Properties of singular moduli

Ken Ono

(University of Wisconsin at Madison).

The j-function.

Throughout let $q := e^{2\pi i z}$, and as usual let

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots .$$

. . . .

Definition. Values of $j(z)$ at imaginary quadratic arguments in $\mathfrak{H}$ are known as **singular moduli**.

Classical Examples.

$$j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0,$$

$$j\left(\frac{1+\sqrt{-15}}{2}\right) = \frac{-191025 - 85995\sqrt{5}}{2}.$$

Theorem.
Singular moduli are algebraic integers.

. . . .

Remark. Singular moduli have many roles.

- Generate class fields of imaginary quadratic fields.

- Explain the interplay between elliptic curves over finite fields and elliptic curves with CM.

- Provide structure for Borcherds' work on infinite product expansions of modular forms.

Here we recall two explicit ‘roles’.

I. Explicit Class Field Theory.

Theorem. If τ is a CM point of discriminant $-d$, where $-d$ is the fundamental discriminant of the quadratic field $K_d := \mathbb{Q}(\sqrt{-d})$, then $K_d(j(\tau))$ is the Hilbert class field of K_d.

. . . .

II. Elliptic Curves.

Definition. An elliptic curve E over $\overline{\mathbb{F}}_p$ is supersingular of $E(\overline{\mathbb{F}}_p)$ has no p-torsion.

Theorem. (Deuring).
If E is an elliptic curve whose j-invariant is a singular modulus with discriminant $-d$ and p is a prime which is inert or ramified in $\mathbb{Q}(\sqrt{-d})$, then E ‘mod p’ is supersingular.

Goal. Here we investigate

- Congruence properties.

- Asymptotic behavior.

Zagier's "Traces" of Singular Moduli.

Notation.

1) Let $\mathcal{Q}_d$ be the set of discriminant $-d$ positive definite integral quadratic forms

$$Q(x,y) = ax^2 + bxy + cy^2.$$

2) Let $\alpha_Q \in \mathfrak{H}$ be a root of $Q(x,1) = 0$.

3) The group $\Gamma := PSL_2(\mathbb{Z})$ acts on $\mathcal{Q}_d$.

4) Define ω_Q by

$$\omega_Q := \begin{cases} 2 & \text{if } Q \sim_\Gamma [a,0,a], \\ 3 & \text{if } Q \sim_\Gamma [a,a,a], \\ 1 & \text{otherwise.} \end{cases}$$

5) Let $J(z)$ be the Hauptmodule

$$\begin{aligned} J(z) &:= j(z) - 744 \\ &= q^{-1} + 196884q + 21493760q^2 + \cdots . \end{aligned}$$

6) If $m \geq 1$, then define $J_m(z) \in \mathbb{Z}[x]$ by

$$J_m(z) := m\,(J(z) \mid T(m)) = q^{-m} + \sum_{n=1}^{\infty} a_m(n) q^n.$$

. . . .

Definition. Define the mth *trace of singular moduli of discriminant* $-d$ by

$$\mathrm{Tr}_m(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{J_m(\alpha_Q)}{\omega_Q}.$$

Remarks.

1) If $m = 1$, then $\mathsf{Tr}_1(d) \in \mathbb{Z}$ is the trace of algebraic conjugates

$$\mathsf{Tr}_1(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{j(\alpha_Q) - 744}{\omega_Q}.$$

2) Newton's formulas for symmetric functions implies that $\mathsf{Tr}_1(d), \ldots, \mathsf{Tr}_{h(-d)}(d)$ determine the Hilbert Class Polynomial

$$H_d(x) = \prod_{Q \in \mathcal{Q}_d/\Gamma} (x - j(\alpha_Q)).$$

Congruence Properties.

Numerical Data I.

$$\mathrm{Tr}_1(3^2\cdot 3) = 12288992 \equiv 239 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 4) = -153541020 \equiv 231 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 7) \equiv 462 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 8) \equiv 0 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 11) \equiv 0 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 12) \equiv 227 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 15) \equiv 705 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 16) \equiv 693 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 19) \equiv 462 \pmod{3^6},$$
$$\mathrm{Tr}_1(3^2\cdot 20) \equiv 0 \pmod{3^6}.$$

Observe. For $n \equiv 2 \pmod 3$, it seems that

$$\mathrm{Tr}_1(9n) \equiv 0 \pmod{3^6}.$$

Some more data...

