Factorisation of Singular Moduli (Gross-Zagier)

Arihant Jain

October 26th 2020

Overview

- Previous Lecture recall
- Precise Result of Gross Zagier
- More details about the Factorisation
- Examples using PARI/GP

Recall

In the previous lecture we saw some results concerning the factorisation of

$$\prod_{\substack{[\tau_1],[\tau_2] \\ disc(\tau_i)=d_i}} \Big(j(\tau_1) - j(\tau_2) \Big)$$

If ℓ divides the difference then

1. $\ell \leq \frac{d_1 d_2 - x^2}{4}$
2. ℓ doesn't split in any of $\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2})$ which is same as saying

$$\left(\frac{d_1}{\ell}\right) \neq 1 \qquad \left(\frac{d_2}{\ell}\right) \neq 1$$

Recall

In this presentation we will see precise result of Gross Zagier which tells us the multiplicities of primes as well. The result concerns the following quantity

$$J(d_1, d_2) = \left(\prod_{\substack{[\tau_1],[\tau_2] \\ disc(\tau_i)=d_i}} \Big(j(\tau_1) - j(\tau_2) \Big) \right)^{\frac{4}{w_1 w_2}}$$

- w_1, w_2 are number of roots of unity in ring of integers of $\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2})$.
- For $d_1, d_2 < -4$, $w_1, w_2 = 2$ and thus $J(d_1, d_2)$ is an integer.
- In general, $J(d_1, d_2)^2$ is an integer.

Result of Gross Zagier

For a prime ℓ satisfying $\left(\frac{d_1 d_2}{\ell}\right) \neq -1$

$$\epsilon(\ell) = \begin{cases} \left(\frac{d_1}{\ell}\right) & (d_1, \ell) = 1 \\ \\ \left(\frac{d_2}{\ell}\right) & (d_2, \ell) = 1 \end{cases}$$

For a natural number n,

$$n = \prod_i \ell_i^{a_i}$$

such that $\left(\frac{d_1 d_2}{\ell_i}\right) \neq -1$ for all i ,

$$\epsilon(n) = \prod_i \epsilon(\ell_i)^{a_i}$$

Precise Result of Gross Zagier

1. $\epsilon(\ell)$ is defined for primes ℓ satisfying $\left(\frac{d_1 d_2}{\ell}\right) \neq -1$
2. $\epsilon(\ell) = \left(\frac{d_1}{\ell}\right)$ or $\left(\frac{d_2}{\ell}\right)$ depending which one is coprime to ℓ.

Theorem (Gross Zagier)

Let $D = d_1 d_2$

$$J(d_1, d_2)^2 = \left(\prod_{\substack{[\tau_1],[\tau_2] \\ disc(\tau_i)=d_i}} \left(j(\tau_1) - j(\tau_2) \right)^{\frac{4}{w_1 w_2}} \right)^2$$

$$= \pm \prod_{|x|<\sqrt{D}} \prod_{n | \frac{D-x^2}{4}} n^{-\epsilon(n)}$$

Theorem (Gross Zagier)

Gross Zagier Factorisation

Let $D = d_1 d_2$

$$J(d_1, d_2)^2 = \pm \prod_{|x|<\sqrt{D}} \prod_{n|\frac{D-x^2}{4}} n^{-\epsilon(n)}$$

1. The primes are less than $\frac{D-x^2}{4}$: immediate from the result.
2. The primes dividing are non-split : We will deduce this in this presentation.

More details about the factorisation

$$J(d_1, d_2)^2 = \pm \prod_{|x|<\sqrt{D}} \prod_{n | \frac{D-x^2}{4}} n^{-\epsilon(n)}$$

Looking at the second product, let us define

$$F(m) := \prod_{n|m} n^{-\epsilon(n)}$$

Interestingly, the function $F(m)$ is either 1 or a power of a single prime. *It is not directly clear from the definition but can be deduced by carefully collecting the powers of each prime $\ell | m$.*

More details about the factorisation

Description of $F(m)$

For $m = \ell^{2a+1} \prod_i \ell_i^{2a_i} \prod_r q_r^{b_r}$ where $\epsilon(\ell) = \epsilon(\ell_i) = -1$ and $\epsilon(q_r) = 1$,

$$F(m) = \ell^{(a+1)(b_1+1)(b_2+1)\ldots(b_r+1)}$$

Any other case, $F(m) = 1$.

