delta_n$ which is ramification.
6. Then $P(\alpha_{n,j})$ correspond to supersingular $(E, C) \in X_0(6)$.
7. **CM $\to$ supersingular reduction.** The CM sum giving $-\Delta_n\, p(n)$ specializes to a sum over supersingular points

$$-\Delta_n\, p(n) = \sum_i \underbrace{h_{\Delta_n}(E_i, C_i)}_{\#\ \text{optimal embeddings}} \cdot \underbrace{P^{(\ell)}(E_i, C_i)}_{\text{reduced CM invariant}}$$

8. **U_ℓ-contraction + growth of *counts*.** Raising the conductor multiplies the **counts** by ℓ, while the Hecke operator U_ℓ contracts the invariant side modulo ℓ.

Sketch of Proof (continued)

5. Ramanujan's congruences have $\ell \mid \Delta_n$ which is ramification.
6. Then $P(\alpha_{n,j})$ correspond to supersingular $(E, C) \in X_0(6)$.
7. **CM → supersingular reduction.** The CM sum giving $-\Delta_n\, p(n)$ specializes to a sum over supersingular points

$$-\Delta_n\, p(n) = \sum_i \underbrace{h_{\Delta_n}(E_i, C_i)}_{\#\ \text{optimal embeddings}} \cdot \underbrace{P^{(\ell)}(E_i, C_i)}_{\text{reduced CM invariant}}$$

8. **U_ℓ-contraction + growth of *counts*.** Raising the conductor multiplies the **counts** by ℓ, while the Hecke operator U_ℓ contracts the invariant side modulo ℓ.
9. **Prime powers.** Combining the ℓ-fold growth of the **counts** with the U_ℓ-contraction yields the congruences. □

General Parity Conjecture

Conjecture (O)

If $f(x) \in \mathbb{Z}[x]$*, then the following are true:*

General Parity Conjecture

Conjecture (O)

If $f(x) \in \mathbb{Z}[x]$, then the following are true:
(1) There are infinitely many n for which $p(f(n))$ is even.

General Parity Conjecture

Conjecture (O)

If $f(x) \in \mathbb{Z}[x]$, then the following are true:
(1) There are infinitely many n for which $p(f(n))$ is even.

(2) There are infinitely many m for which $p(f(m))$ is odd.

General Parity Conjecture

Conjecture (O)

If $f(x) \in \mathbb{Z}[x]$*, then the following are true:*

(1) There are infinitely many n *for which* $p(f(n))$ *is even.*

(2) There are infinitely many m *for which* $p(f(m))$ *is odd.*

Remarks

1. (O $\oplus$ Radu) *True for* $\deg(f) = 1$.

General Parity Conjecture

Conjecture (O)

If $f(x) \in \mathbb{Z}[x]$*, then the following are true:*
(1) There are infinitely many n *for which* $p(f(n))$ *is even.*

(2) There are infinitely many m *for which* $p(f(m))$ *is odd.*

Remarks

1. (O $\oplus$ Radu) *True for* $\deg(f) = 1$.
2. *If* $\deg(f) \geq 3$*, then we have no ideas.*

Special quadratic polynomials

Special quadratic polynomials

Theorem (O, O-Ramsey '12)

If $1 \leq D \equiv 23 \pmod{24}$ *is square-free, then the following are true:*

Special quadratic polynomials

Theorem (O, O-Ramsey '12)

If $1 \leq D \equiv 23 \pmod{24}$ *is square-free, then the following are true:*

(1) There are infinitely many n *coprime to 6 for which*

$$p\left(\frac{Dn^2+1}{24}\right) \text{ is even.}$$

Special quadratic polynomials

Theorem (O, O-Ramsey '12)

If $1 \leq D \equiv 23 \pmod{24}$ *is square-free, then the following are true:*

(1) There are infinitely many n *coprime to 6 for which*

$$p\left(\frac{Dn^2+1}{24}\right) \text{ is even.}$$

(2) There are infinitely many m *coprime to 6 for which*

$$p\left(\frac{Dm^2+1}{24}\right) \text{ is odd,}$$

Special quadratic polynomials

Theorem (O, O-Ramsey '12)

