Don Zagier's work on singular moduli

Benedict H. Gross

Singular moduli are the values of the modular function $j(\tau)$ at the points z in the upper half plane that satisfy a quadratic equation with rational coefficients. In other words, they are the j-invariants of elliptic curves with complex multiplication.

These invariants were studied intensively by the leading number theorists of the nineteenth century. They are algebraic integers, which generate certain abelian extensions of the imaginary quadratic fields $\mathbb{Q}(z)$. The theory was believed to have been brought to a very satisfying completion in the early twentieth century. That was before Don got his hands on it.

In early 1983 Don sent me an amazing letter from Japan containing a proof of a factorization formula for the integer which is the norm of the difference of two singular moduli of relatively prime discriminants D and D'. This was a completely new aspect of the theory, which Don had discovered by extensive numerical experimentation. One particularly striking fact (which should have been noticed earlier) is that any prime p dividing this norm must divide an integer of the form $(DD' - x^2)/4$. This letter (in its original handwritten form, as well as a Latex version prepared by Carl Erickson) is reproduced below.

Don's proof involved the study of a Hilbert modular Eisenstein series for the real quadratic field $\mathbb{Q}(\sqrt{DD'})$. At the end of the letter, he challenged me to find an algebraic proof, which I sketched in a letter of reply (also reproduced below) and reproduced in the talk.

In 2002, Don discovered another wonderful formula, relating the integers which are the traces of singular moduli to the Fourier coefficients of a meromorphic modular form of weight 3/2. I will put this result into the context of computing the images of Heegner points in the Jacobians of modular curves. In this case, the Jacobian of the curve of level 1 is trivial, but the generalized Jacobian relative to the divisor $2(\infty)$ is isomorphic to the additive group.

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'll meant not to look at my brainless 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 $N(j(z)-j(z'))$ $(\mathrm{disc}\, z = \mathrm{disc}\, z' = -p)$ 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 $A_0(E)$ 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 pairs with class number 1 — a somewhat tricky business, since my HP has only 10 places — and found the values

p \ q	11	19	43	67	163
7	$7\cdot13\cdot17\cdot19$	$3^9\cdot13\cdot31$	$3^6\cdot5^3\cdot7\cdot19\cdot73$	$3^7\cdot5^3\cdot7\cdot13\cdot61\cdot97$	$3^8\cdot5^3\cdot7\cdot13\cdot17\cdot31\cdot103\cdot229\cdot283$
11		$2^{16}\cdot13$	$2^{15}\cdot7^2\cdot19\cdot29$	$2^{17}\cdot7^2\cdot13\cdot41\cdot43$	$2^{15}\cdot7^3\cdot11\cdot13\cdot17\cdot73\cdot79\cdot107\cdot10$
19			$2^{15}\cdot3^6\cdot37$	$2^{16}\cdot3^7\cdot13\cdot79$	$2^{15}\cdot3^7\cdot13\cdot19\cdot31\cdot37\cdot67\cdot193$
43				$2^{15}\cdot3^6\cdot5^3\cdot7^2$	$2^{17}\cdot3^5\cdot5^3\cdot7^3\cdot433$
67					$2^{15}\cdot3^7\cdot5^3\cdot7^2\cdot13\cdot139\cdot33$

It seemed pretty clear that these numbers were too highly factorized for this

d = 8	$5^3\cdot7\cdot13$	$2^6\cdot7^2\cdot13$	$2^6\cdot13\cdot29\cdot37$	$2^6\cdot5^3\cdot7^2\cdot37\cdot61$	$2^6\cdot5^4\cdot7^2\cdot13\cdot53\cdot109$	$2^6\cdot5\cdot7$
	p=7	p=11				

[Kyoto, Japan]
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

$$N(j(z)) = N(j(z) - j(\rho)), N(j(z) - 1728) = N(j(z) - j(i)), \text{ and } N(j(z) - j(z'))$$

($\operatorname{disc} z = \operatorname{disc} z' = -p$) 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. Not 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 class number 1 - a somewhat tricky business, since my HP has only 10 places - and found the values

p	$q = 11$	$q = 19$	$q = 43$
7	$7 \cdot 13 \cdot 17 \cdot 19$	$3^7 \cdot 13 \cdot 31$	$3^6 \cdot 5^3 \cdot 7 \cdot 19 \cdot 73$
11		$2^{16} \cdot 13$	$2^{15} \cdot 7^2 \cdot 19 \cdot 29$
19			$2^{15} \cdot 3^6 \cdot 37$

p	$q = 67$	$q = 163$
7	$3^7 \cdot 5^3 \cdot 7 \cdot 13 \cdot 61 \cdot 97$	$3^8 \cdot 5^3 \cdot 7 \cdot 13 \cdot 17 \cdot 31 \cdot 103 \cdot 229 \cdot 283$
11	$2^{17} \cdot 7^2 \cdot 13 \cdot 41 \cdot 43$	$2^{15} \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 73 \cdot 79 \cdot 107 \cdot 109$
19	$2^{16} \cdot 3^7 \cdot 13 \cdot 79$	$2^{15} \cdot 3^7 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 67 \cdot 193$
43	$2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2$	$2^{19} \cdot 3^6 \cdot 5^3 \cdot 7^3 \cdot 37 \cdot 433$
67		$2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 139 \cdot 331$

It seemed pretty clear that these numbers were too highly factorized for this to be accidental. However, since we had $\ell \le p$ for $\ell \mid (j_{-p} - j_{-4})$ and $\ell \le \frac{3p}{4}$ for $\ell \mid (j_{-p} - j_{-3})$, I had expected $\ell \le \frac{pq}{4}$ for $\ell \mid (j_{-p} - j_{-q})$, and although this holds in the above table, I was worried by the fact that I never got as *big* as $\frac{pq}{4}$, e.g. for $p = 67, q = 163$ the biggest ℓ is 331, barely bigger than $2q$. From the formulas

$$\ell \mid p - x^2, \quad \ell \mid \frac{3p - x^2}{4} \qquad \text{for} \qquad \ell \mid (j_{-p} - j_{-4}), \quad \ell \mid (j_{-p} - j_{-3}),$$

I expected $\ell \mid \frac{pq - x^2}{4}$; in a typical case this gave

x	$\frac{7\cdot 163-x^2}{4}$	x	$\frac{7\cdot 163-x^2}{4}$	x	$\frac{7\cdot 163-x^2}{4}$	x	$\frac{7\cdot 163-x^2}{4}$
1	$3\cdot 5\cdot 19$	11	$3\cdot 5\cdot 17$	21	$5^2\cdot 7$	31	$3^2\cdot 5$
3	283	13	3^5	23	$3^2\cdot 17$	33	13
5	$3^2\cdot 31$	15	229	25	$3\cdot 43$		
7	$3\cdot 7\cdot 13$	17	$3\cdot 71$	27	103		
9	$5\cdot 53$	19	$3\cdot 5\cdot 13$	29	$3\cdot 5^2$		

