On the coefficients of certain family of modular equations

Nam Min, Kim[1] (with B. Cho[1] and Y. Park[1])

[1]Department of Mathematical Sciences, KAIST

Jan. 2008, East Asia Number Theory Conference

The definition of the modular equation

- $\mathfrak{H} = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$: the complex upper half plane
- $j(z) = q^{-1} + 744 + 196884q + \cdots$: the elliptic modular function on $SL_2(\mathbb{Z})$ with $z \in \mathfrak{H}$ and $q = e^{2\pi iz}$.

Consider a function

$$\Psi_n(X, z) = \prod_{\substack{a>0 \\ ad=n}} \prod_{\substack{0 \leq b < d \\ (a,b,d)=1}} \left(X - j \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} (z) \right).$$

The coefficients of $\Psi_n(X, z)$ are holomorphic modular functions and they are polynomials in $j(z)$. So there exits a polynomial $\Phi_n(X, Y) \in \mathbb{C}[X, Y]$ s.t. $\Phi_n(X, j(z)) = \Psi(X, z)$.

The definition of the modular equation

- $\mathfrak{H} = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$: the complex upper half plane
- $j(z) = q^{-1} + 744 + 196884q + \cdots$: the elliptic modular function on $SL_2(\mathbb{Z})$ with $z \in \mathfrak{H}$ and $q = e^{2\pi iz}$.

Consider a function

$$\Psi_n(X,z) = \prod_{\substack{a>0 \\ ad=n}} \prod_{\substack{0\le b<d \\ (a,b,d)=1}} \left(X - j \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} (z) \right).$$

The coefficients of $\Psi_n(X,z)$ are holomorphic modular functions and they are polynomials in $j(z)$. So there exits a polynomial $\Phi_n(X,Y) \in \mathbb{C}[X,Y]$ s.t. $\Phi_n(X,j(z)) = \Psi(X,z)$.

The definition of the modular equation

- $\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$: the complex upper half plane
- $j(z) = q^{-1} + 744 + 196884q + \cdots$: the elliptic modular function on $SL_2(\mathbb{Z})$ with $z \in \mathfrak{H}$ and $q = e^{2\pi i z}$.

Consider a function

$$\Psi_n(X, z) = \prod_{\substack{a>0 \\ ad=n}} \prod_{\substack{0 \le b < d \\ (a,b,d)=1}} \left(X - j \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} (z) \right).$$

The coefficients of $\Psi_n(X, z)$ are holomorphic modular functions and they are polynomials in $j(z)$. So there exits a polynomial $\Phi_n(X, Y) \in \mathbb{C}[X, Y]$ s.t. $\Phi_n(X, j(z)) = \Psi(X, z)$.

The definition of the modular equation

Definition + Theorem

$\Phi_n(X, Y)$ is said to be the *nth modular equation*.

- $\Phi_n(X, Y)$ is a polynomial with integral coefficients.
- $\Phi_n(X, Y)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$.
- $\Phi_p(X, Y)$ satisfies the Kronecker's congruences.

But $\Phi_n(X, Y)$ has very large coefficients even for small n.

$$\begin{aligned}\Phi_3(X,Y) &= X(X+2^{15}\cdot 3\cdot 5^3)^3 + Y(Y+2^{15}\cdot 3\cdot 5^3)^3 - X^3Y^3 \\ &+2^3\cdot 3^2\cdot 31X^2Y^2(X+Y) - 2^2\cdot 3^3\cdot 9907XY(X^2+Y^2) \\ &+2\cdot 3^4\cdot 13\cdot 193\cdot 6367X^2Y^2 \\ &+2^{16}\cdot 3^5\cdot 5^3\cdot 17\cdot 263XY(X+Y) \\ &-2^{31}\cdot 5^6\cdot 22973XY.\end{aligned}$$

The definition of the modular equation

Definition + Theorem

$\Phi_n(X,Y)$ is said to be the *nth modular equation*.

- $\Phi_n(X,Y)$ is a polynomial with integral coefficients.
- $\Phi_n(X,Y)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$.
- $\Phi_p(X,Y)$ satisfies the Kronecker's congruences.

But $\Phi_n(X,Y)$ has very large coefficients even for small n.

$$
\begin{aligned}
\Phi_3(X,Y) &= X(X+2^{15}\cdot 3\cdot 5^3)^3 + Y(Y+2^{15}\cdot 3\cdot 5^3)^3 - X^3Y^3 \\
&\quad +2^3\cdot 3^2\cdot 31X^2Y^2(X+Y) - 2^2\cdot 3^3\cdot 9907XY(X^2+Y^2) \\
&\quad +2\cdot 3^4\cdot 13\cdot 193\cdot 6367X^2Y^2 \\
&\quad +2^{16}\cdot 3^5\cdot 5^3\cdot 17\cdot 263XY(X+Y) \\
&\quad -2^{31}\cdot 5^6\cdot 22973XY.
\end{aligned}
$$

The definition of the modular equation

Definition + Theorem

$\Phi_n(X, Y)$ is said to be the *nth modular equation*.

- $\Phi_n(X, Y)$ is a polynomial with integral coefficients.
- $\Phi_n(X, Y)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$.
- $\Phi_p(X, Y)$ satisfies the Kronecker's congruences.

But $\Phi_n(X, Y)$ has very large coefficients even for small n.

$$\begin{aligned}\Phi_3(X, Y) = {} & X(X + 2^{15} \cdot 3 \cdot 5^3)^3 + Y(Y + 2^{15} \cdot 3 \cdot 5^3)^3 - X^3Y^3 \\ & +2^3 \cdot 3^2 \cdot 31X^2Y^2(X + Y) - 2^2 \cdot 3^3 \cdot 9907XY(X^2 + Y^2) \\ & +2 \cdot 3^4 \cdot 13 \cdot 193 \cdot 6367X^2Y^2 \\ & +2^{16} \cdot 3^5 \cdot 5^3 \cdot 17 \cdot 263XY(X + Y) \\ & -2^{31} \cdot 5^6 \cdot 22973XY.\end{aligned}$$

The growth of coefficients of modular equation

- $P(X_1, \cdots, X_r) \in \mathbb{C}[X_1, \cdots, X_r]$: a nonzero polynomial
- $h(P(X_1, \cdots, X_r))$: the *logarithmic height* of $P(X_1, \cdots, X_r)$ defined by the logarithm of the maximum of the absolute values of its coefficients
- f , g : complex valued functions defined on some set S
- h : a real valued positive function on S
- $f = g + \mathcal{O}(h)$: there exists an absolute positive constant A such that $|f - g| \leq A \cdot h$ on S.

