Modular units and cuspidal divisor class groups of $X_1(N)$

Yifan Yang

National Chiao Tung University, Taiwan

East Asia Number Theory Conference, 24 Jan 2008

Modular units

Let Γ be a congruence subgroup of $SL(2,\mathbb{Z})$.

- A modular unit on Γ is a modular function on Γ such that its zeros and poles concentrate on the cusps.
- For example, $\eta(2\tau)^{24}/\eta(\tau)^{24}$ is a modular unit on $\Gamma_0(2)$, where
$$\eta(\tau) = e^{2\pi i\tau/24}\prod_{n=1}^{\infty}(1-e^{2\pi in\tau})$$
is the Dedekind eta function.

Modular units

Let Γ be a congruence subgroup of $SL(2, \mathbb{Z})$.

- A modular unit on Γ is a modular function on Γ such that its zeros and poles concentrate on the cusps.
- For example, $\eta(2\tau)^{24}/\eta(\tau)^{24}$ is a modular unit on $\Gamma_0(2)$, where

$$\eta(\tau) = e^{2\pi i\tau/24} \prod_{n=1}^{\infty} (1 - e^{2\pi in\tau})$$

  is the Dedekind eta function.

Arithmetic significance

- Special values of modular units on $\Gamma(N)$ generate the ray class fields of imaginary quadratic number fields. (The so-called Ramachandra-Robert invariants.)
- Appear in the Kronecker limit formulas for the L-functions associated with characters of the ray class groups of imaginary quadratic number fields.
- Suitable products of Ramachandra-Robert invariants are units in the ray class fields. (The so-called elliptic units.)
- The elliptic units play an important role in Coates and Wiles' proof of the BSD conjecture for elliptic curves with CM by an imaginary quadratic field of class number 1.

Arithmetic significance

- Special values of modular units on $\Gamma(N)$ generate the ray class fields of imaginary quadratic number fields. (The so-called Ramachandra-Robert invariants.)
- Appear in the Kronecker limit formulas for the L-functions associated with characters of the ray class groups of imaginary quadratic number fields.
- Suitable products of Ramachandra-Robert invariants are units in the ray class fields. (The so-called elliptic units.)
- The elliptic units play an important role in Coates and Wiles' proof of the BSD conjecture for elliptic curves with CM by an imaginary quadratic field of class number 1.

Arithmetic significance

- Special values of modular units on $\Gamma(N)$ generate the ray class fields of imaginary quadratic number fields. (The so-called Ramachandra-Robert invariants.)
- Appear in the Kronecker limit formulas for the L-functions associated with characters of the ray class groups of imaginary quadratic number fields.
- Suitable products of Ramachandra-Robert invariants are units in the ray class fields. (The so-called elliptic units.)
- The elliptic units play an important role in Coates and Wiles' proof of the BSD conjecture for elliptic curves with CM by an imaginary quadratic field of class number 1.

Arithmetic significance

- Special values of modular units on $\Gamma(N)$ generate the ray class fields of imaginary quadratic number fields. (The so-called Ramachandra-Robert invariants.)
- Appear in the Kronecker limit formulas for the L-functions associated with characters of the ray class groups of imaginary quadratic number fields.
- Suitable products of Ramachandra-Robert invariants are units in the ray class fields. (The so-called elliptic units.)
- The elliptic units play an important role in Coates and Wiles' proof of the BSD conjecture for elliptic curves with CM by an imaginary quadratic field of class number 1.

Modular units and Jacobians of modular curves

- Consider the cuspidal embedding $i_\infty : X(\Gamma) \to J(\Gamma)$ given by $i_\infty(P) = [(P) - (\infty)]$.
- Manin and Drinfeld: if P is a cusp, then $i_\infty(P)$ is a torsion point on $J(\Gamma)$.
- Assume that $X(\Gamma)$ is defined over $\mathbb{Q}$ and P is a cusp rational over $\mathbb{Q}$. Then $i_\infty(P)$ generates a $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$.
- It is believe that all $\mathbb{Q}$-rational torsion points of $J(\Gamma)$ come from cusps in general.
- The divisor of a modular unit corresponds to 0 of $J(\Gamma)$. Explicit knowledge about modular units gives the structure of the rational torsion subgroup of $J(\Gamma)$ generated by cusps.

Modular units and Jacobians of modular curves

- Consider the cuspidal embedding $i_\infty : X(\Gamma) \to J(\Gamma)$ given by $i_\infty(P) = [(P) - (\infty)]$.
- Manin and Drinfeld: if P is a cusp, then $i_\infty(P)$ is a torsion point on $J(\Gamma)$.
- Assume that $X(\Gamma)$ is defined over $\mathbb{Q}$ and P is a cusp rational over $\mathbb{Q}$. Then $i_\infty(P)$ generates a $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$.
- It is believe that all $\mathbb{Q}$-rational torsion points of $J(\Gamma)$ come from cusps in general.
- The divisor of a modular unit corresponds to 0 of $J(\Gamma)$. Explicit knowledge about modular units gives the structure of the rational torsion subgroup of $J(\Gamma)$ generated by cusps.

Modular units and Jacobians of modular curves

- Consider the cuspidal embedding $i_\infty : X(\Gamma) \to J(\Gamma)$ given by $i_\infty(P) = [(P) - (\infty)]$.
- Manin and Drinfeld: if P is a cusp, then $i_\infty(P)$ is a torsion point on $J(\Gamma)$.
- Assume that $X(\Gamma)$ is defined over $\mathbb{Q}$ and P is a cusp rational over $\mathbb{Q}$. Then $i_\infty(P)$ generates a $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$.
- It is believe that all $\mathbb{Q}$-rational torsion points of $J(\Gamma)$ come from cusps in general.
- The divisor of a modular unit corresponds to 0 of $J(\Gamma)$. Explicit knowledge about modular units gives the structure of the rational torsion subgroup of $J(\Gamma)$ generated by cusps.

- Consider the cuspidal embedding $i_\infty : X(\Gamma) \to J(\Gamma)$ given by $i_\infty(P) = [(P) - (\infty)]$.
- Manin and Drinfeld: if P is a cusp, then $i_\infty(P)$ is a torsion point on $J(\Gamma)$.
- Assume that $X(\Gamma)$ is defined over $\mathbb{Q}$ and P is a cusp rational over $\mathbb{Q}$. Then $i_\infty(P)$ generates a $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$.
- It is believe that all $\mathbb{Q}$-rational torsion points of $J(\Gamma)$ come from cusps in general.
- The divisor of a modular unit corresponds to 0 of $J(\Gamma)$. Explicit knowledge about modular units gives the structure of the rational torsion subgroup of $J(\Gamma)$ generated by cusps.

Modular units and Jacobians of modular curves

- Consider the cuspidal embedding $i_\infty : X(\Gamma) \to J(\Gamma)$ given by $i_\infty(P) = [(P) - (\infty)]$.
- Manin and Drinfeld: if P is a cusp, then $i_\infty(P)$ is a torsion point on $J(\Gamma)$.
- Assume that $X(\Gamma)$ is defined over $\mathbb{Q}$ and P is a cusp rational over $\mathbb{Q}$. Then $i_\infty(P)$ generates a $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$.
- It is believe that all $\mathbb{Q}$-rational torsion points of $J(\Gamma)$ come from cusps in general.
- The divisor of a modular unit corresponds to 0 of $J(\Gamma)$. Explicit knowledge about modular units gives the structure of the rational torsion subgroup of $J(\Gamma)$ generated by cusps.

$\mathbb{Q}$-rational cusps

- If N is squarefree, every cusp of $\Gamma_0(N)$ is rational over $\mathbb{Q}$.
- If $(N, 6) = 1$, then cusps k/N, (k, N), are the only $\mathbb{Q}$-rational cusps on $\Gamma_1(N)$. Call them ∞-cusps.

$\mathbb{Q}$-rational cusps

- If N is squarefree, every cusp of $\Gamma_0(N)$ is rational over $\mathbb{Q}$.
- If $(N,6)=1$, then cusps k/N, (k,N), are the only $\mathbb{Q}$-rational cusps on $\Gamma_1(N)$. Call them ∞-cusps.

