SOME PROBLEMS IN NUMBER THEORY

by

Prem Prakash Pandey

(Math10200604008)

The Institute of Mathematical Sciences

Chennai 600113

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

For the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

July, 2012

Homi Bhabha National Institute

Recommendations of the Viva Voce Board

As members of the Viva Voce Board, we certify that we have read the dissertation prepared by Prem Prakash Pandey entitled "Some Problems in Number Theory" and recommend that it maybe accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.

_____ Date:
Chair and Convener - Prof. R. Balasubramanian

_____ Date:
Member - Prof. K. Srinivas

_____ Date:
Member - Dr. Sanoli Gun

_____ Date:
External Examiner - Prof. B. Sury

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to HBNI.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it may be accepted as fulfilling the dissertation requirement.

Date:

Place: **Guide: Prof. R. Balasubramanian**

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of HBNI.

Brief quotations from this dissertation are allowable without permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the competent authority of HBNI when in his or her judgment proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Prem Prakash Pandey

Candidate

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree/diploma at this or any other Institution/University.

Prem Prakash Pandey

Candidate

Acknowledgement

First and foremost I would like to thank my advisor Prof. R. Balasubramanian, who has been constant inspiration throughout. He granted me all the freedom to enjoy life but also made sure that my stay in the Institute is not limited to enjoyment. I could make any silly mistake and he will correct it cheerfuly and sometimes same mistake he will correct repeatedly with the same smile. Whenever I had a rough phase of life he made sure that I am not grilled in between mental and academic pressure. The enthusiasm he takes in doing any activity was very inspiring throughout. The way he explains ideas it looks that doing Mathematics is so easy. It is wonderful to see him in action. Jahanpanah Tussi Great ho!

Sanoli has always been there to help. If a problem solved, I never cared to write but she has constantly presurrized me to write down the things I work and finish the thesis quickly. Also she has always stood by me as a good friend and made me feel good at times when everything was going otherway. Dr. Purusottam Rath has helped everytime I landed with a problem. He made sure I do not feel inferior when I cant solve a problem and he solved it quickly. I am thankful to Prof. K. Paranjape, Prof. K. Srinivas and Dr. Anirban Mukhopadhyay for their guidance at various stages. I will never forget Umesh's contribution. He was one person who was always available throughout. If I want to discuss any mathematics he will listen, and with him I will be free to utter any nonsense, which was the case with few more friends, but he was one of very few who will not take it till I accept that there is a mistake or we correct it together. He did listen to non academic troubles too but will try to get off these as soon as possible, I guess that eventually helps.

I got opportunity to discuss with Prof. Preda Mihăilescu, it was an enjoying conversation and I am thankful to him. I will like to thank Prof. Joseph Oesterle, Prof. Ram Murty, Prof. Kumar Murty, Prof. K. Soundararajan, Prof. Olivier Ramare, Prof. C. Gasabari for some useful comments. I am very thankful to my teacher Prof. T. K. Das who inspired me to pursue a career in Mathematics. Thanks is due to HRI for being amazing host at many occassions and my friends there.

I am thankful to those friends who have accompained me at various wonderful treks. My Flatmates Rajeev and Somdeb, they both are wonderful person and one can always bank on them. My classmates Sundar, Krishna, Pooja, George, Ajay all were very helpful. It was good to have people like Alok, Mohan, Rohan and Bhavin around. Thanks are also due to some friends whom I might not have named.

Last but not the least, I am very thankful to my family members to have

patience for so long. In particular my mother who will be the happiest person to see me being doctorate. This thesis is dedicated to her.

Contents

Introduction

In this thesis the author has worked on three different problems. Some progress is reported on these three problems.

The first problem considered is about "Higher Residue Symbols". Given a finite set S of integers, the question of finding primes p such that each integer $a \in S$ is a quadratic residue (non-residue) modulo p is dealt by various authors [19]. Many authors including M. Fried and S. Wright [49] have established the infinitude of primes p modulo which each $a \in S$ is a quadratic residue. The density of such primes was considered in [1]. We have generalized the problem and studied the analogous questions. We take a prime number l and consider the l^{th} cyclotomic field $\mathbb{Q}(\zeta_l)$. For a prime $\mathbf{p}$ of $\mathbb{Z}[\zeta_l]$ and an integer $\alpha \in \mathbb{Z}[\zeta_l]$ the l^{th} residue symbol

$$\left(\frac{\alpha}{\mathbf{p}}\right)_l$$

have been studied by various mathematicians e.g.[21]. Given a finite set $S = \{s_i; 1 \leq i \leq n\}$ of rational integers and a corresponding set $T = \{t_i; 1 \leq i \leq n\}$ (with multiplicities allowed) of l^{th} roots of unity we determine the density of primes $\mathbf{p}$ of $\mathbb{Z}[\zeta_l]$ for which

$$\left(\frac{s_i}{\mathbf{p}}\right)_l = t_i, \text{ for all } i.$$

We also describe another approach to look at l^{th} residue symbol using more sophisticated tools, and this might be useful in some contexts. This exposition forms chapter one of the thesis.

The second problem considered is the Catalan's conjecture/ Mihăilescu's Theorem. It was conjectured by Eugene Charles Catalan in 1844 that, the only perfect powers among integers which differ by 1 are 8 and 9. Thus the conjecture says that the exponential Diophantine equation $x^m - y^n = 1$, where x, y are positive integers and m, n are integers bigger than 1, has only one solution, viz, $3^2 - 2^3 = 1$. One observes that it is enough to consider the equation $x^p - y^q = 1$, when p, q are primes. The note stating the problem appeared among erratas of papers which appeared in an earlier volume of the Crelle Journal. Some particular cases of the problem were dealt by various mathematicians including Euler and Lebesgue [18, 28]. Notably Lebesgue had solved the problem for the exponent $q = 2$. The progress was slow

till the work of J W S Cassels and Ko Chao [7, 8, 10]. In early 1960s Ko Chao proved the problem for the exponent $p = 2$ and $q \neq 3$ [10]. The case $x^2 - y^3 = 1$, which gives the non-trivial solution $3^2 - 2^3 = 1$, was already settled by Euler using *The method of descent*. This reduced the Catalan's conjecture to a stage when one can assume that both the primes p and q are odd. By a Catalan problem we will refer the diophantine equation $x^p - y^q = 1$ when p and q are odd primes and any solution will be written as a quadruple (x, y, p, q). Now we will let $x, y \in \mathbb{Z}$ and in this case when (x, y, p, q) is a solution then $(-y, -x, q, p)$ is also a solution. A solution will be called non-trivial if $xy \neq 0$. In 1960s Cassels proved that for any solution (x, y, p, q) of the Catalan problem one always has $q|x$ and $p|y$. This is referred as Cassels criteria. The criteria of Cassels proved to be very important, and all subsequent work depended on this. Some immediate progress was made, most notably due to Inkeri and Tijdeman. In 1976, Tijdeman proved that the Catalan problem can have only finitely many possible solutions, actually Cassels had made this weaker conjecture. The conjecture was finally solved by Preda Mihăilescu. Mihăilescu used deep results from Algebraic Number Theory, notably 'theory of annihilators of class groups', together with his 'power series method'. An overview of the proof is presented in chapter two.

As part of this thesis the author studies the equation $x^p - y^q = 1$ over a number field K, i.e. when $x, y \in \mathbb{O}_K$. Mainly the case considered here is when K is a quadratic imaginary field with class number one. It was proved by Brindza et al. [5] that for a fixed field K this equation has only finitely many solutions, but the bounds obtained are very large. In the subsequent chapters we report certain progress made on this problem.

In chapter three we list all the solution of $x^p - y^q = 1$ when one of the prime is even and x and y run through integers in $\mathbb{Q}(i)$. The method is quite different from that of Lebesgue and Ko Chao. The case $x^2 - y^3 = 1$ is handled separately using theory of torsion points on Elliptic curves.

In chapter four of the thesis we formulate an appropriate Cassels criteria and prove it partially for imaginary quadratic number fields with class number one. Because of the symmetry in solution (whenever (x, y, p, q) is a solution then so is $(-y, -x, q, p)$) we can assume $p > q$, without loss of generality. There are two different cases coming naturally. When q does not split in K and when q splits in K. In the first case we are able to prove that there is a prime $\mathfrak{q}_1$, above q, which divides x and there is a prime $\mathfrak{p}_1$, above p, which divides y. We also succeed in showing that under some assumption on class number from this Cassels criterion we already obtain $q|x$ and $p|y$. In the second case we have demonstrated that $\mathfrak{q}_1|x$.

In chapter five we report further progress made on Catalan problem considered here. We introduce a proper obstruction group, made up of solutions

of Catalan problem, and then trap it in a short exact sequence of fairly well studied objects (namely class groups and unit groups). This is pretty analogous to the work in the case of Catalan's conjecture over $\mathbb{Z}$.

Now we come to the chapter six of the thesis. If G is an abelian group and $A \subset G$ is finite then one defines the doubling constant of A to be $D(A) = \frac{|A+A|}{|A|}$. The characterization of A with $D(A) \leq 2$ is well understood, thanks to the work of Kneser [24]. The case when $D(A) \leq 2.04$ was recently handled by Deshouillers and Freiman [16]. These authors first study the problem when $A \subset \mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ with $D(A) \leq 2.40$ and then use it to prove the result ofr $G = \mathbb{Z}/n\mathbb{Z}$. We shall give simpler proof of this last result with $D(A) \leq 2.50$ and then deduce the result for $G = \mathbb{Z}/n\mathbb{Z}$ with $D(A) \leq 2.11$.

List of Publications :

1. (joint with R. Balasubramanian) *Density of Primes in l^{th} Power Residues*, accepted in Proceeding of Indian Academy of Sciences.

2. (joint with R. Balasubramanian) *Catalan's Equation for even primes over quadratic fields* (submitted) http://arxiv.org/abs/1112.2688.

3. (joint with R. Balasubramanian) *Catalan's conjecture Revisited*, In Preparation.

4. (joint with R. Balasubramanian) *A Remark on a Theorem of Deshouillers and Freiman*, In preparation.

Chapter 1

Higher Residue Symbols

1.1 Introduction

In a recent paper [1] the authors have computed the relative 'density' (for definition see section 3 of this chapter) of primes for which a given finite string $S = \{a_1, \ldots, a_m\}$ of integers are quadratic residues simultaneously. It turns out, via Chebotarev density theorem, that this density is reciprocal of the degree of the multiquadratic extension given by square roots of the finite string of given integers over $\mathbb{Q}$. Given a field K which contains an n^{th} root of unity and given a finite set of integers $S = \{a_1, \ldots, a_m\}$ one can determine the degree of the extension $K(a_1^{\frac{1}{n}}, \ldots, a_m^{\frac{1}{n}})/K$ using Galois theory, for instance see [48]. In this chapter, we study the distribution of primes $\mathbf{p}$ of $\mathbb{Z}[\zeta_l]$ modulo which each of a_i assumes a preassigned l^{th} power residue symbol and then relate it to the degree of the extension $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$. We give two methods to compute the degree of the extension $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$ and either of the two methods may prove to be useful at a given instance. In section 2, we use a ramification argument in place of the classical use of the Eisenstein criterion to compute the degree of the extension $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$. Section 3 deals with the l^{th} power residue symbols and study of the distribution of primes $\mathbf{p}$ modulo which they take a fixed value for each a_i. In section 4, we define a matrix T and then proceed to relate the degree of the extension to the rank of T. The tools we use are basic in nature but for the sake of completeness we will give some of the proofs.

We will fix an odd prime l and ζ_l will stand for a fixed primitive l^{th} root of unity in $\mathbb{C}$. The main theorem proved in this chapter is the following;

Theorem 1.1.1. *For integers $r_1, \ldots, r_m$, the density of prime ideals $\mathbf{p}$ of $\mathbb{Z}[\zeta_l]$*

satisfying $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ *for all* i *is* $[\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}) : \mathbb{Q}]^{-1}$*, whenever there is at least one prime ideal satisfying* $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ *for all* i*.*

The proof of this theorem appears at the end of section 3.

1.2 Determination Of The Degree

To start with, we can assume that $a_i^{'s}$ are l^{th} power free and none of them is 1.

One has the following;

Lemma 1.2.1. *If* $a \in \mathbb{Z}$ *is not a* l^{th} *power of an element of* $\mathbb{Z}$*, then* $X^l - a$ *is irreducible over* $\mathbb{Z}$*.*

Lemma 1.2.2. *Let* $b_1, b_2, \ldots, b_i \in \mathbb{Z}$ *and* b *be an integer which is not a* l^{th} *power and such that there is a prime* $q \neq l$ *which divides* b *but does not divide any of* b_j*. Then* $[\mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}}, b^{\frac{1}{l}}) : \mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}})] = l$*.*

Proof. Let us write $L = \mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}}, b^{\frac{1}{l}})$ and $K = \mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}})$.
Since q does not divide b_j for any j, q is unramified in each of $\mathbb{Q}(b_j^{\frac{1}{l}})$ and hence it is unramified in K as well. On the other hand looking at the factorization of $X^l - b$ over $\mathbb{C}$, we find that if $X^l - b = f_1(X)f_2(X)$ in $K[X]$ then $f_1(0) = b^{\frac{r}{l}}\zeta_l^c \in K$ for some integers r and c in $\{0, \ldots, l-1\}$. Then the discriminant of the field $\mathbb{Q}(b^{\frac{r}{l}}\zeta_l^c)$ is divisible by q (Theorem A.1.3) and hence q ramifies in $\mathbb{Q}(b^{\frac{r}{l}}\zeta_l^c)$. Since $\mathbb{Q}(b^{\frac{r}{l}}\zeta_l^c) \subset K$, we obtain that q ramifies in K, a contradiction. So we have that the polynomial $X^l - b$ is irreducible in $K[X]$. This proves the lemma. □

Algorithm to compute the degree $[\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}) : \mathbb{Q}]$
Claim: There exists an integer $t \leq m$ and integers $b_1, \ldots, b_t$ with the following properties;
(1) For every $1 \leq i \leq t$,there exists a prime q_i which divides b_i but does not divide b_j for $j \neq i$,
(2) None of b_i is a l^{th} power,
(3) The field $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})$ is the same as the field $\mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_t^{\frac{1}{l}})$.
We will generate the numbers $b_i's$ in successive steps. Here upper index will indicate the number of steps.
Let q_1 be a prime divisor of a_1 we put $b_1^{(1)} = a_1$. For $i > 1$ if $q_1 \nmid a_i$ then we will put $b_i^{(1)} = a_i$ and in case $q_1 | a_i$ then we will define $b_i^{(1)}$ as follows:
Let r_1 and r_i be the exponent of q_1 in a_1 and a_i respectively. Without loss

of generality we can assume that $1 \leq r_1, r_i \leq l-1$. As m_i runs modulo l the numbers $m_i r_1 + r_i$ are distinct modulo l and hence for some choice of m_i we will have $m_i r_1 + r_i = \lambda_i l$ and then we define $b_i^{(1)} = \frac{a_1^{m_i} a_i}{q_1^{\lambda_i l}}$. Clearly q_1 does not divide $b_i^{(1)}$. If any of $b_i^{(1)}$ happens to be a l^{th} power then we will omit it and consider only those $b_i^{(1)}$ which are not l^{th} powers, say, $b_1^{(1)}, \ldots, b_{s_1}^{(1)}$. Now one has $q_1 | b_1^{(1)}$ and $q_1 \nmid b_i^{(1)}$ for $i > 1$, and $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}) = \mathbb{Q}((b_1^{(1)})^{\frac{1}{l}}, \ldots, (b_{s_1}^{(1)})^{\frac{1}{l}})$. Next we set $b_2^{(2)} = b_2^{(1)}$ and start with a prime divisor q_2 of $b_2^{(2)}$ and repeat the same process to obtain $b_i^{(2)}$ for all $i \neq 2$. Suppose this process stops at k^{th} step then $b_1^{(k)}, \ldots b_{s_u}^{(k)}$ are the required numbers. We will put $t = s_u$ and this proves the claim.
If $l = q_i$ for any i then we call $b_1 = b_i^{(k)}$ and the rest of $t-1$ numbers can be taken in any order and if $p \neq q_i$ for some i then we can take any ordering. Now Lemma 1.2.1 gives that $[\mathbb{Q}(b_1^{\frac{1}{l}}) : \mathbb{Q}] = l$. Then we use Lemma 1.2.2 successively to obtain $[\mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_t^{\frac{1}{l}}) : \mathbb{Q}] = l^t$, which is the required degree.