The growth of coefficients of modular equation

- $P(X_1, \cdots, X_r) \in \mathbb{C}[X_1, \cdots, X_r]$: a nonzero polynomial
- $h(P(X_1, \cdots, X_r))$: the *logarithmic height* of $P(X_1, \cdots, X_r)$ defined by the logarithm of the maximum of the absolute values of its coefficients
- f , g : complex valued functions defined on some set S
- h : a real valued positive function on S
- $f = g + \mathcal{O}(h)$: there exists an absolute positive constant A such that $|f - g| \leq A \cdot h$ on S.

The growth of coefficients of modular equation

Theorem (K.Mahler, 1972)

$$h(\Phi_{2^n}(X,Y)) \leq 2^n(36n+57)\log 2.$$

Theorem (P. Cohen, 1984)

Let $\psi(n) = n\prod_{p|n}(1+\frac{1}{p})$. Then we have

$$h(\Phi_n(X,Y)) = 6\psi(n)\Big\{\log n - 2\sum_{p|n}\frac{\log p}{p} + O(1)\Big\}.$$

The growth of coefficients of modular equation

Theorem (K.Mahler, 1972)

$$h(\Phi_{2^n}(X,Y)) \leq 2^n(36n+57)\log 2.$$

Theorem (P. Cohen, 1984)

Let $\psi(n) = n\prod_{p|n}(1+\frac{1}{p})$. Then we have

$$h(\Phi_n(X,Y)) = 6\psi(n)\Big\{\log n - 2\sum_{p|n}\frac{\log p}{p} + O(1)\Big\}.$$

The growth of coefficients of modular equation

Theorem (K.Mahler, 1972)

$$h(\Phi_{2^n}(X,Y)) \leq 2^n(36n+57)\log 2.$$

Theorem (P. Cohen, 1984)

Let $\psi(n) = n\prod_{p|n}(1+\frac{1}{p})$. Then we have

$$h(\Phi_n(X,Y)) = 6\psi(n)\Big\{\log n - 2\sum_{p|n}\frac{\log p}{p} + \mathcal{O}(1)\Big\}.$$

The modular equation for $\Gamma(5)$

- $\Gamma(5) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 5 \right\}$
- $j_5(z) = q^{-1/5}(1 + q - q^3 + q^5 + \cdots)$: a Hauptmodul of $\Gamma(5)$.

Note that

$$\frac{1}{j_5(z)} = \cfrac{q^{1/5}}{1 + \cfrac{q}{1 + \cfrac{q^2}{1 + \cfrac{q^3}{1 + \cdots}}}},$$

which is the Rogers-Ramanujan continued fraction.

The modular equation for $\Gamma(5)$

- $\Gamma(5) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 5 \right\}$
- $j_5(z) = q^{-1/5}(1 + q - q^3 + q^5 + \cdots)$: a Hauptmodul of $\Gamma(5)$.

Note that

$$\frac{1}{j_5(z)} = \cfrac{q^{1/5}}{1 + \cfrac{q}{1 + \cfrac{q^2}{1 + \cfrac{q^3}{1 + \cdots}}}},$$

which is the Rogers-Ramanujan continued fraction.

The modular equation for $\Gamma(5)$

- $\Phi_n^{j_5}(X,Y)$: the *nth modular equation* for $j_5(z)$ for $(n,5)=1$.

Theorem

- $\Phi_n^{j_5}(X,Y)$ satisfies $\Phi_n^{j_5}(j_5(z), j_5(nz)) = 0$.
- $\Phi_n^{j_5}(X,Y)$ is a polynomial with integral coefficients.
- $\Phi_n^{j_5}(X,Y)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$.
- $\Phi_p^{j_5}(X,Y)$ satisfies the Kronecker's congruences for $(p,5)=1$.

But $\Phi_n^{j_5}(X,Y)$ has much smaller coefficients :

$$\Phi_3^{j_5}(X,Y) = X^4Y^3 + X^3 - 3X^2Y^2 - XY^4 - Y.$$

The modular equation for $\Gamma(5)$

- $\Phi_n^{j_5}(X,Y)$: the n*th modular equation* for $j_5(z)$ for $(n,5)=1$.

Theorem

- $\Phi_n^{j_5}(X,Y)$ satisfies $\Phi_n^{j_5}(j_5(z),j_5(nz))=0$.
- $\Phi_n^{j_5}(X,Y)$ is a polynomial with integral coefficients.
- $\Phi_n^{j_5}(X,Y)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$.
- $\Phi_p^{j_5}(X,Y)$ satisfies the Kronecker's congruences for $(p,5)=1$.

But $\Phi_n^{j_5}(X,Y)$ has much smaller coefficients :

$$\Phi_3^{j_5}(X,Y)=X^4Y^3+X^3-3X^2Y^2-XY^4-Y.$$

The modular equation for $\Gamma(5)$

- $\Phi_n^{j_5}(X,Y)$: the *nth modular equation* for $j_5(z)$ for $(n,5)=1$.

Theorem

- $\Phi_n^{j_5}(X,Y)$ satisfies $\Phi_n^{j_5}(j_5(z), j_5(nz)) = 0$.
- $\Phi_n^{j_5}(X,Y)$ is a polynomial with integral coefficients.
- $\Phi_n^{j_5}(X,Y)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$.
- $\Phi_p^{j_5}(X,Y)$ satisfies the Kronecker's congruences for $(p,5)=1$.

But $\Phi_n^{j_5}(X,Y)$ has much smaller coefficients :

$$\Phi_3^{j_5}(X,Y) = X^4Y^3 + X^3 - 3X^2Y^2 - XY^4 - Y.$$

The modular equation for $\Gamma(5)$

- $\Phi_n^{j_5}(X, Y)$: the n*th modular equation* for $j_5(z)$ for $(n, 5) = 1$.

Theorem

- $\Phi_n^{j_5}(X, Y)$ satisfies $\Phi_n^{j_5}(j_5(z), j_5(nz)) = 0$.
- $\Phi_n^{j_5}(X, Y)$ is a polynomial with integral coefficients.
- $\Phi_n^{j_5}(X, Y)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$.
- $\Phi_p^{j_5}(X, Y)$ satisfies the Kronecker's congruences for $(p, 5) = 1$.

