國 立 交 通 大 學

應用數學系

碩　士　論　文

非同餘子群的模型式的同餘性質

Atkin and Swinnerton-Dyer Congruences Associated to Fermat Curves

研 究 生：林易萱

指導老師：楊一帆　教授

中 華 民 國 一 百 年 六 月

非同餘子群的模型式的同餘性質

Atkin and Swinnerton-Dyer Congruences Associated to Fermat Curves

研 究 生：林易萱　　Student：Yi-Hsuan Lin

指導教授：楊一帆　　Advisor：Yifan Yang

國 立 交 通 大 學

應用數學系

碩 士 論 文

A Thesis

Submitted to Department of Applied Mathematics

College of Science,

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master

In

Applied Mathematics

June 2011

Hsinchu, Taiwan, Republic of China

中 華 民 國 一 百 年 六 月

非同餘子群的模型式的同餘性質

學生：林易萱　　　　　　　　　　　　　　　　　　　　　指導老師：楊一帆教授

國立交通大學應用數學系(研究所)碩士班

摘　要

眾所周知的，費馬曲線 $x^n + y^n = 1$ 是一個與特殊線性群$SL_2(\mathbb{Z})$的有限指數子群Γ_n相關聯的模曲線，當n不等於1, 2, 4, 8時，Γ_n是一個非同餘子群。現在令費馬曲線的虧格為g，scholl的定理告訴我們，Γ_n上權為2的尖點型式與由此曲線相關聯的Tate模所建構出的$2g$維l進數伽羅瓦表現會滿足Atkin and Swinnerton-Dyer同餘。

在這篇論文中，我們將會分解伽羅瓦表現，然後給一個更加精確的 Atkin and Swinnerton-Dyer 同餘。我們將會解決$\mathrm{n} = 6$的情況。

Atkin and Swinnerton-Dyer Congruences Associated to Fermat Curves

Student: Yi-Hsuan Lin Advisor: Yifan Yang

Department (Institute) of Applied Mathematics

National Chiao Tung University

Abstract

It is known that each Fermat curve $x^n + y^n = 1$ is the modular curve associated to some subgroup Γ_n of $SL_2(\mathbb{Z})$ of finite index. Moreover if $n \neq 1, 2, 4, 8$ then Γ_n is a noncongruence subgroup. Let g be the genus of the Fermat curve, by Scholl's theorem, cuspforms of weight 2 on Γ_n, together with the $2g$-dimensional l-adic Galois representations coming from the Tate module associate this curve, satisfy the Atkin and Swinnerton-Dyer congruence.

In this thesis, we decompose this Galois representation and give a more precise Atkin and Swinnerton-Dyer congruence. The case $n = 6$ will be completely worked out.

誌　謝

遙記當年第一次接觸數論,是大三那年在楊一帆老師的基礎數論課堂上,那時的我，被簡單而漂亮的質數所吸引，或許是這種吸引力，引領著我進入了這個領域。

這篇論文的完成，要感謝所有授我知識的老師，尤其是我的指導教授楊一帆老師，不僅僅啟發我在數論上的興趣以及傳授我課業上所需要的知識,更因老師的平易近人個性，讓我們在生活各方面能與老師共同分享。

不能因為要感謝的人太多，就總是謝天，但若有遺漏到誰，麻煩請連絡我，讓我向您當面致謝以表歉意。首要感謝學姊芳婷無論是對學業或生活上的關心以及帶給我們歡樂的學習氣氛、學長家瑋為我排憂解難，營造學習氣氛、以及學長耀漢時常督促我們要努力用功·再來要感謝遠在英國的摯友廷蓉，時常幫助我解決英文上的困難。還有感謝光祥陪伴我到清大修代數課程，使我不至於孤軍奮戰。也要感謝在碩士生生涯這兩年間與我共同學習共同歡樂的定國、冠緯、敏豪、劭芃、聲華、權益,還有已經畢業的葉彬、文昱等等，是你們豐富了我的人生。

還要感謝吾姊宛儀以及姊夫子濤，雖然你們已經移居香港，但仍時關心我的學業以及生活。最後我要感謝我的父母、祖母、外祖母以及眾多長輩們，沒有你們的支持，在這條道路上我無法走得安穩，我衷心感念，

林易萱

謹誌于交通大學

2011年6月

目　　錄

中文提要 i
英文提要 ii
誌謝 iii
目錄 iv

1 Introduction **1**

2 Review of modular forms on congruence subgroups **2**

- 2.1 Modular forms and cusp forms 2
- 2.2 Hecke operators 5
- 2.3 Petersson inner product 9
- 2.4 Oldforms and Newforms 10
- 2.5 Hecke eigenforms 11

3 Atkin and Swinnerton-Dyer congruences for noncongruence subgroups **12**

- 3.1 Noncongruence subgroups 13
- 3.2 Atkin and Swinnerton-Dyer congruence 13

4 Atkin and Swinnerton-Dyer congruences associated to Fermat curves **17**

- 4.1 Fermat curve 17
- 4.2 Case $x^6 + y^6 = 1$ 18

5 References **24**

1. Introduction

The Fourier coefficients of a normalized newform $f = \sum_{n\geq 1} a_n(f)q^n$ of weight k, level N, and character χ on a congruence subgroup, where $q = e^{2\pi i\tau}$, satisfy the recursive relation

$$a_{np}(f) - a_p(f)a_n(f) + \chi(p)p^{k-1}a_{n/p}(f) = 0 \qquad (1.0.1)$$

for all prime p, $p \nmid N$. For noncongruence subgroups, the recursive relation in (1.0.1) no longer holds. Nevertheless, Atkin and Swinnerton-Dyer observed other congruence relations which are introduced in Chapter 3.

Recall that the Fermat curve $F_n = x^n + y^n = 1$ is the modular curve with genus $g = \frac{(n-1)(n-2)}{2}$ associated to the modular subgroup

$$\Gamma_n = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^n, \Gamma(2)^{'} \right\rangle$$

where $\Gamma(2)^{'}$ denotes the commutator subgroup of $\Gamma(2)$. When $n \neq 1, 2, 4, 8$, Γ_n is noncongruence. Cusp forms of weight 2 can be obtained by differential forms and the parametrization $(x, y) = (\sqrt[n]{1-\lambda},\ \sqrt[n]{\lambda})$, where $\lambda = \frac{\theta_2(\tau)^4}{\theta_3(\tau)^4}$, described in section 4.1. By Scholl's theorem, they satisfy the Atkin and Swinnerton-Dyer congruence with a characteristic polynomial of degree $2g$. However, this means that even in the case of the smallest odd prime 3, we are required to figure out at least 3^{2g} terms in cusp forms. Therefore, this calculation is not a simple task.

In order to reduce difficulty, in Chapter 4, we decompose Scholl's $2g$-dimensional Galois representations into pieces for the case $n = 6$, and give a more precise Atkin and Swinnerton-Dyer congruence.

