Generators of the group of modular units for $\Gamma^1(N)$ over the rationals

Marco Streng

Universiteit Leiden

AGCT
18 May 2015
arXiv:1503.08127

The curve $Y^1(N)$ over $\mathbb{Q}$ $[N \geq 4]$

- $Y^1(N)/\mathbb{Q}$ smooth affine geometrically irreducible curve s.t.
- For fields $K \supseteq \mathbb{Q}$:

$$Y^1(N)(K) = \{(E, P) : E/K \text{ ell. curve, } P \in E(K), \text{order}(P) = N\}/\cong$$

- $X^1(N) = Y^1(N) \sqcup \{\text{cusps}\}$

$$\begin{aligned}\mathcal{O}(Y^1(N))^\times &= \{\text{alg. funct.}/\mathbb{Q} \text{ on } Y^1(N) \text{ with no poles or zeroes}\} \\ &= \{f \in \mathbb{Q}(X^1(N))^\times : \text{div}(f) \in \mathbb{Z}^{\{\text{cusps}\}}\}\end{aligned}$$

- Main result: $\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is freely generated by roughly the defining equations of $Y^1(k)$ for $k \leq N/2 + 1$.
- (Need a single ambient space before this makes sense)

Applications

- Modular curves are used in e.g. coding theory
- Small functions give rise to small models
- Modular units give rise to (almost-)units in ray class fields of imaginary quadratic fields
- Small functions satisfying certain symmetries speed up CM constructions of
  - Hilbert class fields of imaginary quadratic fields
  - elliptic curves with given characteristic polynomial of Frobenius (for e.g. cryptography)

Tate normal form $[N \geq 4]$

- For any field $K \supseteq \mathbb{Q}$, let

$$A(K) = \{(E, P) : E/K \text{ ell. curve, } P \in E(K), \text{order}(P) \neq 1, 2, 3\}/\cong,$$

so $Y^1(N)(K) \subset A(K)$ is given by "order$(P) = N$".

- Every $(E, P) \in A(K)$ can uniquely be written as

$$E : Y^2 + (1 - C)XY - BY = X^3 - BX^2, \quad P = (0, 0)$$

for $B, C \in K$. Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.

Tate normal form $[N \geq 4]$

- For any field $K \supseteq \mathbb{Q}$, let

$$A(K) = \{(E, P) : E/K \text{ ell. curve, } P \in E(K), \text{order}(P) \neq 1, 2, 3\}/\cong,$$

  so $Y^1(N)(K) \subset A(K)$ is given by "order$(P) = N$".
- Every $(E, P) \in A(K)$ can uniquely be written as

$$E : Y^2 + (1 - C)XY - BY = X^3 - BX^2, \quad P = (0, 0)$$

  for $B, C \in K$. Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, any $P \neq O$

Tate normal form $[N \geq 4]$

- For any field $K \supseteq \mathbb{Q}$, let

$$A(K) = \{(E, P) : E/K \text{ ell. curve, } P \in E(K), \text{order}(P) \neq 1, 2, 3\}/\cong,$$

so $Y^1(N)(K) \subset A(K)$ is given by "order$(P) = N$".

- Every $(E, P) \in A(K)$ can uniquely be written as

$$E : Y^2 + (1 - C)XY - BY = X^3 - BX^2, \quad P = (0, 0)$$

for $B, C \in K$. Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.

- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + \cancel{a_6}$, ~~any $P \neq O$~~
  - translate P to $(0, 0)$, then $a_6 = 0$

Tate normal form $[N \geq 4]$

- For any field $K \supseteq \mathbb{Q}$, let

$$A(K) = \{(E, P) : E/K \text{ ell. curve, } P \in E(K), \text{order}(P) \neq 1, 2, 3\}/\cong,$$

  so $Y^1(N)(K) \subset A(K)$ is given by "order$(P) = N$".
- Every $(E, P) \in A(K)$ can uniquely be written as

$$E : Y^2 + (1 - C)XY - BY = X^3 - BX^2, \quad P = (0, 0)$$

  for $B, C \in K$. Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 \cancel{+a_4X + a_6}$, $\cancel{\text{any } P \neq O}$
  - translate P to $(0, 0)$, then $a_6 = 0$
  - as $2P \neq O$, have $a_3 \neq 0$; do $Y \mapsto Y + a_4/a_3X$ to make $a_4 = 0$