- If m has the form

$$\ell_1^{2a_1+1} \ \ell_2^{2a_2+1} \ \ell_3^{2a_3+1} \ \prod_i p_i^{a_i} \prod_j q_j^{b_j}$$

  where $\epsilon(\ell_r) = \epsilon(p_i) = -1$ and $\epsilon(q_j) = 1$ then $F(m) = 1$
- The only case $F(m) > 1$ is when there is <u>exactly one</u> prime $\ell | m$ satisfying : $\epsilon(\ell) = -1$ and $\ell^{odd} || m$.

Examples of F(m)

Consider $d_1 = -3, d_2 = -31$. Let us evaluate $F(21)$.

$$21 = 3 \times 7$$

Calculating the function $\epsilon()$ for each prime

$$\epsilon(3) = \left(\frac{-31}{3}\right) = -1$$
$$\epsilon(7) = \left(\frac{-31}{3}\right) = \left(\frac{-3}{7}\right) = \left(\frac{4}{7}\right) = 1$$

Thus for $d_1 = -3, d_2 = -31$,

$$F(21) = 3^{(1)(2)} = 3^2$$

Primes are non-split

- The only case $F(m) > 1$ is when there is exactly one prime $\ell | m$ satisfying : $\epsilon(\ell) = -1$ and $\ell^{odd} || m$.

$$J(d_1, d_2)^2 = \pm \prod_{|x|<\sqrt{D}} \prod_{d | \frac{D-x^2}{4}} d^{-\epsilon(d)} = \pm \prod_{|x|<\sqrt{D}} F\left(\frac{D-x^2}{4}\right)$$

With the description of $F(\cdot)$, we can clearly see that primes ℓ appearing in the factorisation of are those with $\ell | \frac{D-x^2}{4}$ and $\epsilon(\ell) = -1$. Hence

$$\left(\frac{d_1}{\ell}\right) \neq 1 \qquad \left(\frac{d_2}{\ell}\right) \neq 1$$

This shows our second observation from this result of Gross-Zagier.

Proofs of some results in Gross-Zagier theorem on Factorisation of Difference of Singular Moduli

Arihant Jain

1 Gross-Zagier Theorem

This theorem is from [1].

Let d_1, d_2 be negative fundamental discriminants, $(d_1, d_2) = 1$ and define

$$J(d_1, d_2) = \Bigg(\prod_{\substack{[\tau_1],[\tau_2] \\ disc(\tau_i)=d_i}} (j(\tau_1) - j(\tau_2)) \Bigg)^{\frac{4}{w_1 w_2}}$$

where w_1, w_2 are roots of unity in imaginary quadratic fields. Then we have the following factorisation

$$J(d_1, d_2)^2 = \pm \prod_{|x|<\sqrt{d_1 d_2}} \prod_{n \,|\, \frac{d_1 d_2 - x^2}{4}} n^{-\epsilon(n)}$$

The function $\epsilon(\cdot)$ is defined as follows. For primes ℓ satisfying $\left(\frac{d_1 d_2}{\ell}\right) \neq -1$,

$$\epsilon(\ell) = \begin{cases} \left(\frac{d_1}{\ell}\right) & (\ell, d_1) = 1 \\ \\ \left(\frac{d_2}{\ell}\right) & (\ell, d_2) = 1 \end{cases}$$

For a general n (with the condition that $\ell | n \implies \left(\frac{d_1 d_2}{\ell}\right) \neq 1$, we have

$$n = \prod_i \ell_i^{a_i}$$
$$\epsilon(n) = \prod_i \epsilon(\ell_i)^{a_i}$$

Hence, $\epsilon(\cdot)$ is a completely multiplicative function and defined on specific primes satisfying $(\frac{d_1 d_2}{\ell}) \neq -1$.

There are two results mentioned in the article of Gross-Zagier, which we will prove here.