$$\begin{aligned}
\mathrm{Tr}_1(5^2 \cdot 3) &\equiv 121 \pmod{5^3},\\
\mathrm{Tr}_1(5^2 \cdot 4) &\equiv 0 \pmod{5^3},\\
\mathrm{Tr}_1(5^2 \cdot 7) &\equiv 113 \pmod{5^3},\\
\mathrm{Tr}_1(5^2 \cdot 8) &\equiv 113 \pmod{5^3},\\
\mathrm{Tr}_1(5^2 \cdot 11) &\equiv 0 \pmod{5^3},\\
\mathrm{Tr}_1(5^2 \cdot 12) &\equiv 109 \pmod{5^3}.
\end{aligned}$$

Observe. It seems that if $\left(\frac{n}{5}\right) = 1$, then

$$\mathrm{Tr}_1(5^2 n) \equiv 0 \pmod{5^3}.$$

Theorem 1. *(Ahlgren-O, Compositio Math. 04?). If $p \nmid m$ is an odd prime and n is* **any** *positive integer for which p splits in $\mathbb{Q}(\sqrt{-n})$, then*

$$\mathrm{Tr}_m(p^2 n) \equiv 0 \pmod{p}.$$

. . . .

Question. What if p is inert or ramified?

Theorem 2. *(Ahlgren-O, Compositio Math. 04?). If p is an odd prime and $s \geq 1$, then a positive proportion of the primes ℓ satisfy*

$$\mathrm{Tr}_m(\ell^3 n) \equiv 0 \pmod{p^s}$$

for every positive integer n for which p is inert or ramified in $\mathbb{Q}(\sqrt{-n\ell})$.

. . . .

Example. If $n \equiv 2, 3, 4, 6, 8, 9, 11, 12, 14 \pmod{15}$ is positive, then

$$\mathrm{Tr}_1(125n) \equiv 0 \pmod{9}.$$

Asymptotics for $\mathrm{Tr}_m(d)$.

Recall the classical observation that

$e^{\pi\sqrt{163}} = 262537412640768743.99999999999992\ldots$

is "nearly" an integer.

. . . .

Definition. A primitive positive definite binary quadratic form Q is *reduced* if $|B| \leq A \leq C$, and $B \geq 0$ if either $|B| = A$ or $A = C$.

Notation.

$$H(d) = \begin{array}{c}\text{Hurwitz-Kronecker class number}\\ \text{for discriminant } -d.\end{array}$$

Remarks.

1. If $-d < -4$ is fundamental, then there are $H(d)$ reduced forms with discriminant $-d$.

2. If $-d$ is fundamental, then the set of such reduced forms, say $\mathcal{Q}_d^{\text{red}}$, is a complete set of representatives for $\mathcal{Q}_d/\Gamma$.

3. Every reduced form has $1 \le A \le \sqrt{d/3}$, and has α_Q in the usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

$$\mathcal{F} = \left\{-\frac{1}{2} \le \Re(z) < \frac{1}{2} \text{ and } |z| > 1\right\} \cup \left\{-\frac{1}{2} \le \Re(z) \le 0 \quad \text{and} \quad |z| = 1\right\}.$$

Since

$$J_1(z) = q^{-1} + 196884q + \cdots ,$$

it follows that if $G^{\text{red}}(d)$ is

$$G^{\text{red}}(d) = \sum_{Q=(A,B,C)\in\mathcal{Q}_d^{\text{red}}} e^{\pi Bi/A} \cdot e^{\pi\sqrt{d}/A},$$

then

$$\text{Tr}_1(d) - G^{\text{red}}(d) \text{ is "small."}$$

Remark. This is the $e^{\pi\sqrt{163}}$ example.

Average Values.

It is natural to study the average value

$$\frac{\mathrm{Tr}_1(d) - G^{\mathrm{red}}(d)}{H(d)}.$$

Examples. If $d = 1931, 2028$ and 2111, then

$$\frac{\mathrm{Tr}_1(d) - G^{\mathrm{red}}(d)}{H(d)} = \begin{cases} 11.981\ldots & \text{if } d = 1931, \\ -24.483\ldots & \text{if } d = 2028, \\ -13.935\ldots & \text{if } d = 2111. \end{cases}$$

Remarks.

1. These averages are indeed small.

2. These averages are not uniform.

A more uniform picture exists.

Notation.

1. Let $\mathfrak{F}'$ the semi-circular region obtained by connecting the lower endpoints of $\mathfrak{F}$ by a horizontal line.

2. Let $\mathcal{Q}_d^{\mathsf{old}}$ denote the set of discriminant $-d$ positive definite quadratic forms Q with $\alpha_Q \in \mathfrak{F}'$.