Modular units on congruence subgroups

- Takagi: If N is squarefree, every modular unit is a product of Dedekind eta functions.
- When $\Gamma = \Gamma_1(N)$,
  - Kubert and Lang: the modular units with divisors supported on ∞-cusps are all products of the Siegel functions. Moreover, the group of such modular units (modulo scalars) has rank $\phi(N)/2 - 1$.
  - Jing Yu: gave a formula for the order of the torsion subgroup of $J_1(N)$ generated by cusps k/N, $(k, N) = 1$.
  - In this talk, we will give explicit bases for the group of modular units on $\Gamma_1(N)$ having divisors supported at ∞-cusps.

Modular units on congruence subgroups

- Takagi: If N is squarefree, every modular unit is a product of Dedekind eta functions.
- When $\Gamma = \Gamma_1(N)$,
  - Kubert and Lang: the modular units with divisors supported on ∞-cusps are all products of the Siegel functions. Moreover, the group of such modular units (modulo scalars) has rank $\phi(N)/2 - 1$.
  - Jing Yu: gave a formula for the order of the torsion subgroup of $J_1(N)$ generated by cusps k/N, $(k, N) = 1$.
  - In this talk, we will give explicit bases for the group of modular units on $\Gamma_1(N)$ having divisors supported at ∞-cusps.

Modular units on congruence subgroups

- Takagi: If N is squarefree, every modular unit is a product of Dedekind eta functions.
- When $\Gamma = \Gamma_1(N)$,
  - Kubert and Lang: the modular units with divisors supported on ∞-cusps are all products of the Siegel functions. Moreover, the group of such modular units (modulo scalars) has rank $\phi(N)/2 - 1$.
  - Jing Yu: gave a formula for the order of the torsion subgroup of $J_1(N)$ generated by cusps k/N, $(k, N) = 1$.
  - In this talk, we will give explicit bases for the group of modular units on $\Gamma_1(N)$ having divisors supported at ∞-cusps.

Modular units on congruence subgroups

- Takagi: If N is squarefree, every modular unit is a product of Dedekind eta functions.
- When $\Gamma = \Gamma_1(N)$,
  - Kubert and Lang: the modular units with divisors supported on ∞-cusps are all products of the Siegel functions. Moreover, the group of such modular units (modulo scalars) has rank $\phi(N)/2 - 1$.
  - Jing Yu: gave a formula for the order of the torsion subgroup of $J_1(N)$ generated by cusps k/N, $(k, N) = 1$.
  - In this talk, we will give explicit bases for the group of modular units on $\Gamma_1(N)$ having divisors supported at ∞-cusps.

Modular units on congruence subgroups

- Takagi: If N is squarefree, every modular unit is a product of Dedekind eta functions.
- When $\Gamma = \Gamma_1(N)$,
  - Kubert and Lang: the modular units with divisors supported on ∞-cusps are all products of the Siegel functions. Moreover, the group of such modular units (modulo scalars) has rank $\phi(N)/2 - 1$.
  - Jing Yu: gave a formula for the order of the torsion subgroup of $J_1(N)$ generated by cusps k/N, $(k, N) = 1$.
  - In this talk, we will give explicit bases for the group of modular units on $\Gamma_1(N)$ having divisors supported at ∞-cusps.

Notations

For a positive integer N,

- $C(N)$: the set of cusps k/N of $\Gamma_1(N)$ with $(k,N)=1$,
- $\mathscr{F}(N)$: the group of modular units having divisors supported on $C(N)$,
- $\mathscr{D}(N)$: the group of divisors of degree 0 supported on $C(N)$,
- $\mathscr{P}(N)$: $\operatorname{div}\mathscr{F}(N)$,
- $\mathscr{C}(N)$: the divisor class group $\mathscr{D}(N)/\operatorname{div}\mathscr{F}(N)$.

Notations

For a positive integer N,

- $C(N)$: the set of cusps k/N of $\Gamma_1(N)$ with $(k,N)=1$,
- $\mathscr{F}(N)$: the group of modular units having divisors supported on $C(N)$,
- $\mathscr{D}(N)$: the group of divisors of degree 0 supported on $C(N)$,
- $\mathscr{P}(N)$: $\operatorname{div}\mathscr{F}(N)$.
- $\mathscr{C}(N)$: the divisor class group $\mathscr{D}(N)/\operatorname{div}\mathscr{F}(N)$.

Notations

For a positive integer N,

- $C(N)$: the set of cusps k/N of $\Gamma_1(N)$ with $(k, N) = 1$,
- $\mathscr{F}(N)$: the group of modular units having divisors supported on $C(N)$,
- $\mathscr{D}(N)$: the group of divisors of degree 0 supported on $C(N)$,
- $\mathscr{P}(N)$: div $\mathscr{F}(N)$,
- $\mathscr{C}(N)$: the divisor class group $\mathscr{D}(N)/\operatorname{div}\mathscr{F}(N)$.

Notations

For a positive integer N,

- $C(N)$: the set of cusps k/N of $\Gamma_1(N)$ with $(k, N) = 1$,
- $\mathscr{F}(N)$: the group of modular units having divisors supported on $C(N)$,
- $\mathscr{D}(N)$: the group of divisors of degree 0 supported on $C(N)$,
- $\mathscr{P}(N)$: div $\mathscr{F}(N)$.
- $\mathscr{C}(N)$: the divisor class group $\mathscr{D}(N)/$ div $\mathscr{F}(N)$.

Notations

For a positive integer N,

- $C(N)$: the set of cusps k/N of $\Gamma_1(N)$ with $(k,N)=1$,
- $\mathscr{F}(N)$: the group of modular units having divisors supported on $C(N)$,
- $\mathscr{D}(N)$: the group of divisors of degree 0 supported on $C(N)$,
- $\mathscr{P}(N)$: $\operatorname{div}\mathscr{F}(N)$.
- $\mathscr{C}(N)$: the divisor class group $\mathscr{D}(N)/\operatorname{div}\mathscr{F}(N)$.

Structure of $\mathscr{C}(N)$, computational results

N	structure	N	structure
11	$[5]$	25	$[227555]$
13	$[19]$	26	$[1995]$
14	$[3]$	27	$[3, 52497]$
15	$[4]$	28	$[4, 4, 156]$
16	$[10]$	29	$[4, 4, 64427244]$
17	$[584]$	30	$[340]$
18	$[7]$	31	$[10, 1772833370]$
19	$[4383]$	32	$[2, 12, 11640]$
20	$[20]$	33	$[8474730]$
21	$[182]$	34	$[5, 148920]$
22	$[155]$	35	$[13, 54574260]$
23	$[408991]$	36	$[4, 7812]$
24	$[60]$	37	$[16051668697605]$

p-part of $\mathscr{C}(p^n)$

p^n	p-primary subgroups
2^4	(2)
2^5	$(2)(2^2)^1(2^3)$
2^6	$(2)(2^2)^3(2^3)(2^4)^1(2^5)$
2^7	$(2)(2^2)^7(2^3)(2^4)^3(2^5)(2^6)^1(2^7)$
3^3	$(3)(3^2)^1$
3^4	$(3)(3^2)^5(3^3)(3^4)^1$
3^5	$(3)(3^2)^{17}(3^3)(3^4)^5(3^5)(3^6)^1$
3^6	$(3)(3^2)^{53}(3^3)(3^4)^{17}(3^5)(3^6)^5(3^7)(3^8)^1$
5^2	(5)
5^3	$(5)(5^2)^7(5^3)$
5^4	$(5)(5^2)^{39}(5^3)(5^4)^7(5^5)$

Conjecture on the p-part of $\mathscr{C}(p^n)$

Conjecture. Let p be a regular prime. Then the number of copies of $\mathbb{Z}/p^{2k}\mathbb{Z}$ in the primary decomposition of $\mathscr{C}(p^n)$ is

$$\begin{cases} \frac{1}{2}(p-1)^2p^{n-k-2}-1, & \text{if } p=2 \text{ and } k\le n-3, \\ \frac{1}{2}(p-1)^2p^{n-k-2}-1, & \text{if } p\ge 3 \text{ and } k\le n-2, \\ \frac{1}{2}(p-5), & \text{if } p\ge 5 \text{ and } k=n-1, \\ 0, & \text{else.} \end{cases}$$

and the number of copies of $\mathbb{Z}/p^{2k-1}\mathbb{Z}$ is

$$\begin{cases} 1, & \text{if } p=2 \text{ and } k\le n-3, \\ 1, & \text{if } p=3 \text{ and } k\le n-2, \\ 1, & \text{if } p\ge 5 \text{ and } k\le n-1, \\ 0, & \text{else.} \end{cases}$$

Theorem of Yang and Yu

Theorem (Y. Yang and J.-D. Yu, 2008)

The conjecture is true.