Tate normal form $[N \geq 4]$

- For any field $K \supseteq \mathbb{Q}$, let

$$A(K) = \{(E, P) : E/K \text{ ell. curve, } P \in E(K), \text{order}(P) \neq 1, 2, 3\}/\cong,$$

  so $Y^1(N)(K) \subset A(K)$ is given by "order$(P) = N$".
- Every $(E, P) \in A(K)$ can uniquely be written as

$$E : Y^2 + (1 - C)XY - BY = X^3 - BX^2, \quad P = (0, 0)$$

  for $B, C \in K$. Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 \cancel{+a_4X+a_6}$, $\cancel{\text{any } P \neq O}$
  - translate P to $(0, 0)$, then $a_6 = 0$
  - as $2P \neq O$, have $a_3 \neq 0$; do $Y \mapsto Y + a_4/a_3X$ to make $a_4 = 0$
  - as $3P \neq O$, have $a_2 \neq 0$; scale $(X, Y) \mapsto (u^2X, u^3Y)$ to make $a_2 = a_3$

Tate normal form $[N \geq 4]$

- For any field $K \supseteq \mathbb{Q}$, let

$$A(K) = \{(E, P) : E/K \text{ ell. curve, } P \in E(K), \text{order}(P) \neq 1, 2, 3\}/\cong,$$

so $Y^1(N)(K) \subset A(K)$ is given by "order$(P) = N$".

- Every $(E, P) \in A(K)$ can uniquely be written as

$$E : Y^2 + (1 - C)XY - BY = X^3 - BX^2, \quad P = (0, 0)$$

for $B, C \in K$. Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.

- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 \cancel{+a_4X} \cancel{+a_6}$, $\cancel{\text{any } P \neq O}$
  - translate P to $(0, 0)$, then $a_6 = 0$
  - as $2P \neq O$, have $a_3 \neq 0$; do $Y \mapsto Y + a_4/a_3X$ to make $a_4 = 0$
  - as $3P \neq O$, have $a_2 \neq 0$; scale $(X, Y) \mapsto (u^2X, u^3Y)$ to make $a_2 = a_3$
- Get $A(K) = \{(B, C) \in K^2 : D \neq 0\}$
- Get irreducible $F_N \in \mathbb{Q}[B, C]$ such that $Y^1(N) : F_N = 0$

Main result $[N, k \geq 4]$

- Recall

$$A(K) = \{(E, P) : E/K \text{ elliptic curve, } P \in E(K), \text{order}(P) \neq 1, 2, 3\}/\cong$$
$$= \{(B, C) \in K^2 : D \neq 0\}$$

$Y^1(N) : F_N = 0$ curve in A

- Let $b = (B \bmod F_N)$, $f_k = (F_k \bmod F_N)$, etc.
- Note $f_k \in \mathcal{O}(Y^1(N))^\times$ for $n \neq N$.
  Proof:
  - no poles on A, as $F_k \in \mathbb{Q}[B, C]$
  - zeroes would be (E, P) where P has order N and k

Theorem [Conjecture of Derickx and Van Hoeij $\approx$ 2011]:

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is generated by $b, d, f_4, f_5, \ldots, f_{\lfloor N/2 \rfloor + 1}$.

