ARITHMETIC OF CYCLOTOMIC FIELDS

AND

FERMAT-TYPE EQUATIONS

Thesis by

Sankar Sitaraman

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1994

Submitted May 24, 1994

To my parents and sisters

Acknowledgements

I am grateful to my adviser Dr. Dinakar Ramakrishnan for his guidance and encouragement throughout. During my research I have benefited immensely from his suggestions and infectious enthusiasm for the subject. I would like to thank Drs. R. Wilson, W. Luxemburg and Dr. R. Valenza for agreeing to be on my doctoral committee. Thanks also for the math department, and the Bohnenblust travel fund, for their support. I am indebted to Shekhar and Farshid for sharing their knowledge and enthusiasm for number theory with me, and their comments and suggestions were very useful during my research. I am also grateful to Drs. J. Tilouine, D. Thakur, and L. Washington for their interest and helpful comments regarding my work. I am thankful to Shujuan, Jude, and Alex of the number theory group for their friendship and conversations. I thank Larry, K.M, Wayne, Brian, and other fellow grad students for their friendship and company during these long years. I am grateful to Sara, Marge, Christine and Cheri for their help and cheerfulness. Many thanks are also due to the Millikan library staff for their timely help, especially in digging up old journals. To my parents and my sisters, I owe everything. This thesis is dedicated to them as my humble offering. And to Ivett, for everything.

ABSTRACT

Let l be any odd prime, and ζ a primitive l-th root of unity. Let C_l be the l-Sylow subgroup of the ideal class group of $\mathbf{Q}(\zeta)$. The Teichmüller character $\omega : \mathbf{Z}_l \to \mathbf{Z}_l^*$ is given by $\omega(x) \equiv x \pmod{l}$, where $\omega(x)$ is a $p-1$-st root of unity, and $x \in \mathbf{Z}_l$. Under the action of this character, C_l decomposes as a direct sum of $C_l^{(i)}$, where $C_l^{(i)}$ is the eigenspace corresponding to ω^i. Let the order of $C_l^{(3)}$ be l^{h_3}. The main result of this thesis is the following: *For every $n \geq max(1, h_3)$, the equation $x^{l^n} + y^{l^n} + z^{l^n} = 0$ has no integral solutions (x, y, z) with $l \nmid xyz$.* The same result is also proven with $n \geq max(1, h_5)$, under the assumption that $C_l^{(5)}$ is a cyclic group of order l^{h_5}. Applications of the methods used to prove the above results to the second case of Fermat's last theorem and to a Fermat-like equation in four variables are given.

The proof uses a series of ideas of H. S. Vandiver ([V1],[V2]) along with a theorem of M. Kurihara [Ku] and some consequences of the proof of Iwasawa's main conjecture for cyclotomic fields by B. Mazur and A. Wiles [MW]. In [V1] Vandiver claimed that the first case of Fermat's Last Theorem held for l if l did not divide the class number h^+ of the maximal real subfield of $\mathbf{Q}(e^{\frac{2\pi i}{l}})$. The crucial gap in Vandiver's attempted proof that has been known to experts is explained, and complete proofs of all the results used from his papers are given.

CONTENTS

INTRODUCTION

This thesis grew out of an attempt to understand and fix a paper by H. S. Vandiver. In [V1] Vandiver claimed that the first case of Fermat's Last Theorem held for l if l did not divide the class number h^+ of K^+, the maximal real subfield of the l-th cyclotomic field K. In other words, when $l \nmid h^+$, if x, y, z are non-zero integers such that

$$x^l + y^l + z^l = 0, \tag{I1}$$

then $l|xyz$. It has been known for some time to experts that his paper contained mistakes, some of which were serious. In chapter 2 we explain the crucial gap in Vandiver's attempted proof. In fact we show that the first case of Fermat's last theorem can be proven *without his hypothesis* $l \nmid h^+$, provided we make an assumption regarding the existence of certain prime ideals which seems to be implicit in Vandiver's paper [V1]. (Though it has been conjectured by Kummer and Vandiver that l never divides h^+, and a large amount of numerical evidence exists, no property of the cyclotomic field has been found which suggests that this should be true).

However, two theorems that Vandiver used in this paper [V1], namely Theorems A and B of chapter 3, are correct. Theorem A says that the prime ideals P such that $P|(x+\zeta y)$, where x, y, z satisfy equation (I1), split completely in the Kummer extension over K generated by the l-th roots of certain circular units E_m. Theorem B, which was originally used as a tool to prove explicit reciprocity laws, relates the splitting of prime ideals in extensions generated by l-th roots of such units to certain logarithmic derivatives and l-parts of Bernoulli numbers. In fact, it is shown in chapter 2 that the l- parts of these Bernoulli numbers give the order of the certain subgroups $C_l^{(i)}$ (defined below) of the class group C_l. In chapter 3 and the appendix we provide *complete* proofs of all the results we use from his

(Vandiver's) papers, even if some of them are well known to experts. In chapter 4, we show that theorems A and B can be combined with some recent work on the structure of the ideal class group of the cyclotomic field to prove a result about the first case of Fermat's Last Theorem *without the assumption that* $l \nmid h^+$.

Let l be any odd prime, and ζ a primitive l-th root of unity. Let C_l be the l-Sylow subgroup of the ideal class group of $\mathbf{Q}(\zeta)$. Under the action of the Teichmüller character ω, C_l decomposes as a direct sum of $C_l^{(i)}$, where $C_l^{(i)}$ is the eigenspace corresponding to ω^i. Let $|C_l^{(i)}| = l^{h_i}$.

Kurihara [Ku] (and, independently, R. Greenberg) proved that $C_l^{(3)}$ is cyclic. One of the consequences of the proof of Iwasawa's main conjecture for cyclotomic fields by B. Mazur and A. Wiles [MW] is that for $i = 2, 4, ..., l-3$, $|C_l^{(i)}| = |((A^*)_l^+/CU_l^+)^{(i)}|$, where CU^+ is the group of real cyclotomic units, $(A^*)^+$ is the group of real units, and $((A^*)_l^+/CU_l^+)^{(i)}$ is defined in the same way as $C_l^{(i)}$. We use these and other facts known about the structure of C_l along with theorems A and B to prove the first case of Fermat's Last Theorem for certain exponents.

More precisely, the main theorem of this thesis, proven in chapter 2, is the following:

Theorem. *For every* $n \geq max(1, h_3)$, *the equation*

$$x^{l^n} + y^{l^n} + z^{l^n} = 0 \qquad (I2)$$

has no integral solutions (x, y, z) *with* $l \nmid xyz$.

For $n = 1$, the above theorem is established in [Ku] using a different result of Vandiver. The first result about Fermat's Last Theorem for higher powers of l was given by Maillet [Ri, p. 205]. He gave the lower bound $u+1$ for n in (I2), where u is the largest power of l dividing the class number h. Using Faltings' theorem proving the Mordell conjecture, one knows that the number of rational, and hence integral

solutions of equation (I1) is finite. Since any solution of (I2) provides a solution of (I1), we find that equation (I2) can have integral solutions only for finitely many exponents l^n. In fact, Filaseta [Fi] has shown, using the same theorem, that for every integer $k \geq 3$, there exists an integer $M(k)$ such that if $m > M(k)$ then there are no non-trivial solutions for $x^{mk} + y^{mk} + z^{mk} = 0$. Washington [Wa2] gives the lower bound $max(1, u^* - \sqrt{l} + 3)$ for n in (I2), where u^* is the highest power of l dividing $h^- = h/h^+$, the first factor of the class number. He used the method of Eichler [E], who proved that if the first case fails for l, then $l^{[\sqrt{l}]-1}$ divides the first factor of the class number. Eichler's result has been improved by McCallum [Mc]. Granville and Powell [GP] have also given a strong lower bounds for n in (I2).

In chapter 5, the main theorem discussed above is proven with $n \geq max(1, h_5)$, where l^{h_5} is the order of $C_l^{(5)}$, under the further assumption that $C_l^{(5)}$ is cyclic. In chapters 6 and 7 we give applications of the methods of the previous chapters to the second case of Fermat's last theorem and to a Fermat-like equation in four variables, respectively.

CHAPTER 0

NOTATION AND PRELIMINARIES

l is a prime number with $l > 5$.

ζ is a primitive l-th root of unity. $\lambda = 1 - \zeta$.

$K = \mathbf{Q}(\zeta)$ is the cyclotomic field.

$A = \mathbf{Z}[\zeta]$ and A^* is the group of units in A.

$G = Gal(K/\mathbf{Q})$.

σ is a generator of G and $\sigma(\zeta) = \zeta^r$, where

r is a primitive generator of $(\mathbf{Z}/l\mathbf{Z})^*$.

$A - (1 - \zeta)$ means the set of elements of A which are prime to $(1 - \zeta)$.

$\Phi(x) = 1 + x + ... + x^{l-1}$.

$\sigma_a(\zeta) = \zeta^a$.

C is the ideal class group of K.

h is the order of C.

$K^+ = \mathbf{Q}(\zeta + \zeta^{-1}) =$ Maximal real subfield of K.

C_l is the l–Sylow subgroup of C.

A^+, C^+, h^+, and C_l^+ are defined similarly.

If I is an ideal in A, then $[I]$ is its ideal class in C.

$N(I)$ is the absolute norm of the ideal I.

If n is an integer, n' is an integer such that $nn' \equiv 1 \pmod{l}$.

Teichmüller Character.

Define ω, the Teichmüller character, as follows: Given $x \in \mathbf{Z}_l, \omega(x)$ is the root of unity in $\mathbf{Z}_l$ such that

$$\omega(x) \equiv x \pmod{l}.$$

Sometimes we will use the isomorphism $(\mathbf{Z}_l/l\mathbf{Z}_l)^* \simeq (\mathbf{Z}/l\mathbf{Z})^* \simeq G$ (where the second isomorphism depends on choice of the primitive generator r of $(\mathbf{Z}/l\mathbf{Z})^*$) and write $\omega(\sigma)$ instead of $\omega(r)$, and so on.

Bernoulli numbers:

The Bernoulli numbers are defined by:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \mathbf{B}_n \frac{t^n}{n!}.$$

The generalized Bernoulli numbers:

$\mathbf{B}_{1,\omega^j}$ is the generalized Bernoulli number defined by:

$$\sum_{a=1}^{l-1} \frac{\omega^j(a) x e^{ax}}{e^{(l-1)x} - 1} = \sum_{n=0}^{\infty} \mathbf{B}_{n,\omega^j} \frac{x^n}{n!}.$$

The Jacobi sum and a Stickelberger type relation

Let $p \neq l$ be a prime, $p \equiv 1 \pmod{l}$. Let μ_{p-1} be the group of $p-1$-st roots of unity. Let χ_1, χ_2 be any characters from $(\mathbf{Z}/p\mathbf{Z})^* \to \mu_{p-1}$. The Jacobi sum $J(\chi_1, \chi_2)$ is defined by

$$J(\chi_1, \chi_2) = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} -\chi_1(x)\chi_2(1-x). \tag{0.1}$$

Let ω_p denote the Teichmüller character corresponding to p. Let $\chi_p = {\omega_p}^{-\frac{p-1}{l}}$. Let $\overline{n}$ be the least nonnegative residue modulo l of $n \in \mathbf{Z}$, and n' an integer such

that $nn' \equiv 1 \pmod{l}$. For n_1, n_2 integers, define $[n_1, n_2] = \frac{\overline{n_1}+\overline{n_2}-\overline{n_1+n_2}}{l}$. Then we have the following Stickelberger type relation (cf. [L] p. 13, Fac 3) for any prime ideal P of A above p and integers n_1, n_2 such that $l \nmid (n_1 + n_2)$:

$$\prod_{k=1}^{l-1} (\sigma_{k'}(P))^{[n_1 k, n_2 k]} = (J(\chi_p^{n_1}, \chi_p^{n_2})) \tag{0.2}$$

Note: $J(\chi_p^{n_1}, \chi_p^{n_2}) \in \mathbf{Z}[\zeta]$. Moreover, if we choose our primitive l-th root of unity ζ suitably, then the Jacobi sum defined by (0.1) above is the same as the classical *Jacobi cyclotomic function* (cf. for instance, [Hi, p. 343] or [Ri, p. 117]) multiplied by -1. But this difference in sign between the two sums will have no effect on our proof since they generate the same principal ideal.

Real Cyclotomic Units

Kummer Units: Recall that r is a primitive root mod l and σ a generator of $Gal(K/\mathbf{Q})$. The *Kummer Unit* δ is defined by:

$$\delta = \sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}} = \zeta^{\frac{1-r}{2}} \frac{(1-\zeta^r)}{(1-\zeta)} .$$

Note that δ is a unit in $A^+ = \mathbf{Z}[\zeta + \zeta^{-1}]$ because

$$\delta^2 = \left(\frac{1-\zeta^r}{1-\zeta}\right)\left(\frac{1-\zeta^r}{1-\zeta}\right)^{\sigma-1}$$

and $\left(\frac{1-\zeta^r}{1-\zeta}\right)$ is of the form $\zeta^a \epsilon$ with $\epsilon \in A^+$, $a \in \mathbf{Z}$, because it is a unit in A.

Definition:

$$E_n = \prod_{k=1}^{l-1} (\sigma^{-k}(\delta))^{r^{nk}}. \tag{0.3}$$

Note: This definition of E_n is not standard. For instance, the E_n defined in [Ri, p.82] is actually the square root of the E_n defined above. But all the properties of E_n that we need will follow easily from those of $\sqrt{E_n}$ and vice versa.

The l-th power residue symbol

Definition: Let Q be a prime ideal of A, $Q \neq (\lambda)$. If $\alpha \in A, \alpha \notin Q$, then set

$$\left\{\frac{\alpha}{Q}\right\} = \zeta^a, \tag{0.4}$$

where ζ^a is the unique l-th root of unity such that: $\alpha^{(N(Q)-1)/l} \equiv \zeta^a \pmod{Q}$,

where $N(Q)$ is the (absolute) norm of Q.

It is easy to see that $\left\{\frac{\alpha}{Q}\right\}$ is multiplicative in α *and* Q. Also, we have:

$$\left\{\frac{\alpha}{J}\right\} \alpha^{1/l} = \left(\frac{K(\alpha^{1/l})/K}{J}\right)(\alpha^{1/l}),$$

where J is any ideal of A with $(\lambda) \nmid J$, $\left(\frac{K(\alpha^{1/l})/K}{J}\right)$ is the generalized Frobenius element. So in this case the power residue symbol gives the action of the *Artin map* $J \mapsto \left(\frac{K(\alpha^{1/l})/K}{J}\right)$. *(For details see [Ca-F], exercise 1, pp. 348-349.)*

Congruences of rational numbers

We will write, for two rational numbers $\frac{k}{n}$, $\frac{f}{g}$, and $M \in \mathbf{Z}$, $\frac{k}{n} \equiv \frac{f}{g} \pmod{M}$ if $n \not\equiv 0 \pmod{M}$, $g \not\equiv 0 \pmod{M}$ and $kg - fn \equiv 0 \pmod{M}$.

CHAPTER 1

LOGARITHMIC DERIVATIVES

In this chapter we collect some results that we will need later on, about the logarithmic derivatives of polynomials. Some of these are standard, and we give proofs of the non-obvious assertions, most of which are due to Kummer and Vandiver.

For any $f \in \mathbf{Z}[x]$, $f(1) \not\equiv 0 \pmod{l}$ and any integer $k \geq 1$, define the (*formal*) logarithmic derivative Δ with values in $\mathbf{Q}$ by:

$$\Delta^{(k)}(f) = \frac{d^k}{dv^k}(log(f(e^v)))\Big|_{v=0}.$$

Lemma 1.1. *For* $1 \leq k < l-1$, $G(x), F(x) \in \mathbf{Z}[x]$ *with* $G(1) \not\equiv 0 \pmod{l}$,

$$F(\zeta) = G(\zeta) \Rightarrow \Delta^{(k)}(F) \equiv \Delta^{(k)}(G) \pmod{l}.$$

Proof.

Let $\Phi(x) = 1 + x + x^2 + ... + x^{l-1}$ be the minimal polynomial of ζ. Then

$$F(\zeta) = G(\zeta) \Rightarrow F(e^v) = G(e^v) + \Phi(e^v)U(e^v), \quad U(x) \in \mathbf{Z}[x].$$

Let $H = \Phi W$, where $W = U/G$.

