國立臺灣大學理學院數學研究所

碩士論文

Department of Mathematics

College of Science

National Taiwan University

Master Thesis

卡塔蘭猜想的證明之探討

A Survey of the Proof of Catalan’s Conjecture

賴昱帆

Yu-Fan Lai

指導教授：陳其誠 教授

Advisor: Professor Ki-Seng Tan

中華民國 100 年 7 月

July, 2011

誌 謝

首先，我要感謝我的指導教授陳其誠老師，在這兩年間給了我諸多幫助。陳其誠教授不僅指引我研究的方向，也在我寫論文的過程中給予許多寶貴的意見，也花了許多時間指點我以及幫忙修改。

也非常感謝應邀參與口試的余正道教授以及謝銘倫教授。兩位教授指出此篇論文的缺陷之處，並且給予修改的意見，使我能將此篇論文寫得更為完整。

除此之外，我也要感謝在這過程中鼓勵我與幫助我的同學以及學弟們。其中特別感謝同學鴻仁、昱丞、守正、育齡、任宏、晉宏給了我許多想法和鼓勵，以及在我準備口試時給我的幫助。

最後我也要感謝長久以來支持我的家人。

中文摘要

Catalan’s Conjecture 的敘述是，唯一連續的完全次方數正整數數對是 8 和 9 這一組。換言之，Catalan’s equation，即 $x^p - y^q = 1$， 的唯一正整數解是(3,2,2,3)。這個定理在 1844 年作為猜想被提出，並且在 2002 年被證明。這篇論文沿用了在 J. Daems 所寫的「Cyclotomic Proof of Catalan’s Conjecture」中所使用的各種方法，去重新描述這個定理的部分證明。

整個定理的證明依據 Catalan’s equation 中的兩個指數的各種情況，共分成四部分。這篇論文主要是著重於有利用到 cyclotomic field 相關的理論去進行證明的部分。

Abstract

Catalan’s Conjecture says that the only pair of consecutive powers of positive integers is 8 and 9. Namely, the Clatalan’s equation

$$x^p - y^q = 1$$

has (x, y, p, q) = (3, 2, 2, 3) as its only positive integer solution. This is a theorem in number theory that was proposed by Eugène Charles Catalan in 1844 as a conjecture, and proven in 2002 by Preda Mihăilescu. Following the treatment in the article by J. Daems, this thesis gives partial proof of Catalan’s Conjecture.

The all proof contains four parts, classified according to the two exponents in Catalan’s equation. This thesis focuses on the cases in which the handling contains cyclotomic field theory.

Contents

1. Introduction

A complete proof of Catalan's conjecture was first given by P. Mihăilescu [3]. Following that, several articles have been written with the intention to explain and to modify the original proof. One of them was by J. Daems [2] which I choose as a reading material of a research project on cyclotomic fields. Soon, I was very much attracted by its own style of beauty and simplicity, thus determined to understand it in every detail. This thesis is basically a report on my study.

Recall that Catalan's conjecture says that the only pair of consecutive powers of positive integers is 8 and 9. Obviously, this is actually equivalent to a weaker statement which only involves prime powers. Namely, after Mihăilescu, we have the following theorem:

Theorem 1.1. *The Catalan's equation*

$$x^p - y^q = 1,$$

where p and q are prime numbers, has no positive integer solution except for the case $3^2 - 2^3 = 1$.

The proof of this theorem can be divided into parts corresponding to the following (mutual exclusive) cases:

Case 1: p or q is even.
Case 2: $p, q > 2$ and at least one of them equals 3 or 5.
Case 3: p, $q \geq 7$, $q < p$ and $q \mid (p-1)$ (resp. $p < q$ and $p \mid (q-1)$).
Case 4: p, $q \geq 7$, $q < p$ and $q \nmid (p-1)$ (resp. $p < q$ and $p \nmid (q-1)$).

The proof of the first case is given by L. A. Lebesque (for $q = 2$ [8]) and K. Chao (for $p = 2$ [9]). A nice treatment of this part can be found in [5]. Basically, it is shown by elementary discussion, except for the $p = 2$ and $q = 3$ case which uses the following result on elliptic curves.

Theorem 1.2. *Let E be the elliptic curve defined by the equation*

$$y^2 = x^3 + 1,$$

and let $E(\mathbb{Q})$ denote the group formed by $\mathbb{Q}$-rational points on E. Then

$$E(\mathbb{Q}) = \{(0,1), (0,-1), (2,3), (2,-3), (-1,0)\} \cup \{\infty\},$$

where ∞ is the identity element of the group.

This theorem is a result which comes from the work involving the use of Descent Theorem, Mordell's Theorem and Nagell-Lutz Theorem (for proof of these, see chapter 2 and 3 of [6]). The other detail of the proof of Theorem 1.2 is omitted in this thesis. For a rigorous proof, see page 13 to 16 in [2].

The proofs of the remaining three cases are of quite different nature, they all apply the arithmetic of the cyclotomic field. The proof of Case 2 actually uses the computation of the relative class number, while those of Case 3 and Case 4 use the results on the Stickelberger ideal, the estimation of the absolute norms, as well as a theorem of Cassels that gives information on the cyclotomic unit group. In this thesis, we shall discuss these three cases and show that the Catalan's equation indeed has no nonzero-integer solutions. Note that if $x^p - y^q = 1$, then $(-y)^q - (-x)^p = 1$, and hence without loss of generality, we can assume that $p > q$.

This thesis is organized in the following way that in Chapter 2, we summarize general results on cyclotomic fields which will be further elaborated, in Chapter 3, we proceed the proof by giving a detailed outline, while leaving some key lemmas to Chapter 4.

Finally, we shall emphasize that there is essentially nothing original in this thesis, which should be considered as only a modification of Daems [2].

2. Notations and Basic Materials

In this section, we first set notations and then establish key results for latter application.

2.1. Notations.

Through out, we shall fix odd prime numbers p and q. Except in section, 3.1, we also assume that $p > q$ and let ζ denote a fixed pth root of unity by ζ. Write $K = \mathbb{Q}(\zeta)$, $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$, which is the maximal real subfield of K, and $G = \mathrm{Gal}(K/\mathbb{Q})$, $G^+ = \mathrm{Gal}(K^+/\mathbb{Q})$. Also, let $\mathcal{O}_K$ and $\mathcal{O}_{K^+}$ respectively denote the integral closures of $\mathbb{Z}$ in K and K^+.

Moreover, we fix another prime number q and define the following:

- Let σ_a denote the automorphism in G that sends ζ to ζ^a and let $\iota = \sigma_{-1}$.
- Let $\mathfrak{p}$ denote the ideal $(2 - (\zeta + \zeta^{-1})) = ((1-\zeta)(1-\zeta^{-1}))$ in $\mathcal{O}_{K^+}$.
- Let $H = \{\alpha \in \mathbb{Q}(\zeta + \zeta^{-1})^* : \mathrm{ord}_I(\alpha) \equiv 0 \pmod q,\ \text{for all prime ideal } I \neq \mathfrak{p}\}$.
- Let $\mathcal{E} = \{\alpha \in \mathbb{Q}(\zeta + \zeta^{-1})^* : \mathrm{ord}_I(\alpha) = 0,\ \text{for all prime ideal } I \neq \mathfrak{p}\}$.
- Let V denote the multiplicative group generated by the set $\{\pm\zeta, 1 - \zeta^a : a = 2, 3, ..., p-1\}$.
- Let C denote the group of cyclotomic units of K, i.e. $C = \mathcal{O}_K^* \cap V$.
- Let C^+ denote the group of cyclotomic units of K^+, i.e. $C^+ = \mathcal{O}_{K^+}^* \cap V$.
- We call the element $\theta_S = \sum\limits_{a=1}^{p-1} \frac{a}{p}\sigma_a^{-1}$ in $\mathbb{Q}[G]$ the Stickelberger element.
- Let I_S denote the Stickelberger ideal $\mathbb{Z}[G] \cap \theta_S\mathbb{Z}[G]$.
- Let I_S^- denote the minus part of Stickelberger ideal $(1-\iota)I_S$.
- For a commutative ring A and group H, let
$$w : A[\mathsf{H}] \longrightarrow A$$
$$\sum_{h\in H} a_h h \longmapsto \sum_{h\in H} a_h$$
denote the weight function on the group ring $A[\mathsf{H}]$.
- Let I_0 denote the kernel of weight function on $F_q[G^+]$.

2.2. Cassels' Theorem.

We first recall a theorem of Cassels:

Proposition 2.1. *Let x and y be nonzero integers satisfying the Catalan's equation $x^p - y^q = 1$. Then $p \mid y$ and $q \mid x$. Furthermore, we have $x - 1 = p^{q-1}a^q$ and $\frac{x^p-1}{x-1} = pu^q$ for some integers a, u such that* (1) *$p \nmid u$,* (2) *$gcd(a,u) = 1$, and* (3) *$y = pau$. Similarly, we have $y + 1 = q^{p-1}b^p$ and $\frac{y^q+1}{y+1} = qv^p$ for some integers b, v such that* (4) *$q \nmid v$,* (5) *$gcd(b,v) = 1$, and* (6) *$x = qbv$.*

Proof. First, observe that $\gcd(\frac{y^q+1}{y+1}, y+1) = 1$ or q, for we have $\frac{y^q+1}{y+1} = \sum\limits_{i=0}^{q-1} y^i(-1)^{q-1-i}$, which is congruent to q modulo $y+1$. Similar argument also implies that $\gcd(\frac{x^p-1}{x-1}, x-1) = 1$ or p.

Then we claim that the following two inequalities hold, for $\alpha = \frac{p}{q} > 1$:

(A) $f(t) := (t^\alpha - 1)^{\frac{1}{\alpha}} - t + 1 > 0$, for $t > 1$;

(B) $g(t) := (t^\alpha + 1)^{\frac{1}{\alpha}} - t - 1 < 0$, for $t > 0$.

By applying $t = c^q$ and $t = (-c)^q$ respectively to (A) and (B), we conclude that

$$(c^q - 1)^p - (c^p - 1)^q < 0, \text{ for all non-zero } c \in \mathbb{Z}$$

except for the case $c = 1$, which leads to $y = 0$. Suppose that $\gcd(\frac{y^q+1}{y+1}, y+1) = 1$. Since $x^p = \frac{y^q+1}{y+1} \cdot (y+1)$, we must have $y + 1 = c^p$ for some non-zero integers c. It follows that $x^p - (c^p - 1)^q = 1$. Since the value of $h(t) := t^p - (c^p - 1)^q$ strictly increases with t, we must have $x > c^q - 1$. On the other hand, the value of $h(c^q) = c^{pq} - (c^p - 1)^q$ is greater than 1. This would imply that $c^q - 1 < x < c^q$, a contradiction to the fact $x \in \mathbb{Z}$. Therefore, we must have $\gcd(\frac{y^q+1}{y+1}, y+1) = q$ and $q \mid x$.

Write $y = -1 + q^r \cdot z$, with $q \nmid z$. Then we have $y^q = -1 + q^{r+1} \cdot w$, $q \nmid w$. As $y^q + 1 = x^p$ is divisible by q^p, we must have $q \| \frac{y^q+1}{y+1}$ as well as the conditions (4), (5) and (6).

To prove the claim, we just argue that $f(1) = 0$ and the derivative

$$f'(t) = \left(\frac{t^\alpha}{t^\alpha - 1}\right)^{\frac{\alpha-1}{\alpha}} - 1 > 0, \text{ for } t > 1;$$

as well as $g(0) = 0$ and

$$g'(t) = \left(\frac{t^\alpha}{t^\alpha + 1}\right)^{\frac{\alpha-1}{\alpha}} - 1 < 0, \text{ for } t > 0.$$

It is much more difficult to show that $\gcd(x - 1, \frac{x^p-1}{x-1}) = p$ (theorem 6.4 of [5]). However, once it is proved. A similar argument can be applied to show that (1), (2) and (3) hold.

□

An immediate consequence of the proposition is in order.

Lemma 2.1. *Under the assumption of* Proposition 2.1, *the element* $\frac{x-\zeta}{1-\zeta} \in \mathcal{O}_K$ *and there exists an* $\mathcal{O}_K$*-ideal* $\mathfrak{a}$ *so that the principal ideal*

$$\left(\frac{x-\zeta}{1-\zeta}\right) = \mathfrak{a}^q.$$

Proof. In $\mathcal{O}_K$, $p = (1-\zeta)^{p-1} \cdot \mu$, for some $\mu \in \mathcal{O}_K^*$. By Proposition 2.1, $x - 1$ is divisible by p and hence $x - \zeta = x - 1 + 1 - \zeta$ is divisible by $1 - \zeta$ but not divisible by $(1-\zeta)^2$. In particular, the first statement of the lemma is proved.

Next, we claim that $(\frac{x-\zeta}{1-\zeta})^\sigma$ and $(\frac{x-\zeta}{1-\zeta})^\tau$ are coprime for all pairs of distinct σ and τ in G. Indeed, the gcd of $\frac{x-\zeta^\sigma}{1-\zeta^\sigma}$ and $\frac{x-\zeta^\tau}{1-\zeta^\tau}$ must divide $(1-\zeta)$, as we have

$$(1-\zeta^\sigma)\frac{x-\zeta^\sigma}{1-\zeta^\sigma} - (1-\zeta^\tau)\frac{x-\zeta^\tau}{1-\zeta^\tau} = \zeta^\sigma - \zeta^\tau = \zeta^\sigma(1-\zeta^{\tau-\sigma}).$$

On the other hand, neither $\frac{x-\zeta^\sigma}{1-\zeta^\sigma}$ nor $\frac{x-\zeta^\tau}{1-\zeta^\tau}$ is divisible by $(1-\zeta)$ as we have seen that $x - \zeta$ is not divisible by $(1-\zeta)^2$.

