Don Zagier’s work on singular moduli

Benedict Gross

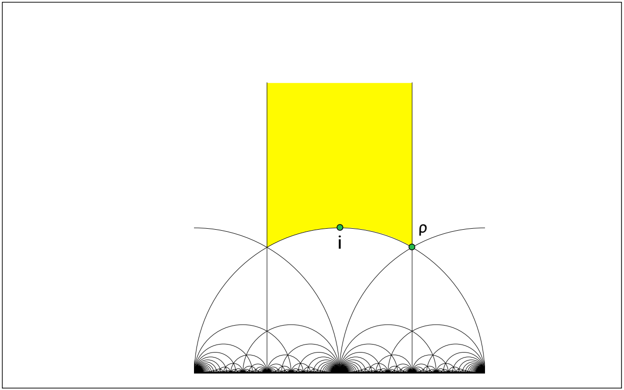
Harvard University

June, 2011

Don in 1976

The orbit space $SL_2(\mathbb{Z})\backslash\mathfrak{H}$ has the structure a Riemann surface, isomorphic to the complex plane $\mathbb{C}$.

We can fix an isomorphism $J : SL_2(\mathbb{Z})\backslash\mathfrak{H} \to \mathbb{C}$ which maps the orbits $[i]$ and $[\rho]$ to the points to 1 and 0 respectively, and has a simple pole at ∞, using the local parameter $q = e^{2\pi i\tau}$.



There is a unique scaling so that the simple pole at ∞ has residue 1.

$$j(\tau) = 1728J(\tau) = 1/q + 744 + 196884q + 21493760q^2 + ...$$

For this normalization $j(\rho) = 0$ and $j(i) = 1728 = 12^3$.

We can still add an integer:

$$j^*(\tau) = j(\tau) - 744 = 1/q + 0 + 196884q + ...$$

$$j^{**}(\tau) = j(\tau) - 720 = 1/q + 24 + 196884q + ... = \theta(\Lambda_{24})/\Delta$$

The difference $j(\tau) - j(\tau')$ is well-defined.

Complex multiplication

If $z \in \mathfrak{H}$ satisfies a quadratic equation over $\mathbb{Q}$, then

$$az^2 + bz + c = 0$$

with $a > 0$ and $\gcd(a, b, c) = 1$.

$D = b^2 - 4ac < 0$ is an invariant of the $SL_2(\mathbb{Z})$-orbit $[z]$.

The complex elliptic curve $E = \mathbb{C}/2\pi i(\mathbb{Z} + \mathbb{Z}z)$ has endomorphism ring isomorphic to $O_D = \mathbb{Z} + \mathbb{Z}.(D + \sqrt{D})/2$.

$Pic(O_D)$ acts simply transitively on the $h(D)$ orbits: $[z] \to [z_A]$.

For each orbit, $j(z)$ is an algebraic integer of degree $h(D)$.

These singular moduli are all conjugate: $j(z_A) = j(z)^{\sigma(A)}$ and generate the ring class field over $\mathbb{Q}(\sqrt{D})$.

D	$h(D)$	$j(z)$
-3	1	0
-4	1	1728
-7	1	-3375
-67	1	-14719795200
-163	1	-262537412640768000
-15	2	$(-191025 + 85995\sqrt{5})/2$

For $N \geq 1$ there is a finite covering

$$Y_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathfrak{H} \to SL_2(\mathbb{Z})\backslash\mathfrak{H}$$

The meromorphic functions on $Y_0(N)$ are generated by $j(\tau)$ and $j(N\tau)$. These satisfy the modular equation $\phi_N(x, y) = 0$ in $\mathbb{Q}[x, y]$, which defines the curve $Y_0(N)$ over $\mathbb{Q}$.

If all primes dividing N split in O_D, there are Heegner points $P_A = P_{A,\mathfrak{n}}$ on $Y_0(N)$ which lie above the singular moduli $j(z_A)$ and are defined over the SAME class field.

Bryan Birch introduced the classes of the divisors $d_A = (P_A) - (\infty)$ of degree zero in the Jacobian $J_0(N)$, and made some suggestive computations.

I conjectured a formula for the Néron-Tate height pairing $\langle d, d_A\rangle$ in terms of the first derivative of a Rankin L-series associated to a cusp form of weight $k = 2$ for $\Gamma_0(N)$ and a binary theta series θ_A associated to the class A.