- (rank is exactly $\lfloor N/2 \rfloor$)

Step 1: Division polynomials $[N \geq 4]$

- For $E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$ elliptic curve over $K \supseteq \mathbb{Q}$ and $n \in \mathbb{Z}$, we have

$$\psi_k := k \sqrt{\prod_{\substack{Q \in E[k] \\ Q \neq O}} (x - x(Q))} \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x, y] \subset K(E),$$

and for all $P \in E(K)$: $\quad \psi_k(P) = 0 \quad \Longleftrightarrow \quad kP = 0$

Step 1: Division polynomials $[N \geq 4]$

- For $E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$ elliptic curve over $K \supseteq \mathbb{Q}$ and $n \in \mathbb{Z}$, we have

$$\psi_k := k \sqrt{\prod_{\substack{Q \in E[k] \\ Q \neq O}} (x - x(Q))} \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x, y] \subset K(E),$$

  and for all $P \in E(K)$: $\quad \psi_k(P) = 0 \quad \Longleftrightarrow \quad kP = 0$

- Let $P_k \in \mathbb{Z}[B, C]$ be $\psi_k((0, 0))$ for the Tate form

$$E : Y^2 + (1 - C)XY - BY = X^3 - BX^2$$

- If $k \geq 4$, then F_k is the unique "new" factor of P_k
- $\langle B, D, P_4, \ldots, P_{\lfloor N/2 \rfloor + 1} \rangle = \langle B, D, F_4, \ldots, F_{\lfloor N/2 \rfloor + 1} \rangle$.

Equivalent theorem: $\mathcal{O}(Y^1(N))^\times / \mathbb{Q}^\times$ gen. by $b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor + 1}$ (where $p_k = (P_k \bmod F_N)$)

Recurrence

$$
\begin{aligned}
\psi_{m+n}\psi_{m-n}\psi_k^2 &= \psi_{m+k}\psi_{m-k}\psi_n^2 - \psi_{n+k}\psi_{n-k}\psi_m^2, \\
\psi_{2\ell+1} &= \psi_{\ell+2}\psi_\ell^3 - \psi_{\ell+1}^3\psi_{\ell-1}, \\
\psi_{2\ell} &= \psi_2^{-1}\psi_\ell\left(\psi_{\ell+2}\psi_{\ell-1}^2 - \psi_{\ell-2}\psi_{\ell+1}^2\right), \\
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y + a_1x + a_3
\end{aligned}
$$

Recurrence

$$
\begin{aligned}
P_{m+n}P_{m-n}P_k^2 &= P_{m+k}P_{m-k}P_n^2 - P_{n+k}P_{n-k}P_m^2, \\
P_{2\ell+1} &= P_{\ell+2}P_\ell^3 - P_{\ell+1}^3 P_{\ell-1}, \\
P_{2\ell} &= P_2^{-1}P_\ell \left(P_{\ell+2}P_{\ell-1}^2 - P_{\ell-2}P_{\ell+1}^2\right), \\
P_0 &= 0 \\
P_1 &= 1 \\
P_2 &= -B
\end{aligned}
$$

Recurrence

$$
\begin{aligned}
P_{m+n}P_{m-n}P_k^2 &= P_{m+k}P_{m-k}P_n^2 - P_{n+k}P_{n-k}P_m^2, \\
P_{2\ell+1} &= P_{\ell+2}P_\ell^3 - P_{\ell+1}^3 P_{\ell-1}, \\
P_{2\ell} &= P_2^{-1}P_\ell \left(P_{\ell+2}P_{\ell-1}^2 - P_{\ell-2}P_{\ell+1}^2\right), \\
P_0 &= 0 \\
P_1 &= 1 \\
P_2 &= -B \\
P_3 &= -B^3 \\
P_4 &= CB^5
\end{aligned}
$$

Recurrence

$$
\begin{aligned}
P_{m+n}P_{m-n}P_k^2 &= P_{m+k}P_{m-k}P_n^2 - P_{n+k}P_{n-k}P_m^2, \\
P_{2\ell+1} &= P_{\ell+2}P_\ell^3 - P_{\ell+1}^3 P_{\ell-1}, \\
P_{2\ell} &= P_2^{-1}P_\ell \left(P_{\ell+2}P_{\ell-1}^2 - P_{\ell-2}P_{\ell+1}^2\right), \\
P_0 &= 0 \\
P_1 &= 1 \\
P_2 &= -B \\
P_3 &= -B^3 \\
P_4 &= CB^5 \\
P_5 &= P_4P_2^3 - P_3^3P_1 = -B^8(C-B)
\end{aligned}
$$