To complete the proof, observe that

$$\prod_{\sigma\in G} \frac{x-\zeta^\sigma}{1-\zeta^\sigma} = \frac{1}{p}\prod_{\sigma\in G}(x-\zeta^\sigma) = \frac{x^p-1}{p(x-1)} = u^q$$

for some integer u, by Proposition 2.1. In view of the claim, we see that each factor $(\frac{x-\zeta^{\sigma}}{1-\zeta^{\sigma}})$ is a qth power. □

2.3. **Stickelberger Ideals.** In this section, we explicitly give a set of generators of the Stickelberger ideal I_S. As usual, for a real number x, let the Gauss symbol $[x]$ denote the integral part of x. For an integer c coprime to p, denote

$$\theta_c := (c - \sigma_c)\theta_S.$$

Proposition 2.2. *For an integer c with $gcd(c, p) = 1$, the equality*

$$\sum_{a=1}^{p-1} \left[\frac{ca}{p}\right] \sigma_a^{-1} = \theta_c$$

holds. Furthermore, the set

$$\{\theta_c \mid c \text{ is coprime to } p\}$$

generates the Stickelberger ideal I_S.

Proof. We have $c \cdot \theta_S = \sum_{a=1}^{p-1} \frac{ca}{p}\sigma_a^{-1}$, while $\sigma_c \cdot \theta_S = \sum_{a=1}^{p-1} \frac{j_a}{p}\sigma_a^{-1}$ with $1 \leq j_a \leq p-1$ so that $j_a \equiv c \cdot a \pmod{p}$, for each a. Thus, $\frac{j_a}{p}$ is just the fractional part of $\frac{ca}{p}$, and the first statement is proved. In particular, $\theta_c \in \mathbb{Z}[G]$, and hence $\theta_c \in I_S = \mathbb{Z}[G] \cap \ \theta_S Z[G]$.

To complete the proof we need to show that if $\xi = \left(\sum\limits_{a=1}^{p-1} z_a\sigma_a\right)\theta_S \in \mathbb{Z}[G]$, with $z_a \in \mathbb{Z}$, for each a, then ξ can be written as $\sum_c \alpha_c \cdot \theta_c$, with each $\alpha_c \in \mathbb{Z}[G]$. Observe that

$$\begin{aligned}\left(\sum_{a=1}^{p-1} z_a\sigma_a\right)\theta_S &= \left(\sum_{a=1}^{p-1} z_a\sigma_a\right)\left(\sum_{a=1}^{p-1} \frac{a}{p}\sigma_a^{-1}\right)\\ &= \sum_{a=1}^{p-1}\sum_{c=1}^{p-1} z_a\frac{c}{p}\sigma_a\sigma_c^{-1}.\end{aligned}$$

In particular, the coefficient of the term $\sigma_a\sigma_{a^{-1}} = \sigma_1$ is

$$\beta := \sum_{a=1}^{p-1} z_a\frac{a}{p} = \frac{1}{p}\sum_{a=1}^{p-1} z_a a.$$

The assumption that $\left(\sum\limits_{a=1}^{p-1} z_a\sigma_a\right)\theta_S$ belongs to $\mathbb{Z}[G]$ implies $\beta \in \mathbb{Z}$. By writing

$$p = p + \sigma_1 - \sigma_1 = (p+1) - \sigma_{p+1}$$

and

$$\sum_{a=1}^{p-1} z_a\sigma_a = \sum_{a=1}^{p-1} z_a a + \sum_{a=1}^{p-1} z_a(\sigma_a - a) = -\beta(\sigma_{p+1} - (p+1)) + \sum_{a=1}^{p-1} z_a(\sigma_a - a),$$

we can express ξ as the sum $-\beta\theta_{p+1} - \sum\limits_{a=1}^{p-1} z_a\theta_a$.

□

2.4. **Mihăilescu's Lemma.** Next, we introduce a lemma that plays an important role in the proof of Case 4.

Lemma 2.2 (Mihăilescu)**.** *Let x and y be non-zero integers satisfying the Catalan's equation $x^p - y^q = 1$. Then for any $\theta \in I_S^-$, the element $(x-\zeta)^\theta$ is a qth power in K. Furthermore, we have $q^2 \mid x$.*

Proof. Let $\mathbb{Z}_{(\mathfrak{q})}$ denote the localization of $\mathbb{Z}$ at the prime ideal (q) and let $\mathcal{O}_{(\mathfrak{q})}$ denote the integral closure of $\mathbb{Z}_{(\mathfrak{q})}$ in $\mathcal{O}_K$.

Let $\theta = (1-\iota)\theta' \in I_S^-$, for some $\theta' \in I_S$. By Lemma 2.1, the ideal $\left(\frac{x-\zeta}{1-\zeta}\right) = \mathfrak{a}^q$, for some $\mathfrak{a} \subset \mathcal{O}_K$. On the other hand, Stickelberger's theorem says that $\mathfrak{a}^{\theta'}$ is principal in $\mathcal{O}_K$. Thus we can write $\mathfrak{a}^{\theta'} = (\alpha)$, for some $\alpha \in \mathcal{O}_K$, and consequently, $\left(\frac{x-\zeta}{1-\zeta}\right)^{\theta'} = \eta_0\alpha^q$, for some $\mathcal{O}_K$-unit η_0.

Note that, for each a, $(1-\zeta)^{\sigma_a^{-1}} = \mu_a \cdot (1-\zeta)$, for some unit $\mu_a \in \mathcal{O}_K^*$, and hence $(1-\zeta)^{\theta'} = \eta_1 \cdot (1-\zeta)^l$, for some $l \in \mathbb{Z}$ and $\eta_1 \in \mathcal{O}_K^*$. Therefore, we can write

$$\begin{aligned}(x-\zeta)^\theta &= \left(\left(\frac{x-\zeta}{1-\zeta}\right)(1-\zeta)\right)^{(1-\iota)\theta'} \\ &= (\eta_0\eta_1\alpha^q(1-\zeta)^l)^{(1-\iota)} \\ &= \frac{\eta_0\eta_1}{\bar{\eta}_0\bar{\eta}_1}\frac{\alpha^q}{\bar{\alpha}^q}\left(\frac{1-\zeta}{1-\bar{\zeta}}\right)^l.\end{aligned}$$

Obviously, $\frac{1-\zeta}{1-\bar{\zeta}} = -\bar{\zeta}$, which is a $2p$-th root of unity and hence a qth power in K. Also, as $\frac{\eta_0\eta_1}{\bar{\eta}_0\bar{\eta}_1}$ is a unit of $\mathcal{O}_K$ with absolute value 1 at every archimedean place, it is a pth root of unity and is a qth power, too. This shows that $(x-\zeta)^\theta$ is a qth power in K.

The element $(1-x\bar{\zeta})^\theta = (-\bar{\zeta})^\theta(x-\zeta)^\theta$ is also a qth power in K. Furthermore, as x is divisible by q (Proposition 2.1), $1-x\bar{\zeta}$ is a unit of $\mathcal{O}_{(\mathfrak{q})}$ and so is $(1-x\bar{\zeta})^\theta$. Therefore, $(1-x\bar{\zeta})^\theta = f^q$ for some $f \in \mathcal{O}_{(\mathfrak{q})}$.

To continue the proof, we note that as q is unramified in K (see [1]),

$$(q) = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_r,$$

where $\mathfrak{q}_i$, $i = 1, \ldots, r$, are distinct prime ideals in $\mathcal{O}_{(\mathfrak{q})}$, and hence, by Chinese Remainder Theorem,

$$\mathcal{O}_{(\mathfrak{q})}/(q) \cong \mathcal{O}_{(\mathfrak{q})}/\mathfrak{q}_1 \times \mathcal{O}_{(\mathfrak{q})}/\mathfrak{q}_2 \times \cdots \times \mathcal{O}_{(\mathfrak{q})}/\mathfrak{q}_r.$$

In particular, the quotient $\mathcal{O}_{(\mathfrak{q})}/(q)$ contains no non-zero nilpotent element. This together with the following congruence (note that $q \mid x$):

$$(f-1)^q \equiv f^q - 1 \equiv (1-\bar{\zeta}x)^{\theta'} - 1 \equiv 0 \pmod{q},$$

implies that $f = 1 + kq$ for some element $k \in \mathcal{O}_{(\mathfrak{q})}$. Then we obtain the equality

$$(1-\bar{\zeta}x)^\theta = f^q = 1 + kq^2 + \frac{kq^2(q-1)}{2} + \cdots \equiv 1 \pmod{q^2}.$$

On the other hand, if $\theta = \sum\limits_{\sigma \in G} n_\sigma \sigma$, then

$$\begin{aligned}(1-\bar{\zeta})^\theta x &= \prod_{\sigma \in G} \sigma(1-\bar{\zeta}x)^{n_\sigma} \\ &\equiv \prod_{\sigma \in G} (1 - n_\sigma \sigma(\bar{\zeta})x) \pmod{q^2} \\ &\equiv 1 - x \sum_{\sigma \in G} n_\sigma \sigma(\bar{\zeta}) \pmod{q^2},\end{aligned}$$

and hence q^2 divides $x \sum\limits_{\sigma \in G} n_\sigma \sigma(\bar{\zeta})$.

If $q^2 \nmid x$, then q divides $\sum\limits_{\sigma \in G} n_\sigma \sigma(\bar{\zeta})$. Therefore, each n_σ is divisible by q. From this, we can easily deduce a contradiction by choosing

$$\theta = (1-\iota)(2-\sigma_2)\theta_S = -\sum_{a=1}^{\frac{p-1}{2}} \sigma_a^{-1} + \sum_{a=\frac{p+1}{2}}^{p-1} \sigma_a^{-1},$$

which is indeed contained in I_S^- (Proposition 2.2).

□

2.5. **The Class Group and the Group of Cyclotomic Units.** We close this chapter with some results on the structure of $\mathcal{E}/\mathcal{E}^q$, $H/(K^+)^{*q}$ and $Cl_{K^+}[q]$, viewed as $\mathbb{F}_q[G^+]$-modules. To do so, we shall assume that

$$q \nmid p-1,$$

as the results will be only used for dealing with Case 4.

Let $\bar{\sigma}_a$ denote the image of σ_a, under the natural map (the restriction of Galois action): $G \longrightarrow G^+$. Since $G^+ =< \bar{\sigma}_2 >$ is cyclic of order $(p-1)/2$, the homomorphism

$$\mathbb{F}_q[G^+] \longrightarrow \mathbb{F}_q[x]/(x^{\frac{p-1}{2}} - 1),$$

sending $\bar{\sigma}_2^i$ to (the residue class of) x^i is an isomorphism. Also, as the derivative $(x^{\frac{p-1}{2}} - 1)' = \frac{p-1}{2} x^{\frac{p-3}{2}}$ is relatively prime to $x^{\frac{p-1}{2}} - 1$, the algebra $\mathbb{F}_q[G^+]$ is separable. In this sense if

$$x^{\frac{p-1}{2}} - 1 = \prod_{k=1}^{r} g_k(x),$$

is the factorization into product of irreducible polynomials over $\mathbb{F}_q[x]$, then (Chinese Remainder Theorem)

$$\mathbb{F}_q[G^+] \cong \mathbb{F}_q[x]/(x^{\frac{p-1}{2}} - 1) \cong \prod_{k=1}^{r} \mathbb{F}_q[x]/(g_k(x)),$$

where the right-hand side is a finite product of finite fields.

Recall that $\mathcal{E}$ is included in H and $\mathcal{E}^q$ is included in $(K^+)^{*q}$. Thus, we have a natural homomorphism

$$\psi : \mathcal{E}/\mathcal{E}^q \longrightarrow H/(K^+)^{*q},$$

which obviously is a monomorphism.

The principal ideal generated by each element $\alpha \in H$ can be expressed as $(\alpha) = \mathfrak{p}^k \mathfrak{a}^q$, where $\mathfrak{a}$ is relatively prime to the prime ideal $\mathfrak{p}$. Let $[\mathfrak{a}] \in Cl_{K^+}$ denote the ideal class of $\mathfrak{a}$. As $\mathfrak{p}$ is actually principal, $\mathfrak{a}^q = (\alpha) \cdot \mathfrak{p}^{-k}$ is also principal, and hence $[\mathfrak{a}] \in Cl_{K^+}[q]$. It is easy to see that the assignment $\alpha \mapsto [\mathfrak{a}]$ induces a homomorphism

$$\psi' : H/(K^+)^{*q} \longrightarrow Cl_{K^+}[q].$$

Obviously, ψ and ψ' are both homomorphisms of $\mathbb{F}_q[G^+]$-modules. We claim that the induced

$$1 \longrightarrow \mathcal{E}/\mathcal{E}^q \xrightarrow{\psi} H/(K^+)^{*q} \xrightarrow{\psi'} Cl_{K^+}[q] \longrightarrow 1. \tag{1}$$

is an exact sequence. That ψ' is an $\mathbb{F}_q[G^+]$-epimorphism is quite obvious, since if $[\mathfrak{a}] \in Cl_{K^+}[q]$, then $\mathfrak{a}^q$ is a principal ideal, say, generated by some α that must be contained in H, and hence $\psi'(\alpha \pmod{(K^+)^{*q}}) = [\mathfrak{a}]$. On the other hand, if α is an element in H such that $\alpha \pmod{(K^+)^{*q}}$ is in the kernel of ψ', then the ideal (α) equals to $\mathfrak{p}^k \mathfrak{b}^q$ for some principal ideal $\mathfrak{b}$ generated by an element $\beta \in (K^+)^{*q}$. Thus, $\alpha = \mu(1-\zeta)^k(1-\bar{\zeta})^k\beta^q$, $\mu \in \mathcal{O}^*_{K^+}$ and $\psi(\mu(1-\zeta)(1-\bar{\zeta}) \pmod{\mathcal{E}^q}) = \alpha \pmod{(K^+)^{*q}}$. This shows the kernel of ψ' equals to the image of ψ.