But $\Phi_n^{j_5}(X, Y)$ has much smaller coefficients :

$$\Phi_3^{j_5}(X, Y) = X^4Y^3 + X^3 - 3X^2Y^2 - XY^4 - Y.$$

The growth of coefficients of modular equation for $\Gamma(5)$

n	$H(\Phi_n^j)$
32	$2^{12}3^{144}5^{144}11^{72}17^{18}23^{36}29^{36}47^{27}53^{18}59^{18}71^{9}83^{18}89^{18}$
41	$2^{684}3^{126}5^{126}11^{36}17^{18}23^{27}29^{36}41^{3}47^{18}59^{9}71^{18}107^{9}$
47	$2^{774}3^{144}5^{153}11^{72}17^{36}23^{27}29^{27}41^{9}47^{3}89^{18}113^{18}137^{9}$
53	$2^{900}3^{162}5^{162}11^{54}17^{54}23^{18}29^{18}41^{18}47^{18}53^{3}59^{9}83^{18}107^{18}131^{18}$

n	$H(\Phi_n^{j_5})$	$h(\Phi_n^j)/h(\Phi_n^{j_5})$
32	$2 \cdot 5 \cdot 937 \cdot 1997 \cdot 5381$	51.4514292315...
41	$2^9 \cdot 3^4 \cdot 5^3 \cdot 41 \cdot 1459$	52.7001592098...
47	$3^4 \cdot 5 \cdot 47 \cdot 311 \cdot 337 \cdot 4129$	55.3569927370...
53	$2^3 \cdot 53 \cdot 843701 \cdot 2543873$	55.1097204607...

The growth of coefficients of modular equation for $\Gamma(5)$

n	$H(\Phi_n^j)$
32	$2^{12}3^{144}5^{144}11^{72}17^{18}23^{36}29^{36}47^{27}53^{18}59^{18}71^{9}83^{18}89^{18}$
41	$2^{684}3^{126}5^{126}11^{36}17^{18}23^{27}29^{36}41^{3}47^{18}59^{9}71^{18}107^{9}$
47	$2^{774}3^{144}5^{153}11^{72}17^{36}23^{27}29^{27}41^{9}47^{3}89^{18}113^{18}137^{9}$
53	$2^{900}3^{162}5^{162}11^{54}17^{54}23^{18}29^{18}41^{18}47^{18}53^{3}59^{9}83^{18}107^{18}131^{18}$

n	$H(\Phi_n^{j_5})$	$h(\Phi_n^j)/h(\Phi_n^{j_5})$
32	$2 \cdot 5 \cdot 937 \cdot 1997 \cdot 5381$	51.4514292315...
41	$2^9 \cdot 3^4 \cdot 5^3 \cdot 41 \cdot 1459$	52.7001592098...
47	$3^4 \cdot 5 \cdot 47 \cdot 311 \cdot 337 \cdot 4129$	55.3569927370...
53	$2^3 \cdot 53 \cdot 843701 \cdot 2543873$	55.1097204607...

The growth of coefficients of modular equation for $\Gamma(5)$

n	$H(\Phi_n^j)$
32	$2^{12}3^{144}5^{144}11^{72}17^{18}23^{36}29^{36}47^{27}53^{18}59^{18}71^{9}83^{18}89^{18}$
41	$2^{684}3^{126}5^{126}11^{36}17^{18}23^{27}29^{36}41^{3}47^{18}59^{9}71^{18}107^{9}$
47	$2^{774}3^{144}5^{153}11^{72}17^{36}23^{27}29^{27}41^{9}47^{3}89^{18}113^{18}137^{9}$
53	$2^{900}3^{162}5^{162}11^{54}17^{54}23^{18}29^{18}41^{18}47^{18}53^{3}59^{9}83^{18}107^{18}131^{18}$

n	$H(\Phi_n^{j_5})$	$h(\Phi_n^j)/h(\Phi_n^{j_5})$
32	$2 \cdot 5 \cdot 937 \cdot 1997 \cdot 5381$	51.4514292315...
41	$2^9 \cdot 3^4 \cdot 5^3 \cdot 41 \cdot 1459$	52.7001592098...
47	$3^4 \cdot 5 \cdot 47 \cdot 311 \cdot 337 \cdot 4129$	55.3569927370...
53	$2^3 \cdot 53 \cdot 843701 \cdot 2543873$	55.1097204607...

The growth of coefficients of modular equation for $\Gamma(5)$

Theorem (B. Cais and B. Conrad, 2006)

For a positive integer n with $(n,5)=1$, we have

$$h(\Phi_n^{j_5}(X,Y)) = \frac{1}{10}\psi(n)\Big\{\log n - 2\sum_{p|n}\frac{\log p}{p} + \mathcal{O}(1)\Big\}.$$

Corollary

For a positive integer n with $(n,5)=1$, we have

$$\lim_{\substack{n\to\infty\\(n,5)=1}} \frac{h(\Phi_n^{j_5}(X,Y))}{h(\Phi_n^{j}(X,Y))} = \frac{1}{60}.$$

Note that $[\overline{\Gamma(1)}:\overline{\Gamma(5)}]=60$.

The growth of coefficients of modular equation for $\Gamma(5)$

Theorem (B. Cais and B. Conrad, 2006)

For a positive integer n with $(n, 5) = 1$, we have

$$h(\Phi_n^{j_5}(X,Y)) = \frac{1}{10}\psi(n)\Big\{\log n - 2\sum_{p|n}\frac{\log p}{p} + \mathcal{O}(1)\Big\}.$$

Corollary

For a positive integer n with $(n, 5) = 1$, we have

$$\lim_{\substack{n\to\infty \\ (n,5)=1}} \frac{h(\Phi_n^{j_5}(X,Y))}{h(\Phi_n^{j}(X,Y))} = \frac{1}{60}.$$

Note that $[\overline{\Gamma(1)} : \overline{\Gamma(5)}] = 60$.

The growth of coefficients of modular equation for $\Gamma(5)$

Theorem (B. Cais and B. Conrad, 2006)

For a positive integer n with $(n,5)=1$, we have

$$h(\Phi_n^{j_5}(X,Y)) = \frac{1}{10}\psi(n)\Big\{\log n - 2\sum_{p|n}\frac{\log p}{p} + \mathcal{O}(1)\Big\}.$$

Corollary

For a positive integer n with $(n,5)=1$, we have

$$\lim_{\substack{n\to\infty \\ (n,5)=1}} \frac{h(\Phi_n^{j_5}(X,Y))}{h(\Phi_n^{j}(X,Y))} = \frac{1}{60}.$$

Note that $[\overline{\Gamma(1)} : \overline{\Gamma(5)}] = 60$.