Recurrence

$$
\begin{aligned}
P_{m+n}P_{m-n}P_k^2 &= P_{m+k}P_{m-k}P_n^2 - P_{n+k}P_{n-k}P_m^2, \\
P_{2\ell+1} &= P_{\ell+2}P_\ell^3 - P_{\ell+1}^3 P_{\ell-1}, \\
P_{2\ell} &= P_2^{-1}P_\ell \left(P_{\ell+2}P_{\ell-1}^2 - P_{\ell-2}P_{\ell+1}^2\right), \\
P_0 &= 0 \\
P_1 &= 1 \\
P_2 &= -B \\
P_3 &= -B^3 \\
P_4 &= CB^5 \\
P_5 &= P_4P_2^3 - P_3^3P_1 = -B^8(C-B) \\
P_6 &= P_2^{-1}P_3(P_5P_2^2 - P_1P_4^2) = -B^{12}(C^2+C-B)
\end{aligned}
$$

Recurrence

$$
\begin{aligned}
P_{m+n}P_{m-n}P_k^2 &= P_{m+k}P_{m-k}P_n^2 - P_{n+k}P_{n-k}P_m^2, \\
P_{2\ell+1} &= P_{\ell+2}P_\ell^3 - P_{\ell+1}^3 P_{\ell-1}, \\
P_{2\ell} &= P_2^{-1}P_\ell \left(P_{\ell+2}P_{\ell-1}^2 - P_{\ell-2}P_{\ell+1}^2\right), \\
P_0 &= 0 \\
P_1 &= 1 \\
P_2 &= -B \\
P_3 &= -B^3 \\
P_4 &= CB^5 \\
P_5 &= -B^8(C-B) \\
P_6 &= -B^{12}(C^2+C-B) \\
P_7 &= B^{16}\cdot(C^3-B^2+BC) \\
P_8 &= C\cdot B^{21}\cdot(BC^2-2B^2+3BC-C^2)
\end{aligned}
$$

Example

$$D = B^3 \cdot (C^4 - 8BC^2 - 3C^3 + 16B^2 - 20BC + 3C^2 + B - C)$$

$$P_1 = 1$$

$$P_2 = (-1) \cdot B$$

$$P_3 = (-1) \cdot B^3$$

$$P_4 = C \cdot B^5$$

$$P_5 = (-1) \cdot (C - B) \cdot B^8$$

$$P_6 = (-1) \cdot B^{12} \cdot (C^2 + C - B)$$

$$P_7 = B^{16} \cdot (C^3 - B^2 + BC)$$

$$P_8 = C \cdot B^{21} \cdot (BC^2 - 2B^2 + 3BC - C^2)$$

- So $Y^1(6)$ is given by $F_6 = C^2 + C - B = 0$
- $\mathcal{O}(Y^1(6))^\times = \mathbb{Q}^\times \times \langle b, d, p_4 \rangle$
- $\langle b, d, p_4 \rangle = \langle c(c+1), c^6(c+1)^3(9c+1), c^6(c+1) \rangle = \langle c, c+1, 9c+1 \rangle$

Example [N=6]

$$D = B^3 \cdot (C^4 - 8BC^2 - 3C^3 + 16B^2 - 20BC + 3C^2 + B - C)$$

$$P_1 = 1$$

$$P_2 = (-1) \cdot B$$

$$P_3 = (-1) \cdot B^3$$

$$P_4 = C \cdot B^5$$

$$P_5 = (-1) \cdot (C - B) \cdot B^8$$

$$P_6 = (-1) \cdot B^{12} \cdot (C^2 + C - B)$$

$$P_7 = B^{16} \cdot (C^3 - B^2 + BC)$$

$$P_8 = C \cdot B^{21} \cdot (BC^2 - 2B^2 + 3BC - C^2)$$

- So $Y^1(6)$ is given by $F_6 = C^2 + C - B = 0$
- $\mathcal{O}(Y^1(6))^\times = \mathbb{Q}^\times \times \langle b, d, p_4 \rangle$
- $\langle b, d, p_4 \rangle = \langle c(c+1), c^6(c+1)^3(9c+1), c^6(c+1) \rangle = \langle c, c+1, 9c+1 \rangle$