Proposition 2.3. *The module $\mathcal{E}/\mathcal{E}^q$ is free over $\mathbb{F}_q[G^+]$ of rank* 1.

Proof. For each $\alpha \in \mathcal{E}$, $(\alpha) = \mathfrak{p}^k$, for some integer k. Let $\lambda = (1-\zeta)(1-\bar{\zeta})$, we have $\alpha = u\lambda^k$ for some u in $\mathcal{O}^*_{K^+}$. It follows that $\mathcal{E}$ is isomorphic to $\langle\lambda\rangle \times \mathcal{O}^*_{K^+}$. By the Dirichlet Theorem on the units group, $\mathcal{O}^*_{K^+}$ is isomorphic to $\mu_{K^+} \times \langle\gamma_1\rangle \times \langle\gamma_2\rangle \times ... \times \langle\gamma_{\frac{p-3}{2}}\rangle$, where μ_{K^+} is the subgroup of $\mathcal{O}^*_{K^+}$ consisting of roots of unity, and γ_i, $i = 1, ..., \frac{p-3}{2}$, are fundamental units in $\mathcal{O}^*_{K^+}$. Since the roots of unity in $\mathbb{R}$ are only ± 1, we have

$$\mathcal{O}^*_{K^+} \cong \{\pm 1\} \times \mathbb{Z}^{\frac{p-3}{2}},$$

and hence

$$\mathcal{E} \cong \langle\lambda\rangle \times \{\pm 1\} \times \mathbb{Z}^{\frac{p-3}{2}} \cong \{\pm 1\} \times \mathbb{Z}^{\frac{p-1}{2}}.$$

Consider the map

$$\begin{aligned} l : \mathcal{E} &\longrightarrow \prod_{\sigma \in G^+} \mathbb{R} = \mathbb{R}^{\frac{p-1}{2}} \\ x &\longmapsto (\ln|\sigma(x)|)_{\sigma \in G^+}. \end{aligned}$$

It is well known that the kernel of l consists of only roots of unity, i.e. only $\{\pm 1\}$, and the image of $l(\mathcal{O}^*_{K^+})$ is a lattice of rank $\frac{p-3}{2}$ contained in the subspace

$$W := \{(x_\sigma)_{\sigma \in G^+} \mid \sum_{\sigma \in G^+} x_\sigma = 0\} \subset \prod_{\sigma \in G^+} \mathbb{R},$$

while we do have $l(\lambda) \notin W$, as

$$\sum_{\sigma \in G^+} \ln|\sigma(\lambda)| = \ln(\prod_{a=1}^{p-1} |1-\zeta^a|) = \ln(p) \neq 0.$$

Therefore, $l(\mathcal{E})$ is a lattice of rank $\frac{p-1}{2}$ in $\prod_{\sigma \in G^+} \mathbb{R}$.

It is straightforward to check that the map l is indeed a $\mathbb{Z}[G^+]$-homomorphism and hence l induces an obvious $\mathbb{Z}[G^+]$-isomorphism:

$$\mathcal{L} : \mathcal{E}/\mathcal{E}^q \longrightarrow l(\mathcal{E})/ql(\mathcal{E}).$$

Denote $L = l(\mathcal{E})$. It is remained to prove that

$$L/qL \cong_{\mathbb{Z}[G^+]} \mathbb{F}_q[G^+].$$

By identifying $\prod_{\sigma\in G^+} \mathbb{R}$ with $\prod_{\sigma\in G^+} \mathbb{R}\cdot\sigma$, we can view it as a free $\mathbb{R}[G^+]$-module of rank 1 and view each $\sigma \in G^+$ as an $\mathbb{R}$-linear operator on it. Then the minimal polynomial of $\bar{\sigma}_1$, which is viewed as a linear operator, equals $x^{\frac{p-1}{2}} - 1$. For each proper factor $g(x)$ of $x^{\frac{p-1}{2}} - 1$, the set

$$U_g := \{v \in \prod_{\sigma\in G^+} \mathbb{R} \ \mid \ g(\bar{\sigma}_1)(v) = 0\}$$

is a proper subspace of $\prod_{\sigma\in G^+} \mathbb{R}$. Let U denote the union of all these proper subspaces. As $\mathbb{Q}$ is dense in $\mathbb{R}$ and L is a lattice in $\prod_{\sigma\in G^+} \mathbb{R}$ of full rank, we have $\mathbb{Q}\cdot L \not\subset U$. Obviously, for any element $v \in \mathbb{Q}\cdot L$ not contained in U, the module $\mathbb{Z}[G^+]\cdot v$ is free over $\mathbb{Z}[G^+]$ of rank 1. Let v be a such kind of element contained in L and denote $L' = \mathbb{Z}[G^+]\cdot v$. Then L' is a free $\mathbb{Z}[G^+]$-module of rank 1 contained in L. Note that as L' is also a lattice of full rank, so the quotient L/L' is finite. The multiplication by q induces a $\mathbb{Z}[G^+]$-isomorphic

$$L/L' \cong_{\mathbb{Z}[G^+]} qL/qL'.$$

Note that L/qL' is of finite order and it has two composition series of $\mathbb{Z}[G^+]$-modules:

$$L/qL' \supset M_1 \supset ... \supset M_{r-1} \supset M_r = L'/qL' \supset M_{r+1} \supset ... \supset M_s \supset \{0\}$$

and

$$L/qL' \supset N_1 \supset ... \supset N_{k-1} \supset N_k = qL/qL' \supset N_{k+1} \supset ... \supset N_t \supset \{0\}.$$

By Jordan-Hölder theorem, this two series has the same length and permutation equivalent factors, i.e. $s = t$ and there is a permutation ω such that $M_i/M_{i+1} = N_{\omega(i)}/N_{\omega(i)+1}$ for all $i = 1, 2, ..., t$. From the isomorphism

$$(L/qL')/(L'/qL') \cong L/L' \cong qL/qL' \cong (qL/qL')/\{0\},$$

it follows that the two series

$$L/qL' \supset M_1 \supset ... \supset M_{r-1} \supset L'/qL'$$

and

$$qL/qL' \supset N_{k+1} \supset ... \supset N_t \supset \{0\}$$

have the same factors up to permutation. Thus, the two series

$$L'/qL' \supset M_{r+1} \supset ... \supset M_s \supset \{0\}$$

and

$$L/qL' \supset N_1 \supset ... \supset N_{k-1} \supset qL/qL'$$

also have the same factors up to permutation. Namely, $L'/qL' \cong (L'/qL')/\{0\}$ and $L/qL \cong (L/qL')/(qL/qL')$, as $\mathbb{F}_q[G^+]$-modules, have the same Jordan-Hölder factors.

Since q is assumed to be relatively prime to $\frac{p-1}{2}$, the order of G^+, every finite $\mathbb{F}_q[G^+]$-module is isomorphic to the product of its Jordan-Hölder factors. Thus, L/qL is isomorphic to $L'/qL' \simeq \mathbb{F}_q[G^+]$.

□

The subgroup $C^+ \subset \mathcal{E}$ gives rise to the $\mathbb{F}_q[G^+]$ submodule $C^+\mathcal{E}^q/\mathcal{E}^q \subset \mathcal{E}/\mathcal{E}^q$. By identifying $\mathcal{E}/\mathcal{E}^q$ to $\mathbb{F}_q[G^+]$, we can identify $C^+\mathcal{E}^q/\mathcal{E}^q \subset \mathcal{E}/\mathcal{E}^q$ to an $\mathbb{F}_q[G^+]$-ideal $\mathfrak{a}$. Since

$$\mathbb{F}_q[G^+] \cong F_1 \times F_2 \times \ldots \times F_r,$$

where $F_1, F_2, \ldots, F_r$ are finite fields, we have

$$\mathfrak{a} \cong \mathfrak{a}_1 \times \mathfrak{a}_2 \times \ldots \times \mathfrak{a}_r,$$

where each $\mathfrak{a}_i$, being an ideal of F_i, equals F_i or $\{0\}$. Thus, each $\mathfrak{a}_i$ is a principal ideal generated by an idempotent e_i, and hence $\mathfrak{a}$ itself is also a principal ideal generated by an idempotent, say $\mathfrak{a} = (e)$ with $e^2 = e$. Let κ denote the isomorphism from $C^+\mathcal{E}^q/\mathcal{E}^q$ to $\mathfrak{a}$.

Suppose $c \in C^+$ and hence $\kappa(c\mathcal{E}^q) = a = \sum_{\sigma\in G^+} a_\sigma \sigma \in \mathfrak{a}$. Then

$$\kappa((c\mathcal{E}^q)^{\sum_{\sigma\in G^+}\sigma}) = \left(\sum_{\sigma\in G^+}\sigma\right)\cdot\kappa(c\mathcal{E}^q) = \left(\sum_{\sigma\in G^+}\sigma\right)\cdot a = \left(\sum_{\sigma\in G^+}\sigma\right)\cdot\left(\sum_{\tau\in G^+}a_\tau\tau\right)$$
$$= \sum_{\gamma\in G^+}\left(\sum_{\sigma\in G^+}a_\sigma\right)\gamma.$$

On the other hand, since $c^{\sum_{\sigma\in G^+}\sigma} = N_{K/\mathbb{Q}}(c) = 1$ (see, for example, Chapter 8 of [7]),

$$\begin{aligned}\kappa((c\mathcal{E}^q)^{\sum_{\sigma\in G^+}\sigma}) &= \kappa(c^{\sum_{\sigma\in G^+}\sigma}\mathcal{E}^q)\\ &= \kappa(\mathcal{E}^q) = 0\end{aligned}$$

and hence $\sum\limits_{\sigma\in G^+} a_\sigma = 0$. This leads to the conclusion that the weight of any element in $\mathfrak{a}$ is zero, and hence $\mathfrak{a} \subset I_0$.

In the following, we shall lift the generator e of the ideal $\mathfrak{a}$ to an element $\epsilon \in \mathbb{Z}[G^+]$ via the canonical map $\mathbb{Z}[G^+] \longrightarrow \mathbb{F}_q[G^+]$.

Proposition 2.4. *The ideal $\mathfrak{a}$ annihilates $Cl_{K^+}[q]$.*

The proof of this proposition needs the following result of Thaine (for a rigorous proof, see [5], theorem 16.3):

Theorem 2.1 (Thaine). *If $\epsilon \in \mathbb{Z}[G^+]$ annihilates the Sylow-q-subgroup of $(\mathcal{O}^*_{K^+}/C^+)$ and q does not divides $p-1$, then ϵ also annihilates the Sylow-q-subgroup of (Cl_{K^+}).*

With Thaine's theorem, we can prove Proposition 2.4.

Proof of Proposition 2.4. First, remember that the $\mathbb{F}_q[G^+]$-isomorphism from $\mathcal{E}/\mathcal{E}^q$ to $\mathbb{F}_q[G^+]$ gives an $\mathbb{F}_q[G^+]$-isomorphism from $C^+\mathcal{E}/\mathcal{E}^q$ to $\mathfrak{a}$. Since $\mathfrak{a}$ annihilates $\mathbb{F}_q[G^+]/\mathfrak{a}$, so $\mathfrak{a}$ also annihilates $\mathcal{E}/C^+\mathcal{E} \cong (\mathcal{E}/\mathcal{E}^q)/(C^+\mathcal{E}/\mathcal{E}^q)$. It follows that e, the generator of $\mathfrak{a}$, also annihilates $\mathcal{E}/C^+\mathcal{E}$, and so its preimage in $\mathbb{Z}[G^+]$. Because $\mathcal{O}^*_{K^+}/C^+\mathcal{O}^{*q}_{K^+} \subset \mathcal{E}/C^+\mathcal{E}$, we also have the fact that ϵ annihilates $\mathcal{O}^*_{K^+}/C^+\mathcal{O}^{*q}_{K^+}$. In another word, ϵ sends $\mathcal{O}^*_{K^+}$ into $C^+\mathcal{O}^{*q}_{K^+}$.

To arrive our goal, we have to make connection between ϵ and the annihilator of $\mathcal{O}^*_{K^+}/C^+$. Note that $\mathcal{O}^*_{K^+}/C^+$ is a finite abelian group, so it is isomorphic to direct product of its Sylow-subgroups, say

$$\mathcal{O}^*_{K^+}/C^+ \cong S_{p_1} \times S_{p_2} \times ... \times S_{p_n},$$

with p_i being distinct prime divisors of $|\mathcal{O}^*_{K^+}|$ and S_{p_i} are Sylow-p_i-subgroups of $\mathcal{O}^{*q}_{K^+}$. Let m be the integer such that the order of the Sylow-q-subgroup of $\mathcal{O}^{*q}_{K^+}$ is q^m, then it follows that

$$\begin{aligned} &(\mathcal{O}^*_{K^+}/C^+)^{q^m} \cong S^{q^m}_{p_1} \times S^{q^m}_{p_2} \times ... \times S^{q^m}_{p_n} \\ \Rightarrow &(\mathcal{O}^*_{K^+}/C^+)/(\mathcal{O}^*_{K^+}/C^+)^{q^m} \cong S_q, \end{aligned}$$

since $S_{p_i} \cong S^{q^m}_{p_i}$ if $p_i \neq q$ and $S^{q^m}_q \cong \{1\}$.