3. Define $G^{\mathsf{old}}(d)$ by

$$G^{\mathsf{old}}(d) = \sum_{Q=(A,B,C)\in\mathcal{Q}_d^{\mathsf{old}}} e^{\pi Bi/A} \cdot e^{\pi\sqrt{d}/A}.$$

Examples. We have the following data:

$$\frac{\mathrm{Tr}_1(d) - G^{\mathrm{red}}(d) - G^{\mathrm{old}}(d)}{H(d)} = \begin{cases} -24.67.. & d = 1931, \\ -24.48.. & d = 2028, \\ -23.45.. & d = 2111. \end{cases}$$

. . . .

Theorem 3. *(Bruinier-Jenkins-Ono, and Duke) For fundamental discriminants $-d < 0$, we have*

$$\lim_{-d \to -\infty} \frac{\mathrm{Tr}_1(d) - G^{\mathrm{red}}(d) - G^{\mathrm{old}}(d)}{H(d)} = -24.$$

Proofs of Theorems 1, 2 and 3.

Zagier's generating functions

Notation.

For non-negative integers λ, let

$$M^!_{\lambda+\frac{1}{2}} = \left\{ \begin{array}{c} \text{weight } \lambda + \frac{1}{2} \text{ weakly holomorphic} \\ \text{modular forms on } \Gamma_0(4) \text{ satisfying} \\ \text{the ``Kohnen plus-space'' condition.} \end{array} \right\}$$

Zagier's Generating Functions.

1. For $1 \leq D \equiv 0, 1 \pmod 4$, let $g_D(z) \in M^!_{3/2}$ be the unique form with
$$g_D = q^{-D} + B(D,0) + \sum_{0<d\equiv 0,3 \pmod 4} B(D,d)q^d.$$

2. For $m \geq 1$, define integers $B_m(D,d)$ by
$$B_m(D,d) \;=\; \text{coefficient of } q^d \text{ in } g_D(z) \,\Big|\, T_{\frac{3}{2}}(m^2).$$

. . . .

Theorem. (Zagier)
If $m \geq 1$ and $-d < 0$ is a discriminant, then
$$\mathrm{Tr}_m(d) = -B_m(1,d).$$

Remarks.

1. Theorems 1 and 2 concern the congruence properties of $\mathrm{Tr}_m(d)$.

2. Theorem 1 follows from Zagier's Theorem combined with a simple analysis of Hecke operators.

3. Theorem 2 is more involved.

. . . .

Theorem 2. If p is an odd prime and $s \geq 1$, a proportion of the primes ℓ satisfy

$$\mathrm{Tr}_m(\ell^3 n) \equiv 0 \pmod{p^s}$$

for every positive integer n for which p is inert or ramified in $\mathbb{Q}(\sqrt{-n\ell})$.

Sketch of the Proof of Thm 2 when $m = 1$

Step 1. The generating function is

$$-g_1(z) = -\frac{\eta(z)^2}{\eta(2z)} \cdot \frac{E_4(4z)}{\eta(4z)^6}$$

$$= -q^{-1} + 2 + \sum_{d \equiv 0,3 \pmod 4} \mathrm{Tr}_1(d) q^d$$

Step 2. $g_1(z)$ is a weight $\frac{3}{2}$ modular form which is holomorphic on $\mathfrak{H}$, but has poles **at infinity and some cusps**.

. . . .

Remark. Poles "present" problems.

Proving congruences typically requires:

- q-series identities.
- Hecke eigenforms.
- Finite dimensionality of spaces of holomorphic modular forms.

$\Longrightarrow$ $g_1(z)$ is unhappy.

Step 3. If $s \geq 1$, we investigate

$$g_1(p,z) := 2 + \sum_{\substack{0<d\equiv 0,3 \pmod 4 \\ p|d}} \mathrm{Tr}_1(d) q^d + 2 \sum_{\substack{0<d\equiv 0,3 \pmod 4 \\ (\frac{-d}{p})=-1}} \mathrm{Tr}_1(d) q^d.$$

This is obtained by

$$g_1(p,z) := g_1 \pm \left(g_1 \otimes \left(\frac{\bullet}{p}\right) \right).$$

Step 4. The form $g_1(p,z)$ is holomorphic **at infinity** and on $\mathfrak{H}$, but is now on $\Gamma_0(Np^2)$.

It still has poles at "other cusps".