Outline of proof

Let $\pi_n : \mathscr{D}(p^{n+1}) \to \mathscr{D}(p^n)$ be the natural projection.

- If p is a regular prime, then p does not divide $|\mathscr{C}(p)|$.
- If p is a regular prime, then the p-rank of $\mathscr{C}(p^{n+1})$ is $p^{n-1}(p-1)/2-1$.
- The index of $\pi_n(\mathscr{P}(p^{n+1}))$ in $\mathscr{P}(p^n)$ is $p^{p^{n-1}(p-1)-3}$.
- If p is a regular prime, then the p-part of $\mathscr{C}(p^{n+1})$ is isomorphic to the p-part of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}(p^{n+1}))$.
- Assume p is a regular prime. Let $[p^2]$ be the multiplication-by-p^2 map. Then the p-part of $\mathscr{C}(p^{n+1})/\ker[p^2]$ is isomorphic to the p-part of $\mathscr{C}(p^n)$.

Outline of proof

Let $\pi_n : \mathscr{D}(p^{n+1}) \to \mathscr{D}(p^n)$ be the natural projection.

- If p is a regular prime, then p does not divide $|\mathscr{C}(p)|$.
- If p is a regular prime, then the p-rank of $\mathscr{C}(p^{n+1})$ is $p^{n-1}(p-1)/2-1$.
- The index of $\pi_n(\mathscr{P}(p^{n+1}))$ in $\mathscr{P}(p^n)$ is $p^{p^{n-1}(p-1)-3}$.
- If p is a regular prime, then the p-part of $\mathscr{C}(p^{n+1})$ is isomorphic to the p-part of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}(p^{n+1}))$.
- Assume p is a regular prime. Let $[p^2]$ be the multiplication-by-p^2 map. Then the p-part of $\mathscr{C}(p^{n+1})/\ker[p^2]$ is isomorphic to the p-part of $\mathscr{C}(p^n)$.

Outline of proof

Let $\pi_n : \mathscr{D}(p^{n+1}) \to \mathscr{D}(p^n)$ be the natural projection.

- If p is a regular prime, then p does not divide $|\mathscr{C}(p)|$.
- If p is a regular prime, then the p-rank of $\mathscr{C}(p^{n+1})$ is $p^{n-1}(p-1)/2-1$.
- The index of $\pi_n(\mathscr{P}(p^{n+1}))$ in $\mathscr{P}(p^n)$ is $p^{p^{n-1}(p-1)-3}$.
- If p is a regular prime, then the p-part of $\mathscr{C}(p^{n+1})$ is isomorphic to the p-part of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}(p^{n+1}))$.
- Assume p is a regular prime. Let $[p^2]$ be the multiplication-by-p^2 map. Then the p-part of $\mathscr{C}(p^{n+1})/\ker[p^2]$ is isomorphic to the p-part of $\mathscr{C}(p^n)$.

Outline of proof

Let $\pi_n : \mathscr{D}(p^{n+1}) \to \mathscr{D}(p^n)$ be the natural projection.

- If p is a regular prime, then p does not divide $|\mathscr{C}(p)|$.
- If p is a regular prime, then the p-rank of $\mathscr{C}(p^{n+1})$ is $p^{n-1}(p-1)/2-1$.
- The index of $\pi_n(\mathscr{P}(p^{n+1}))$ in $\mathscr{P}(p^n)$ is $p^{p^{n-1}(p-1)-3}$.
- If p is a regular prime, then the p-part of $\mathscr{C}(p^{n+1})$ is isomorphic to the p-part of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}(p^{n+1}))$.
- Assume p is a regular prime. Let $[p^2]$ be the multiplication-by-p^2 map. Then the p-part of $\mathscr{C}(p^{n+1})/\ker[p^2]$ is isomorphic to the p-part of $\mathscr{C}(p^n)$.

Outline of proof

Let $\pi_n : \mathscr{D}(p^{n+1}) \to \mathscr{D}(p^n)$ be the natural projection.

- If p is a regular prime, then p does not divide $|\mathscr{C}(p)|$.
- If p is a regular prime, then the p-rank of $\mathscr{C}(p^{n+1})$ is $p^{n-1}(p-1)/2-1$.
- The index of $\pi_n(\mathscr{P}(p^{n+1}))$ in $\mathscr{P}(p^n)$ is $p^{p^{n-1}(p-1)-3}$.
- If p is a regular prime, then the p-part of $\mathscr{C}(p^{n+1})$ is isomorphic to the p-part of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}(p^{n+1}))$.
- Assume p is a regular prime. Let $[p^2]$ be the multiplication-by-p^2 map. Then the p-part of $\mathscr{C}(p^{n+1})/\ker[p^2]$ is isomorphic to the p-part of $\mathscr{C}(p^n)$.

Outline of proof

Let $\pi_n : \mathscr{D}(p^{n+1}) \to \mathscr{D}(p^n)$ be the natural projection.

- If p is a regular prime, then p does not divide $|\mathscr{C}(p)|$.
- If p is a regular prime, then the p-rank of $\mathscr{C}(p^{n+1})$ is $p^{n-1}(p-1)/2-1$.
- The index of $\pi_n(\mathscr{P}(p^{n+1}))$ in $\mathscr{P}(p^n)$ is $p^{p^{n-1}(p-1)-3}$.
- If p is a regular prime, then the p-part of $\mathscr{C}(p^{n+1})$ is isomorphic to the p-part of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}(p^{n+1}))$.
- Assume p is a regular prime. Let $[p^2]$ be the multiplication-by-p^2 map. Then the p-part of $\mathscr{C}(p^{n+1})/\ker[p^2]$ is isomorphic to the p-part of $\mathscr{C}(p^n)$.

Outline of proof

(All groups refer to the p-parts.)

$$\begin{tikzcd}
\mathscr{C}(p^{n+1}) \arrow[r, "\simeq"] \arrow[d, "{[p^2]}"'] & \mathscr{D}(p^n)/\pi_n(\mathscr{P}(p^{n+1})) \arrow[d, "{[p^2]}"] \\
\mathscr{C}(p^{n+1})/\ker[p^2] \arrow[r, "\simeq"'] & \mathscr{C}(p^n)
\end{tikzcd}$$

Outline of proof

- Assume that the p-part of $\mathscr{C}(p^n)$ is $\prod_{i=1}^{k}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$.
- Since $\mathscr{C}(p^{n+1})/\ker[p^2] \simeq \mathscr{C}(p^n)$, the p-part of $\mathscr{C}(p^{n+1})$ is $(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod_{i=1}^{k}(\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$.
- By the formula for the p-ranks, $s_1 + s_2 = p^{n-2}(p-1)^2/2$.
- By the third and fourth properties, $s_1 + 2s_2 = p^{n-2}(p-1)^2 - 1$.
- Thus, $s_1 = 1$ and $s_2 = p^{n-2}(p-1)^2/2 - 1$.
- By the first property, the p-part of $\mathscr{C}(p)$ is trivial. Then an induction argument gives the result.