The main question

Question

- Γ : a genus zero discrete subgroup of $SL_2(\mathbb{R})$
- $f(z)$: a Hauptmodul of Γ

When can we define the modular equation $\Phi_n^f(X, Y)$?
If so, can we show

$$\lim_{\substack{n\to\infty \\ \text{some conditions}}} \frac{h(\Phi_n^f(X, Y))}{h(\Phi_n^j(X, Y))} = \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]}?$$

The main question

Question

- Γ : a genus zero discrete subgroup of $SL_2(\mathbb{R})$
- $f(z)$: a Hauptmodul of Γ

When can we define the modular equation $\Phi_n^f(X,Y)$?
If so, can we show

$$\lim_{\substack{n\to\infty \\ \text{some conditions}}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]}?$$

The main question

Question

- Γ : a genus zero discrete subgroup of $SL_2(\mathbb{R})$
- $f(z)$: a Hauptmodul of Γ

When can we define the modular equation $\Phi_n^f(X, Y)$?
If so, can we show

$$\lim_{\substack{n\to\infty \\ \text{some conditions}}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]}?$$

The main question

Question

- Γ : a genus zero discrete subgroup of $SL_2(\mathbb{R})$
- $f(z)$: a Hauptmodul of Γ

When can we define the modular equation $\Phi_n^f(X,Y)$?
If so, can we show

$$\lim_{\substack{n\to\infty \\ \text{some conditions}}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)}:\overline{\Gamma}]}?$$

The main question

Question

- Γ : a genus zero discrete subgroup of $SL_2(\mathbb{R})$
- $f(z)$: a Hauptmodul of Γ

When can we define the modular equation $\Phi_n^f(X,Y)$?

If so, can we show

$$\lim_{\substack{n\to\infty \\ \text{some conditions}}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)}:\overline{\Gamma}]}?$$

The main question

Question

- Γ : a genus zero discrete subgroup of $SL_2(\mathbb{R})$
- $f(z)$: a Hauptmodul of Γ

When can we define the modular equation $\Phi_n^f(X,Y)$?
If so, can we show

$$\lim_{\substack{n\to\infty \\ \text{some conditions}}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]}?$$

Congruence subgroups

For a positive integer N, we define congruence subgroups

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\} \\
\Gamma^0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \bmod N \right\} \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\} \\
\Gamma^1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \bmod N \right\} \\
\Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}.
\end{aligned}$$

The modular equation of classical congruence subgroup

- $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$: a genus zero subgroup
- $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$: a Hauptmodul of Γ with $a_n \in \mathbb{R}$.

The modular equation of classical congruence subgroup

Definition + Theorem

For an integer n with $(n, mN) = 1$ we define the nth modular equation as

$$\Phi_n^f(X, f(z)) = f(z)^{r_n} \cdot \prod_{\substack{a>0 \\ ad=n}} \prod_{\substack{0 \le b < d \\ (a,b,d)=1}} \left(X - f \circ \sigma_a \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} (z) \right).$$

where $\sigma_a \in SL_2(\mathbb{Z})$ s.t $\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \bmod mN$.

If $a_n \in \mathbb{Z}$, then $\Phi_n^f(X, Y) \in \mathbb{Z}[X, Y]$ and $\Phi_p^f(X, Y)$ satisfies the Kronecker's congruences.

The modular equation of classical congruence subgroup

Note that $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$.
If $\Gamma' = \Gamma_0(N_1) \cap \Gamma^0(N_2) \cap \Gamma_1(N_3) \cap \Gamma^1(N_4) \cap \Gamma(N_5)$ is an arbitrary intersection of classical congruence subgroups, then we have

$$\alpha^{-1}\Gamma'\alpha = \Gamma_1(N) \cap \Gamma_0(mN)$$

where $N = lcm(N_3, N_4, N_5)$ and

$$\alpha = \begin{pmatrix} lcm(N_2, N_4, N_5) & 0 \\ 0 & 1 \end{pmatrix}, m = \frac{lcm(N_1, N_3, N_5)lcm(N_2, N_4, N_5)}{N}.$$

The modular equation of classical congruence subgroup

- $\Gamma' = \Gamma_0(N_1) \cap \cdots \cap \Gamma(N_5)$: a genus zero subgroup.
- $g(z) = q_h^{-1} + \sum_{n=0}^{\infty} a_n q_h^n$: a Hauptmodul of Γ' ($q_h = e^{2\pi iz/h}$)

$\Rightarrow \Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$: a genus zero subgroup.
$\Rightarrow f(z) := (g \circ \alpha)(z) = g(hz) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ is a Hauptmodul of Γ.

The nth modular equation $\Phi_n^g(X, Y)$ for $g(z)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$ satisfying $\Phi_n^g(g(z), g(nz)) = 0$.
$\Rightarrow \Phi_n^g(g(hz), g(hnz)) = \Phi_n^g(f(z), f(nz)) = 0$.
$\Rightarrow \Phi_n^f(X, Y) = \Phi_n^g(X, Y)$.

The modular equation of classical congruence subgroup

- $\Gamma' = \Gamma_0(N_1) \cap \cdots \cap \Gamma(N_5)$: a genus zero subgroup.
- $g(z) = q_h^{-1} + \sum_{n=0}^{\infty} a_n q_h^n$: a Hauptmodul of Γ' ($q_h = e^{2\pi i z/h}$)

$\Rightarrow \Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$: a genus zero subgroup.
$\Rightarrow f(z) := (g \circ \alpha)(z) = g(hz) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ is a Hauptmodul of Γ.

The nth modular equation $\Phi_n^g(X, Y)$ for $g(z)$ is irreducible as a polynomial in X over $\mathbb{C}(Y)$ satisfying $\Phi_n^g(g(z), g(nz)) = 0$.
$\Rightarrow \Phi_n^g(g(hz), g(hnz)) = \Phi_n^g(f(z), f(nz)) = 0$.
$\Rightarrow \Phi_n^f(X, Y) = \Phi_n^g(X, Y)$.

The modular equation of classical congruence subgroup

For an example, since

$$\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma(5) \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} = \Gamma_1(5) \cap \Gamma_0(25)$$

and $f(z) := j_5(5z)$ is a Hauptmodul of $\Gamma_1(5) \cap \Gamma_0(25)$, we have the same nth modular equations $\Phi_n^{j_5}(X, Y) = \Phi_n^{f}(X, Y)$ when $(n, 5) = 1$.

The modular equation for noncongruence subgroup

- $N > 1$: an integer
- e : a Hall divisor of N (a positive divisor of N s.t $(e, N/e) = 1$).

Definition

For a Hall divisor e of N, an Atkin-Lehner involution of $\Gamma_0(N)$ is a matrix with determinant 1 of the form

$$\begin{pmatrix} a\sqrt{e} & b/\sqrt{e} \\ cN/\sqrt{e} & d\sqrt{e} \end{pmatrix} \text{ where } a, b, c, d \in \mathbb{Z}.$$

The modular equation for noncongruence subgroup

- $N > 1$: an integer
- e : a Hall divisor of N (a positive divisor of N s.t $(e, N/e) = 1$).