For any $S(x) \in \mathbf{Z}[x]$, let

$$d_0^k(S) = \frac{d^k}{dv^k}(S(e^v))\Big|_{v=0}.$$

Claim:

$$d_0^k(H) \equiv 0 \pmod{l} \text{ for } k \geq 0.$$

Proof of claim: Since $l \mid \Phi(1), d_0^0(H) \equiv 0 \pmod{l}$.

$$\text{For } 1 \leq k \leq l-1, d_0^k(H) = \sum_{i=0}^{k} \binom{k}{i} (d_0^i \Phi(e^v))(d_0^{k-i} W)$$
$$\equiv \sum_{i=0}^{k} \binom{k}{i} \left(\sum_{n=0}^{l-1} n^i \right) d_0^{k-i}(W). \pmod{l}$$

Note that the denominator of $d_0^{k-i}(W)$ is a power of $G(1)$ which is prime to l by assumption; moreover, $\sum_{n=0}^{l-1} n^i \equiv 0 \pmod{l}$ for $i = 1, 2, .., k$. Thus $d_0^k(H) \equiv 0 \pmod{l}$, for $1 \leq k \leq l-1$. Hence the claim.

$$\text{Now, } \frac{d^k}{dv^k} log \frac{F(e^v)}{G(e^v)} = \frac{d^k}{dv^k} log\ (1 + H(e^v)) = \frac{d^{k-1}}{dv^{k-1}} \left(\frac{e^v H'(e^v)}{1 + H(e^v)} \right) = S/T,$$

where S is a $\mathbf{Q}$-linear combination of $\frac{d^i}{dv^i} H(e^v)$ for $0 \leq i \leq k$, and T is an integral power of $1 + H(e^v)$. Thus by the claim above, when $v = 0, S \equiv 0 \pmod{l}$ and $T \equiv 1 \pmod{l}$.

Lemma 1.1 follows.

The definition of Δ acting on algebraic numbers

Let $\alpha \in A = \mathbf{Z}[\zeta]$ be such that $(1-\zeta) \nmid (\alpha)$. Write $\alpha = f(\zeta)$, with $f \in \mathbf{Z}[x]$. Then $f(1) \not\equiv 0 \pmod{l}$ and $\Delta^{(k)}(f)$ is defined.

For $1 \leq k < l-1$, set $\Delta^{(k)}(\alpha) = \Delta^{(k)}(f)$. This definition is independent modulo l of the choice of f by Lemma 1.1.

Lemma 1.1 can be generalized as follows:

Lemma 1.2. ([V4, pp. 401-408]) *Let $F, G \in \mathbf{Z}[x]$. Assume:*

(1) $F(\zeta) = G(\zeta)$;

(2) $G(1) \not\equiv 0 \pmod{l}$;

(3) *For a positive integer i,* $F(1) \equiv G(1) \pmod{l^{i+1}}$.

Then for any positive integer k prime to $l-1$,

$$\Delta^{(kl^i)}(F) \equiv \Delta^{(kl^i)}(G) \ (mod\ l^{i+1}).$$

A proof is given in the Appendix. In fact, a stronger version of this result, i.e, without assuming condition (3), was stated by Kummer [K2, p. 54] and Hilbert [Hi, p. 353].

Lemma 1.3. [V4, p.399] *Let $f \in \mathbf{Z}[x]$ be such that $f(1) \not\equiv 0 \pmod{l}$. Then for any positive integer k prime to $l-1$, and all positive integers i,*

$$\Delta^{(kl^i)}(f) \equiv \Delta^{(kl^{i+1})}(f) \ (mod\ l^{i+1}).$$

Proof.

Throughout this proof, the congruences are modulo l^{i+1}.

We have

$$\Delta^{(kl^{i+1})}(f) = \frac{d^{kl^{i+1}-1}}{dv^{kl^{i+1}-1}} \left(\frac{\frac{d}{dv}(f(e^v))}{f(e^v)} \right) \Bigg|_{v=0}.$$

Now,

$$\begin{aligned} &(f(1))^{l^{i+1}} \frac{d^{kl^{i+1}-1}}{dv^{kl^{i+1}-1}} \left(\frac{\frac{d}{dv}(f(e^v))}{f(e^v)} \right) \Bigg|_{v=0} \\ &= \frac{d^{kl^{i+1}-1}}{dv^{kl^{i+1}-1}} \left((f(e^v))^{l^{i+1}} \frac{\frac{d}{dv}(f(e^v))}{f(e^v)} \right) \Bigg|_{v=0}. \end{aligned} \tag{1.1}$$

Let

$$\left((f(e^v))^{l^{i+1}} \frac{\frac{d}{dv}(f(e^v))}{f(e^v)}\right) = a_0 + a_1 e^v + a_2 e^{2v} + ... + a_m e^{mv},$$

where $a_0, a_1, ..., a_m \in \mathbf{Z}$.

Then

$$\frac{d^{kl^{i+1}-1}}{dv^{kl^{i+1}-1}} \left((f(e^v))^{l^{i+1}} \frac{\frac{d}{dv}(f(e^v))}{f(e^v)}\right)\Bigg|_{v=0} = a_1 + 2^{kl^{i+1}-1} a_2 + ... + m^{kl^{i+1}-1} a_m.$$

Because for any integer n, $n^{kl^{i+1}} \equiv n^{kl^i}$, we get from (1.1)

$$(f(1))^{l^{i+1}} \frac{d^{kl^{i+1}-1}}{dv^{kl^{i+1}-1}} \left(\frac{\frac{d}{dv}(f(e^v))}{f(e^v)}\right)\Bigg|_{v=0} \equiv \frac{d^{kl^i-1}}{dv^{kl^i-1}} \left((f(e^v))^{l^{i+1}} \frac{\frac{d}{dv}(f(e^v))}{f(e^v)}\right)\Bigg|_{v=0}$$

Dividing both sides by $(f(1))^{l^{i+1}}$, we get Lemma 1.3. $\mathcal{QED}$.

For $\alpha \in A$, let $\overline{\alpha}$ denote the complex conjugate of α.

Proposition 1.4. *Let $\alpha \in A-(1-\zeta)$. Then for positive integers $1 \leq n < l-1, i \geq 1$, we have*

$$\Delta^{(n)}(\alpha^i) \equiv i\Delta^{(n)}(\alpha) \pmod{l}. \qquad (a)$$

$$\Delta^{(n)}(\overline{\alpha}) \equiv (-1)^n \Delta^{(n)}(\alpha) \pmod{l} \qquad (b)$$

$$\Delta^{(n)}(\alpha^\sigma) \equiv r^n \Delta^{(n)}(\alpha) \pmod{l} \qquad (c)$$

Proof. (a) is straightforward. (b) follows from (c) by applying $\sigma^{\frac{l-1}{2}}$.

We will now prove the following claim, from which (c) will follow if we observe that for $\alpha = f(\zeta) \in \mathbf{Z}[\zeta]$, with $f \in \mathbf{Z}[x], \sigma(\alpha) = f(\zeta^r)$.

Claim ([V5, p. 619]) For $n \in \mathbf{Z}, n \geq 1$, and $F \in \mathbf{Z}[x]$,

$$\frac{d^n}{dv^n} log\ F(e^{rv})\Big|_{v=0} = r^n \frac{d^n}{dv^n} log\ F(e^v)\Big|_{v=0} \qquad (1.2)$$

Let $D = \frac{d}{dv}$. To prove the claim, first we prove by induction on n that

$$D^{(n)} log\ F(e^{rv}) = r^n G(e^{rv}) \qquad \text{for some } G \in \mathbf{Q}[x].$$

Clearly this is true for $n = 2$. Suppose we can write

$$D^{(n-1)} log\ F(e^{rv}) = r^{n-1} \frac{A(e^{rv})}{B(e^{rv})} \text{ for some } A, B \in \mathbf{Z}[x]. \tag{1.3}$$

Then we have

$$D^{(n)} log F(e^{rv}) = r^n (\frac{BD(A) - AD(B)}{B^2}) = r^n G(e^{rv}). \tag{1.4}$$

Now, setting $r = 1$ in (1.3) and differentiating, we get

$$D^{(k)} log\ F(e^v) = G(e^v). \tag{1.5}$$

Setting $v = 0$ in (1.4) and (1.5) we get (1.2).

$\mathcal{QED}$.

Proposition 1.5. *Let $\eta \in A^*$. For every odd integer $1 < m < l - 1$, we have*

$$\Delta^{(m)}(\eta) \equiv 0 \pmod{l}.$$

Proof. By a basic result, $\eta = \zeta^k \epsilon$, where $k \in \mathbf{Z}$ and ϵ is a real unit. Clearly, when $m > 1$, $\Delta^{(m)}(\zeta^k) \equiv 0 \pmod{l}$. By Prop 1.4,(b), we have

$$\Delta^{(m)}(\epsilon) = \Delta^{(m)}(\overline{\epsilon}) \equiv -\Delta^{(m)}(\epsilon) \pmod{l}.$$

$$\Rightarrow \Delta^{(m)}(\epsilon) \equiv 0 \pmod{l}.$$

Hence, after using Lemma 1.1 we get Prop 1.5.

Remark: Note that $\Delta^{(1)}(\zeta^k) \equiv k \pmod{l}$.

CHAPTER 2

AN UPDATED VERSION OF VANDIVER'S 'THEOREM'

In [V2, pp. 118-122], Vandiver tried to prove that $l \nmid h^+$ implies the first case of Fermat's last theorem. In this chapter, we give the method of his attempted proof. We actually prove the first case *without assuming* $l \nmid h^+$, but modulo another assumption which seems to be implicit in Vandiver's paper. Our proof follows closely the method of Vandiver, but we also indicate a shortcut which simplifies the proof considerably. It is not clear how the other assumption can be satisfied or eliminated.

Recall that r is a primitive root modulo the odd prime l. Also, ζ is a primitive l-th root of 1. The l-Sylow subgroup C_l of the ideal class group A of $\mathbf{Q}(\zeta)$ decomposes into a direct sum of eigenspaces $C_l^{(i)}$ which are defined as follows:

$$C_l^{(i)} = \{\ x \in C_l \mid \sigma(x) = x^{\omega^i(\sigma)} = x^{\omega^i(r)} = x^{r^i} y^l \text{with } y \in C_l\ \}.$$

Theorem 2.1.

$$\textit{If} \quad x^l + y^l + z^l = 0 \tag{2.1}$$

is satisfied with $x, y, z \in \mathbf{Z}$, $l \nmid xyz$, *then* $P \nmid (z)$ *for any prime ideal* P *whose ideal class generates* $C_l^{(3)}$.

Remark: It is not necessary that P be a prime ideal. Assuming that P is prime simply makes matters easier.

Proof.

Assume equation (2.1) is possible, with $l \nmid xyz$. Changing z to $-z$, equation (2.1) can be written as

$$\prod_{i=0}^{l-1}(x+\zeta^i y) = z^l. \tag{2.1a}$$

Recall that $\lambda = 1-\zeta$. We have

Lemma 2.1a.

(1) *The ideals* $(x+\zeta^i y)$ *in equation (2.1a) are prime to each other and* (λ).

(2) $(x+\zeta^j y) = I_j^l$, *where for* $1 \le j \le l-1$, I_j *is an ideal in* A.

(3) $(x+y) = v^l$ *where* $v \in \mathbf{Z}$.

(4) *If* P *is a prime ideal divisor of* I_j *for some* j, *then* $N(P) = p$ *for some prime number* p *such that* $p \equiv 1 \pmod{l}$ *and* $p \mid \dfrac{x^l+y^l}{x+y}$ *but* $p \nmid x+y$.

Proof.

(1). Suppose P is a prime ideal that divides both $(x+\zeta^{i_1}y)$ and $(x+\zeta^{i_2}y)$, where $i_1 \neq i_2$. Then P divides $(\zeta^{i_1}y - \zeta^{i_2}y)$, which means $P|(\lambda)$ or $P|(y)$. But $P|(\lambda) \Rightarrow (\lambda)|(z) \Rightarrow l|z$, which is impossible. So assume $P|(y)$. Now we also have $P|(\zeta^{i_2}(x+\zeta^{i_1}y) - \zeta^{i_1}(x+\zeta^{i_2}y)) \Rightarrow P|(\lambda)$ or $P|(x)$. Since we already showed $P \nmid (\lambda)$, we should have $P|(x)$ and $P|(y)$, which is impossible because $(x,y)=1$.

(2). Follows from equation (2.1a), (1) above, and the fact that A, being a Dedekind domain, admits unique factorization by ideals.

(3). We have

$$x+y = \frac{z^l}{N(x+\zeta y)} = \frac{z^l}{N(I_1^l)} = \frac{z^l}{N(I_1)^l} = v^l, \text{ where } v = \frac{z}{N(I_1)}.$$

(4). Fix $j, 1 \leq j \leq l-1$. If P is a prime ideal such that $P|(x+\zeta^j y)$, then $\sigma_n(P)|(x+\zeta^{jn}y)$. Now, $j \mapsto jn$ is a permutation of $(\mathbf{Z}/l\mathbf{Z})^*$. From (1), $(x+\zeta^i y)$ are relatively prime for $i = 1, 2, .., l-1$. Hence we get $l-1$ prime ideals lying over $(p) = P \cap A$, which means (p) splits completely in A, because K has degree $l-1$ over $\mathbf{Q}$. Thus, $N(P) = p \equiv 1 \pmod{l}$. Also, it follows from (1) that $p \nmid (x+y)$.

$\mathcal{QED}$.

Henceforth, let $I_1 = I$. We have from Lemma 2.1a (1),

$$(x+\zeta y) = I^l. \tag{2.1b}$$

As is well known, Kummer proved that if I is principal, then (2.1) is impossible. Therefore, we may (and will) assume that I is nonprincipal. Thus $[I]$ has order precisely l in the ideal class group C and l is irregular. Let $\mathbf{B}_{i_1}$, $\mathbf{B}_{i_2}$, ...$\mathbf{B}_{i_s}$, with $\{i_1, ..., i_s\} \subset \{2, 4, ..., l-1\}$, be the Bernoulli numbers divisible by l.

Similarly to the definition of the $C_l^{(i)}$, let V_l be the $\mathbf{Z}/l\mathbf{Z}$ vector space C_l/C_l^l, and $V_l^{(i)}$ the eigenspace consisting of elements on which G acts via ω^i.

We have the following criterion due to Herbrand and Ribet.

Theorem. ([R. p. 151],[He. p. 430])

$$V_l^{(i)} \neq 0 \Leftrightarrow l|\mathbf{B}_{l-i}.$$

Since $V_l^{(i)} = 0 \Leftrightarrow C_l^{(i)} = 0$, we can write

$$C_l = C_l^{(l-i_1)} \oplus ..... \oplus C_l^{(l-i_s)}.$$

It is a well known result of Kummer (cf. for instance, [Ri], p. 125) that if equation (2.1) is true with $l \nmid xyz$, then $l | \mathbf{B}_{l-3}$. Hence we may let $l - i_1 = 3$ in the above decomposition. (In fact, this is not essential to our proof.)

The following result of Kurihara is a consequence of the proof of the main conjecture for cyclotomic fields due to Mazur-Wiles [MW], the computation of $K_4(\mathbf{Z})$ by Lee and Sczcarba, and the surjectivity, due to C. Soulé, for $l > 2$ of the l-adic Chern class map

$$c_l : K_4(\mathbf{Z}) \otimes \mathbf{Z}_l \longrightarrow H^2(\mathbf{Z}[1/l], \mathbf{Z}_l(3)).$$

Theorem. ([Ku], p. 223): $C_l^{(3)}$ *is cyclic.*

Remark: This fact, which was also independently observed by R. Greenberg, is essential to our proof.

Decomposing each $C_l^{(i)}$ in terms of its cyclic summands, we get

$$C_l = C_l^{(3)} \oplus M_1 \oplus ..... \oplus M_n,$$

where n is a positive integer and each M_j is a cyclic subgroup of some $C_l^{(i)}$ with $i \neq 3$.

Suppose P is a prime ideal such that the ideal class$[P]$ generates $C_l^{(3)}$, and P divides (z). So P has to divide $x + \zeta^k y$ for a unique $k \in \{1, 2, ..., l\}$. By choosing ζ suitably, we may assume that $k = 1$. By the Tchebotarev density theorem, we choose prime ideals Q_j for $j = 1, 2, .., n$, representing an ideal class which generates M_j.

As already mentioned, $[I]$ has order exactly l in C_l and thus $[I] \in C_l$. Hence we have

$$[I] = [P]^m [Q_1]^{k_1} .... [Q_n]^{k_n}, \text{ where } m, k_1, ..., k_n \in \mathbf{Z}^{\geq 0}. \tag{2.2}$$

This gives

$$I = P^m Q_1^{k_1} .... Q_n^{k_n} \frac{(\gamma)}{(\delta)}, \text{ where } \gamma, \delta \in A. \tag{2.3}$$

Claim: γ, δ can be chosen so that $(\lambda) \nmid (\gamma), (\lambda) \nmid (\delta)$.

Indeed, since $(\lambda) \nmid I, P, Q_1, .., Q_m$, we have $v_\lambda(\gamma) = v_\lambda(\delta)$. Then we can replace γ, δ by $\frac{\gamma}{\lambda^{v_\lambda(\gamma)}}, \frac{\delta}{\lambda^{v_\lambda(\delta)}}$ respectively, to get the claim. But note that we cannot make (γ) and (δ) relatively prime. Thus, the ideal P need not *a priori* divide the ideal I. In fact, it is not clear that there would be any ideal in the class $C_l^{(3)}$ which divides I. The crucial mistake made by Vandiver in [V1] is that in a similar situation he seems to assume P divides I.