Outline of proof

- Assume that the p-part of $\mathscr{C}(p^n)$ is $\prod_{i=1}^k (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$.
- Since $\mathscr{C}(p^{n+1})/\ker[p^2] \simeq \mathscr{C}(p^n)$, the p-part of $\mathscr{C}(p^{n+1})$ is $(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod_{i=1}^k (\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$.
- By the formula for the p-ranks, $s_1 + s_2 = p^{n-2}(p-1)^2/2$.
- By the third and fourth properties, $s_1 + 2s_2 = p^{n-2}(p-1)^2 - 1$.
- Thus, $s_1 = 1$ and $s_2 = p^{n-2}(p-1)^2/2 - 1$.
- By the first property, the p-part of $\mathscr{C}(p)$ is trivial. Then an induction argument gives the result.

Outline of proof

- Assume that the p-part of $\mathscr{C}(p^n)$ is $\prod_{i=1}^{k}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$.
- Since $\mathscr{C}(p^{n+1})/\ker[p^2] \simeq \mathscr{C}(p^n)$, the p-part of $\mathscr{C}(p^{n+1})$ is $(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod_{i=1}^{k}(\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$.
- By the formula for the p-ranks, $s_1 + s_2 = p^{n-2}(p-1)^2/2$.
- By the third and fourth properties, $s_1 + 2s_2 = p^{n-2}(p-1)^2 - 1$.
- Thus, $s_1 = 1$ and $s_2 = p^{n-2}(p-1)^2/2 - 1$.
- By the first property, the p-part of $\mathscr{C}(p)$ is trivial. Then an induction argument gives the result.

Outline of proof

- Assume that the p-part of $\mathscr{C}(p^n)$ is $\prod_{i=1}^{k}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$.
- Since $\mathscr{C}(p^{n+1})/\ker[p^2] \simeq \mathscr{C}(p^n)$, the p-part of $\mathscr{C}(p^{n+1})$ is $(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod_{i=1}^{k}(\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$.
- By the formula for the p-ranks, $s_1 + s_2 = p^{n-2}(p-1)^2/2$.
- By the third and fourth properties, $s_1 + 2s_2 = p^{n-2}(p-1)^2 - 1$.
- Thus, $s_1 = 1$ and $s_2 = p^{n-2}(p-1)^2/2 - 1$.
- By the first property, the p-part of $\mathscr{C}(p)$ is trivial. Then an induction argument gives the result.

Outline of proof

- Assume that the p-part of $\mathscr{C}(p^n)$ is $\prod_{i=1}^{k}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$.
- Since $\mathscr{C}(p^{n+1})/\ker[p^2] \simeq \mathscr{C}(p^n)$, the p-part of $\mathscr{C}(p^{n+1})$ is $(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod_{i=1}^{k}(\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$.
- By the formula for the p-ranks, $s_1 + s_2 = p^{n-2}(p-1)^2/2$.
- By the third and fourth properties, $s_1 + 2s_2 = p^{n-2}(p-1)^2 - 1$.
- Thus, $s_1 = 1$ and $s_2 = p^{n-2}(p-1)^2/2 - 1$.
- By the first property, the p-part of $\mathscr{C}(p)$ is trivial. Then an induction argument gives the result.

Outline of proof

- Assume that the p-part of $\mathscr{C}(p^n)$ is $\prod_{i=1}^{k}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$.
- Since $\mathscr{C}(p^{n+1})/\ker[p^2] \simeq \mathscr{C}(p^n)$, the p-part of $\mathscr{C}(p^{n+1})$ is $(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod_{i=1}^{k}(\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$.
- By the formula for the p-ranks, $s_1 + s_2 = p^{n-2}(p-1)^2/2$.
- By the third and fourth properties, $s_1 + 2s_2 = p^{n-2}(p-1)^2 - 1$.
- Thus, $s_1 = 1$ and $s_2 = p^{n-2}(p-1)^2/2 - 1$.
- By the first property, the p-part of $\mathscr{C}(p)$ is trivial. Then an induction argument gives the result.

Some ingredients

- Define $\iota_n : \mathscr{D}(p^n) \to \mathscr{D}(p^{n+1})$ by $\iota_n(P) = p \sum_{Q:\ \pi_n(Q)=P} Q$.

  Then
  - If $D \in \mathscr{P}(p^n)$, then $\iota_n(D) \in \mathscr{P}(p^{n+1})$.
  - If $D \in \mathscr{D}(p^n)$ satisfies $\iota_n(D) \in \mathscr{P}(p^{n+1})$, then $D \in \mathscr{P}(p^n)$.
  - $\pi_n \circ \iota_n = p^2$.
- Let p be a regular prime. For $N = p^n$, $n \ge 2$,
  $$p \prod_{\chi \text{ even primitive}} B_{2,\chi} \equiv 1 \mod p.$$

Some ingredients

- Define $\iota_n : \mathscr{D}(p^n) \to \mathscr{D}(p^{n+1})$ by $\iota_n(P) = p \sum_{Q:\ \pi_n(Q)=P} Q$.

  Then
  - If $D \in \mathscr{P}(p^n)$, then $\iota_n(D) \in \mathscr{P}(p^{n+1})$.
  - If $D \in \mathscr{D}(p^n)$ satisfies $\iota_n(D) \in \mathscr{P}(p^{n+1})$, then $D \in \mathscr{P}(p^n)$.
  - $\pi_n \circ \iota_n = p^2$.
- Let p be a regular prime. For $N = p^n$, $n \geq 2$,
  $$p \prod_{\chi \text{ even primitive}} B_{2,\chi} \equiv 1 \mod p.$$

Some ingredients

- Define $\iota_n : \mathscr{D}(p^n) \to \mathscr{D}(p^{n+1})$ by $\iota_n(P) = p \sum_{Q:\ \pi_n(Q)=P} Q$.

  Then
  - If $D \in \mathscr{P}(p^n)$, then $\iota_n(D) \in \mathscr{P}(p^{n+1})$.
  - If $D \in \mathscr{D}(p^n)$ satisfies $\iota_n(D) \in \mathscr{P}(p^{n+1})$, then $D \in \mathscr{P}(p^n)$.
  - $\pi_n \circ \iota_n = p^2$.
- Let p be a regular prime. For $N = p^n$, $n \geq 2$,
$$p \prod_{\chi \text{ even primitive}} B_{2,\chi} \equiv 1 \mod p.$$

Some ingredients

- Define $\iota_n : \mathscr{D}(p^n) \to \mathscr{D}(p^{n+1})$ by $\iota_n(P) = p \sum_{Q:\ \pi_n(Q)=P} Q$.

  Then
  - If $D \in \mathscr{P}(p^n)$, then $\iota_n(D) \in \mathscr{P}(p^{n+1})$.
  - If $D \in \mathscr{D}(p^n)$ satisfies $\iota_n(D) \in \mathscr{P}(p^{n+1})$, then $D \in \mathscr{P}(p^n)$.
  - $\pi_n \circ \iota_n = p^2$.
- Let p be a regular prime. For $N = p^n$, $n \geq 2$,
  $$p \prod_{\chi \text{ even primitive}} B_{2,\chi} \equiv 1 \mod p.$$

- Define $\iota_n : \mathscr{D}(p^n) \to \mathscr{D}(p^{n+1})$ by $\iota_n(P) = p \sum_{Q:\ \pi_n(Q)=P} Q$.