Definition

For a Hall divisor e of N, an Atkin-Lehner involution of $\Gamma_0(N)$ is a matrix with determinant 1 of the form

$$\begin{pmatrix} a\sqrt{e} & b/\sqrt{e} \\ cN/\sqrt{e} & d\sqrt{e} \end{pmatrix} \text{ where } a, b, c, d \in \mathbb{Z}.$$

The modular equation for noncongruence subgroup

- W_e : the set of all Atkin-Lehner involutions with a fixed Hall divisor e of N.
- These sets satisfy the multiplication rule :

$$W_e W_f = W_f W_e = W_k \text{ where } k = \frac{e}{(e,f)} \cdot \frac{f}{(e,f)}.$$

- S : a subset of the Hall divisors of N closed under the above multiplication rule.
- $< \Gamma_0(N), W_e >_{e \in S}$: the subgroup of $SL_2(\mathbb{R})$ generated by all elements of $\Gamma_0(N)$ and W_e for all $e \in S$.

The modular equation for noncongruence subgroup

- W_e : the set of all Atkin-Lehner involutions with a fixed Hall divisor e of N.
- These sets satisfy the multiplication rule :

$$W_eW_f = W_fW_e = W_k \text{ where } k = \frac{e}{(e,f)} \cdot \frac{f}{(e,f)}.$$

- S : a subset of the Hall divisors of N closed under the above multiplication rule.
- $< \Gamma_0(N), W_e >_{e\in S}$: the subgroup of $SL_2(\mathbb{R})$ generated by all elements of $\Gamma_0(N)$ and W_e for all $e \in S$.

The modular equation for noncongruence subgroup

Definition + Theorem (I. Chen and N. Yui, 1996)

Suppose $< \Gamma_0(N), W_e >_{e \in S}$ has genus zero.

- $\exists!$ a Hautmodul $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ s.t. $a_n \in \mathbb{Z}$.
- For a positive integer n prime to N, *the n-th modular equation* $\Phi_n^f(X, Y) = 0$ can be defined as

$$\Phi_n^f(X, f(z)) = \prod_{\substack{a>0 \\ ad=n}} \prod_{\substack{0 \le b < d \\ (a,b,d)=1}} \left(X - f \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} (z) \right).$$

- $\Phi_n^f(X, Y)$ has integral coefficients and is irreducible as a polynomial in X over $\mathbb{C}(Y)$.

The main theorem

The main theorem 1 (Cho, Kim and Park)

Let $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ be a Hauptmodul of $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$ with $a_n \in \mathbb{R}$. For a positive integer n with $(n, mN) = 1$, we have

$$h(\Phi_n^f(X,Y)) = \frac{6\psi(n)}{[\overline{\Gamma(1)} : \overline{\Gamma}]} \left\{ \log n - 2 \sum_{p|n} \frac{\log p}{p} + \mathcal{O}(1) \right\}$$

and

$$\lim_{\substack{n \to \infty \\ (n,mN)=1}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]}.$$

The main theorem

The main theorem 1 (Cho, Kim and Park)

Let $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ be a Hauptmodul of $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$ with $a_n \in \mathbb{R}$. For a positive integer n with $(n, mN) = 1$, we have

$$h(\Phi_n^f(X,Y)) = \frac{6\psi(n)}{[\overline{\Gamma(1)} : \overline{\Gamma}]}\left\{\log n - 2\sum_{p|n}\frac{\log p}{p} + \mathcal{O}(1)\right\}$$

and

$$\lim_{\substack{n\to\infty \\ (n,mN)=1}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]}.$$

The main theorem

The main theorem 1 (Cho, Kim and Park)

Let $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ be a Hauptmodul of $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$ with $a_n \in \mathbb{R}$. For a positive integer n with $(n, mN) = 1$, we have

$$h(\Phi_n^f(X,Y)) = \frac{6\psi(n)}{[\overline{\Gamma(1)} : \overline{\Gamma}]} \left\{ \log n - 2 \sum_{p|n} \frac{\log p}{p} + \mathcal{O}(1) \right\}$$

and

$$\lim_{\substack{n\to\infty \\ (n,mN)=1}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]}.$$

The main theorem

The main theorem 2 (Cho, Kim and Park)

Let $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ be a Hauptmodul of $< \Gamma_0(N), W_e >_{e \in S}$ with $a_n \in \mathbb{R}$. For a positive integer n with $(n, N) = 1$, we have

$$h(\Phi_n^f(X,Y)) = \sum_{e \in S} \frac{6\psi(n)}{\overline{[\overline{\Gamma(1)} : \overline{\Gamma_0(N/e)}]}} \left\{ \log n - 2 \sum_{p|n} \frac{\log p}{p} + \mathcal{O}(1) \right\}$$

and

$$\lim_{\substack{n \to \infty \\ (n,N)=1}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \sum_{e \in S} \frac{1}{\overline{[\overline{\Gamma(1)} : \overline{\Gamma_0(N/e)}]}}.$$

The main theorem

The main theorem 2 (Cho, Kim and Park)

Let $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ be a Hauptmodul of $< \Gamma_0(N), W_e >_{e \in S}$ with $a_n \in \mathbb{R}$. For a positive integer n with $(n, N) = 1$, we have

$$h(\Phi_n^f(X,Y)) = \sum_{e \in S} \frac{6\psi(n)}{\overline{[\Gamma(1) : \Gamma_0(N/e)]}} \left\{ \log n - 2 \sum_{p|n} \frac{\log p}{p} + \mathcal{O}(1) \right\}$$

and

$$\lim_{\substack{n \to \infty \\ (n,N)=1}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \sum_{e \in S} \frac{1}{\overline{[\Gamma(1) : \Gamma_0(N/e)]}}.$$

The main theorem

The main theorem 2 (Cho, Kim and Park)

Let $f(z) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n$ be a Hauptmodul of $< \Gamma_0(N), W_e >_{e \in S}$ with $a_n \in \mathbb{R}$. For a positive integer n with $(n, N) = 1$, we have

$$h(\Phi_n^f(X,Y)) = \sum_{e \in S} \frac{6\psi(n)}{[\overline{\Gamma(1)} : \overline{\Gamma_0(N/e)}]} \left\{ \log n - 2 \sum_{p|n} \frac{\log p}{p} + \mathcal{O}(1) \right\}$$

and

$$\lim_{\substack{n \to \infty \\ (n,N)=1}} \frac{h(\Phi_n^f(X,Y))}{h(\Phi_n^j(X,Y))} = \sum_{e \in S} \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma_0(N/e)}]}.$$

Proof of the main theorem 1

Lemma

Γ (and $< \Gamma_0(N), W_e >_{e \in S}$) have no elliptic points on $i\mathbb{R}_{>1}$.

We have assumed that $f(z) = q^{-1} + \cdots$ has real Fourier coefficients.

$\Rightarrow f(it)$ is real and $f(it) \to \infty$ as $t \to \infty$
$\Rightarrow f'(z)$ is nonvanishing on $i\mathbb{R}_{>1}$ by Lemma.
$\Rightarrow f(it)$ is strictly increasing for $t \geq 1$.
$\Rightarrow$ We can choose real numbers $s > 1$ and $1 \leq t_0 \leq t_1$ such that $f(it_0) = s, f(it_1) = 2s$.