Step 2: Complex elliptic curves

- $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \frac{a\tau+b}{c\tau+d}$. Let
$$\Gamma^1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv 0, a \equiv d \equiv 1 \bmod N \right\}.$$
-
$$\begin{array}{ccc} \Gamma^1(N)\backslash\mathcal{H} & \cong & Y^1(N)(\mathbb{C}) \\ \tau & \mapsto & (E_\tau, P_\tau(\frac{1}{N}\tau)), \end{array}$$
where $E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$
and $P_\tau(z) = (\wp_\tau(z), \wp'_\tau(z)) \in E_\tau(\mathbb{C})$.
- In fact:
$$\mathcal{O}(Y^1(N))^\times \longleftrightarrow \left\{ \begin{array}{l} \text{holomorphic } f : \Gamma^1(N)\backslash\mathcal{H} \to \mathbb{C}^* \\ \text{that are meromorphic at cusps} \\ \text{with } q\text{-expansion coefficients in } \mathbb{Q} \end{array} \right\}$$

Step 2: Complex elliptic curves

- $$\begin{array}{ccc} \Gamma^1(N)\backslash\mathcal{H} & \cong & Y^1(N)(\mathbb{C}) \\ \tau & \mapsto & (E_\tau, P_\tau(\frac{1}{N}\tau)), \end{array}$$

  where $E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$
  and $P_\tau(z) = (\wp_\tau(z), \wp'_\tau(z)) \in E_\tau(\mathbb{C})$.
- In fact:

$$\mathcal{O}(Y^1(N))^\times \longleftrightarrow \left\{ \begin{array}{l} \text{holomorphic } f : \Gamma^1(N)\backslash\mathcal{H} \to \mathbb{C}^* \\ \text{that are meromorphic at cusps} \\ \text{with } q\text{-expansion coefficients in } \mathbb{Q} \end{array} \right\}$$

- Division polynomials on E_τ:

$$\psi_{k,E_\tau}(P_\tau(z)) = \sigma_\tau(kz)/\sigma_\tau(z)^{k^2}.$$

- Explicit rewrite between $(E_\tau, P_\tau(\frac{1}{N}\tau))$ and Tate normal form gives....

Step 2: Complex elliptic curves

- Explicit rewrite between Classical Weierstrass equation E_τ and Tate normal form (using $\psi_k = \sigma(kz)/\sigma(z)^{k^2}$) gives....
- For $a \in \mathbb{Q} \cap (0, \frac{1}{2}]$ define the Siegel function $h_{(a,0)}$ by

$$h_{(a,0)}(\tau) = i q^{\frac{1}{2}(a^2-a+\frac{1}{6})}(1-q^a)\prod_{n=1}^{\infty}(1-q^{n+a})(1-q^{n-a}),$$

$$\text{with} \qquad q = \exp(2\pi i \tau)$$

- Then $\langle -b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor + 1} \rangle$

$$\begin{aligned} &= \left\{ \prod_{k=1}^{\lfloor N/2 \rfloor} h_{(k/N,0)}^{e(k)} : \begin{array}{rcl} e & \in & \mathbb{Z}^{\lfloor N/2 \rfloor}, \\ \sum_k e(k) & \in & 12\mathbb{Z}, \\ \sum_k k^2 e(k) & \in & \gcd(N,2)N\mathbb{Z} \end{array} \right\} =: S \\ &\subset \quad \langle h_{(k/N,0)} : k = 1, \ldots, \lfloor N/2 \rfloor \rangle \end{aligned}$$