2. Review of modular forms on congruence subgroups

§ 2.1 Modular forms and cusp forms

The **modular group** is the group of 2×2 matrices with integer entries and determinant 1,

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

The modular group is generated by the two matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Each element of the modular group is also viewed as an automorphism (invertible self-map) of the Riemann sphere $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, the fractional linear transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \tau \in \widehat{\mathbb{C}}.$$

This is understood to mean that if $c \neq 0$ then $-d/c$ maps to ∞ and ∞ maps to a/c, and if $c = 0$ then ∞ maps to ∞. The identity matrix I and its negative $-I$ both give the identity transformation, and more generally each pair $\pm\gamma$ of matrices in $SL_2(\mathbb{Z})$ gives a single transformation. The group of transformations defined by the modular group is generated by the maps described by the two matrix generators,

$$\tau \mapsto \tau + 1 \text{ and } \tau \mapsto -1/\tau$$

The **upper half plane** is

$$\mathbb{H} = \{\tau \in \mathbb{C} : \text{Im}(\tau) > 0\}.$$

The formula

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2},\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

shows that if $\gamma \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$ then also $\gamma(\tau) \in \mathbb{H}$, i.e., the modular group maps the upper half plane back to itself. In fact the modular group acts on the upper half plane, meaning that $I(\tau) = \tau$ where I is the identity matrix and $(\gamma\gamma^{'})(\tau) = \gamma(\gamma^{'}(\tau))$ for all $\gamma, \gamma^{'} \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$.

Let N be a positive integer. The **principal congruence subgroup of level** N is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\ N) \right\}$$

In particular $\Gamma(1) = SL_2(\mathbb{Z})$. Being the kernel of the natural homomorphism $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$, the subgroup $\Gamma(N)$ is normal in $SL_2(\mathbb{Z})$. In fact the map is a surjection, inducing an isomorphism

$$SL_2(\mathbb{Z})/\Gamma(N) \xrightarrow{\sim} SL_2(\mathbb{Z}/N\mathbb{Z}).$$

This shows that $[SL_2(\mathbb{Z}) : \Gamma(N)]$ is finite for all N. Specifically, the index is $[SL_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$ where the product is taken over all prime divisors of N.

Definition 2.1. A subgroup Γ of $SL_2(\mathbb{Z})$ is a **congruence subgroup** if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{N}$, in which case Γ is a congruence subgroup of **level** N. If Γ does not contain $\Gamma(N)$ for any N, then we say Γ is a **noncongruence subgroup**.

Every congruence subgroup Γ has finite index in $SL_2(\mathbb{Z})$. Besides the principal congruence subgroups, the most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ (\mathrm{mod}\ N) \right\}$$

(where "$*$" means "unspecified") and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

satisfying

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$$

Two pieces of notation are essential before we continue. For any matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ define the **factor of automorphy** $j(\gamma, \tau) \in \mathbb{C}$ for $\tau \in \mathbb{H}$ to be

$$j(\gamma, \tau) \ = \ c\tau + d$$

and for $\gamma \in SL_2(\mathbb{Z})$ and any integer k define the **weight-k operator** $[\gamma]_k$ on functions $f : \mathbb{H} \longrightarrow \mathbb{C}$ by

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \ \tau \in \mathbb{H}$$

Since the factor of automorphy is never zero or infinity, if f is meromorphic then $f[\gamma]_k$ is also meromorphic and has the same zeros and poles as f.

Definition 2.2. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let k be an integer. A function $f : \mathbb{H} \longrightarrow \mathbb{C}$ is a **modular form of weight k with respect to Γ** if

(1) f is holomorphic,

(2) f is weight-k invariant under Γ,

(3) $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

If in addition,

(4) $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$,

then f is a **cusp form of weight k with respect to Γ**. The modular forms of weight k with respect to Γ are denoted $\mathcal{M}_k(\Gamma)$, the cusp forms $\mathcal{S}_k(\Gamma)$.

§ 2.2 Hecke operators

Let Γ_1 and Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$. Then Γ_1 and Γ_2 are subgroups of $GL_2^+(\mathbb{Q})$, the group of 2×2 matrices with rational entries and positive determinant. For each $\alpha \in GL_2^+(\mathbb{Q})$ the set

$$\Gamma_1 \alpha \Gamma_2 = \{\gamma_1 \alpha \gamma_2 \ : \ \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$$

is a **double coset** in $GL_2^+(\mathbb{Q})$. Under a definition to be developed in this section, such double cosets transform modular forms with respect to Γ_1 into modular forms with respect to Γ_2.

The group Γ_1 acts on the double coset $\Gamma_1 \alpha \Gamma_2$ by left multiplication, partitioning it into orbits. A typical orbit is $\Gamma_1 \beta$ with representative $\beta = \gamma_1 \alpha \gamma_2$, and the orbit space $\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2$ is thus a disjoint union $\bigcup \Gamma_1 \beta_j$ for some choice of representatives β_j. The next two lemmas combine to show that this union is finite.

Lemma 2.3 ([2] Lemma 5.1.1)**.** *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let α be an element of $GL_2^+(\mathbb{Q})$. Then $\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z})$ is again a congruence subgroup of $SL_2(\mathbb{Z})$.*

Lemma 2.4 ([2] Lemma 5.1.2)**.** *Let Γ_1 and Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$, and let α be an element of $GL_2^+(\mathbb{Q})$. Set $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$, a subgroup of Γ_2. Then left multiplication by α,*

$$\Gamma_2 \longrightarrow \Gamma_1 \alpha \Gamma_2 \quad \text{given by} \quad \gamma_2 \mapsto \alpha\gamma_2,$$

induces a natural bijection from the coset space $\Gamma_3 \backslash \Gamma_2$ to the orbit space $\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2$. In concrete terms, $\{\gamma_{2,j}\}$ is a set of coset representatives for $\Gamma_3 \backslash \Gamma_2$ if and only if $\{\beta_j\} = \{\alpha\gamma_{2,j}\}$ is a set of orbit representatives for $\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2$.

We say that two subgroups H_1 and H_2 of a group G are **commensurable**, if the indices $[H_1 : H_1 \cap H_2]$ and $[H_2 : H_1 \cap H_2]$ are finite.

Theorem 2.5. *Any two congruence subgroups* Γ_1 *and* Γ_2 *of* $SL_2(\mathbb{Z})$ *are commensurable.*

Proof. First we know $[SL_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$ is finite. Consider for any subgroups Γ_1, Γ_2 of $SL_2(\mathbb{Z})$, take N_1, $N_2 \in \mathbb{N}$ such that $\Gamma(N_1) \subset \Gamma_1$ and $\Gamma(N_2) \subset \Gamma_2$, and let $N_3 = \text{lcm}(N_1, N_2)$, then we have

$$\Gamma(N_3) \subset \Gamma(N_1) \cap \Gamma(N_2) \subset \Gamma_1 \cap \Gamma_2$$

which implies $[SL_2(\mathbb{Z}) : \Gamma(N_3)] \geq [\Gamma_1 : \Gamma(N_3)] \geq [\Gamma_1 : \Gamma(N_1) \cap \Gamma(N_2)] \geq [\Gamma_1 : \Gamma_1 \cap \Gamma_2]$

Similarly, we can prove $[\Gamma_2 : \Gamma_1 \cap \Gamma_2]$ is finite. □

In particular, since $\alpha^{-1}\Gamma_1\alpha \cap SL_2(\mathbb{Z})$ is a congruence subgroup of $SL_2(\mathbb{Z})$ by Lemma 2.3, the coset space $\Gamma_3 \backslash \Gamma_2$ in Lemma 2.4 is finite and hence so is the orbit space $\Gamma_1 \backslash \Gamma_1\alpha\Gamma_2$. With finiteness of the orbit space established, the double coset $\Gamma_1\alpha\Gamma_2$ can act on modular forms.