1.3 l^{th} power residue symbol

Let p be a prime different from l and f be the inertia degree of p in $\mathbb{Z}[\zeta_l]$. For any prime ideal $\mathbf{p}$ of $\mathbb{Q}(\zeta_l)$ dividing p and an integer $\alpha \in \mathbb{Q}(\zeta_l)$ not contained in $\mathbf{p}$ one has $l | p^f - 1$ and $\alpha^{p^f-1} \equiv 1 \pmod{\mathbf{p}}$. Hence there is an l^{th} root of unity $\zeta_l^i, 0 < i \leq l$ such that $\alpha^{\frac{p^f-1}{l}} \equiv \zeta_l^i \pmod{\mathbf{p}}$. Since l^{th} roots of unity are distinct modulo $\mathbf{p}$ there is unique such i.
Definition: We define the l^{th} residue symbol of α with respect to $\mathbf{p}$ by $(\frac{\alpha}{\mathbf{p}})_l = \zeta_l^i$, where i is as defined above.
We state some results about the higher residue symbols [21, 35].

Theorem 1.3.1. *(Kummer's Criterion)* $(\frac{\alpha}{\mathbf{p}})_l \equiv \alpha^{\frac{p^f-1}{l}} \pmod{\mathbf{p}}$.

Theorem 1.3.2. *The l^{th} power residue symbols are completely multiplicative.*

Theorem 1.3.3. *$\alpha \in \mathbb{Q}(\zeta_l)$ is an l^{th} power modulo $\mathbf{p}$ if and only if $(\frac{\alpha}{\mathbf{p}})_l = 1$.*

Given any ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_l)$, we will define $(\frac{\alpha}{\mathfrak{a}})_l = \prod_{\mathbf{p}|\mathfrak{a}} (\frac{\alpha}{\mathbf{p}})_l$ with multiplicity counted. For $\beta \in \mathbb{Q}(\zeta_l)$ we will define $(\frac{\alpha}{\beta})_l = (\frac{\alpha}{<\beta>})_l$ where $<\beta>$ stands for the principal ideal generated by β.
An integer $\alpha \in \mathbb{Q}(\zeta_l)$ is called primary if it is congruent to a rational integer modulo $(1-\zeta_l)^2$.

Theorem 1.3.4. *(Eisenstein's Reciprocity Law) If α is a primary integer and a is a rational integer coprime to α and coprime to l then one has $(\frac{a}{\alpha})_l = (\frac{\alpha}{a})_l$.*

We will now introduce some more terminologies and see an alternate way to define the l^{th} residue symbol.
Let L/K be a Galois extension of number fields. For an unramified prime $\mathbf{p}$ of $prime\mathbb{O}_L$ we will write k_L for the residue field of $\mathbf{p}$ and k will denote the residue field of $\mathbf{p} \cap \mathbb{O}_K$. There is an isomorphism [37],

$$D_{\mathbf{p}} \cong Gal(k_L/k),$$

where $D_{\mathbf{p}}$ is the decomposition group of $\mathbf{p}$. Let $\sigma_{\mathbf{p}} \in Gal(k_L/k)$ be the Frobenius at $\mathbf{p}$ then its inverse image (in the above exact sequence) in $D_{\mathbf{p}}$ is called Artin symbol of $\wp$ for the extension L/K and is written as $\left(\frac{\wp}{L/K}\right)$.
We note that if $\mathbf{p}$ and $\mathbf{p}'$ are primes in $\mathbb{O}_L$ above the same prime of $\mathbb{O}_K$ then $\left(\frac{\mathbf{p}}{L/K}\right)$ and $\left(\frac{\mathbf{p}'}{L/K}\right)$ are conjugate, by an element of $Gal(L/K)$ which maps $\mathbf{p}$ to $\mathbf{p}'$. In particular if L/K is abelian then, for prime $\mathbf{p} = \mathbf{p} \cap \mathbb{O}_K$ in $\mathbb{O}_K$, we can define $\left(\frac{\mathbf{p}}{L/K}\right) = \left(\frac{\mathbf{p}}{L/K}\right)$.

Definition: For any set $\mathcal{S}$ of prime ideals of ring of integers $\mathbb{O}_K$ in a number field K, the density of $\mathcal{S}$ is defined by

$$lim_{x \longrightarrow \infty} \frac{|\{\mathbf{p} \in \mathcal{S} : N_{K/\mathbb{Q}}(\mathbf{p}) \leq x\}|}{|\{\mathbf{p} : N_{K/\mathbb{Q}}(\mathbf{p}) \leq x\}|},$$

if the limit exists. Here for any finite set A by $|A|$ we denote its cardinality and $N_{K/\mathbb{Q}}$ is the norm for the extension $K/\mathbb{Q}$.
For any $\sigma \in Gal(L/K)$ let $P_{L/K}(\sigma)$ denote the set of prime ideals $\mathbf{p}$ in $\mathbb{O}_K$ such that there is a prime ideal $\mathbf{p}$ of $\mathbb{O}_L$ above $\mathbf{p}$ such that $\left(\frac{\mathbf{p}}{L/K}\right) = \sigma$. We recall the theorem of Cebotarev [37]

Theorem 1.3.5. *(Cebotarev Density Theorem) Let $\sigma \in Gal(L/K)$ and C_σ stand for the conjugacy class of σ. Then density of $P_{L/K}(\sigma)$ is $\frac{|C_\sigma|}{[L:K]}$.*

In particular, if L/K is abelian then the density of primes $\mathbf{p}$ of $\mathbb{O}_K$ such that $\left(\frac{\mathbf{p}}{L/K}\right) = \sigma$ is $\frac{1}{[L:K]}$.

The following lemma can be easily verified.

Lemma 1.3.6. *Let L/K be a Galois extension of number fields and let F be an intermediate field such that F/K is Galois. Then for any unramified prime $\mathbf{p}$ of $\mathbb{O}_L$ one has $\left(\frac{\mathbf{p}}{L/K}\right)_{|F} = \left(\frac{\mathbf{p}\cap\mathbb{O}_F}{L/K}\right)$.*

For a fixed prime l, we want to define the l^{th} residue symbol $(\frac{a}{p})_l$ for each prime $p \neq l$ and integer a coprime to p. We will write $f_a(X) = X^l - a$ and let K_a denote splitting field of $f_a(X)$. Then $K_a \supset \mathbb{Q}(\zeta_l)$. For any prime $\mathbf{p}$ of $\mathbb{Z}[\zeta_l]$ above p we let $\sigma_{\mathbf{p},a} \in Gal(K_a/\mathbb{Q}(\zeta_l))$ denote the Artin symbol for the prime $\mathbf{p}$ for the extension $K_a/\mathbb{Q}(\zeta_l)$. Then $\frac{\sigma_{\mathbf{p},a}(a^{1/l})}{a^{1/l}}$ is an l^{th} root of unity. Note that this is independent of the choice of $a^{\frac{1}{l}}$.
Definition: We define the residue symbol $\left(\frac{a}{\mathbf{p}}\right)_l$ by $\frac{\sigma_{\mathbf{p},a}(a^{1/l})}{a^{1/l}}$.

Lemma 1.3.7. *The definition of l^{th} residue symbol given here and the one given earlier are equivalent.*

Proof. Let f be the inertia degree of $\mathbf{p}$ in the extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$. Then the Artin symbol $\sigma_{\mathbf{p},a}$ satisfies

$$\sigma_{\mathbf{p},a}(a^{\frac{1}{l}}) \equiv a^{\frac{p^f}{l}} \quad (\text{ mod } \mathbf{p}).$$

This gives

$$\frac{\sigma_{\mathbf{p},a}(a^{\frac{1}{l}})}{a^{\frac{1}{l}}} \equiv a^{\frac{p^f-1}{l}} \quad (\text{ mod } \mathbf{p}),$$

which proves the lemma.

□

For any positive real number x let $\pi(x)$ denote the number of rational primes not bigger than x. We will consider the following sum

$$\sum_{\mathbf{p};Norm(\mathbf{p})\leq x} (\frac{n}{\mathbf{p}})_l,$$

where sum runs over the prime ideals $\mathbf{p}$ of $\mathbb{Z}[\zeta_l]$.
Let p be a prime number. Since $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ is abelian, all the primes $\mathbf{p}$ above p have same stabilizer in the Galois group $Gal(\mathbb{Q}(\zeta_l)/\mathbb{Q})$. Hence the sum is invariant under the action of the Galois group and is a rational number. The following theorem is well known but we supply a proof for the sake of completeness.

Theorem 1.3.8. *If n is not an l^{th} power of an integer then the estimate*

$$\sum_{\mathbf{p};Norm(\mathbf{p})\leq x}(\frac{n}{\mathbf{p}})_l = o(\pi(x))$$

holds as $x \to \infty$. Here Norm denotes for Norm map of the extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$.

Proof. One has

$$\sum_{\mathbf{p};Norm(\mathbf{p})\leq x}(\frac{n}{\mathbf{p}})_l = \sum_{b=1}^{l}\left(\sum_{Norm(\mathbf{p})\leq x,\sigma_{\mathbf{p},n}=\tau_b}(\frac{n}{\mathbf{p}})_l\right),$$

where τ_b is automorphism of K_n which sends $n^{\frac{1}{l}} \longmapsto (\zeta_l)^b n^{\frac{1}{l}}$. Hence

$$\sum_{\mathbf{p};Norm(\mathbf{p})\leq x}(\frac{n}{\mathbf{p}})_l = \sum_{b=1}^{l}\left(\sum_{Norm(\mathbf{p})\leq x,\sigma_{\mathbf{p},n}=\tau_b}\zeta_l^b\right).$$

Thus we obtain

$$\sum_{\mathbf{p};Norm(\mathbf{p})\leq x}(\frac{n}{\mathbf{p}})_l = \sum_{b=1}^{l}\zeta_l^b(\frac{1}{l}\pi(x)+o(\pi(x))) = \frac{1}{l}\pi(x)\sum_{b=1}^{l}\zeta_l^b + o(\pi(x)).$$

The first term is zero and this proves the result. □

Given an integer m, a set of m integers $a_1, \ldots, a_m$ and m elements $\zeta_l^{r_i}$ in μ_l, not necessarily distinct, we want to determine density of primes $\mathbf{p}$ which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$. For this, we will consider the counting function

$$S_x = \frac{1}{ul^m}\sum_{\mathbf{p};Norm(\mathbf{p})\leq x,\mathbf{p}\notin S'}\prod_{k=1}^{m}\left(\prod_{j=1,j\neq r_k}^{l}(\zeta_l^j - (\frac{a_k}{\mathbf{p}})_l)\right).$$

Here S' is the set of primes dividing $la_1 \ldots a_m$ and u is a unit satisfying

$$ul^m = \prod_{k=1}^{m}\prod_{j=1,j\neq r_k}^{l}(\zeta_l^j - \zeta_l^{r_k}).$$

We note that S_x exactly counts number of primes $\mathbf{p}$ of Norm up to x which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ for all i. Note that the choices of r_i can not be arbitrary because of the multiplicativity of l^{th} power residue symbol. That is to say that the assignment $a_i \longrightarrow \zeta_l^{r_i}$ shall be restriction of some morphism of

semi groups $\mathbb{Z}^*/\mathbb{Z}^{*l} \longrightarrow \mu_l$, but the counting function already takes care of this. To show this we note that any multiplicative relation among $a_i^{'}$s can be brought into the form $\prod_{k=1}^{m} a_i^{c_i} = c^l$ for some integers c_i and c. Now the corresponding relation expected in μ_l is $\prod_{i=1}^{m} \zeta_l^{r_i c_i} = 1$. If this does not hold then it is easy to see from Theorem 1.3.3 that for each prime $\mathbf{p}$ there is an i such that $(\frac{a_i}{\mathbf{p}})_l \neq \zeta_l^{r_i}$. Thus if r_i's satisfy the required condition then S_x exactly counts number of primes of Norm up to x which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ for all i. In case there is inconsistency among choices of r_i, then $S_x = 0$.

