Marco Streng – Modular Units via EDS recurrence

arXiv: 1503.08127

§ Intro

For $N \in \mathbb{Z}$, $N \geq 4$, $K \supseteq \mathbb{Q}$ field,

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

- affine algebraic curves $Y'(N)/\mathbb{Q}$

- $Y'(N)(\mathbb{C}) \xleftarrow{\sim} \Gamma'(N) \backslash \mathbb{H}$

$\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right) \bmod N$

Def $\mathcal{O}(Y'(N)) = \left\{ \begin{array}{l} \text{regular functions} \\ \text{on } Y'(N) \text{ over } \mathbb{Q} \end{array} \right\}$

Then $\mathcal{O}(Y'(N))^* \xrightarrow{\sim} \left\{ \begin{array}{l} \text{meromorphic functions} \\ \text{on } \Gamma'(N) \backslash (\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})) \\ \text{with poles \& zeroes only at cusps,} \\ \text{and } q\text{-expansion coefficients in } \mathbb{Q} \end{array} \right\}$

Punchline

$\mathcal{O}(Y'(N))^*$ is more-or-less generated by the defining equations of $Y'(k)$ for $k \leq \lfloor N/2 \rfloor + 1$.

Steps
- §1 ambient space
- §2 division polynomials
- §3 q-expansions

§1

Let $A(K) = \left\{ (E,P) : \begin{array}{l} E/K \text{ ell. curve} \\ P \in E(K) \text{ not order } 1,2,3 \end{array} \right\} / \cong$

$\supseteq Y'(N)(K)$

Tate normal form:

bijection $A(K) \longleftrightarrow \{ (B,C) \in K^2 : D \neq 0 \}$

$(E,P) \longleftarrow (B,C)$

where $E: y^2 + (1-C)xy - By = x^3 - Bx^2$

$P = (0,0)$

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

Now $Y'(N) \subset A \cong \mathbb{A}^2 \setminus (D=0)$

given by irred. $F_N \in \mathbb{Q}[B,C]$

Example Can show $4P = 0 \iff C = 0$

$F_4 = C$.

Similarly $F_5 = C - B$

$F_6 = C^2 - B + C$.

Fix $N \geq 4$, let $f_k = (F_k \bmod F_N) \in \mathcal{O}(Y'(N))^*$ for $k \neq N$

$\boxed{\text{If it has a zero on } Y'(N) \text{ at } (E,P), \text{ then } P \text{ has order } N \text{ and } k \text{ ↯}}$

$b = (B \bmod F_N)$

$d = (D \bmod F_N)$

$\in \mathcal{O}(Y'(N))^*$

Theorem (S; Conj. of Derickx & Van Hoeij)

For all $N \geq 4$, $\mathcal{O}(Y'(N))^* / \mathbb{Q}^*$ is the free abelian group with basis $b, d, f_4, f_5, \ldots, f_{\lfloor N/2 \rfloor + 1}$.

Marco Streng – Modular Units via EDS recurrence

arXiv: 1503:08127

§2 Division polynomials

- $\Psi_k \in \mathbb{Z}[a_1, a_2, \dots, a_6][x,y]/(\text{weierstrass eqn})$
- For E/K and $P \in E(K)$
  $$\Psi_k(E,P) = 0 \iff [k]P = 0$$
- $$\Psi_{m+n}\Psi_{m-n}\Psi_k^2 = \Psi_{m+k}\Psi_{m-k}\Psi_n^2 - \Psi_{n-k}\Psi_{n+k}\Psi_m^2$$

Let $P_k = \Psi_k(\text{Tate N.F.}) \in \mathbb{Z}[B,C]$

$a_1 = 1-C$
$a_2 = a_3 = -B$
$a_4 = a_6 = x = y = 0$

$P_1 = 1,\ P_2 = B,\ P_3 = -B^3,\ P_4 = \underbrace{C}_{F_4}B^5,$
$P_5 = -\underbrace{(C-B)}_{F_5}B^8$

Note: For $k \geq 4$:
F_k = ("new" factor of P_k)