If $1 \leq D \equiv 23 \pmod{24}$ *is square-free, then the following are true:*

(1) There are infinitely many n *coprime to 6 for which*

$$p\left(\frac{Dn^2+1}{24}\right) \text{ is even.}$$

(2) There are infinitely many m *coprime to 6 for which*

$$p\left(\frac{Dm^2+1}{24}\right) \text{ is odd,}$$

if there is at least one such m*.*

Special quadratic polynomials

Theorem (O, O-Ramsey '12)

If $1 \leq D \equiv 23 \pmod{24}$ *is square-free, then the following are true:*

(1) There are infinitely many n *coprime to 6 for which*

$$p\left(\frac{Dn^2+1}{24}\right) \quad \text{is even.}$$

(2) There are infinitely many m *coprime to 6 for which*

$$p\left(\frac{Dm^2+1}{24}\right) \quad \text{is odd,}$$

if there is at least one such m*. Furthermore, the smallest* m *(if any) satisfies* $m \leq 12h(-D) + 2$.

$\Uparrow$

Class Number

New theorem on parity

Theorem (O (2025))

If $D \equiv 23 \pmod{24}$ is square-free and every prime $\ell \mid D$ satisfies $\ell \equiv 1, 7 \pmod{8}$, then along the progression

$$n = \frac{Dm^2 + 1}{24} \qquad \text{with } (m, 6) = 1,$$

the partition numbers $p(n)$ take both parities infinitely often.

Ramanujan's mock theta functions

1. We start with Ramanujan's mock theta functions:

$$f(q) := 1 + \sum_{n=1}^{\infty} \frac{q^{n^2}}{(1+q)^2(1+q^2)^2 \cdots (1+q^n)^2},$$

$$\omega(q) := \sum_{n=0}^{\infty} \frac{q^{2n^2+2n}}{(q;q^2)_{n+1}^2}.$$

Sketch of the proof

2. By the work of Zwegers, $f(q)$ and $\omega(q)$ are the "holomorphic parts" of a weight $1/2$ vector-valued harmonic Maass form.

Sketch of the proof

2. By the work of Zwegers, $f(q)$ and $\omega(q)$ are the "holomorphic parts" of a weight $1/2$ vector-valued harmonic Maass form.

3. Work with Bruinier gives *Generalized Borcherds Products* using weight $1/2$ *harmonic Maass forms.*

Sketch of the proof

2. By the work of Zwegers, $f(q)$ and $\omega(q)$ are the "holomorphic parts" of a weight $1/2$ vector-valued harmonic Maass form.

3. Work with Bruinier gives *Generalized Borcherds Products* using weight $1/2$ *harmonic Maass forms.*

4. This theory applies for $f(q)$ and $\omega(q)$.

Sketch of the proof

5. More precisely, for $0 \leq j \leq 11$ we let

$$H_j(z) = \sum C(j;n)q^n := \begin{cases} \pm q^{-1} f(q^{24}) & \text{if } j = 1, 5, 7, 11, \\ 2\left(\pm\omega(q^{12}) \pm \omega(-q^{12})\right) & \text{if } j = 2, 4, 8, 10, \\ 0 & \text{otherwise.} \end{cases}$$

Sketch of the proof

5. More precisely, for $0 \leq j \leq 11$ we let

$$H_j(z) = \sum C(j;n)q^n := \begin{cases} \pm q^{-1} f(q^{24}) & \text{if } j = 1,5,7,11, \\ 2\left(\pm\omega(q^{12}) \pm \omega(-q^{12})\right) & \text{if } j = 2,4,8,10, \\ 0 & \text{otherwise.} \end{cases}$$

6. Note that $H_j(z) \equiv 0 \pmod 2$ for $j \notin \{1,5,7,11\}$.

Sketch of the proof

7. Letting $P_D(X) := \prod_{b \pmod{D}} (1 - e(-b/D)X)^{\left(\frac{-D}{b}\right)}$, we then let

$$\Psi_D(z) := \prod_{m=1}^{\infty} P_D(q^m)^{C(\overline{m};Dm^2)}.$$

Sketch of the proof

7. Letting $P_D(X) := \prod_{b \pmod{D}} (1 - e(-b/D)X)^{\left(\frac{-D}{b}\right)}$, we then let

$$\Psi_D(z) := \prod_{m=1}^{\infty} P_D(q^m)^{C(\overline{m}; Dm^2)}.$$

8. *Generalized Borcherds Products* $\Longrightarrow$ $\Psi_D(z)$ is a modular function on $\Gamma_0(6)$ with a discriminant $-D$ Heegner divisor.