- Equivalent theorem: $\mathcal{O}(Y^1(N))^\times = \mathbb{Q}^\times \times S$

Overview

- $S := \left\{ \prod_{k=1}^{\lfloor N/2 \rfloor} h_{(k/N,0)}^{e(k)} : \begin{array}{rcl} e & \in & \mathbb{Z}^{\lfloor N/2 \rfloor}, \\ \sum_k e(k) & \in & 12\mathbb{Z}, \\ \sum_k k^2 e(k) & \in & \gcd(N,2)N\mathbb{Z} \end{array} \right\}$
- suffices to prove: $S \times \mathbb{Q}^\times \to \mathcal{O}(Y^1(N))^\times$ is bijective
- Kubert-Lang does this for $Y(N)_{\mathbb{C}}$ up to power-of-2 index of the image

Steps:

3a every $f \in \mathcal{O}(Y^1(N))^\times$ can uniquely be written as $f = c \prod_{k=1}^{\lfloor N/2 \rfloor} h_{(k/N,0)}^{e(k)}$ with $c \in \mathbb{C}^\times$ and $e \in \mathbb{Q}^{\lfloor N/2 \rfloor}$

3b $e \in \mathbb{Z}^{\lfloor N/2 \rfloor}$ (then $c \in \mathbb{Q}^\times$)

4 $\sum_k e(k) \in 12\mathbb{Z}$ and $\sum_k k^2 e(k) \in \gcd(N,2)N\mathbb{Z}$

Step 3a $[N \geq 4$ odd$]$

- $h_{(a,0)}(\tau) = iq^{\frac{1}{2}(a^2-a+\frac{1}{6})}(1-q^a)\prod_{n=1}^{\infty}(1-q^{n+a})(1-q^{n-a})$
- $S \to \mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$
- $\text{rank(codomain)} \leq \#\frac{\{\text{cusps}\}}{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} - 1 = \lfloor N/2 \rfloor$

Claim: $\text{rank(image)} = \lfloor N/2 \rfloor$ (this is enough)

- Tool: divide by leading term, that is,

$$h^*_{(a,0)} = (1-q^a)\prod_{n=1}^{\infty}(1-q^{n+a})(1-q^{n-a}) = 1 - q^a + O(q^{1-a})$$

Step 3a $[N \geq 4$ odd$]$

- $h_{(a,0)}(\tau) = iq^{\frac{1}{2}(a^2-a+\frac{1}{6})}(1-q^a)\prod_{n=1}^{\infty}(1-q^{n+a})(1-q^{n-a})$
- $S \to \mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$
- $\text{rank(codomain)} \leq \#\frac{\{\text{cusps}\}}{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} - 1 = \lfloor N/2 \rfloor$

Claim: $\text{rank(image)} = \lfloor N/2 \rfloor$ (this is enough)

- Tool: divide by leading term, that is,

$$h^*_{(a,0)} = (1-q^a)\prod_{n=1}^{\infty}(1-q^{n+a})(1-q^{n-a}) = 1 - q^a + O(q^{1-a})$$

- We show that if $e \neq 0$, then $f = \prod_{k=1}^{\lfloor N/2 \rfloor} h^{e(k)}_{(k/N,0)} \notin \mathbb{C}^\times$.
- Take k_0 minimal with $e(k_0) \neq 0$.
- Then $f^* = 1 - e(k_0)q^{k_0/N} + O(q^{(k_0+1)/N}) \neq 1$, so $f \notin \mathbb{C}^\times$