Consider the $\mathbb{F}_q[G^+]$-homomorphism

$$\begin{aligned} \pi : (\mathcal{O}^*_{K^+}/C^+)^{q^m} &\longrightarrow \mathcal{O}^{*q^m}_{K^+}/(C^+ \cap \mathcal{O}^{*q^m}_{K^+}) \\ u^{q^m}C^+ &\longmapsto u^{q^m}(C^+ \cap \mathcal{O}^{*q^m}_{K^+}), \end{aligned}$$

which is obviously an $\mathbb{F}_q[G^+]$-isomorphism. So we have that

$$\begin{aligned} S_q &\cong (\mathcal{O}^*_{K^+}/C^+)/(\mathcal{O}^*_{K^+}/C^+)^{q^m} \\ &\cong (\mathcal{O}_{K^+}/C^+)/(\mathcal{O}^{*q^m}_{K^+}/(C^+ \cap \mathcal{O}^{*q^m}_{K^+})) \\ &\cong \mathcal{O}^*_{K^+}/C^+\mathcal{O}^{*q^m}_{K^+}. \end{aligned}$$

Since ϵ sends $\mathcal{O}^*_{K^+}$ into $C^+\mathcal{O}^{*q}_{K^+}$, it also sends $C^+\mathcal{O}^{*q^i}_{K^+}$ into $C^+\mathcal{O}^{*q^{i+1}}_{K^+}$ for $i = 1, 2, ..., m-1$. Therefore, we have the result that ϵ^m sends $\mathcal{O}^*_{K^+}$ into $C^+\mathcal{O}^{*q^m}_{K^+}$, which is equivalent to saying that ϵ^m annihilates S_q. By Theorem 2.1(Thaine's theorem), ϵ^m also annihilates the Sylow-q-subgroup of Cl_{K^+}. Since the elements in $Cl_{K^+}[q]$ are of order 1 or q, by Cauchy's theorem, the order of $Cl_{K^+}[q]$ equals q^k for some integer k. It follows that $Cl_{K^+}[q] \subset S_q$, and so is annihilated by ϵ^m.

Recall that e is just ϵ times a qth power, and $e^m = e$. So for any ideal class $[\mathfrak{b}] \in Cl_{K^+}[q]$, we have that

$$[1] = [\mathfrak{b}]^{\epsilon^m} = [\mathfrak{b}]^{e^m} = [\mathfrak{b}]^e.$$

This equality shows that $Cl_{K^+}[q]$ is annihilated by e, and so is annihilated by $\mathfrak{a}$, and the proof is complete. □

If we let $\alpha \in H$, then $\phi'((\alpha(K^+)^{*q})^{\mathfrak{a}}) \subset Cl_{K^+}[q]^{\mathfrak{a}}$. Since Proposition 2.4 says that $\mathfrak{a}$ annihilates $Cl_{K^+}[q]$, it also means that $\mathfrak{a}$ sends $H/(K^+)^{*q}$ into ker(ϕ') =Im(ϕ) $= C^+\mathcal{E}^q/\mathcal{E}^q$. In another word, $(H/(K^+)^{*q})^{\mathfrak{a}} \subset C^+\mathcal{E}^q/\mathcal{E}^q$.

Suppose x and y are non-zero integers satisfying the Catalan'e equation $x^p - y^q = 1$. Denote

$$\xi_0 = (x-\zeta)(x-\zeta^{-1}).$$

By Lemma 2.1, $\xi_0 \in H$. Let ξ denote the image of ξ_0 under the quotient map $H \longrightarrow H/(K^+)^{*q}$. Then we have the important inclusion relation:

$$\xi^{\mathfrak{a}} \subset (H/(K^+)^{*q})^{\mathfrak{a}} \subset C^+\mathcal{E}^q/\mathcal{E}^q \cong \mathfrak{a}. \tag{2}$$

3. An Overview of the Proof

In this chapter, we give an overview of the proof of the main theorem. We shall list some key results, namely, Lemma 3.1, Theorem 3.1 and Lemma 3.4, which will be proved in Chapter 4, and show how these lead to the proof.

3.1. **Case 2.**

In this section, we do not require p to be greater than q. The proof for Case 2 is based on the following Lemma concerning the relative class number h_p^-.

Lemma 3.1. *Suppose p and q are two odd prime number such that q does not divide h_p^-, the relative class number of $K = \mathbb{Q}(\zeta)$. Then the Catalan's equation $x^p - y^q = 1$ has no nonzero integer solutions.*

Then the proof follows, as we can assume that $p = 3$, or 5, and in this case, the relative class number $h_p^- = 1$ (see table 7.1 of [5]).

3.2. **Case 3.**

In this section, we consider Case 3. Thus, we shall assume that $q \mid p - 1$.

Theorem 3.1 (**Mihăilescu**)**.** *Let $p, q \geq 5$ be odd primes satisfying the inequality*

$$\binom{\left[\frac{3p}{2(q-1)^2}\right] + \frac{q-1}{2}}{\left[\frac{3p}{2(q-1)^2}\right]} > \frac{4}{3}\left(\left[\frac{3p}{2(q-1)^2}\right] + 1\right)\left(\frac{q-1}{2}\right)^2 + 1.$$

Then the equation $x^p - y^q = 1$ has no solutions in non-zero integers x and y.

The power of the theorem is amplified via the following simple lemma.

Lemma 3.2. *Let $\mathcal{P}(s, k)$ denote the inequality*

$$\binom{s+k}{s} > \frac{4(s+1)k^2}{3} + 1.$$

If $\mathcal{P}(s, k)$ holds for some pair of integers $s \geq 4$ and $k \geq 2$ and $s' \geq s$, $k' \geq k$, then $\mathcal{P}(s', k')$ also holds.

Proof. The proof is by induction on s and k respectively. It only needs the works on the steps $s \mapsto s + 1$ and $k \mapsto k + 1$ if s and k we choose make $\mathcal{P}(s, k)$ holds.

First, observe the inequalities:

$$\begin{aligned}\binom{(s+1)+k}{(s+1)} &= \frac{s+1+k}{s+1}\binom{s+k}{s} \\ &> \frac{s+1+k}{s+1}\left(\frac{4}{3}(s+1)k^2 + 1\right) \\ &> \frac{4}{3}\frac{s+1+k}{s+1}(s+1)k^2 + 1 \\ &> \frac{4}{3}(s+2)k^2 + 1,\end{aligned}$$

where the last inequality holds since $k \geq 2$. So the step $s \mapsto s + 1$ is done.

Next, we write another estimation to see the correctness of step $k \mapsto k+1$:

$$\begin{aligned}\binom{s+(k+1)}{s} &= \frac{s+k+1}{k+1}\binom{s+k}{s} \\ &> \frac{s+k+1}{k+1}\left(\frac{4}{3}(s+1)k^2+1\right) \\ &> \frac{4}{3}(s+1)\frac{s+k+1}{k+1}k^2+1 \\ &\geq \frac{4}{3}(s+1)\frac{(k+5)k^2}{k+1} \\ &> \frac{4}{3}(s+1)(k+1)^2,\end{aligned}$$

where the second to last inequality is by the condition $s \geq 4$, and the last is by $k \geq 2$. □

It is easy to check that $\mathcal{P}(s,k)$ holds for $(s,k) = (6,4)$, $(7,3)$ and $(9,2)$. According to the theorem and the lemma together, we only need to deal with the following situations:

(1) $\frac{q-1}{2} = 1$, or equivalently, $q = 3$.
(2) $\frac{3p}{2(q-1)^2} < 9$ and $\frac{q-1}{2} = 2$, or equivalently, $p < 96$ and $q = 5$.
(3) $\frac{3p}{2(q-1)^2} < 7$, and $\frac{q-1}{2} = 3$, or equivalently, $p < 168$ and $q = 7$.
(4) $\frac{3p}{2(q-1)^2} < 6$, and $\frac{q-1}{2} = 4$, or equivalently, $p < 256$ and $q = 9$.
(5) $\frac{3p}{2(q-1)^2} \leq 5$, and $\frac{q-1}{2} \geq 5$.

First, (1) is ruled out, as we are in Case 3. Also, (4) is ruled out, as q is assumed to be a prime number. To complete the proof, we apply the following lemma.

Lemma 3.3. *Suppose $q \mid p-1$ and there exist non-zero integers x and y satisfying the catalan's equation $x^p - y^q = 1$. Then $p = 1 + k_1 q^2$ for some integer $k_1 \geq 4$.*

Since $p \geq 1 + 4q^2 \geq 1 + 4(q-1)^2$, we know that $\left[\frac{3p}{2(q-1)^2}\right] \geq 6$ and (5) is ruled out. Also, if $q = 5$, then $p \geq 101$; if $q = 7$, then $p \geq 197$, and hence (2) and (3) are ruled out.

Proof. (of Lemma 3.3) By Proposition 2.1, we have

$$x = 1 + p^{q-1} \cdot a^q \equiv 0 \pmod{q}.$$

This implies that $a \equiv a^q \equiv -1 \pmod{q}$, since $p^{q-1} \equiv 1 \pmod{q}$. It then follows that

$$a^q \equiv -1 \pmod{q^2}.$$

Therefore, $p^{q-1} \equiv -p^{q-1} \cdot a^q = 1 - x \pmod{q^2}$. Furthermore, Lemma 2.2 says $x \equiv 0 \pmod{q^2}$, and thus,

$$p^{q-1} \equiv 1 \pmod{q^2}.$$

On the other hand, by the assumption, there exist an integer k such that $p = 1 + kq$, and consequently,

$$\begin{aligned}p^{q-1} &= 1 + (q-1)kq + (\frac{q-1}{2})(kq)^2 + ... \\ &\equiv 1 + (q-1)kq \pmod{q^2}.\end{aligned}$$

These two congruence equations show that k is divisible by q and $p-1$ is divisible by q^2. Write $p = 1 + k_1q^2$. Then k_1 is even, which must be at least 4, for otherwise p must be divisible by 3, a contradiction.

□

3.3. **Case 4.** Finally, we deal with Case 4. Our main tool is the following:

Lemma 3.4. *Suppose p, q are two prime numbers with $p > q$ and x, y are two non-zero integers so that $x^p - y^q = 1$. If $q \nmid p-1$, then the element $1+\zeta$ in K is a q-th power modulo $q^2\mathcal{O}_K$.*

As before, let σ_q denote the automorphism in G sending ζ to ζ^q. For each $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + ... + a_{p-1}\zeta^{p-1} \in \mathcal{O}_K$, with $a_i \in \mathbb{Z}$ for each i, we certainly have

$$\begin{aligned}\sigma_q(\alpha) &= a_0 + a_1\zeta^q + a_2\zeta^{2q} + ... + a_{p-1}\zeta^{q(p-1)} \\ &\equiv (a_0 + a_1\zeta + a_2\zeta^2 + ... + a_{p-1}\zeta^{p-1})^q \pmod q \\ &\equiv \alpha^q \pmod q.\end{aligned}$$

Consequently, by raising the above to the qth power, we see that

$$\sigma_q(\alpha^q) \equiv \alpha^{q^2} \pmod{q^2}.$$

By the lemma, $1+\zeta \equiv \alpha^q \pmod{q^2}$, for some $\alpha \in \mathcal{O}_K$. Then we have

$$\begin{aligned}(1+\zeta)^q &\equiv \alpha^{q^2} \\ &\equiv \sigma_q(\alpha^q) \\ &\equiv \sigma_q(1+\zeta) \\ &\equiv 1+\zeta^q \pmod{q^2\mathcal{O}_K}.\end{aligned}$$

This means the sum $\sum_{i=1}^{q-1}\binom{q}{i}\zeta^i$ is divisible by q^2 in $\mathcal{O}_K$. However, since $\zeta, \zeta^2, ..., \zeta^{p-1}$ form a $\mathbb{Z}$-basis of $\mathcal{O}_K$, so $\zeta, \zeta^2, ...\zeta^{q-1}$ are $\mathbb{Z}$-independent. This would imply that each $\binom{q}{i}$ is divisible by q^2 , which is absurd.

4. Proof of the Key Results

In this chapter, we complete the main theorem by giving the proofs of Lemma 3.1, Theorem 3.1 and Lemma 3.4 in the following consecutive sections.

4.1. The proof of Lemma 3.1.

Proof of lemma3.1. Recall that $h_p^- = \frac{h_p}{h_p^+}$, where h_p and h_p^+ are respectively the orders of the class groups Cl_{K^+} and Cl_K, and we have the natural injection:

$$\phi : Cl_{K^+} \longrightarrow Cl_K.$$

By the assumption, $q \nmid h_p^-$ and hence ϕ induces an isomorphism $Cl_{K^+}[q] \cong Cl_K[q]$ on the q-torsion subgroups of the class groups.