Sketch of the proof

9. $\Longrightarrow$ Log derivative of $\Psi_D(z)$ is a weight 2 modular form with simple poles at disc. $-D$ CM points.

Sketch of the proof

9. $\Longrightarrow$ Log derivative of $\Psi_D(z)$ is a weight 2 modular form with simple poles at disc. $-D$ CM points.

10. Using the combinatorial properties of $f(q)$, we have that

$$P(D;z) := \sum_{\substack{m\geq 1 \\ \gcd(m,6)=1}} p\left(\frac{Dm^2+1}{24}\right) \sum_{\substack{n\geq 1 \\ \gcd(n,D)=1}} q^{mn} \pmod{2}$$

is the mod 2 reduction of a wgt 2 meromorphic modular form.

Sketch of the proof

11. **Elliptic curves at 2.** On the special fiber at 2, the divisor of Ψ_D reduces to a Frobenius orbit.

Sketch of the proof

11. **Elliptic curves at 2.** On the special fiber at 2, the divisor of Ψ_D reduces to a Frobenius orbit.

12. In characteristic 2, $\ker(d\log) = (k(X)^\times)^2$, so odd residues force a nonzero mod 2 form.

Sketch of the proof

11. **Elliptic curves at 2.** On the special fiber at 2, the divisor of Ψ_D reduces to a Frobenius orbit.

12. In characteristic 2, $\ker(d\log) = (k(X)^\times)^2$, so odd residues force a nonzero mod 2 form.

13. **Odd residue via genus theory.**
If every $\ell \mid D$ satisfies $\ell \equiv 1, 7 \pmod 8$, then some ordinary point has an *odd* residue for $d\log\Psi_D$.

Sketch of the proof

11. **Elliptic curves at 2.** On the special fiber at 2, the divisor of Ψ_D reduces to a Frobenius orbit.

12. In characteristic 2, $\ker(d\log) = (k(X)^\times)^2$, so odd residues force a nonzero mod 2 form.

13. **Odd residue via genus theory.**
If every $\ell \mid D$ satisfies $\ell \equiv 1, 7 \pmod{8}$, then some ordinary point has an *odd* residue for $d\log\Psi_D$.

14. These D have a first $p(n) \implies$ infinitely many by earlier work.
$\square$

Bruinier–O formula revisited

Theorem (O (2025))

Let $\Delta_n := 1 - 24n < 0$ *and let* $\mathcal{A}_{\Delta_n}$ *is its* $X_0(6)$ *CM packet, then*

$$p(n) \;=\; -\frac{1}{\Delta_n}\sum_{\alpha\in\mathcal{A}_{\Delta_n}} P(\alpha),$$

Bruinier–O formula revisited

Theorem (O (2025))

Let $\Delta_n := 1 - 24n < 0$ *and let* $\mathcal{A}_{\Delta_n}$ *is its* $X_0(6)$ *CM packet, then*

$$p(n) \;=\; -\frac{1}{\Delta_n} \sum_{\alpha \in \mathcal{A}_{\Delta_n}} P(\alpha),$$

where for each CM point α *with* $J = j(\alpha)$ *and* $\Phi = \Phi_{\Delta_n}(X, Y)$,

$$P(\alpha) \;=\; -D_{-2}F(\alpha) \;+\; \frac{1}{6}\,F(\alpha)\,\frac{\Phi_{YY} - \Phi_{XY}}{\Phi_Y}\bigg|_{(J,J)}.$$

Bruinier–O formula revisited

Theorem (O (2025))

Let $\Delta_n := 1 - 24n < 0$ and let $\mathcal{A}_{\Delta_n}$ is its $X_0(6)$ CM packet, then

$$p(n) = -\frac{1}{\Delta_n} \sum_{\alpha \in \mathcal{A}_{\Delta_n}} P(\alpha),$$

where for each CM point α with $J = j(\alpha)$ and $\Phi = \Phi_{\Delta_n}(X, Y)$,

$$P(\alpha) = -D_{-2}F(\alpha) + \frac{1}{6} F(\alpha) \left. \frac{\Phi_{YY} - \Phi_{XY}}{\Phi_Y} \right|_{(J,J)}.$$

Remark

Recasts $p(n)$ as a sum of tangents at CM points on $X_0(6)$.