Proof of the main theorem 1

Lemma

Γ (and $< \Gamma_0(N), W_e >_{e \in S}$) have no elliptic points on $i\mathbb{R}_{>1}$.

We have assumed that $f(z) = q^{-1} + \cdots$ has real Fourier coefficients.

$\Rightarrow f(it)$ is real and $f(it) \to \infty$ as $t \to \infty$

$\Rightarrow f'(z)$ is nonvanishing on $i\mathbb{R}_{>1}$ by Lemma.

$\Rightarrow f(it)$ is strictly increasing for $t \geq 1$.

$\Rightarrow$ We can choose real numbers $s > 1$ and $1 \leq t_0 \leq t_1$ such that $f(it_0) = s, f(it_1) = 2s$.

Proof of the main theorem 1

Lemma

Γ (and $< \Gamma_0(N), W_e >_{e \in S}$) have no elliptic points on $i\mathbb{R}_{>1}$.

We have assumed that $f(z) = q^{-1} + \cdots$ has real Fourier coefficients.

$\Rightarrow f(it)$ is real and $f(it) \to \infty$ as $t \to \infty$

$\Rightarrow f'(z)$ is nonvanishing on $i\mathbb{R}_{>1}$ by Lemma.

$\Rightarrow f(it)$ is strictly increasing for $t \geq 1$.

$\Rightarrow$ We can choose real numbers $s > 1$ and $1 \leq t_0 \leq t_1$ such that $f(it_0) = s, f(it_1) = 2s$.

Proof of the main theorem 1

Lemma

Γ (and $< \Gamma_0(N), W_e >_{e \in S}$) have no elliptic points on $i\mathbb{R}_{>1}$.

We have assumed that $f(z) = q^{-1} + \cdots$ has real Fourier coefficients.

- $\Rightarrow f(it)$ is real and $f(it) \to \infty$ as $t \to \infty$
- $\Rightarrow f'(z)$ is nonvanishing on $i\mathbb{R}_{>1}$ by Lemma.
- $\Rightarrow f(it)$ is strictly increasing for $t \geq 1$.
- $\Rightarrow$ We can choose real numbers $s > 1$ and $1 \leq t_0 \leq t_1$ such that $f(it_0) = s, f(it_1) = 2s$.

Proof of the main theorem 1

Lemma 1

Let $1 \leq t_0 \leq t \leq t_1$. We have

$$h(\Phi_n^f(X, f(it))) = \frac{6\psi(n)}{[\overline{\Gamma(1)} : \overline{\Gamma}]}\Big(\log n - 2\sum_{p|n}\frac{\log p}{p} + \mathcal{O}(1)\Big),$$

Lemma (P. Cohen)

Let $P(X) \in \mathbb{C}[X]$ be any nonzero polynomial of degree $\leq D$. Then for any $s > 0$, there exists an absolute constant $c_s > 0$, depending only on s, such that

$$|(h(P(X)) - \log \sup_{s \leq x \leq 2s} |P(x)|| \leq c_s D.$$

Proof of the main theorem 1

Lemma 1

Let $1 \leq t_0 \leq t \leq t_1$. We have

$$h(\Phi_n^f(X, f(it))) = \frac{6\psi(n)}{[\overline{\Gamma(1)} : \overline{\Gamma}]}\Big(\log n - 2\sum_{p|n}\frac{\log p}{p} + \mathcal{O}(1)\Big),$$

Lemma (P. Cohen)

Let $P(X) \in \mathbb{C}[X]$ be any nonzero polynomial of degree $\leq D$. Then for any $s > 0$, there exists an absolute constant $c_s > 0$, depending only on s, such that

$$|(h(P(X)) - \log \sup_{s \leq x \leq 2s} |P(x)|| \leq c_s D.$$

Proof of the main theorem 1

Proof of the main theorem 1. Let $D = \psi(n)$. If we write $\Phi_n^f(X,Y) = P_0(Y)X^D + P_1(Y)X^{D-1} + \cdots + P_D(Y)$, then $h(\Phi_n^f(X,Y)) = \max_{0\le j\le D} h(P_j(Y))$. Since $\deg P_j(Y) \le D$,

$$\begin{aligned} h(\Phi_n^f(X,Y)) &= \max_{0\le j\le D} \log \sup_{s\le y\le 2s} |P_j(y)| + \mathcal{O}(D) \\ &= \sup_{s\le y\le 2s} \max_{0\le j\le D} \log |P_j(y)| + \mathcal{O}(D) \\ &= \sup_{s\le y\le 2s} h(\Phi_n^f(X,y)) + \mathcal{O}(D) \\ &= \sup_{t_0\le t\le t_1} h(\Phi_n^f(X,f(it))) + \mathcal{O}(D), \end{aligned}$$

because the interval $[t_0, t_1]$ corresponds bijectively to the interval $[s, 2s]$ □

Proof of the main theorem 1

Proof of the main theorem 1. Let $D = \psi(n)$. If we write $\Phi_n^f(X,Y) = P_0(Y)X^D + P_1(Y)X^{D-1} + \cdots + P_D(Y)$, then $h(\Phi_n^f(X,Y)) = \max_{0\leq j\leq D} h(P_j(Y))$. Since $\deg P_j(Y) \leq D$,

$$\begin{aligned} h(\Phi_n^f(X,Y)) &= \max_{0\leq j\leq D} \log \sup_{s\leq y\leq 2s} |P_j(y)| + \mathcal{O}(D) \\ &= \sup_{s\leq y\leq 2s} \max_{0\leq j\leq D} \log |P_j(y)| + \mathcal{O}(D) \\ &= \sup_{s\leq y\leq 2s} h(\Phi_n^f(X,y)) + \mathcal{O}(D) \\ &= \sup_{t_0\leq t\leq t_1} h(\Phi_n^f(X, f(it))) + \mathcal{O}(D), \end{aligned}$$

because the interval $[t_0, t_1]$ corresponds bijectively to the interval $[s, 2s]$ $\square$

Thank you!