Suppose x and y are non-zero integers satisfying $x^p - y^q = 1$. Then, by Lemma 2.1, there is an $\mathcal{O}_K$-ideal $\mathfrak{a}$ such that

$$\left(\frac{x-\zeta}{1-\zeta}\right) = \mathfrak{a}^q.$$

This implies that the class $[\mathfrak{a}] \in Cl_K$ is actually contained in $Cl_K[q]$. The above isomorphism implies that $[\mathfrak{a}] = [\mathfrak{b}\mathcal{O}_K]$, for some $\mathcal{O}_{K^+}$-ideal $\mathfrak{b}$. Consequently, we have $\mathfrak{a} = \gamma\mathfrak{b}\mathcal{O}_K$, for some $\gamma \in K^*$. For convenience, write $\mathfrak{b}'$ for $\mathfrak{b}\mathcal{O}_K$. Then

$$\bar{\mathfrak{b}'} = \mathfrak{b}'.$$

Denote $\mu = \frac{x-1}{1-\zeta}$. Then $\mu + 1 = \frac{x-\zeta}{1-\zeta}$. Therefore,

$$\left(\frac{\mu+1}{\bar{\mu}+1}\right) = \left(\frac{x-\zeta}{1-\zeta}\right)^{1-\iota} = \frac{\mathfrak{a}^q}{\bar{\mathfrak{a}}^q} = \left(\frac{\gamma^q}{\bar{\gamma}^q}\right),$$

and hence

$$\frac{\mu+1}{\bar{\mu}+1} = \frac{\gamma^q}{\bar{\gamma}^q} \cdot z,$$

for some $z \in \mathcal{O}_K^*$. Note that z has absolute value equal to 1 at each archimedean place of K, and hence is a root of 1. In particular, z is a qth power and we can write, for some $\alpha \in K^*$,

$$\frac{\mu+1}{\bar{\mu}+1} = \alpha^q.$$

Denote $\eta = (\sqrt[q]{\mu+1} + \zeta^{\frac{-1}{q}}\sqrt[q]{\bar{\mu}+1})^q$. Then, from the identity

$$\eta = (\bar{\mu}+1)(\alpha + \zeta^{\frac{-1}{q}})^q,$$

we see that $\eta \in \mathcal{O}_K$. Denote $\pi = \zeta - 1$ and let $\mathcal{O}_\pi$ denote the π-adic completion of $\mathcal{O}_K$. By Proposition 2.1,

$$\mu = \frac{x-1}{1-\zeta} = \frac{p^{q-1}a^q}{-\pi} \equiv 0 \pmod{\pi^7},$$

and it follows from the Hensel's lemma that both the equations $X^q - (\mu+1) = 0$ and $X^q - (\bar{\mu}+1) = 0$ have solutions in $\mathcal{O}_\pi$. Therefore, $u := \sqrt[q]{\mu+1} + \zeta^{\frac{-1}{q}}\sqrt[q]{\bar{\mu}+1}$ is contained in $\mathcal{O}_\pi$ and $u^q = \eta$. Moreover, the equality

$$(1+\mu) + \zeta^{-1}(1+\bar{\mu}) = \frac{x-\zeta}{1-\zeta} + \zeta^{-1}\frac{x-\zeta^{-1}}{1-\zeta^{-1}} = \frac{x-\zeta}{1-\zeta} + \frac{\zeta^{-1}-x}{1-\zeta} = \zeta^{-1}\frac{1-\zeta^2}{1-\zeta}$$

implies that $(1+\mu) + \zeta^{-1}(1+\bar{\mu})$ is a unit in $\mathcal{O}_K$. Furthermore,

$$(1+\mu+\zeta^{-1}(1+\bar{\mu}))^q = (\sqrt[q]{1+\mu} + \zeta^{\frac{-1}{q}}\sqrt[q]{1+\bar{\mu}})^q \left(\sum_{i=0}^{q-1} \sqrt[q]{1+\mu}^{\,q-1-i}\zeta^{\frac{-i}{q}}\sqrt[q]{1+\bar{\mu}}^{\,i}\right)^q.$$

implies that η, dividing $((1+\mu) + \zeta^{-1}(1+\bar{\mu}))^q$, is also a unit. In particular, $N_{K/\mathbb{Q}}(\eta) = 1$ and hence $N_{K_\pi/\mathbb{Q}_p}(u) = 1$, too. Here K_π denote the π-adic completion of K.

The next step is to express this $N_{K_\pi/\mathbb{Q}_p}(u)$ in terms of x and ζ. First, note that $\zeta^{\frac{-1}{q}} = \zeta^r$ for some integer $r \in \{1, 2, ..., p-1\}$. Then

$$\begin{aligned}
\frac{\frac{1}{1-\zeta} + \frac{\zeta^r}{1-\zeta}}{1+\zeta^r} &= \frac{1-\zeta^{r+1}}{(1-\zeta)(1+\zeta^r)} \\
&= \frac{1-(1+\pi)^{r+1}}{-\pi(1+(1+\pi)^r)} \\
&= \frac{1-1-(r+1)\pi - \binom{r+1}{2}\pi^2 + \dots}{-\pi(1+1+r\pi+\binom{r}{2}\pi^2+\dots)} \\
&\equiv \frac{r+1}{2} \pmod{\pi}
\end{aligned}$$

This congruence holds for any choice of ζ. Thus, taking the sum over all possible choice of ζ, we obtain a congruence of rational integers:

$$\sum_{\zeta\neq 1} \frac{\frac{1}{1-\zeta} + \frac{\zeta^r}{1-\zeta}}{1+\zeta^r} \equiv \frac{(r+1)(p-1)}{2} \pmod{p}.$$

The Hensel's lemma tells us that

$$\sqrt[q]{1+\mu} \equiv 1 + \frac{\mu}{q} \pmod{\mu^2},$$

and

$$\sqrt[q]{1+\bar{\mu}} \equiv 1 + \frac{\bar{\mu}}{q} \pmod{\bar{\mu}^2}.$$

We have $(\mu^2) = (\bar{\mu}^2) = (\frac{x-1}{\pi})^2$. Therefore,

$$\begin{aligned}
1 = N_{K_\pi/\mathbb{Q}_p}(u) &\equiv \prod_{\zeta\neq 1} 1 + \frac{\mu}{q} + \zeta^r(1+\frac{\bar{\mu}}{q}) \pmod{\frac{(x-1)^2}{\pi^2}} \\
&\equiv \prod_{\zeta\neq 1}(1+\zeta) \prod_{\zeta\neq 1}\left(1 + \frac{\frac{\mu}{q}+\frac{\zeta^r\bar{\mu}}{q}}{1+\zeta^r}\right) \pmod{\frac{(x-1)^2}{\pi^2}} \\
&\equiv N_{K/\mathbb{Q}}(1+\zeta) \cdot \prod_{\zeta\neq 1}\left(1 + \frac{x-1}{q}\frac{\frac{1}{1-\zeta}+\frac{\zeta^r}{1-\zeta}}{1+\zeta^r}\right) \pmod{\frac{(x-1)^2}{\pi^2}} \\
&\equiv N_{K/\mathbb{Q}}(1+\zeta) \cdot (1 + \frac{x-1}{q} \cdot \sum_{\zeta\neq 1}\left(\frac{\frac{1}{1-\zeta}+\frac{\zeta^r}{1-\zeta}}{1+\zeta^r}\right) \pmod{\frac{(x-1)^2}{\pi^2}} \\
&\equiv N_{K/\mathbb{Q}}(1+\zeta) \cdot (1 + \frac{x-1}{q} \cdot \frac{(r+1)(p-1)}{2}) \pmod{p(x-1)}.
\end{aligned}$$

Since $N_{K/\mathbb{Q}}(1+\zeta) = \prod\limits_{\zeta\neq 1}(-1-\zeta) = (-1)^{p-1} + \cdots + (-1) + 1 = 1$, we must have

$$r+1 \equiv 0 \pmod p,$$

which means

$$q \equiv 1 \pmod p,$$

and hence

$$\mu + \zeta^{\frac{-1}{q}}\bar{\mu} = \frac{x-1}{1-\zeta} + \zeta^{-1}\frac{x-1}{1-\zeta^{-1}} = 0.$$

This implies (as $\zeta^r = \zeta^{-1}$)

$$u \equiv 1 + \binom{\frac{1}{q}}{2}\mu^2 + \zeta^{-1} + \zeta^{-1}\binom{\frac{1}{q}}{2}\bar{\mu}^2 \pmod{(\frac{x-1}{\pi})^3}.$$

As the congruence holds for any choice of ζ, we have

$$\begin{aligned}
N(u) &\equiv \prod_{\zeta\neq 1}(1 + \binom{\frac{1}{q}}{2}\mu^2 + \zeta^{-1} + \zeta^{-1}\binom{\frac{1}{q}}{2}\bar{\mu}^2) \\
&\equiv \prod_{\zeta\neq 1}[(1+\zeta^{-1}) + \binom{\frac{1}{q}}{2}(\mu^2 + \zeta^{-1}\bar{\mu}^2)] \\
&\equiv \prod_{\zeta\neq 1}(1 + \frac{\binom{\frac{1}{q}}{2}(\mu^2+\zeta^{-1}\bar{\mu}^2)}{1+\zeta^{-1}}) \\
&\equiv 1 + \binom{\frac{1}{q}}{2}(x-1)^2\sum_{\zeta\neq 1}\frac{1}{1+\zeta^{-1}}[\frac{1}{(1-\zeta)^2} + \frac{\zeta^{-1}}{(1-\bar{\zeta})^2}] \\
&\equiv 1 + \binom{\frac{1}{q}}{2}(x-1)^2\sum_{\zeta\neq 1}\frac{1+\zeta}{(1+\zeta^{-1})(1-\zeta)^2} \\
&\equiv 1 + \binom{\frac{1}{q}}{2}(x-1)^2\sum_{\zeta\neq 1}\frac{(1+\zeta)\zeta}{(1+\zeta)(1-\zeta)^2} \\
&\equiv 1 + \binom{\frac{1}{q}}{2}(x-1)^2\sum_{\zeta\neq 1}\frac{\zeta}{(1-\zeta)^2} \pmod{(\frac{x-1}{\pi})^3}.
\end{aligned}$$

This means

$$\binom{\frac{1}{q}}{2}\sum_{\zeta\neq 1}\frac{\zeta}{(1-\zeta)^2} \equiv 0 \pmod{\frac{x-1}{\pi^3}}.$$

To show this leads to a contradiction, we need to evaluate the sum $\sum\limits_{\zeta\neq 1}\frac{\zeta}{(1-\zeta)^2}$. Let

$$f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \sum_{i=0}^{p-1} X^i.$$

$$g(X) = X^{p-2} + 2X^{p-3} + \cdots + (p-2)X + (p-1) = \sum_{i=0}^{p-2}(p-1-i)X^i.$$

Then

$$\frac{f'(X)}{f(X)} = \sum_{\zeta\neq 1}\frac{1}{X-\zeta} = \sum_{\zeta\neq 1}\frac{\zeta^{-1}}{\zeta^{-1}X-1} = \sum_{\zeta\neq 1}\frac{\zeta}{\zeta X-1},$$

and

$$\begin{aligned}\sum_{\zeta\neq 1}\frac{\zeta}{\zeta-X} &= \frac{1}{X}\sum_{\zeta\neq 1}\frac{\zeta}{\zeta\frac{1}{X}-1} = \frac{f'(\frac{1}{X})}{Xf(\frac{1}{X})} = \frac{X^{p-2}f'(\frac{1}{X})}{X^{p-1}f(\frac{1}{X})}\\ &= \frac{X^{p-2}(1+\frac{2}{X}+\frac{3}{X^2}+\cdots+\frac{(p-2)}{X^{p-3}}+\frac{(p-1)}{X^{p-2}})}{X^{p-1}(1+\frac{1}{X}+\cdots+\frac{1}{X^{p-2}}+\frac{1}{X^{p-1}})}\\ &= \frac{X^{p-2}+2X^{p-3}+\cdots+(p-2)X+(p-1)}{X^{p-2}+2X^{p-3}+\cdots+(p-2)X+1} = \frac{g}{f}.\end{aligned}$$

Observe that

$$\begin{aligned}\sum_{\zeta\neq 1}\frac{\zeta}{(1-\zeta)^2} &= \sum_{\zeta\neq 1}\frac{\zeta}{(x-\zeta)^2}|_{x=1} = \left(\sum_{\zeta\neq 1}\frac{\zeta}{\zeta-x}\right)'|_{x=1}\\ &= \left(\frac{g(x)}{f(x)}\right)'|_{x=1} = \frac{f(1)g'(1)-f'(1)g(1)}{f(1)^2}\end{aligned}$$

It can be seen that $f(1) = p$, $f'(1) = g(1) = \frac{p(p-1)}{2}$, and

$$\begin{aligned}g'(1) &= \sum_{i=1}^{p-1}(p-i)(i-1) = \sum_{i=1}^{p-1}(pi+i-p-i^2)\\ &= \frac{p(p+1)(p-1)}{2} - p(p-1) - \frac{p(p-1)(2p-1)}{6}\\ &= \frac{p}{12}(6p^2-6-12p+12-4p^2+6p-2) = \frac{p}{12}(2p^2-6p+4).\end{aligned}$$

Then we conclude that

$$\sum_{\zeta\neq 1}\left(\frac{\zeta}{1-\zeta^2}\right) = \frac{1-p^2}{12}.$$

This implies

$$(x-1) \quad \text{divides} \quad \frac{(1-q)(1-p^2)\pi^3}{24q^2} \in \mathbb{Z}_p[\zeta].$$

By Proposition 2.1, $x-1$ is divided by p^{q-1}. Therefore, p^{q-2} divides $q-1$. But this is absurd, since $p^{q-2} > q-1$. □

4.2. **The Proof of Theorem 3.1.** Theorem 3.1 is proved in this section. To have things fit into our previous results, we need to replace "p and q" by "q and p". Namely, we shall exchange the roles of p and q. Note that Doing so will not alter the statement in the theorem, as it is symmetric in p and q. For an element $\theta = \sum_\sigma n_\sigma\sigma \in \mathbb{Z}[G^+]$, denote

$$\|\theta\| = \sum_\sigma |n_\sigma|.$$

Lemma 4.1. *If*

$$\binom{\left[\frac{3q}{2(p-1)^2}\right]+\frac{p-1}{2}}{\left[\frac{3q}{2(p-1)^2}\right]} > \frac{(\left[\frac{3q}{2(p-1)^2}\right]+1)(p-1)^2}{3}+1,$$

then there are more than q elements $\theta \in I_S^-$ such that

$$\|\theta\| \leq \frac{3q}{2(p-1)}.$$

Proof. First, we claim that there exists a $\mathbb{Z}$-basis $\beta = \{\ \widetilde{\theta}_k \in I_S^-;\ k = 1, 2, ..., \frac{p-1}{2}\ \}$ of I_S^- such that each $\|\widetilde{\theta}_k\| \leq p-1$. Then consider the set

$$\Upsilon = \{\theta = \sum_{i=1}^{\frac{p-1}{2}} c_i\widetilde{\theta}_i \ \mid\ c_i \geq 0, \text{ for every } i, \text{ and } \sum_{i=1}^{\frac{p-1}{2}} c_i \leq \frac{3q}{2(p-1)^2}\}.$$