Consequently,

$$I^l = (x + \zeta y) = P^{ml} Q_1^{k_1 l} ... Q_n^{k_n l} (\frac{\gamma}{\delta})^l. \tag{2.4}$$

This gives the following relation in C_l, written additively:

$$[P]^{ml} + [Q_1]^{k_1 l} + ... + [Q_j]^{k_n l} = 0.$$

Since C_l is a direct sum $C_l^{(3)} \oplus M_1 \oplus .... \oplus M_n$, this implies that $[P]^{ml}, [Q_1]^{k_1 l}, ..., [Q_n]^{k_n l}$ must all be trivial in C_l. So we can write

$$P^{ml} = (\varpi), \text{ and } Q_j^{k_j l} = (\alpha_j), \text{ for some } \varpi, \alpha_1, ..., \alpha_n \in A = \mathbf{Z}[\zeta].$$

By Prop. 1.4a, we know that $\Delta^{(n)}$ vanishes on l-th powers of elements in $A - (1 - \zeta)$. Note that in equation (2.4), the numbers occurring on the right-hand side are not divisible by $(1 - \zeta)$, because $(1 - \zeta) \nmid (x + \zeta y)$. Thus $\Delta^{(n)}$ is

defined for all of them. By the remark above, $\Delta^{(n)}(\gamma^l) \equiv 0 \pmod{l}$. By Prop. 1.5, $\Delta^{(n)}(\eta) \equiv 0 \pmod{l}$, $\forall n \in \{3, 5, ..., l-3\}$. Taking $n = 3$ and using Lemma 1.1, we get the following by the additivity of the logarithmic derivative:

$$\Delta^{(3)}(x + \zeta y) \equiv \Delta^3(\varpi) + \left(\sum_{j=1}^{n} \Delta^{(3)}(\alpha_j) \right) \pmod{l}. \tag{2.5}$$

We claim that $\Delta^{(3)}(x + \zeta y) \equiv \Delta^3(\varpi) \pmod{l}$.

The claim follows from the following

Proposition 2.2.

$$\Delta_0^{(3)}(\alpha_j) \equiv 0 \pmod{l}, \text{ for } j = 1, 2, .., n.$$

Proof. Fix such a j. We have $[Q_j] \in C_l^{(i)}$ for some $i \neq 3$. Now, from the definition of $C_l^{(i)}$, $Q_j^\sigma = Q_j^{\omega^i(r)}(\nu_j)$ with $\nu_j \in K^*$. Note that (ν_j) is prime to (λ), because Q_j and hence Q_j^σ are prime to (λ). Since $\omega^i(r) \equiv r^i \pmod{l}$, let $\omega^i(r) = r^i + a_j l$. We get

$$Q_j^\sigma = Q_j^{r^i} Q_j^{a_j l}(\nu_j) \Rightarrow \left(Q_j^\sigma\right)^{k_j l} = (\alpha_j^{r^i} \theta_j^l), \quad \theta_j \in K^*, (\theta_j, \lambda) = 1.$$

On the other hand we have

$$\left(Q_j^\sigma\right)^{k_j l} = (\alpha_j)^\sigma.$$

Hence we get

$$\alpha_j^\sigma = \xi_j \alpha_j^{r^i} \theta_j^l, \quad \xi_j \in A^*. \tag{2.6}$$

From Prop 1.4,(c) we have, for $n \geq 1$:

$$\Delta^{(3)}(\alpha_j)^\sigma \equiv r^3 \Delta^{(3)}(\alpha_j) \pmod{l}. \tag{2.7}$$

Using (2.6) in conjunction with Lemma 1.1, Prop 1.4(a) and Prop 1.5, we get:

$$\Delta^{(3)}(\alpha_j)^\sigma \equiv r^i \Delta^{(3)}(\alpha_j) \pmod{l}. \tag{2.8}$$

Combining (2.7) with (2.8) gives $(r^3 - r^i)\Delta^{(3)}(\alpha_j) \equiv 0 \pmod{l}$.

Since $i \in \{i_2, ...i_s\}$ and $i \neq 3$, we get

$$\Delta^{(3)}(\alpha_j) \equiv 0 \pmod{l}, \text{ for } j = 1, 2, ..., n.$$

Hence Prop 2.2. $\mathcal{QED}$.

Proposition 2.3. $\Delta^{(3)}(\varpi) \equiv 0$ *(mod l).*

We first need some results (Theorems A and B) essentially due to Vandiver and a theorem of Mazur-Wiles. Complete proofs of Theorems A and B will be given in Section 3.

Theorem A. [V1, pp.118-122] *Let E_{l-3} be the real unit defined by (0.3). If x, y, z satisfy (2.1) with $l \nmid xyz$, then we have:*

$$\left\{\frac{E_{l-3}}{P}\right\} = 1 \qquad \textit{where } P \textit{ is as defined before.}$$

Remark: The above theorem holds for any prime ideal Q such that $Q|(x + \zeta y)$.

Next we appeal to a theorem of Mazur and Wiles:

Theorem. ([MW]) *Let j be an odd positive integer, $j \not\equiv 1 \pmod{l}$.*

Then $v_l(|(C_l^{(j)})|) = v_l(\mathbf{B}_{1,\omega^{-j}})$.

Remark: See also the discussion in [Wa, p. 198, Remark]. Also, V. A. Kolyvagin [Ko] has given a purely cyclotomic proof of this result.

We need the following proposition:

Proposition 2.4. *Let $c_k = (l-4)l^k + 1$, for any positive integer k, and $n = v_l(\mathbf{B}_{1,\omega^{-j}})$. Then*

$$v_l(\mathbf{B}_{c_n}) = v_l(\mathbf{B}_{1,\omega^{-j}}).$$

Proof.

It is known ([Ha], p. 89-90) that

$$\mathbf{B}_{1,\omega^{-j}} \equiv \mathbf{B}_{(l-4)l^m+1} \pmod{l^m} \text{ for all positive integers } m. \tag{2.9}$$

.

Setting $m = n$ in (2.9), and using the fact that $v_l(\mathbf{B}_{1,\omega^{-j}}) = n$, we get $l^n | \mathbf{B}_{c_n}$.

From the generalized Kummer congruence relations for Bernoulli numbers (cf. [Wa] p. 61), we get $\mathbf{B}_{c_{n+1}} \equiv \frac{\mathbf{B}_{c_n}}{c_n} \pmod{l^{n+1}}$.

So if $l^{n+1} | \mathbf{B}_{c_n}$, then $l^{n+1} | \mathbf{B}_{c_{n+1}}$. Then from (2.9), with $m = n+1$, we get

$$\mathbf{B}_{1,\omega^{-j}} \equiv 0 \pmod{l^{n+1}}, \text{ a contradiction.}$$

$\mathcal{QED}$.

Let $h_3 = v_l(|C_l^{(3)}|)$, and $c = (l-4)l^{h_3} + 1$. From the theorem of Mazur-Wiles, we have $v_l(\mathbf{B}_{1,\omega^{-3}}) = h_3$. Setting $n = h_3$ in Prop. 2.4, we get $v_l(\mathbf{B}_c) = h_3$. Thus $l \nmid \frac{\mathbf{B}_c}{l^{h_3}}$.

Theorem B. [V4, pp. 393-408] *Assume $C_l^{(i)}$ is cyclic for $i = 3, 3, ..., l-2$. (For $i = 3$, we already know $C_l^{(3)}$ is cyclic by the theorem of Kurihara.) Let P is a prime ideal whose ideal class generates $C_l^{(i)}$. Let $h_i = v_l(|C_l^{(i)}|)$, and set $P^{l^{h_i}} = (\upsilon)$. Let $\left\{\frac{E_{l-3}}{P}\right\} = \zeta^e$, with $e \in (\mathbf{Z}/l\mathbf{Z})$. Recall that $c = (l-4)l^{h_i} + 1$.*

Then we have

$$e \equiv \pm \frac{r^{l-i}-1}{2} \frac{\mathbf{B}_c}{l^{h_i}} \Delta^{(i)}(\upsilon) \qquad (mod\ l). \tag{2.10}$$

Proof of Prop. 2.3:

From Theorem A, $e \equiv 0 \pmod{l}$. Since r is a primitive root modulo l, we get from Theorem B (with $i = 3$) and Prop. 2.4,

$$\Delta^{(3)}(\upsilon) \equiv 0 \pmod{l}. \tag{2.11}$$

Let $\frac{ml}{l^{h_3}} = q$, so that $P^{ml} = (\upsilon)^q = (\varpi)$. Then, by using Prop 1.5 and Lemma 1.1, we have

$$q\Delta^{(3)}(\upsilon) \equiv \Delta^{(3)}(\varpi) \pmod{l} \tag{2.12}$$

Combining (2.11) and (2.12), we get Prop. 2.3. $\mathcal{QED}$.

Proof of Main Theorem (contd.)

Applying Propositions 2.2 and 2.3 to equation (2.5), we get $\Delta^{(3)}(x + \zeta y) \equiv 0 \pmod{l}$.

$$\text{Now,} \qquad \Delta^{(3)}(x+\zeta y) = \frac{d^3}{dv^3} log\ (x + (e^v)y)\Big|_{v=0} = \frac{xy(x-y)}{(x+y)^3}.$$

Since $l \nmid xyz$, we get $x - y \equiv 0 \pmod{l}$.

Now change $-z$ back to z, so that we have $x^l + y^l + z^l = 0$. Note that the roles of x, y, z are interchangeable in this equation as well as the arguments above. Hence we also get $y - z \equiv x - z \equiv 0 \pmod{l}$. Thus $x \equiv y \equiv z \pmod{l}$. Reducing $x^l + y^l + z^l$ modulo l, we get $x + y + z \equiv 0 \pmod{l}$. This gives $3x \equiv 3y \equiv 3z \equiv 0 \pmod{l}$. Since l is irregular, we certainly have $l > 3$. So $l|x, l|y, l|z$, a contradiction.

Alternate proof, without using Theorem B.

The proof of Prop. 2.3 can be simplified considerably if we use the following lemma (the proof is in Chapter 4). In particular, we can avoid the use of Theorem B.

Lemma 4.5. *If the ideal class of the ideal $\mathcal{I}$ generates $C_l^{(3)}$, then* $\left\{\frac{E_{l-3}}{\mathcal{I}}\right\} \neq 1$.

From Theorem A we get $\left\{\frac{E_{l-3}}{P}\right\} = 1$. Since by definition the ideal class of P generates $C_l^{(3)}$, lemma 4.5 gives a contradiction.

CHAPTER 3

PROOFS OF THEOREMS A AND B

The proof of Theorem A was sketched by Vandiver in [V1, p. 122]. His argument is correct, and the proof with necessary details is included here for completeness.

1. Proof of Theorem A

Equation (2.1) can be written as

$$\prod_{i=0}^{l-1}(x+\zeta^i y) = (-z)^l. \tag{3.1}$$

Let P be any prime ideal such that $P|I,\ P|(x+\zeta y)$. Let $N(P)$ be the norm of P. When $l \nmid z$, we get from Lemma 2.1a that:

(1) The ideals $(x+\zeta^i y)$ in (3.1) are prime to each other and (λ).

(2) $(x+y) = v^l$ where v is a rational integer.

(3) $N(P)$ divides $\frac{x^l+y^l}{x+y}$ but $N(P)$ does not divide $(x+y)$.

Let $N(P) = p^m$, where m is a positive integer. In fact, m is the least positive integer n such that $p^n \equiv 1 \pmod{l}$. It is easy to show ([Ri] p. 52) that, for such $p, N(P) = p \equiv 1 \pmod{l}$. We now need the following result:

Proposition 3.1 ([V2],p.217) Recall that when $n \in \mathbf{Z}$, n' is an integer such that $nn' \equiv 1 \ (mod\ l)$. If equation (2.1) is satisfied in integers $x, y, and\ z$ prime to each

other with z prime to l then $\exists \alpha \in A$ such that

$$\prod_{n=1}^{\frac{l-1}{2}} (x + \zeta^{n'} y) = \zeta^g \alpha^l \tag{3.1}$$

Proof. Recall, from Prop. 2.1a, we have

$$x + y = v^l, \qquad \text{with } v \in \mathbf{Z}. \tag{3.2}$$

$$x + \zeta y = I^l, \qquad I \text{ an integral ideal}, \tag{3.3}$$

when x, y, z are as in the statement of this proposition.

Applying the Stickelberger type relation (0.2) from Chapter 0 with $n_1 = n_2 = 1$, and using the fact that all prime ideals dividing $(x + \zeta y)$ with x, y, z as in Theorem 2.1 are of degree 1 (as proved in Lemma 2.1a (4)), we find that the product $\prod_{n=1}^{\frac{l-1}{2}} \sigma_{n'}(I)$ is principal. Applying this to equation (3.3), we get

$$\prod_{n=1}^{\frac{l-1}{2}} (x + \zeta^{n'} y) = \eta \beta^l, \qquad \text{where } \eta \in A \text{ is a unit, and } \beta \in A. \tag{3.4}$$

Applying σ_{-1} to (3.4), we get

$$\prod_{n=1}^{\frac{l-1}{2}} (x + \zeta^{-n'} y) = \overline{\eta}(\overline{\beta})^l. \tag{3.5}$$

Multiplying (3.4) and (3.5), and using (2.1) and (3.2), we find that the ideal $(\beta\overline{\beta}) = (\frac{z}{v})$, where Hence $\beta\overline{\beta} = E(z/v)$, where $E \in A$ is a unit. Taking the product of (3.4) and (3.5) again, we find that

$$\eta\overline{\eta}E^l = 1. \tag{3.6}$$

But we know, by a basic result, that

$$\eta = \zeta^g \epsilon, \tag{3.7}$$

where $\epsilon \in A^+ = \mathbf{Z}[\zeta + \zeta^{-1}]$ is a real unit and $g \in \mathbf{Z}$.

From (3.6) and (3.7) we get $\epsilon^2 = E^{-l}$. Since l is odd, we can find integers a, b such that $2a = 1 + bl$, so that $\epsilon^{2a} = \epsilon\epsilon^{bl} = E^{-al}$. Hence $\epsilon = (\epsilon^{-b}E^{-a})^l$, and $\eta = \zeta^g(\epsilon^{-b}E^{-a})^l$. Letting $\alpha = \epsilon^{-b}E^{-a}\beta$, we get Proposition 3.1.

$\mathcal{QED}$.

Let P be a prime ideal as defined such that $P|(x + \zeta y)$, where x, y, z are as in equation (2.1). Then we also have

Prop. 3.1a. $N(P) = p \equiv 1 \pmod{l^2}$.

Proof. We use the following result of Fürtwangler.

Theorem 3.2.([F], p. 589-592) If x, y, z are integers prime to each other such that $x^l + y^l + z^l = 0$, l is an odd prime such that $l \nmid z$, and b is a positive integer such that $b|z$, then $b^{l-1} \equiv 1 \pmod{l^2}$.

From Lemma 2.1a (4), we have $p \equiv 1 \pmod{l}$. Let $b = p$ in Theorem 3.2. We know $p|z$. So we get $p^{l-1} \equiv 1 \pmod{l^2}$.

But when $p^{l-1} \equiv 1 \pmod{l^2}$ and $p \equiv 1 \pmod{l}$, we have $p \equiv 1 \pmod{l^2}$.

$\mathcal{QED}$.

Proof of Theorem A (contd.).

Claim : *Let* $u = \frac{l-3}{2}$. *Let* $k \in \{1, 2, ..., u\}$. *Then* $\exists\ s(k) \in \{\pm 1\}$ *such that* $s(k)kn' \not\equiv 1 \pmod{l}$ *for all* $n, 1 \leq n \leq \frac{l-1}{2}$.

Proof. Suppose $km_1' \equiv 1$ and $-km_2' \equiv 1 \pmod{l}$ for some $m_1, m_2 \in \{1, 2, ..., \frac{l-1}{2}\}$. Then $m_1 + m_2 \equiv 0 \pmod{l}$, which is impossible.

Choose $s(k)$ as above. Since $P|(x+\zeta y)$, we get $P \nmid (x+\zeta^{s(k)kn'}y)$, $\forall n \in \{1,2,..,\frac{l-1}{2}\}$ by the claim just proved.

In (3.1) apply $\sigma_{(s(k)k)}$ to both sides where $1 \leq k \leq \frac{l-1}{2}$ to get

$$\prod_{n=1}^{\frac{l-1}{2}} \left\{ \frac{x+\zeta^{s(k)kn'}y}{P} \right\} = \left\{ \frac{\zeta^{s(k)kg}}{P} \right\}, \tag{3.8}$$

where the l-th power residue symbol $\left\{\frac{\alpha}{P}\right\}$ is as defined by equation (0.4).

From Prop. 3.1a, we have $N(P) = p \equiv 1 \pmod{l^2}$.