A week in Maryland

To simplify the analytic computation of the derivative of the Rankin L-series, Don assumed that $N = 1$. In this case, the modular curve $Y_0(1)$ has genus zero and the Jacobian is trivial....

He also assumed that the weight satisfied $k \geq 4$.

We set $k = 2$ in the final formula for $\langle d, d_A \rangle$ just to see what would happen. As expected, all of the sums were non-convergent, except for one term:

$$\sum_{n=1}^{|D|} r_A(|D| - n) \sum_{d|n} \epsilon_A(d, n) log(n/d^2)$$

$$= \sum_{p \leq |D|} m_A(p) log(p).$$

Néron's local decomposition of the height: $\langle d, d_A \rangle = \sum \langle d, d_A \rangle_v$

When $A \neq 1$, I guessed:

$\langle d, d_A \rangle_v =_? log|j(z) - j(z_A)|_v = -ord_v(j(z) - j(z_A))log(NP_v)$

Don differentiated $q\frac{d}{dq}j(\tau)/\eta(\tau)^4 = j(\tau)^{2/3}(j(\tau) - 1728)^{1/2}$

When $A = 1$ $\langle d, d \rangle_v =_? log|j(z)^{2/3}(j(z) - 1728)^{1/2}|_v$

Suppose that the finite sum $\sum_{p \leq |D|} m_A(p)log(p)$ was the contribution to the global height pairing $\langle d, d_A \rangle$ of all the local heights at finite primes v of the class field.

Then all primes P_v dividing the algebraic integers $j(z)$ or $j(z) - 1728$ or $j(z) - j(z_A)$ have characteristic $p \leq |D|$.

D	$h(D)$	$j(z)$
-3	1	0
-4	1	$1728 = 2^6 3^3$
-7	1	$-3375 = -3^3 5^3$
-67	1	$-147197952000 = -2^{15} 3^3 5^3 11^3$
-163	1	$-262537412640768000 = -2^{18} 3^3 5^3 23^3 29^3$
-15	2	$(-191025 + 85995\sqrt{5})/2$ $N(j(z)) = -121287375 = -3^6 5^3 11^3$

D	$h(D)$	$j(z) - 1728$
-3	1	$-2^6 3^3$
-4	1	0
-7	1	$-3^6 7$
-67	1	$-2^6 3^6 7^2 31^2 67$
-163	1	$-2^6 3^6 7^2 11^2 19^2 127^2 163$
-15	2	$N(j(z) - 1728) = 3^6 7^4 11^2$ $N(j(z) - j(z_A)) = 3^6 5^3 7^4 13^2$

From September to December of 1982, we worked out the proof for $k = 2$ and $N > 1$.

Based on our formulae for the factorization of

$$j(z_D) - 0 = j(z_D) - j(\rho) = j(z_D) - j(z_{-3})$$

$$j(z_D) - 1728 = j(z_D) - j(i) = j(z_D) - j(z_{-4})$$

Don asked me if there was a formula for the factorization of

$$j(z_D) - j(z_{D'}).$$

We might have factored:

$$j(z_{-67}) - j(z_{-163}) = 262537265442816000 = 2^{15}.3^{7}.5^{3}.7^{2}.13.139.331$$

A letter from Don

(1)

Monday, Feb. 7 (1983)

Dick,

I've been in Japan for two weeks now and am enjoying it tremendously, both for sightseeing and mathematics. However, telling you about the trip can wait till you get to Germany; I'm writing now for mathematical reasons only. I'd meant not to look at our business until returning to Germany, since I have several other things to finish writing up, but this weekend I returned to it after all, and came up with something.

As you may remember, I had asked you whether our results on $N(j(z)) = N(j(z) - j(\rho))$, $N(j(z)-1728) = N(j(z)-j(i))$ and $N(j(z)-j(z'))$ $(\operatorname{disc} z = \operatorname{disc} z' = -p)$ might not generalize to results on $N(j(z)-j(z'))$ (or $j(z)-j(z')$) for arbitrary CM points z and z', with unrelated discriminants. You pooh-poohed the idea, explaining why your method applies only to $\mathrm{Aut}(E)$ or to $\mathrm{Hom}(E,E')$ with E, E' having CM by the same order. Nothing daunted (actually, I was: I didn't do the calculations till now), I calculated $j(z) - j(z')$ for $z = \frac{1+i\sqrt{p}}{2}$, $z' = \frac{1+i\sqrt{q}}{2}$ for the primes with

Let D and D' be relatively prime discriminants. Then every prime p which divides the norm of the algebraic integer $j(z_D) - j(z_{D'})$ is less than or equal to $DD'/4$.