Now for $\beta \in GL_2^+(\mathbb{Q})$ and $k \in \mathbb{Z}$, and $\tau \in \mathbb{H}$, extend the formula $j(\beta, \tau) = c\tau + d$ to $\beta \in GL_2^+(\mathbb{Q})$, and extend the weight-$k$ operator to $GL_2^+(\mathbb{Q})$ which called the **weight-k β operator** by the rule

$$(f[\beta]_k)(\tau) = (\det\beta)^{k-1} j(\beta, \tau)^{-k} f(\beta(\tau)), \quad \text{for} \quad f : \mathbb{H} \to \mathbb{C}$$

Definition 2.6. For congruence subgroups Γ_1 and Γ_2 of $SL_2(\mathbb{Z})$ and $\alpha \in GL_2^+(\mathbb{Q})$, the **weight-$k$ $\Gamma_1\alpha\Gamma_2$ operator** takes functions $f \in \mathcal{M}_k(\Gamma_1)$ to

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k$$

where $\{\beta_j\}$ are orbit representatives, i.e., $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$ is a disjoint union.

Now we introduces two operators on $\mathcal{M}_k(\Gamma_1(N))$. Consider the map

$$\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^* \quad \text{taking} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ to } d \pmod N$$

is a surjective homomorphism with kernel $\Gamma_1(N)$. This shows that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ and induces an isomorphism

$$\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^* \quad \text{where} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ to } d \pmod N$$

To define the first type of Hecke operator, take any $\alpha \in \Gamma_0(N)$, set $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, and consider the weight-k double coset operator $[\Gamma_1\alpha\Gamma_2]_k$. Since $\Gamma_1(N) \lhd \Gamma_0(N)$ this operator translating each function $f \in \mathcal{M}_k(\Gamma_1(N))$ to

$$f[\Gamma_1\alpha\Gamma_2]_k = f[\alpha]_k, \quad \alpha \in \Gamma_0(N),$$

again in $\mathcal{M}_k(\Gamma_1(N))$. Thus the group $\Gamma_0(N)$ acts on $\mathcal{M}_k(\Gamma_1(N))$, and since its subgroup $\Gamma_1(N)$ acts trivially, this is really an action of the quotient $(\mathbb{Z}/N\mathbb{Z})^*$. The action of α determined by $d \pmod N$ and denoted $\langle d \rangle$, is

$$\langle d \rangle \ : \ \mathcal{M}_k(\Gamma_1(N)) \longrightarrow \mathcal{M}_k(\Gamma_1(N))$$

given by

$$\langle d \rangle f = f[\alpha]_k \text{ for any } \alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N) \text{ with } \delta \equiv d \ (\text{mod} N)$$

This type of Hecke operator is also called a **diamond operator**. Now we are going to define the second type of Hecke operator, again $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, but now $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, where p is a prime, we define a weight-k double coset operator

$$T_p \ : \ \mathcal{M}_k(\Gamma_1(N)) \longrightarrow \mathcal{M}_k(\Gamma_1(N)), \ p \text{ prime}$$

is given by

$$T_p f = f[\Gamma_1(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_1(N)]_k.$$

The double coset here is

$$\Gamma_1(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_1(N) = \left\{\gamma \in M_2(\mathbb{Z}) \ : \ \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \pmod N, \ det\gamma = p\right\},$$

so in fact $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ can be replaced by any matrix in this double coset in the definition of T_p.

Proposition 2.7 ([2] Proposition 5.2.4)**.** *Let d and e be elements of $(\mathbb{Z}/N\mathbb{Z})^*$, and let p and q be prime. Then*
(1)$\langle d\rangle T_p = T_p\langle d\rangle$
(2)$\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle = \langle de\rangle$
(3)$T_pT_q = T_qT_p$

Now we can extend the definitions of $\langle d\rangle$ and T_p to $\langle n\rangle$ and T_n for all $n \in \mathbb{Z}^+$. For $n \in \mathbb{Z}^+$ with $(n, N) = 1$, $\langle n\rangle$ is determined by $n \pmod N$. For $n \in \mathbb{Z}^+$ with $(n, N) > 1$, define $\langle n\rangle = 0$, the zero operator on $\mathcal{M}_k(\Gamma_1(N))$. The mapping $n \mapsto \langle n\rangle$ is totally multiplicative.

To define T_n, set $T_1 = 1$ (the identity operator); T_p is already defined for primes p. For prime powers, define inductively

$$T_{p^r} = T_pT_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}, \quad \text{for } r \geq 2,$$

and note that inductively on r and s starting from Proposition 2.7(c), $T_{p^r}T_{q^s} = T_{q^s}T_{p^r}$ for distinct primes p and q. Extend the definition multiplicatively to T_n for all n,

$$T_n = \prod T_{p_i^{e_i}} \quad \text{where} \quad n = \prod p_i^{e_i}$$

so that the T_n all commute by Proposition 2.7 and

$$T_{nm} = T_n T_m \quad \text{if } (n,m) = 1.$$

Theorem 2.8 ([2] Proposition 5.3.1)**.** *Let $f \in \mathcal{M}_k(\Gamma_1(N))$ have Fourier expansion*

$$f(\tau) = \sum_{m=0}^{\infty} a_m(f) q^m \text{ where } q = e^{2\pi i \tau}.$$

Then for all $n \in \mathbb{Z}^+$, $T_n f$ has Fourier expansion

$$(T_n f)(\tau) = \sum_{m=0}^{\infty} a_m(T_n f) q^m$$

where

$$a_m(T_n f) = \sum_{d|(m,n)} d^{k-1} a_{mn/d^2}(\langle d \rangle f). \tag{2.8.1}$$

In particular, if $f \in \mathcal{M}_k(N, \chi)$ then

$$a_m(T_n f) = \sum_{d|(m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f). \tag{2.8.2}$$

§ 2.3 Petersson inner product

In this section, we make the space of cusp forms $\mathcal{S}_k(\Gamma)$ into an inner product space, the integral in the following definition is well defined and convergent.