All factors $(3, 5, 7, 13, 17, 31, 103, 229, 283)$ dividing $j_{-7} - j_{-163}$ appear on this list, but so do several others. However, for $\ell \mid j_{-p} - j_{-3}$ we had $\left(\frac{-p}{\ell}\right) = -1, \left(\frac{-3}{\ell}\right) = -1$ and similarly for $\ell \mid j_{-p} - j_{-4}$, so here we should have $\left(\frac{-p}{\ell}\right) = \left(\frac{-q}{\ell}\right) = -1$ or $\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{q}\right) = -1$. Moreover, if $\ell \mid \frac{pq-x^2}{4}$ and $\ell \neq p, q$, then $\left(\frac{pq}{\ell}\right) = +1$, so $\left(\frac{-p}{\ell}\right)$ and $\left(\frac{-q}{\ell}\right)$ are always the same. This suggests defining $\chi(d)$ on prime divisors ℓ of $\frac{pq-x^2}{4}$ by

$$\chi(\ell) = \begin{cases} \left(\frac{\ell}{p}\right) = \left(\frac{\ell}{q}\right) & \ell \neq p, q \\ \left(\frac{\ell}{p}\right) & \ell = q \\ \left(\frac{\ell}{q}\right) & \ell = p \end{cases},$$

and extend multiplicatively, setting $R(n) = \sum_{d|n} \chi(d)$, and conjecturing

Theorem.

$$\nu_\ell(N(j(\frac{1+i\sqrt{p}}{2}) - j(\frac{1+i\sqrt{q}}{2}))) = \sum_{\substack{k\in\mathbb{Z} \\ k^2<pq \\ k \text{ odd}}} \sum_{\substack{n\geq 1 \\ n \text{ odd}}} R(\frac{pq-k^2}{4\ell^n})$$

for $p \equiv q \equiv 3 \pmod 4, p, q > 3$, where N is the absolute norm to $\mathbb{Q}$.

Before trying to prove this, I worked out several examples. In particular, I wanted to understand why so *few* and such *small* primes occur in the above table; in the above theorem you'd expect $\frac{1}{4}$ of all primes $< \frac{pq}{4}$ or about 50 primes going up to 2700 in the case $p = 67, q = 163$. So I worked out that case:

x	$\frac{67\cdot 163-x^2}{4}$	Contr.	x	$\frac{67\cdot 163-x^2}{4}$	Contr.	x	$\frac{67\cdot 163-x^2}{4}$	Contr.
1	$2\cdot 3\cdot 5\cdot 7\cdot 13$	–	35	$2^3\cdot 3\cdot 101$	–	69	$2^2\cdot 5\cdot 7\cdot 11$	–
3	$2^3\cdot 11\cdot 31$	–	37	$2^2\cdot 3\cdot 199$	3^2	71	$2\cdot 3\cdot 5\cdot 7^2$	–
5	$2^2\cdot 3\cdot 227$	3^2	39	$2\cdot 5^2\cdot 47$	2^2	73	$2\cdot 3\cdot 233$	–
7	$2\cdot 3^2\cdot 151$	2^2	41	$2\cdot 3\cdot 5\cdot 7\cdot 11$	–	75	$2^2\cdot 331$	331
9	$2\cdot 5\cdot 271$	–	43	$2^2\cdot 3^4\cdot 7$	7	77	$2^5\cdot 3\cdot 13$	–
11	$2^2\cdot 3^3\cdot 5^2$	3^2	45	$2^4\cdot 139$	139	79	$2\cdot 3^2\cdot 5\cdot 13$	–
13	$2^7\cdot 3\cdot 7$	–	47	$2\cdot 3^2\cdot 11^2$	2	81	$2\cdot 5\cdot 109$	–
15	$2\cdot 7\cdot 191$	–	49	$2\cdot 3\cdot 5\cdot 71$	–	83	$2^4\cdot 3^2\cdot 7$	7
17	$2\cdot 3\cdot 443$	–	51	$2^5\cdot 5\cdot 13$	–	85	$2^2\cdot 3\cdot 7\cdot 11$	–
19	$2^4\cdot 3\cdot 5\cdot 11$	–	53	$2^2\cdot 3\cdot 13^2$	3	87	$2\cdot 419$	2^2
21	$2^2\cdot 5\cdot 131$	5^2	55	$2\cdot 3\cdot 7\cdot 47$	–	89	$2\cdot 3\cdot 5^3$	–
23	$2\cdot 3\cdot 433$	–	57	$2\cdot 7\cdot 137$	–	91	$2^2\cdot 3\cdot 5\cdot 11$	–
25	$2\cdot 3^2\cdot 11\cdot 13$	–	59	$2^2\cdot 3\cdot 5\cdot 31$	–	93	$2^3\cdot 71$	2^4
27	$2^2\cdot 7^2\cdot 13$	13	61	$2^3\cdot 3^2\cdot 5^2$	2^2	95	$2\cdot 3\cdot 79$	–
29	$2^3\cdot 3^2\cdot 5\cdot 7$	–	63	$2\cdot 11\cdot 79$	–	97	$2\cdot 3^3\cdot 7$	–
31	$2\cdot 3\cdot 5\cdot 83$	–	65	$2\cdot 3^3\cdot 31$	–	99	$2^3\cdot 5\cdot 7$	–
33	$2\cdot 1229$	2^2	67	$2^3\cdot 3\cdot 67$	–	101	$2^2\cdot 3^2\cdot 5$	5
						103	$2\cdot 3\cdot 13$	–