Obviously, if $\theta \in \Upsilon$, then $\|\theta\| \leq \frac{3q}{2(p-1)}$. The cardinality $|\Upsilon|$ equals the number of choices of non-negative integers $c_1, c_2, ..., c_{\frac{p-1}{2}}$ whose sum is not more than $\left[\frac{3q}{2(p-1)^2}\right]$, and hence equals $\binom{\left[\frac{3q}{2(p-1)^2}\right]+\frac{p-1}{2}}{\left[\frac{3q}{2(p-1)^2}\right]}$. Let $-\Upsilon$ denote the set $\{-\theta \mid \theta \in \Upsilon\}$. Then $-\Upsilon \cup \Upsilon$ has the cardinality

$$\begin{aligned}
2\binom{\left[\frac{3q}{2(p-1)^2}\right]+\frac{p-1}{2}}{\left[\frac{3q}{2(p-1)^2}\right]} - 1 &> \frac{2(p-1)^2}{3}(\left[\frac{3q}{2(p-1)^2}\right]+1)+1 \\
&> \frac{2(p-1)^2}{3}(\left[\frac{3q}{2(p-1)^2}\right]+1) \\
&> q \quad .
\end{aligned}$$

Thus, it remains to prove the claim. Next, we recall the element θ_c, where c is relatively prime to p, defined in Proposition 2.2, and set $\widetilde{\theta}_k = (1-\iota)(\theta_{k+1}-\theta_k)$ for $k = 1, 2, ..., \frac{p-1}{2}$. According to the proposition, each θ_k is contained in I_S^- and

$$\theta_{k+1} - \theta_k = \sum_{a=1}^{p-1}(\left[\frac{a(k+1)}{p}\right] - \left[\frac{ak}{p}\right])\sigma_a^{-1}.$$

Thus, all coefficients of $\theta_{k+1}-\theta_k$ are non-negative and we have

$$\begin{aligned}
\|\theta_{k+1}-\theta_k\| &= w(\theta_{k+1}-\theta_k) \\
&= w(k+1-\sigma_{k+1}-k+\sigma_k)\cdot w(\theta_S) \\
&= 1\cdot w(\sum_{a=1}^{p-1}\frac{a}{p}\sigma_a^{-1}) \\
&= \frac{p-1}{2}.
\end{aligned}$$

This implies the required bound:

$$\begin{aligned}\|\widetilde{\theta}_k\| &= \|(\theta_{k+1}-\theta_k)(1-\iota)\| \\ &\leq \|\theta_{k+1}-\theta_k\| \cdot \|1-\iota\| \\ &= p-1.\end{aligned}$$

Notice that $\theta_1 = 0$, so $\widetilde{\theta}_1 = \theta_2(1-\iota)$ and $\widetilde{\theta}_k = (\theta_{k+1}-\theta_k)(1-\iota)$, for $k = 2, 3, ..., \frac{p-1}{2}$. Therefore, the two sets $\{\widetilde{\theta}_k \mid k = 1, ..., \frac{p-1}{2}\}$ and $\{\theta_k(1-\iota) \mid k = 1, ..., \frac{p+1}{2}\}$ generate the same subgroup, denoted as J, of I_S^-. The equality

$$\begin{aligned}\theta_{p-c}(1-\iota) &= \theta_S(p-c-\sigma_{p-c})(1-\iota) \\ &= p\theta_S(1-\iota) - \theta_S(c+\sigma_{-c})(1-\iota) \\ &= p\theta_S(1-\iota) - \theta_S(c+\sigma_{-c}-c\iota-\sigma_c) \\ &= p\theta_S(1-\iota) - \theta_c(1-\iota)\end{aligned}$$

shows in particular that $p\theta_S(1-\iota) = \theta_{\frac{p+1}{2}}(1-\iota) + \theta_{\frac{p-1}{2}}(1-\iota) \in \mathsf{J}$. Then it together with the equality

$$\theta_{c+p} = \sum_{a=1}^{p-1}\left[\frac{a(c+p)}{p}\right]\sigma_a^{-1} = \sum_{a=1}^{p-1}\left[\frac{ac}{p}\right] + p\sum_{a=1}^{p-1}\frac{a}{p}\sigma_a^{-1} = \theta_c + p\theta_S.$$

shows that for every c relatively prime to p, the element $\theta_c(1-\iota)$ is contained in J. This means $\mathsf{J} = I_S^-$ (Proposition 2.2).

We complete the proof by showing that the $\mathbb{Z}$-rank of I_S^- is actually $\frac{p-1}{2}$. Consider the exact sequence

$$0 \longrightarrow \ker(j) \longrightarrow \mathbb{Z}[G] \xrightarrow{j} (1-\iota)\mathbb{Z}[G] \longrightarrow 0,$$

where $j(\xi) = (1-\iota)\xi$, for $\xi \in \mathbb{Z}[G]$. Obviously, $\ker(j)$ consists of all elements $\xi = \sum_{a=0}^{p-1} n_a\sigma_a$ such that $n_{-a} = n_a$, for every σ, and hence it is of rank $\frac{p-1}{2}$ over $\mathbb{Z}$. This shows that $(1-\iota)\mathbb{Z}[G]$ is also of rank $\frac{p-1}{2}$. But it is well known that the index of I_S^- in $(1-\iota)\mathbb{Z}[G]$ equals to the relative class number h^- (Iwasawa's Theorem, proof of which can be found in chapter 6 of [7]) which is finite.

□

Proof of Theorem 3.1. We shall emphasize again that the roles of p and q have been exchanged. Namely, we assume that

$$\binom{\left[\frac{3q}{2(p-1)^2}\right] + \frac{p-1}{2}}{\left[\frac{3q}{2(p-1)^2}\right]} > \frac{(\left[\frac{3q}{2(p-1)^2}\right]+1)(p-1)^2}{3} + 1,$$

and hence the conclusion statement of Lemma 4.1 holds. Suppose there were non-zero integers x and y satisfies the equality

$$x^p - y^q = 1.$$

First, we shall obtain a lower bound of $\sqrt{|x|+1}$, by estimating the value of $|x|$. By Proposition 2.1, $\frac{y^q+1}{y+1} = qv^p$, $y+1 = q^{p-1}b^p$ and $x = qbv$ for some nonzero integer b and positive integer

v. From the equality:

$$\begin{aligned} q(v^p - 1) &= \frac{y^q + 1}{y + 1} - q \\ &= y^{q-1} - y^{q-2} + ... - y + 1 - q \\ &= \sum_{i=1}^{q-1} ((-y)^i - 1) \end{aligned}$$

we find that $q(v^p - 1)$ is divided by $y + 1 = q^{p-1}b^p$, whence

$$v^p \equiv 1 \pmod{q^{p-2}}.$$

Notice that the order of the multiplicative group $(\mathbb{Z}/q^{p-2}\mathbb{Z})^*$ is $q^{p-3}(q-1)$. If p does not divide $q - 1$, then

$$v \equiv 1 \pmod{q^{p-2}}.$$

It follows that q^{p-2} divides $v - 1$ and $v \geq q^{p-2} + 1$, whence

$$|x| = |qbv| \geq qv \geq q(q^{p-2} + 1) > q^{p-1}.$$

If p divides $q - 1$, then $p < q$ and hence $|x| > |y| = q^{p-1}|b|^p - 1 \geq q^{p-1} - 1$. Thus, we always have

$$|x| \geq q^{p-1}.$$

As $q \geq 5$,

$$\sqrt{|x| + 1} > \sqrt{5}^{p-1}.$$

Next, we shall find an upper bound of $\sqrt{|x| + 1}$. By Lemma 2.2, for any $\theta \in I_S^-$, there exists unique $\alpha \in K^*$ such that $(x - \zeta)^\theta = \alpha^q$. The assignment $\theta \mapsto \alpha$ gives rise to a map

$$\phi : I_S^- \longrightarrow K^*.$$

The map ϕ is indeed a homomorphism of groups. We claim that it is injective. Suppose $\theta = \sum_\sigma n_\sigma \sigma$ is contained in the kernel of ϕ. Then we have

$$\prod_\sigma (x - \zeta^\sigma)^{n_\sigma} = 1.$$

Lemma 2.1 says that each $(x - \zeta^\sigma)$ is divisible by $1 - \zeta$. On the other hand, in the proof of the lemma, it has been shown that for different σ and τ, the numbers $\frac{x-\zeta^\sigma}{1-\zeta}$ and $\frac{x-\zeta^\tau}{1-\zeta}$ are relatively prime, and hence the great common divisor of the ideals $(x - \zeta^\sigma)$ and $(x - \zeta^\tau)$ is the prime ideal $(1 - \zeta)$. As $|N_{K/\mathbb{Q}}(x - \zeta^\sigma)| = |\frac{x^p-1}{x-1}| \geq |x - 1| > p$ (by. for instance, Proposition 2.1), we see that $x - \zeta^\sigma$ must be divisible by some prime ideal, say $\mathfrak{l}_\sigma$, other than $(1 - \zeta)$ and $\mathfrak{l}_\sigma$, $\mathfrak{l}_\tau$ are different for distinct σ and τ. Therefore, from the above equality, we deduce that $n_\sigma = 0$ for every σ, and hence $\theta = 0$. This proves the claim.

Since for each embedding $\tau : K \hookrightarrow \mathbb{C}$,

$$|\tau(t^\iota)| = |\tau(t)|,$$

for every $t \in K$, we must have

$$|\tau(\phi(\theta))| = 1,$$

for every $\theta \in I_S^-$, which is divided by $1-\iota$. Moreover, since $x^\iota = x$, we also have, for $\theta \in I_S^-$,

$$\phi(\theta)^q = (x-\zeta)^\theta = x^\theta \cdot \left(\frac{x-\zeta}{x}\right)^\theta = \left(1-\frac{\zeta}{x}\right)^\theta.$$

For the further estimation, consider the principal branch logarithm $\log(z)$ and the principal value of the argument $\mathrm{Arg}(z)$, of a complex number z as follow:

$$z = |z|e^{i\mathrm{Arg}(z)}, \quad -\pi < \mathrm{Arg}(z) \leq \pi,$$

$$\log(z) = \log(|z|) + i\mathrm{Arg}(z), \quad -\pi < \mathrm{Arg}(z) \leq \pi.$$

Now choose an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and an element $\theta_0 = \sum\limits_{\tau \in G} n_\tau \tau \in I_S^-$, and write $\alpha_0 = \phi(\theta_0)$. From the Taylor expansion of $\log(1+X)$ and the fact that $|x| \geq 3$, it follows

$$\begin{aligned}
|\log(\sigma(\alpha_0)^q)| &= |\log(\sigma(\alpha_0^q))| \\
&= \left|\log(\sigma((1-\frac{\zeta}{x})^{\theta_0}))\right| \\
&= \left|\log(\prod_{\tau\in G}\left(1-\frac{\sigma(\tau(\zeta))}{x}\right)^{n_\tau})\right| \\
&\leq \sum_{\tau\in G}|n_\tau|\cdot\left|\log\left(1-\frac{\sigma(\tau(\zeta))}{x}\right)\right| \\
&= \sum_{\tau\in G}|n_\tau|\cdot\left|-\sum_{j=1}^{\infty}\frac{1}{j}\left(\frac{\sigma(\tau(\zeta))}{x}\right)^j\right| \\
&\leq \sum_{\tau\in G}|n_\tau|\cdot\sum_{j=1}^{\infty}\left|\frac{\sigma(\tau(\zeta))^j}{jx^j}\right| \\
&\leq \sum_{\tau\in G}|n_\tau|\cdot\frac{1}{|x|}\cdot\sum_{j=0}^{\infty}\frac{1}{|x|^j} \\
&= \sum_{\tau\in G}|n_\tau|\cdot\frac{1}{|x|}\cdot\frac{1}{1-\frac{1}{|x|}} \\
&\leq \sum_{\tau\in G}|n_\tau|\cdot\frac{1}{|x|}\cdot\frac{1}{1-\frac{1}{3}} \\
&= \sum_{\tau\in G}|n_\tau|\frac{3}{2|x|} \\
&= \frac{3\|\theta_0\|}{2|x|}.
\end{aligned}$$

Since $|\sigma(\alpha_0)^q| = 1$, we have the equality

$$|\log(\sigma(\alpha_0)^q)| = |\log|\sigma(\alpha_0)^q| + i\mathrm{Arg}(\sigma(\alpha_0)^q)| = |\mathrm{Arg}(\sigma(\alpha_0)^q)|,$$

whence $|\mathrm{Arg}(\sigma(\alpha_0)^q)| \leq \frac{3\|\theta_0\|}{2|x|}$. Since $\mathrm{Arg}(\sigma(\alpha_0)^q) \equiv q\mathrm{Arg}(\sigma)\alpha_0 \pmod{2\pi}$, there exists an integer $k \in (-\frac{q}{2}, \frac{q}{2})$ such that $\mathrm{Arg}(\sigma(\alpha_0)^q) + 2k\pi = q\mathrm{Arg}(\sigma(\alpha_0))$, and consequently,

$$|\mathrm{Arg}(\sigma(\alpha_0)) - \frac{2k\pi}{q}| = \frac{1}{q}|\mathrm{Arg}(\sigma(\alpha_0)^q)| \leq \frac{3\|\theta_0\|}{2q|x|}.$$

In general, there could be more than one integer k satisfying the above inequality. however, if $\|\theta_0\| \leq \frac{3q}{2(p-1)}$, then k is unique. For if there are two integers k, k' satisfy the inequality, then

$$|\frac{2k\pi}{q} - \frac{2k\pi}{q}| \leq |\mathrm{Arg}(\sigma(\alpha_0)) - \frac{2k\pi}{q}| + |\mathrm{Arg}(\sigma(\alpha_0)) - \frac{2k\pi}{q}| \leq \frac{3\|\theta_0\|}{q|x|}.$$

As $|x| \geq q^{p-1}$, this implies

$$|k - l| \leq \frac{3\|\theta_0\|}{2\pi|x|} \leq \frac{3}{2\pi} \cdot \frac{3q}{2(p-1)} \cdot \frac{1}{q^{p-1}} < 1,$$

a contradiction. This let we even corresponds each $\theta \in I_S^-$ an integer. By lemma 4.1, there are more than q $\theta_0 \in I_S^-$ with $\|\theta_0\| \leq \frac{3q}{2(p-1)}$, while there are only q integers in $(-\frac{q}{2}, \frac{q}{2})$. Therefore, by the Pigeonhole Principle, there are two elements $\theta_1, \theta_2 \in I_S^-$, with $\|\theta_i\| \leq \frac{3q}{2(p-1)}$, $i = 1, 2$, corresponds to the same integer k. Write $\alpha_1 = \phi(\theta_1), \alpha_2 = \phi(\theta_2)$, and put $\bar{\theta} = \theta_1 - \theta_2$, $\alpha_0 = \phi(\bar{\theta}) = \frac{\alpha_1}{\alpha_2} \neq 1$, as ϕ is injective.