Definition 2.9. Let $\Gamma \subset SL_2(\mathbb{Z})$ be a congruence subgroup. The **Petersson inner product**,

$$\langle , \rangle_\Gamma : \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \longrightarrow \mathbb{C},$$

is given by

$$\langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X_{(\Gamma)}} f(\tau) \overline{g(\tau)} (\mathrm{Im}(\tau))^k d\mu(\tau).$$

where V_Γ is the volume of $X_{(\Gamma)}$ and $d\mu(\tau) = \frac{dxdy}{y^2}$ for $\tau = x + iy$.

This product is linear in f, conjugate linear in g, Hermitiansymmetric, and positive definite. The normalizing factor $1/V_\Gamma$ ensures that if $\Gamma' \subset \Gamma$ then $\langle , \rangle_\Gamma' = \langle , \rangle_\Gamma$ on $\mathcal{S}_k(\Gamma)$.

§ 2.4 Oldforms and Newforms

So far the theory has all taken place at one generic level N. This section begins results that move between levels, taking forms from lower levels $M|N$ up to level N, mostly with $M = Np^{-1}$ where p is some prime factor of N.

Lemma 2.10. *If $M|N$ then $\mathcal{S}_k(\Gamma_1(M)) \subset \mathcal{S}_k(\Gamma_1(N))$*

Proof. If $M|N$, we have $\Gamma_1(N) \subset \Gamma_1(M)$ since for any $\gamma \in \Gamma_1(N)$, write $\gamma = \begin{pmatrix} k_1N+1 & * \\ k_2N & k_3N+1 \end{pmatrix}$, and write $N = lM$ for some integer l, then $\gamma = \begin{pmatrix} k_1lM+1 & * \\ k_2lM & k_3lM+1 \end{pmatrix}$, hence $r \in \Gamma_1(M)$.

Now if f is a modular form with respect to $\Gamma_1(M)$, it is also a modular form with respect to $\Gamma_1(N)$ since $\Gamma_1(N) \subset \Gamma_1(M)$. □

Lemma 2.11. *For any h factor of N/M, let $\alpha_h = \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix}$, so that $(f[\alpha_h]_k)(\tau) = h^{k-1}f(h\tau)$ for $f : \mathbb{H} \longrightarrow \mathbb{C}$. The linear map $[\alpha_h]_k$ takes $\mathcal{S}_k(\Gamma_1(M))$ to $\mathcal{S}_k(\Gamma_1(N))$, lifting the level from M to N.*

Proof. Let $\gamma = \begin{pmatrix} aN+1 & b \\ cN & dN+1 \end{pmatrix} \in \Gamma_1(N)$. We have

$$h\gamma\tau = \frac{(aN+1)(h\tau)+hb}{(cN/h)(h\tau)+dN+1} = \begin{pmatrix} aN+1 & hb \\ cN/h & dN+1 \end{pmatrix}(h\tau)$$

By h is a factor of N/M, we have $\gamma' = \begin{pmatrix} aN+1 & hb \\ cN/h & dN+1 \end{pmatrix}$ is in $\Gamma_1(M)$. Therefore

$$f(h\gamma\tau) = f(\gamma'(h\tau)) = (cN\tau + dN + 1)^k f(h\tau).$$

This shows $g(\tau) = f(h\tau)$ is a cusp form on $\Gamma_1(N)$. □

Combining preceding two lemmas, it is natural to distinguish the part of $\mathcal{S}_k(\Gamma_1(N))$ coming from lower levels.

Definition 2.12. For each divisor d of N, let i_d be the map

$$i_d : (\mathcal{S}_k(\Gamma_1(Nd^{-1})))^2 \longrightarrow \mathcal{S}_k(\Gamma_1(N))$$

given by

$$(f, g) \mapsto f + g[\alpha_d]_k.$$

The subspace of **oldforms at level** N is

$$\mathcal{S}_k(\Gamma_1(N))^{\text{old}} = \sum_{\substack{p|N \\ prime}} i_p((\mathcal{S}_k(\Gamma_1(Nd^{-1})))^2)$$

and the subspace of **newforms at level** N is the orthogonal complement with respect to the Petersson inner product,

$$\mathcal{S}_k(\Gamma_1(N))^{\text{new}} = (\mathcal{S}_k(\Gamma_1(N))^{\text{old}})^{\perp}.$$

§ 2.5 Hecke eigenforms

In this section, we will show if $f \in \mathcal{M}(N, \chi)$ is a normalized eigenform, then its Fourier coefficients will satisfy the recursive relation $a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - \chi(p)p^{k-1}a_{p^{r-2}}(f)$ for all p prime and $r \geq 2$.

Definition 2.13. Let f be a non-vanishing modular form. If f is a simutaneous eigenfunction for all Hecke operator T_n, then we say f is a **Hecke eigenform**. If the Fourier expansion of f has leading coefficient 1, then f is **normalized**.

Definition 2.14. Let χ be a Dirichlet character modulo N, we define the χ-eigenspace of $\mathcal{M}_k(\Gamma_1(N))$ by

$$\mathcal{M}_k(N, \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : f[\gamma]_k = \chi(d_\gamma)f \ for \ all \ \gamma \in \Gamma_0(N)\},$$

where d_γ is the lower right entry of γ.

Theorem 2.15. *Let $f \in \mathcal{M}_k(N,\chi)$. Then f is a normalized eigenform if and only if its Fourier coefficients satisfy the conditions*
(1) $a_1(f) = 1$,
(2) $a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - \chi(p)p^{k-1}a_{p^{r-2}}(f)$ *for all p prime and $r \geq 2$,*
(3) $a_{mn}(f) = a_m(f)a_n(f)$ *when $(m,n) = 1$.*

Proof. The only if part is follows from the definition of T_n. Now we prove the other way. Suppose f satisfies the three conditions. Then f is normalized, and to be an eigenform for all the Hecke operators it need only satisfy $a_m(T_pf) = a_p(f)a_m(f)$ for all p prime and $m \in \mathbb{Z}^+$. If $p \nmid m$ then formula (2.8.2) gives $a_m(T_pf) = a_{pm}(f)$ and by the third condition this is $a_p(f)a_m(f)$ as desired. On the other hand, if $p|m$ write $m = p^r m^{'}$ with $r \geq 1$ and $p \nmid m^{'}$. This time

$$\begin{aligned} a_m(T_pf) &= a_{p^{r+1}m'}(f) + \chi(p)p^{k-1}a_{p^{r-1}m'}(f) && \text{by formula (2.8.2)} \\ &= (a_{p^{r+1}}(f) + \chi(p)p^{k-1}a_{p^{r-1}}(f))a_{m'}(f) && \text{by the third condition} \\ &= a_p(f)a_{p^r}(f)a_{m'}(f) && \text{by the second condition} \\ &= a_p(f)a_m(f) && \text{by the third condition.} \end{aligned}$$

□

3. Atkin and Swinnerton-Dyer congruences for noncongruence subgroups

Last section we have develop some properties of the modular forms for congruence subgroups. Given a cuspidal normalized newform $g = \sum_{n\geq 1} a_n(g)q^n$, where $q = e^{2\pi i\tau}$, of weight $k \geq 2$ level N and character χ, the Fourier coefficients of g satisfy the recursive relation

$$a_{np}(g) - a_p(g)a_n(g) + \chi(p)p^{k-1}a_{n/p}(g) = 0 \qquad (3.0.1)$$

for all primes p not dividing N and for all $n \geq 1$.