The last column is the contribution of $\frac{pq-x^2}{4}$ to $j(z_p)-j(z_q)$, i.e. it is

$$\ell^{s\cdot R(\frac{pq-x^2}{4\ell^2})} \text{ if } \ell^{2s-1} \mid\mid \frac{pq-x^2}{4}$$

and ℓ is the *only* non-residue dividing $\frac{pq-x^2}{4}$ to an odd power, and 1 (denoted $-$) if there are several such ℓ. The product of these contributions is

$$2^{15}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 13\cdot 139\cdot 331$$

as required, confirming the conjectured formula; the reason that there are so few contributions is that, since $-p$ and $-q$ have $h=1$, there are exceptionally many ℓ with $\left(\frac{-p}{\ell}\right)=\left(\frac{-q}{\ell}\right)=-1$ (in particular, all $\ell<17$), so almost all $\frac{pq-x^2}{4}$ have more than one such ℓ occurring to an odd power. Indeed, if we fix a prime ℓ then we can do some heuristics on the

size of the number ν_ℓ given by the formula in the theorem for $p,q\to\infty$, $\left(\frac{-p}{\ell}\right)=\left(\frac{-q}{\ell}\right)=-1$;

$$\begin{aligned}\nu_\ell &= \sum_{\substack{k^2<pq\\ k\ \text{odd}}}\ \sum_{\substack{n\geq 1\\ \ell^n\mid\frac{pq-k^2}{4}\\ n\ \text{odd}}}\ \sum_{\substack{d\geq 1\\ d\mid\frac{pq-k^2}{4\ell^n}}}\chi(d)\\ &= \sum_{\substack{n\geq 1\\ n\ \text{odd}}}\sum_{d\geq 1}\chi(d)\cdot\#\{k\in\mathbb{Z}\mid -\sqrt{pq}<k<\sqrt{pq}, k^2\equiv pq \pmod{4\ell^n d}\}\end{aligned}$$

For d small, $\#\{k\dots\}\approx\frac{\sqrt{pq}}{\ell^n d}N_{pq}(\ell^n d)$, where $N_D(d)=\#\{k \pmod{2d}\mid k^2\equiv D \pmod{4d}\}$, so ν_ℓ looks like

$$\sqrt{pq}\sum_{n\geq 1}\sum_{d\geq 1}\chi(d)\frac{N(\ell^n d)}{d}.$$

But for D a fundamental discriminant (as here) we have $\sum_{d\geq 1}N(d)d^{-s}=\zeta_{\mathbb{Q}(\sqrt{p})}(s)/\zeta(2s)$, and here ($D=pq, p\equiv q\equiv 3 \pmod 4$) we have $N(d)>0 \iff d=N(\mathfrak{a})$ for some primitive ideal $\mathfrak{a}$ of $\mathbb{Q}(\sqrt{\ell})$, $\chi(d)=\chi(\mathfrak{a})$ (genus character corresponding to $D=(-p)\cdot(-q)$,

$$\sum_{d\geq 1}\chi(d)N(d)d^{-s}=\frac{L_{-p}(s)L_{-q}(s)}{\zeta(2s)}.$$

Also, ℓ splits in $\mathbb{Q}(\sqrt{\ell})$, so

$$N(\ell^n d)=N(\ell d)=\begin{cases}2N(d) & \ell\nmid d\\ N(d) & \ell\nmid d\end{cases}\quad\text{for } n\geq 1 \text{ odd};$$

hence

$$\nu_\ell\sim\sqrt{pq}\cdot\sum_{\substack{n\geq 1\\ n\ \text{odd}}}\frac{1}{\ell^n}\cdot\frac{L_{-p}(1)L_{-q}(1)}{\zeta(2)}\cdot\frac{2}{1-\ell^{-1}}=\frac{12\ell^2}{(\ell-1)^2(\ell+1)}h(-p)h(-q)$$

where the factor $\frac{2}{1-\ell^{-1}}$ appears becase the Euler factor in

$$\frac{L_{-p}(1)L_{-p}(1)}{\zeta(2)}=\frac{1+\ell^{-1}}{1-\ell^{-1}}=1+\frac{2}{\ell}+\frac{2}{\ell^2}+\cdots$$

gets replaced here by

$$2+\frac{2}{\ell}+\frac{2}{\ell^2}+\cdots=\frac{2}{1-\ell^{-1}}.$$

For $h(-p)=h(-q)=1$ and $\ell=2,3,5,7$ this gives $16,\frac{27}{4}\approx 7,\frac{25}{8}\approx 3,\frac{49}{24}\approx 2$ in accordance with the powers to which these primes occur in the table on page 1 (when they do occur). In any case, we see that the powers of ℓ depend more on $h(-p)$ and $h(-q)$ than on p and q, which explains why they do not grow in the table on page 1.

In the formula given on page 2, I wrote $N(j_{-p}-j_{-q})$ although all j-values so far have been in $\mathbb{Q}$. Although this was the obvious conjecture, I thought I should test one case of $h>1$. The first one is $p=7,q=23$, where we get
(here every x contributes, not like the $67,163$ - case!), i.e. we should have

$$N(j(\frac{1+i\sqrt{7}}{2})-j(\frac{1+i\sqrt{23}}{2}))=5^9\cdot 7^3\cdot 17\cdot 19.$$

x	$\frac{7\cdot 23-x^2}{4}$	Contribution	x	$\frac{7\cdot 23-x^2}{4}$	Contribtuion
1	$2^3\cdot 5$	5^4	7	$2^2\cdot 7$	7^3
3	$2\cdot 19$	19^2	9	$2^2\cdot 5$	5^3
5	$2\cdot 17$	17^2	11	$2\cdot 5$	5^2

From Berwick we have (with $\theta^3-\theta-1$)

$$\begin{aligned} j(\frac{1+i\sqrt{7}}{2})-j(\frac{1+i\sqrt{23}}{2}) &= -3^3\cdot 5^3+5^3(5\theta^2+11\theta+7)^3 \\ &= 5^3\cdot[(5\theta^2+11\theta+7)-3] \\ &\quad\cdot[(5\theta^2+11\theta+7)^2+3(5\theta^2+11\theta+7)+3^2] \\ &= 5^3\cdot 7\cdot(5\theta^2+11\theta+4)(33\theta^2+46\theta+27) \end{aligned}$$

Now

$$x=5\theta^2+11\theta+4 \implies \begin{array}{l} x^2=186\theta^2+223\theta+126, \\ x^3=4757\theta^2+6369\theta+3665=22x^2+133x+361 \end{array}$$

and

$$y=33\theta^2+46\theta+27 \implies \begin{array}{l} y^2=4987\theta^2+6609\theta+3765, \\ y^3=727479\theta^2+963703\theta+549154=147y^2-170y+289 \end{array}$$

so $N(x)=19^2, N(y)=17^2$, and the formula works. In fact, we have $x=\frac{19}{\pi_{19}}\theta^7, y=\frac{17}{\pi_{17}}\theta^{14}$ where $\pi_{17}=3\theta+2, \pi_{19}=3\theta+1$, so $j(\frac{1+i\sqrt{7}}{2})-j(\frac{1+i\sqrt{23}}{2})=5^3\cdot 7\cdot\pi_{17}^*\cdot\pi_{19}^*\cdot\theta^{21}$ where $\pi_\ell^*=\frac{\ell}{\pi_\ell}$ with norm ℓ^2. This corresponds to the prime factorization you'd expect from the analogue of your results on $N(j), N(j-1728), N(j-j')$, viz.