Step 3b: integer powers of $h_{(k/N,0)}$ $[N \geq 4$ odd$]$

- $h^*_{(k/N,0)} = 1 - q^{k/N} + O(q^{1-k/N})$
- Given $f \in \mathcal{O}(Y^1(N))^\times$, get $f = c \prod_{k=1}^{\lfloor N/2 \rfloor} h^{e(k)}_{(k/N,0)}$ with $e \in \mathbb{Q}^{\lfloor N/2 \rfloor}$ and $c \in \mathbb{C}^\times$
- To show: if $f \in \mathcal{O}(Y^1(N))^\times$, then $e \in \mathbb{Z}^{\lfloor N/2 \rfloor}$
- Claim: f^* has integral q-expansion.
- Proof of claim:
  - $\Delta^k f$ is a cusp form for some $k \in \mathbb{Z}_{\geq 0}$
  - the q-expansion of any fixed cusp form has bounded denominator
  - Gauss lemma for power series: if $f, g \in \mathbb{Q}[[x]]$ with $f(0) = g(0) = 1$ have bounded denominator and $fg \in \mathbb{Z}[[x]]$, then $f, g \in \mathbb{Z}[[x]]$.
  - Note, $(f^*)^d \in \mathbb{Z}[[x]]$ for some d, hence $f^* \in \mathbb{Z}[[x]]$.
- Let k_0 be minimal with $e(k_0) \notin \mathbb{Z}$. Apply the claim to f^* and note $f^* / \prod_{k=1}^{k_0-1} (h^*_{(k/N,0)})^{e(k)} = 1 - e(k_0) q^{k_0/N} + O(q^{(k_0+1)/N}$.
- Contradiction, so $e \in \mathbb{Z}^{\lfloor N/2 \rfloor}$.

Step 4: $12 \mid \sum e(k)$ etc.

- Functions in $\mathbb{Q}(X^1(N))^\times$ are invariant under $\Gamma^1(N) \ni \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
- $h_{(a,0)} \circ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \exp(-2\pi i/12) h_{(a,0)}$.
- So if $\prod_{k=1}^{\lfloor N/2 \rfloor} h_{(k/N,0)}^{e(k)} \in \mathcal{O}(Y^1(N))^\times$, then $\sum e(k) \in 12\mathbb{Z}$.
- Similarly $\sum e(k)k^2 \in \gcd(2,N)N\mathbb{Z}$

Conclusion: $\mathcal{O}(Y^1(N))^\times$ is $\mathbb{Q}^\times \times S$, where S is

- $\langle -b, d, f_4, \ldots, f_{\lfloor N/2 \rfloor + 1} \rangle$ (defining equations of $Y^1(k)$)
- $\langle -b, d, p_4, \ldots, f_{\lfloor N/2 \rfloor + 1} \rangle$ (terms of a recurrent sequence)
- $\left\{ \prod_{k=1}^{\lfloor N/2 \rfloor} h_{(k/N,0)}^{e(k)} : \begin{array}{rcl} e & \in & \mathbb{Z}^{\lfloor N/2 \rfloor}, \\ \sum_k e(k) & \in & 12\mathbb{Z}, \\ \sum_k k^2 e(k) & \in & \gcd(N,2)N\mathbb{Z} \end{array} \right\}$ (Siegel functions)

Summary

Conclusion: $\mathcal{O}(Y^1(N))^\times$ is $\mathbb{Q}^\times \times S$, where S is

- $\langle -b, d, f_4, \ldots, f_{\lfloor N/2 \rfloor + 1} \rangle$ (defining equations of $Y^1(k)$)
- $\langle -b, d, p_4, \ldots, f_{\lfloor N/2 \rfloor + 1} \rangle$ (terms of a recurrent sequence)
- $\left\{ \prod_{k=1}^{\lfloor N/2 \rfloor} h_{(k/N,0)}^{e(k)} : \begin{array}{rcl} e & \in & \mathbb{Z}^{\lfloor N/2 \rfloor}, \\ \sum_k e(k) & \in & 12\mathbb{Z}, \\ \sum_k k^2 e(k) & \in & \gcd(N,2)N\mathbb{Z} \end{array} \right\}$
  (Siegel functions)

Proof:

1. Connect F_k to P_k
2. Transformation between E_τ and Tate normal form
   (using some tricks not in talk)
3. Use q-expansions and Gauss' lemma
   (inspired by Kubert-Lang, but simpler and stronger)
4. Explicit action of $\Gamma^1(N)$

Work in progress

- $Y(N)$ and elliptic nets
- $Y^0(N)$ and class invariants
- moduli of abelian varieties: Hilbert/Siegel modular forms