The following sections will introduce the substitution of the recursive relation for noncongruence subgroups.

§ 3.1 Noncongruence subgroups

Let $f = \sum_{n \geq n_0} a_n w^n$ be the modular form with coefficients a_n in a fixed number field. According to Hecke operators, a basis consisting of forms with integral coefficients exists in each space of holomorphic congruence modular forms. Consequently, for every congruence holomorphic modular form with algebraic coefficients, the sequence $\{a_n\}$ has bounded denominators in the sense that there exists an algebraic number M such that Ma_n is algebraic integral for all n. Therefore, the sequence $\{b_n\}$ having unbounded denominators implies $g = \sum_{n \geq n_0} b_n w^n$ is noncongruence.

Some other distinctions between congruence and noncongruence subgroups are demonstrated in [5].

§ 3.2 Atkin and Swinnerton-Dyer congruence

Before we state the Atkin and Swinnerton-Dyer congruences conjecture, let us introduce a model of a modular curve over $\mathbb{Q}$.

Let $\mathbb{H}$ be the upper half plane $\{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$, and $\mathbb{H}^*$ denotes the compactified half plane $\mathbb{H} \cup \mathbf{P}^1(\mathbb{Q})$.

Definition 3.1. Let Γ be a subgroup of $SL_2(\mathbb{Z})$ of finite index. Consider the compactified quotient space $\Gamma \backslash \mathbb{H}^*$, and the canonical map

$$\Gamma \backslash \mathbb{H}^* \to \Gamma(1) \backslash \mathbb{H}^*.$$

We will say Γ **is defined over** $\mathbb{Q}$ if there exist

(1)a nonsingular projective curve $V/\mathbb{Q}$;

(2)a finite morphism $\pi: \ V \to \mathbf{P}^1_{\mathbb{Q}}$;

(3)a point $e \in V(\mathbb{Q})$; and

(4)an isomorphism $\phi : \Gamma\backslash\mathbb{H}^* \xrightarrow{\sim} V(C)$ such that $\phi(i\infty) = e$ and the diagram

$$\begin{array}{ccc} \Gamma\backslash\mathbb{H}^* & \longrightarrow & \Gamma(1)\backslash\mathbb{H}^* \\ \simeq \big\downarrow \phi & & \simeq \big\downarrow j \\ V(C) & \xrightarrow{\pi_C} & \mathbf{P}^1(C) \end{array}$$

commutes (where here j is the usual modular invariant of level 1).

As explained in [1][6][7], there exists a subfield L of K, an element $\kappa \in K$ with $\kappa^\mu \in L$, where μ is the width of the cusp ∞, and a positive integer M such that κ^μ is integral outside M and $\mathcal{S}_k(\Gamma)$ has a basis consisting of M-integral forms. Here a form f of Γ is called M**-integral** if in its Fourier expansion at the cusp ∞

$$f(\tau) = \sum_{n\geq 1} a_n(f) q^{n/mu},$$

the Fourier coefficients $a_n(f)$ can be written as $\kappa^n c_n(f)$ with $c_n(f)$ lying in the ring $\mathcal{O}_L[1/M]$, where $\mathcal{O}_L$ denotes the ring of integers of L.

Conjecture 3.2. *(Atkin and Swinnerton-Dyer congruences). Suppose that the modular curve X_Γ has a model over $\mathbb{Q}$ in the sense of Definition 3.1. There exist a positive integer M and a basis of $\mathcal{S}_k(\Gamma)$ consisting of M-integral forms f_j, $1 \leq j \leq d$, such that for each prime p not dividing M, there exists a nonsingular $d \times d$ matrix $(\lambda_{i,j})$ whose entries are in a finite extension of $\mathbb{Q}_p$, algebraic integers $A_p(j)$, $1 \leq j \leq d$, with $|\sigma(A_p(j))| \leq 2p^{(k-1)/2}$ for all embeddings σ ,and characters χ_j unramified outside M so that for each j the Fourier coefficients of $h_j \ := \ \sum_i \lambda_{i,j} f_i$ satisfy the congruence relation*

$$\mathrm{ord}_p(a_{np}(h_j) - A_p(j)a_n(h_j) + \chi_j(p)p^{k-1}a_{n/p}(h_j)) \geq (k-1)(1 + \mathrm{ord}_p n) \tag{3.2.1}$$

for all $n \geq 1$*; or equivalently, for all* $n \geq 1$*,*

$$(a_{np}(h_j) - A_p(j)a_n(h_j) + \chi_j(p)p^{k-1}a_{n/p}(h_j))/(np)^{k-1}$$

is integral at all places dividing p*.*

In other words, the recursive relation (3.0.1) on Fourier coefficients of modular forms for congruence subgroups is replaced by the congruence relation (3.2.1) for forms of noncongruence subgroups.

Theorem 3.3 (Scholl)**.** *Suppose that* X_Γ *has a model over* $\mathbb{Q}$ *as before. Attached to* $\mathcal{S}_k(\Gamma)$ *is a compatible family of* $2d$*-dimensional* l*-adic representations* ρ_l *of the Galois group* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *unramified outside* lM *such that for primes* $p > k+1$ *not dividing* Ml*, the following hold.*
(1) *The characteristic polynomial*

$$H_p(T) = \sum_{0 \leq r \leq 2d} B_r(p)T^{2d-r}$$

of $\rho_l(Frob_p)$ *lies in* $\mathbb{Z}[T]$ *and is independent of* l*, and its roots are algebraic integers with absolute value* $p^{(k-1)/2}$*;*
(2) *For any* M*-integral form* f *in* $\mathcal{S}_k(\Gamma)$*, its Fourier coefficients* $a_n(f)$*,* $n \geq 1$*, satisfy the congruence relation*

$$\mathrm{ord}_p(a_{np^d}(f) + B_1(p)a_{np^{d-1}}(f) + \ldots + B_{2d-1}(p)a_{n/p^{d-1}}(f) + B_{2d}(p)a_{n/p^d}(f)) \geq (k-1)(1 + \mathrm{ord}_p n)$$

for $n \geq 1$*.*

Remark 3.4. When $k = 2$, the $2d$-dimensional representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ can be presented explicitly by considering the Tate module of the Jacobian of X_Γ (See [9] for the definition of Tate module).

Definition 3.5. The two forms f and g above are said to satisfy the **Atkin and Swinnerton-Dyer congruence relations** if, for all primes p not dividing MN and for all $n \geq 1$,

$$(a_{np}(f) - b_p(g)a_n(f) + \chi(p)p^{k-1}a_{n/p}(f))/(np)^{k-1}$$

is integral at all places dividing p.

The following are two examples satisfy the Atkin and Swinnerton-Dyer congruence relations.