The next step is to estimate the value $|\sigma(\alpha_0) - 1|$. To do so, we first estimate

$$\begin{aligned}
|\log(\sigma(\alpha_0))| &= |\mathrm{Arg}(\sigma(\alpha_0))| \\
&\leq |\mathrm{Arg}(\sigma(\alpha_1)) - \mathrm{Arg}(\sigma(\alpha_2))| \\
&\leq |\mathrm{Arg}(\sigma(\alpha_1) - \frac{2k\pi}{q}| + |\mathrm{Arg}(\sigma(\alpha_2)) - \frac{2k\pi}{q}| \\
&\leq \frac{3\|\theta_1\|}{2q|x|} + \frac{3\|\theta_2\|}{2q|x|} \\
&\leq \frac{3}{2q|x|}\frac{3q}{2(p-1)} + \frac{3}{2q|x|}\frac{3q}{2(p-1)} \\
&= \frac{3^2}{2}\frac{1}{|x|(p-1)}.
\end{aligned}$$

Then,

$$\begin{aligned}
|\sigma(\alpha_0) - 1| &= |e^{\log(\sigma(\alpha_0))} - 1| \\
&= |\log(\sigma(\alpha_0)) + \frac{1}{2!}\log(\sigma(\alpha_0))^2 + \frac{1}{3!}\log(\sigma(\alpha_0))^3 + \dots| \\
&\leq |\log(\sigma(\alpha_0))| + \frac{1}{2!}|\log(\sigma(\alpha_0))^2| + \frac{1}{3!}|\log(\sigma(\alpha_0))^3| + \dots \\
&\leq \frac{3^2}{2}\frac{1}{|x|(p-1)}\left(\sum_{j=0}^{\infty}\frac{1}{|x|^j}\right) \\
&\leq \frac{3^2}{2}\frac{1}{|x|(p-1)}\frac{1}{1-\frac{1}{|x|}} \leq \frac{3^2}{2}\frac{1}{|x|(p-1)}\frac{1}{1-\frac{1}{3}} = \frac{3^3}{2^2|x|(p-1)}.
\end{aligned}$$

Consequently,

$$\begin{aligned} |N_{K/\mathbb{Q}}(\alpha_0 - 1)| &= |\textstyle\prod_{\tau\in G}\tau(\alpha_0 - 1)| \\ &= |\sigma(\alpha_0 - 1)\overline{\sigma(\alpha_0 - 1)}| \prod_{\tau\neq\sigma,\iota\sigma} |\tau(\alpha_0 - 1)| \\ &= |\sigma(\alpha_0 - 1)\overline{\sigma(\alpha_0 - 1)}| \prod_{\tau\neq\sigma,\iota\sigma} (|\tau(\alpha_0)| + 1) \\ &\leq \left(\tfrac{3^3}{2^2|x|(p-1)}\right)^2 \cdot 2^{p-3}. \end{aligned}$$

For simplicity, for the rest of the proof, we let $N(X)$ denote the norm $N_{K/\mathbb{Q}}(X)$, where X is either a number in K or a fractional ideal contained in K. Write $(\alpha_0) = \frac{J'}{J}$, where J and J' are coprime $\mathcal{O}_K$-ideals, and write $\bar{\theta} = \sum_\tau n_\tau\tau = \bar{\theta}_1 - \bar{\theta}_2$, with $\bar{\theta}_1 = \sum_{n_\tau>0} n_\tau\tau$ and $\bar{\theta}_2 = \sum_{n_\tau<0} -n_\tau\tau$. Since $(x-\zeta)^{\bar{\theta}} = \alpha_0^q$, we have

$$\frac{N((x-\zeta)^{\bar{\theta}_1})}{N((x-\zeta)^{\bar{\theta}_2})} = N((x-\zeta)^{\bar{\theta}}) = N(\alpha_0^q) = \frac{N(J')^q}{N(J)^q}.$$

This means that $N((x-\zeta)^{\bar{\theta}_1}) = N(J')k$ and $N((x-\zeta)^{\bar{\theta}_2}) = N(J)^q k$, for some nonzero integer k. Then, as $N(\alpha_0) = 1$,

$$\begin{aligned} N(J)^{2q} &= N(J') \cdot N(J)^q \\ &\leq N((x-\zeta)^{\bar{\theta}_1}) \cdot N((x-\zeta)^{\bar{\theta}_2}) \\ &= N(\prod_{\tau\in G}(x-\zeta)^{|n_\tau|}) \\ &= \prod_{\tau\in G} N(x-\zeta)^{|n_\tau|} \\ &= \prod_{\tau\in G}(\prod_{\gamma\in G}(x-\zeta^\gamma))^{|n_\tau|} \\ &= \prod_{\tau\in G}(\prod_{i=1}^{p-1}(x-\zeta^i)))^{|n_\tau|} \\ &= \prod_{\tau\in G}(\sum_{i=0}^{p-1} x^i)^{|n_\tau|} \\ &\leq \prod_{\tau\in G}(\sum_{i=0}^{p-1}\binom{p}{i}|x|^i)^{|n_\tau|} \\ &= \prod_{\tau\in G}(|x|+1)^{(p-1)|n_\tau|} \\ &= (|x|+1)^{(p-1)\|\bar{\theta}\|} \\ &= (|x|+1)^{(p-1)(\|\theta_1\|+\|\theta_2\|)} \\ &\leq (|x|+1)^{(p-1)\frac{3q}{p-1}} \end{aligned}$$

In other words,

$$N(J) \leq (|x|+1)^{\frac{3}{2}}.$$

Since $J \cdot (\alpha_0 - 1) = J' - J \subset \mathcal{O}_K$, we have

$$N(J)^{-1} \leq |N(\alpha_0 - 1)| \leq (\frac{3^3}{2^2|x|(p-1)})^2 \cdot 2^{p-3}.$$

Finally, putting all things together, we have the inequality:

$$\begin{aligned}
\sqrt{5}^{p-1} &\leq \sqrt{|x|+1} \\
&= \frac{(|x|+1)^2}{(|x|+1)^{\frac{3}{2}}} \\
&\leq \frac{(|x|+1)^2}{N(J)} \\
&\leq (|x|+1)^2 (\frac{3^3}{2^2|x|(p-1)})^2 \cdot 2^{p-3} \\
&\leq \frac{729}{16(p-1)^2} \cdot 2 \cdot 2^{p-3} \\
&< \frac{46}{(p-1)^2} 2^{p-2}.
\end{aligned}$$

But this is absurd. To see it, let $m(t) = \frac{46}{(t-1)^2} 2^{t-2}$ and $n(t) = \sqrt{5}^{t-1}$. Then $m(5) = 23 < 25 = n(5)$ and $m(t+1) < 2m(t) < 2n(t) < n(t+1)$.

□

4.3. **the Proof of Lemma 3.4.** In this section, we prove Lemma 3.4. Through out the section, we shall assume that $q \nmid p-1$ and there are non-zero integers x and y satisfying $x^p - y^q = 1$.

Theorem 4.1. *Let θ be an element in $\mathbb{Z}[G]$, divided by $1+\iota$. If the weight $w(\theta)$ is divided by q and $(x-\zeta)^\theta = \alpha^q$ for some $\alpha \in K^*$, then $\theta \in q\mathbb{Z}[G]$.*

This is a theorem of Mihăilescu who proves it by using Runge's method. We shall apply the proof given in [2] that follows the treatments in [5] and [4].

Proof. First, we note that α is indeed contained in K^+, since $\iota \cdot \theta = \theta$, and hence

$$(\frac{\alpha}{\alpha^\iota})^q = \frac{(x-\zeta)^\theta}{(x-\zeta)^\theta} = 1.$$

Then, we shall make some reduction. Let $\theta = \sum_{\tau \in G} n_\tau \tau$ and let $\theta' = \sum_{\tau \in G} n'_\tau \tau$ with $n_\tau \equiv n'_\tau \pmod{q}$ and $0 \leq n_\tau \leq q-1$ for each τ. As we also have $n'_{\iota\tau} = n'_\tau$, θ' is divisible by $1+\iota$. Thus, by replacing θ by θ' if necessary, we can assume that $n_\tau \in [0, q-1]$. Moreover, as

$$w(\theta + (q\sum_{\tau \in G} \tau - \theta)) = w(q\sum_{\tau \in G} \tau) = q(p-1),$$

by replacing θ with $q\sum\limits_{\tau \in G} \tau - \theta$ if necessary, we can assume that $mq := w(\theta) \leq \frac{q(p-1)}{2}$.

Next, define

$$(1-\zeta^\tau t)^{\frac{n_\tau}{q}} = \sum_{k\geq 0} \binom{\frac{n_\tau}{q}}{k} (-\zeta^\tau t)^k \in K[[t]]$$

and set

$$F(t) := (1-\zeta t)^{\frac{\theta}{q}} = \prod_{\tau\in G} (1-\zeta^\tau t)^{\frac{n_\tau}{q}},$$

which is contained in $K^+[[t]]$, as $n_{\tau\iota} = n_\tau$.

We have

$$\begin{aligned} (1-\zeta^\tau qT)^{\frac{n_\tau}{q}} &= 1 + \sum_{k=1}^{\infty} \left(\frac{1}{q}\right)^k \frac{n_\tau(n_\tau - q)(n_\tau - 2q)\dots(n_\tau - (k-1)q)}{k!} (-\zeta^\tau qT)^k \\ &= 1 + \sum_{k=1}^{\infty} \frac{n_\tau(n_\tau - q)(n_\tau - 2q)\dots(n_\tau - (k-1)q)}{k!} (-\zeta^\tau T)^k. \end{aligned}$$

The T^k coefficient of this power series is of the form $\frac{a_k}{k!}$ with

$$a_k = n_\tau(n_\tau - q)(n_\tau - 2q)\dots(n_\tau - (k-1)q)(-\zeta^\tau)^k \equiv (-n_\tau\zeta^\tau)^k \quad (\text{mod} q).$$

We interpolate this by writing

$$(1-\zeta^\tau qT)^{\frac{n_\tau}{q}} \equiv e^{-n_\tau\zeta^\tau T} \pmod q.$$

Therefore,

$$F(qT) \equiv e^{-\sum_\tau n_\tau \zeta^\tau T} \pmod q.$$

Then, writing $F(t) = F(q\cdot\frac{t}{q}) = F(q\cdot T)$, we see that

$$F(t) = \sum_{k\geq 0} \frac{a_k}{k! q^k} t^k \quad \text{with} \quad a_k \equiv (-\sum_{\tau\in G} n_\tau \zeta^\tau)^k \quad (\text{mod} q). \tag{3}$$

Next, we estimate the absolute values of the coefficients of $F(t)$ at each non-archimedean place. To do this, we fix any embedding

$$\sigma : K^+ \hookrightarrow \mathbb{R}$$

and note

$$\begin{aligned} \left|\sigma\left(\binom{\frac{n_\tau}{q}}{k}(-\zeta^\tau)^k\right)\right| &= \left|\binom{\frac{n_\tau}{q}}{k}\right| \cdot \left|\sigma(\zeta^\tau)^k\right| \\ &= \left|\frac{\frac{n_\tau}{q}(\frac{n_\tau}{q}-1)(\frac{n_\tau}{q}-2)...(\frac{n_\tau}{q}-(k-1))}{k!}\right| \\ &\leq (-1)^k \frac{-\frac{n_\tau}{q}(-\frac{n_\tau}{q}-1)(-\frac{n_\tau}{q}-2)...(-\frac{n_\tau}{q}-(k-1))}{k!} \\ &= (-1)^k \binom{-\frac{n_\tau}{q}}{k}, \end{aligned}$$

which is the coefficient of t^k in $\sum_{k\geq 0}\binom{\frac{-n_\tau}{q}}{k}(-t)^k = (1-t)^{\frac{-n_\tau}{q}}$. This shows the absolute value of the coefficient of t^k in $\sum_{k\geq 0}\binom{\frac{n_\tau}{q}}{k}(-\zeta^\tau t)^k$ is bounded by that in $\sum_{k\geq 0}\binom{\frac{-n_\tau}{q}}{k}(-t)^k$, and hence the absolute value of t^k coefficients of $F^\sigma(t)$ (the image of $F(t)$ under σ) is bounded by that of

$$\prod_{\tau\in G}(1-t)^{\frac{-n_\tau}{q}} = (1-t)^{\frac{1}{q}\sum_{\tau\in G} n_\tau} = (1-t)^{-m}.$$

