Elliptic divisibility sequences and modular units

Marco Streng

Universiteit Leiden

Journées Arithmétiques
7 July 2015
slides: `http://bit.ly/streng`
arXiv:1503.08127

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

$$Y^1(N)(K) = \left\{ (E, P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K), \ \text{order}(P) = N \end{array} \right\} / \cong$$

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

- Modular units

$$\mathcal{O}(Y^1(N))^\times = \{\text{alg. funct.}/\mathbb{Q} \text{ on } Y^1(N) \text{ with no poles or zeroes}\}$$

Theorem (Conjecture of Derickx and Van Hoeij 2011)

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is freely generated by roughly the defining equations of $Y^1(k)$ for $k \leq N/2+1$.

Modular units $[N \geq 4]$

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

$$Y^1(N)(K) = \left\{ (E,P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \text{order}(P) = N \end{array} \right\} / \cong$$

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

- Modular units

$$\mathcal{O}(Y^1(N))^\times = \{\text{alg. funct.}/\mathbb{Q} \text{ on } Y^1(N) \text{ with no poles or zeroes}\}$$

Theorem (Conjecture of Derickx and Van Hoeij 2011)

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is freely generated by roughly the defining equations of $Y^1(k)$ for $k \leq N/2+1$.

Modular units $[N \geq 4]$

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

$$Y^1(N)(K) = \left\{ (E,P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \text{order}(P) = N \end{array} \right\} / \cong$$

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

- Modular units

$$\mathcal{O}(Y^1(N))^\times = \{\text{alg. funct.}/\mathbb{Q} \text{ on } Y^1(N) \text{ with no poles or zeroes}\}$$

Theorem (Conjecture of Derickx and Van Hoeij 2011)

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is freely generated by roughly the defining equations of $Y^1(k)$ for $k \leq N/2+1$.

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

$$A(K) = \left\{ (E, P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \text{order}(P) \neq 1, 2, 3 \end{array} \right\} / \cong,$$

so $Y^1(N) \subset A$.

- Tate normal form:

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 $B, C \in K$.

- Proof:

$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, any P

- Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.
- Get $A(K) = \{(B, C) \in K^2 : D \neq 0\}$

The ambient space

- For any field $K \supseteq \mathbb{Q}$, let
$$A(K) = \left\{ (E, P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \text{order}(P) \neq 1, 2, 3 \end{array} \right\} / \cong,$$
so $Y^1(N) \subset A$.
- Tate normal form:
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 $B, C \in K$.
- Proof:
$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, any P
    - translate P to $(0, 0)$, then $a_6 = 0$
    - as $2P \neq O$, have $a_3 \neq 0$; do $Y \mapsto Y + a_4/a_3 X$ to make $a_4 = 0$
    - as $3P \neq O$, have $a_2 \neq 0$; scale $(X, Y) \mapsto (u^2X, u^3Y)$ to make $a_2 = a_3$ □
- Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.
- Get $A(K) = \{(B, C) \in K^2 : D \neq 0\}$

The ambient space

$$A(K) = \left\{ (E,P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \mathrm{order}(P) \neq 1,2,3 \end{array} \right\} / \cong$$

- Tate normal form:
  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 $B, C \in K$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, any P
  - 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 $a_2 = a_3$ □
- Let $D = \Delta(E) \in \mathbb{Z}[B,C]$.
- Get $A(K) = \{(B,C) \in K^2 : D \neq 0\}$

The curve $Y^1(N)$ is the zero locus of an irreducible

The ambient space

$$A(K) = \left\{ (E,P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \text{order}(P) \neq 1,2,3 \end{array} \right\} / \cong$$

- Tate normal form:
  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 $B, C \in K$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, any P
  - 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 $a_2 = a_3$ $\square$
- Let $D = \Delta(E) \in \mathbb{Z}[B,C]$.
- Get $A(K) = \{(B,C) \in K^2 : D \neq 0\}$

The curve $Y^1(N)$ is the zero locus of an irreducible

The ambient space

$$A(K) = \left\{ (E,P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \text{order}(P) \neq 1,2,3 \end{array} \right\} / \cong$$

- Tate normal form:
  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 $B, C \in K$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X \cancel{+a_6}$, ~~any~~ $P = (0,0)$
  - 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 $a_2 = a_3$ □
- Let $D = \Delta(E) \in \mathbb{Z}[B,C]$.
- Get $A(K) = \{(B,C) \in K^2 : D \neq 0\}$

The curve $Y^1(N)$ is the zero locus of an irreducible

The ambient space

$$A(K) = \left\{ (E,P) : \begin{array}{l} E/K \text{ elliptic curve} \\ P \in E(K),\ \text{order}(P) \neq 1,2,3 \end{array} \right\} / \cong$$