Example 3.6. For the noncongruence subgroup Γ_{711} studied in [1], the space $\mathcal{S}_4(\Gamma_{711})$ is 1-dimensional. Let f be a nonzero 14-integral form in $\mathcal{S}_4(\Gamma_{711})$. Scholl proved in [8] that there is a normalized newform g of weight 4 level 14 and trivial character such that f and g satisfy the Atkin and Swinnerton-Dyer congruence relations.

Example 3.7. An another example is demonstrated in [4]. Let Γ be the index 3 noncongruence subgroup of $\Gamma^1(5)$ such that the widths at two cusps ∞ and -2 are 15.

(1) Then X_Γ has a model over $\mathbb{Q}$, $\kappa = 1$, and the space $S_3(\Gamma)$ is 2-dimensional with a basis consisting of 3-integral forms

$$f_+(\tau) = q^{1/15} + iq^{2/15} - \frac{11}{3}q^{4/15} - i\frac{16}{3}q^{5/15} - \frac{4}{9}q^{7/15} + i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} + O(q^{11/15}),$$

$$f_-(\tau) = q^{1/15} - iq^{2/15} - \frac{11}{3}q^{4/15} + i\frac{16}{3}q^{5/15} - \frac{4}{9}q^{7/15} - i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} + O(q^{11/15}),$$

(2) The 4-dimensional l-adic representation ρ_l of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ associated to $S_3(\Gamma)$ constructed by Scholl is modular. More precisely, there are two cuspidal newforms of weight 3 level 27 and character χ_{-3} given by

$$g_+(\tau) = q - 3iq^2 - 5q^4 + 3iq^5 + 5q^7 + 3iq^8 + 9q^{10} + 15iq^{11} - 10q^{13} - 15iq^{14} - 11q^{16} - 18iq^{17} - 16q^{19} - 15iq^{20} + 45q^{22} + 12iq^{23} + O(q^{24}),$$

$$g_-(\tau) = q + 3iq^2 - 5q^4 - 3iq^5 + 5q^7 - 3iq^8 + 9q^{10} - 15iq^{11} - 10q^{13} + 15iq^{14} - 11q^{16} + 18iq^{17} - 16q^{19} + 15iq^{20} + 45q^{22} - 12iq^{23} + O(q^{24}),$$

such that over the extension by joining $\sqrt{-1}$, ρ_l decomposes into the direct sum of the two λ-adic representations attached to g_+ and g_-, where λ is a place of $\mathbb{Q}(i)$ dividing l.

(3) f_+ and g_+ (resp. f_- and g_-) satisfy the Atkin and Swinnerton-Dyer congruence relations.

4. Atkin and Swinnerton-Dyer congruences associated to Fermat curves

§ 4.1 Fermat curve

For a positive integer n, let F_n denote the **Fermat curve** $x^n + y^n = 1$ of degree n. There are some properties of Fermat curves.

Lemma 4.1. *For $n \geq 1$, the genus of F_n is $(n-1)(n-2)/2$, and for $n \geq 3$, a basis for the space of holomorphic 1-form is*

$$\omega_{i,j} = \frac{x^i dx}{y^{j+2}}, \quad 0 \leq i \leq j \leq n-3.$$

As shown in [10], we have following two lammas.

Lemma 4.2. *The Fermat curve F_n is the modular curve associated to the group Γ_n generated by*

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^n, \Gamma(2)^{'},$$

where $\Gamma(2)^{'}$ denotes the commutator subgroup of $\Gamma(2)$.

Moreover, let

$$\theta_2(\tau) = \sum_{n\in\mathbb{Z}} q^{(2n+1)^2/8}, \ \theta_3(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2/2}, \ \theta_4(\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2/2},$$

and $\lambda = \theta_2^4/\theta_3^4$. Then the Fermat curve $x^n + y^n = 1$ is parameterized by $(x, y) = (\sqrt[n]{1-\lambda}, \ \sqrt[n]{\lambda})$.

Lemma 4.3. *If $n \neq 1, 2, 4, 8$, then Γ_n is a noncongruence subgroup.*

Let $\zeta = e^{2\pi i/n}$ and μ_n be the group of nth root of unity. The group $G = \mu_n \times \mu_n$ acts on F_n by $(\zeta^i, \zeta^j) \, : \, (x, y) \mapsto (\zeta^i x, \zeta^j y)$. Let

$$\sigma \, : \, (x, y) \mapsto (\zeta x, y), \quad \tau \, : \, (x, y) \mapsto (x, \zeta y).$$

Assume that H is a subgroup of G. We consider the quotient curve F_n/H. The pullbacks of holomorphic 1-forms on F_n/H will be holomorphic 1-forms on F_n that are invariant under the action of H. Say, $\omega_{i,j} = x^i dx/y^{j+2}$ is invariant under the action of H. Using the parameterization given in Lemma 4.2, we get a cusp form

$$f_{i,j} = \frac{x^i q dx/dq}{y^{j+2}} = \sum_{k=1}^{\infty} a_k q^{k/2n}$$

on Γ_n. On the other hand, we may consider the L-function $L(s, F_n/H)$, i.e., the L-function of the Galois representation $\rho_{F_n/H}$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ attached to the algebraic curve F_n/H. (We assume for the moment that F_n/H is always defined over $\mathbb{Q}$ for all H and n).

§ 4.2 Case $x^6 + y^6 = 1$

Noticing that $\lambda = 16q^{1/2} + \cdots$, we slightly modify the Fermat curve and consider the curve

$$x^n + 16y^n = 1$$

instead(so that the cusp form $f_{i,j} = x^i q dx/y^{j+2} dq$ has rational Fourier coefficient). We shall still let F_n denote this curve. Also we let

$$\sigma : (x, y) \mapsto (\zeta x, y), \; \tau : (x, y) \mapsto (x, \zeta y),$$

where $\zeta = e^{2\pi i/n}$. Note that a differential form $x^i dx/y^{j+2}$ is fixed by $\sigma^a\tau^b$ if and only if

$$(i+1)a - (j+2)b \equiv 0 \mod 6.$$

The following table lists the subgroup $H_{i,j}$ of $G = \mu_6 \times \mu_6$ that fixes $\omega_{i,j}$.

$\omega_{0,0}$	$\omega_{0,1}$	$\omega_{1,1}$	$\omega_{0,2}$	$\omega_{1,2}$	$\omega_{2,2}$	$\omega_{0,3}$	$\omega_{1,3}$	$\omega_{2,3}$	$\omega_{3,3}$
$\langle\sigma^2\tau\rangle$	$\langle\sigma^3\tau\rangle$	$\langle\sigma^3\tau^2\rangle$	$\langle\sigma^4\tau\rangle$	$\langle\sigma^2\tau,\sigma^3\rangle$	$\langle\sigma^2\tau^3\rangle$	$\langle\sigma^5\tau\rangle$	$\langle\sigma^5\tau^2\rangle$	$\langle\sigma\tau^3\rangle$	$\langle\sigma\tau^2\rangle$

We now work out the equations for the curves $F_6/H_{i,j}$.