This implies

$$\left\{\frac{\zeta}{P}\right\} = 1 \quad \Rightarrow \left\{\frac{\zeta^{s(k)kg}}{P}\right\} = 1,$$

by the definition of the power residue symbol.

$$\text{Now, } (x+\zeta^i y) = (x+\zeta y) + (y\zeta)(\zeta^{i-1}-1)$$

$$\Rightarrow (x+\zeta^i y) \equiv (y\zeta)(\zeta^{i-1}-1) \pmod{P}.$$

$$\text{Hence we get } \left\{\frac{x+\zeta^i y}{P}\right\} = \left\{\frac{(y\zeta)(\zeta^{i-1}-1)}{P}\right\} = \left\{\frac{(y)(\zeta^{i-1}-1)}{P}\right\}$$

because $\left\{\frac{\zeta}{P}\right\} = 1$, as we just proved using Prop. 3.1a.

$$\text{Now,} \qquad y(\zeta^{i-1}-1) = \left(\frac{\zeta^{i-1}-1}{\zeta-1}\right)(y(\zeta-1)).$$

$$\text{But,} \qquad y(\zeta-1) = (x+\zeta y)-(x+y) \equiv -v^l = (-v)^l \pmod{P} \Rightarrow \left\{\frac{(y)(\zeta-1)}{P}\right\} = 1.$$

$$\text{Hence} \qquad \left\{\frac{x+\zeta^i y}{P}\right\} = \left\{\frac{(y)(\zeta^{i-1}-1)}{P}\right\} = \left\{\frac{\frac{\zeta^{i-1}-1}{\zeta-1}}{P}\right\}.$$

Hence (3.8) becomes:

$$\prod_{n=1}^{\frac{l-1}{2}} \left\{ \frac{\left(\frac{\zeta^{s(k)kn'-1}-1}{\zeta-1}\right)}{P} \right\} = 1. \tag{3.9}$$

Let $b \in \mathbf{Z}$, $b \not\equiv 0 \pmod{l}$. We need the following fact relating the l-th power residue characters of $\frac{\zeta^b-1}{\zeta-1}$ and E_{2m} with respect to a prime ideal P:

Fact ([K3], p. 277):

For $\alpha \in A, \alpha \notin P$ define $ind(\alpha)$ by:

$$\zeta^{ind(\alpha)} = \left\{ \frac{\alpha}{P} \right\}.$$

Then,

$$ind\left(\frac{\zeta^b-1}{\zeta-1}\right) \equiv \sum_{m=1}^{u} \frac{(b^{2m}-1)ind(E_{2m})}{r^{2m}-1} - \frac{1}{2}(b-1)ind(\zeta) \pmod{l}. \tag{3.10}$$

where $u = (l-3)/2$ as before.

Since $\left\{ \frac{\zeta}{P} \right\} = 1$, we get $ind(\zeta) = 0$. Applying (3.10) to (3.9) we get

$$\sum_{m=1}^{u} \sum_{n=1}^{\frac{l-1}{2}} \frac{((s(k)kn'-1)^{2m}-1)ind(E_{2m})}{r^{2m}-1} \equiv 0 \pmod{l}. \tag{3.11}.$$

Expanding the left-hand side in powers of k, we get

$$\pm kA_1R_1 + k^2A_2R_2 \pm \ldots\ldots + k^{l-3}A_{l-3}R_{l-3} \equiv 0 \ mod(\ l). \tag{3.12}$$

where the $A_j's$ are expressions involving r and E_m, and $R_j = \sum_{n=1}^{\frac{l-1}{2}} (n')^j$.

When j is even, $2R_j = \sum_{n \in (\mathbf{Z}/l)^*} n^j \equiv 0 \pmod{l} \Rightarrow R_j \equiv 0 \pmod{l}$.

$$\text{So we get} \quad \pm kA_1R_1 \pm k^3A_3R_3 \pm ..... \pm k^{l-4}A_{l-4}R_{l-4} \equiv 0 \pmod{l}$$

$$\Rightarrow kA_1R_1 + k^3A_3R_3 + ...k^{l-4}A_{l-4}R_{l-4} \equiv 0 \pmod{l}$$

Letting k run over $1, 2, ..., u$, we see that the A_jR_j 's have to be zero in $\mathbf{Z}/l\mathbf{Z}$ because the determinant of the matrix (k^j), $k = 1, 2, .., u; j = 1, 3, ..., l-4$ (a Vandermonde determinant) is not 0 in $\mathbf{Z}/l\mathbf{Z}$. In particular, for $j = l-4$ we have $A_{l-4}R_{l-4} \equiv 0 \pmod{l}$.

By ([V3], p. 114), we have the following relation between R_j 's and the Bernoulli numbers $\mathbf{B}_i$:

$$\sum_{n=1}^{\frac{l-1}{2}} n^{i-1} \equiv \frac{1-2^i}{2^{i-1}i}\mathbf{B}_i \pmod{l}, \quad i \geq 2, (l-1) \nmid i. \tag{3.13}$$

Remark: The above congruence is also a consequence of Voronoi's congruences(cf, for instance, [Ri. p. 108, 5B]).

Let $i = 4$. From (3.13) we have:

$$\frac{(1-2^4)}{2^3.4}\mathbf{B}_4 \equiv R_{l-4} \pmod{l}.$$

Since $A_{l-4}R_{l-4} \equiv 0 \pmod{l}$, multiplying both sides of this congruence by A_{l-4} gives $A_{l-4}\mathbf{B}_4\frac{1-2^4}{2^5} \equiv 0 \pmod{l}$.

Since l is irregular, certainly $l > 5$, and we get $A_{l-4} \equiv 0 \pmod{l}$.

But we defined:

$$A_{l-4} = \frac{1}{2}\frac{l-3}{r^{l-3}-1}(ind(E_{l-3})).$$

Hence

$$A_{l-4} \equiv 0 \pmod{l} \Rightarrow ind(E_{l-3}) \equiv 0 \pmod{l} \Rightarrow \left\{ \frac{E_{l-3}}{P} \right\} = 1.$$

This concludes the proof of Theorem A.

2. Proof of Theorem B

This result is due to Vandiver. However, his proof contains some ambiguities. So we present a complete proof by exploiting his ideas in conjunction with the theorem of Mazur-Wiles, and with some additional simplications. In addition, we establish this result for any l by exploiting his ideas in conjunction with the theorem of Mazur-Wiles stated in chapter 2. Note that, for any l, one knows that $C_l^{(3)}$ is cyclic by the theorem of Kurihara, stated in chapter 2.

For the convenience of the reader, we gather some notations that will be needed during the proof.

Fix $i \in \{3, 5, ..., l-2\}$. Let $a \in \mathbf{Z}$, $0 < a < (l-1)$, such that $(1 + a^i - (a+1)^i)$ is prime to l. Let $N(P) = p$. Since P is of degree 1, $p \equiv 1 \pmod{l}$. Let J_a be the Jacobi sum $J(\chi_p, \chi_p^a)$.

Let E_{l-i} be as defined by equation (0.3).

Recall that in chapter 2 we proved that $l \nmid \frac{\mathbf{B}_c}{l^{h_i}}$, where $c = (l-1-i)l^{h_i} + 1$, and $h_i = v_l(|C_l^{(i)}|)$.

Let $\upsilon \in A$ be a generator of $P^{l^{h_i}}$, where the class of the prime ideal P generates $C_l^{(i)}$.

Let $\overline{x}$ be the least positive residue of $x \pmod{l}$. As before, if n is an integer, let n' be the integer such that $nn' \equiv 1 \pmod{l}$.

Define $I_a = \{1 \leq n \leq (l-1) \mid \overline{an'} + \overline{n'} > l\}$ and $S = \sum_{n \in I_a} n^b$, where $b = il^{h_i+1}$.

Let $\upsilon_1 = \upsilon^{l-1}$. Then $\upsilon_1 \equiv 1 \pmod{(1-\zeta)}$.

If $\alpha = a_0 + a_1\zeta + ... + a_{l-2}\zeta^{l-2}$, and $\alpha \equiv 1 \pmod{(1-\zeta)}$, then we can find a polynomial, $G \in \mathbf{Z}[x]$, such that $G(\zeta) = \alpha$, and $G(1) = 1$. In fact, $G(x) = a_0 + a_1 + ... + a_{l-2} + \frac{1-(a_0+...+a_{l-2})}{l}\Phi(x)$, where $\Phi(x) = 1 + x + ... + x^{l-1}$. We will denote the polynomial obtained in this way from α by $\tilde{\alpha}(x)$.

Thus $\tilde{v}_1(\zeta) = v_1$, and $\tilde{v}_1(1) = 1$.

Let $\tilde{J}_a(x) = f$ be a polynomial in $\mathbf{Z}[x]$ such that $f(\zeta) = J_a$.

We will write $a \sim b$ if $a \equiv bm \pmod{l}$, with m prime to l.

The proof will be through the series of congruences (*) shown below:

$$(*) \qquad \begin{aligned} ind(E_{l-i}) &\overset{(1)}{\sim} \Delta^{(i)}(J_a) \overset{(2)}{\sim} \Delta^{(b)}(\tilde{J}_a) \\ &\overset{(3)}{\sim} \frac{S}{l^{h_i}}\Delta^{(b)}(\tilde{v}_1) \overset{(4)}{\sim} \frac{\mathbf{B}_c}{l^{h_i}}\Delta^{(i)}(v). \end{aligned}$$

In the proof of relation (4) we would obtain the constant $\pm\frac{r^{l-i}-1}{2}$ and thus complete the proof of Theorem B as it was stated in chapter 2.

Proof of (1)

We need the following proposition:

Proposition 3.3.

$$ind(E_{2n}) \equiv \left(\frac{r^{(2n)} - 1}{2(1 + a^{l-2n} - (a+1)^{l-2n})}\right)\Delta^{(l-2n)}(J_a) \pmod{l} \qquad (3.14)$$

where $1 < l - 2n < l - 1$.

Proof. See [K, pp. 95-103].

Remark: The above result is also proved by Hilbert [Hi, pp. 343-351].

Putting $2n = l - i$ in the above proposition, we get the relation (1), which is given below:

$$ind(E_{l-i}) \equiv \left(\frac{r^{(l-i)} - 1}{2(1 + a^i - (a+1)^i)}\right) \Delta^{(i)}(J_a) \pmod{l} \tag{3.15}$$

Since $\frac{r^{(l-i)}-1}{2(1+a^i-(a+1)^i)}$ is prime to l, we get relation (1).

$\mathcal{QED}$.

Proof of (2).

Applying Lemma 1.3 to $(\Delta^{(il^{h_i}+1)}(\tilde{J}_a)$, we have

$$\Delta^{(il^{h_i}+1)}(\tilde{J}_a) \equiv \Delta^{(i)}(\tilde{J}_a) \pmod{l}$$

But $\Delta^{(i)}(\tilde{J}_a) \equiv \Delta^{(i)}(J_a) \pmod{l}$, by Lemma 1.1.

Hence we get relation (2).

$\mathcal{QED}$.

Proof of (3).

(3) is given by the following proposition:

Recall: $v_1 = v^{l-1}$. a is an integer such that $0 < a < l - 1$ and $(1 + a^i - (a+1)^i)$ is prime to l. J_a is the Jacobi sum $J(\chi_p, \chi_p^a)$.

$\overline{x}$ is the least positive residue of $x \pmod{l}$. If n is an integer, n' is integer such that $nn' \equiv 1 \pmod{l}$. Also, $I_a = \{1 \leq n \leq (l-1) \mid \overline{an'} + \overline{n'} > l\}$.

Proposition 3.4. *Let $\tilde{J}_a$ and $\tilde{v}_1$ be defined as before. Let $S = \sum_{n \in I_a} n^{il^{h_i}+1}$. Then,*

$$\Delta^{(il^{h_i}+1)}(\tilde{J}_a) \equiv \frac{S}{l^{h_i}} \Delta^{(il^{h_i}+1)}(\tilde{v_1}) \pmod{l}$$

Proof.

Recall that $N(P) = p \equiv 1 \pmod{l}$.

From chapter 0 we have the following Stickelberger type relation (0.2) for the ideal P:

$$\prod_{n \in I_a} \sigma_n(P) = (J_a). \tag{3.16}$$

From (3.16) we get

$$\prod_{n \in I_a} (\sigma_n(P))^{l^{h_i}} = \prod_{n \in I_a} (\sigma_n(\upsilon)) = (J_a)^{l^{h_i}}$$

$$\Rightarrow \beta \prod_{n \in I_a} \sigma_n(\upsilon) = (J_a)^{l^{h_i}}, \text{ with } \beta \in A^*. \tag{3.17}$$

Let $\beta = \zeta^k \epsilon$, where $k \in \{1, 2, .., l\}$ and ϵ is a real unit.

Raising both sides of (3.17) to the power of $(l-1)$, we get

$$\zeta^{(l-1)k} \epsilon^{l-1} \prod_{n \in I_a} (\sigma_n(\upsilon))^{l-1} = J_a^{(l-1)l^{h_i}}. \tag{3.18}$$

Let $\epsilon^{l-1} = \epsilon_1$, and $\upsilon^{l-1} = \upsilon_1$. Recall that $\lambda = 1 - \zeta$.

Then $\epsilon_1 \equiv 1 \ (mod \ (\lambda))$, and $\upsilon_1 \equiv 1 \ (mod \ (\lambda))$. Let $\tilde{\epsilon_1}(x)$ and $\tilde{\upsilon_1}(x)$ be integral polynomials obtained from ϵ_1 and υ_1 as described in the beginning of the proof of Theorem B. Recall that $\tilde{J}_a(x) = f$ where $f \in \mathbf{Z}[x]$, such that $f(\zeta) = J_a$.

Claim.

$$l^{h_i}(l-1)\Delta^{(il^{h_i+1})}(\tilde{J}_a) \equiv \sum_{n \in I_a} \Delta^{(il^{h_i+1})}(\sigma_n(\tilde{\upsilon_1})) \ (mod \ l^{h_i+1}) \tag{3.19}$$

First we show $\Delta^{(il^{h_i+1})}(\tilde{\epsilon_1}) \equiv 0 \ (mod\ l^{h_i+1})$. If $\tilde{\epsilon_1}(x) = a_0 + a_1 x + ... + a_{l-2}x^{l-2} + \frac{1-(a_0+a_1+...+a_{l-2})}{l}\Phi(x)$, then $\tilde{\epsilon_1}(x^{l-1}) = E(x)$ is a polynomial such that $E(1) = 1$ and $E(\zeta) = \sigma_{l-1}(\tilde{\epsilon_1}) = \tilde{\epsilon_1}$. Hence we can apply Lemma 1.2 and get

$$\Delta^{(il^{h_i+1})}(E) \equiv \Delta^{(il^{h_i+1})}(\tilde{\epsilon_1}) \quad (mod\ l^{h_i+1}).$$

Using equation (1.2) from the proof of Prop 1.4(c), we get

$$\Delta^{(il^{h_i+1})}(\tilde{\epsilon_1}(x^{l-1})) = (l-1)^{il^{h_i+1}} \Delta^{(il^{h_i+1})}(\tilde{\epsilon_1}(x)).$$

Since $(l-1)^{il^{h_i+1}} \equiv -1 \quad (mod\ l^{h_i+1})$, we get

$$\Delta^{(il^{h_i+1})}(\tilde{\epsilon_1}) \equiv -\Delta^{(il^{h_i+1})}(\tilde{\epsilon_1}(x)) \quad (mod\ l^{h_i+1}).$$

Hence $\Delta^{(il^{h_i+1})}(\tilde{\epsilon_1}) \equiv 0 \quad (mod\ l^{h_i+1})$.

If $\tilde{v_1}(x) = b_0 + b_1 x + ... + b_{l-2}x^{l-2} + \frac{1-(b_0+b_1+...+b_{l-2})}{l}\Phi(x)$, then let $\sigma_n(\tilde{v_1}) = \tilde{v_1}(x^n) = V(x)$. Then $V \in \mathbf{Z}[x]$ is a polynomial such that $V(1) = 1$ and $V(\zeta) = \sigma_n(\tilde{v_1}(\zeta))$.

Also $(\tilde{J}_a(1))^{(l-1)l^{h_i+1}} \equiv 1 \ (mod\ l^{h_i+1})$.

Now let $F(x) = x^{(l-1)k}\tilde{\epsilon_1}(x) \prod_{n \in I_a} (\tilde{v_1}(x^n))$ and $G(x) = \tilde{J}_a(x)^{(l-1)l^{h_i}}$.

Then $F(\zeta) = G(\zeta)$ and $F(1) = 1 \equiv G(1) \ (mod\ l^{h_i+1})$.

Then we can apply Lemma 1.2 and (1.2) from the proof of Prop. 1.4(c) to (3.18) and get the claim.

$\mathcal{QED}$.

Proof of Prop 3.4 (contd.)

Using (1.2) from the proof of Prop 1.4(c), we have

$$\sum_{n \in I_a} \Delta^{(il^{h_i+1})}(\sigma_n(\tilde{v_1})) \equiv (\sum_{n \in I_a} n^{il^{h_i+1}})\Delta^{(il^{h_i+1})}(\tilde{v_1}) \quad (mod\ l^{h_i+1})$$

Now divide both sides of (3.19) by l^{h_i}, after using the above relation. We get

$$(\Delta^{(il^{h_i}+1)}(\tilde{J}_a) \equiv -\frac{\sum_{n\in I_a} n^{il^{h_i}+1}}{l^{h_i}}\Delta^{(il^{h_i}+1)}(\tilde{v_1}) \ (mod\ l) \tag{3.20}$$

Hence relation (3). $\mathcal{QED}$.

