The Gross-Zagier Theorem on Singular Moduli

Bahare Mirza

September 4, 2010
What Is The Question?

When do two elliptic curves, $E$ and $E'$, over $\bar{\mathbb{Q}}$ with Complex Multiplicatin, have the same reduction modulo a prime $p$ of the field of definition?

- When reduced curves mod $p$ have the same j-invariant.
- This happens when the prime $p$ devides $j(E) - j(E')$.

This reduces the question to factoring $j(E) - j(E')$ into primes.
Convention and Notation

Let \( d_1 \) and \( d_2 \) be two fundamental discriminants with \( \gcd(d_1, d_2) = 1 \). Define

\[
J(d_1, d_2) = \left\{ \prod_{[\tau_1], [\tau_2], \text{disc}_{\tau_i} = d_i} (j(\tau_1) - j(\tau_2)) \right\}^{4/w_1w_2},
\]

where \( w_i \) is the number of roots of unity in the quadratic field of discriminant \( d_i \).

- If \( d_1, d_2 < -4 \), \( J(d_1, d_2) \) is the absolute norm of the algebraic integer \( j(\tau_1) - j(\tau_2) \) and hence is an integer.
- In general \( J(d_1, d_2)^2 \) is an integer.

The main result of this article concerns factoring this integer.
Statement of the Theorem

Theorem

\[ J(d_1, d_2)^2 = \pm \prod_{x, n, n' \in \mathbb{Z}, \ n.n' > 0} n^{\varepsilon(n')}, \]

where \( \varepsilon \) is defined as follows; if \( n=l \) a prime with \( \left( \frac{d_1 d_2}{l} \right) \neq -1 \), let

\[ \varepsilon(l) = \begin{cases} 
\left( \frac{d_1}{l} \right) & \text{if } (d_1, l) = 1, \\
\left( \frac{d_2}{l} \right) & \text{if } (d_2, l) = 1.
\end{cases} \]

And if \( n = \prod_i l_i^{a_i} \), with \( \left( \frac{d_1 d_2}{l_i} \right) \neq -1 \), for all \( i \) (which covers all integers, \( n \), occurring in the above product), then we define

\[ \varepsilon(n) = \prod_i \varepsilon(l_i)^a. \]
Yet More Notation

For simplicity we assume \( d_1 = -p \), but let \( d_2 \) be any negative discriminant. Fix the following notation,

\[
\tau = \frac{1 + \sqrt{-p}}{2} \\
K = \mathbb{Q}(\sqrt{-p}) \\
\mathcal{O} = \mathbb{Z}[[\tau]] \text{ ring of integers in } K \\
j = j(\tau) \\
H = K(j) \text{ the Hilbert class field of } K \\
\nu \text{ a finite place in } H \\
A_{\nu} \text{ the completion of the maximal unramified extension of the ring of } \nu\text{-integers in } H \\
W_{\nu} \text{ an extension of } A_{\nu} \text{ by an element } w \text{ which satisfies a quadratic equation of discriminant } d_2 \\
e \text{ ramification index of } W_{\nu}/A_{\nu}\]
In the first step we analyze the algebraic integer

\[ \alpha = \prod_{[\tau_2]} (j - j(\tau_2))^4 \frac{w_1w_2}{\text{disc}\tau_2 = d_2} \]

in \( H \), and calculate its valuation at each finite prime, \( \nu \), of \( H \). To do this, we consider elliptic curves, \( E \) and \( E' \), over \( W = W_\nu \) with complex multiplication by \( \mathcal{O} \) and \( \mathbb{Z}[w] \) respectively, and \( j \)-invariant equal to \( j \) and \( j' = j(\tau_2) \) and good reduction at \( \nu \) and try to realize \( \text{ord}_\nu(\alpha) \) as a geometric invariant related to these two curves.
E and E’ are elliptic curves over W which is a complete discrete valuation ring. Its quotient field has characteristic zero and residue field has characteristic $l > 0$ and is algebraically closed. We wish to calculate the order of $j - j'$ with respect to $\nu$ normalized so that $\nu(\pi) = 1$ for $\pi$ a uniformizer of W. The main tool for proving the theorem is the following proposition, which interprets $\nu(j - j')$ geometrically;
**Theorem**

Let $\text{Iso}_n(E, E')$ be the set of isomorphisms from $E$ to $E'$ defined over $W/\pi^n$ and $i(n) = \frac{\text{Card}(\text{Iso}_n(E, E'))}{2}$, then we have

$$\nu(j - j') = \sum_{n \geq 1} i(n).$$

This can be proved using the fact that, to find an element of $\text{Iso}_n(E, E')$ we should solve the following system of congruences modulo $\pi^n$

$$\begin{align*}
\{ a_4 &\equiv u^4 a'_4 \\
   a_6 &\equiv u^6 a'_6,
\end{align*}$$

for $u$, unit in $W/\pi^n$. 
Next we rewrite the above equation in a manner that is merely dependant on $E$;

To every isomorphism $f : E \rightarrow E'$ corresponds an endomorphism of $E$, which has the same norm and trace as $w$ and induces the same action on the tangent space to $E$ at the origin, namely $w_f = f^{-1} \cdot w \cdot f$.