Conjecture. *Let $K=\mathbb{Q}(\sqrt{-p}), j=j(\frac{1+i\sqrt{p}}{2}), h=h(-p)$, $A_0, A_{\pm 1}, \ldots, A_{\pm\frac{h-1}{2}}$ the ideal classes of K, $(\ell)=\ell_0\ell_1\cdots\ell_{\frac{h-1}{2}}$ the correspondingly numbered decomposition of (ℓ) in $\mathbb{Q}(j)$ ("correspondingly" means as in your paper, i.e. via the Artin symbol twisted by $\mathfrak{a}\mapsto\mathfrak{a}^2$) with $N\ell_0=\ell, N\ell_j=\ell^2$ (here $\left(\frac{\ell}{p}\right)=0$ or -1). Then*

$$\prod_{\mathrm{disc}(z)=q}\left(j(\frac{1+i\sqrt{p}}{2})-j(z)\right)=\prod_{j=0}^{\frac{h-1}{2}}\ell_j^{\sum_{k^2<pq}\sum_{n\geq 1,n\ \mathrm{odd}}R_j(\frac{pq-x^2}{4\ell^n})}.$$

($R_j(n)=\#\{\mathfrak{a}\in A_j \mid N\mathfrak{a}=n\}$).

Presumably a clever fellow like you will be able to prove the theorem on page 2 by supersingular methods, and then your proof will automatically give this; you should also be able to work out the full splitting of $j(z_{-p})-j(z_{-q})$ in the composition of $\mathbb{Q}(j_{-p})$ and $\mathbb{Q}(j_{-q})$. However, I have an analytic proof of the theorem (hence theorem & not conjecture) and, as in the cases we studied already, it gives only the norm. On the other hand, it works for $q=-3$ or -4 (or any fund. disc. $-q$ prime to p), so that I now have an analytic proof of our results for A and B separately rather than just A^2B, making me a fully justified author of our future j-paper.

Before describing my proof, let me describe a different method of getting at the above result by using the results we already have. This result strongly supports the formula given on page 2, but does not quite prove it (unless you can think of an improvement); on the other hand, it gets at $(j(z_{-p}) - j(z_{-q}))$ rather than just the norm.

Let $h_D(X)$ and $\mathcal{H}_D(X)$ be the near-polynomials

$$h_D(X) = \begin{cases} X^{1/3} & D = -3 \\ (X - 1728)^{1/2} & D = -4 \\ \prod_{\substack{\text{disc } z = D \\ \text{mod } \mathrm{SL}_2(\mathbb{Z})}} (X - j(z)) & D < -4, \end{cases}$$

$$\mathcal{H}_N(X) = \prod_{f^2 | N} h_{-N/f^2}(X) \qquad (N > 0, N \equiv 0, 3 \pmod 4)$$

so that $\deg h_D = h(D)/\frac{1}{2}w(D), \deg \mathcal{H}_N = H(N)$ (Hurwitz-Kronecker notation). If $\Phi_m(X, Y)$ is the usual modular polynomial, then, as is well known

$$\Phi_m(X, X) = \prod_{x^2 < 4m} \mathcal{H}_{4m - x^2}(X) \qquad (m \neq \square);$$

this is an actual polynomial because the multiplicity of, say, $h_{-3}(X)$ is

$$\#\{x, y \mid 4m - x^2 = 3y^2\} \equiv 0 \pmod 3.$$

For $m = \square$ we still have this formula for $\Phi_m(j, j)$ if we replace the term $\Phi_1(X, Y) = X - Y$ dividing $\Phi_m(X, Y) \pmod \square$ by $j'/2\pi i \eta(z)^4 = j^{2/3}(j - 1728)^{1/2} = \prod_{x^2 < 4} \mathcal{H}_{4 - x^2}(j)$. Then our old formula was (roughly; there are some twists for $\ell \mid m$ or $\ell = p$)

$$\nu_\ell \left(N_{\mathbb{Q}(j)/\mathbb{Q}} \Phi_m(j, j) \right) = \sum_{\substack{n \geq 1 \\ n \text{ odd}}} \sum_{\substack{x, y \in \mathbb{Z} \\ Q(x,y) < mp}} R\left(\frac{mp - Q(x, y)}{\ell^n} \right)$$

(where $j = j(\frac{1 + i\sqrt{p}}{2}), Q(x, y) =$ principal form $= (x^2 + py^2)/4$) while the new formula we want is

$$\nu_\ell \left(N_{\mathbb{Q}(j)/\mathbb{Q}} \mathcal{H}_N(j) \right) = \sum_{\substack{n \geq 1 \\ n \text{ odd}}} \sum_{x^2 < Np} R\left(\frac{Np - x^2}{\ell^n} \right) \qquad (N > 0, N \equiv 0, 3 \pmod 4).$$

But $\Phi_m(j, j) = \prod_{y^2 < 4m} \mathcal{H}_{4m - y^2}$, as stated, so the first formula can be written

$$\sum_{y^2 < 4m} \nu_\ell(N(\mathcal{H}_{4m - y^2}(j))) = \sum_{y^2 < 4m} \sum_{n \geq 1} \sum_{x^2 < (4m - y^2)p} R\left(\frac{(4m - y^2)p - x^2}{4\ell^n} \right).$$

In other words, if $(*)_N$ is the desired identity $(N > 0, N \equiv 0, 3 \pmod 4)$, then our result on Φ_m proves $\sum_{y^2 < 4m} (*)_{4m - y^2}$. Unfortunately, this is not quite enough; for each new m we get $(*)_{4m}$ and $(*)_{4m-1}$ together, so we can prove the result we need by induction. If we could prove, say, $\sum_{y^2 < 4m} y^2 \cdot (*)_{4m - y^2}$, then at each new stage we'd get $(*)_{4m-1}$ and $(*)_{4m}$ separately, which would suffice; however, I see no way to get this. (Notice, however, that the identity

$$\sum_{y^2 - 4m} H(4m - y^2) = \sum_{d | m} \max(d, \frac{m}{d}) + \begin{cases} \frac{1}{6} & m = \square \\ 0 & m \neq \square \end{cases}$$

obtained by taking the degrees of $\Phi_m(X,X) = \prod \mathcal{H}_{4m-y^2}$ is the first of an infinite series of identities giving

$$\sum_{y^2<4m} p_\nu(m,y^2)H(4m-y^2)$$

in terms of $\mathrm{tr}(T(m), S_{2\nu+2}(\mathrm{SL}_2\mathbb{Z}))$ for certain homogenous polynomials p_ν of degree ν; can these be sharpened to express $\prod \mathcal{H}_{4m-y^2}(X)^{p_\nu(m,y^2)}$ as a polynomial in X which for $X = j(E)$ relates somehow to $\mathrm{End}(E)$?)