Step 5. Happily, we can construct integer weight modular forms $\mathcal{E}_p(z)$ on $\Gamma_0(p^2)$ with

- $\mathcal{E}_p(z) \equiv 1 \pmod{p}$,

- $\text{ord}_\tau(g_1(p,z)) < 0 \implies \mathcal{E}_p(\tau) = 0$.

Step 6. Therefore, for every $s \gg 1$ we have:

$$\mathcal{G}_1(p^s, z) := g_1(p,z) \cdot \mathcal{E}_p(z)^{p^{s-1}}$$

is a **holomorphic** modular form.

Moreover, we have

$$\mathcal{G}_1(p^s, z) \equiv g_1(p,z) \pmod{p^s}.$$

Step 7. Write $\mathcal{G}_1(p^s, z)$ as

$$\mathcal{G}_1(p^s, z) := \mathcal{G}^{eis}(p^s, z) + \mathcal{G}^{cusp}(p^s, z).$$

Step 8. Using

- Galois representations.
- Shimura's correspondence.
- Hecke operators,

$\exists$ primes $\ell \equiv -1 \pmod{p^s}$ with

$$\mathcal{G}^{cusp}(p^s, z) \mid T(\ell^2) \equiv 0 \pmod{p^s}.$$

For these same ℓ, one can show that

$$\mathcal{G}^{eis}(p^s, z) \mid T(\ell^2) \equiv 0 \pmod{p^s}.$$

Step 9. Recall the action of $T(\ell^2)$:

$$\left(\sum_{n=0}^{\infty} a(n)q^n\right) \mid T(\ell^2)$$

$$= \sum_{n=0}^{\infty} a(\ell^2 n)q^n + \chi^*(\ell)\left(\frac{n}{\ell}\right)\ell^{\lambda-1}a(n)q^n$$

$$+ \chi^*(\ell^2)\ell^{2\lambda-1}a(n/\ell^2)q^n.$$

Step 10. If $T(\ell^2)$ is an annihilator $\pmod{p^s}$, then for all n

$$a(\ell^2 n) + \chi^*(\ell)\Big(\frac{n}{\ell}\Big)\ell^{\lambda-1}a(n)$$

$$+ \chi^*(\ell^2)\ell^{2\lambda-1}a(n/\ell^2) \equiv 0 \pmod{p^s}.$$

Note. $\left(\frac{n\ell}{\ell}\right) = 0$, and $a(n\ell/\ell^2) = 0$ if $\ell \nmid n$.

Step 11. By replacing $n = n\ell$, we get

$$a(\ell^3 n) \equiv 0 \pmod{p^s}$$

for every n coprime to ℓ.

Apply this to $g_1(p, z)$.

$\square$

Sketch of the Proof of Theorem 3.

Theorem 3.
For fundamental discriminants $-d < 0$, we have

$$\lim_{-d \to -\infty} \frac{\mathrm{Tr}(d) - G^{\mathrm{red}}(d) - G^{\mathrm{old}}(d)}{H(d)} = -24.$$

. . . .

Remark. To prove Theorem 3, we first obtain an "exact formula for" all the $\mathrm{Tr}_m(d)$.

Notation.

- If v is odd, then let

$$\epsilon_v = \begin{cases} 1 & \text{if } v \equiv 1 \pmod 4, \\ i & \text{if } v \equiv 3 \pmod 4. \end{cases}$$

- Let $e(w) = e^{2\pi i w}$.

- Define the Kloosterman sum

$$K(m,n,c) = \sum_{v\ (c)^*} \left(\frac{c}{v}\right) \epsilon_v^{-1} e\left(\frac{m\bar{v} + nv}{c}\right).$$

  Here v runs through the primitive residues classes modulo c, and $\bar{v}$ is the multiplicative inverse of v modulo c.

Theorem 4. *(Bruinier-Jenkins-Ono)*
If $m \geq 1$ *and* $-d < 0$ *is a discriminant, then*

$$\mathrm{Tr}_m(d) = -\sum_{n|m} nB(n^2, d),$$

where $B(n^2, d)$ *is the integer given by*

$$B(n^2, d) = 24H(d)$$
$$-(1+i) \sum_{\substack{c>0 \\ c \equiv 0\ (4)}} (1 + \delta(\frac{c}{4})) \frac{K(-n^2, d, c)}{n\sqrt{c}} \sinh\left(\frac{4\pi n\sqrt{d}}{c}\right).$$

Here the function δ *is defined by*

$$\delta(v) = \begin{cases} 1 & \text{if } v \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

. . . .

Remark. Theorem 4 is analogous to the exact formula for the partition function $p(n)$ obtained by Rademacher using the "circle method".