Now to estimate S_x, we can actually pass down to the corresponding counting function for $b_j^{'}s$ which also will be denoted by S_x. When we change from the set $S = \{a_1, \ldots, a_m\}$ to the set $T = \{b_1, \ldots, b_t\}$ obtained as in the algorithm in section 2, then, the given m elements $\zeta_l^{r_i}$ uniquely determine a set of t elements $\zeta_l^{s_j}$ such that $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, for all $1 \leq i \leq m$ if and only if $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$. If the conditions $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, for all $1 \leq i \leq m$ lead to a condition of the form $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$ with b_j an l^{th} power and $s_j \neq 0$, then we can immediately conclude that there is no prime $\mathbf{p}$ satisfying the condition. Studying the counting function with the b_j makes it easier, since there will be only one main term with one root of unity in it (not a sum of roots of unity). Hence, it is enough to study the behavior of primes $\mathbf{p}$ which satisfy $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$. Now we consider the counting function

$$S_x = \frac{1}{vl^t} \sum_{\mathbf{p}; Norm(\mathbf{p}) \leq x, \mathbf{p} \notin S'} \prod_{k=1}^{t} \left(\prod_{j=1, j \neq r_k}^{l} (\zeta_l^j - (\frac{b_k}{\mathbf{p}})_l) \right).$$

Here v is a unit satisfying

$$vl^t = \prod_{k=1}^{t} \prod_{j=1, j \neq s_k}^{l} (\zeta_l^j - \zeta_l^{s_k}).$$

We emphasize that S_x exactly counts number of primes of Norm up to x which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ for all i. Because of multiplicativity of l^{th} power residue symbol one obtains

$$S_x = \frac{1}{ul^t} \sum_{\mathbf{p}; Norm(\mathbf{p}) \leq x, \mathbf{p} \notin S'} \sum_{0 \leq d_i \leq l-1, n = \prod b_i^{d_i}} \zeta_l^{t_n} (\frac{n}{\mathbf{p}})_l,$$

for some integer t_n. Now we change the order of summation to obtain

$$S_x = \frac{1}{ul^t} \sum_{0 \leq d_i \leq l-1, n = \prod b_i^{d_i}} \zeta_l^{t_n} \sum_{\mathbf{p}; Norm(\mathbf{p}) \leq x, \mathbf{p} \notin S'} (\frac{n}{\mathbf{p}})_l.$$

By Theorem 1.3.8 if n is not an l^{th} power then the contribution due to inner sum is $o(\pi(x))$. From the construction of b_j its clear that no $n \neq 1$ will be an l^{th} power. Hence, the main term will give, in absolute value, $\frac{1}{l^t}(\pi(x) - |S'|)$. Thus density of the primes $\mathbf{p}$ satisfying $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$ and hence satisfying $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, for all $1 \leq i \leq m$ is $\frac{1}{l^t}$.

Remark 1.3.9. *1. Note that the density does not depend upon the choice of r_i as long as there is the required consistency.*
2. One can also obtain the density of primes $\mathbf{p}$ of $\mathbb{Z}[\zeta_l]$ which satisfy $(\frac{\alpha_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, where α_i are integers of $\mathbb{Q}(\zeta_l)$ and r_i's are as in the Introduction. The above proof may not work in this case, since the ring $\mathbb{Z}[\zeta_l]$ need not be principal domain and hence the algorithm may not work. However we see from the second definition of l^{th} residue symbol in section 3 that if the requirement $\left(\frac{\alpha_i}{\mathbf{p}}\right)_l = \zeta_l^{r_i}$ is consistent (in the same sense as in section 3) then it uniquely determines an element in $Gal(\mathbb{Q}(\zeta_l, \alpha_1^{\frac{1}{l}}, \ldots, \alpha_m^{\frac{1}{l}})/\mathbb{Q}(\zeta_l))$, and hence density of such primes $\mathbf{p}$ is $[\mathbb{Q}(\zeta_l, \alpha_1^{\frac{1}{l}}, \ldots, \alpha_m^{\frac{1}{l}}) : \mathbb{Q}(\zeta_l)]^{-1}$, see [26].

1.4 Another way to find the degree

Let $p_1, p_2, \ldots, p_n$ be all the primes dividing $a_1 \ldots a_m$. Let us write λ_{ij} for exact power of p_j dividing a_i. Then we will consider the $m \times n$ matrix T whose $(i,j)^{th}$ entry is λ_{ij}. Note that for our purpose we can assume that $0 \leq \lambda_{ij} \leq l-1$.

Lemma 1.4.1. *The cardinality of the set $A = \{(\lambda_i)_{i=1}^m : 0 \leq \lambda_i \leq l-1, \prod_i a_i^{\lambda_i} \in \mathbb{Z}^l\}$ is a power of l.*

Proof. Consider the $\mathbb{Z}/l\mathbb{Z}$ vector space $(\mathbb{Z}/l\mathbb{Z})^m$ with basis $S = \{a_1, \ldots, a_m\}$. $\mathbb{Z}/l\mathbb{Z}$ acts on $\mathbb{Q}^*/(\mathbb{Q}^*)^l$ by $\alpha.x = x^\alpha$. Consider the map T:$(\mathbb{Z}/l\mathbb{Z})^m \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^l$ which sends $a_i \to \bar{a_i}$, where $\bar{a_i}$ denotes the class represented by integer a_i in $\mathbb{Q}^*/(\mathbb{Q}^*)^l$ and extend it linearly then $\sum_i \lambda_i a_i \in kerT$ iff $(\lambda_i) \in A$. This proves that $|A|$ is an l^{th} power. □

As mentioned in [48] the degree $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}, \zeta_l)/\mathbb{Q}(\zeta_l)$ is l^m/l^r where l^r is the cardinality of set A. Now we relate this degree to the rank of the matrix T.

Theorem 1.4.2. *The rank of the matrix T is $m-r$.*

Proof. If there are $x_i, 1 \leq i \leq m$ with $0 \leq x_i \leq l-1$ such that $\prod_{i=1}^m a_i^{x_i} \in \mathbb{Z}^l$, then for all j we have $x_1\lambda_{1j} + \ldots + x_m\lambda_{mj} = 0(\text{ mod } l)$, i.e the row vectors

$(\lambda_{i1}, \ldots, \lambda_{in}), 1 \leq i \leq m$ in $(\mathbb{Z}/l\mathbb{Z})^n$ are linearly dependent. Conversely any such linear dependence among row vectors of matrix T will give exactly l many relations of the type in set A. Let r be the rank of the matrix T. After a rearrangement we can assume that the row vectors $(\lambda_{i1}, \ldots, \lambda_{in}), 1 \leq i \leq r$ are linearly independent. Then we see that for any choice of $x_i, 1 \leq i \leq r$ with $1 \leq x_i \leq l-1$ the condition $\prod_{i=1}^{r} a_i^{x_i} \in \mathbb{Z}^l$ does not hold. On the other hand for any selection of $x_j, j > r$ we have l many relation of the form $\prod_{i=1}^{m} a_i^{x_i} \in \mathbb{Z}^l$ (this can be seen by looking at the vectors $(\lambda_{i1}, \ldots, \lambda_{in}), 1 \leq i \leq r$ and $x_{r+1}(\lambda_{r+11}, \ldots, \lambda_{r+1n}) + \ldots + x_m(\lambda_{m1}, \ldots, \lambda_{mn})$ which are linearly dependent). This proves the theorem. $\square$

Chapter 2

Catalan's Conjecture

This chapter gives a sketch of a proof of the Catalan's conjecture over $\mathbb{Z}$, mainly based on the exposition of Rene Schoof [41]. We shall also be referring to the articles by Yuri Bilu [3, 4]. In section one, we state the conjecture and mention some early developments made towards the solution. Section two is devoted to the Cassels' criteria, the first significant progress towards the solution of the Catalan's conjecture. All the later results depend on Cassels criteria. Through section 3-5 we present, very briefly, Mihăilescu's three theorems from which Catalan's conjecture follows. In section 6 we mention the generalization of Catalan's conjecture to the number fields. Most of the proofs will be suppressed due to the technicality.

2.1 Introduction

In 1844, Roman mathematician Eugene Charles Catalan, in a letter to the editor of the Crelle's journal, made the following;
Conjecture: The only pair of consecutive integers both of which are perfect powers is $(8, 9)$.
An integer is a perfect power if it can be written in the form t^s for integers $t \neq 0, \pm 1$ and $s > 1$. In terms of (exponential) Diophantine equation the Catalan's conjecture amounts to the,
Conjecture: The only solution (x, y, m, n) of the Diophantine equation $x^m - y^n = 1$ with $x, y \in \mathbb{Z}, xy \neq 0$ and $m \geq 2, n \geq 2$ are $(\pm 3, 2, 2, 3)$.
A Diophantine equation in which the exponents are also varying is called exponential Diophantine equation. We see that if the equation $x^p - y^q = 1$ with p, q primes and $xy \neq 0$ has only solution $(\pm 3, 2, 2, 3)$ then the equation $x^m - y^n = 1$ for general $m, n \geq 2$ and $xy \neq 0$ has only the above solution. From now on by a Catalan equation over $\mathbb{Z}$ we will mean the equation $x^p -$

$y^q = 1$, where $x, y \in \mathbb{Z}$ and p, q are primes. A solution (x, y, p, q) of the Catalan's equation is called trivial if $xy = 0$. Thus the Catalan's conjecture reads as,
Conjecture: The only non trivial solutions of Catalan's equation over $\mathbb{Z}$ are $(3, 2, 2, 3)$ and $(-3, 2, 2, 3)$.
The particular case "$q = 2$" was solved by V. A. Lebesgue in 1850.

Theorem 2.1.1. *(Lebesgue) The Diophantine equation $x^p - y^2 = 1$ has no non trivial solutions in integers.*

For a proof we refer chapter 2 from [41] or [28]. Chapter 3 of this thesis also contains a proof, in more general setup.
Euler had shown, by the method of descent, that the only non trivial solutions of the equation $x^2 - y^3 = 1$ are $(\pm 3)^2 - 2^3 = 1$. Also the equation $x^2 = y^3 + 1$ represents an elliptic curve of rank 0. Using the method of descent one finds out that the group of rational points on this curve are precisely $(0, -1), (\pm 1, 0), (\pm 3, 2)$ and 'the point at infinity'. For a complete solution we refer to [18] or [41].
In 1965, Ko Chao proved that the Catalan's equation has no non trivial solution when $p = 2, q \geq 5$.

Theorem 2.1.2. *(Ko Chao) The equation $x^2 - y^q = 1$ has no non trivial solution in integers when $q \geq 5$.*

A proof can be found in chapter 3. Also [41, 10] contain a good account of the proof.
With these developments, we see that to solve the Catalan's conjecture it remains to consider the case when both the exponents p and q are odd primes.
Definition: Any non-trivial solution (x, y, p, q) of the Catalan's equation with p and q odd primes will be referred as a Catalan tuple.
Note that if (x, y, p, q) is a Catalan tuple then so is $(-y, -x, q, p)$.
The first major breakthrough for general Catalan's equation was made by J. W. S. Cassels in 1960 [8]. Cassels gave the following criteria for a solution of Catalan's equation.

Theorem 2.1.3. *(Cassels) Whenever (x, y, p, q) is a Catalan tuple then q divides x and p divides y.*

We remark that all the subsequent developments, including the Mihăilescu's proof, use Cassels criteria. In the next section we will sketch a proof of Cassels criteria. For a complete proof we refer the reader to [41] or [7, 8]. Also chapter 4 contains a proof in some cases for $\mathbb{Q}(i)$, and it is easy to deduce

Theorem 2.1.3 from that.
The work of Robert Tijdeman needs a special mention. In 1976, Tijdeman [46] proved, using the theory of linear forms in logarithms, that the Catalan's equation has only finitely many solutions. The bound obtained in Tijdeman's work are large and way beyond the reach of computer calculation.
The conjecture was finally proven by Preda Mihăilescu. Between the years 2000-2003 Preda Mihăilescu proved the following three theorems [32, 33, 34];

Theorem 2.1.4. *(Mihăilescu) For a Catalan tuple (x, y, p, q), we have*

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

Theorem 2.1.5. *(Mihăilescu) Whenever (x, y, p, q) is a Catalan tuple, one has*

$$p \equiv 1 \pmod{q} \text{ or } q \equiv 1 \pmod{p}.$$

Theorem 2.1.6. *(Mihăilescu) If (x, y, p, q) is a Catalan tuple then*

$$p < 4q^2 \text{ and } q < 4p^2.$$

Now we show, how these three theorems give a complete proof of the Catalan's conjecture.

Proof. (Catalan's conjecture) It is sufficient to prove that there is no Catalan tuple. Let (x, y, p, q) be a Catalan tuple. It is easy to establish $p \neq q$. Also due to symmetry of Catalan tuple, we can assume $p > q$. Now by Theorem 2.1.5, we have $p \equiv 1 \pmod{q}$, that is $p = 1+kq$ for some integer k. Now using Theorem 2.1.4 it is easy to see that $q|k$ and thus we have $p = 1 + k'q^2$. Using Theorem 2.1.6 we see that $k' \in \{0, 1, 2, 3\}$. But p is a prime so $k' \neq 0, 1, 3$. On the other hand we see that $2q^2 + 1$ is divisible by 3 and hence $p = 3$, but $p > q$ and both are odd primes. This is not possible. □

We remark that theorem 2.1.4 and Theorem 2.1.5 already imply Catalan's conjecture, when aided with the estimates due to linear form in logarithms [4]. Mihăilescu's Theorem 2.1.6 completely removed the need of estimates and computer calculation. In order to make Theorem 2.1.5 and Theorem 2.1.6 to work, Mihăilescu needed to rule out any solution of Catalan equation when one of the primes p or q is smaller than or equal to 5. In this direction, he proved the following theorem.

Theorem 2.1.7. *There is no Catalan tuple (x, y, p, q) with $p, q \leq 5$.*

The theorem proved by Mihăilescu was much stronger, but this is sufficient to make Theorem 2.1.5 and Theorem 2.1.6 work. The proof of these 4 theorems, of Mihăilescu, uses two main ingredients: Runge method and theory of cyclotomic fields [3, 4, 32, 33, 34, 41].

2.2 Cassels criteria

The proof of Cassels criteria is based on Runge's method [39]. Here we will briefly sketch the proof. A detailed proof of more general theorem appears in chapter 4.
For a Catalan tuple (x, y, p, q), it is easy to notice that $p \neq q$. So we assume $p > q$ throughout this section.
If $q \nmid x$, then $y+1$ and $\frac{y^q+1}{y+1}$ are co-prime and hence p^{th} powers of integers, say

$$y + 1 = b^p \text{ and } \frac{y^q + 1}{y + 1} = v^p.$$

The function $f(X) = X^p - (b^p - 1)^q$ is strictly increasing function of X. We see at once that $f(b^q) > 1$ and $f(b^q - 1) < 1$, and hence there is no integer X satisfying $X^p - (b^p - 1)^q = 1$. This contradiction shows that $q|x$. With this we obtain $gcd(\frac{y^q+1}{y+1}, y + 1) \neq 1$. Let

$$\frac{y^q + 1}{y + 1} = q^r u^p \text{ and } y + 1 = q^s b^p.$$

One checks that $r = 1$ and $s = kp - 1$. Now using the fact $\frac{y^q+1}{y+1} \equiv q \pmod{y+1}$ we obtain $|x| \geq q + q^{p-1}$. We record these as,

Proposition 2.2.1.
(1)q divides x,
(2)we have that $|x|$ is at least as big as $q + q^{p-1}$.