Summary: Congruences modulo $\ell \geq 5$

Theorem (O (2025))

If $\ell \geq 5$ *is prime and* $\left(\frac{\Delta_n}{\ell}\right) = -1$*, then*

$$p(n) = -\frac{1}{\Delta_n} \sum_{(E,C) \in SS_\ell(6)} h_{\Delta_n}(E,C) \cdot P^{(\ell)}(E,C),$$

Summary: Congruences modulo $\ell \geq 5$

Theorem (O (2025))

If $\ell \geq 5$ is prime and $\left(\frac{\Delta_n}{\ell}\right) = -1$, then

$$p(n) = -\frac{1}{\Delta_n} \sum_{(E,C) \in SS_\ell(6)} h_{\Delta_n}(E,C) \cdot P^{(\ell)}(E,C),$$

where $SS_\ell(6)$ is the supersingular locus of $X_0(6)$ in char ℓ and

$h_{\Delta_n}(E,C) := \#\,\{\text{oriented optimal embeddings of } \mathcal{O}_{\Delta_n} \mapsto \mathrm{End}(E,C).\}$

Summary: Congruences modulo $\ell \geq 5$

Theorem (O (2025))

If $\ell \geq 5$ is prime and $\left(\frac{\Delta_n}{\ell}\right) = -1$, then

$$p(n) = -\frac{1}{\Delta_n} \sum_{(E,C) \in SS_\ell(6)} h_{\Delta_n}(E,C) \cdot P^{(\ell)}(E,C),$$

where $SS_\ell(6)$ is the supersingular locus of $X_0(6)$ in char ℓ and

$h_{\Delta_n}(E,C) := \#\{\text{oriented optimal embeddings of } \mathcal{O}_{\Delta_n} \mapsto \mathrm{End}(E,C).\}$

Remarks

(1) Conceptual proof of the congruences mod powers of 5, 7 and 11.

Summary: Congruences modulo $\ell \geq 5$

Theorem (O (2025))

If $\ell \geq 5$ is prime and $\left(\frac{\Delta_n}{\ell}\right) = -1$, then

$$p(n) = -\frac{1}{\Delta_n} \sum_{(E,C) \in SS_\ell(6)} h_{\Delta_n}(E,C) \cdot P^{(\ell)}(E,C),$$

where $SS_\ell(6)$ is the supersingular locus of $X_0(6)$ in char ℓ and

$h_{\Delta_n}(E,C) := \#\{\text{oriented optimal embeddings of } \mathcal{O}_{\Delta_n} \mapsto \text{End}(E,C).\}$

Remarks

(1) Conceptual proof of the congruences mod powers of 5, 7 and 11.
(2) The primes $5, 7, and 11$ are "lucky" in that these are the only primes for which $j = 0, 1728$ cover all supersingular curves.

Summary: Congruences modulo $\ell \geq 5$

Theorem (O (2025))

If $\ell \geq 5$ is prime and $\left(\frac{\Delta_n}{\ell}\right) = -1$, then

$$p(n) = -\frac{1}{\Delta_n} \sum_{(E,C) \in SS_\ell(6)} h_{\Delta_n}(E,C) \cdot P^{(\ell)}(E,C),$$

where $SS_\ell(6)$ is the supersingular locus of $X_0(6)$ in char ℓ and

$$h_{\Delta_n}(E,C) := \#\{\text{oriented optimal embeddings of } \mathcal{O}_{\Delta_n} \mapsto \mathrm{End}(E,C).\}$$

Remarks

(1) Conceptual proof of the congruences mod powers of 5, 7 and 11.
(2) The primes $5, 7, and 11$ are "lucky" in that these are the only primes for which $j = 0, 1728$ cover all supersingular curves. Index formula contributes "half prime powers."

Summary: New theorem on parity

Theorem (O (2025))

If $D \equiv 23 \pmod{24}$ *is square-free and every prime* $\ell \mid D$ *satisfies* $\ell \equiv 1, 7 \pmod 8$, *then along the progression*

$$n = \frac{Dm^2 + 1}{24} \qquad \text{with } (m, 6) = 1,$$

the partition numbers $p(n)$ *take both parities infinitely often.*