More precisely, p must divide an integer of the form $(DD' - x^2)/4$.

Don established an exact formula for the factorization of $N(j(z_D) - j(z_{D'}))$ using Hecke's Eisenstein series $E(z_1, z_2, s)$ of weight one and genus character χ for the Hilbert modular group of the real quadratic field $\mathbb{Q}(\sqrt{DD'})$.

In fact, $E(z_1, z_2, 0) = 0$. Don calculated the Fourier coefficients of the non-holomorphic form $\frac{d}{ds}E(z_1, z_2, s)|_{s=0}$ when restricted to the diagonal $z_1 = z_2$.

He challenged me to find an algebraic proof.

A prime P divides the algebraic integer $j(z_D) - j(z_{D'})$ if and only if the elliptic curves $E = E(z_D)$ and $E' = E(z_{D'})$ become isomorphic when reduced modulo P:

$$E(mod\ P) \cong E'(mod\ P) \cong F.$$

The curve E has an endomorphism e with $e^2 = D$. The curve E' has an endomorphism e' with $e'^2 = D'$.

The curve F is supersingular in characteristic p, and End(F) contains the quaternion ring

$$R = \mathbb{Z} + \mathbb{Z}.e + \mathbb{Z}.e' + \mathbb{Z}.ee'$$

The ring End(F) has reduced discriminant p.The ring R has reduced discriminant $4(DD' - x^2)$, where $2x = ee' + e'e$.

Hence p divides $4(DD' - x^2)$.

For a discriminant $D < 0$, define the Hurwitz class number

$$H(D) = \sum_{D=df^2} \sum_{Pic(O_d)} 1/u(d) = \sum_{D=df^2} h(d)/u(d).$$

For example,

$$H(-12) = h(-12) + h(-3)/3 = 1 + 1/3 = 4/3.$$

In 1975 Don showed

$$E(q) = -\frac{1}{12} + \sum_{D} H(D) q^{|D|} + y^{-1/2} \sum_{n \in \mathbb{Z}} \beta(4\pi n^2 y) q^{-n^2}$$

$$\beta(x) = \frac{1}{16\pi} \int_1^\infty u^{-3/2} e^{-xu}\, du$$

is the Fourier expansion of the (non-holomorphic) Eisenstein series of weight $3/2$ for $\Gamma_0(4)$.

Let

$$P(D) = \sum_{D=df^2} \sum_{Pic(O_d)} d_A/u(d)$$

If we also sum over the different choices of $\mathfrak{n}$ we get a point in $J_0(N)^+(\mathbb{Q})$. How do these points vary with D?

$$F(q) = \sum_D P(D) q^{|D|}$$

is the Fourier expansion of a holomorphic form of weight $3/2$ for $\Gamma_0(4N)$ with coefficients in $J_0(N)^+(\mathbb{Q})$.

For composite N, it is better to use the Fourier expansions of Jacobi forms.

In 2002, Don returned to treat the case of level $N = 1$.

Recall that $j^*(\tau) = j(\tau) - 744 = 1/q + 0 + 196884q + ...$

Define

$$Tr(D) = \sum_{D=df^2} \sum_{Pic(O_d)} j^*(z_A)/u(d)$$

Then the series

$$f(q) = -q^{-1} + 2 + \sum_D Tr(D)q^{|D|}$$

is the Fourier expansion of a weakly holomorphic modular form of weight $3/2$ for $\Gamma_0(4)$. In fact,

$$f(\tau) = -\eta(\tau)^2 E_4(\tau)/\eta(2\tau)\eta(4\tau)^6$$

$$\eta(\tau) = q^{1/24} \prod_{n \geq 1} (1 - q^n) \quad E_4(\tau) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$$

Thanks Don, and Happy Birthday!