Now we recall the following,

Lemma 2.2.2. *Let $F(t) = ((t + 1)^p - t^p)^{1/q}$ denote the function of real variable t for $|t| < 1$. Put $m = [\frac{p}{q}] + 1$ and let $F_m(t)$ denote the sum of terms of degree at most m of Taylor expansion of $F(t)$ around 0. Then we have*

$$|F(t) - F_m(t)| \leq \frac{|t|^{m+1}}{(1 - |t|)^2},$$

for $|t| < 1$.

In order to establish the Cassels criteria it remains to prove that $p|y$. Assume the contrary. Then we obtain $x - 1 = a^q$ for some integer a. Thus $(a^q + 1)^p - 1$ is a q^{th} power, also a^{pq} is a q^{th} power and hence $|[(a^q + 1)^p - 1]^{1/q} - a^p|$ is a non zero integer. Observe that $y = a^p F(\frac{1}{a^q})$. Put $z = a^{mq-p}y - a^{mq}F_m(\frac{1}{a^q})$, then for $D = q^{m+ord_q(m!)}$ the number Dz is a non zero integer. Using the lower bound on x in Proposition 2.2.1 and from Lemma

2.2.2 we conclude that $|Dz| < 1$, whenever $q \geq 3$. This contradiction proves that $p|y$.
In next proposition we will record some important consequences of Cassels criteria;

Proposition 2.2.3. *For any Catalan tuple (x, y, p, q) we have integers a, b, u, v satisfying*
$\frac{y^q+1}{y+1} = qu^{p-1}$ *and* $y + 1 = q^{p-1}b^p$
$\frac{x^p-1}{x-1} = pv^q$ *and* $x - 1 = p^{q-1}a^q$.
Also $|x| \geq max(p^{q-1} - 1, q^{p-1} + q)$ *and* $|y| \geq max(q^{p-1} - 1, p^{q-1} + p)$.

2.3 Wieferich Criterion

In this section we will introduce the 'obstruction group' and will sketch the proof of the Theorem 2.1.4 and the Theorem 2.1.7. We will need ideas from 'annihilator of class groups'. [47, 27]. Throughout this section, as earlier, (x, y, p, q) will denote a Catalan tuple. Let ζ_p denote a fixed primitive p^{th} root of unity. Let G denote the Galois group of the p^{th} cyclotomic extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. For integers a co-prime to p, we denote, by σ_a, the element of G which sends ζ_p to ζ_p^a, e.g. σ_{-1} is complex conjugation. Consider the elements

$$\theta_i = \sum_{a=1}^{p-1} [\frac{ia}{p}]\sigma_a^{-1} \in \mathbb{Z}[G].$$

Let J denote the ideal in $\mathbb{Z}[G]$ generated by $\theta_i's$. Then, as a consequence of Stickelberger's theorem we have

Theorem 2.3.1. *The ideal J annihilates the class group of $\mathbb{Q}(\zeta_p)$.*

We will put $e_i = (1-\sigma_{-1})(\theta_{i+1}-\theta_i)$ and denote the ideal in $\mathbb{Z}[G]$ generated by $e_i's$ by I. The following lemma is a matter of routine verification,

Lemma 2.3.2. *Let $e_i = \sum_{\sigma \in G} n_\sigma^i \sigma^{-1}$, then $n_\sigma^i \in \{\pm 1\}$.*

Now we define the obstruction group:

$$H = \{\alpha \in \mathbb{Q}(\zeta_p)^* : ord_\tau(< \alpha >) \equiv 0 \pmod{q} \text{ if } \tau \nmid p\}/\mathbb{Q}(\zeta_p) *^q .$$

Here $< \alpha >$ denotes the principal ideal generated by α and $ord_\tau(< \alpha >)$ denotes the highest power of prime ideal τ dividing $< \alpha >$. For $\alpha \in \mathbb{Q}(\zeta_p)^*$, the corresponding element of H will be denoted by $\tilde{\alpha}$. Whenever $\tilde{\alpha} \in H$, we immediately have $< \alpha >= \mathbf{a}^q(1 - \zeta_p)^r$, for some ideal $\mathbf{a}$ and integer r. The following lemma justifies the name obstruction group. The lemma will be proved, in a more general setting, in chapter 5.

Lemma 2.3.3. *For any Catalan tuple (x, y, p, q) the class of $(x - \zeta_p)$ in $\mathbb{Q}(\zeta_p) * /\mathbb{Q}(\zeta_p)*^q$ is in H.*

Let $E_p = \mathbb{Z}[\zeta_p, \frac{1}{p}]$ be the $\mathbb{Z}$ algebra generated by ζ_p and $\frac{1}{p}$. We have following,

Proposition 2.3.4. *There is a natural exact sequence of $\mathbf{F}_q[G]$-modules*

$$0 \mapsto E_p/E_p^q \mapsto H \mapsto Cl_q[p] \mapsto 0,$$

where $Cl_q[p]$ denotes the $q-$part of class group of $\mathbb{Q}(\zeta_p)$ and the map $H \mapsto Cl_q[p]$ is given by $\tilde{\alpha} \mapsto \mathbf{a}$.

For any G module M, we will denote the G module $M/\sigma_{-1}M$ by M^- and similarly M^+ will denote $M\sigma_{-1}M$. Using Proposition 2.3.4 and Theorem 2.3.1 we can deduce the following,

Proposition 2.3.5.
(1) $H^- \cong Cl_q^-[p]$,
(2) The elements e_i are in annihilator of the $\mathbb{Z}[G]$ module H.

With these ingredients in hand, now we are in a position to sketch the proof of the Theorem 2.1.4.

Theorem 2.3.6. *If (x, y, p, q) is a Catalan tuple then q^2 divides x and p^2 divides y.*

Proof. It is enough to prove $q^2|x$ and the other follows from symmetry . Let $\theta \in I$, then by Proposition 2.3.5, we have $(1 - \zeta_p x)^\theta = \beta^q$ for some $\beta \in \mathbb{Q}(\zeta_p)$ (note that $x - \zeta_p$ and $1 - \zeta_p x$ give same element in H). Since $q|x$ we obtain $1 \equiv \beta^q \pmod{q\mathbb{Z}[\zeta_p]}$. From Lemma 4.2.9, to be proved in chapter 4, we immediately obtain $1 \equiv \beta^q \pmod{q^2\mathbb{Z}[\zeta_p]}$. Now substituting $(1 - \zeta_p x)^\theta$ for β^q and expanding it we obtain

$$1 - \sum_{\sigma \in G} n_\sigma \sigma(\zeta_p) x \equiv 1 \pmod{q^2\mathbb{Z}[\zeta_p]},$$

where $\theta = \sum_{\sigma \in G} n_\sigma \sigma$. If $q^2 \nmid x$ then we see that $q|\theta$ but $\theta \in I$ was arbitrary. Taking $\theta = e_i$, we see that $q \nmid \theta$. So we obtain $q^2|x$. □

Proof. (Theorem 2.1.4) From Proposition 2.2.1 we have integer a such that $x - 1 = p^{q-1}a^q$. Using Fermat's little theorem and Cassels criteria we get $-1 \equiv a^q \pmod{q}$. Lemma 4.2.9 can be used to conclude $-1 \equiv a^q \pmod{q^2}$. From this and Theorem 2.3.6 we derive $p^{q-1} \equiv 1 \pmod{q^2}$. □

Proof. (Theorem 2.1.7) Due to symmetry in Catalan tuple we can assume $p \leq 5$. For $p \leq 5$ the group $Cl_q^-[p]$ is trivial [47] and hence from (1) in Proposition 2.3.5 we see that H^- is trivial which implies that $(x-\zeta_p)^{1-\sigma_{-1}} = \alpha^q$ for some $\alpha \in \mathbb{Q}(\zeta_p)$. But this last assertion is not true [41, 17]. This contradiction establishes the theorem. □

2.4 Proof of the Theorem 2.1.6

In this section we want to prove $p < 4q^2$ and $q < 4p^2$. We assume this is not the case. Due to symmetry we can assume that $q \geq 4p^2$. We intend to arrive at a contradiction. In order to do this one needs to study the effects of embeddings of $\mathbb{Q}(\zeta_p)$ into $\mathbb{C}$ on the elements α which satisfy $(x-\zeta_p)^\theta = \alpha^q$ for $\theta \in I$. In this direction we will mention following result, proof of which can be found in [41].

Proposition 2.4.1. *For any embedding $\phi : \mathbb{Q}(\zeta_p) \mapsto \mathbb{C}$, there exists an element $\theta \in I$ with $||\theta|| \leq \frac{3q}{p-1}$ and with the property that $(x-\zeta_p)^\theta = \alpha^q$ for some $1 \neq \alpha \in \mathbb{Q}(\zeta_p)^*$ and*

$$|\phi(\alpha) - 1| \leq \frac{2||\theta||}{q(|x|-1)},$$

where for $\theta = \sum n_\sigma \sigma$ we define $||\theta|| = \sum |n_\sigma|$. Also $\psi(\alpha)$ is contained in the unit circle, for any embedding ψ.

We now prove the Theorem 2.1.6.

Proof. (Theorem 2.1.6) We fix an embedding $\phi : \mathbb{Q}(\zeta_p) \mapsto \mathbb{C}$ and let $\theta \in I$ and $\alpha \in \mathbb{Q}(\zeta_p)^*$ be as in the Proposition 2.4.1, then we have

$$|\phi(\alpha) - 1| \leq \frac{2||\theta||}{q(|x|-1)}.$$

The same inequality is true for the complex conjugate of $\phi(\alpha)$. For any other embedding ψ we have $|\psi(\alpha) - 1| \leq 2$. Thus we obtain

$$N(\alpha - 1) \leq \frac{2^{q-1}}{q^2} \left(\frac{||\theta||}{|x|-1} \right)^2.$$

Let $< \alpha >= \frac{\mathfrak{a}}{\mathfrak{a}'}$ for co-prime ideals $\mathfrak{a}$ and $\mathfrak{a}'$. Note that $< \alpha - 1 >$ also has denominator $\mathfrak{a}'$. We have

$$(x-\zeta_p)^\theta = \prod_{\sigma \in G} (x - \sigma(\zeta_p))^{n_\sigma} = \mathfrak{a}^q / \mathfrak{a}'^q.$$

Since $\theta \in I$ the norm of $(x-\zeta_p)^\theta$ is 1. Hence $N(\mathfrak{a}) = N(\mathfrak{a}')$. Also

$$N(\mathfrak{a}')^{2q} = N(\mathfrak{a}\mathfrak{a}')^q = \prod_{\sigma\in G} N((x-\sigma(\zeta_p))^{|n_\sigma|}).$$

Now the latter one is at most $(|x|+1)^{(p-1)||\theta||}$ and hence $N(\mathfrak{a}') \leq (|x|+1)^{(p-1)||\theta||}$. With this we conclude

$$(|x|+1)^{-\frac{(p-1)}{2q}||\theta||} \leq N(\alpha-1) \leq \frac{2^{p-1}}{q^2}\left(\frac{||\theta||}{|x|-1}\right)^2.$$

Since $|x| > q^{p-1} > 80$ we have $(|x|+1) \leq \frac{4}{3}(|x|-1)$, also $||\theta|| \leq \frac{3q}{p-1}$ so we obtain

$$(|x|+1)^{1/2} \leq \frac{16}{(p-1)^2}2^{p-1}.$$

This gives $q^{(p-1)/2} < 2^{p-1}$, which is impossible as $q \geq 5$. With this contradiction Theorem 2.1.6 is established. □

2.5 Mihăilescu and Cyclotomic Fields in the context of Catalan Conjecture

In this section we aim to sketch the proof of the Theorem 2.1.5. For any $s \in \mathbb{Q}$ we let $(1+T)^s$ denote the power series in $\mathbb{Q}[[T]]$ defined by

$$(1+T)^s = \sum_{k\geq 0}\binom{s}{k}T^k.$$

For an element $\theta = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbb{Z}[G]$ we define

$$F(T) = (1-\zeta_p T)^{\theta/q} = \prod_\sigma (1-\sigma(\zeta_p)T)^{n_\sigma/q} \in \mathbb{Q}(\zeta_p)[[T]].$$

For each embedding $\phi : \mathbb{Q}(\zeta_p) \mapsto \mathbb{C}$ we let $F^\phi(T)$ denote the power series obtained by applying ϕ to the coefficients of $F(T)$. If, for a complex number t the power series $F(T)$ converges at $T = t$, then its limit will be denoted by $F(t)$. Among many results of Mihăilescu concerning this power series the following is of utmost importance;

Proposition 2.5.1. *Suppose that for some θ in the ideal of $\mathbb{Z}[G]$ generated by $(1+\sigma_{-1})$ and for some $t \in \mathbb{Q}$ satisfying $|t| < 1$ we have $(1-\zeta_p t)^\theta = \beta^q$ for some $\beta \in \mathbb{Q}(\zeta_p)^+$, the maximal real sub field of $\mathbb{Q}(\zeta_p)$. Then we have that $F^\phi(t) = \phi(\beta)$, for every embedding $\phi : \mathbb{Q}(\zeta_p)^+ \mapsto \mathbb{R}$.*

The proof is quite technical. Let G^+ denote the Galois group of the extension $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$. Using Proposition 2.5.1 Mihăilescu proves the following;

Theorem 2.5.2. *For any Catalan tuple (x, y, p, q) with $p, q \geq 7$, the $\mathbb{F}_q[G]$ submodule of H generated by $(x - \zeta_p)^{1+\sigma_{-1}}$ is a free module over the group ring $\mathbb{F}_q[G^+]$.*

The proof is based on the Runge's method on the line of the proof of Cassels criteria. Next we have the following;
Definition: An $\alpha \in \mathbb{Q}(\zeta_p)^*$ is called a $q - adic\ q^{th}$ power if it is q^{th} power in the completion of $\mathbb{Q}(\zeta_p)$ with respect to every prime ideal dividing q.
Next we consider the Selmer group

$$S = \{\tilde{\alpha} \in H : \alpha \text{ is a } q - adic\ q^{th} \text{ power } \}.$$

Then, as was the case with the negative component, we see that $(x - \zeta_p)^{1+\sigma_{-1}} \in S^+$.
Using theory of semi simple group rings Mihăilescu obtains an injection of $\mathbb{F}_q[G^+]-$modules:

$$S^+ \hookrightarrow C^{(q)}E^q/E^q \times E/CE^q \times Cl_q^+[p],$$

where E is the subgroup of $p-$units of $\mathbb{Q}(\zeta_p)^*$, C is the subgroup of $p-$cyclotomic units which is the multiplicative $\mathbb{Z}[G]$ module generated by $1 - \zeta_p$. In above $C^{(q)}, E^{(q)}$ stands for the elements in C and E respectively which are $q - adic\ q^{th}$ powers. Now, using the theorem of Thaine [45], Mihăilescu establishes the following;

Theorem 2.5.3. *If $p > q$ are odd primes and $p \neq 1 \pmod q$ then as an $\mathbb{F}_q[G^+]-$modules the annihilators of $C^{(q)}E^q/E^q \times E/CE^q$ also annihilate $Cl_q^+[p]$.*

Next he shows that $C^{(q)}E^q/E^q \times E/CE^q$ has non-trivial annihilators whenever $p > q$. Thus given any Catalan tuple (x, y, p, q), with $p > q$, and if $p \neq 1 \pmod q$ then by the Theorem 2.5.3 we see that as an $\mathbb{F}_q[G^+]-$module the submodule of S^+ generated by $(x-\zeta_p)^{1+\sigma_{-1}}$ has a non trivial annihilator and this contradicts the Theorem 2.5.2. This contradiction establishes $p \equiv 1 \pmod q$ and we are done with the proof of the Theorem 2.1.5.