1. For $D = d_1 d_2$, and $|x| < \sqrt{D}$,

$$\epsilon\left(\frac{D - x^2}{4}\right) = -1$$

2. Let us define

$$F(m) := \prod_{n|m} n^{-\epsilon(n)}$$

$F(m)$ is always 1 except just one case when there is exactly one prime ℓ with $\epsilon(\ell) = -1$ and odd exponent in the factorisation of m.

Precisely, if

$$m = \ell^{2a+1} \prod_i p_i^{2a_i} \prod_j q_j^{b_j}$$

where $\epsilon(\ell) = \epsilon(p_i) = -1$ and $\epsilon(q_j) = 1$, then

$$F(m) = \ell^{(a+1)(b_1+1)\ldots(b_j+1)}$$

2 Proof of first result

We start with $(d_1, d_2) = 1$, thus at least one of them has to be odd. Let d_1 be odd. Notice that for $d_1 < 0$, d_1 square free and $d_1 \equiv 1 (mod\, 4) \implies -d_1 \equiv 3 (mod\, 4)$, using quadratic reciprocity (for some odd prime ℓ),

$$\begin{aligned}
\left(\frac{-d_1}{\ell}\right)\left(\frac{\ell}{-d_1}\right) &= (-1)^{\frac{\ell-1}{2}} \\
\left(\frac{-1}{\ell}\right)\left(\frac{d_1}{\ell}\right)\left(\frac{\ell}{-d_1}\right) &= (-1)^{\frac{\ell-1}{2}} \\
\left(\frac{d_1}{\ell}\right)\left(\frac{\ell}{-d_1}\right) &= 1 \\
\left(\frac{d_1}{\ell}\right) &= \left(\frac{\ell}{-d_1}\right)
\end{aligned}$$

For $\ell | \frac{D-x^2}{4}$ and $(d_1, \ell) = 1$,

$$\begin{aligned}
\epsilon(\ell) &= \left(\frac{d_1}{\ell}\right) \\
&= \left(\frac{\ell}{-d_1}\right)
\end{aligned}$$

Hence for $n = \prod_i \ell_i^{a_i}$ ($l_i | \frac{D-x^2}{4}$) and $(n, d_1) = 1$, we have

$$\epsilon(n) = \left(\frac{n}{-d_1}\right)$$

The above calculation wil be helpful in proving the required result. Now let us define

$$N := \frac{d_1 d_2 - x^2}{4}$$

Let $(d_1, N) = n'$ then we have

$$N = n'n \qquad d_1 = n'd'$$

Since n' is a gcd of d_1, N, then we have $(n, d') = 1$.

$$\begin{aligned} 4n'n &= n'd'd_2 - x^2 \\ x^2 &= n'(d'd_2 - 4n) \end{aligned}$$

Clearly $n'|x^2$, thus $x = n'x'$,

$$(x')^2 n' = d'd_2 - 4n$$

As $(d_1, d_2) = 1$ it implies $(n', d_2) = 1$.

$$\epsilon(n') = \left(\frac{d_2}{n'}\right)$$

Also the calculation in the beginning shows

$$\epsilon(n) = \left(\frac{n}{-d_1}\right)$$

By multiplicativity of ϵ and $N = nn'$,

$$\epsilon(N) = \epsilon(n)\epsilon(n')$$

Thus

$$\epsilon(N) = \left(\frac{d_2}{n'}\right)\left(\frac{n}{-d_1}\right)$$

Consider $\left(\frac{n}{-d_1}\right)$. Since $d_1 = n'd'$, we have

$$\left(\frac{n}{-d_1}\right) = \left(\frac{n}{-d'}\right)\left(\frac{n}{n'}\right)$$

From the equation $(x')^2 n' = d'd_2 - 4n$, it is clear that

$$d'd_2 \equiv 4n (mod\, n') \qquad\qquad (x')^2 n' \equiv -4n (mod\, d')$$

Thus we have

$$\begin{aligned}\left(\frac{n}{-d_1}\right) &= \left(\frac{n}{-d'}\right)\left(\frac{n}{n'}\right)\\ &= \left(\frac{-n'}{-d'}\right)\left(\frac{d'd_2}{n'}\right)\\ &= \left(\frac{-n'}{-d'}\right)\left(\frac{d'}{n'}\right)\left(\frac{d_2}{n'}\right)\end{aligned}$$