Proof of Theorem 3.

1) By Thm 4, Theorem 3 is equivalent to

$$\sum_{\substack{c>\sqrt{d/3} \\ c\equiv 0\ (4)}} (1+\delta(\frac{c}{4}))\frac{K(-1,d,c)}{\sqrt{c}} \sinh\left(\frac{4\pi}{c}\sqrt{d}\right) = o\left(H(d)\right).$$

2) By Siegel's theorem that

$$H(d) \gg_\epsilon d^{\frac{1}{2}-\epsilon},$$

it suffices to show that such sums are $\ll d^{\frac{1}{2}-\gamma}$, for some $\gamma > 0$.

3) Estimates of this type are basically known, and are intimately connected to the problem of bounding coefficients of half-integral weight cusp forms (for example, see works by Duke and Iwaniec).

$\square$

Sketch of the Proof of Theorem 4.

Remark. It suffices to find an exact expression for Zagier's generating functions

$$g_D(z) = q^{-D} + B(D,0) + \sum B(D,d)q^d.$$

By the "method of Poincaré series," we have:

Theorem 5. *(Bruinier-Jenkins-Ono)*
There is a Poincaré series $F_m(z, 3/2)$ *which is a weak Maass form of weight* $3/2$ *for the group* $\Gamma_0(4)$*. Its Fourier coefficients of positive index* n *are*

$$c(n, y, 3/2) = 2\pi i^{-3/2} \left|\frac{n}{m}\right|^{\frac{1}{4}} \times \sum_{\substack{c>0 \\ c\equiv 0\ (4)}} \frac{K(m,n,c)}{c} I_{1/2}\left(\frac{4\pi}{c}\sqrt{|mn|}\right) e^{-2\pi n y}.$$

Near ∞ *the function* $F_m(z, 3/2) - e(mz)$ *is bounded. Near the other cusps the function* $F_m(z, 3/2)$ *is bounded.*

Remark. We must relate these to Zagier's

$$g_D(z) \in M^!_{3/2}.$$

Recall another function of Zagier, $G(z)$,

$$G(z) = \sum_{n=0}^{\infty} H(n)q^n + \frac{1}{16\pi\sqrt{y}} \sum_{n=-\infty}^{\infty} \beta(4\pi n^2 y) q^{-n^2},$$

where $H(0) = \zeta(-1) = -\frac{1}{12}$, and

$$\beta(s) = \int_1^{\infty} t^{-3/2} e^{-st} dt.$$

Proposition. Let $F_m^+(z)$ be the "projection" of $F_m(z, 3/2)$ to Kohnen's plus space.

1. If $-m$ is a non-zero square, then

$$F_m^+(z) + 24G(z) \in M_{3/2}^!.$$

2. If $-m$ is not a square, then $F_m^+(z) \in M_{3/2}^!$.

Remark. Theorem 4 now follows easily.

$\square$

Summary

Theorem 1. (Ahlgren-O).
If $p \nmid m$ is an odd prime and n is **any** positive integer for which p splits in $\mathbb{Q}(\sqrt{-n})$, then

$$\mathrm{Tr}_m(p^2 n) \equiv 0 \pmod{p}.$$

. . . .

Theorem 2. (Ahlgren-O).
If p is an odd prime and $s \geq 1$, then a positive proportion of the primes ℓ satisfy

$$\mathrm{Tr}_m(\ell^3 n) \equiv 0 \pmod{p^s}$$

for every positive integer n for which p is inert or ramified in $\mathbb{Q}(\sqrt{-n\ell})$.

Theorem 3. (Bruinier-Jenkins-Ono, and Duke) For fundamental discriminants $-d < 0$, we have

$$\lim_{-d \to -\infty} \frac{\mathrm{Tr}_1(d) - G^{\mathrm{red}}(d) - G^{\mathrm{old}}(d)}{H(d)} = -24.$$

. . . .

Theorem 3 follows from Theorem 4.

Theorem 4. (Bruinier-Jenkins-Ono) If $m \geq 1$ and $-d < 0$ is a discriminant, then

$$\mathrm{Tr}_m(d) = -\sum_{n|m} nB(n^2, d),$$

where $B(n^2, d)$ is the integer given by

$$B(n^2, d) = 24H(d)$$
$$-(1+i) \sum_{\substack{c>0 \\ c \equiv 0\ (4)}} (1 + \delta(\frac{c}{4})) \frac{K(-n^2, d, c)}{n\sqrt{c}} \sinh\left(\frac{4\pi n\sqrt{d}}{c}\right).$$