  Then
  - If $D \in \mathscr{P}(p^n)$, then $\iota_n(D) \in \mathscr{P}(p^{n+1})$.
  - If $D \in \mathscr{D}(p^n)$ satisfies $\iota_n(D) \in \mathscr{P}(p^{n+1})$, then $D \in \mathscr{P}(p^n)$.
  - $\pi_n \circ \iota_n = p^2$.
- Let p be a regular prime. For $N = p^n$, $n \geq 2$,
  $$p \prod_{\chi \text{ even primitive}} B_{2,\chi} \equiv 1 \mod p.$$

Cases of $J_1(mp^n)$

mp^n	p-primary subgroups
$2 \cdot 3^3$	$(3^2)^2$
$2 \cdot 3^4$	$(3^2)^6(3^4)^2$
$2 \cdot 3^5$	$(3^2)^{18}(3^4)^6(3^6)^2$
$2 \cdot 5^2$	(5^2)
$2 \cdot 5^3$	$(5^2)^8(5^4)$
$2 \cdot 5^4$	$(5^2)^{40}(5^4)^8(5^6)$
$2 \cdot 7^2$	$(7^2)^2$
$2 \cdot 7^3$	$(7^2)^{18}(7^4)^2$
$3 \cdot 2^3$	(2^2)
$3 \cdot 2^4$	$(2^2)^2(2^4)$
$3 \cdot 2^5$	$(2^2)^4(2^4)^2(2^6)$

Conjecture. Assume that $p \geq 5$ does not divide $\mathscr{C}(mp)$. Then the number of copies of $\mathbb{Z}/p^{2k}\mathbb{Z}$ is

$$\begin{cases} \frac{1}{2}\phi(mp)p^{n-k-2}(p-1), & \text{if } k \leq n-2, \\ \frac{1}{2}\phi(mp) - 1, & \text{if } k = n-1, \\ 0, & \text{else,} \end{cases}$$

and the number of copies of $\mathbb{Z}/p^{2k-1}\mathbb{Z}$ is 0.

Case of irregular primes

mp^n	p-primary subgroups
$6 \cdot 5$	(5)
$6 \cdot 5^2$	$(5)(5^2)^2(5^3)$
$6 \cdot 5^3$	$(5)(5^2)^{15}(5^3)(5^4)^2(5^5)$
$6 \cdot 7$	$(7)^2$
$6 \cdot 7^2$	$(7)^2(7^2)^3(7^3)^2$
$6 \cdot 7^3$	$(7)^2(7^2)^{34}(7^3)^2(7^4)^3(7^5)^2$

Speculation. The p-part of $J_1(mp^n)$ is determined by that of $J_1(mp)$.

Case of irregular primes

mp^n	p-primary subgroups
$6 \cdot 5$	(5)
$6 \cdot 5^2$	$(5)(5^2)^2(5^3)$
$6 \cdot 5^3$	$(5)(5^2)^{15}(5^3)(5^4)^2(5^5)$
$6 \cdot 7$	$(7)^2$
$6 \cdot 7^2$	$(7)^2(7^2)^3(7^3)^2$
$6 \cdot 7^3$	$(7)^2(7^2)^{34}(7^3)^2(7^4)^3(7^5)^2$

Speculation. The p-part of $J_1(mp^n)$ is determined by that of $J_1(mp)$.

Siegel functions

Definition. Let $a=(a_1,a_2)\in\mathbb{Q}^2\backslash\mathbb{Z}^2$ and set $z=a_1\tau+a_2$. Then the Siegel function $g_a(\tau)$ is defined as

$$g_a(\tau)=-e^{2\pi i a_2(a_1-1)/2}q_\tau^{B(a_1)/2}(1-q_z)\prod_{n=1}^\infty(1-q_\tau^n q_z)(1-q_\tau^n/q_z),$$

where $q_z=e^{2\pi i z}$, $q_\tau=e^{2\pi i\tau}$, and $B(x)=x^2-x+1/6$ is the second Bernoulli polynomial.

We also set for integers a not congruent to 0 modulo N,

$$\begin{aligned}E_a(\tau)&=-g_{(a/N,0)}(N\tau)\\&=q^{NB(a/N)/2}\prod_{n=1}^\infty\left(1-q^{(n-1)N+a}\right)\left(1-q^{nN-a}\right)\end{aligned}$$

Definition. Let $a=(a_1,a_2)\in\mathbb{Q}^2\backslash\mathbb{Z}^2$ and set $z=a_1\tau+a_2$. Then the Siegel function $g_a(\tau)$ is defined as

$$g_a(\tau)=-e^{2\pi i a_2(a_1-1)/2}q_\tau^{B(a_1)/2}(1-q_z)\prod_{n=1}^\infty(1-q_\tau^n q_z)(1-q_\tau^n/q_z),$$

where $q_z=e^{2\pi i z}$, $q_\tau=e^{2\pi i\tau}$, and $B(x)=x^2-x+1/6$ is the second Bernoulli polynomial.

We also set for integers a not congruent to 0 modulo N,

$$\begin{aligned}E_a(\tau)&=-g_{(a/N,0)}(N\tau)\\&=q^{NB(a/N)/2}\prod_{n=1}^\infty\left(1-q^{(n-1)N+a}\right)\left(1-q^{nN-a}\right)\end{aligned}$$

Siegel functions

Definition. Let $a = (a_1, a_2) \in \mathbb{Q}^2 \backslash \mathbb{Z}^2$ and set $z = a_1\tau + a_2$. Then the Siegel function $g_a(\tau)$ is defined as

$$g_a(\tau) = -e^{2\pi i a_2(a_1-1)/2} q_\tau^{B(a_1)/2}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n/q_z),$$

where $q_z = e^{2\pi i z}$, $q_\tau = e^{2\pi i\tau}$, and $B(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial.

We also set for integers a not congruent to 0 modulo N,

$$\begin{aligned} E_a(\tau) &= -g_{(a/N,0)}(N\tau) \\ &= q^{NB(a/N)/2}\prod_{n=1}^{\infty}\left(1-q^{(n-1)N+a}\right)\left(1-q^{nN-a}\right) \end{aligned}$$

Definition. Let $a = (a_1, a_2) \in \mathbb{Q}^2 \backslash \mathbb{Z}^2$ and set $z = a_1\tau + a_2$. Then the Siegel function $g_a(\tau)$ is defined as

$$g_a(\tau) = -e^{2\pi i a_2(a_1-1)/2} q_\tau^{B(a_1)/2}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n/q_z),$$

where $q_z = e^{2\pi i z}$, $q_\tau = e^{2\pi i\tau}$, and $B(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial.
We also set for integers a not congruent to 0 modulo N,

$$\begin{aligned} E_a(\tau) &= -g_{(a/N,0)}(N\tau) \\ &= q^{NB(a/N)/2}\prod_{n=1}^{\infty}\left(1-q^{(n-1)N+a}\right)\left(1-q^{nN-a}\right) \end{aligned}$$

Properties of E_g

- $E_{g+N} = E_{-g} = -E_g$.
- For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, we have

$$E_g(\gamma\tau) = \epsilon e^{\pi i(g^2ab/N - gb)} E_{ag}(\tau)$$

for some 12th root of unity ϵ.

- If

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

and

$$\sum_g g^2 e_g \equiv 0 \mod 2N,$$

then $\prod_g E_g^{e_g}$ is modular on $\Gamma_1(N)$. (QUAD.)

Properties of E_g

- $E_{g+N} = E_{-g} = -E_g$.
- For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, we have

$$E_g(\gamma\tau) = \epsilon e^{\pi i(g^2ab/N - gb)} E_{ag}(\tau)$$

for some 12th root of unity ϵ.

- If

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

and

$$\sum_g g^2 e_g \equiv 0 \mod 2N,$$

then $\prod_g E_g^{e_g}$ is modular on $\Gamma_1(N)$. (QUAD.)

Properties of E_g

- $E_{g+N} = E_{-g} = -E_g$.
- For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, we have

$$E_g(\gamma\tau) = \epsilon e^{\pi i(g^2 ab/N - gb)} E_{ag}(\tau)$$

  for some 12th root of unity ϵ.
- If

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

  and

$$\sum_g g^2 e_g \equiv 0 \mod 2N,$$

  then $\prod_g E_g^{e_g}$ is modular on $\Gamma_1(N)$. (QUAD.)

Properties of E_g

- For odd N,

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g^2 e_g \equiv 0 \mod N$$

  are sufficient.
- If, in addition, for all $p|N$ and all a,

$$\sum_{g\equiv\pm a \mod N/p} e_g = 0,$$

  then $\prod_g E_g^{e_g}$ has a divisor supported on $C(N)$. (ORBIT.)
- Yu: If N has more than one distinct prime divisors, then ORBIT implies QUAD.