2.6 Number Field Analog

In this section we mention the analog of the Catalan conjecture over number fields. Some, albeit small, progress is made by the author. These results

are main theme of chapter 3-5. Here we give the summary of those three chapters.

We will use letter K to denote a number field. There are accounts of studies of the Catalan's equation over number fields [5, 38]. Given any number field K one can ask the following

Catalan Problem: Describe all the solution of $x^p - y^q = 1$ with p, q primes and $x, y \in \mathcal{O}_K, xy \neq 0$.

There is no precise conjecture made for the number field analog of the problem. It is known [5] that for any fixed number field K the Catalan problem has only finitely many solutions. But the bounds are too big to solve the problem completely. The problem is extremely difficult and no progress has been made till the date, apart from the finiteness established by Brindza et. al.[5]

We focus on the field $K = \mathbb{Q}(i)$. Here i is the complex number satisfying $i^2 = -1$. It seems that the only solutions of Catalan problem are $(\pm 3, 2, 2, 3), (-2, \pm 3i, 3, 2)$ but we are unable to say something conclusive. Some of the results are true in more general setting (quadratic imaginary number field with class number one) and we will take liberty to state the results for these class of fields, whenever possible. But our main focus will be on the field $\mathbb{Q}(i)$.

Even primes exhibited different behavior in rational case [10, 28] and so is the case for $\mathbb{Z}[i]$. In our attempt to study the Catalan problem for $\mathbb{Z}[i]$ we first need to dispose off the case when one of the primes is even. This is the content of chapter 3. In Chapter 3 we present a solution of the Catalan problem when one of the exponents is even.

In Chapter 4 we give an analog of Cassels criterion. Chapter 5 introduces the obstruction group, and some more results are reported in this investigation.

Chapter 3

Catalan Problem over $\mathbb{Z}[i]$ with even exponents

3.1 Introduction

Consider a tuple (x, y, p, q), with $x, y \in \mathbb{Z}[i]$ satisfying $x^p - y^q = 1$. In this chapter we are interested in the case when one of the primes is even. Recall that we call a solution to be trivial if $xy = 0$. When both $p = q = 2$ then $x-y$ and $x+y$ are units and this gives a trivial solution. Thus we can assume that one of p and q is even and the other is odd. The equation $x^p - y^2 = 1$ translates to $y^2 - x^p$ by the change of coordinates $x \longrightarrow -x$ and $y \longrightarrow iy$. Thus, its enough to study any one of the equations $x^p - y^2 = 1$ and $x^2 - y^q = 1$ in order to solve the Catalan equation with even exponent.
In the first section we assume that the prime $p > 5$. The method is on the line of Liouville's idea of approximations of algebraic numbers by rationals. In section 2 we give solution for the equations $x^2 - y^3 = 1$ and $x^3 - y^2 = 1$, which exhibit some non-trivial solutions. This computation is based on some ideas on elliptic curves. In section 3 we handle the left cases $x^2 - y^5 = 1$ and $x^5 - y^2 = 1$ which were not covered earlier and require delicate analysis than in section 1. For the primes $p > 5$ the approach is to reduce the solvability of the equation $x^p - y^2 = 1$ to solvability of an equation of the form $(x^{'})^p - 4(y^{'})^p = 4$, and then solve the latter one.

3.2 Primes $p > 5$ and $q > 5$

In this section, we prove

Theorem 3.2.1. *The equation $x^p - y^2 = 1$ for $p > 5$ has only trivial solutions $x, y \in \mathbb{Z}[i]$.*

Proof. Suppose that $x^p - y^2 = 1$ has a solution. Then we have;
$x^p = y^2 + 1 = (y + i)(y - i)$.
Note that y can not be real. If y is real, then y is a rational integer and $x^p = y^2 + 1$ is a positive integer. If $y^2 + 1$ is a p^{th} power of a rational integer then we obtain a solution to the Catalan equation $x^p - y^2 = 1$ in rational integers, but such a solution does not exist. If $y^2 + 1$ is not p^{th} power of a rational integer then the polynomial $X^p - (y^2 + 1)$ is irreducible over $\mathbb{Z}$, as mentioned in Lemma 1.2.1, and hence can not have a solution in $\mathbb{Z}[i]$.
We consider following two cases;
Case (1): $y + i$ and $y - i$ are coprime.
This will give $y + i$ and $y - i$ are p^{th} powers up to a unit. Since all the units in $\mathbb{Z}[i]$ are p^{th} powers so $y + i$ and $y - i$ are p^{th} powers themselves.

One has $y + i = x_1^p$ and $y - i = x_2^p$, which leads to;

$$x_1^p - x_2^p = 2i. \tag{3.1}$$

Since y is not real, $|y + i| \neq |y - i|$. So one has $|x_1| \neq |x_2|$. Without loss of generality we can assume that $|x_1| > |x_2| = \sqrt{n}$ for some positive integer n. So one has $|x_1| \geq \sqrt{n + 1}$. Now using equation (3.1) we obtain;

$$\begin{aligned} 2 = |2i| &= |x_1^p - x_2^p| \\ &\geq |x_1^p| - |x_2^p| \\ &\geq (n + 1)^{p/2} - n^{p/2} \\ &\geq 5/2. \end{aligned}$$

This is a contradiction.
case (2): $y + i$ and $y - i$ are not coprime.
Claim: $gcd(y + i, y - i) = 2i$
Any common divisor of $y+i$ and $y-i$ will divide $2i$. If $gcd(y+i, y-i) = 1+i$ then at least one of $y + i$ and $y - i$ is divisible by $(1 + i)^2 = 2i$, as the power of $1 + i$ in $(y + i)(y - i)$ is at least $p > 3$. Also $y + i$ and $y - i$ differ by $2i$ so the other one too is divisible by $2i$. This proves the claim.
Hence one has,

$$y + i = (1 + i)^{r_1} x_1^p, \quad y - i = (1 + i)^{r_2} x_2^p, \quad x = (1 + i)^k x_1 x_2,$$

where r_1, r_2 are positive integers satisfying $r_1 + r_2 \equiv 0 \pmod{p}$, $min\{r_1, r_2\} = 2$ and k is a positive integer.
Let us assume that $min\{r_1, r_2\} = r_2$, so one gets $(1+i)^{r_1} x_1^p - (1+i)^2 x_2^p = 2i$, which in turn, by putting $x_3 = -(1 + i)^k x_1$ with $r_1 + r_2 = kp$, leads to $\frac{1}{4} x_3^p - x_2^p = 1$ for some integers x_3, x_2 in $\mathbb{Z}[i]$. Also $x_3 = 0$ or $x_2 = 0$ will lead to $y = \pm i$, which corresponds to a trivial solution. The case $min\{r_1, r_2\} = r_1$ is similar. Thus the theorem is proved once we show that the equation

$\frac{1}{4}x_3^p - x_2^p = 1$ has no non-trivial solutions in $\mathbb{Z}[i]$. This is done in next proposition. □

Proposition 3.2.2. *Let $p \geq 7$ be a rational prime. The equation $\frac{1}{4}x_3^p - x_2^p = 1$ has no non-trivial solution in $\mathbb{Z}[i]$.*

Lemma 3.2.3. *For any solution (x, y, p, q) of the Catalan's equation with $y + i$ and $y - i$ not coprime one has $|x| > 2^{\frac{1}{2}}(2^{\frac{p-4}{2}} - 1)$.*

Proof. As earlier we will obtain $-2i = (1+i)^2 x_2^p - (1+i)^{kp-2} x_1^p$, which gives $(-x_2)^p \equiv 1 \pmod{(1+i)^{p-4}}$, since $k \geq 1$. As p does not divide $2^{p-4} - 2^{p-5} = \#(\mathbb{Z}[i]/(1+i)^{p-4})^*$ we get $-x_2 \equiv 1 \pmod{(1+i)^{p-4}}$ and hence $|x_2| \geq 2^{(p-4)/2} - 1$. Now $|x| \geq 2^{\frac{1}{2}}|x_2| \geq 2^{1/2}(2^{(p-4)/2} - 1)$, proving the lemma. □

Lemma 3.2.4. *Let x_3, x_2 be as in Proposition 3.2.2, then one has*

$$|x_3 - 4^{1/p}x_2| \leq 4^{1/p}\frac{1}{p}\frac{1}{|x_2|^{p-1}}|(1 + \frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}} + \ldots)|.$$

Proof. Since x_3, x_2 satisfy $x_3^p - 4x_2^p = 4$, we have $\frac{x_3}{x_2} = 4^{1/p}\zeta_p^n(1 + \frac{1}{x_2^p})^{1/p}$, for some integer n, here $\zeta_p = e^{\frac{2\pi i}{p}}$. Using binomial expansion we see that,

$$|x_3 - 4^{1/p}\zeta_p^n x_2| = 4^{1/p}\frac{1}{p}\frac{1}{|x_2|^{p-1}}|(1 + \frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}} + \ldots)|.$$

We note that the following claim will establish the lemma.
Claim: $n = 0 \pmod{p}$.
Clearly $|x_3| \leq |x_2|^2$, this gives us, after multiplying by $\bar{x_3}$,

$$||x_3|^2 - 4^{1/p}\zeta_p^n \bar{x_3} x_2| \leq 4^{1/p}\frac{1}{p}\frac{1}{|x_2|^{p-3}}|(1 + \frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}} + \ldots)|.$$

Let $\bar{x_3}x_2 = a + ib$, then $Im(|x_3|^2 - 4^{1/p}\zeta_p^n \bar{x_3} x_2) = -4^{\frac{1}{p}}\frac{[b(\zeta_p^n + \bar{\zeta_p}^n) + a(\zeta_p^n - \bar{\zeta_p}^n)]}{2}$ and hence one obtains

$$|4^{\frac{1}{p}}[b(\zeta_p^n + \bar{\zeta_p}^n) + a(\zeta_p^n - \bar{\zeta_p}^n)]| \leq 4^{1/p}\frac{2}{p}\frac{1}{|x_2|^{p-3}}|(1 + \frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}} + \ldots)|.$$

Let λ be a solution of $\frac{\lambda^2+1}{\lambda^2-1} + \frac{a}{b} = 0$, then $\lambda^2 = \frac{a-b}{b+a}$ is a real number. We have

$$|\frac{\zeta_p^n + \bar{\zeta_p}^n}{\zeta_p^n - \bar{\zeta_p}^n} - \frac{\lambda^2+1}{\lambda^2-1}| \leq \frac{2}{p}\frac{1}{|x_2|^{p-3}}|\frac{(1 + \frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}} + \ldots)}{\zeta_p^n - \bar{\zeta_p}^n}|,$$

i.e.

$$|\frac{2(\lambda^2-\zeta_p^{2n})}{(\zeta_p^{2n}-1)(\lambda^2-1)}| \leq \frac{2}{p}\frac{1}{|x_2|^{p-3}}|\frac{(1+\frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}}+\ldots)}{\zeta_p^n-\bar{\zeta_p}^n}|.$$

i.e.

$$|\frac{(\lambda^2-\zeta_p^{2n})}{(\lambda^2-1)}| \leq \frac{1}{p}\frac{1}{|x_2|^{p-3}}|(1+\frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}}+\ldots)|.$$

Since $p \geq 7$ and $|x_2| > \sqrt{3}$, the right side quantity in above inequality is at most $\frac{2}{p}\frac{1}{\sqrt{3}^{p-3}}$.
Now if $|\lambda^2-1| \geq 3$, then $|\lambda^2-\zeta_p^{2n}| \geq |\lambda^2-1|-2$. This will force that left hand side is at least $1/3$, which is in contradiction to the upper bound.
In case $|\lambda^2-1| \leq 3$, then we obtain $|\lambda^2-\zeta_p^{2n}| \leq \frac{6}{p}\frac{1}{\sqrt{3}^{p-3}}$. Since λ^2 is real we obtain $|Im(\zeta_p^{2n})| \leq \frac{6}{p}\frac{1}{\sqrt{3}^{p-3}}$. i.e $|sin(\frac{2\pi n}{p})| \leq \frac{6}{p}\frac{1}{\sqrt{3}^{p-3}}$. If $n \neq 0 \pmod p$ then $|sin(\frac{2\pi n}{p})| \geq |sin(\frac{2\pi}{p})|$. But since $p \geq 5$ we have $|sin(\frac{2\pi}{p})| \geq \frac{4}{p}$ (when $x \leq \frac{1}{4}$ then $|sin(2\pi x)| \geq 4x$). This gives $\frac{4}{p} < \frac{6}{p}\frac{1}{\sqrt{3}^{p-3}}$ One checks that the last inequality does not hold, thereby establishing the claim.

□

Now we give the proof of the Proposition 3.2.2.

Proof. (Proposition 3.2.2) One observes that if there is a non-trivial solution, then x_3 is even and x_2 is odd (i.e $1+i|x_3$ and $1+i \nmid x_2$). As $p > 5$, x_2 can not be a unit. One checks that both$|x_3|, |x_2|$ are bigger than $\sqrt{3}$. Let us write $x_3 = a_3 + ib_3$, $x_2 = a_2 + ib_2$.