- Tate normal form:
  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 $B, C \in K$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 \cancel{+a_4X} \cancel{+a_6}$, ~~any~~ $P = (0,0)$
  - 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 $a_2 = a_3$ $\square$
- Let $D = \Delta(E) \in \mathbb{Z}[B,C]$.
- Get $A(K) = \{(B,C) \in K^2 : D \neq 0\}$

The curve $Y^1(N)$ is the zero locus of an irreducible

The ambient space

- Tate normal form:
  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 $B, C \in K$.
- Proof:
  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 \cancel{+ a_4X} \cancel{+ a_6}$, ~~any~~ $P = (0, 0)$
  - 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 $a_2 = a_3$ $\square$
- Let $D = \Delta(E) \in \mathbb{Z}[B, C]$.
- Get $A(K) = \{(B, C) \in K^2 : D \neq 0\}$
  The curve $Y^1(N)$ is the zero locus of an irreducible $F_N \in \mathbb{Z}[B, C]$ (for $N \geq 4$).

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

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

$A \supset Y^1(N) : F_N = 0$

- Notation: blah $=$ (BLAH mod F_N)
- Note $f_k \in \mathcal{O}(Y^1(N))^\times$ for $k \neq N$.
  Proof: Polynomials have no poles,
  and zeroes would be (E, P) where P has order N and k. $\square$

Theorem (Conjecture of Derickx and Van Hoeij $\approx$ 2011)

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

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

- For $E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $k \in \mathbb{Z}$, the k-th division polynomial of E is

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

- For all $P \in E(K)$: $\psi_k(P) = 0 \iff kP = 0$
- 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

Theorem

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is freely generated by $b, d, p_4, \ldots, p_{\lfloor N/2\rfloor+1}$

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

- For $E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $k \in \mathbb{Z}$, the k-th division polynomial of E is

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

- For all $P \in E(K)$: $\quad \psi_k(P) = 0 \quad \iff \quad kP = 0$
- 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

Theorem

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is freely generated by $b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor + 1}$

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

- For $E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $k \in \mathbb{Z}$, the k-th division polynomial of E is

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

- 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

Theorem

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ is freely generated by $b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor + 1}$

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

- 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

Theorem

$\mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$ *is freely generated by* $b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor + 1}$

Elliptic divisibility sequences and recurrence

Sequences that satisfy

$\psi_{m+n}\psi_{m-n}\psi_k^2 = \psi_{m+k}\psi_{m-k}\psi_n^2 - \psi_{n+k}\psi_{n-k}\psi_m^2,$,

$\psi_1\psi_2\psi_3 \neq 0$, and

$m \mid n \Rightarrow \psi_m \mid \psi_n$

are called elliptic divisibility sequences.

The 'new' prime factors of a term are called primitive divisors.

P_1, P_2, P_3, P_4, ... is an elliptic divisibility sequence, and for $N \geq 4$, the term P_N has a unique primitive divisor F_N, which defines $Y^1(N)$.

Special cases of the recursion allow for computation:

$$\psi_{2\ell+1} = \psi_{\ell+2}\psi_\ell^3 - \psi_{\ell+1}^3\psi_{\ell-1},$$
$$\psi_{2\ell} = \psi_2^{-1}\psi_\ell\left(\psi_{\ell+2}\psi_{\ell-1}^2 - \psi_{\ell-2}\psi_{\ell+1}^2\right)$$

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

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

Step 2: Complex elliptic curves

- $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \frac{a\tau+b}{c\tau+d}$.
  $\Gamma^1(N) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \bmod N \right\}$.
-
$$\begin{aligned} \Gamma^1(N)\backslash\mathcal{H} &\cong Y^1(N)(\mathbb{C}) \\ \tau &\mapsto (E_\tau, P_\tau(\frac{1}{N}\tau)), \end{aligned}$$
  where $\quad E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ and $P_\tau(z) \in E_\tau(\mathbb{C})$.
- 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

Step 2: Complex elliptic curves

- $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \frac{a\tau+b}{c\tau+d}$.
  $\Gamma^1(N) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \bmod N \right\}$.
- $$\begin{aligned} \Gamma^1(N)\backslash\mathcal{H} &\cong Y^1(N)(\mathbb{C}) \\ \tau &\mapsto (E_\tau, P_\tau(\frac{1}{N}\tau)), \end{aligned}$$
  where $E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ and $P_\tau(z) \in E_\tau(\mathbb{C})$.
- 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

Step 2: Complex elliptic curves

- $E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ and $P_\tau(z) \in E_\tau(\mathbb{C})$.
- 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 P_k as function on $\Gamma^1(N)\backslash\mathcal{H}$.