So $w_f$ belongs to the following subset of $\text{End}_n(E)$

$$S_n = \{ \alpha_0 | \text{Tr}(\alpha_0) = \text{Tr}(w), N(\alpha_0) = N(w), \alpha_0 = w \text{ on Lie}(E) \}$$

On the other hand, every element in $S_n$ is of the form $w_f$ for some isomorphism $f : E \rightarrow E' \mod \pi^n$, for some elliptic curve $E'$ with complex multiplication by the ring $\mathbb{Z}[w]$. This follows from the lifting theorem below;
Theorem

Let $E_0$ be an elliptic curve over $W/\pi^n$ and $\alpha_0$ an endomorphism of $E_0$. Assume that $\mathbb{Z}[\alpha_0]$ has rank 2 as a $\mathbb{Z}$ module and that it is integrally closed. Assume further that $\alpha_0$ induces multiplication by a quadratic element $w_0$ on $\text{Lie}(E_0)$. If there exists $w$ such that $w \equiv w_0 \mod \pi^n$ and $w^2 - \text{Tr}(w_0)w + N(w_0) = 0$, then there exists an elliptic curve over $W$ and an endomorphism $\alpha$ of $E$ such that $(E, \alpha) \equiv (E_0, \alpha_0) \mod \pi^n$, and $\alpha$ induces multiplication by $w$ on $\text{Lie}(E)$.

So we are reduced to counting the elements of $S_n$. 

Lifting Theorem
Counting $S_n$

We consider several cases;

- If $(\frac{l}{p}) = 1$, then $End_n E = \mathcal{O}$ which does not contain any element of discriminant $d_2$. So $S_n$ is empty in this case.

- If $(\frac{l}{p}) \neq 1$ then $End_1 E$ is a maximal order in the quaternion algebra which ramifies at $l$ and infinity. Here, $l$ is the residual characteristic of $\nu$.

Now we investigate more the structure of the Quaternion algebra mentioned above.

There exists a unique Quaternion algebra, up to isomorphism, over $K$ which ramifies exactly at the primes $l$ and $\infty$. This quaternion algebra can be given by the following subalgebra of 2 by 2 matrices over $K$,

$$B = \left\{ [\alpha, \beta] = \begin{pmatrix} \alpha & \beta \\ -l\bar{\beta} & \bar{\alpha} \end{pmatrix} \right\}. $$
Maximal orders of $B$ which can occur as endomorphism ring of $E$ reduced modulo $\pi$, up to isomorphism, are in 1-1 correspondence with ideal classes of $\mathcal{O}$. More precisely, if the ideal corresponding to $\tilde{E}$, curve given by reducing $E \mod \pi$, is $a$ then,

$$\text{End}_1(E) = \{[\alpha, \beta]| \alpha \in \mathcal{D}^{-1}, \beta \in \mathcal{D}^{-1} \bar{a}/a, \alpha \equiv \lambda \beta \mod \mathcal{O}_p\},$$

where $\mathcal{D}^{-1}$ is the inverse different of $\mathcal{O}$ and $\lambda$ is a square root of $-l$ modulo $\mathcal{D}$.

Again we split to several cases;

- case 1, $l$ does not divide $pq$ in which $e = 1$
- case 2, $l$ divides $q$ in which $e = 2$
- case 3, $l = p$ in which $e = 1$ again.
Case 1

Here we have,

\[ \text{End}_n(E) = \{ [\alpha, \beta] | \alpha \in \mathcal{D}^{-1}, \beta \in \mathcal{D}^{-1} l^{n-1} \bar{a}/a, \alpha \equiv \lambda \beta \mod \mathcal{O}_p \}. \]

every element of \( \text{End}_n \) with norm and trace equal to norm and trace of \( w \), is of the form \([\alpha, \beta]\) where \( \alpha = \frac{x + \text{Tr}(w) \sqrt{-p}}{2 \sqrt{-p}} \) and \( \beta = \frac{\gamma l^{n-1}}{\sqrt{-p}} \) with \( \gamma \in \bar{a}/a \). If we set \((b) = (\gamma) a/\bar{a} \), \( b \) is an integral ideal in the class of \( a^2 \). The pair \((x, b)\) satisfies the following equation,

\[ x^2 + 4 l^{2n-1} N(b) = pq. \]

On the other hand, any such pair, with a choice of generator for \( b\bar{a}/a \) gives an element, \([\alpha, \beta]\) in \( B \). If it further satisfies \( \alpha \equiv \lambda \beta \mod \mathcal{O}_p \), it would be in \( \text{End}_n(E) \) and if it induces multiplication by \( w \) on \( \text{Lie}(E) \) then it is in \( S_n \).
Counting $S_n$

Using these considerations we can count the number of elements of $S_n$. Similar considerations also gives the other two cases. We have;

- In the first case, the number of elements of $S_n$ equals $w_1/2$ times the number of solutions $(x, b)$ of

$$x^2 + 4l^{2n-1}N(b) = pq,$$

where solutions with $x \equiv 0 \mod p$ should be counted twice.

- In the second case $S_n$ is empty for $n \geq 2$ and $\#S_1$ is given the same way as the first case.

- In the third case also, for $n \geq 2$, $S_n$ is empty and $\#S_1$ is given just as above.
Conclusion

Putting together the above results for different (finite) primes, and letting $j$ vary in the set of $j$-invariants of all elliptic curves with CM with an order in a quadratic field of discriminant $d_1$, the proof of the main theorem is complete.
Thank you!