§3 q-expansions

$$\Gamma'(N)\backslash\mathbb{H} \xrightarrow{\sim} Y'(N)(\mathbb{C})$$
$$\tau \longmapsto \left(\mathbb{C}/(\tau\mathbb{Z}+\mathbb{Z}), \tfrac{\tau}{N}\right)$$

Def
- $q^\alpha := \exp(2\pi i \alpha\tau)$ for $\alpha \in \mathbb{R}$
- Siegel function
  $$h_a(\tau) = i q^{\frac{1}{2}(a^2 - a + \frac{1}{6})}(1-q^a) \cdot \prod_{n=1}^{\infty}(1-q^{n+a})(1-q^{n-a})$$

Proposition

$$\mathbb{Q}^*\langle b, d, p_4, \dots, p_{\lfloor N/2\rfloor+1}\rangle = S := \mathbb{Q}^* \cdot \left\{ \prod_{k=1}^{\lfloor N/2\rfloor} h_{k/N}^{e(k)} : \begin{array}{l} e \in \mathbb{Z}^{\lfloor N/2\rfloor} \\ \sum_k e(k) \in 12\mathbb{Z} \\ \sum_k k^2 e(k) \\ \in \gcd(N,2)N\mathbb{Z} \end{array} \right\}$$

Proof ...... $\square$

TO DO: prove $S = \mathcal{O}(Y'(N))^*$.

Counting cusps $\rightsquigarrow \operatorname{rk}\left(\mathcal{O}(Y'(N))^*/\mathbb{Q}^*\right) \leq \lfloor N/2 \rfloor$

Claim $\operatorname{rk} S/\mathbb{Q}^* = \lfloor N/2 \rfloor$

and $\forall f \in \mathcal{O}(Y'(N))^*$
$\forall \ell \in \mathbb{Z}_{>0}$
$$f^\ell \in S \implies f \in S.$$

Note Claim $\implies$ Thm.

Proof of claim (say N odd)

For $e \in \mathbb{Z}^{\lfloor N/2 \rfloor}$, let
$$h^e = \prod_{k=1}^{\lfloor N/2\rfloor} h_{k/N}^{e(k)}$$

For $f \in \mathbb{C}((q^{\frac{1}{12N^2}}))$, write
$$f^* = \frac{f}{\text{leading term}} = 1 + \text{h.o.t.}$$

so $h_a^* = 1 - q^a + \text{h.o.t.}$
if $0 < a < \frac{1}{2}$

Marco Streng - Modular Units via EDS recurrence

arXiv: 1503:08127

(1) rank

Suppose $h^e \in \mathbb{C}^*$ for some $e \neq 0$

Take k minimal s.t. $e(k) \neq 0$.

Then $1 = (h^e)^* = \prod_{k=1}^{\lfloor N/2 \rfloor} (h^*_{k/N})^{e(k)}$

$$= \underbrace{\left(1 - q^{k/N}\right)}_{h^*_{k/N}}^{e(k)} \cdot (1 + \cdots)$$

$$= 1 - e(k) q^{k/N} + h.o.t.$$

So $e(k) = 0$, contraction

So $\mathbb{Z}^{\lfloor N/2 \rfloor} \hookrightarrow \mathbb{C}((q^{\frac{1}{12N^2}}))^* / \mathbb{C}^*$

$e \longmapsto h^e$

□ rank.

(2) If $f^\ell \in S$, then

$f^\ell = h^e$, so

$$(\boxed{f^*})^\ell = \boxed{(h^e)^*}$$

bounded denominator (modular functions)

integer coefficients.

Both $1 + h.o.t.$

Gauss' lemma: f^* has integer coefficients.

Trick as in (1) $\rightsquigarrow \frac{1}{\ell} e \in \mathbb{Z}^{\lfloor N/2 \rfloor}$

$$\boxed{f^* = 1 - \tfrac{1}{\ell} e(k) q^{k/N} + h.o.t.}$$

So $f = h^{e'}$ for some $e' \in \mathbb{Z}^{\lfloor N/2 \rfloor}$

up to $\mathbb{Q}^*$-scaling.

Then using action of $\Gamma^1(N)$: prove congruences in def of S.