Enough digressions; let me show you my proof of the theorem. Strangely enough, almost all of the ingredients — finding an Eisenstein series which vanishes at $s=0$ and computing $\frac{\partial}{\partial s}|_{s=0}$ of its coefficients, using Sturm's holomorphic projection in weight 2, and expressing $\log(j(z)-j(z'))$ as $\lim_{s\to 0}\left(\sum_{\gamma\in\Gamma}\ldots - \text{pole}\right)$ — are the same as in the analytic proof of the result on $N(j(z)-j(z'))$ for $\mathrm{disc}(z) = \mathrm{disc}(z') = -p$, but the starting point is completely different: instead of using Rankin's method, one uses Siegel's way (actually due to Eichler, as I think I once told you) of computing L-series of real number fields by restricting Hilbert Eisenstein series to the diagonal. More precisely, let us rewrite our conjectural result

$$\log|N(j(z_1)-j(z_2))| = \sum_{\substack{\ell \text{ prime} \\ \left(\frac{D_1}{\ell}\right)=\left(\frac{D_2}{\ell}\right)=-1}} \Big(\sum_{\substack{|k|<\sqrt{D} \\ k\equiv D \pmod 2}} \sum_{\ell^n \mid \frac{D-k^2}{4}} \sum_{d\mid \frac{D-k^2}{4\ell^n}} \chi(d)\Big)\log\ell$$

(where we have replaced $-p$ and $-q$ by arbitrary coprime fundamental discriminants $\mathrm{disc}\, z_1 = D_1, \mathrm{disc}\, z_2 = D_2 < 0$ and set $D = D_1D_2$) as

$$\begin{aligned}\sum_{\substack{\mathrm{disc}\, z_i = D_i \\ i=1,2}} \sum_{\pmod{\mathrm{SL}_2(\mathbb{Z})}} \log|j(z_1)-j(z_2)| &= \sum_{\substack{|k|<\sqrt{D} \\ k\equiv D \pmod 2}} \Big(\sum_{d\mid\frac{D-k^2}{4}} \chi(d)\log d\Big) \\ &= \sum_{\substack{\nu\in\mathcal{D}^{-1} \\ v\gg 0 \\ \mathrm{tr}(\nu)=1}} \Big(\sum_{\mathfrak{a}\mid(\nu)\mathcal{D}} \chi(\mathfrak{a})\log N(\mathfrak{a})\Big);\end{aligned}$$

here $\mathcal{D}^{-1}$ = inverse different of $\mathbb{Q}(\sqrt{D}), \nu = \frac{k+\sqrt{D}}{2\sqrt{D}}$, and $\chi(\mathfrak{a})$ in the inner sum is the genus character associated to the decomposition $D = D_1D_2$. Note that $\sum\chi(\mathfrak{a})\log N(\mathfrak{a}) = \frac{d}{ds}\left(\sum\chi(\mathfrak{a})N(\mathfrak{a})^2\right)|_{s=0}$ and that $\sum\chi(\mathfrak{a})N(\mathfrak{a})^s$ vanishes at $s=0$ ($(\nu)\mathcal{D}$ is a principal ideal with a generator $\nu\sqrt{D}$ of negative norm, and the character χ is of norm signature type since $D_1, D_2 < 0$). In other words, we are looking at the number

$$\frac{d}{ds}\sum_{\substack{\nu\gg 0 \\ \mathrm{tr}(\nu)=1}} \sigma_{s,\chi}\left((\nu)\mathcal{D}\right),$$

where

$$\sigma_{s,\chi}(\mathfrak{a}) = \sum_{\substack{\mathfrak{b}\mid\mathfrak{a} \\ \mathfrak{b}\text{ integral}}} \chi(\mathfrak{b})N(\mathfrak{b})^s.$$

for an (integral) ideal $\mathfrak{a}$.

Now in Siegel's paper, the number

$$\sum_{\substack{\nu \gg 0 \\ \mathrm{tr}\nu = m}} \sigma_{k-1,\chi}((\nu)\mathcal{D})$$

occurs as the m^{th} Fourier coefficient of the restriction to $\mathrm{SL}_2(\mathbb{Z})$ of the Eisenstein series of weight k on $\mathrm{SL}_2(\mathcal{O}_D)$ corresponding to the character χ. Siegel looked at the case $\chi =$ wide ideal class character (i.e. $\chi((\lambda)) \ \forall\ \lambda \in \mathcal{O}$), k even, but his method works equally well for χ of norm signature type (i.e. $\chi((\lambda)) = \mathrm{sign}(N(\lambda)) \ \forall\ \lambda \in \mathcal{O}$) and k odd. However, for $k = 1$ the corresponding Eisenstein series, which can be defined despite non-convergence by Hecke's method, vanishes identically. It is interesting that Hecke studied these series but failed to notice their vanishing — in fact, he claimed to show they weren't 0 — so that his whole paper was invalidated (as pointed out by Schoenberg in his footnotes to H.'s *Werke*). Van der Geer and I in our paper on $\mathbb{Q}(\sqrt{13})$ pointed out that Hecke's *method* was correct and that one could get examples of non-vanishing Eisenstein series of weight 1 on the Hilbert modular group by going to congruence subgroups. However, what I (unfortunately) didn't think of doing then was to take Hecke's series that vanish at $s = 0$ and look at their derivatives there.