Properties of E_g

- For odd N,

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g^2 e_g \equiv 0 \mod N$$

  are sufficient.
- If, in addition, for all $p|N$ and all a,

$$\sum_{g \equiv \pm a \mod N/p} e_g = 0,$$

  then $\prod_g E_g^{e_g}$ has a divisor supported on $C(N)$. (ORBIT.)
- Yu: If N has more than one distinct prime divisors, then ORBIT implies QUAD.

Properties of E_g

- For odd N,

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g^2 e_g \equiv 0 \mod N$$

  are sufficient.
- If, in addition, for all $p|N$ and all a,

$$\sum_{g \equiv \pm a \mod N/p} e_g = 0,$$

  then $\prod_g E_g^{e_g}$ has a divisor supported on $C(N)$. (ORBIT.)
- Yu: If N has more than one distinct prime divisors, then ORBIT implies QUAD.

Prime cases

Theorem (Yang, 2007)

Let $p \geq 5$ be a prime. Let a be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and b be its multiplicative inverse. Then a basis for $\mathscr{F}(p)$ modulo scalars is

$$f_i = \frac{E_{a^i-1}E_{a^{i+1}}^{b^2}}{E_{a^i}^{1+b^2}}, \quad (i = 1, \ldots, \frac{p-1}{2} - 2), \qquad f_{(p-1)/2-1} = \frac{E_{b^2}^p}{E_b^p}.$$

Idea

- Set $n=(p-1)/2$ and let $P_i=i/p$, $i=1,\ldots,n$, be the cusps in $C(p)$.
- Embed $\mathscr{D}(p)$ into $\mathbb{R}^n$ by

$$\rho:\ c_1P_1+\cdots+c_nP_n\mapsto(c_1,\ldots,c_n)$$

- The image $\rho(\mathscr{D}(p))$ is the lattice Λ generated by $(0,\ldots,0,1,-1,0,\ldots,0)$.
- Let $f_1,\ldots,f_{n-1}$ be modular units in $\mathscr{F}(p)$, and let Λ' be the lattice generated by $\rho(\operatorname{div} f_i)$. Then

$$|\mathscr{D}(p)/\langle\operatorname{div} f_i\rangle|=|\Lambda/\Lambda'|.$$

Idea

- Set $n = (p-1)/2$ and let $P_i = i/p$, $i = 1, \ldots, n$, be the cusps in $C(p)$.
- Embed $\mathscr{D}(p)$ into $\mathbb{R}^n$ by

$$\rho: \; c_1P_1 + \cdots + c_nP_n \mapsto (c_1, \ldots, c_n)$$

- The image $\rho(\mathscr{D}(p))$ is the lattice Λ generated by $(0, \ldots, 0, 1, -1, 0, \ldots, 0)$.
- Let $f_1, \ldots, f_{n-1}$ be modular units in $\mathscr{F}(p)$, and let Λ' be the lattice generated by $\rho(\operatorname{div} f_i)$. Then

$$|\mathscr{D}(p)/\langle \operatorname{div} f_i \rangle| = |\Lambda/\Lambda'|.$$

Idea

- Set $n = (p-1)/2$ and let $P_i = i/p$, $i = 1, \ldots, n$, be the cusps in $C(p)$.
- Embed $\mathscr{D}(p)$ into $\mathbb{R}^n$ by

$$\rho : \; c_1P_1 + \cdots + c_nP_n \mapsto (c_1, \ldots, c_n)$$

- The image $\rho(\mathscr{D}(p))$ is the lattice Λ generated by $(0, \ldots, 0, 1, -1, 0, \ldots, 0)$.
- Let $f_1, \ldots, f_{n-1}$ be modular units in $\mathscr{F}(p)$, and let Λ' be the lattice generated by $\rho(\operatorname{div} f_i)$. Then

$$|\mathscr{D}(p)/\langle \operatorname{div} f_i \rangle| = |\Lambda/\Lambda'|.$$

Idea

- Set $n = (p-1)/2$ and let $P_i = i/p$, $i = 1, \dots, n$, be the cusps in $C(p)$.
- Embed $\mathscr{D}(p)$ into $\mathbb{R}^n$ by

$$\rho: \ c_1P_1 + \cdots + c_nP_n \mapsto (c_1, \dots, c_n)$$

- The image $\rho(\mathscr{D}(p))$ is the lattice Λ generated by $(0, \dots, 0, 1, -1, 0, \dots, 0)$.
- Let $f_1, \dots, f_{n-1}$ be modular units in $\mathscr{F}(p)$, and let Λ' be the lattice generated by $\rho(\operatorname{div} f_i)$. Then

$$|\mathscr{D}(p)/\langle \operatorname{div} f_i \rangle| = |\Lambda/\Lambda'|.$$

Class number formula

Theorem (Yu)

We have

$$|\mathscr{D}(p^n)/\operatorname{div}\mathscr{F}(p^n)| = p^{L(p,n)} \prod_{\chi\neq\chi_0 \text{ even}} \frac{1}{4}B_{2,\chi},$$

where

$$L(p,n) = \begin{cases} p^{n-1} - 2n + 2, & \text{if } p \text{ is odd}, \\ 2^{n-1} - 2n + 3, & \text{if } p = 2. \end{cases}$$

and $B_{2,\chi}$ is the generalized Bernoulli number associated with χ.

Proof of the case $p = 11$

- Choose $a = 6$ and $b = 2$.
- Form a 5×5 matrix M whose (j,k)-entry is the order of $E_{a^{j-1}}$ at the cusp $a^{k-1}/11$.
- We have

$$\det M = \prod_{\chi \text{ even}} \frac{1}{4} B_{2,\chi}.$$

- Let

$$U = \begin{pmatrix} 1 & -5 & 4 & 0 & 0 \\ 0 & 1 & -5 & 4 & 0 \\ 0 & 0 & 1 & -5 & 4 \\ 0 & 0 & 0 & 11 & -11 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

whose (i,j)-entry is the exponent of $E_{a^{j-1}}$ in f_i for $i = 1, \ldots, 4$.

Proof of the case $p = 11$

- Choose $a = 6$ and $b = 2$.
- Form a 5×5 matrix M whose (j,k)-entry is the order of $E_{a^{j-1}}$ at the cusp $a^{k-1}/11$.
- We have

$$\det M = \prod_{\chi \text{ even}} \frac{1}{4} B_{2,\chi}.$$

- Let

$$U = \begin{pmatrix} 1 & -5 & 4 & 0 & 0 \\ 0 & 1 & -5 & 4 & 0 \\ 0 & 0 & 1 & -5 & 4 \\ 0 & 0 & 0 & 11 & -11 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

whose (i,j)-entry is the exponent of $E_{a^{j-1}}$ in f_i for $i = 1, \ldots, 4$.

Proof of the case $p = 11$

- Choose $a = 6$ and $b = 2$.
- Form a 5×5 matrix M whose (j,k)-entry is the order of $E_{a^{j-1}}$ at the cusp $a^{k-1}/11$.
- We have
$$\det M = \prod_{\chi \text{ even}} \frac{1}{4} B_{2,\chi}.$$
- Let
$$U = \begin{pmatrix} 1 & -5 & 4 & 0 & 0 \\ 0 & 1 & -5 & 4 & 0 \\ 0 & 0 & 1 & -5 & 4 \\ 0 & 0 & 0 & 11 & -11 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
whose (i,j)-entry is the exponent of $E_{a^{j-1}}$ in f_i for $i = 1, \ldots, 4$.

Proof of the case $p = 11$

- Choose $a = 6$ and $b = 2$.
- Form a 5×5 matrix M whose (j,k)-entry is the order of $E_{a^{j-1}}$ at the cusp $a^{k-1}/11$.
- We have

$$\det M = \prod_{\chi \text{ even}} \frac{1}{4} B_{2,\chi}.$$

- Let

$$U = \begin{pmatrix} 1 & -5 & 4 & 0 & 0 \\ 0 & 1 & -5 & 4 & 0 \\ 0 & 0 & 1 & -5 & 4 \\ 0 & 0 & 0 & 11 & -11 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

whose (i,j)-entry is the exponent of $E_{a^{j-1}}$ in f_i for $i = 1, \ldots, 4$.