Proof of (4)

Let $c = (l-1-i)l^{h_i}+1$ and $S = \sum_{n\in I_a} n^{il^{h_i}+1}$ as before. Relation (4) is the following congruence:

$$\frac{S}{l^{h_i}}\Delta^{(il^{h_i}+1)}(\tilde{v_1}) \equiv \pm((a+1)^{il^{h_i}+1} - a^{il^{h_i}+1} - 1)\frac{\mathbf{B}_c}{l^{h_i}}\Delta^{(i)}(v) \ (mod\ l)$$

This congruence will be proved through Lemma 3.5.

Lemma 3.5. *Let $c = (l-1-i)l^{h_i}+1$ as before. Then*

$$S = \sum_{n\in I_a} n^{il^{h_i}+1} \equiv \pm((a+1)^{il^{h_i}+1} - a^{il^{h_i}+1} - 1)\frac{\mathbf{B}_c}{c} \ (mod\ l^{h_i+1})$$

Proof of Lemma 3.5

For the sake of convenience we will denote $\sum_{n\in I_a}$ by $\sum$ and h_i+1 by m.

We have

$$\sum n^{il^m} \equiv \sum (n')^{(l-1-i)l^m} \ (mod\ l^{m+1}).$$

Let $L = \sum (n')^{(l-1-i)l^m}$. Clearly we have

$$L = \sum_{k=1}^{l-1} \frac{\overline{ak} + \overline{k} - \overline{(a+1)k}}{l} k^{(l-1-i)l^m}.$$

From $(ak)^{(l-1-i)l^m} \equiv \overline{ak}^{(l-1-i)l^m} \ (mod\ l^{m+1})$ we get $k^{(l-1-i)l^m} \equiv a^{il^m}\overline{ak}^{(l-1-i)l^m} \ (mod\ l^m$

Similarly, $k^{(l-1-i)l^m} \equiv \overline{k}^{(l-1-i)l^m}$ and $k^{(l-1-i)l^m} \equiv (a+1)^{il^m}\overline{(a+1)k}^{(l-1-i)l^m} \ (mod\ l^{m+1})$.

Let $b = il^m$ and $d = (l-1-i)l^m + 1$. Then we can write

$$L \equiv \frac{a^b + 1 - (a+1)^b}{l} \sum_{k=1}^{l-1} k^d \pmod{l^m}.$$

Following the notation of Ribenboim ([Ri], p. 124), we let

$$\sum_{k=1}^{l-1} k^d = S_d(l-1).$$

Thus $S \equiv \frac{a^b+1-(a+1)^b}{l} S_d(l-1) \pmod{l^m}$.

Lemma 3.5 follows from the following claim:

Claim:

$$S_d(l-1) \equiv l\frac{\mathbf{B}_c}{c} \pmod{l^{m+1}}.$$

where $c = (l-1-i)l^{h_i} + 1$ as before.

It is well known (See [Ri, p. 100]) that

$$S_d(l-1) = l\mathbf{B}_d + \frac{d}{2}l^2\mathbf{B}_{d-1} + \frac{l^3}{3}\binom{d}{2}\mathbf{B}_{d-2} + \ldots\ldots + \frac{l^k}{k+1}\binom{d}{k}\mathbf{B}_{d-k+1} + \ldots. + \frac{l^{d+1}}{d+1}.$$

$\mathbf{B}_{d-1} = 0$ since $d-1$ is odd. By the theorem of von Staudt-Clausen (cf, for instance, [Ri, p. 102, 2D]), the denominator of $l\mathbf{B}_N$ is prime to l for any even integer N. So clearly $\frac{l^3}{3}\binom{d}{2}\mathbf{B}_{d-2} \equiv 0 \pmod{l^{m+2}}$.

Now, consider the general term $\frac{l^k}{k+1}\binom{d}{k}\mathbf{B}_{d-k+1}$. We know that the denominator of $l\mathbf{B}_{d-k+1}$ is prime to l. We have

$$\frac{l^{k-1}}{k+1}\binom{d}{k} = \frac{l^{k-1}d(d-1)..(d-k+1)}{(k+1)!}.$$

Since $l > 3$ and $l^{k-1} > k+1$, $v_l(\frac{l^{k-1}}{(k+1)k(k-1)}) \geq 1$. Also because $d-1 \geq k-1$, $v_l((d-1)-(k-j)) \geq v_l(k-j)$ for $j = 2,..,k-2$. Thus

$$v_l(\frac{(d-2)(d-3)...(d-k+1)}{(k-2)!}) \geq 0.$$

Since $v_l(d-1) = m$, we get

$$v_l(\frac{l^{k-1}d(d-1)..(d-k+1)}{(k+1)!}) = v_l(\frac{l^{k-1}}{(k+1)!}d(d-1)(d-2)...(d-k+1)) \geq m+1.$$

Thus

$$S_d(l-1) \equiv l\mathbf{B}_d \ (mod\ l^{m+1})$$

By generalized Kummer congruences for Bernoulli numbers (See [Wa], p. 61), we have

$$\mathbf{B}_d \equiv \frac{\mathbf{B}_c}{c} \ (mod\ l^m).$$

Hence the claim, and Lemma 3.5.

Now we prove relation (4).

Applying Lemma 3.5, (3.20) becomes

$$(\Delta^{(il^{h_i+1})}(\tilde{J}_a) \equiv \pm((a+1)^{il^{h_i+1}} - a^{il^{h_i+1}} - 1)\frac{\mathbf{B}_c}{l^{h_i}}\Delta^{(il^{h_i+1})}(\tilde{v_1}) \ (mod\ l) \quad (3.21)$$

As mentioned at the beginning of the proof of the present theorem, $l \nmid \frac{\mathbf{B}_c}{l^{h_i}}$.

Applying Lemma 1.3, we have

$$\Delta^{(il^{h_i+1})}(\tilde{v_1}) \equiv \Delta^{(i)}(\tilde{v_1}) \quad (mod\ l)$$

Moreover,

$$\Delta^{(i)}(\tilde{v_1}) \equiv -\Delta^{(i)}(v) \quad (mod\ l),$$

by Lemma 1.1 and Prop 1.4(a).

Thus (3.21) becomes

$$\Delta^{(il^{h_i+1})}(\tilde{J}_a) \equiv \pm((a+1)^{il^{h_i+1}} - a^{il^{h_i+1}} - 1)\frac{\mathbf{B}_c}{l^{h_i}}\Delta^{(i)}(v) \quad (\text{mod } l) \qquad (3.21a)$$

Combining (3.21a) with (3.20) we get relation(4). $\mathcal{QED}$.

Proof of Theorem B.

Now we combine the relations (1) through (4) to get Theorem B.

From (2) we have

$$\Delta^{(il^{h_i+1})}(\tilde{J}_a) \equiv \Delta^{(i)}(J_a) \ (mod\ l)$$

Thus (3.21a) becomes

$$\Delta^{(i)}(J_a) \equiv \pm((a+1)^{il^{h_i+1}} - a^{il^{h_i+1}} - 1)\frac{\mathbf{B}_c}{l^{h_i}}\Delta^{(i)}(v) \ (mod\ l) \tag{3.22}$$

Using Kummer's Proposition (3.14) in (3.22) we get

$$ind(E_{l-i}) \equiv \left(\frac{r^{(l-i)} - 1}{2(1 + a^i - (a+1)^i)}\right) \pm((a+1)^{il^{h_i+1}} - a^{il^{h_i+1}} - 1)\frac{\mathbf{B}_c}{l^{h_i}}\Delta^{(i)}(v) \ (mod\ l) \tag{3.23}$$

Theorem B follows if we note that for any integer n, $n^{l^j} \equiv n \ (mod\ l)$ for $j = 1, 2, \ldots$ $\mathcal{QED}$.

Chapter 4

THE MAIN THEOREM

Recall that r is a primitive root modulo l, and A the ideal class group of $\mathbf{Q}[\zeta]$. The l-Sylow subgroup C_l of A decomposes into a direct sum of eigenspaces $C_l^{(i)}$ which are defined as follows:

$$C_l^{(i)} = \{\ x \in C_l\ |\sigma(x) = x^{\omega^i(\sigma)} = x^{\omega^i(r)} = x^{r^i} y^l \text{with } y \in C_l\ \}.$$

Let $|C_l^{(3)}| = l^{h_3}$.

Theorem 4.1. *For $n \geq max(1, h_3)$,*

$$x^{l^n} + y^{l^n} + z^{l^n} = 0 \tag{4.1}$$

is impossible with $x, y, z\ \in \mathbf{Z},\ l \nmid xyz$.

Proof.

Assume equation (4.1) is possible, with $l \nmid xyz$. We may also assume that x, y, z are relatively prime. Let $X = x^{l^{n-1}}, Y = y^{l^{n-1}}$. Then equation (4.1) can be written as

$$\prod_{i=0}^{l-1}(X + \zeta^i Y) = (-z)^{l^n}. \tag{4.1a}$$

Recall that $\lambda = 1 - \zeta$. We have

Lemma 4.1a.

(1) *The ideals $(X + \zeta^i Y)$ in equation (4.1a) are prime to each other and (λ).*

(2) $(X + \zeta^j Y) = I_j^{l^n}$, *where for* $1 \leq j \leq l-1$, I_j *is an ideal in* A.

(3) $(X + Y) = v^l$ *where* $v \in \mathbf{Z}$.

(4) *If* P *is a prime ideal divisor of* I_j *for some* j, *then* $N(P) = p$ *for some prime number* p *such that* $p \equiv 1 \pmod{l}$ *and* $p | \dfrac{X^l + Y^l}{X + Y}$ *but* $p \nmid X + Y$.

Proof. Same as proof of lemma 2.1a, since X, Y and $Z = z^{l^{n-1}}$ satisfy equation (2.1), with $l \nmid XYZ$.

Henceforth, let $I_1 = I$. We have from Lemma 4.1a (1),

$$(X + \zeta Y) = I^{l^n}. \tag{4.1b}$$

As in chapter 2, we can assume I is non-principal, and l is irregular. From equation (4.1b) we get that $[I]$ has order a power of l in C_l and thus $[I] \in C_l$. Decomposing each $C_l^{(i)}$ in terms of its cyclic summands, we get as in chapter 2,

$$C_l = C_l^{(3)} \oplus M_1 \oplus ..... \oplus M_n,$$

where n is a positive integer and each M_j is a cyclic subgroup of some $C_l^{(i)}$ with $i \neq 3$. Let $[P]$ be an ideal class which generates $C_l^{(3)}$. Using the Tchebotarev density theorem, we choose a prime ideal P to represent it. Similarly, for $j = 1, 2, .., n$, let Q_j be a prime ideal representing an ideal class which generates M_j. We get:

$$[I] = [P]^t [Q_1]^{k_1} .....[Q_m]^{k_m} \tag{4.2}$$

where $t, k_1, ..., k_m$ are non-negative integers. Then we can write

$$I = P^t Q_1^{k_1} ....Q_m^{k_m} (\frac{\gamma}{\delta}) \tag{4.3}$$

where γ, δ are nonzero algebraic integers, and (as in chapter 2) $(\lambda) \nmid (\gamma), (\lambda) \nmid (\delta)$.

Using Theorem A of chapter 2 we get, after writing the ideal I as a product of prime ideals, and using the multiplicativity of the l-th power residue symbol,

$$\left\{ \frac{E_{l-3}}{I} \right\} = 1 \tag{4.4}$$

We also need the following:

Lemma 4.2. *$K(E_{l-3}^{1/l})$ is a nontrivial, unramified, abelian extension of K.*

Let H_l be the maximal abelian unramified l-extension of K. Then the Artin map gives the isomorphism $C_l \xrightarrow{\sim} Gal(H_l/K)$ which sends the ideal class [P] of any prime ideal P in K to the Frobenius element $\left(\frac{H_l/K}{P} \right)$.

Definition: A unit $\eta \in A^*$ is called *singular primary* if:

$$\eta \equiv u^l \pmod{\lambda^l} \text{ for some } u \in A.$$

Proof of Lemma 4.2. By the theorem of Kurihara, $C_l^{(l-3)} = 0$. A consequence of the proof of the main conjecture of Iwasawa is that for $i = 2, 4, ..., l-3$, $|C_l^{(i)}| = |((A^*)_l^+ / CU_l^+)^{(i)}|$, where CU^+ is the group of real cyclotomic units, $(A^*)^+$ is the group of real units, and $((A^*)_l^+ / CU_l^+)^{(i)}$ is defined in the same way as $C_l^{(i)}$. From this it follows that $C_l^{(l-3)} = 0 \Rightarrow E_{l-3}$ cannot be an l-th power (cf., [Wa, Chapter 8, pp. 146 and 157]). Thus $K(E_{l-3}^{1/l})$ is a nontrivial extension of K.

We also know $K(\eta^{1/l})$ is unramified iff η is singular primary (See [Wa, exercise 9.3, p. 182]). As already mentioned, we have $l | \mathbf{B}_{l-3}$. By ([Mo], p.115), E_n is singular primary if $l | \mathbf{B}_n$. Hence the lemma.

Corollary. *For any principal ideal* (α) *of* K,

$$\left\{\frac{E_{l-3}}{(\alpha)}\right\} = 1.$$

Proof. By the lemma, $K(E_{l-3}^{1/l})$ is a subfield of H_l, the Hilbert l-class field of K. Under the Artin map, the principal ideals map to the trivial automorphism. Hence the l-th power residue symbol $\left\{\frac{E_{l-3}}{(\alpha)}\right\}$ should be trivial, since it gives the action of the trivial automorphism on $K(E_{l-3}^{1/l})$.

Now, recall that from equation (4.3) we have $I = P^t Q_1^{k_1} \ldots . Q_m^{k_m} (\frac{\gamma}{\delta})$. Using the multiplicativity of the l-th power residue symbol, the Corollary of Lemma 4.2, and Theorem A, we have

$$1 = \left\{\frac{E_{l-3}}{I}\right\} = \left\{\frac{E_{l-3}}{P^t}\right\}\left\{\frac{E_{l-3}}{Q_1^{k_1}}\right\} \ldots . \left\{\frac{E_{l-3}}{Q_m^{k_m}}\right\} \tag{4.5}$$

Proposition 4.3. *Let* t *be as in equation (4.5) above. Then* $t \equiv 0 \pmod{l}$.

Remark: If $C_l^{(3)} = 0$, then we have $t = 0$. So we may assume $C_l^{(3)} \neq 0$.

Proof of Prop. 4.3.

First we need the following

Lemma 4.4. ([He], p. 434) Let $k \in \{5, \ldots, l-2\}$, and P_k be any ideal prime to (λ) whose class belongs to $C_l^{(k)}$. Then

$$\left\{\frac{E_{l-3}}{P_k}\right\} = 1.$$

Proof. We have

$$\left\{\frac{E_{l-3}}{P_k^\sigma}\right\} = \left\{\frac{E_{l-3}^{\sigma^{-1}}}{P_k}\right\}^r = \left\{\frac{E_{l-3}^{r^{3-1}}}{P_k}\right\}^r = \left\{\frac{E_{l-3}}{P_k}\right\}^{r^3}. \tag{4.6}$$

But $P_k^\sigma = P_k^{r^k} J^l(\alpha)$ for some ideal J of A and $\alpha \in K$. So we get,

$$\left\{\frac{E_{l-3}}{P_k^\sigma}\right\} = \left\{\frac{E_{l-3}}{P_k^{r^k} J^l(\alpha)}\right\} = \left\{\frac{E_{l-3}}{P_k}\right\}^{r^k} \left\{\frac{E_{l-3}}{J}\right\}^{l} \left\{\frac{E_{l-3}}{(\alpha)}\right\} = \left\{\frac{E_{l-3}}{P_k}\right\}^{r^k}. \quad (4.7)$$

From equations (4.6) and (4.7), we get

$$\left\{\frac{E_{l-3}}{P_k}\right\}^{r^3} = \left\{\frac{E_{l-3}}{P_k}\right\}^{r^k}.$$

Since $k \in \{5, ..., l-2\}$, we get the lemma.

Proof of Proposition 4.3 (contd.)

Now, assume $t \not\equiv 0 \pmod{l}$. We will get a contradiction. From the equation (4.4), we know $\left\{\frac{E_{l-3}}{I}\right\} = 1$. Applying Lemma 4.4 to equation (4.5), we get $\left\{\frac{E_{l-3}}{P^t}\right\} = \left\{\frac{E_{l-3}}{P}\right\}^t = 1$. Then the assumption $t \not\equiv 0 \pmod{l} \Rightarrow \left\{\frac{E_{l-3}}{P}\right\} = 1$. Now Prop. 4.3 will be proved if we show the following:

Lemma 4.5. *If the ideal class of the ideal $\mathcal{P}$ generates $C_l^{(3)}$, then* $\left\{\frac{E_{l-3}}{\mathcal{P}}\right\} \neq 1$.