Since $a_3 - 4^{1/p}a_2 = Re(x_3 - 4^{1/p}x_2)$ so, using Lemma 3.2.4 one obtains

$$|a_3 - 4^{1/p}a_2| \leq 4^{1/p}\frac{1}{p}\frac{1}{x_2^{p-1}}(1+\frac{(1/p-1)}{2!}\frac{1}{x_2^{2p-1}}+\ldots). \tag{3.2}$$

One knows that $\frac{1}{\sqrt{2}}|x_2| \geq min\{|a_2|, |b_2|\}$. We make the following
Claim: $min\{|a_2|, |b_2|\} \neq 0$.
If $a_2 = 0$, then from inequality (3.2) we find that $|a_3| = 0$. This will give $(ib_3)^p - 4(ib_2)^p = 4$, a contradiction as left hand side is not real.
If $b_2 = 0$ then considering the imaginary part we will obtain $b_3 = 0$. Thus, in this case, x_2 and x_3 are real. Define y by $y - i = (1+i)^2x_2^p$, then $y + i = -(1+i)^{-2}x_3^p$ and $y^2 + 1 = (-x_2x_3)^p$. Thus y satisfies $x^p - y^2 = 1$ with $x = -x_2x_3 \in \mathbb{Z}$. Since y is purely imaginary, by putting $x' = -x$ and $y' = y/i$ we obtain an integral solution $y'^2 - x'^p = 1$ of the Catalan's equation, a contradiction. This contradiction establishes the claim.
Let us assume that $min\{|a_2|, |b_2|\} = |a_2|$. Now consider the function $f(x) =$

$x^p - 4$, Then one has ,

$$\frac{1}{|a_2|^p} \leq |f(\frac{a_3}{a_2}) - f(4^{1/p})| = |\frac{a_3}{a_2} - 4^{1/p}||p\xi^{p-1}|,$$

for some point ξ between $\frac{a_3}{a_2}$ and $4^{1/p}$. Now using above estimate we get

$$\frac{1}{|a_2|^p} \leq \frac{1}{|a_2|} 4^{1/p} \frac{1}{p} \frac{1}{|x_2|^{p-1}} |(1 + \frac{(1/p-1)}{2!} \frac{1}{x_2^{2p-1}} + \ldots)||p\xi^{p-1}|.$$

Also we have $|a_2| \leq \frac{1}{\sqrt{2}}|x_2|$ and hence one obtains,

$$\frac{1}{|a_2|^p} \leq \frac{1}{|a_2|} 4^{1/p} \frac{1}{p} \frac{1}{2^{\frac{p-1}{2}}|a_2|^{p-1}} |(1 + \frac{(1/p-1)}{2!} \frac{1}{x_2^{2p-1}} + \ldots)||p\xi^{p-1}|.$$

i.e.

$$2^{\frac{p-1}{2}} \leq 4^{1/p} |(1 + \frac{(1/p-1)}{2!} \frac{1}{x_2^{2p-1}} + \ldots)||\xi^{p-1}|.$$

Now we note that $1 + \frac{(1/p-1)}{2!} \frac{1}{x_2^{2p-1}} + \ldots$ is dominated by the geometric series $1 + \frac{1}{|x_2|^p} + \frac{1}{|x_2|^{2p}} + \ldots$. Now, using the lower bound on x_2 obtained in Lemma 3.2.3 ($|x_2| \geq 2^{3/2} - 1$), we see that $2^{\frac{p-1}{2}} < 4^{1/p}|\xi^{p-1}|(1 + \frac{1}{10})$. If $|\frac{a_3}{a_2}| < 4^{1/p}$ then we obtain $2^{\frac{p-1}{2}} < 4(1 + \frac{1}{10})$ but this is not possible for $p \geq 7$.
Now we handle the case $|\frac{a_3}{a_2}| > 4^{1/p}$. In this case we have $\xi = 4^{1/p} + \epsilon$, where

$$|\epsilon| \leq |\frac{a_3 - 4^{1/p} a_2}{|a_2|}|.$$

So $|\xi|^{p-1} \leq (4^{1/p} + \epsilon)^{p-1} \leq 4^{(p-1)/p} + 1$. To see the last inequality we just notice that $|\binom{p-1}{k} 4^{(p-1-k)/p} \epsilon^k| \leq 1/p$ and using this we obtain that p satisfies $2^{\frac{p-1}{2}} \leq 4 + 4^{1/p}$ and this does not hold for $p \geq 7$. □

3.3 Elliptic curve case

In this section we intend to settle the equations $x^3 - y^2 = 1$ and $x^2 - y^3 = 1$. They both represent elliptic curves defined over $\mathbb{Q}$.
We will consider the equation $x^2 - y^3 = 1$, which after change of co-ordinate takes the form $y^2 = x^3 + 1$. The first one is dealt similarly. We will let E denote the set of $\mathbb{Q}$-rational points on the curve $y^2 = x^3 + 1$ and $E(i)$ will denote the $\mathbb{Q}(i)$-rational point on the same. Both $E(i)$ and E have a group structure under 'elliptic curve addition +'. Given any point $P = (a, b)$ in

$E(i)$, the point $\bar{P} = (\bar{a}, \bar{b})$ is also in $E(i)$. Here $z \longmapsto \bar{z}$ is complex conjugation. The point $P + \bar{P}$ of $E(i)$ is stable under complex conjugation and hence is in E. Thus we have the trace map $T : E(i) \longrightarrow E$ sending $P \longmapsto P + \bar{P}$. To know the points in $E(i)$ it is enough to find $T^{-1}(Q)$ for $Q \in E$. Thus if $P = (a, b)$ with $a, b \in \mathbb{Z}[i]$ satisfies $b^2 = a^3 + 1$, then $T(P)$ is in E and has integer co-ordinates. Hence to find all the solution of $y^2 = x^3 + 1$ with $x, y \in \mathbb{Z}[i]$ we shall find inverse images of the points in E with integer co-ordinates under the trace map T. Using Cremona's table [12] we see that that E is of rank 0 and the torsion group is of order 6. The six torsion points are $R = (2, 3),\ 2R = (0, 1),\ 3R = (-1, 0),\ 4R = (0, -1),\ 5R = (2, -3),\ 6R = (\infty, \infty)$.

First consider $4R = (0, -1) \in E$, assume that there is a point $P = (a, b) \in E(i)$ such that $T(P) = 4R$, i.e. $P, \bar{P}$ and $(0, 1)$ are collinear. A line passing through $P, \bar{P}$ and $(0, 1)$ is given by $y = mx + 1$, with $m = \frac{b-\bar{b}}{a-\bar{a}}$. To get the points P and $\bar{P}$ we solve the equations $y = mx + 1$ and $y^2 = x^3 + 1$. This gives a cubic equation in x, namely, $(mx + 1)^2 = x^3 + 1$. The three solution of this equations are $0, a$ and $\bar{a}$. Thus $a, \bar{a}$ satisfy $x^2 - m^2x - 2m = 0$.

Since we are interested in the case when $a \in \mathbb{Z}[i]$, we have $a + \bar{a} = m^2$ is an even integer. Further we want the point P in $E(i)$ and not in E so the equation $x^2 - m^2x - 2m = 0$ shall have two non real roots which are in $\mathbb{Z}[i]$. Hence the discriminant $m^4 + 8m$ shall be $-ve$ of square of an integer. One observes that this is impossible. Thus there are no points in $E(i)$ with $T(P) = 4R$. Since T is a homomorphism so there are no points on $E(i)$ whose image under T is $R, 2R$ (if $P \longmapsto R$ then $4P \longmapsto 4R$) and hence also there is no point on $E(i)$ whose image is $5R = -R$.
Now consider the case $3R = (-1, 0)$. We consider the line through this point, which is given by $y = m(x+1)$, we substitute this in the equation defining the curve to obtain the points of the intersection. We have $(m(x+1))^2 = x^3 + 1$. Canceling the factor$x + 1$ we obtain $x^2 - (m^2 + 1)x + (1 - m^2) = 0$. Again we obtain $m^2 + 1$ is an even integer and so m is an odd integer. Also the discriminant $(m^2 + 1)^2 - 4(1 - m^2)$ is $-ve$ of square of an integer. This is impossible for any integer m. Hence there are no points P on the curve mapping to $3R$ under T.
Now we consider the last case, of point at infinity, the identity of the group law. Here we are looking for points P on the curve $E(i)$ such that $P = -\bar{P}$. If we write $P = (a + ib, k + il)$ then at once we have $b = 0,\ k = 0$. But then from the equation of the elliptic curve we obtain $(il)^2 = a^3 + 1$, i.e. $(-a, l)$ is a solution to $x^3 - y^2 = 1$ in rational integers, this forces $l = 0$ and hence

$P \in E$. So there are no solution to the equation $x^2 - y^3 = 1$ in $E(i)$ which are not in E.
For the equation $x^3 - y^2 = 1$ we see that the point at infinity corresponds to one solution $(-2, \pm 3i)$ in $E(i)$. There are no more solution.

3.4 Equations $x^5 - y^2 = 1$ and $x^2 - y^5 = 1$

We will work with one of the equations,viz. , $x^5 - y^2 = 1$. The other one is analogous. Again as remarked in section 1 it boils down to proving an analogue of Proposition 3.2.2 for $p = 5$. Here we prove the following;

Theorem 3.4.1. *Equation $x_3^5 - 4x_2^5 = 4$ has no non-trivial solution except $x_3 = -(1+i)$ and $x_2 = i$ and $x_3 = -1+i$ and $x_2 = -i$.*

Proof. We note that if one of x_3 and x_2 is a unit then $x_3 = -(1+i)$ and $x_2 = i$ or $x_3 = -1+i$ and $x_2 = -i$. Now assume that none of them is a unit. So we can assume that both $|x_3|, |x_2|$ are bigger than 2. Let us put $x_3 = a_3 + ib_3, x_2 = a_2 + ib_2$. Using the Lemma 3.2.4 we get $|(x_3 - 4^{1/5}x_2)| < \frac{1}{20}$.
We begin with $x_3^5 - 4x_2^5 = 4$,
i.e.

$$(x_3 - 4^{1/5}x_2)(x_3^4 + 4^{1/5}x_3^3x_2 + \ldots + 4^{4/5}x_2^4) = 4.$$

Let us put $\frac{4^{1/5}x_2}{x_3} = \eta$, then $|1 - \eta| < \frac{1}{40}$. One has

$$|(x_3 - 4^{1/5}x_2)| = \frac{4}{5|x_3|^4}(\frac{1-\eta}{1-\eta^5}).$$

Similarly one also obtains

$$|b_3^5 - 4b_2^5| = |b_3 - 4^{1/5}b_2|5|b_3|^4|(1 + \tau + \ldots + \tau^4)|$$

for $\tau = \frac{4^{1/5}b_2}{b_3}$. Since $|b_3 - 4^{1/5}b_2| \leq |(x_3 - 4^{1/5}x_2)|$, one gets, $|1 - \tau| < \frac{1}{20}$.
Using $|b_3 - 4^{1/5}b_2| \leq |(x_3 - 4^{1/5}x_2)|$, we have

$$|b_3^5 - 4b_2^5| \leq \frac{4}{5|x_3|^4}\left(\frac{1-\eta}{1-\eta^5}\right)5|b_3|^4|(1 + \tau + \ldots + \tau^4)|. \tag{3.3}$$

Note that $(1 + \tau + \ldots + \tau^4) = \frac{1-(1-\epsilon)^5}{\epsilon}$, for $\epsilon = 1 - \tau$. Now using the upper bound on ϵ we obtain $|(1+\tau+\ldots+\tau^4)| < 5 + \frac{10}{(20)} + \frac{10}{(20)^2} + \frac{5}{(20)^3} + \frac{1}{(20)^4} < 5.6$.

Similarly we have $|\left(\frac{1-\eta}{1-\eta^5}\right)| > 4.7$.
Now if $|b_3| < 0.8|x_3|$, then from equation (3.3) we obtain

$$|b_3^5 - 4b_2^5| \leq 4(0.80)^4 \frac{5.6}{4.7} < 2.$$

We show that this is not possible. Since $b_3^5 - 4b_2^5$ is a non zero rational integer so we need to show that $|b_3^5 - 4b_2^5| \neq 1$.
Let us assume that $|b_3^5 - 4b_2^5| = 1$. Since $x_3^5 - 4x_2^5 = 4$, we obtain

$$(a_3 + ib_3)^5 - 4(a_2 + ib_2)^5 = 4.$$

Comparing the imaginary parts and taking $|b_3^5 - 4b_2^5| = 1$ into account we have
$5a = 1$, for some rational integer a, which is not possible. In case $|b_3| \geq 0.8|x_3|$, then $|a_3| < 0.6|x_3|$. Now, as done with the imaginary part, using the real part of $x_3 - 4^{1/5}x_2$ we obtain $|a_3^5 - 4a_2^5| < 1$, which is a contradiction.
□

Remark 3.4.2. *We note that proof of this section also works for the section 1 (in the sense that it works for any exponent $p > 3$) but we have included that proof, as it involves a different method.*

Now using Lemma 3.2.3, Theorem 3.2.1, Theorem 3.4.1 we see that the equation $x^p - y^2 = 1$ and $x^2 - y^q = 1$ have no non-trivial solution in $\mathbb{Z}[i]$ for $p \geq 5$ and $q \geq 5$. This with section 2 shows that the non-trivial solution to the equation $x^p - y^2 = 1$ in $\mathbb{Z}[i]$ are $(-2, \pm 3i)$ and that to the equation $x^2 - y^q = 1$ in $\mathbb{Z}[i]$ are $(\pm 3, 2)$.

Chapter 4

Cassels Criterion for Catalan Problem over $\mathbb{Z}[i]$

4.1 Introduction

In this chapter we continue our study of Catalan problem over the imaginary quadratic number field $\mathbb{Q}(i)$. Most of the results are true for any imaginary quadratic number field K with class number one and we will state them in that generality. We will follow the same notations as in section 2.3. As remarked, in chapter 2, it is enough to consider the equation

$$x^p - y^q = 1, \tag{4.1}$$

when p, q are rational primes. For $K = \mathbb{Q}(i)$, the cases $p = 2$ and $q = 2$ have been dealt with in chapter 3. Thus it remains to find all the Catalan tuples (x, y, p, q) with $x, y \in \mathbb{Z}[i]$. It seems that there are no Catalan tuples with $x, y \in \mathbb{Z}[i]$ and p, q odd primes. In this chapter we make some progress towards this on the line of Cassels [7, 8].

It is worthwhile to remark that it was proved in 1986 by R. Tijdeman, K. Gyory and B. Brindza [5] that for a fixed number field K the equation (4.1) has only finitely many solutions.