Proof of lemma 1

lemma

For $t_0 \le t \le t_1$, we have $h(\Phi_n^f(X, f(it))) = \sum_{\substack{a>0 \\ ad=n}} S_d(t) + \mathcal{O}(\psi(n))$,
where $S_d(t) = \sum_{\substack{0 \le b < d \\ (a,b,d)=1}} \log\max\{1, |f \circ \sigma_a(\frac{ait+b}{d})|\}$

Proof. The coefficients of polynomial $P(x) = (x - w_1)\cdots(x - w_d)$ lie between $2^{-d}M$ and $2^d M$ where $M = \prod_{j=1}^d \max\{1, |w_j|\}$.

$$\Rightarrow h(P) = \sum_{j=1}^d \log\max\{1, |w_j|\} + \mathcal{O}(d).$$

$$\therefore \Phi_n^f(X, f(it)) = f(z)^{r_n} \prod_{\substack{a>0 \\ ad=n}} \prod_{\substack{0 \le b < d \\ (a,b,d)=1}} \left(X - (f \circ \sigma_a)\left(\frac{ait+b}{d}\right)\right)$$

$$\Rightarrow h(\Phi_n^f(X, f(it))) = r_n \log f(it) + \sum_{\substack{a>0 \\ ad=n}} \sum_{\substack{0 \le b < d \\ (a,b,d)=1}} \log\max\left\{1, \left|f \circ \sigma_a\left(\frac{ait+b}{d}\right)\right|\right\} + \mathcal{O}(\psi(n)),$$

where $r_n \log f(it) = \mathcal{O}(\psi(n))$. □

Proof of lemma 1

Next goal is to calculate each term in the summation

$$S_d(t) = \sum_{\substack{0 \le b < d \\ (a,b,d)=1}} \log\max\left\{1, \left|f \circ \sigma_a\left(\frac{ait+b}{d}\right)\right|\right\}.$$

Lemma

For $z = \xi + i\eta \in \mathfrak{H}$, let $g(z) = a_{-1}q_h^{-1} + \sum_{n=0}^{\infty} a_n {q_h}^n$ with $q_h = e^{2\pi i z/h}$ for a positive integer h. We assume that if $a_{-1} = 0$ (respectively, $a_{-1} \neq 0$), then $g(z)$ (respectively, $q_h g(z)$) is absolutely convergent for $\eta > 0$. Then for $\eta \geq 1/2$, we have

$$\log\max\{1, |g(z)|\} = \begin{cases} \mathcal{O}(1) & \text{if } a_{-1} = 0, \\ 2\pi i\eta/h + \mathcal{O}(1) & \text{if } a_{-1} \neq 0. \end{cases}$$

Proof of lemma 1

It is necessary to study the behavior of Hauptmodul at each cusp of $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$ (or $< \Gamma_0(N), W_e >_{e \in S}$).

Lemma

Let $\Gamma = \Gamma_1(N) \cap \Gamma_0(mN)$ and

$$\Delta = \{\overline{\pm(1+Nk)} \in (\mathbb{Z}/mN\mathbb{Z})^\times \mid k = 0, \cdots, m-1\}.$$

We assume that a, c, a' and c' are integers such that $(a,c) = (a',c') = 1$. By $\frac{\pm 1}{0}$ we mean ∞. Then the cusp $\frac{a}{c}$ is equivalent to $\frac{a'}{c'}$ under Γ if and only if there exist $x \in \Delta$ and $n \in \mathbb{Z}$ such that

$$\begin{pmatrix} a' \\ c' \end{pmatrix} \equiv \begin{pmatrix} x^{-1}a + nc \\ xc \end{pmatrix} \bmod mN.$$

Proof of lemma 1

Let M be a positive integer. P. Cohen proved that

$$I_M = [\frac{1}{M+1}, \frac{M+2}{M+1}) = \bigcup_{k=1}^{M} \bigcup_{\substack{h=1 \\ (h,k)=1}}^{k} I_M(h/k),$$

which is a disjoint union of sets $I_M(h/k)$. Here each $I_M(h/k)$ is an interval of the form $[\rho_1^{(h/k)}, \rho_2^{(h/k)})$ containing h/k and

$$\frac{1}{2Mk} \leq h/k - \rho_1^{(h/k)} \leq \frac{1}{(M+1)k}$$

$$\frac{1}{2Mk} \leq \rho_2^{(h/k)} - h/k \leq \frac{1}{(M+1)k}.$$

Proof of lemma 1

Note that we may reindex the sum in $S_d(t)$ via

$$b \mapsto \begin{cases} b & \text{if } \frac{b}{d} \in [\frac{1}{N+1}, 1), \\ b+d & \text{if } \frac{b}{d} \in [0, \frac{1}{N+1}). \end{cases}$$

For real numbers h, k and x, we put

$$g_{h,k}(x) = \frac{2\pi nt/d^2k^2}{(\frac{at}{d})^2 + (x - \frac{h}{k})^2}.$$

Proof of lemma 1

Lemma

Let $T(t,z,b,d) = \log\max\left\{1, \left|f\circ\sigma_a\left(\frac{ait+b}{d}\right)\right|\right\}$.
(1) If $at/d \geq 1/2$, then

$$T(t,z,b,d) = \begin{cases} 2\pi nt/d^2 + \mathcal{O}(1) & \text{if } \overline{a}\in\Delta, \\ \mathcal{O}(1) & \text{otherwise.} \end{cases}$$

(2) Put $M = [d/\sqrt{nt}]$. If $at/d \leq 1$, then $M \geq 1$ and, for $b/d \in I_M(h/k)$, then

$$T(t,z,b,d) = \begin{cases} g_{h,k}(b/d) + \mathcal{O}(1) & \text{if } k\equiv 0 \bmod mN \text{ and } \overline{h}\in\overline{a}\Delta, \\ \mathcal{O}(1) & \text{otherwise.} \end{cases}$$

Proof of lemma 1

Now, we calculate $S_d(t)$ more precisely. To this end we need the following lemma.

Lemma

Let k, j and a be positive integers satisfying $j|k$ and $(j, a) = 1$. We further let ζ be a primitive kth root of unity and let

$$c'_k(l) = \sum_{\substack{h \in (\mathbb{Z}/k\mathbb{Z})^\times \\ h \equiv a \bmod j}} \zeta^{hl} \text{ for } l \in \mathbb{Z}.$$

Then

$$|c'_k(l)| \leq j \cdot (k, l) \text{ for any } l \in \mathbb{Z}. \tag{1}$$

Proof of lemma 1

Lemma 2

(1) If $d < \sqrt{nt}$, then $S_d(t) = \mathcal{O}(n/d)$.
(2) If $d \geq \sqrt{nt}$, then

$$\begin{aligned} S_d(t) &= \frac{1}{[\overline{\Gamma(1)} : \overline{\Gamma}]} \cdot \frac{6d}{(a,d)} \phi((a,d)) \log(d^2/n) \\ &+ \mathcal{O}\left(\sigma_1\left(\frac{d}{(a,d)}\right)\right) + \mathcal{O}\left(\frac{d\sigma_1((a,d))}{(a,d)}\right), \end{aligned}$$

where $\phi(x)$ is the Euler function and $\sigma_1(x)$ is the sum of positive divisors of x.