Step 2: Complex elliptic curves

- For $a \in \mathbb{Q} \cap (0, \frac{1}{2}]$ define the Siegel function $h_{(a,0)}$ by

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

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

- Then
$\langle -b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor+1}\rangle \quad \subset \quad \langle h_{(k/N,0)} : k = 1, \ldots, \lfloor N/2 \rfloor \rangle$

- Notation: $m = \lfloor N/2 \rfloor$
Notation: for $e \in \mathbb{Z}^m$, let $h^e = \prod_{k=1}^{m} h_{(k/N,0)}^{e_k}$

- Let $T = \left\{ e \in \mathbb{Z}^m : \begin{array}{rcl} \sum_k e_k & \in & 12\mathbb{Z}, \\ \sum_k k^2 e_k & \in & \gcd(N,2)N\mathbb{Z} \end{array} \right\}.$

- Then $\langle -b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor+1}\rangle = \{h^e : e \in T\}.$

Step 2: Complex elliptic curves

- For $a \in \mathbb{Q} \cap (0, \frac{1}{2}]$ define the Siegel function $h_{(a,0)}$ by

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

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

- Then
$\langle -b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor + 1} \rangle \quad \subset \quad \langle h_{(k/N,0)} : k = 1, \ldots, \lfloor N/2 \rfloor \rangle$

- Notation: $m = \lfloor N/2 \rfloor$
Notation: for $e \in \mathbb{Z}^m$, let $h^e = \prod_{k=1}^m h_{(k/N,0)}^{e_k}$
- Let $T = \left\{ e \in \mathbb{Z}^m : \begin{array}{rcl} \sum_k e_k & \in & 12\mathbb{Z}, \\ \sum_k k^2 e_k & \in & \gcd(N,2)N\mathbb{Z} \end{array} \right\}$.
- Then $\langle -b, d, p_4, \ldots, p_{\lfloor N/2 \rfloor + 1} \rangle = \{ h^e : e \in T \}$.

- $T = \left\{ e \in \mathbb{Z}^m : \begin{array}{rcl} \sum_k e_k & \in & 12\mathbb{Z}, \\ \sum_k k^2 e_k & \in & \gcd(N,2)N\mathbb{Z} \end{array} \right\}$
- Main theorem is equivalent to bijectivity of
  $T \to \mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times \; : \; e \mapsto h^e$.

Steps:

3 injective with finite cokernel,
so all $f \in \mathcal{O}(Y^1(N))^\times$ are uniquely of the form ch^e with $e \in \mathbb{Q}^m$.

4 $h^e \in \mathcal{O}(Y^1(N))^\times \Rightarrow e \in \mathbb{Z}^m$.

5 $h^e \in \mathcal{O}(Y^1(N))^\times \Rightarrow$ the congruences

Steps 3 and 4 are inspired by Kubert-Lang who treat $\mathcal{O}(Y(N)_\mathbb{C})^\times$ up to power-of-2 index.

- $T \to \mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$
- rank(codomain) $\leq \# \frac{\{\text{cusps}\}}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} - 1 = \lfloor N/2 \rfloor =$ rank(domain) so injectivity is enough
- We show that if $e \neq 0$, then $h^e \notin \mathbb{Q}^\times$.
- Take k_0 minimal with $e_{k_0} \neq 0$.
- Divide by leading terms, that is,

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

- Then $(h^e)^* = 1 - e_{k_0} q^{k_0/N} + O(q^{(k_0+1)/N}) \neq 1$, so $h^e \notin \mathbb{Q}^\times$

Step 3: Injective with finite cokernel $\quad [N \geq 4 \text{ odd}]$

- $T \to \mathcal{O}(Y^1(N))^\times/\mathbb{Q}^\times$
- $\mathrm{rank}(\text{codomain}) \leq \#\frac{\{\text{cusps}\}}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} - 1 = \lfloor N/2 \rfloor = \mathrm{rank}(\text{domain})$
  so injectivity is enough
- We show that if $e \neq 0$, then $h^e \notin \mathbb{Q}^\times$.
- Take k_0 minimal with $e_{k_0} \neq 0$.
- Divide by leading terms, that is,

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

- Then $(h^e)^* = 1 - e_{k_0} q^{k_0/N} + O(q^{(k_0+1)/N}) \neq 1$, so $h^e \notin \mathbb{Q}^\times$

Steps 4 and 5 [N odd]

Step 4:

- Combine the above with Gauss' lemma for power series with bounded denominators, and the fact that cusp forms have q-expansions with bounded denominators.
- This gives $e \in \mathbb{Z}^m$.

Step 5:

- Explicit action of $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \Gamma^1(N)$
- This gives congruences on e.

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 elliptic divisibility sequence P_k

2 Transformation between E_τ and Tate normal form (using some tricks not in talk)

3/4 Use q-expansions and Gauss' lemma (inspired by Kubert-Lang, but simpler and stronger)

5 Explicit action of $\Gamma^1(N)$

Work in progress

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