In this chapter, we define Cassels' criterion and prove it in a few cases. By the Cassels' criterion for K we mean the following;

Criterion 4.1.1. *For any Catalan tuple (x, y, p, q) for K, we have*

$$gcd(q, x) \neq 1 \text{ and } gcd(p, y) \neq 1.$$

As a consequence we have that $\mathbf{q}$ divides x and $\mathbf{p}$ divides y, for any Catalan tuple (x, y, p, q). Here $\mathbf{q}$ is some prime above q and $\mathbf{p}$ is some prime

above p. When q does not divide x and p does not divide y, we will refer it as weak Cassels criterion. The case q divides x and p divides y will be referred as strong Cassels criterion.

4.2 Some preliminary results

Lemma 4.2.1. *Let K be an imaginary quadratic number field and ϵ be a unit in $\mathbb{O}_K$. Let $p > 3$ be a rational prime and $\mathbf{p}$ be a prime ideal in $\mathbb{O}_K$ above p. If $\epsilon \equiv 1 (mod\ \mathbf{p})$, then $\epsilon = 1$.*

Proof. We note that the only units in K are roots of unity. Since K is quadratic, the only possible roots of unity in K are ± 1, $\pm i$, $\pm\omega, \pm\omega^2$, where ω is a cube root of unity. Now $Norm(\epsilon - 1) = 2 - 2Re\ \epsilon$. From this it follows that $Norm(\epsilon - 1) \leq 4$, hence if $\epsilon - 1 \neq 0$ then only possible primes dividing $Norm(\epsilon - 1)$ are 2 and 3. Hence $\epsilon \equiv 1 (\text{mod } \mathbf{p})$ can not hold for $p > 3$ unless $\epsilon = 1$. □

Lemma 4.2.2. *Let K be an imaginary quadratic number field with class number one. Then the equation $x^p - y^q = 1$ with p and q odd primes and x and y in $\mathbb{O}_K$ has no non trivial solution for $p = q$.*

Proof. On the contrary, let us assume $p = q$, then we have $x^p - y^p = 1$. Since $(x - y)$ divides the left side, we see that $\epsilon = x - y$ is a unit in $\mathbb{O}_K$.
In case $p = 3$, the only exception to Lemma 4.2.1 is $K = \mathbb{Q}(\omega)$ and $\epsilon = \omega$ or $\epsilon = \omega^2$. One easily rules out this possibilty, so we can assume $p \geq 5$.
Case-1. p is not inert in K. In this case the residue field $\mathbb{O}_K/\mathbf{p}$ has order p, where $\mathbf{p}$ is a prime ideal in $\mathbb{O}_K$ lying above p. Hence $(x - y)^p \equiv x - y$ (mod $\mathbf{p}$).

Since for each $1 \leq j \leq p - 1$ the binomial coefficient $\binom{p}{j}$ is divisible by p we have $(x - y)^p \equiv x^p - y^p \pmod{\mathbf{p}}$. Thus we get $\epsilon \equiv 1 \pmod{\mathbf{p}}$. Then by Lemma 4.2.1 we have $x = 1 + y$. Substituting this in the Catalan equation, we get $(1 + y)^p - y^p = 1$. This leads to $(n+1)^{p/2} - n^{p/2} \leq 1$ for some positive integer n, as $||1 + y|^2 - |y|^2| \geq 1$. But this is not possible.
Case- 2. p is inert in K. In this case one has $\sigma(x - y) \equiv 1 \pmod{\mathbf{p}}$ where σ is an element of $Gal(K/\mathbf{Q})$, which reduces to the Frobenius at p This gives $x - y \equiv 1 (\text{mod } \mathbf{p})$, as σ fixes p and is of order 2. From this we get $\epsilon \equiv 1 (\text{mod } \mathbf{p})$. A contradiction is obtained as above.

□

Lemma 4.2.3. *Let K be an imaginary quadratic number field with class number one then 3 does not split in K as product of two distinct primes except for $K = \mathbf{Q}(\sqrt{-11})$.*

Proof. If 3 factors in two distinct primes then $12 = (a^2 - db^2)$ with $d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$ and $a, b \in \mathbb{Z}$. This implies $d = -3$ or $d = -11$. In case $d = -3$, 3 is ramified. In case $d = -11$, 3 splits as product of two distinct primes. □

Lemma 4.2.4. *Let K be a number field and p a rational prime then for any $x \in \mathbb{O}_K$ one has $gcd(< x^p \pm 1/x \pm 1 >, < x \pm 1 >)$ divides p.*

Proof. We will give the proof for the negative sign, and the proof for the positive sign is similar.
If the $gcd(< x^p - 1/x - 1 >, < x - 1 >) = \mathbb{O}_K$ then we are done, otherwise we have $x \equiv 1 \pmod{\wp^r}$ where r is the exact power of $\wp$ in $gcd(< x^p - 1/x - 1 >, < x - 1 >)$. Now we have $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + ... + 1$. Reading this equation modulo $\wp^r$ we get $\wp^r | p$, as needed. □

Remark 4.2.5. *using Chinese remainder theorem one can see that in general $\wp \neq p$ in above lemma.*

Lemma 4.2.6. *Let $a \in \mathbf{R}^+$ and $z \in \mathbf{C}$ with $|z| \lneq 1$ and $m \in \mathbf{N}$. Consider $(1 + z)^a = \sum_{r=0}^{m-1} \binom{a}{r} z^r + E_1(a, m)$. and $(1 - |z|)^{-a} = \sum_{r=0}^{m-1} \binom{-a}{r} (-|z|)^r + E_2(a, m)$. Then one has*
$|E_1(a, m)| \leq |E_2(a, m)|$.

Proof. First note that every term in the expansion of $(1 - |z|)^{-a}$ is positive. r^{th} term in $(1 + z)^a$ is $\binom{a}{r} z^r$ and r^{th} term in the expansion of $(1 - |z|)^{-a}$ is $\binom{-a}{r} (-|z|)^r$ and one has $|\binom{a}{r} z^r| \leq \binom{-a}{r} (-|z|)^r$ hence the result follows.
□

Lemma 4.2.7. *For $x \in \mathbf{R}^+$ and $a \in \mathbf{R}^+$ with $|x| \leq 1$ one has $|E_2(a, m)| \leq \frac{a(a+1)...(a+(m-1))}{m!} |x|^m (1 - |x|)^{-a-m}$.*

Proof. We will use induction on m. For $m = 1$ we want to prove $((1 - x)^{-a} - 1) \leq ax(1 - x)^{-a-1}$
Here the left side is $-\int_{1-x}^{1} \frac{d}{dt}(t^{-a}) dt = a \int_{1-x}^{1} t^{-a-1} dt \leq a(1 - x)^{-a-1} x$. as wanted. Let us write $E(x) \equiv E(a, m)(x) \equiv (1 - x)^{-a} - \sum_{r=0}^{m-1} \binom{-a}{r} (-x)^r$ then one has

$$\begin{aligned}\frac{\partial E(x)}{\partial x} &= a(1-x)^{-a-1} - \sum_{r=1}^{m-1} r\binom{-a}{r}(-1)^r x^{r-1} \\ &= a(1-x)^{-a-1} - \sum_{r=0}^{m-2}(r+1)\binom{-a}{r+1}(-1)^{r+1}x^r \\ &= a(1-x)^{-a-1} - \sum_{r=0}^{m-2} -a\binom{-a-1}{r}(-1)^{r+1}x^r \\ &= aE(a+1,m-1)(x).\end{aligned}$$

Now

$$\begin{aligned}E(a,m)(x) &= \int_0^x \frac{\partial E(a,m)(t)}{\partial t}dt \\ &= a\int_0^x E(a+1,m-1)(t)dt.\end{aligned}$$

By induction hypothesis

$$\begin{aligned}E(a,m)(x) &\leq \frac{a(a+1)...(a+(m-1))}{(m-1)!}\int_0^x t^{m-1}(1-t)^{-a-m}dt \\ &\leq \frac{a(a+1)...(a+(m-1))}{(m-1)!}(1-x)^{-a-m}\int_0^x t^{m-1}dt \\ &= \frac{a(a+1)...(a+(m-1))}{(m-1)!}(1-x)^{-a-m}\frac{x^m}{m} \\ &= \frac{a(a+1)...(a+(m-1))}{m!}(1-x)^{-a-m}x^m\end{aligned}$$

as needed.

□

Remark 4.2.8. *By Lemma 4.2.6 one has* $|E_1(a,m)| \leq \frac{a(a+1)...(a+(m-1))}{m!}|x|^m(1-|x|)^{-a-m}$.

Lemma 4.2.9. *Let R be a commutative ring with unity and q be a rational prime such that R/qR has no nil-potent elements. For $x, y \in R$ satisfying $x^q \equiv y^q \pmod{qR}$ we have $x^q \equiv y^q \pmod{q^2R}$.*

Proof. We are given $x^q \equiv y^q \pmod{qR}$. Since $q|\binom{q}{k}$ for $0 < k < q$, so we obtain $(x-y)^q = 0$ in R/qR. But R/qR has no nil-potent elements, hence $x - y = 0$ in R/qR. Thus $x = y + q\alpha$, for some $\alpha \in R$. Then one easily checks that $x^q \equiv y^q \pmod{q^2R}$. □

Lemma 4.2.10. *(Kronecker) If α is an algebraic integer all whose conjugates have absolute value less than or equal to 1 then α is a root of unity.*

Proof. Let α be of degree n over $\mathbf{Q}$. If $m_\alpha(X)$ is the minimal polynomial of α, then

$$m_\alpha(X) = \prod_{j=1}^{n}(X - \alpha^{(j)}),$$

where $\alpha^{(j)}$ denote the conjugates of α. Since $|\alpha^{(j)}| \leq 1$ for all j, it follows that all the coefficients in $m_\alpha(X)$ are bounded by 2^n. Similarly coefficients of the minimal polynomial of any of α^m are bounded by n. Thus there are finitely many polynomials whose roots are $\alpha^m, m \in \mathbf{N}$. This forces that $\alpha^{m_1} = \alpha^{m_2}$ for $m_1 \neq m_2$, from which the lemma follows. □

Theorem 4.2.11. *Let $b \in \mathbf{C}$ and $|b| \geq \sqrt{2}$ then for primes $p > q \geq 3$ one has $0 < |((b^p-1)^q + 1)^{\frac{1}{p}} - b^q| < 1$.*

Proof.

$$\begin{aligned} |((b^p-1)^q+1)^{\frac{1}{p}} - b^q| &= |b^q(((1-b^{-p})^q + b^{-pq})^{\frac{1}{p}} - 1)| \\ &= |b^q((1-b^{-p})^{\frac{q}{p}}(1+A)^{\frac{1}{p}} - 1)|, \end{aligned} \tag{4.2}$$

where $A = b^{-pq}(1-b^{-p})^{-q}$.
Now we will use Lemma 4.2.6 , Lemma 4.2.7 and Remark 4.2.8 successively with various values of m.
From Remark 4.2.8 one gets

$$|(1-b^{-p})^{\frac{q}{p}} - (1 - \frac{q}{p}b^{-p})| \leq \frac{(\frac{q}{p})(\frac{q}{p}+1)}{2}|b|^{-2p}(1-|b|^{-p})^{-\frac{q}{p}-2}.$$

Hence one has

$$(1-b^{-p})^{\frac{q}{p}} = (1 - \frac{q}{p}b^{-p})| + \lambda_1\frac{(\frac{q}{p})(\frac{q}{p}+1)}{2}|b|^{-2p}(1-|b|^{-p})^{-\frac{q}{p}-2},$$

where $\lambda_1 \in \mathbf{C}$ and $|\lambda_1| < 1$.
Similarly one gets

$$(1+A)^{\frac{1}{p}} = 1 + \lambda_2\frac{1}{p}|A|(1-A)^{\frac{-1}{p}-1},$$

where $\lambda_2 \in \mathbf{C}$ and $|\lambda_2| \lneq 1$.
Now since $q < p$ and $|b| \geq \sqrt{2}$ from above one has

$$(1 - b^{-p})^{\frac{q}{p}} = 1 - \frac{q}{p} b^{-p} + 2\lambda_1^{'} |b|^{-2p},$$

for some $\lambda_1' \in \mathbb{C}$ with $|\lambda_1'| < 1$ (As $\frac{(\frac{q}{p})(\frac{q}{p}+1)}{2} \leq 1$ and $(1 - |b|^{-p})^{\frac{-q}{p}-2} < 2$).
Similarly one obtains

$$(1 + A)^{1/p} = 1 + 2\lambda_2^{'} \frac{|b|^{-(p+1)q}}{p}$$

($|(1 - A)^{\frac{-1}{p}-1}| < 2$ and $\frac{|A|}{|b|^{-(p+1)q}} < 1$)
Feeding this into equation (4.2) one obtains

$$|((b^p - 1)^q + 1)^{\frac{1}{p}} - b^q| = |b^q(\frac{-q}{p} + 2\lambda_1^{'} |b|^{-2p} + 4\lambda_2^{''} |b|^{-(p+1)q})|$$

where $\lambda_2^{''} \in \mathbf{C}$ and $|\lambda_2^{''}| < 1$ Hence one has

$$\begin{aligned}
&|((b^p - 1)^q + 1)^{\frac{1}{p}} - b^q| \\
&\leq |b|^q(|\tfrac{q}{p}|b|^{-p} + 2|b|^{-2p} + 4|b|^{-(p+1)q}) \\
&= |\tfrac{q}{p}|b|^{-p+q} + 2|b|^{-2p+q} + 4|b|^{-pq} \\
&\leq |b|^{-p+q} + 2|b|^{-2p+q} + 4|b|^{-pq} \\
&< 1 \\
&\qquad\qquad\qquad\qquad\qquad\qquad (\text{As } |b| \geq \sqrt{2}, p > q \geq 3)
\end{aligned}$$

Of course the quantity is nonzero hence the theorem. □

4.3 Cassels Criteria

Lemma 4.3.1. *Let K be an imaginary quadratic field with class number one. For any Catalan tuple (x, y, p, q) in K with $p > q$ we have $|y| > 2$.*

Proof. On the contrary, let us assume that $|y| \leq 2$. Since $p > q$, so by equation (4.1) we obtain $|x| \leq 2$. But, for any fixed number field K in consideration, there do not exist two co-prime integers $x, y \in \mathbb{O}_K$ with $1 < |x|, |y| \leq 2$. If $|x| > 1$ then we immediately check that $|y| = 1$ and y is a unit. Thus we obtain either x or y is a unit, say x. Again from equation (4.1) we have $|y|^q \leq 2$. This gives $|y| = 1$, as $q \geq 3$, that is y is a unit. But it is easy to see that there are no Catalan tuple in K with both x and y being unit. The other case is similar. □

Theorem 4.3.2. *Let K be an imaginary quadratic number field with class number one. Then for any solution of Catalan's equation*

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

with primes $p > q \geq 3$ and x, y in $\mathbb{O}_K$ one has
(1) there is a prime ideal $\mathfrak{q}$ in $\mathbb{O}_K$ above q such that $\mathfrak{q}|x$,
(2) either $|x| \leq 4(3q)^{\frac{p}{q}}$ or $\mathfrak{p}|y$ for some prime ideal $\mathfrak{p}$ in $\mathbb{O}_K$ above p.