Proof of the case $p = 11$, continued

- We have
$$UM = \begin{pmatrix} 2 & -1 & 2 & 1 & -4 \\ -1 & 2 & 1 & -4 & 2 \\ 2 & 1 & -4 & 2 & -1 \\ -5 & -4 & 10 & -3 & 2 \\ \frac{13}{132} & \frac{61}{132} & -\frac{59}{132} & -\frac{23}{132} & -\frac{47}{132} \end{pmatrix}$$
whose first 4 rows are $\rho(\operatorname{div} f_i)$.
- Also,
$$\det(UM) = 11 \prod_{\chi \text{ even}} \frac{1}{4} B_{2,\chi}.$$

Proof of the case $p = 11$, continued

- We have

$$UM = \begin{pmatrix} 2 & -1 & 2 & 1 & -4 \\ -1 & 2 & 1 & -4 & 2 \\ 2 & 1 & -4 & 2 & -1 \\ -5 & -4 & 10 & -3 & 2 \\ \frac{13}{132} & \frac{61}{132} & -\frac{59}{132} & -\frac{23}{132} & -\frac{47}{132} \end{pmatrix}$$

  whose first 4 rows are $\rho(\operatorname{div} f_i)$.

- Also,

$$\det(UM) = 11 \prod_{\chi \text{ even}} \frac{1}{4} B_{2,\chi}.$$

Proof of the case $p = 11$, continued

- The matrix

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ \frac{13}{132} & \frac{61}{132} & -\frac{59}{132} & -\frac{23}{132} & -\frac{47}{132} \end{pmatrix}$$

  has determinant $\frac{1}{4}B_{2,\chi_0}$.

- Then the lattice spanned by $\rho(\operatorname{div} f_i)$ has index

$$\left(11\prod_{\chi\ \text{even}}\frac{1}{4}B_{2,\chi}\right)\Big/\frac{1}{4}B_{2,\chi_0} = 11\prod_{\chi\neq\chi_0\ \text{even}}\frac{1}{4}B_{2,\chi}$$

  in the lattice generated by $(0,\dots,0,1,-1,0,\dots,0)$.

- That is, f_i generate $\mathscr{F}(11)$.

Proof of the case $p = 11$, continued

- The matrix

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ \frac{13}{132} & \frac{61}{132} & -\frac{59}{132} & -\frac{23}{132} & -\frac{47}{132} \end{pmatrix}$$

  has determinant $\frac{1}{4}B_{2,\chi_0}$.

- Then the lattice spanned by $\rho(\operatorname{div} f_i)$ has index

$$\left(11 \prod_{\chi \text{ even}} \frac{1}{4}B_{2,\chi}\right) \Big/ \frac{1}{4}B_{2,\chi_0} = 11 \prod_{\chi \neq \chi_0 \text{ even}} \frac{1}{4}B_{2,\chi}$$

  in the lattice generated by $(0,\dots,0,1,-1,0,\dots,0)$.

- That is, f_i generate $\mathscr{F}(11)$.

Proof of the case $p = 11$, continued

- The matrix

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ \frac{13}{132} & \frac{61}{132} & -\frac{59}{132} & -\frac{23}{132} & -\frac{47}{132} \end{pmatrix}$$

  has determinant $\frac{1}{4}B_{2,\chi_0}$.

- Then the lattice spanned by $\rho(\operatorname{div} f_i)$ has index

$$\left(11 \prod_{\chi \text{ even}} \frac{1}{4}B_{2,\chi}\right) \Big/ \frac{1}{4}B_{2,\chi_0} = 11 \prod_{\chi \neq \chi_0 \text{ even}} \frac{1}{4}B_{2,\chi}$$

  in the lattice generated by $(0, \ldots, 0, 1, -1, 0, \ldots, 0)$.

- That is, f_i generate $\mathscr{F}(11)$.

Prime power cases

- Modular units from lower levels are required.
- If $p|N$ and $f(\tau) \in \mathscr{F}(N)$, then $f(p\tau) \in \mathscr{F}(pN)$.
- If $p|N$ and $f(\tau) = \prod_g E_g(p\tau)^{e_g}$ satisfies

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

  and

$$\sum_g g^2 e_g \equiv 0 \mod 2N/p,$$

  then $f(\tau)$ is modular on $\Gamma_1(pN)$.
- Assume that $N = nM$. Then

$$N \sum_{k=0}^{n-1} B_2\left(\frac{kM+a}{N}\right) = MB_2\left(\frac{a}{M}\right).$$

  (Bernoulli distribution relation.)
- Results are too complicated to be stated here.

Prime power cases

- Modular units from lower levels are required.
- If $p|N$ and $f(\tau) \in \mathscr{F}(N)$, then $f(p\tau) \in \mathscr{F}(pN)$.
- If $p|N$ and $f(\tau) = \prod_g E_g(p\tau)^{e_g}$ satisfies

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

  and

$$\sum_g g^2 e_g \equiv 0 \mod 2N/p,$$

  then $f(\tau)$ is modular on $\Gamma_1(pN)$.
- Assume that $N = nM$. Then

$$N \sum_{k=0}^{n-1} B_2\left(\frac{kM+a}{N}\right) = MB_2\left(\frac{a}{M}\right).$$

  (Bernoulli distribution relation.)
- Results are too complicated to be stated here.

Prime power cases

- Modular units from lower levels are required.
- If $p|N$ and $f(\tau) \in \mathscr{F}(N)$, then $f(p\tau) \in \mathscr{F}(pN)$.
- If $p|N$ and $f(\tau) = \prod_g E_g(p\tau)^{e_g}$ satisfies

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

  and

$$\sum_g g^2 e_g \equiv 0 \mod 2N/p,$$

  then $f(\tau)$ is modular on $\Gamma_1(pN)$.
- Assume that $N = nM$. Then

$$N \sum_{k=0}^{n-1} B_2\left(\frac{kM+a}{N}\right) = MB_2\left(\frac{a}{M}\right).$$

  (Bernoulli distribution relation.)
- Results are too complicated to be stated here.

Prime power cases

- Modular units from lower levels are required.
- If $p|N$ and $f(\tau)\in\mathscr{F}(N)$, then $f(p\tau)\in\mathscr{F}(pN)$.
- If $p|N$ and $f(\tau)=\prod_g E_g(p\tau)^{e_g}$ satisfies

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

  and

$$\sum_g g^2 e_g \equiv 0 \mod 2N/p,$$

  then $f(\tau)$ is modular on $\Gamma_1(pN)$.
- Assume that $N=nM$. Then

$$N\sum_{k=0}^{n-1} B_2\left(\frac{kM+a}{N}\right)=MB_2\left(\frac{a}{M}\right).$$

  (Bernoulli distribution relation.)
- Results are too complicated to be stated here.

Prime power cases

- Modular units from lower levels are required.
- If $p|N$ and $f(\tau) \in \mathscr{F}(N)$, then $f(p\tau) \in \mathscr{F}(pN)$.
- If $p|N$ and $f(\tau) = \prod_g E_g(p\tau)^{e_g}$ satisfies

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

  and

$$\sum_g g^2 e_g \equiv 0 \mod 2N/p,$$

  then $f(\tau)$ is modular on $\Gamma_1(pN)$.
- Assume that $N = nM$. Then

$$N \sum_{k=0}^{n-1} B_2\left(\frac{kM+a}{N}\right) = MB_2\left(\frac{a}{M}\right).$$

  (Bernoulli distribution relation.)
- Results are too complicated to be stated here.

Non-prime power cases

Theorem (Yu)

Assume that N has at least two distinct prime factors. Then $f(\tau) \in \mathscr{F}(N)$ if and only if $f(\tau) = c\prod_g E_g^{e_g}$ with

$$\sum_{g \equiv \pm a \mod N/p} e_g = 0$$

for all $p|N$ and all a.