Enough talk; let's calculate. Let $K = \mathbb{Q}(\sqrt{D})$ $(D > 0)$ be a real quadratic field, χ a narrow ideal class character of K of norm signature type (later, χ will be a genus character). Set

$$\begin{aligned} E(z,z';s) &= E_{k,\chi,1}(z,z',s) \\ &= \sum_{[\mathfrak{a}]} \overline{\chi(\mathfrak{a})} N(\mathfrak{a})^{1+2s} \sum_{(m,n)\in(\mathfrak{a}\times\mathfrak{a}-(0,0))/\mathcal{O}^\times} \frac{y^s y'^s}{(mz+n)(m'z'+n')(mz+n)^{2s}(m'z'+n')^{2s}} \end{aligned}$$

$(z = x+iy, z' = x'+iy' \in \mathcal{H}, s \in \mathbb{C}, \Re(s) \gg 0)$, where $[\mathfrak{a}]$ runs over all *wide* ideal classes (the summand is unchanged by $\mathfrak{a} \mapsto (\lambda)\mathfrak{a}$); this is a non-holomorphic Eisenstein series for $\mathrm{SL}_2\mathcal{O}$ and transforms like a holomorphic Hilbert modular form of weight 1. (Such forms needn't be 0, since $\mathcal{O}_K$ cannot contain a unit of norm -1.) The usual Fourier coefficient calculation gives

$$\begin{aligned} E(z,z';s) =& L_K(1+2s,\chi) y^s y'^s + D^{-1/2} L_K(2s,\chi) \Phi_s(0)^2 y^{-s} y'^{-s} \\ &+ D^{-1/2} y^{-s} y'^{-s} \sum_{\substack{\nu \in \mathcal{D}^{-1} \\ \nu \neq 0}} \sigma_{-2s,\chi}((\nu)\mathcal{D}) \Phi_s(2\pi\nu y) \Phi_s(2\pi\nu' y) e^{2\pi i(\nu x + \nu' x')} \end{aligned}$$

where

$$\Phi_s(t) = \int_{-\infty}^{\infty} \frac{e^{-ixt}}{(x+i)(x^2+1)^s} dx \qquad (t \in \mathbb{R}).$$

Now $\Phi_s(t)$ has an analytic continuation to all s (so $E(z,z';s)$ also does) with

$$\Phi_0(t) = \begin{cases} -2\pi i e^{-t} & t > 0 \\ -\pi i & t = 0 \\ 0 & t < 0 \end{cases}$$

Hence if $\chi = \bar{\chi}$ (i.e. χ is a genus character), then

$$E(z,z';0) = L_K(1,\chi) - \pi^2 D^{-1/2} L_K(0,\chi) - 4\pi^2 D^{-1/2} \sum_{\nu \gg 0} \sigma_{0,\chi}((\nu)\mathcal{D}) e^{2\pi i(\nu z + \nu' z')} \equiv 0$$

by the functional equation of $L_K(s,\chi)$ and the fact that $\chi((\nu)\mathcal{D}) = -1$ for $\nu \gg 0$. (This was the vanishing that Hecke failed to notice.) In this case we look at $\frac{d}{ds}|_{s=0}$. For $\nu \gg 0$ the factor $\Phi_s(2\pi\nu y), \Phi_s(2\pi\nu' y)$ are $\neq 0$ at $s=0$, so we replace $\sigma_{-2s,\chi}$ by its derivative and Φ_s by Φ_0. For $N(\nu) < 0$, $\sigma_{0,\chi}((\nu)\mathcal{D})$ is non-0 but one of the Φ_s vanishes. For $\nu \ll 0$, all 3 factors $\sigma_{-2,\chi}(\nu\mathcal{D}), \Phi_s(2\pi\nu y), \Phi_s(2\pi\nu' y')$ vanish, so they don't contribute. Hence

$$\frac{\partial}{\partial s}E(z,z';s)|_{s=0} = 2L_K(1,\chi)\log(yy') + 4C_\chi + 8\pi^2 D^{-1/2}\sum_{\substack{\nu\in\mathcal{D}^{-1}\\ \nu\gg 0}} \sigma'_\chi((\nu)\mathcal{D})e^{2\pi i(\nu z+\nu' z')}$$
$$-2\pi i D^{-1/2}\sum_{\substack{\nu\in\mathcal{D}^{-1}\\ \nu>0>\nu'}} \sigma_{0,\chi}((\nu)\mathcal{D})\Phi(2\pi\,|\nu'|\,y)e^{2\pi i(\nu z+\nu' z')} - (\text{same with } \nu \leftrightarrow \nu'),$$

where

$$\begin{aligned} C_\chi &= L'_K(1,\chi) + L_K(1,\chi)(\text{constant expression involving } \Gamma'(\frac{1}{2}),\ \text{etc.}),\\ \sigma'_\chi(\mathfrak{a}) &= \frac{\partial}{\partial s}\sigma_{s,\chi}(\mathfrak{a})|_{s=0} = \sum_{\mathfrak{b}|\mathfrak{a}} \chi(\mathfrak{b})\log N(\mathfrak{b}) \qquad (\mathfrak{a}\text{ integral}),\\ \Phi(t) &= e^t\cdot\frac{\partial}{\partial s}\Phi_s(-t)|_{s=0} = -2\pi i\int_1^\infty e^{-2tx}\frac{dx}{x} \qquad (t>0), \end{aligned}$$

and the term $(\nu \leftrightarrow \nu')$ is like its predecessor with ν, ν' and y, y' interchanged. Setting $z = z'$, we deduce that the function

$$E(z) = L_K(1,\chi)\log y + C_\chi + \frac{2\pi^2}{\sqrt{D}}\sum_{m=1}^\infty\Big(\sum_{\substack{\nu\in\mathcal{D}^{-1}\\ \nu\gg 0\\ \mathrm{tr}(\nu)=m}}\sigma'_\chi((\nu)\mathcal{D})\Big)e^{2\pi imz}$$
$$-\frac{\pi i}{\sqrt{D}}\sum_{m=1}^\infty\Big(\sum_{\substack{\nu\in\mathcal{D}^{-1}\\ \nu>0>\nu'\\ \mathrm{tr}(\nu)=m}}\sigma_{0,\chi}((\nu)\mathcal{D})\Phi(2\pi\,|\nu'|\,u)\Big)e^{2\pi imz}$$

transforms under $\mathrm{SL}_2(\mathbb{Z})$ like a modular form of weight 2. (Here we have divided by 4; the calculation is a little cleaner if we replace $E(z,z';s)$ by

$$E^*(z,z';s) = \pi^{-2s}D^s\Gamma(s+1)^2E(z,z';s) = -E^*(z,z';-s)$$

and work with $\Lambda_K(s,\chi)$ instead of $L_K(s,\chi)$.) Applying the holomorphic projection lemma of our paper, we deduce

$$\sum_{\substack{\nu\in\mathcal{D}^{-1}\\ \nu\gg 0\\ \mathrm{tr}(\nu)=m}}\sigma'_\chi((\nu)\mathcal{D}) = \lim_{s\to 0}\Big[2im\sum_{\substack{\nu\in\mathcal{D}^{-1}\\ \nu>0>\nu'\\ \mathrm{tr}(\nu)=m}}\sigma_{0,\chi}((\nu)\mathcal{D})\int_0^\infty\Phi(2\pi\,|\nu'|\,y)e^{-2\pi my}y^s dy + \frac{12i}{m}\frac{\sigma_1(m)}{m}\frac{L_K(1,\chi)}{s}\Big]$$
$$+\frac{12i}{\pi}\frac{\sigma_1(m)}{m}C_\chi + (\text{elementary expression})\cdot L_K(1,\chi)$$