Lemma 4.4. *We have*

group	*differential forms*	*equation*
$\langle\sigma^2\tau\rangle$	$\omega_{0,0},\omega_{1,2}$	$v^2 = u^6 + 1$
$\langle\sigma^3\tau\rangle$	$\omega_{0,1}$	$v^2 = u^3 - 1$
$\langle\sigma^4\tau\rangle$	$\omega_{0,2}$	$v^2 = u^3 + 4$
$\langle\sigma^5\tau\rangle$	$\omega_{0,3},\omega_{1,2}$	$v^2 = u^6 - 1$
$\langle\sigma\tau^2\rangle$	$\omega_{1,2},\omega_{3,3}$	$v^2 = u^6 + 1$
$\langle\sigma^3\tau^2\rangle$	$\omega_{1,1}$	$v^2 = u^3 + 1$
$\langle\sigma^5\tau^2\rangle$	$\omega_{1,3}$	$v^2 = u^3 + 16$
$\langle\sigma^2\tau^3\rangle$	$\omega_{2,2}$	$v^2 = u^3 + 4$
$\langle\sigma\tau^3\rangle$	$\omega_{2,3}$	$v^2 = u^3 - 16$
$\langle\sigma^2\tau,\sigma^3\rangle$	$\omega_{1,2}$	$v^2 = u^3 + 1$

Proof. Here we prove the case $\langle\sigma^2\tau\rangle$. Consider both of xy^4 and y^6 are fixed by $\langle\sigma^2\tau\rangle$, and the mapping $(x,y) \mapsto (xy^4, y^6)$ is 6-to-1. Thus, xy^4 and y^6 generate the subfield of the function field of F_6 that is fixed by $\langle\sigma^2\tau\rangle$ and an equation for $F_6/\langle\sigma^2\tau\rangle$ is given by the relation

$$U^6 = V^4 - 16V^5$$

between $U = xy^4$ and $V = y^6$. Now the curve $U^6 = V^4 - 16V^5$ is birationally equivalent to $v^2 = u^6 + 1$ with the birational maps

$$u = \frac{2V}{U}, \quad v = \frac{V^2(8V-1)}{U^3}, \quad U = \frac{u^2}{4(u^3-v)}, \quad V = \frac{u^3}{8(u^3-v)}$$

This proves the case $\langle \sigma^2 \tau \rangle$. □

Remark 4.5. *We can compute the genus of F_6/H using the Riemann-Hurwitz formula. Taking $H = \langle \sigma^2 \tau \rangle$ for example. For the affine part of F_6, the covering $F_6 \to F_6/H$ is unramified at those points of F_6 where $P_j(\zeta^{2j}x, \zeta^j y)$, $j = 0, \dots, 5$ are 6 distinct points. If $y \neq 0$, then the six points are distinct. At those points, the covering is unramified. On the other hand, if $y = 0$, then $P_0 = P_3$, $P_1 = P_4$, $P_2 = P_5$. The covering is ramified at those points with ramification index 2. There are totally 6 such points $(\zeta^k, 0)$, $k = 0, \dots, 5$. Thus, the contribution from the affine part to the total branch number is 6. The infinity part of F_6 consist of 6 points $Q_j = (\zeta^{j+1/2} : 1 : 0)$ We have*

$$\sigma^2\tau(Q_j) = (\zeta^{j+5/2} : \zeta : 0) \sim (\zeta^{j+3/2} : 1 : 0) = Q_{j+1}$$

Therefore, the covering is unramified at the 6 infinity points, and the total branch number is 6. By the Riemann-Hurwitz formula, if g is the genus of $F_6/\langle \sigma^2 \tau \rangle$, then

$$10 - 1 = 6(g-1) + \frac{6}{2}.$$

Hence, we conclude that the genus of $F_6/\langle \sigma^2 \tau \rangle$ is 2 and the subspace of differential 1-forms on F_6 that are invariant under $\langle \sigma^2 \tau \rangle$ should have dimension 2.

Theorem 4.6. *The genus of F_n/H for a cyclic subgroup $H = \langle \sigma^a \tau^b \rangle$ of $\mu_n \times \mu_n$ with a, b are relative primes is*

$$g = \frac{n - d_a - d_b - d_{(a-b)}}{2} + 1$$

where d_x is the greatest common divisor of x and n.

Proof. By the Riemann-Hurwitz formula, we only need to verify the total branch number B is $n(d_a + d_b + d_{(a-b)} - 3)$.

For the affine part of F_n, the covering $F_n \to F_n/H$ is unramified at those point of F_n where $P_j = (\zeta^{aj}x, \zeta^{bj}y)$, $j = 0, \ldots, n-1$ are n distinct points. If $x \neq 0$ and $y \neq 0$, since a, b are relative primes, we know the n points are distinct. At those points, the covering is unramified. On the other hand, if $x = 0$, then $P_0 = P_{n/d_b} = \ldots = P_{(d_b-1)n/d_b}$, $P_1 = P_{n/d_b+1} = \ldots = P_{(d_b-1)n/d_b+1}$, …, $P_{n/d_b-1} = P_{n/d_b+n/d_b-1} = \ldots = P_{(d_b-1)n/d_b+n/d_b-1}$. The covering is ramified at those points with ramification index d_b. There are totally n such points. Similarly, we can determine the case $y = 0$. Thus, the contribution from the affine part to the total branch number is $n(d_a - 1) + n(d_b - 1)$. The infinity part of F_n consist of n points $Q_j = (\zeta^{j+1/2} : 1 : 0)$ We have

$$\sigma^a \tau^b (Q_j) = (\zeta^{j+a+1/2} : \zeta^b : 0) \sim (\zeta^{j+(a-b)+1/2} : 1 : 0) = Q_{j+(a-b)}$$

Replaces $a - b$ by $a - b \mod n$ if necessary. Therefore, the ramification index of the covering is $d_{(a-b)}$, and the total branch number of the infinity part is $n(d_{a-b} - 1)$. Sum up the total branch numbers of the affine part and the infinity part, we have $B = n(d_a + d_b + d_{(a-b)} - 3)$. □

Lemma 4.7. *The L-functions for the curves in Lemma 4.4 are*

equation	*L-function*
$v^2 = u^3 + 16$	$L(s, f_{27})$
$v^2 = u^3 + 1$	$L(s, f_{36})$
$v^2 = u^3 + 4$	$L(s, f_{108})$
$v^2 = u^3 - 1$	$L(s, f_{36} \otimes \chi_{-4})$
$v^2 = u^3 - 16$	$L(s, f_{27} \otimes \chi_{-4})$
$v^2 = u^6 + 1$	$L(s, f_{36})^2$
$v^2 = u^6 - 1$	$L(s, f_{36})L(s, f_{36} \otimes \chi_{-4})$

Here

$$f_{27}(\tau) = \eta(3\tau)^2\eta(9\tau)^2, \qquad f_{36}(\tau) = \eta(6\tau)^4$$