Proof. Assume $\left\{\frac{E_{l-3}}{\mathcal{P}}\right\} = 1$. Let $[X]$ be any ideal class in C_l. Represent it by a prime ideal J different from (λ). In C_l we can write (additively),

$$[J] = [\mathcal{P}^{a_0}] + \sum_{j=1}^{N} [P_j^{a_j}], \text{ where } a_0, a_1, ..a_N \in \mathbf{Z}, \text{and} [P_j] \in C_l^{(i)}, i \neq 3.$$

Hence we can write $J = \mathcal{P}^{a_0} P_1^{a_1} .... P_N^{a_N}(\beta)$, where $\beta \in K^*$, and β can be written as the ratio of two algebraic integers which are prime to (λ). Consider $\left\{\frac{E_{l-3}}{J}\right\} = \left\{\frac{E_{l-3}}{\mathcal{P}^{a_0} P_1^{a_1} .... P_{i_N}^{a_N}(\beta)}\right\}$. By Lemma 4.4, $\left\{\frac{E_{l-3}}{P_k}\right\} = 1$ if $k \neq 3$. By assumption, $\left\{\frac{E_{l-3}}{\mathcal{P}}\right\} = 1$. Since (β) is principal, $\left\{\frac{E_{l-3}}{(\beta)}\right\} = 1$. Thus, by the multiplicativity of the power residue symbol, we get $\left\{\frac{E_{l-3}}{J}\right\} = 1$. This implies that the Frobenius

$\left(\frac{H_l/K}{J}\right)$ induces the trivial automorphism of $K(E_{l-3}^{1/l})$ over K, for all J as above. This is impossible, since $K(E_{l-3}^{1/l})$ is a nontrivial extension of K contained in H_l, by Lemma 4.4. Hence the lemma and Prop. 4.3. $\mathcal{QED}$.

From equation (4.3) we have

$$I^{l^n} = (X + \zeta Y) = P^{tl^n} Q_1^{k_1 l^n} ... Q_m^{k_m l^n} (\frac{\gamma}{\delta})^{l^n}.$$

This gives the following relation in C_l, written additively:

$$[P^{tl^n}] + [Q_1^{k_1 l^n}] + ... + [Q_m^{k_m l^n}] = 0.$$

Since C_l is a direct sum $C_l^{(3)} \oplus M_1 \oplus .... \oplus M_m$, this implies that $[P^{tl^n}], [Q_1^{k_1 l^n}], ..., [Q_m^{k_m l^n}]$ must all be trivial in C_l. So we can write

$$P^{tl^n} = (\varpi), \text{ and } Q_j^{k_j l^n} = (\alpha_j), \text{ for some } \varpi, \alpha_1, ..., \alpha_m \in A = \mathbf{Z}[\zeta].$$

Since $l^n \geq |C_l^{(3)}|$ by assumption, and $t \equiv 0 \pmod{l}$ by $P^{tl^n} = (\varpi) = (\varpi')^l$ for some $\varpi' \in A$. Thus we get

$$X + \zeta Y = \eta \alpha_1 ..... \alpha_m \beta^l, \quad \beta \in K^*, \eta \in A^*. \tag{4.8}$$

By Prop. 1.2a, we know that $\Delta^{(k)}$ vanishes on the l-th powers of elements in $A - (1 - \zeta)$. Note that in equation (4.8), the numbers occurring on the right-hand side are not divisible by $(1 - \zeta)$, because $(1 - \zeta) \nmid (X + \zeta Y)$. Thus $\Delta^{(k)}$ is defined for all of them. By the remark above, $\Delta^{(k)}(\beta^l) \equiv 0 \pmod{l}$. By Prop. 1.5, $\Delta^{(k)}(\eta) \equiv 0 \pmod{l}$, $\forall k \in \{3, 5, ..., l-3\}$. Taking $k = 3$ and using Lemma 1.1, we get the following by the additivity of the logarithmic derivative:

$$\Delta^{(3)}(X+\zeta Y) \equiv \left(\sum_{j=1}^{m} \Delta^{(3)}(\alpha_j)\right) \pmod{l}. \tag{4.9}$$

Proposition 4.6.

$$\Delta_0^{(3)}(\alpha_j) \equiv 0 \pmod{l}, \text{ for } j = 1, 2, .., m.$$

Proof. Same as the proof of Prop. 2.2.

Thus from equation (4.9) we get $\Delta^{(3)}(X+\zeta Y) \equiv 0 \pmod{l}$.

$$\text{Now,} \quad \Delta^{(3)}(X+\zeta Y) = \frac{d^3}{dv^3} log\ (X+(e^v)Y)\Big|_{v=0} = \frac{XY(X-Y)}{(X+Y)^3}.$$

Since $l \nmid XYz$, we get $X - Y \equiv 0 \pmod{l} \Rightarrow x \equiv y \pmod{l}$. We had $x^{l^n} + y^{l^n} + z^{l^n} = 0$. Note that the roles of x, y, z are interchangeable in this equation as well as the arguments above. Hence we also get $y - z \equiv x - z \equiv 0 \pmod{l}$. Thus $x \equiv y \equiv z \pmod{l}$. Reducing $x^l + y^l + z^l$ modulo l, we get $x + y + z \equiv 0 \pmod{l}$. This gives $3x \equiv 3y \equiv 3z \equiv 0 \pmod{l}$. Since l is irregular, we certainly have $l > 3$. So $l|x, l|y, l|z$, a contradiction.

$\mathcal{QED}$.

CHAPTER 5

AUXILIARY RESULTS

In this chapter we prove some results assuming the cyclicity of $C_l^{(5)}$.

Let $|C_l^{(5)}| = l^{h_5}$.

Theorem 5.1. *Assume that $C_l^{(5)}$ is cyclic.*

(1) *For $n \geq max(1, h_5)$,*

$$x^{l^n} + y^{l^n} + z^{l^n} = 0 \tag{5.1}$$

is impossible with $x, y, z \in \mathbf{Z}$, $l \nmid xyz$.

(2) *If $C_l^{(l-5)}$ is non-trivial, then $x^l + y^l + z^l = 0$ is impossible with $l \nmid xyz$.*

Remark: Note that if $C_l^{(5)}$ is cyclic, $C_l^{(l-5)}$ is also cyclic by Leopoldt's reflection theorem.

Proof of (2).

Assume $\exists x, y, z \in \mathbf{Z}$, such that $x^l + y^l + z^l = 0$. We may also assume, as before, that x, y, z are relatively prime.

As in chapter 2, we have $x + \zeta y = I^l$, and we may assume that I is nonprincipal, and that l is irregular. Then, choosing a prime ideal P_5 whose ideal class generates $C_l^{(5)}$ (since $C_l^{(5)}$ is cyclic, by assumption), we get (as in chapter 4)

$$I = P_5^{a_0} Q_1^{a_1} ... Q_m^{a_m}(\alpha), \tag{5.2}$$

where $\alpha \in K^*$, and for $i = 1, 2, .., m, [Q_i] \in C_l^{(j)}$ with $j \neq 5$. From this, we get $I^l = (x + \zeta y) = (\varpi_5 \alpha_1 ... \alpha_m \alpha^l)$, where $P_5^{la_0} = (\varpi_5)$, $Q_i^{la_i} = (\alpha_i)$. As in Prop. 2.2 we get $\Delta^{(5)}(x + \zeta y) \equiv \Delta^{(5)}(\varpi_5) \pmod{l}$.

Lemma 5.2. *If $C_l^{(l-5)}$ is non-trivial, then $\Delta^{(5)}(\varpi_5) \equiv 0 \pmod{l}$.*

Proof.

As already mentioned in chapter 4, a consequence of the proof of the main conjecture of Iwasawa is that for $i = 2, 4, ..., l-3$, $|C_l^{(i)}| = |((A^*)_l^+ / CU_l^+)^{(i)}|$, where CU^+ is the group of real cyclotomic units, $(A^*)^+$ is the group of real units, and $((A^*)_l^+ / CU_l^+)^{(i)}$ is defined in the same way as $C_l^{(i)}$. From this it follows that $C_l^{(l-5)} \neq 0 \Rightarrow E_{l-5}$ is an l-th power (cf., [Wa, chapter 8, pp. 146 and 157]). Thus $\left\{ \frac{E_{l-5}}{J} \right\} = 1$ for any ideal J. In particular, letting $J = P_5, \zeta^e = \left\{ \frac{E_{l-5}}{P_5} \right\}$ and using Theorem B of chapter 3, we get

$$0 = e \equiv \pm \frac{r^{l-5} - 1}{2} \frac{\mathbf{B}_{c_5}}{l^{h_5}} \Delta^{(5)}(\upsilon_5) \pmod{l}, \tag{5.3}$$

where $c_5 = (l-6)l^{h_5} + 1$, and $P_5^{l^{h_5}} = (\upsilon_5)$. By Prop. 2.4 and the subsequent remarks, we have $l \nmid \frac{\mathbf{B}_{c_5}}{l^{h_5}}$. Hence $\Delta^{(5)}(\upsilon_5) \equiv 0 \pmod{l}$. We have $P^{la_0} = (\varpi_5)$ and $la_0 \equiv 0 \pmod{l^{h_5}}$. Thus $\Delta^{(5)}(\upsilon_5) \equiv 0 \Rightarrow \Delta^{(5)}(\varpi_5) \equiv 0 \pmod{l}$. $\mathcal{QED}$.

Proof of Theorem 5.1 (2) (contd.)

By the lemma, $\Delta^{(5)}(x + \zeta y) \equiv \Delta^{(5)} \varpi_5 \equiv 0 \pmod{l}$. Since in all of the above x, y, z are interchangeable, we get $\Delta^{(5)}(x + \zeta y) \equiv \Delta^{(5)}(y + \zeta z) \equiv \Delta^{(5)}(z + \zeta x) \equiv 0 \pmod{l}$.

Theorem 5.1 (2) will be proven once we prove the following:

Lemma 5.3. *If x, y, z are as in Theorem 5.1 (1), then*

$$\Delta^{(5)}(x+\zeta y) \equiv \Delta^{(5)}(y+\zeta z) \equiv \Delta^{(5)}(z+\zeta x) \equiv 0 \pmod{l}$$

is impossible.

Proof. let T denote any element of $\{\frac{x}{y}, \frac{y}{z}, \frac{z}{x}\}$. Then an easy computation shows that

$$\Delta^{(5)}(x+\zeta y) \equiv \Delta^{(5)}(y+\zeta z) \equiv \Delta^{(5)}(z+\zeta x) \equiv 0 \Rightarrow T(1-T)(1-10T+T^2) \equiv 0 \pmod{l}.$$

In the remainder of this proof, the congruences will be modulo l.

Clearly, $T \not\equiv 0$ for any $T \in \{\frac{x}{y}, \frac{y}{z}, \frac{z}{x}\}$. If $1 - T \equiv 0 \pmod{l}$ for any two $T \in \{\frac{x}{y}, \frac{y}{z}, \frac{z}{x}\}$, then we get $x \equiv y \equiv z \pmod{l}$. Then $x^l + y^l + z^l = 0$ gives $3x \equiv 3y \equiv 3z \pmod{l}$, which is impossible since l is irregular (and so $l > 3$), and also by assumption $l \nmid xyz$. Suppose 6 has a square root in $\mathbf{Z}/l\mathbf{Z}$, and $1 - 10T + T^2 \equiv 0$ for exactly two $T \in \{\frac{x}{y}, \frac{y}{z}, \frac{z}{x}\}$, and $T \equiv 1$ for the remaining element. Let $u_1, u_2 \in (\mathbf{Z}/l\mathbf{Z})^*$ be the two roots of $1-10T+T^2$. By symmetry, we may assume $x \equiv y$ and $y \equiv u_k z$ where $k \in \{1,2\}$. Then we get, using $x + y + z \equiv 0, z(1 + 2u_k) \equiv 0$. This implies $2u_k \equiv -1$. Using the fact that u_k satisfies $1 - 10T + T^2 \equiv 0$, we get $l|5$, which is impossible. Hence we should have $1 - 10T + T^2 \equiv 0$ for all $T \in \{\frac{x}{y}, \frac{y}{z}, \frac{z}{x}\}$. Then there are at least two elements in $\{\frac{x}{y}, \frac{y}{z}, \frac{z}{x}\}$ which are both equal to the same u_k. We may assume $x \equiv u_1 y, y \equiv u_1 z$. Then we have $x + y + z \equiv 0 \Rightarrow u_1^2 + 2 \equiv 0 \Rightarrow 10u_1 \equiv -1 \Rightarrow l|102 = 3.17.2$, which is impossible. $\mathcal{QED}$.

Proof of (1)

If $C_l^{l-5} \neq 0$, then (1) follows trivially from (2). So we can assume $C_l^{(l-5)} = 0$. We assumed in the beginning that $C_l^{(5)}$ is cyclic. Now we have satisfied for $C_l^{(5)}$ all the conditions that were required for $C_l^{(3)}$ while proving Theorem 4.1. Note that Theorem A of chapter 3 can be easily extended to E_{l-5}. Following exactly the same arguments as in the proof of Theorem 4.1, we arrive at $\Delta^{(5)}(X + \zeta Y) \equiv \Delta^{(5)}(Y + \zeta Z) \equiv \Delta^{(5)}(X + \zeta Y) \equiv 0 \pmod{l}$, where $X = x^{l^{n-1}}, Y = y^{l^{n-1}}, Z = z^{l^{n-1}}$. Applying Lemma 5.3 to X, Y, Z, we arrive at a contradiction.

CHAPTER 6

APPLICATION TO THE SECOND CASE

In this chapter we prove a result in the second case of Fermat's last theorem using the methods discussed in the previous chapters. This result may be known using other methods, but our proof explains the interesting role played by the structure of the ideal class group of the cyclotomic field extension.

Recall that h^+ is of the class number of the maximal real subfield of $\mathbf{Q}(\zeta)$.

Theorem 6.1. If l does not divide h^+, and the equation $x^l + y^l = z^l$ has non-zero integral solutions (x, y, z) with $l|xyz$, then $(x + \zeta y) = I^l$, where I is a *principal* ideal.

Proof.

Assume equation $x^l + y^l = z^l$ has non-zero integral solutions (x, y, z), with $l|xyz$. We may assume that x, y, z are pairwise relatively prime. So l divides exactly one of these. Renaming the variables, we may assume that $l|x$. Changing z to $-z$, equation (2.1) can be written as

$$\prod_{i=0}^{l-1}(x + \zeta^i y) = z^l. \tag{6.1}$$

We have from Lemma 2.1a (2),

$$(x + \zeta y) = I^l. \tag{6.1a}$$

If I is principal, we are done. Therefore, assume that I is nonprincipal. Thus $[I]$ has order precisely l in the ideal class group C. Let $\mathbf{B}_{i_1}$, $\mathbf{B}_{i_2}$, ...$\mathbf{B}_{i_s}$, with

$\{i_1, ..., i_s\} \subset \{2, 4, ..., l-1\}$, be the Bernoulli numbers divisible by l. By Herbrand's theorem (see chapter 2), and the assumption that $l \nmid h^+$, we have $C_l = C_l^{(3)} \oplus C_l^{(5)} \oplus .....C_l^{(l-2)}$, the $C_l^{(i)}$ being the eigenspaces under the action of the Teichmüller Character (as defined in chapter 2). When $l \nmid h^+$, we have [Wa], p. 197, Cor. 10.15]

$$C_l^{(i)} \simeq \mathbf{Z}_l / \mathbf{B}_{1,\omega^{-i}} \mathbf{Z}_l, \quad \text{for } i = 3, 5, .., l-2. \tag{6.2a}$$

Thus $C_l^{(i)}$ is cyclic for $i = 3, 5, ..., l-2$..

Note: Even when $l | h^+$, a theorem of Mazur and Wiles ([MW]; See also [Wa], p. 198, Remark) says that the order of $C_l^{(i)}$ is the l-part of $\mathbf{B}_{1,\omega^{-i}}$. But we will not need this result here.

For $i = 3, 5, .., l-2$, let X_i be an ideal class which generates $C_l^{(i)}$. By the Tchebotarev density theorem, we may (and we will) choose a prime ideal Q_i *of degree* 1, which is different from (λ), such that X_i is the class $[Q_i]$.

As already mentioned, $[I]$ has order exactly l in C_l and thus $[I] \in C_l$. Let $\mathcal{J} \subseteq \{3, 5, ..., l-2\}$ be the set of indices j such that $[I]$ has non-trivial component in $C_l^{(j)}$. Let $m = |\mathcal{J}|$. Note that $m \geq 1$ because I is not principal. We get:

$$[I] = \prod_{j \in \mathcal{J}} [Q_j^{k_j}] \tag{6.2}$$

where the $k_j, j \in \mathcal{J}$, are non-negative integers. Then we can write

$$I = \prod_{j \in \mathcal{J}} Q_j^{k_j} (\frac{\gamma}{\delta}) \tag{6.3}$$

where γ, δ are nonzero elements of A. As before, γ, δ, can be chosen so that $(\lambda) \nmid (\gamma), (\lambda) \nmid (\delta)$.