Combining

$$\begin{aligned}\left(\frac{d_2}{n'}\right)\left(\frac{n}{-d_1}\right) &= \left(\frac{d_2}{n'}\right)\left(\frac{-n'}{-d'}\right)\left(\frac{d'}{n'}\right)\left(\frac{d_2}{n'}\right)\\ &= \left(\frac{-n'}{-d'}\right)\left(\frac{d'}{n'}\right)\\ &= \left(\frac{-1}{-d'}\right)\left(\frac{n'}{-d'}\right)\left(\frac{d'}{n'}\right)\\ &= \left(\frac{-1}{-d'}\right)\left(\frac{n'}{-d'}\right)\left(\frac{-1}{n'}\right)\left(\frac{-d'}{n'}\right)\\ &= \left(\frac{-1}{-d'}\right)\left(\frac{-1}{n'}\right)\left(\frac{n'}{-d'}\right)\left(\frac{-d'}{n'}\right)\\ &= \left(\frac{-1}{-d_1}\right)\left(\left(\frac{n'}{-d'}\right)\left(\frac{-d'}{n'}\right)\right)\\ &= \left(\frac{-1}{-d_1}\right)\end{aligned}$$

Last step follows by quadratic reciprocity, as $-d'n' = -d \equiv 3(mod\, 4)$. Further, $-d_1 \equiv 3(mod\, 4)$, -1 is not a quadratic residue and $\left(\frac{-1}{-d}\right) = -1$

3 Proof of Second Result

Let us first show a special property of function $F(\cdot)$.

1. For $(m, n) = 1$

$$F(mn) = F(m)^{\sum_{d|n} \epsilon(d)}\, F(n)^{\sum_{d|m} \epsilon(d)}$$

Proof: Let us rewrite $F(mn)$ as

$$\begin{aligned} F(mn) &= \prod_{d|mn} d^{-\epsilon(d)} \\ &= \prod_{d_1|m}\prod_{d_2|n}(d_1d_2)^{-\epsilon(d_1d_2)} \\ &= \prod_{d_1|m}\prod_{d_2|n} d_1^{-\epsilon(d_1d_2)}\ d_2^{-\epsilon(d_1d_2)} \\ &= \left(\prod_{d_1|m}\prod_{d_2|n} d_1^{-\epsilon(d_1d_2)}\right)\left(\prod_{d_1|m}\prod_{d_2|n} d_2^{-\epsilon(d_1d_2)}\right) \end{aligned}$$

Using $\epsilon(d_1d_2) = \epsilon(d_1)\epsilon(d_2)$

$$\begin{aligned} &= \left(\prod_{d_2|n}\prod_{d_1|m} (d_1^{-\epsilon(d_1)})^{\epsilon(d_2)}\right)\left(\prod_{d_1|n}\prod_{d_2|n} (d_2^{-\epsilon(d_2)})^{\epsilon(d_1)}\right) \\ &= \left(\prod_{d_2|n} F(m)^{\epsilon(d_2)}\right)\left(\prod_{d_1|m} F(n)^{\epsilon(d_1)}\right) \\ &= F(m)^{\sum_{d|n}\epsilon(d)}F(n)^{\sum_{d|m}\epsilon(d)} \end{aligned}$$

Let us now introduce some notation, which makes this writing and the whole proof a bit more clear. For any integer N, define

$$S(N) := \sum_{d|N}\epsilon(d)$$

So we rewrite the result just proved in this notation. For $(m, n) = 1$,

$$F(mn) = F(m)^{S(n)}F(n)^{S(m)}$$

It is easy to note that $S(\cdot)$ is multiplicative, ie, for $(m, n) = 1$

$$\sum_{d|mn}\epsilon(d) = \left(\sum_{d|m}\epsilon(d)\right)\left(\sum_{d|n}\epsilon(d)\right) \implies S(mn) = S(n)S(m)$$

Thus it is sufficient to know the behaviour of $S(\cdot)$ on prime powers. The table below lists the values of $S(p^e)$ for different possible cases.