Remark 4.8. *The modular forms f_{27}, f_{36}, f_{108} have the following description in terms of Hecke characters.*

Let $K = \mathbb{Q}(\sqrt{-3})$ and $\zeta = e^{2\pi i/6}$. The ring of integers $\mathcal{O}_K$ is $\mathbb{Z} + \mathbb{Z}\zeta$. Let $m = 3$ and define χ as follows. If $a + b\zeta \in \mathcal{O}_K$ is not relatively prime to 3, we let $\chi(a + b\zeta) = 0$. For each $a + b\zeta$ in $\mathcal{O}_K$ relatively prime to m, there exists a unique integer j with $0 \le j < 6$ such that $a + b\zeta \equiv \zeta^j \mod m$. We set $\chi(a + b\zeta) = \zeta^{-j}(a + b\zeta)$. That is,

$(a,b) \mod 3$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,2)$	$(2,0)$	$(2,1)$
$\chi(a+b\zeta)/(a+b\zeta)$	ζ^5	ζ^2	1	ζ	-1	ζ^4

Then

$$f_{27}(\tau) = \frac{1}{6} \sum_{a+b\zeta \in \mathcal{O}_K} \chi(a + b\zeta) q^{a^2+ab+b^2}.$$

For f_{36}, we let $m = 2\sqrt{-3}$ and define χ as follows. If $a + b\zeta \in \mathcal{O}_K$ is not relatively prime to m, we set $\chi(a + b\zeta) = 0$. For each $a + b\zeta$ in $\mathcal{O}_K$ that is relatively prime to $2\sqrt{-3}$, there exists a unique integer j with $0 \le j < 6$ such that $a + b\zeta \equiv \zeta^j \mod m$. We set $\chi(a + b\zeta) = \zeta^{-j}(a + b\zeta)$ Then

$$f_{36}(\tau) = \frac{1}{6} \sum_{a+b\zeta \in \mathcal{O}_K} \chi(a + b\zeta) q^{a^2+ab+b^2}.$$

Proof. The only parts that requires a proof are $v^2 = u^6 + 1$ and $v^2 = u^6 - 1$. Here we consider the case $v^2 = u^6 - 1$. Let $x = u^2$ and $y = v$. Then we have $v^2 = u^3 - 1$. In other words, we have a two-fold cover from $v^2 = u^6 - 1$ to $y^2 = x^3 - 1$. Likewise, let $x = -1/u^2$ and $y = v/u^3$. We have $y^2 = x^3 + 1$. Then $L(s, v^2 - u^6 + 1) = L(s, f_{36})L(s, f_{36} \otimes \chi_{-4})$. □

Theorem 4.9. *The cusp forms $f_{i,j} = x^i y^{-j-2} q dx/dq$ satisfy the ASD congruences with the following L-function.*

$f_{i,j}$	*L-function*
$f_{0,0}$	$L(s, f_{36})$
$f_{0,1}$	$L(s, f_{36} \otimes \chi_{-4})$
$f_{1,1}$	$L(s, f_{36})$
$f_{0,2}$	$L(s, f_{108})$
$f_{1,2}$	$L(s, f_{36})$
$f_{2,2}$	$L(s, f_{108})$
$f_{0,3}$	$L(s, f_{36} \otimes \chi_{-4})$
$f_{1,3}$	$L(s, f_{27})$
$f_{2,3}$	$L(s, f_{27} \otimes \chi_{-4})$
$f_{3,3}$	$L(s, f_{36})$

In fact, we find

$$f_{0,0}(\tau) = f_{36}(2\tau/3), \qquad f_{1,2}(\tau) = f_{36}(\tau/3),$$

$$f_{3,3}(\tau) = f_{36}(\tau/6), \qquad f_{0,3}(\tau) = f_{36} \otimes \chi_{-4}(\tau/6).$$

Also,

$$f_{0,1}(2\tau) = q + \frac{4}{3}q^3 - \frac{10}{9}q^5 - \frac{40}{81}q^7 - \frac{553}{243}q^9 - \frac{3740}{729}q^{11} + \cdots,$$

$$f_{1,1}(2\tau) = q - \frac{4}{3}q^3 - \frac{10}{9}q^5 + \frac{40}{81}q^7 - \frac{553}{243}q^9 + \frac{3740}{729}q^{11} + \cdots,$$

$$f_{0,2}(3\tau) = q + \frac{8}{3}q^4 - \frac{4}{9}q^7 - \frac{320}{81}q^{10} - \frac{154}{243}q^{13} - \frac{3328}{729}q^{16} + \cdots,$$

$$f_{2,2}(3\tau) = q - \frac{8}{3}q^4 - \frac{4}{9}q^7 + \frac{320}{81}q^{10} - \frac{154}{243}q^{13} + \frac{3328}{729}q^{16} + \cdots,$$

$$f_{1,3}(6\tau) = q + \frac{4}{3}q^7 - \frac{46}{9}q^{13} - \frac{472}{81}q^{19} + \frac{1985}{243}q^{25} + \frac{3532}{729}q^{31} + \cdots,$$

$$f_{2,3}(6\tau) = q - \frac{4}{3}q^7 - \frac{46}{9}q^{13} + \frac{472}{81}q^{19} + \frac{1985}{243}q^{25} - \frac{3532}{729}q^{31} + \cdots.$$

5. References

[1] A.O.L. Atkin, H.P.F. Swinnerton-Dyer, *Modular forms On non-congruence subgroups*, Combinatorics (Proceedings of the Symposium on Pure Mathematics, Vol. XIX, University of California, Los Angeles, CA, 1968), American Mathematical Society, Providence, RI, 1971, pp. 1-25.

[2] F. Diamond J. Shurman, *A First Course in Modular Forms*, Springer, 2005.

[3] K.-I Hashimoto, L. Long, Y. Yang, *Jacobsthal identity for* $\mathbb{Q}(\sqrt{2})$, Forum Mathematicum, doi:10.1515/FORM.2011.102.

[4] W.-C. W. Li, L. Long, Z. Yang, *On Atkin-Swinnerton-Dyer congruence relations*, J. Number Theory 113 (2005), no. 1, 117-148.

[5] L. Long, *The finite index subgroups of the modular group and their modular forms,Fields institute Communications*, American Mathematical Society Volume 54 (2008), pp 83-102.

[6] A.J. Scholl, *Modular forms and de Rham cohomology; AtkinVSwinnerton-Dyer congruences*, Invent. Math. 79 (1985) 49-77.

[7] A.J. Scholl, *Modular forms on noncongruence subgroups. Séminaire de Théorie des Nombres*, Paris 1985-86, Progress in Mathematics, Vol. 71, Birkhäuser, Boston, MA, 1987, pp. 199-206.

[8] A.J. Scholl, *The l-adic representations attached to a certain non-congruence subgroup*, J. Reine Angew. Math. 392 (1988) 1-15.

[9] J.H. Silverman, *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[10] T. Yang, *Cusp form of weight* 1 *associated to Fermat curves*, Duke Math J. 83 (1996), 141-156.