Let $F_l(t)$ and $s_l(t)$ respectively denote the lth partial sum of $F(t)$ and $(1-t)^{-m}$. Then, $F^\sigma(t_0))$ does converge, for $t_0 \in \mathbb{R}$, $|t_0| < 1$, as by Taylor's theorem, there exists $\rho \in \mathbb{R}$ with $|\rho| < |t_0| < 1$ so that

$$\begin{aligned}
|F^\sigma(t_0) - \sigma(F_l(t_0))| &\leq \left|(1-t_0)^{-m} - s_l(t_0)\right| && (4)\\
&= \frac{t_0}{(l+1)!}\frac{d^{l+1}(1-z)^{-m}}{dz^{l+1}}|_{z=\rho}\\
&= \frac{|t_0|^{l+1}}{(l+1)!}\frac{(m+l)!}{(m-1)!}(1-|\rho|)^{-m-l-1}\\
&= |t_0|^{l+1}\binom{m+l}{l+1}\frac{1}{(1-|\rho|)^{m+l+1}}\\
&\leq \binom{m+l}{l+1}\frac{|t_0|^{l+1}}{(1-|t_0|)^{m+l+1}}. && (5)
\end{aligned}$$

In particular, if t_0 is a rational number with absolute value smaller than 1, then $F^\sigma(t_0)$ is defined for each σ, and we have

$$F^\sigma(t_0)^q = \sigma((1-\zeta t_0)^\theta).$$

Now, consider the case where $t_0 = \frac{1}{x}$. Then,

$$F^\sigma\left(\frac{1}{x}\right) = \sigma\left(\frac{\alpha}{x^m}\right),$$

since 1 is the only qth root of unity in $\mathbb{R}$ and we also have $(x-\zeta)^\theta = \alpha^q$, whence

$$F^\sigma\left(\frac{1}{x}\right)^q = \sigma\left(\left(1-\frac{\zeta}{x}\right)^\theta\right) = \sigma\left(\left(\frac{\alpha}{x^m}\right)\right)^q.$$

Also, the fact that $\theta = (1+\iota)\theta'$ for some $\theta' \in \mathbb{Z}[G]$ implies that if we extend σ to an embedding $K \xrightarrow{\sigma} \mathbb{C}$, then

$$F^\sigma\left(\frac{1}{x}\right)^q = N_{\mathbb{C}/\mathbb{R}}\left(\left(1-\frac{\zeta}{x}\right)^{\theta'}\right) > 0.$$

Suppose M is an integer prime to q. Then, for each τ, there exists an integer A_τ so that

$$n_\tau \equiv q\cdot A_\tau \pmod{M},$$

whence

$$\frac{n_\tau}{q}(\frac{n_\tau}{q}-1)\dots(\frac{n_\tau}{q}-k+1) \equiv \binom{A_\tau}{k}\cdot k! \pmod{M}.$$

This shows that each $\binom{\frac{n_\tau}{q}}{k}(-\zeta)^k$ is an M-adic integer. Consequently, the coefficients of the partial sum $F_m(t)$ of $F(t)$ all have powers of q as their denominators. Thus, in view of (3), we see that the element $q^{m+\mathrm{ord}_q(m!)}x^m F_m\left(\frac{1}{x}\right)$ is contained in $\mathcal{O}_{K^+}$, and hence so is

$$f_m := q^{m+\mathrm{ord}_q(m!)}\alpha - q^{m+\mathrm{ord}_q(m!)}F_m\left(\frac{1}{x}\right).$$

The next step is to show that $f_m = 0$ by showing that

$$|\sigma(f_m)| < 1, \text{ for every } \sigma.$$

If $m = 0$, then $\theta = 0$ and there is nothing to prove. therefore, we assume that $m \geq 1$, for the rest of the proof. Then,

$$\begin{aligned}
& |\sigma(f_m)| \\
= \; & q^{m+\mathrm{ord}_q(m!)}|\sigma(x^m)||F^\sigma(\frac{1}{x}) - \sigma(F_m(\frac{1}{x}))| \\
= \; & q^{m+\mathrm{ord}_q(m!)}|x^m||F^\sigma(\frac{1}{x}) - F_m^\sigma(\frac{1}{x})| \\
\leq \; & q^{m+\mathrm{ord}_q(m!)}|x^m|\binom{m+m}{m+1}\frac{\frac{1}{|x|^{m+1}}}{(1-\frac{1}{|x|})^{m+m+1}} \\
< \; & q^{m+\mathrm{ord}_q(m!)}\binom{2m}{m+1}\left(\frac{49}{48}\right)^{2m+1}\frac{1}{|x|},
\end{aligned}$$

where the last inequality comes from the estimation

$$|x| \geq q^{p-1} \geq 7^{7-1} > 49.$$

As $1 \leq m \leq \frac{p-1}{2}$, we have the further estimation:

$$\begin{aligned}
& q^{m+\mathrm{ord}_q(m!)}\binom{2m}{m+1}\left(\frac{49}{48}\right)^{2m+1}\frac{1}{|x|} \\
\leq & q^{m+\sum_{k\geq 1}\left[\frac{m}{q^k}\right]}2^{2m}\left(\frac{49^2}{48^2}\right)^{2m}\frac{1}{|x|} \\
\leq & q^{m+\frac{m}{q-1}}\left(\frac{2401}{1152}\right)^{2m}\frac{1}{|x|} \\
\leq & \left(q^{\frac{q}{2(q-1)}}\left(\frac{2401}{1152}\right)\right)^{p-1}\frac{1}{|x|} \\
\leq & \left(q^{\frac{7}{12}}\left(\frac{2401}{1152}\right)\right)^{p-1}\frac{1}{q^{p-1}}.
\end{aligned} \tag{6}$$

To have the desired inequality, we only need to observe that

$$\left(\frac{2401}{1152}\right)^{12} < 2.09^{12} < 16807 = 7^5 \leq q^5.$$

Now, we have the equality:

$$q^{m+\mathrm{ord}_q(m!)}\alpha = q^{m+\mathrm{ord}_q(m!)}x^m F\left(\frac{1}{x}\right) = \sum_{k=0}^{m} q^{m+\mathrm{ord}_q(m!)}\frac{a_k}{k!q^k}x^{m-k},$$

where $a_k \equiv (-\sum_{\tau\in G} n_\tau\zeta^\tau)^k \pmod q$. Then, since q divides $q^{m+\mathrm{ord}_q(m!)}\frac{a_k}{k!q^k}$, $k=1,2,...,m-1$, and $q^{m+\mathrm{ord}(m!)}\alpha$ must be divided by q, we conclude that

$$\left(-\sum_{\tau\in G} n_\tau\zeta^r\right)^m \equiv a_m \equiv 0 \quad (\mathrm{mod} q).$$

We have seen in the proof for Lemma 2.2, $\mathcal{O}_K/(q)$ has no nilpotent elements. Therefore, $\sum\limits_{\tau\in G} n_\tau\zeta^r$ must be divisible by q. Since the elements ζ^i, $i=1,...,p-1$ form a $\mathbb{Z}$ basis of $\mathcal{O}_K$, each n_τ is divisible by q and so is θ. □

What we actually need is the following counterpart of Theorem 4.1 for $\mathcal{O}_{K^+}$ and $\mathbb{Z}[G^+]$.

Lemma 4.2. *Suppose θ is an element in $\mathbb{Z}[G^+]$ with weight divisible by q. If the element $((x-\zeta)(x-\bar{\zeta}))^\theta$ is a qth power in K^+, then $\theta \in q\mathbb{Z}[G^+]$.*

Proof. For simplicity, we also let σ_a, $a \in \{1,2,...,p-1\}$, denote the restriction of it to K^+. then we have $\sigma_a = \sigma_{p-a}$ on K^+ and write $\theta = \sum_{a=1}^{\frac{p-1}{2}} n_{\sigma_a}\sigma_a$. Using this expression of θ, we view it as an element in $\mathbb{Z}[G]$ and set $\hat{\theta} = (1+\iota)\theta = \sum_{a=1}^{\frac{p-1}{2}} n_{\sigma_a} + \sum_{a=\frac{p+1}{2}}^{p-1} n_{\sigma_a}$. Then

$$(x-\zeta)^{\hat{\theta}} = ((x-\zeta)(x-\bar{\zeta}))^\theta$$

is a qth power is K, while

$$w(\hat{\theta}) = 2w(\theta) \equiv 0 \pmod q.$$

Thus, by Theorem 4.1, $\hat{\theta} \in \mathbb{Z}[G]$, and hence each n_{σ_a} is divisible by q. □

Recall that C^+ denote the group of cyclotomic units in K^+ and I_0 denote the kernel of the weight function on $\mathbb{F}_q[G^+]$. Also, $\xi_0 = (x-\zeta)(x-\zeta^{-1}) \in H$ and ξ denotes the image of $(x-\zeta)(x-\zeta^{-1})$ under the natural projection map $H \longrightarrow H/\mathbb{Q}(K^+)^{*q}$.

Lemma 4.3. *Every $\gamma \in C^+$ is congruent to a qth power modulo $q^2\mathcal{O}_{K^+}$.*

Proof. Obviously, if $\theta \in q\mathbb{Z}[G^+]$, then $\xi^\theta \in (K^+)^{*q}$. Thus, we the homomorphism

$$\begin{aligned} \chi : I_0 &\longrightarrow H/(K^+)^{*q} \\ \theta &\longmapsto \xi^\theta. \end{aligned}$$

is well-defined. Moreover, Lemma 4.2 actually insures that χ is a monomorphism. In particular, if $\mathfrak{a} \subset I_0$, the $\mathbb{F}_q[G^+]$-ideal defined in Section 2.5, then χ induces an isomorphism from $\mathfrak{a}$ to $\xi^\mathfrak{a}$. Also, the inclusion (2) in Section 2.5 implies that

$$\mathfrak{a} \cong \xi^\mathfrak{a} \subset (H/(K^+)^{*q})^\mathfrak{a} \subset C^+\mathcal{E}^q/\mathcal{E}^q \cong \mathfrak{a},$$

whence

$$\mathfrak{a} \cong \xi^\mathfrak{a} = (H/(K^+)^{*q})^\mathfrak{a} = C^+\mathcal{E}^q/\mathcal{E}^q,$$

which implies

$$C^+/(C^+ \cap \mathcal{E}^q) = \xi^\mathfrak{a} \subset \xi^{I_0}.$$

Therefore, for the given $\gamma \in C^+$, there exists some $\theta = \sum_{a=1}^{\frac{p-1}{2}} n_a\sigma_a \in \mathbb{Z}[G^+]$, with each $n_a \geq 0$, and some $\delta \in (K^+)^*$ so that

$$\gamma^{-1}\delta^q = \xi_0^\theta.$$

The condition that each $n_a \geq 0$ implies that ξ_0^θ and hence δ is contained in $\mathcal{O}_{K^+}$. Also, as we have (note that $x \equiv 0 \pmod{q^2}$)

$$\xi^\sigma = (x - \zeta^\sigma)(x - \bar{\zeta}^\sigma) \equiv 1 \pmod{q^2}, \quad \text{for each } \sigma \in G^+,$$

we have

$$\gamma^{-1}\delta^q \equiv 1 \pmod{q^2},$$

and finally

$$\gamma \equiv \delta^q \pmod{q^2}.$$

□

Now, the last lemma is proved.

Proof of Lemma 3.4. First,

$$\zeta^{-\frac{p+1}{2}} + \zeta^{\frac{p+1}{2}} = \zeta^{-\frac{p+1}{2}}(1+\zeta) = \zeta^{-\frac{p+1}{2}} \cdot \frac{1-\zeta^2}{1-\zeta}$$

is a cyclotomic unit and is contained in C^+. Then the above lemma says that

$$\zeta^{-\frac{p+1}{2}} + \zeta^{\frac{p+1}{2}} \equiv \delta^q \pmod{q^2\mathcal{O}_{K^+}},$$

and hence

$$1 + \zeta = \zeta^{rq} \cdot \delta^q \pmod{q^2\mathcal{O}_K},$$

where r is an integer so that $rq \equiv \frac{p+1}{2} \pmod{p}$.

□

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*. Academic Press, London, 1964.

[2] J. Daems, *A Cyclotomic Proof of Catalan's Conjecture*. manuscript Sept. 29, 2003, http://www.math.leidenuniv.nl/ jdaems/scriptie/Catalan.pdf.

[3] Preda Mihăilescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, J. reine angrew. Math. 572 (2004), 167-195.

[4] Yuri F. Bilu. *Catalan's Conjecture(after Mihăilescu)*. S'eminaire Bourbaki, 909, 2002-2003.

[5] René Schoof, *Catalan's Conjecture*. Springer-Verlag, London, 2008.

[6] Joseph H. Silverman and John Tate, *Rational Points on elliptic curves*. Springer-Verlag, New York, 1992.

[7] Lawrence C. Washington, *Introduction to Cyclotomic Fields*. Springer-Verlag, New York, 1982.

[8] V. A. Lebesque. *Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$*. Nouvelles annales de mathématiques, 9:178-181, 1850.

[9] Ko Chao. *On the Diophatine equation $x^2 = y^n + 1, xy \neq 0$*. Scientia Sinica, 14:457-460, 1965.