We want to show that for $m = 1$ this reduces to

$$\sum_{\substack{\operatorname{disc} z_1 = D_1 \\ \operatorname{disc} z_2 = D_2 \\ (\mathrm{mod}\ \mathrm{SL}_2(\mathbb{Z}))}} \log|j(z_1) - j(z_2)| \qquad (\chi \leftrightarrow D = D_1 \cdot D_2);$$

the result for higher m will correspond to non-maximal orders. The calculation is exactly analogous to the one in our paper: one shows that the integral

$$\int_0^\infty \Phi(2\pi|\nu'|\, y) e^{-2\pi m y} y^s dy \quad \left(= \frac{-2\pi i \Gamma(s+1)}{(2\pi m)^{s+1}} \int_1^\infty \frac{dx}{x(1+2|\nu'|\, x)^{s+1}} \right)$$

in the above expression can be replaced by (elementary factor)$Q_s(1+\frac{2|\nu'|}{m})$ without changing the value of the limit; one then observes that

$$\sum_{\substack{\nu > 0 > \nu' \\ \operatorname{tr}(\nu) = m}} \sigma_{0,\chi}((\nu)\mathcal{D}) Q_s(1 + \frac{2|\nu'|}{m}) = \sum_{\substack{n > m\sqrt{D} \\ n \equiv mD \pmod 2}} \sigma_{0,\chi}(\frac{n + m\sqrt{D}}{2}) Q_s(\frac{n}{m\sqrt{D}}).$$

Hence (for $m = 1$)

$$\sum_{\substack{\nu \gg 0 \\ \operatorname{tr}(\nu) = 1}} \sigma'_\chi((\nu)\mathcal{D}) = (\text{elem.}) \cdot \lim_{s \to 0} \Big(\sum_{\substack{n > \sqrt{D} \\ n \equiv D \pmod 2}} R(\frac{n^2 - D}{4}) Q_s(\frac{n}{\sqrt{D}}) - \frac{\text{const.}}{s} \Big) + \text{ const.}$$

where the first constant is (elem.) $\cdot\, L_K(1,\chi) =$ (elem.) $\cdot\, h(D_1)h(D_2)$ and the second is (elem.) $\cdot\, L'_K(1,\chi) +$ (elem.) $\cdot\, L_K(1,\chi)$. On the other hand,

$$\sum_{\substack{z_1 \in \mathcal{H}/\Gamma \\ \operatorname{disc} z_1 = D_1}} \sum_{\substack{z_2 \in \mathcal{H}/\Gamma \\ \operatorname{disc} z_2 = D_2}} \log|j(z) - j(z')| =$$

$$\lim_{s \to 0} \Big(\sum_{\substack{(z_1,z_2) \in \mathcal{H}^2/\Gamma \\ \operatorname{disc} z_j = D_j\, (j=1,2)}} Q_s\Big(1 + \frac{(z_1 - z_2)^2}{2y_1 y_2}\Big) - \frac{\text{const.}}{s} \Big) + (\text{const.})$$

and one easily checks $1 + \frac{(z_1 - z_2)^2}{2y_1 y_2} = \frac{n}{\sqrt{D}}$ for some $n > \sqrt{D}$ with $\frac{n^2 - D}{4} = N\mathfrak{a}$ and that this is a 1-1 correspondence. Modulo details, that completes the proof.

This letter is getting very long and I should sign off, especially as it's 4:45 A.M. and I have a Japanese lesson today and am supposed to go skiing tomorrow. There was one other thing I wanted to mention, though. I always liked the higher Green's functions $R_k(z,z')$, whereas you prefer to stick to $j(z) - j(z')$ (or its analogues for $\Gamma_D(N)$) since you can only make sense of the finite heights in that case. However, I urge you to think seriously about R_k for $k > 1$. Our result shows that, for instance, the function $R_k(z) = \lim_{z \to z'}(R_k(z,z') - \text{singularity})$ satisfies

$$\sum_{\operatorname{disc} z = -p \pmod \Gamma} R_k(z) = \sum_{0 < n < p} \left(\sum_{d | n} \left(\frac{d}{p}\right) \log d \right) R_{Q_0}(p - n) \cdot (\frac{2n}{p} - 1)$$

if $S_{2k} = 1$ ($k = 2, 3, 4, 5, 7$). I had checked this numerically for $k = 2$ and $h(-p) = 1$, using

$$R_2(z) = \frac{\pi}{3} y + \frac{119\zeta(3)}{4\pi^2} y^{-2} - \left(4 - \frac{240}{\pi y} - \frac{120}{\pi^2 y^2}\right) e^{-2\pi y} \cos 2\pi x + \ldots$$

and got agreement (not perfect, since I don't know the coefficient of $e^{-4\pi y}$). I now looked at $p = 23$ and $p = 31$ and found (to accuracy $e^{-2\pi\sqrt{p}}$, i.e. very nearly exactly on my HP-37)

$$R_2\left(\tfrac{1+i\sqrt{23}}{2}\right) = \tfrac{1}{23}[21\log 11 + 15\log(3\theta+1) + 5\log 7 - 14\log(\theta+2) + 22\log(3\theta+2)$$
$$+15\log 5 - 40\log(2-\theta) - 23\log(2\theta-1) - 250\log\theta] + \tfrac{1}{2}\log\theta + \tfrac{1}{2}\log(3-\theta)$$
$$(\theta^3 - \theta - 1 = 0)$$

$$R_2\left(\tfrac{1+i\sqrt{31}}{2}\right) = \tfrac{1}{31}[30\log(-\theta^2+2\theta+2) + 31\log 3 + 23\log(\theta+1) - 31\log(3\theta-4)$$
$$+6\log(3-\theta) + 13\log 11 - 181\log\theta] + \tfrac{1}{2}\log(3\theta+1)$$
$$(\theta^3 - \theta^2 - 1 = 0)$$

which except for the coefficients 250 and 181 of $\log\theta$ (i.e. the choice of generator of a principal ideal) is what you would get by supposing that $pR_2(z)$ is the log of a number in $\mathbb{Q}(j)$ of the appropriate norm, found by splitting up the norm in the same way as you did for $\log N(j(z) - j(z'))$. So $R_2(z)$ (and presumably also R_3, R_4, R_5, R_7) can be used just as well as $j(z)$ to generate class fields and hence is worthy of your algebraically oriented attention; moreover, the wealth of such functions suggests that there may be canonical generators for a great many ideals in $\mathbb{Q}(j)$ or $K(j)$, so that one gets relations in the class group à la Stickelberger.