Case $N = 21$

- If $f(\tau) = \prod_{g=1}^{10} E_g^{e_g} \in \mathscr{F}(21)$, then e_g satisfy

  $$e_7 = 0, \quad e_3 = -e_4 - e_{10}, \quad e_6 = -e_1 - e_8, \quad e_9 = -e_2 - e_5$$

  and

  $$e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0.$$

- That is,

  $$f = \left(\frac{E_1}{E_6}\right)^{e_1} \left(\frac{E_2}{E_9}\right)^{e_2} \left(\frac{E_4}{E_3}\right)^{e_4} \left(\frac{E_5}{E_9}\right)^{e_5} \left(\frac{E_8}{E_6}\right)^{e_8} \left(\frac{E_{10}}{E_3}\right)^{e_{10}}$$

  subject to $e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0$.

- Let F_i, $i = 1, 2, 4, 5, 8, 10$, denote the quotients above. Then F_1/F_2, F_2/F_4, F_4/F_5, F_5/F_8, and F_8/F_{10} generate $\mathscr{F}(21)$.

Case $N = 21$

- If $f(\tau) = \prod_{g=1}^{10} E_g^{e_g} \in \mathscr{F}(21)$, then e_g satisfy

$$e_7 = 0, \quad e_3 = -e_4 - e_{10}, \quad e_6 = -e_1 - e_8, \quad e_9 = -e_2 - e_5$$

and

$$e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0.$$

- That is,

$$f = \left(\frac{E_1}{E_6}\right)^{e_1} \left(\frac{E_2}{E_9}\right)^{e_2} \left(\frac{E_4}{E_3}\right)^{e_4} \left(\frac{E_5}{E_9}\right)^{e_5} \left(\frac{E_8}{E_6}\right)^{e_8} \left(\frac{E_{10}}{E_3}\right)^{e_{10}}$$

subject to $e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0$.

- Let F_i, $i = 1, 2, 4, 5, 8, 10$, denote the quotients above. Then F_1/F_2, F_2/F_4, F_4/F_5, F_5/F_8, and F_8/F_{10} generate $\mathscr{F}(21)$.

Case $N = 21$

- If $f(\tau) = \prod_{g=1}^{10} E_g^{e_g} \in \mathscr{F}(21)$, then e_g satisfy

  $$e_7 = 0, \quad e_3 = -e_4 - e_{10}, \quad e_6 = -e_1 - e_8, \quad e_9 = -e_2 - e_5$$

  and

  $$e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0.$$

- That is,

  $$f = \left(\frac{E_1}{E_6}\right)^{e_1} \left(\frac{E_2}{E_9}\right)^{e_2} \left(\frac{E_4}{E_3}\right)^{e_4} \left(\frac{E_5}{E_9}\right)^{e_5} \left(\frac{E_8}{E_6}\right)^{e_8} \left(\frac{E_{10}}{E_3}\right)^{e_{10}}$$

  subject to $e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0$.

- Let F_i, $i = 1, 2, 4, 5, 8, 10$, denote the quotients above. Then F_1/F_2, F_2/F_4, F_4/F_5, F_5/F_8, and F_8/F_{10} generate $\mathscr{F}(21)$.

General cases

- Identify $\phi(N)/2 - 1$ “free variables” e_g.
- Expressing the rest of e_g in terms of these free variables, we get a basis.
- Modular units from lower levels are required.
- The results are too complicated to present here.

General cases

- Identify $\phi(N)/2 - 1$ “free variables” e_g.
- Expressing the rest of e_g in terms of these free variables, we get a basis.
- Modular units from lower levels are required.
- The results are too complicated to present here.

General cases

- Identify $\phi(N)/2-1$ “free variables” e_g.
- Expressing the rest of e_g in terms of these free variables, we get a basis.
- Modular units from lower levels are required.
- The results are too complicated to present here.

General cases

- Identify $\phi(N)/2 - 1$ “free variables” e_g.
- Expressing the rest of e_g in terms of these free variables, we get a basis.
- Modular units from lower levels are required.
- The results are too complicated to present here.

- Consider $N = 42$. Let

$$F_1 = \frac{E_1E_6E_{14}E_{21}}{E_{20}E_{15}E_7}, \quad F_5 = \frac{E_5E_{12}E_{14}E_{21}}{E_{16}E_9E_7},$$
$$F_{11} = \frac{E_{11}E_{18}E_{14}E_{21}}{E_{10}E_3E_7}, \quad F_{13} = \frac{E_{13}E_6E_{14}E_{21}}{E_8E_{15}E_7},$$
$$F_{17} = \frac{E_{17}E_{18}E_{14}E_{21}}{E_4E_3E_7}, \quad F_{19} = \frac{E_{19}E_{12}E_{14}E_{21}}{E_2E_9E_7}.$$

- A basis is $f_1 = F_1/F_5$, $f_2 = F_5/F_{11}$, $f_3 = F_{11}/F_{13}$, $f_4 = F_{13}/F_{17}$, $f_5 = F_{17}/F_{19}$.

Structure of $\mathscr{C}(N)$, an example

- Consider $N = 42$. Let

$$F_1 = \frac{E_1E_6E_{14}E_{21}}{E_{20}E_{15}E_7}, \quad F_5 = \frac{E_5E_{12}E_{14}E_{21}}{E_{16}E_9E_7},$$
$$F_{11} = \frac{E_{11}E_{18}E_{14}E_{21}}{E_{10}E_3E_7}, \quad F_{13} = \frac{E_{13}E_6E_{14}E_{21}}{E_8E_{15}E_7},$$
$$F_{17} = \frac{E_{17}E_{18}E_{14}E_{21}}{E_4E_3E_7}, \quad F_{19} = \frac{E_{19}E_{12}E_{14}E_{21}}{E_2E_9E_7}.$$

- A basis is $f_1 = F_1/F_5$, $f_2 = F_5/F_{11}$, $f_3 = F_{11}/F_{13}$, $f_4 = F_{13}/F_{17}$, $f_5 = F_{17}/F_{19}$.

- Let

$$M = \begin{pmatrix} 5 & 9 & -5 & 6 & -14 & -1 \\ 6 & -8 & -1 & 2 & 12 & -11 \\ 5 & -6 & 9 & -14 & -1 & 5 \\ 8 & -12 & -2 & 11 & -6 & 1 \\ -2 & 11 & -12 & -6 & 1 & 8 \end{pmatrix}$$

whose rows are the orders of f_i at $1/42$, $5/42$, $11/42$, $13/42$, $17/42$, and $19/42$, respectively.

Structure of $\mathscr{C}(N)$, an example

- We can find a unimodular matrix U such that

$$UM = \begin{pmatrix} 1 & 0 & 0 & 1 & -1021 & 1019 \\ 0 & 1 & 0 & -20 & 109 & -90 \\ 0 & 0 & 1 & -18 & -640 & 657 \\ 0 & 0 & 0 & 91 & 910 & -1001 \\ 0 & 0 & 0 & 0 & 2730 & -2730 \end{pmatrix}.$$

- This shows that $\mathscr{C}(42)$ is isomorphic to $C_{2730} \times C_{91}$ and generated by the divisor classes of

$$(17/42) - (19/42), \quad (13/42) + 10(17/42) - 11(19/42).$$

Structure of $\mathscr{C}(N)$, an example

- We can find a unimodular matrix U such that

$$UM = \begin{pmatrix} 1 & 0 & 0 & 1 & -1021 & 1019 \\ 0 & 1 & 0 & -20 & 109 & -90 \\ 0 & 0 & 1 & -18 & -640 & 657 \\ 0 & 0 & 0 & 91 & 910 & -1001 \\ 0 & 0 & 0 & 0 & 2730 & -2730 \end{pmatrix}.$$

- This shows that $\mathscr{C}(42)$ is isomorphic to $C_{2730} \times C_{91}$ and generated by the divisor classes of

$$(17/42) - (19/42), \quad (13/42) + 10(17/42) - 11(19/42).$$