Lemma 6.2. *There exist* $\alpha_1, ..., \alpha_n \in A - (\lambda)$ *such that* $Q_j^{k_j l} = (\alpha_j), \forall\, j \in \mathcal{J}$, *and*

$$(x + \zeta y)\delta^l = \eta\alpha_1 ... \alpha_m \gamma^l, \text{ with } \eta \in A^* \text{ and } \gamma, \delta \in A - (\lambda). \tag{6.4}$$

Proof.

$$\text{Since } I^l = (x + \zeta y), \text{ we get } (x + \zeta y)(\delta)^l = \prod_{j \in \mathcal{J}} Q_j^{k_j l} (\gamma)^l.$$

This gives the following relation in C_l, written additively: $\sum_{j \in \mathcal{J}} [Q_j^{k_j l}] = 0$. Since C_l is a direct sum of the $C_l^{(j)}$, and since $[Q_j^{k_j l}] \in C_l^{(j)}$, this implies that each $[Q_j^{k_j l}]$ must be trivial in C_l. So we can write, $\forall\, j \in \mathcal{J}$, $Q_j^{k_j l} = (\alpha_j)$, for some $\alpha_j \in A - (\lambda)$. Hence the lemma. $\mathcal{QED}$.

Remark: For every $j \in \mathcal{J}$, $[Q_j^{k_j}]$ has order exactly l in C_l.

Since in equation (6.4), $\gamma, \delta, \alpha_1, ..., \alpha_m$ were chosen such that they were not divisible by λ, the logarithmic derivative operator $\Delta^{(k)}$ is defined for all of them, for any $k = 1, ..., l - 2$. Apply $\Delta^{(k)}$ to both sides of equation(6.4). By Prop. 1.4a, we know that $\Delta^{(k)}$ vanishes on the l-th powers of elements in $A - (1 - \zeta)$. Thus $\Delta^{(k)}(\gamma^l) \equiv \Delta^{(k)}(\delta^l) \equiv 0 \pmod{l}$. By Prop. 1.5, $\Delta^{(k)}(\eta) \equiv 0 \pmod{l}$, $\forall k \in \{3, 5, ..., l - 2\}$. Using Lemma 1.1, we get the following for any odd k, $1 < k < l$, by the additivity of the logarithmic derivative:

$$\Delta^{(k)}(x + \zeta y) \equiv \left(\sum_{j=1}^{m} \Delta^{(k)}(\alpha_j) \right) \pmod{l}. \tag{6.5}$$

Henceforth, for the sake of clarity, let i_0 be a fixed element of $\mathcal{J}$. All the results below that involve i_0 will hold for any element of $\mathcal{J}$. Applying Prop. 2.2 to

equation (6.5), we get

$$\Delta^{(i_0)}(x+\zeta y) \equiv \Delta^{(i_0)}(\alpha_{i_0}) pmodl.$$

Proposition 6.3. *Let i_0 be as above. Then $\Delta^{(i_0)}(\alpha_{i_0}) \not\equiv 0 \ (mod\ l)$.*

Note that for theorem B, we only need to assume that $C_l^{(i)}$ is cyclic, where $i \in \{3,5,..,l-2\}$. Let P be a prime ideal *of degree 1* whose ideal class generates $C_l^{(i)}$. Let $h_i = v_l(|C_l^{(i)}|)$, and set $P^{l^{h_i}} = (v)$. Let $c = (l-1-i)l^{h_i}+1$, and set $\left\{\frac{E_{l-i}}{P}\right\} = \zeta^e$, with $e \in (\mathbf{Z}/l\mathbf{Z})$. Then we have

$$e \equiv \pm \frac{r^{l-i}-1}{2} \frac{\mathbf{B}_c}{l^{h_i}} \Delta^{(i)}(v) \qquad (mod\ l). \tag{6.6}$$

From equation (6.2a) above we have, $\forall\ i \in \{3,5,...,l-2\}$, $v_l(|(C_l^{(i)})|) = v_l(\mathbf{B}_{1,\omega^{-i}})$. For such i, let $h_i = v_l(|(C_l^{(i)})|)$. Then $v_l(\mathbf{B}_{1,\omega^{-i}}) = h_i$. Setting $n = h_i$ in Prop. 2.4, we get $v_l(\mathbf{B}_{c_{h_i}}) = h_i$. Dropping the subscript h_i from c_{h_i} as we did in Theorem B (chapter 3), we get $l \nmid \frac{\mathbf{B}_c}{l^{h_i}}$.

Note: Even when $l|h^+$, we can get the result above by using a theorem of Mazur-Wiles [MW], which says that $v_l(\mathbf{B}_{1,\omega^{-i}}) = h_i$, for every $i \in \{3,5,...,l-2\}$.

Proof of Prop. 6.3: As already shown by equation(6.2), when $l \nmid h^+$, $C_l^{(i)}$ is cyclic. So Theorem V is valid, with $i = i_0$, $P = Q_{i_0}$, and $\zeta^e = \left\{\frac{E_{l-i_0}}{Q_{i_0}}\right\}$. Since r is a primitive root modulo l, we get from Theorem V using the fact that $l \nmid \frac{\mathbf{B}_c}{l^{h_{i_0}}}$ (proved above),

$$\Delta^{(i_0)}(v) \equiv 0 \ \Leftrightarrow e \equiv 0 \pmod{l}. \tag{6.7}$$

By the remark following Lemma 6.2, $[Q_{i_0}^{k_{i_0}}]$ has order exactly l in C_l. So we must have $k_{i_0} l = t l^{h_{i_0}}$, with t prime to l, and $(\alpha_{i_0}) = Q_{i_0}^{k_{i_0} l} = (v)^t$. Then, by using

Prop 1.5 and Lemma 1.1, we have

$$t\Delta^{(i_0)}(v) \equiv \Delta^{(i_0)}(\alpha_{i_0}) \qquad (\text{mod } l) \tag{6.8}$$

Thus

$$\Delta^{(i_0)}(\alpha_{i_0}) \equiv 0 \ \Leftrightarrow e \equiv 0(mod\ l).$$

Prop 6.3 is hence a consequence of the following:

Proposition 6.4. *Let e be defined, as above, by $\zeta^e = \left\{\frac{E_{l-i_0}}{Q_{i_0}}\right\}$. Then $l \nmid e$.*

Proof of Prop. 6.4. Let H_l be the maximal abelian unramified l-extension of K. Then the Artin map gives the isomorphism $C_l \xrightarrow{\sim} Gal(H_l/K)$ which sends the ideal class [P] of any prime ideal P in K to the Frobenius element $\left(\frac{H_l/K}{P}\right)$.

Definition: A unit $\eta \in A^*$ is called *singular primary* if:

$$\eta \equiv u^l \ \ (mod\ \lambda^l) \ \text{ for some } u \in A.$$

If, for $i \in \{3, 5, ..., l-2\}$, $C_l^{(i)}$ is nontrivial, then by Herbrand's theorem, $l|\mathbf{B}_{l-i}$. Thus by Lemma 4.2, $K(E_{l-i}^{1/l})$ is a nontrivial extension of K contained in H_l. Moreover, by the corollary to lemma 4.2, $\left\{\frac{E_{l-i}}{M}\right\} = 1$ when M is a principal ideal which is prime to (λ).

Now, assume $l|e$, where $e = \left\{\frac{E_{l-i_0}}{Q_{i_0}}\right\}$. We will get a contradiction. Let $[X]$ be any ideal class in C_l. Represent it by a prime ideal J different from (λ).

Claim:

$$l|e \Rightarrow \left\{\frac{E_{l-i_0}}{J}\right\} = 1.$$

Indeed, in C_l we can write (additively),

$$[J] = \sum_{m=1}^{s} a_m[Q_{i_m}], \text{ where } a_1, ..a_s \in \mathbf{Z}.$$

Hence we can write $J = Q_{i_1}^{a_1} ....Q_{i_s}^{a_s}(\beta)$, where $\beta \in K^*$, and β can be written as the ratio of two algebraic integers which are prime to (λ).

Consider $\left\{\frac{E_{l-i_0}}{J}\right\} = \left\{\frac{E_{l-i_0}}{Q_{i_1}^{a_1} ....Q_{i_s}^{a_s}(\beta)}\right\}$.

By Lemma 4.4, $\left\{\frac{E_{l-i_0}}{Q_{i_m}}\right\} = 1$ if $i_m \neq i_0$. By the assumption that $l|e$, $\left\{\frac{E_{l-i_0}}{Q_{i_0}}\right\} = 1$. Since (β) is principal, $\left\{\frac{E_{l-i_0}}{(\beta)}\right\} = 1$. Thus by the multiplicativity of the power residue symbol, we get $\left\{\frac{E_{l-i_0}}{J}\right\} = 1$. Hence the claim.

This claim implies that the Frobenius $\left(\frac{H_l/K}{J}\right)$ induces the trivial automorphism of $K(E_{l-i_0}^{1/l})$ over K, for all J as above. This is impossible, since $K(E_{l-i_0}^{1/l})$ is a nontrivial extension of K contained in H_l, as noted in the beginning of this proof. Hence we get a contradiction. This proves Prop. 6.4 and Prop. 6.3. $\mathcal{QED}$.

Note: Proposition 6.4 could also have been proven using the following:

Fact: ([Wa], p. 166, exercise 8.9) Let $\mathcal{G} = Gal(K(E_{i_1}^{1/l}, ..., E_{i_s}^{1/l})/K)$, where $i_1, ..., i_s$ are the indices for which $l|\mathbf{B}_m, 2 \leq m \leq l-3$. When $l \nmid h^+$, we have

$$\mathcal{G} \simeq C_l/lC_l.$$

Proof of Main Theorem (contd.)

Claim.

$$\Delta^{(i)}(x + \zeta y) \equiv 0 \ (mod\ l) \text{ for } i = 3, 5, ..., l-2.$$

Indeed, for $m = 1, 3, .., l-4$,

$$\Delta^{(2+m)}(x+\zeta y) = \frac{d^m}{dv^m}\left(\frac{d^2}{dv^2} log\ (x+(e^v)y)\right)\Big|_{v=0}$$
$$= \frac{d^m}{dv^m}\left(\frac{xye^v}{(x+e^v y)^2}\right)\Big|_{v=0} = xy\left[\frac{d^m}{dv^m}\left(\frac{e^v}{(x+e^v y)^2}\right)\Big|_{v=0}\right]$$

Since $l|x$, we get $\Delta^{(i)}(x+\zeta y) \equiv 0\ (mod\ l)$ for $i = 3, 5, ..., l-2$. Done.

By Proposition 6.2, we get $\Delta^{(i_0)}(x+\zeta y) \equiv \Delta^{(i_0)}(\alpha_{i_0})$ (mod l), which is $\equiv 0$ (mod l) by the claim. Now we get a contradiction in view of Proposition 6.3.

$\mathcal{QED}$.

Chapter 7

APPLICATION TO AN EQUATION IN FOUR VARIABLES

In this chapter we describe an application of Vandiver's methods described in the previous chapters to prove a result about a diophantine equation in four variables. This equation is a generalization of the equation (2.1). This result is only preliminary, and it is included here in the hope that further improvements of the techniques used above would strengthen it.

In the three variable case, we have the "Fermat equation" (equation (2.1)) which can be factorized as a product of linear terms.

$$x^l + y^l = \prod_{i=0}^{l-1}(x + \zeta^i y) = z^l$$

We now consider the following equation in four variables:

$$\prod_{i-0}^{l-1}(x + \zeta^i y + \zeta^{2i} z) = w^l. \tag{7.1}$$

Though this equation is in $\mathbf{Z}[x, y, z, w]$, there is no short and simple expression for this equation as in the three variable case. Furthermore, if equation (2.1) is satisfied, i.e, $x^l + y^l = z^l$, and $l \nmid xyz$, then we know that the principal ideals $(x + \zeta^i y)$ in (7.1) are relatively prime to each other for $i = 0, 1, .., (l-1)$ and to $\lambda = (1 - \zeta)$. But for the four variable case, there are no such simple conditions for the trinomials in (7.1) to be relatively prime to each other. For example, if $l = 3$, we needed $l \nmid w$ and $(y^3 - z^3, w) = 1$ in order that the corresponding trinomials

are relatively prime.

So for the rest of this chapter, we will simply assume that the terms $(x+\zeta^i y+\zeta^{2i}z)$ *in equation (7.1) are relatively prime, for* $i=0,1,...,(l-1)$.

Main result.

Theorem 7.1. *Assume* $h_3 = v_l(|C_l^{(3)}|) = 1$. *If the equation (7.1) has nontrivial integral solutions, then*

(1) $l|xyw$, *or*

(2) $l \nmid z$, *or*

(3) $\exists$ *an odd prime* q *such that* $q|w$, *but* $q \nmid z$, *or*

(4) $x \equiv y \pmod{l}$.

Proof.

For the proof we need the following easy extension of Prop. 3.1. The proof follows that of Vandiver ([V2], p. 217).

Theorem 7.2.

If x,y,z,w *satisfy equation (7.1), then*

$$\prod_{n=1}^{\frac{l-1}{2}}(x+\zeta^{n'}y+\zeta^{2n'}z) = \zeta^g\omega^l\ , \tag{7.2}$$

where $\omega \in A$ *and* $g \in \mathbf{Z}$.

Proof. Since we assumed that the factors $(x+\zeta^i y+\zeta^{2i}z)$ for $i=0,1,2,..,(l-1)$ are relatively prime, equation (7.1) gives

$$x+y+z=c^l, \qquad \text{with } c \in \mathbf{Z}. \tag{7.3}$$

$$x+\zeta y+\zeta^2 z = I^l, \qquad I \text{ an integral ideal.} \tag{7.4}$$

For any ideal J of A, we have the following Stickelberger type relation:

$$\prod_{n=0}^{\frac{l-1}{2}} \sigma_{n'}(J) = (\alpha)^l, \text{ where } \alpha \in A.$$

Applying this to equation (7.4), we get

$$\prod_{n=0}^{\frac{l-1}{2}} (x + \zeta^{n'} y + \zeta^{2n'} z) = \eta \alpha^l, \qquad \text{where } \eta \in A \text{ is a unit, and } \alpha \in A. \tag{7.5}$$

Let $\eta = \eta(\zeta)$, and $\alpha = \alpha(\zeta)$, where $\eta(x), \alpha(x) \in \mathbf{Z}[x]$.

Applying σ_{-1} to (7.5), we get

$$\prod_{n=0}^{\frac{l-1}{2}} (x + \zeta^{-n'} y + \zeta^{-2n'} z) = \eta(\zeta^{-1})(\alpha(\zeta^{-1}))^l. \tag{7.6}$$

Multiplying (7.5) and (7.6), and using (7.1) and (7.2), we find that the ideal $(\alpha(\alpha(\zeta^{-1}))) = (\frac{w}{c})$. Hence $\alpha(\alpha(\zeta^{-1}) = E(w/c)$, where $E \in A$ is a unit. Taking the product of (7.5) and (7.6) again, we find that

$$\eta(\eta(\zeta^{-1}))E^l = 1. \tag{7.7}$$

But we know, by a basic result, that

$$\eta = \zeta^g \epsilon, \tag{7.8}$$

where $\epsilon \in A^+ = \mathbf{Z}[\zeta + \zeta^{-1}]$ is a real unit and $g \in \mathbf{Z}$. From (7.5) and (7.8) we get $\epsilon^2 = E^{-l}$. Since l is odd, we can find integers a, b such that $2a = 1 + bl$, so that $\epsilon^{2a} = \epsilon\epsilon^{bl} = E^{-al}$. Hence $\epsilon = (\epsilon^{-b} E^{-a})^l$, and $\eta = \zeta^g (\epsilon^{-b} E^{-a})^l$. Substituting for η in (7.5), we get Theorem 7.2.

Assume that none of the conditions of Theorem 7.1 are satisfied and that equation (7.1) has solutions. We will get a contradiction. By the contrapositive of

condition (3), any prime number that divides w also divides z. Thus any prime ideal of A that divides $(x+\zeta y+\zeta^2 z)$ also divides (z). Let P be such a prime ideal. We will prove that $\left\{\frac{E_{l-3}}{P}\right\} = 1$, which will yield $\left\{\frac{E_{l-3}}{I}\right\} = 1$ by multiplicativity, where I is as in equation (7.4). The proof is almost identical to that of Theorem A in chapter 3:

Recall the following claim that was proven in Chapter 3, Section 1:

Either $kn' \not\equiv 1 \pmod{l}$, *for all* n, $1 \leq n \leq \frac{l-1}{2}$ *(Or)* $-kn' \not\equiv 1 \pmod{l}$, *for all* n, $1 \leq n \leq \frac{l-1}{2}$.

By this claim, we have, if $P|(x+\zeta y+\zeta^2 z)$, then $P \nmid (x+\zeta^{\pm kn'}+\zeta^{(\pm k)2n'}z)$ $\forall n \in \{1,2,..,\frac{l-1}{2}\}$.