Sketch of proof of lemma 2

Proof of lemma 2.(2) Note that the assumption $d \geq \sqrt{nt}$ implies $\frac{at}{d} \leq 1$. Put $M = [\frac{d}{\sqrt{nt}}] \geq 1$. Then we have

$$\begin{aligned} S_d(t) &= \sum_{k=1}^{M} \sum_{\substack{h=1 \\ (h,k)=1}}^{k} \sum_{\substack{b/d \in I_M(h/k) \\ 0 \leq b < d \\ (a,b,d)=1}} \log\max\left\{1, \left| f \circ \sigma_a\left(\frac{ait+b}{d}\right)\right| \right\} \\ &= \sum_{\substack{1 \leq h \leq k \leq M \\ (h,k)=1 \\ k \equiv 0 \bmod mN \\ h \in \bar{a}\Delta}} \sum_{\substack{b/d \in I_M(h/k) \\ 0 \leq b < d \\ (a,b,d)=1}} g_{h,k}(b/d) + \mathcal{O}(d). \end{aligned}$$

Sketch of proof of lemma 2

Take

$$\sum_{\substack{b/d\in I_M(h/k)\\ 0\le b<d,(a,b,d)=1}} g_{h,k}(b/d) = k^{-2}\sum_{f|(a,d)}\mu(f)F_f\left(\frac{dh}{fk}\right)+\mathcal{O}\left(\frac{\sqrt{n}\sigma_1((a,d))}{k(a,d)}\right),$$

where $F_f(\theta)=\frac{2\pi^2 d}{f}\sum_{v\in\mathbb{Z}} e^{-2\pi|v|nt/df}e^{2\pi iv\theta}$ and $\mu(x)$ is the Möbius function.

$$S_d(t)=\sum_{f|(a,d)}\mu(f)\sum_{\substack{1\le h\le k\le M\\ (h,k)=1\\ k\equiv 0 \bmod mN\\ \overline{h}\in\overline{a}\Delta}} k^{-2}F_f(dh/fk)+\mathcal{O}\left(\frac{d\sigma_1((a,d))}{(a,d)}\right).$$

Sketch of proof of lemma 2

We now consider the sum

$$\sum_{\substack{1\le h\le k\le M\\(h,k)=1\\k\equiv 0 \bmod mN\\ \overline{h}\in\overline{a}\Delta}} k^{-2}F_f(dh/fk) = \frac{2\pi^2 d}{f}\sum_{\nu\in\mathbb{Z}} C_M(d\nu/f)e^{-2\pi|\nu|nt/df}, \qquad (2)$$

where

$$C_M(l) = \sum_{\substack{1\le k\le M\\k\equiv 0 \bmod mN}} k^{-2}c_k(l)$$

and

$$c_k(l) = \sum_{\substack{1\le h\le k\\(h,k)=1\\ \overline{h}\in\overline{a}\Delta}} e^{2\pi ihl/k} \text{ for any } l\in\mathbb{Z}.$$

Sketch of proof of lemma 2

We have to calculate $C_M(l)$ and $c_k(l)$ to know the upper bound of the sum of (2). By lemma, $|c_k(l)| \leq |\Delta| mN(k,l)$ for $l \in \mathbb{Z} - \{0\}$. So when $l \neq 0$, we have

$$\begin{aligned} |C_M(l)| &\leq |\Delta| mN \sum_{k=1}^{\infty} k^{-2}(k,l) \leq |\Delta| mN \sum_{d|l} d \sum_{j=1}^{\infty} \frac{1}{j^2 d^2} \\ &= |\Delta| mN \frac{\pi^2}{6} \frac{1}{|l|} \sum_{d|l} \frac{|l|}{d} = |\Delta| mN \frac{\pi^2}{6} \frac{\sigma_1(|l|)}{|l|}. \end{aligned}$$

So $|C_M(l)| = \mathcal{O}\left(\frac{\sigma_1(|l|)}{|l|}\right)$ for $l \neq 0$.

Sketch of proof of lemma 2

For $l = 0$, $\pi : (\mathbb{Z}/k\mathbb{Z})^\times \to (\mathbb{Z}/mN\mathbb{Z})^\times$ gives us

$$c_k(0) = |\pi^{-1}(\Delta)| = |\Delta||\ker \pi| = |\Delta|\frac{\phi(k)}{\phi(mN)}.$$

$$\begin{aligned} C_M(0) &= \sum_{\substack{1 \le k \le M \\ k \equiv 0 \bmod mN}} k^{-2} \frac{|\Delta|}{\phi(mN)} \phi(k) \\ &= \frac{6}{\pi^2} \frac{|\Delta|}{\phi(mN)[\Gamma(1) : \Gamma_0(mN)]} \log M + \mathcal{O}(1) \\ &= \frac{6}{\pi^2[\overline{\Gamma(1)} : \overline{\Gamma}]} \log M + \mathcal{O}(1), \end{aligned}$$

because

$$[\overline{\Gamma(1)} : \overline{\Gamma}] = [\overline{\Gamma(1)} : \overline{\Gamma_0(mN)}][\overline{\Gamma_0(mN)} : \overline{\Gamma}] = \frac{[\overline{\Gamma(1)} : \overline{\Gamma_0(mN)}]\phi(mN)}{|\Delta|}.$$

Sketch of proof of lemma 2

Therefore we get

$$\sum_{\substack{1\le h\le k\le M\\ (h,k)=1\\ h\equiv 0 \bmod mN\\ \overline{h}\in\overline{a}\Delta}} k^{-2}F_f(dh/fk) = \frac{12d}{f[\overline{\Gamma(1)}:\overline{\Gamma}]}\log M + \mathcal{O}\left(d/f\right)$$

So we obtain

$$\begin{aligned} S_d(t) &= \sum_{f|(a,d)} \mu(f)\left(\frac{6d}{f[\overline{\Gamma(1)}:\overline{\Gamma}]}\log(d^2/n) + \mathcal{O}(d/f)\right. \\ &+ \left.\mathcal{O}\left(\sigma_1(d/f)e^{-2\pi n/df}\right)\right) + \mathcal{O}\left(\frac{d\sigma_1((a,d))}{(a,d)}\right). \square \end{aligned}$$

Proof of lemma 1

Proof of lemma 1. We have shown that

$$h(\Phi_n^f(X, f(it))) = \sum_{\substack{a>0 \\ ad=n}} S_d(t) + \mathcal{O}(\psi(n)) = H_1 + H_2 + \mathcal{O}(\psi(n)),$$

where

$$H_1 = \sum_{\substack{a>0, ad=n \\ d<\sqrt{nt}}} S_d(t) = \mathcal{O}(\psi(n))$$

and

$$H_2 = \sum_{\substack{a>0, ad=n \\ d\geq\sqrt{nt}}} S_d(t) = \frac{6\psi(n)}{[\overline{\Gamma(1)} : \overline{\Gamma}]} \left(\log n - 2 \sum_{p|n} \frac{\log p}{p} + \mathcal{O}(1) \right). \square$$