$\epsilon(p) = 1$	$\epsilon(p) = -1$	
e: odd/even	e : even	e : odd
e+1	1	0

Table 1: Values of $S(p^e)$ depending on $\epsilon(p)$ and multiplicity e

With the results above and special property of $F(\cdot)$, we find how $F(N)$ for $N = \prod_i p_i^{e_i}$ looks like.

$$
\begin{aligned}
F(N) &= F(p_1^{e_1})^{S(p_2^{e_2} \dots p_r^{e_r})} \, F\left(p_2^{e_2} \dots p_r^{e_r}\right)^{S(p_1^{e_1})} \\
&= F(p_1^{e_1})^{S(p_2^{e_2} \dots p_r^{e_r})} \, \left[F(p_2^{e_2})^{S(p_3^{e_3} \dots p_r^{e_r})} \times F\left(p_3^{e_3} \dots p_r^{e_r}\right)^{S(p_2^{e_2})}\right]^{S(p_1^{e_1})} \\
&= F(p_1^{e_1})^{S(p_2^{e_2} \dots p_r^{e_r})} \, F(p_2)^{S(p_1^{e_1} p_3^{e_3} \dots p_r^{e_r})} \, F\left(p_3^{e_3} \dots p_r^{e_r}\right)^{S(p_1^{e_1} p_2^{e_2})}
\end{aligned}
$$

Continuing in this manner we will have

$$
\begin{aligned}
F(N) &= \left(F(p_1^{e_1})\right)^{S(p_2^{e_2} \dots p_r^{e_r})} \left(F(p_2^{e_2})\right)^{S(p_1^{e_1} p_3^{e_3} \dots p_r^{e_r})} \dots \left(F(p_r^{e_r})\right)^{S(p_1^{e_1} p_2^{e_2} \dots p_{r-1}^{e_{r-1}})} \\
&= \left(F(p_1^{e_1})\right)^{S(N/p_1^{e_1})} \left(F(p_2^{e_2})\right)^{S(N/p_2^{e_2})} \dots \left(F(p_r^{e_r})\right)^{S(N/p_r^{e_r})}
\end{aligned}
$$

where for $1 \leq k \leq r$

$$
S(N/p_k^{e_k}) = \prod_{\substack{i=1 \\ i \neq k}}^{r} S(p_i^{e_i}) S(p_1^{e_1}) S(p_2^{e_2}) \dots S(p_{k-1}^{e_{k-1}}) S(p_{k+1}^{e_{k+1}}) \dots S(p^r)^{e_r} =
$$

Let us say p_1 is the unique prime with odd multiplicity and ϵ equals to -1, ie, $\epsilon(p_1) = -1$ and e_1 is odd, then $S(p_1^{e_1}) = 0$. This makes all the powers of $F(p_2^{e_2}), F(p_3^{e_3}), \dots, F(p_r)^{e_r}$ zero, only saving powers of $F(p_1^{e_1})$. Similarly if we have more than one prime with this property then all factors will have power 0.

Existence of prime p with $\epsilon(p) = -1$: Since $\epsilon\left(\frac{d_1 d_2 - x^2}{4}\right) = -1$, then there has to be at least one prime with ϵ equal to -1.

- For exact value of $F(m)$ the following calculation is helpful.

$$
F(p^r) = \prod_{k=1}^{r} (p^k)^{-\epsilon(p^k)} = \prod_{k=1}^{r} p^{-k\epsilon(p^k)} = p^{-\sum_{k=1}^{r} k \, \epsilon(p)^k}
$$

Now we know that prime which contributes satisfies $\epsilon(p) = -1$ and r is odd. Hence,

$$
F(p^r) = p^{\frac{r+1}{2}}
$$

References

[1] Z. D. B. Gross, B.H., "On singular moduli.," *Journal für die reine und angewandte Mathematik*, vol. 355, pp. 191–220, 1984.