So from (7.2), using the fact that $P|(z)$, we get

$$\prod_{n=1}^{\frac{l-1}{2}} \left\{\frac{x+\zeta^{\pm kn'}y}{P}\right\} = \left\{\frac{\zeta^{\pm kg}}{P}\right\}. \tag{7.9}$$

But this is just equation (3.9). The rest of the proof for showing $\left\{\frac{E_{l-3}}{P}\right\} = 1$ is exactly the same as in chapter 3. Now from equation (7.4), we have that I^l is principal, which means that $[I] \in C_l$. If I were principal, we get from equation (7.4) that $x+\zeta y+\zeta^2 z = \eta\alpha^l$, where η is a unit in A and α is a nonzero element in A. Taking logarithmic derivatives, we get $\Delta^{(3)}(x+\zeta y+\zeta^2 z) \equiv 0 \pmod{l}$.

Claim. $\Delta^{(3)}(x+\zeta y+\zeta^2 z) \equiv 0 \pmod{l}$ *is impossible, if all the conditions (1) to (4) of equation (7.1) are not satisfied.*

Proof.

Since, by the contrapositive of condition (2), we have $z \equiv 0 \pmod{l}$, we get $\Delta^{(3)}(x+\zeta y+\zeta^2 z) \equiv \Delta^{(3)}(x+\zeta y) \equiv 0 \pmod{l} \Rightarrow \frac{xy(x-y)}{x+y} \equiv 0 \pmod{l}$. By the

contrapositive of condition (1) we get $l \nmid x, y$, and w. Now reducing equation (7.1) modulo l we get $x+y+z \equiv x+y \equiv w \pmod{l}$. Thus $\frac{xy(x-y)}{x+y} \equiv 0 \pmod{l} \Rightarrow x \equiv y \pmod{l}$ which would imply that condition (4) is satisfied, a contradiction.

Thus we may assume I is not principal. We have $\left\{\frac{E_{l-3}}{I}\right\} = 1$. But now we are in the same situation as in equation (4.4), chapter 4. Proceeding as in that chapter, with $n = 1$, we get $\Delta^{(3)}(x+\zeta y+\zeta^2 z) \equiv 0 \pmod{l}$, which contradicts the claim that was just proved.

APPENDIX

Proof of Lemma 1.2.

The following proof is essentially the same as in [V4, pp.401-408]. It is included here for completeness.

Let k be an integer such that $1 < k < l-1$, and $F, G \in \mathbf{Z}[x]$ such that

(1) $F(\zeta) = G(\zeta)$.

(2) $F(1) = G(1) \pmod{l^{i+1}}$.

(3) $G(1) \not\equiv 0 \pmod{l}$.

Then we have to show:

$$\Delta^{(kl^i)}(F) \equiv \Delta^{(kl^i)}(G) \pmod{l^{i+1}}.$$

Proof

Recall $\Phi(x) = 1 + x + x^2 + ... + x^{l-1}$.

$$F(\zeta) = G(\zeta) \Rightarrow F(e^v) = G(e^v) + (e^{lv} - 1)V + m\Phi(e^v)$$

for some $V \in \mathbf{Z}[x], m \in \mathbf{Z}$. By condition (2), we get $m = c_1 l^i$, with $c_1 \in \mathbf{Z}$. Therefore, to prove the lemma, it is enough to show that

$$\Delta^{(kl^i)}(1 + \frac{(e^{lv}-1)}{G(e^v)}V + \Phi(e^v)\frac{c_1 l^i}{G(e^v)}) \equiv 0 \pmod{l^{i+1}}.$$

Let $W = \dfrac{V}{G(e^v)}, Z = \dfrac{c_1 l^i}{G(e^v)}, x = (e^{lv}-1)W, y = x + \Phi(e^v)Z.$

We have to show:

Lemma A1.

$$\Delta^{(kl^i)}(1+y) \equiv \Delta^{(kl^i)}(1+x) \equiv 0 \pmod{l^{i+1}}.$$

Proof. First we show $\Delta^{(kl^i)}(1+y) \equiv \Delta^{(kl^i)}(1+x) \pmod{l^{i+1}}$.

Define $D = \frac{d}{dv}$ and $D_0^m(f(v)) = \frac{d^m}{dv^m}(f(v))\Big|_{v=0}$. Then

$$D^{(kl^i)}(log(1+y)) = D^{(kl^i-1)}(\frac{Dy}{(1+y)}).$$

Expanding by Leibnitz's rule and taking the value at $v = 0$, we get

$$D_0^{(kl^i-1)}(\frac{Dy}{(1+y)}) = \frac{1}{1+y}D_0^{(kl^i)}y + (kl^i-1)D_0(\frac{1}{1+y})D_0^{(kl^i-1)}y + ...$$
$$..... + D_0^{(kl^i-1)}(\frac{1}{1+y})D_0y$$

From the above expansion, we see that

$$D_0^{(kl^i-1)}(\frac{Dy}{(1+y)}) \equiv D_0^{(kl^i-1)}(\frac{Dx}{(1+x)}) \pmod{l^{i+1}}$$

because:

(1) $D_0y \equiv 0 \pmod{l}$.

(2) Let $m \neq 0$. Note that if $l-1 \nmid k$, then for any $m \geq 0$, we have $l-1 \nmid kl^i - m$ or $l-1 \nmid m$, and hence:

$$D_0^{(m)}\left(\frac{1}{1+y}\right)D_0^{(kl^i-m)}y \equiv D_0^{(m)}\left(\frac{1}{1+x}\right)D_0^{(kl^i-m)}x \pmod{l^{i+1}}.$$

(3) $D_0^{(kl^i)}y \equiv D_0^{(kl^i)}x \pmod{l^{i+1}}$ because $l-1 \nmid kl^i$.

Hence

$$\Delta^{(kl^i)}(1+y) \equiv \Delta^{(kl^i)}(1+x) \pmod{l^{i+1}}.$$

Now we only have to show that $\Delta^{(kl^i)}(1+x) \equiv 0 \pmod{l^{i+1}}$.

Claim

$$\Delta^{(kl^i)}(1+x) \equiv D_0^{(kl^i-1)}(D(x)(1+x)^{l^i-1}) \pmod{l^{i+1}}.$$

We have $D_0(x) \equiv 0 \pmod{l}$, and $D_0^{(m)}((1+x)^{l^i}) \equiv 0 \pmod{l^{i+1}}$ if $m \geq 1$.

Moreover, $(1+x)|_{v=0} = 1$.

So we get

$$D_0^{(kl^i-1)}(D(x)(1+x)^{l^i-1}) = D_0^{(kl^i-1)}(\frac{D(x)}{(1+x)}(1+x)^{l^i})) = (D_0^{(kl^i-1)}(\frac{D(x)}{(1+x)}))((1+x)^{l^i})_{v=0}$$
$$\equiv D_0^{(kl^i-1)}(\frac{D(x)}{(1+x)}) \equiv \Delta^{(kl^i)}(1+x) \pmod{l^{i+1}}$$

Hence the Claim.

Thus we need to show $M = D_0^{(kl^i-1)}(D(x)(1+x)^{l^i-1}) \equiv 0 \pmod{l^{i+1}}$.

Claim

$$M \equiv (-1)^{n-1} \sum_{n=1}^{l^i} \frac{1}{n}(D_0^{(kl^i)}(x^n)) \pmod{l^{i+1}}.$$

We have

$$M = D_0^{(kl^i)}(D(x) + (l^i-1)xD(x) + \binom{l^i-1}{2}x^2D(x) + \ldots\ldots\ldots + x^{l^i-1}D(x))$$
$$= \sum_{n=1}^{l^i}((\frac{1}{n}D_0^{(kl^i)}(x^n))\binom{l^i-1}{n-1}).$$

Since $D^{(m)}(x) \equiv 0 \pmod{l}$ $\forall m \geq 0$ and $\binom{l^i-1}{n-1} \equiv (-1)^{n-1} \pmod{l^i}$, we get

$$M \equiv (-1)^{n-1} \sum_{n=1}^{l^i} \frac{1}{n}(D_0^{(kl^i)}(x^n)) \pmod{l^{i+1}}.$$

Hence the Claim.

So we have to show that

$$(-1)^{n-1}\sum_{n=1}^{l^i}\frac{1}{n}(D_0^{(kl^i)}(x^n))\equiv 0 \pmod{l^{i+1}}.$$

Let $x^n=((e^{lv}-1)W)^n=W_1(e^{lv}-1)$ for some rational function W_1. Lemma 1.2 will be proved if we show:

Lemma A2.

$$\frac{1}{n}D_0^{(kl^i)}(x^n)\equiv 0 \pmod{l^{i+1}}.$$

Proof. We consider two cases.

Case A $n\not\equiv 0 \pmod{l}$.

In this case we only need to show

$$D_0^{(kl^i)}(x^n)\equiv 0 \pmod{l^{i+1}}.$$

We have

$$\begin{aligned}D^{(kl^i)}(x^n)&=D^{(kl^i)}(W_1(e^{lv}-1))\\&=(e^{lv}-1)D^{(kl^i)}(W_1)+(kl^i)D(e^{lv}-1)D^{(kl^i-1)}(W_1)+\ldots\\&\quad\ldots..+(W_1)D^{(kl^i)}(e^{lv}-1)\\&=(e^{lv}-1)D^{(kl^i)}(W_1)+(kl^i)le^{lv}D^{(kl^i-1)}(W_1)+\ldots\\&\quad\ldots..+\binom{kl^i}{m}l^m e^{lv}D^{(kl^i-m)}(W_1)+\ldots...+(W_1)D^{(kl^i)}(e^{lv}-1).\end{aligned}$$

We are done if we show that $\binom{kl^i}{m}l^m\equiv 0 \pmod{l^{i+1}}$ for $0<m\le kl^i$.

$$\text{i.e., }\frac{(kl^i)(kl^i-1)\ldots(kl^i-m+1)}{m(m-1)..3.2.1}l^m\equiv 0 \pmod{l^{i+1}}.$$

Since $m\ge 1$, enough to show

Prop A3. $v_l(\frac{(kl^i-1)...(kl^i-m+1)}{(m-1)..3.2.1}) \geq 0.$

Indeed, for each $1 \leq j \leq m-1$, $v_l(\frac{kl^i-m+j}{m-j}) = 0.$

Hence Prop A3 and Case A of the lemma.

Case B $n = l^u m$, for some m prime to l, and $l^u m \leq l^i k$. Let $x^n = W_2(e^{(lv)}-1)^{l^u}$, where W_2 is some rational function.

We can write

$$\frac{1}{n}D^{(kl^i)}(x^n) = \frac{1}{n}D^{(kl^i)}(W_2(e^{lv}-1)^{l^u}) = \sum_{j=0}^{l^u}\frac{1}{n}D^{(kl^i)}(W_2(e^{lv})^{l^u-j}(-1)^j)\binom{l^u}{j}.$$

In the general term of the above sum, neglect the parts which are prime to l and consider the expression $\frac{1}{l^u}D^{(kl^i)}(W_2(e^{lv})^{l^u-j})\binom{l^u}{j}$, $0 \leq j \leq l^u$. The general term in its Leibnitz expansion can be written as

$$\frac{1}{l^u}\binom{kl^i}{k_1 l^{i_1}}\binom{l^u}{j}D^{k_1 l^{i_1}}((e^{lv})^{l^u-j})D^{(kl^i-k_1 l^{i_1})}(W_2), \text{ where } i_1 \geq 0, l \nmid k_1. \qquad (A1)$$

Claim

$$\frac{1}{l^u}\binom{l^u}{j}D^{m_1}((e^{lv})^{l^u-j}) \equiv 0 \pmod{l^{m_1}}.$$

We need to show

$$l^{m_1}(l^u-j)^{m_1}\binom{l^u}{j}\frac{1}{l^u} \equiv 0 \pmod{l^{m_1}}.$$

Clearly, $v_l(\frac{l^{m_1}(l^u-j)^{m_1}}{j}) \geq m_1$. Using Prop. A3, $v_l(\binom{l^u-1}{j-1}) \geq 0$. Hence

$$v_l(\frac{1}{l^u}\binom{l^u}{j}D^{m_1}((e^{lv})^{l^u-j})) \geq m_1.$$

Hence the Claim.

Using the above claim on eqn (A1), we get

$$v_l\left(\left[\frac{1}{l^u}\binom{l^u}{j}D^{(k_1 l^{i_1})}((e^{lv})^{l^u-j})\right]\binom{kl^i}{k_1 l^{i_1}}D^{(kl^i-k_1 l^{i_1})}(W_2)\right)$$

$$\geq v_l\left(\binom{kl^i}{k_1 l^{i_1}}D^{(kl^i-k_1 l^{i_1})}(W_2)\right)+k_1 l^{i_1}$$

Now, $v_l(\binom{kl^i}{k_1 l^{i_1}}) = i - i_1 + v_l(\binom{kl^i-1}{k_1 l^{i_1}-1}) \geq i - i_1$, using Prop A3.

Thus

$$v_l\left(\frac{1}{l^u}\binom{kl^i}{k_1 l^{i_1}}\binom{l^u}{j}D^{k_1 l^{i_1}}((e^{lv})^{l^u-j})D^{(kl^i-k_1 l^{i_1})}(W_2)\right) \geq i - i_1 + k_1 l^{i_1} \geq i+1.$$

From this Lemma A2 follows. Hence Lemma A1 and Lemma 1.2 $\mathcal{QED}$.

References

[Ca-F]. J. W. S. Cassels and A. Frohlich, *Algebraic Number Theory*, Thompson Book Co. Inc., 1967.

[E]. M. Eichler, *Eine bemerkung zur Fermatschen vermutung*, Acta Arithmetica **11** (1965), 129-131.

[Fi]. M. Filaseta, *An application of Falting's result to Fermat's Last Theorem*, C. R. Acad. Sci. Canada **6** (1984), 31-32.

[F]. P. Fürtwangler, *Letzter Fermatschen satz und Eisensteins'schen Reziprozitatsgesetz.*, Sitzungsber. Akad. d. Wissen. Wien.IIa **121** (1912), 589-592.

[GP]. A. Granville and B. Powell, *On Sophie Germain type criteria for Fermat's Last Theorem*, Acta Arithmetica (1988), 265-277.

[Ha]. H. Hasse, *Vandiver's congruence for the relative class number of the p-th cyclotomic field*, J. of Math. Anal. and Appl., **15** (1966), 87-90.

[He]. J. Herbrand, *Sur les classes des corps circulaires*, J. Math. et Phys. **11** (1932), 417-441.

[Hi]. D. Hilbert, *Theorie des Corps de Nombres Algebriques*, Librairie Scientifique, 1913.

[Ko]. V. A. Kolyvagin, *Euler systems* (translated by Neal Koblitz) in The Grothendieck Festschrift (Vol II), P. Cartier, et al., eds., (1990), Birkhäuser, Boston, 435-483.

[K]. E. E. Kummer, *Über die Erganzungsatze zu den allgemeinen Reziprozitatsgesetzen.*, J. fur Mathematik **44** (1852), 95-106.

[K2]. E. E. Kummer, *Einige Satze Über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen...*, Mathematische Abhandlungen (1857), 41-74.

[K3]. E. E. Kummer, *Über die Erganzungsatze zu den allgemeinen Reziprozitatsgesetzen.*, J. fur Mathematik **56** (1859), 270-279.

[Ku]. M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbf{Z}$., Compositio Mathematica **81** (1992), 223-236.

[L]. S. Lang, *Cyclotomic Fields*, Springer Verlag, 1980.

[MW]. B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Inventiones Mathematicae **76** (1984), 179-330.

[Mc]. W. G. McCallum, *The arithmetic of Fermat curves*, Mathematische Annalen **294** (1992), 503-511.

[Mo]. T. Morishima, *Über die Einheiten und Idealklassen des Galoisschen Zahlkorpers und die Theorie des Kreiskorper de* l^ν*-ten Einheitswurzeln*, Japan J. of Math. **10** (1933), 83-66.

[Ri]. P. Ribenboim, *Thirteen Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[R]. K. Ribet, *A modular construction of unramified p-extensions of* $\mathbf{Q}(\mu_p)$., Inventiones Mathematicae **34** (1976), 151-162.

[V1]. H.S. Vandiver, *Fermat's last theorem and the second factor in the cyclotomic class number*, Bull. of Amer. Math. Soc. (1934), 118-123.

[V2]. H.S. Vandiver, *A property of cyclotomic integers and its relation to the Fermat's last theorem*, Annals of Math. **26** (1925), 217-232.

[V3]. H.S. Vandiver, *Symmetric functions formed by systems of elements of a finite algebra and their connection with Fermat's quotient and Bernoulli numbers*, Annals of Math. **18** (1917), 105-114.

[V4]. H. S. Vandiver, *On power characters of singular integers in a properly irregular cyclotomic field*, AMS Transactions **32** (1930), 391-408.

[V5]. H. S. Vandiver, *On Fermat's Last Theorem*, AMS Transactions **31** (1929), 613-642.

[Wa]. L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

[Wa2]. L. Washington, *On Fermat's Last Theorem*, J. reine.u.amgew. Math. **289** (1977), 115-117.