Yours, Don

[Providence, RI]
Feb 18, 1983

Dear Don,

Mea culpa – this letter is intended as my repentance. Let $p \equiv 3 \pmod 4$ be prime with $p > 3$, $K = \mathbb{Q}(\sqrt{-p}), j = j(\frac{1+\sqrt{-p}}{2}), H = K(j)$ as usual. Let N be a positive integer with $N \equiv 0, 3 \pmod 4$, so $-N$ is a discriminant of a positive definite binary quadratic form. Assume further that N is prime to p, and define $\mathcal{H}_N(x) = \prod_{f^2|N} h_{-N/f^2}(x)$ as in page 6 of your letter. For example

$$\begin{aligned} \mathcal{H}_4(x) &= (x - 1728)^{1/2} \\ \mathcal{H}_{12}(x) &= x^{1/3}(x - 2^4 3^3 5^3) \\ &\vdots \quad \text{etc.} \end{aligned}$$

The value $\mathcal{H}_N(j)$ is an algebraic integer in H, and the following theorem gives its prime factorization.

Proposition 1. *Let λ be a finite prime of H dividing the rational prime ℓ.*

(1) *If $\left(\frac{\ell}{p}\right) = +1$ then $\operatorname{ord}_\lambda(\mathcal{H}_N(j)) = 0$*

(2) *If $\left(\frac{\ell}{p}\right) = -1$ and $\lambda = \lambda_\tau$, then*

$$\operatorname{ord}_\lambda(\mathcal{H}_N(j)) = \sum_{z \geq 0} \sum_{k \geq 1} \delta(z) r_{\tau^2}\left(\frac{Np - z^2}{4\ell^k}\right)$$

where $r_{\tau^2}(m)$ is the number of integral ideals of norm m of K in the class of τ^2 ($\tau \in \operatorname{Gal}(H/K)$, and where $\delta(z) = 2$ if $z > 0$ and $z \equiv 0 \pmod p$, and $\delta(z) = 1$ otherwise.

Before the proof, some more examples:

$$\begin{aligned} p = 11 \qquad & \mathcal{H}_{12}(j) = 2^9 \cdot 11 \cdot 17 \cdot 29 \\ p = 7 \qquad & \mathcal{H}_{12}(j) = 3^4 \cdot 5^4 \cdot 17 \\ p = 11 \qquad & \mathcal{H}_{28}(j) = 7^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 41 \cdot 61 \cdot 73 \end{aligned}$$

and an obvious *corollary*: if ℓ divides $\mathbb{N}_{H/\mathbb{Q}}\mathcal{H}_N(j)$ then $\ell \leq Np/4$.

Now a sketch of the proof. If $\left(\frac{\ell}{p}\right) = +1$, the elliptic curve E with invariant j has good *ordinary* reduction $\pmod \ell$. Let E' be any curve with multiplication by an order containing $\mathcal{O}_{-N} = \mathbb{Z} + \frac{N+\sqrt{-N}}{2}\mathbb{Z}$; then $j' \neq j$ in characteristic zero, and by Deuring's theorem on the reduction of singular moduli at ordinary primes $\therefore j' \not\equiv j \pmod \lambda$.

If $\left(\frac{\ell}{p}\right) \neq +1$ the curve E has supersingular reduction $\pmod \ell$. Let W denote the integers in the maximal unramified extension of the completion H_2 and to a prime of W. We'll assume $\ell > 3$ and $\ell \neq p$ for simplicity, but everything works in those cases too. By the results in singular moduli, $\operatorname{End}_{W/\pi^k}(\tilde{E}) = R(\mathfrak{a})_k$, where $\mathfrak{a}$ is an ideal with class τ in G. If $\tilde{E}$ is isomorphic to any $\tilde{E}'$ as above, $R(\mathfrak{a})_k$ must contain an element $[\alpha, \beta]$ which satisfies the

same characteristic polynomial as $\frac{N+\sqrt{-N}}{2}$. That is:

$$\operatorname{Tr}\alpha \Rightarrow \alpha = \frac{x + N\sqrt{-p}}{2\sqrt{-p}} \quad \text{with } x \in \mathbb{Z}$$

$$\mathbb{N}[\alpha, \beta] = \alpha\bar{\alpha} + \ell^{2k-1}\beta\bar{\beta} = \frac{N^2 + N}{4}.$$

But $\alpha\bar{\alpha} = \frac{x^2+pN^2}{4p}$ and $\beta = \gamma/\sqrt{-p}$ with $\gamma \in \bar{\mathfrak{a}}/\mathfrak{a}$. Thus we get a solution to the equation:

$$(*) \qquad x^2 + 4\ell^{2k-1}\mathbb{N}\mathfrak{b} = Np$$

with $\mathfrak{b} = (\gamma)\mathfrak{a}/\bar{\mathfrak{a}}$ an integral ideal in the class of τ^2. Conversely, if we *have* a solution $(x, \mathfrak{b})$ to $(*)$, we can reverse the process to recover $\pm\mathfrak{b}$. The insistence that $x \geq 0$ fixes the sign of β whenever $x \not\equiv 0 \pmod{p}$, as we must have the congruence $\alpha \equiv \mu\beta \pmod{\mathcal{O}_{\sqrt{-p}}}$. If $x \equiv 0 \pmod{p}$ we get two possibilities (but $x = 0$ really only contributes *one*). Furthermore, if we *have* any $[\alpha, \beta]$ in $R(\mathfrak{a})_k$ satisfying the equation of $\left(\frac{N+\sqrt{-N}}{2}\right)$, by Deuring's theory we can lift the curve *together* with this endomorphism to characteristic zero. This gives a curve E' over W with $\operatorname{End}_W(E') \supseteq \mathcal{O}_{-N}$. Putting all this together in the right order gives the proof. To check the $\delta = 2$ business, try $p = 11$ and $N = 43$.

Sorry I didn't see this before - it's really identical with the formulae for $j^{1/3}$ and $(j - 1728)^{1/2}$, where I was looking for elements like i or $\rho = \frac{1+\sqrt{-3}}{2}$ in $R(\mathfrak{a})_k$. I think it should definitely go in the paper on singular moduli.

Your idea about relations in the class group had occurred to me before, but then I saw only a *finite* number of relations for each p. Now each choice of N gives a *new* principal ideal, so it's probably worth looking into carefully. But I'm worried that the primes of residue characteristic $\left(\frac{\ell}{p}\right) = +1$ never enter in ....

Best, Dick