Proof. From Lemma 4.2.4 it follows that we need to prove

$$gcd(< \frac{y^q+1}{y+1} >, < y+1 >) \neq 1$$

wehre $< t >$ denotes the ideal in $\mathbb{O}_K$ generated by t.
On the contrary assume that

$$gcd(< \frac{y^q+1}{y+1} >, < y+1 >) = 1$$

But one has $(\frac{y^q+1}{y+1})(y+1) = x^p$
Therefore both $y+1$ and $\frac{y^q+1}{y+1}$ are p^{th} powers up to a unit, since K has class number one.
Also $p \geq 5$ so every unit is a p^{th} power and hence one obtains
$y+1 = b^p \qquad \frac{y^q+1}{y+1} = u^p \qquad$ for some $b, u \in \mathbb{O}_K$
Claim: One can assume that $|b| \geq \sqrt{2}$.
Note that $|b| = 1$ will give $|y| \leq 2$, which contradicts Lemma 4.3.1. So now one has
$x^p = (b^p-1)^q + 1$ with $b \in \mathbb{O}_K$ and $|b| \geq \sqrt{2}$. Then, $x = \zeta_p^j((b^p-1)^q+1)^{\frac{1}{p}}$, for some j. Note that $\zeta_p^{-j}x$ also satisfies the Catalan equation, hence one can replace x by $\zeta_p^{-j}x$.
Now, as in Theorem 4.2.11, we get

$$0 < |\zeta_p^{-j}x - b^q| < \frac{4}{p}|b|^{-p}.$$

As done in Lemma 3.2.4, we establish $-j \equiv 0 \pmod{p}$. This gives $|x - b^q| < 1$, which is not possible.
This proves (1) of the theorem.
Thus one has $\mathfrak{q}|x$, let $gcd(< x >, < q >) = \mathfrak{q}$ then one obtains

$$< y+1 >=< b^p > \mathfrak{q}^{p-1} \qquad < \frac{y^q+1}{y+1} >=< u^p > \mathfrak{q} \qquad < x >=< ub > \mathfrak{q} \tag{4.3}$$

Now we will prove (2). In case we have $|x| \leq 4(3q)^{\frac{p}{q}}$ then nothing to prove. So let us assume that $|x| > 4(3q)^{\frac{p}{q}}$.
From Lemma 4.2.4 we either have $\wp | y$ or

$$gcd(< \frac{x^p - 1}{x - 1} >, < x - 1 >) = 1.$$

Assume the latter. Then one obtains

$$x - 1 = a^q \qquad \frac{x^p - 1}{x - 1} = v^q,$$

with $a, v \in \mathbb{O}_K$. Note that $|x| > 4(3q)^{p/q}$ and $|a| \geq 2$. Now consider the power series

$$F(t) = (1 + t)^{\frac{p}{q}} = \sum_{k=0}^{\infty} \binom{\frac{p}{q}}{k} t^k,$$

series converges absolutely for $|t| < 1$
Let m be chosen so that $p = (m - 1)q - \mu$ for some $0 \leq \mu < q$. Since $|\binom{\frac{p}{q}}{k}|$ is a decreasing function of k we obtain

$$\sum_{k \geq m} |\binom{\frac{p}{q}}{k} t^k| \leq |\binom{\frac{p}{q}}{m}| \sum_{k \geq m} |t|^k \leq \frac{1}{m} |t|^m (1 - |t|)^{-1}.$$

Thus

$$F(t) = \sum_{k=0}^{m-1} \binom{\frac{p}{q}}{k} t^k + \frac{\lambda}{m} |t|^m (1 - |t|)^{-1},$$

for some complex number λ of absolute value at most 1. Putting $t = a^{-q}$ and multiplying by $a^{p+\mu}$, we get

$$a^{\mu}(a^q + 1)^{p/q} = a^{p+\mu} \sum_{k=0}^{m-1} \binom{\frac{p}{q}}{k} a^{-qk} + \frac{\lambda}{m} |a|^{-q} (1 - |a|^{-q})^{-1}.$$

Thus

$$a^{\mu} x^{p/q} = a^{p+\mu} \sum_{k=0}^{m-1} \binom{\frac{p}{q}}{k} a^{-qk} + \frac{\lambda}{m} |a|^{-q} (1 - |a|^{-q})^{-1}. \tag{4.4}$$

Now

$$a^{\mu}(x^p - 1)^{1/q} = a^{\mu} x^{p/q} + 2x^{p/q} \frac{\lambda a^{\mu}}{q x^p}.$$

The λ appearing here is some complex number (not necessarily the same as one in above expression) of absolute value smaller than 1. Using equation (4.4) we obtain

$$a^{\mu}(x^p-1)^{1/q} = a^{p+\mu}\sum_{k=0}^{m-1}\binom{\frac{p}{q}}{k}a^{-qk} + \frac{3\lambda}{m}a^{-q}.$$

Multiplying by $D = q^{(m-1)+ord_q((m-1)!)}$ we obtain

$$Da^{\mu}(x^p-1)^{1/q} = Da^{p+\mu}\sum_{k=0}^{m-1}\binom{\frac{p}{q}}{k}a^{-qk} + \frac{3\lambda D}{m}a^{-q},$$

say $S_1 = S_2 + S_3$. Clearly $S_1, S_2 \in \mathbb{O}_K$ hence $S_3 \in \mathbb{O}_K$. But from the bound on $a^q = x-1$ we see that $|S_3| < 1$, hence $S_3 = 0$. But $S_1 - S_2 \neq 0$ as it is not divisible by q. This contradiction proves the theorem.

□

Remark 4.3.3. *We remark that $4(3q)^{\frac{p}{q}} \leq \frac{1}{2}q^{p-1}$ holds except when $q = 3$ and $p = 5$ or 7. In these two exceptions also we see that $|x| \geq \frac{1}{2}q^{p-1}$ is enough to achieve a contradiction in above theorem. Hence we have Cassels' criterion if we establish $|x| \geq \frac{1}{2}q^{p-1}$.*

Now we intend to obtain lower bounds on x, whenever there is a Catalan tuple (x, y, p, q). If one can prove that $|x| > 4(3q)^{\frac{p}{q}}$ then by Theorem 4.3.1 we obtain the Cassels criteria as stated in the introduction. In this regard we have following results.

Proposition 4.3.4. *For a solution of the equation equation $x^5 - y^3 = 1$ in field $K = \mathbf{Q}(\sqrt{-11})$ the Cassels criterion is true.*

Proof. In case $|x| \leq 30$ then from $x^5 - y^3 = 1$ it follows that $|y+1| \leq ((30)^5+1)^{\frac{1}{3}} + 1$ but we also have that $< y+1 >=< b^p > \mathfrak{q}^{p-1}$. Hence $|b|^2 < 4$, giving us $|b|^2 \in \{1, 2, 3\}$ but $|b|^2 = 2$ does not hold for any $b \in O_K$. Also $|b|^2 = 3$ will give that $gcd(b, 3) \neq 1$, which is the Cassels criterion. Hence we are left with $|b|^2 = 1$. Thus b is a unit which has been ruled out in proof of Theorem 4.3.2. This establishes the lower bound on x, for the Theorem 4.3.2 to be applicable. □

Proposition 4.3.5. *Consider a Catalan tuple (x, y, p, q) in an imaginary quadratic number field K with class number one. If q does not split in K then we have $|x| > \frac{1}{2}q^{p-1}$.*

Proof. By expanding one can see that

$$\frac{y^q+1}{y+1} \equiv q \pmod{(y+1)}. \tag{4.5}$$

We consider following cases:
Case (a): q is inert in K.
Here we have $\mathfrak{q} =< q >$. From equation (4.3) and (4.5) one has $u^p q \equiv q \pmod{q^{p-1}}$ Thus one obtains $u^p \equiv 1 \pmod{q^{p-2}}$. Since $p > q$, we see $gcd(p, \phi(q^{p-2})) = 1$. This gives $u \equiv 1 \pmod{q^{p-2}}$ Now we will note that $u = 1$ is not possible. If $u = 1$ then
$\frac{y^q+1}{y+1} = q$ i.e. $|y|^q - q|y| \leq q - 1$
But the left side is an increasing function of $|y|$ for $|y| \geq 1$, but above inequality does not hold if $|y| > 2$. Since $|y| > 2$, by Lemma 4.3.1 so we obtain that $u \neq 1$.
Hence $|u| \geq \frac{1}{2}q^{p-2}$ giving us $|x| \geq \frac{1}{2}q^{p-1}$ from which the bound follows.
Case (b): q ramifies in K. Here one has $q = \pi^2$ and equation (4.3) and (4.5) lead to
$u^p\pi = \pi^2 \pmod{\pi^{p-1}}$ giving us $u^p = \pi \pmod{\pi^{p-2}}$.
So one has $\pi|u$ hence $\pi^p|u^p$ giving us $\pi^2|\pi$ (note that $p > 4$). This contradiction shows that q divides x. So in this case we will have $gcd(< \frac{y^q+1}{y+1} >, < y + 1 >) = q$ and then one can handle the bound on u as in case (a). □

Proposition 4.3.6. *Let (x, y, p, q) be a Catalan tuple for an imaginary quadratic number field K with class number one other than $\mathbb{Q}(\omega), \omega$ being cube root of unity. If $gcd(< y >, < p >) = 1$ then we have; $\mathfrak{q}^2|x$ for some prime ideal $\mathfrak{q}$ in $\mathbb{O}_K$ above q.*

Proof. Since $gcd(< y >, < p >) = 1$, hence by Lemma 4.2.4 we see that both $\frac{x^q-1}{x-1}$ and $x - 1$ are q^{th} powers. Thus there is some $a \in \mathbb{O}_K$ with $x - 1 = a^q$. We obtain $-1 = a^q \pmod{\mathfrak{q}}$. Now an application of Lemma 4.2.9 yields $-1 = a^q \pmod{\mathfrak{q}^2}$. But $a^q = x - 1$, from which the proposition follows. □

In this section we aimed at proving a weaker Cassels criterion (Criterion 4.1.1) for imaginary quadratic number field $\mathbb{Q}(i)$, viz, $\mathfrak{p}_1|y$ and $\mathfrak{q}_1|x$. We succeeded in establishing this only under the assumption on lower bound on x (Theorem 4.3.2). The lower bound was obtained only in few cases, namely, when the primes p and q do not split in $\mathbb{Q}(i)$.
Next, we intend to show that under some hypothesis on the class number of $\mathbb{Q}(\zeta_p)$, the weak Cassels criterion implies the strong Cassels criterion, namely q divides x and p divides y. We shall prove the first assertion (Theorem 4.3.9) and the second one follows similarly.

Here we assume the weak Cassels criterion. As a consequence, for any Catalan tuple (x, y, p, q) in an imaginary quadratic number field K with class number one, we have

$$x - 1 = \mathfrak{p}_1^{q-1} a^q \qquad \frac{x^p - 1}{x - 1} = \mathfrak{p}_1 u^p \tag{4.6}$$

$$y + 1 = \mathfrak{q}_1^{p-1} b^p \qquad \frac{y^q + 1}{y + 1} = \mathfrak{q}_1 v^p \tag{4.7}$$

Where $\mathfrak{p}_1$ is a prime in $\mathbb{O}_K$ above p and $\mathfrak{q}_1$ is a prime in $\mathbb{O}_K$ above q.
We will write $N(\mathfrak{a})$ for the norm of ideal $\mathfrak{a}$ for the relative extension $K(\zeta_p)/\mathbf{Q}(\zeta_p)$. Let ${h_p}^-$ denote the relative class number of extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$. We will write $R = \mathbf{Z}[G], R^- = (1 - \sigma_{-1})R, J^- = (1 - \sigma_{-1})J$. The following result can be found in [23].

Theorem 4.3.7. *We have $[R^- : J^-] = h_p^-$. Further, if l is a rational prime and $l \nmid h_p^-$ then for $\alpha, \beta \in \mathbf{Q}(\zeta), \alpha^\phi \equiv \beta^\phi \pmod{l^r}$ for all $\phi \in J^-$ gives $\alpha^\Theta \equiv \beta^\Theta \pmod{l^r}$ for all $\Theta \in R^-$, where r is any positive integer.*

Lemma 4.3.8. *Suppose $\alpha = a_0 + a_1\zeta_p + ... + a_{p-1}\zeta_p^{p-1}$ with $a_i \in \mathbf{Z}$ and atleast one $a_i = 0$. If $n \in \mathbf{Z}$ divides α then $n | a_j$ for each j.*

Proof. This follows because any subset of $1, \zeta_p, ..., \zeta_p^{p-1}$ with $p - 1$ elements forms a $\mathbf{Z}$ basis for $\mathbf{Z}[\zeta_p]$. □

Theorem 4.3.9. *For a solution (x,y,p,q) of equation (4.1), with $q \nmid h_p^-$ one has $q | x$.*

Proof. We will put $s = 1$, if p splits in K and $s = 2$ otherwise. From equation (4.6) it follows that $\frac{N(x-\zeta)}{(1-\zeta)^s} \in \mathbf{Z}[\zeta]$ and $< \frac{N(x-\zeta)}{(1-\zeta)^s} >= \mathfrak{a}^q$, for some ideal $\mathfrak{a}$ in $\mathbf{z}[\zeta]$.
For $\phi = (1 - j)\theta \in \mathbf{Z}[G]$, where $\theta \in J$, one has $\mathfrak{a}^\phi =< \beta >$.
Thus $N(x - \zeta)^\phi = (1 - \zeta)^{s\phi}\eta^\phi\beta^q$ for some unit η. But then $(1 - \zeta)^\phi$ and η^ϕ being roots of unity are q^{th} powers. Hence we obtain,

$$N(x - \zeta)^\phi = \alpha^q \text{ for some } \alpha \in \mathbf{Z}[\zeta_p]^*.$$

Also $N(x - \zeta) \equiv -\zeta(t - \zeta) \pmod{q}$ where $t = x + \bar{x}$.
Since ζ is a q^{th} power and $t \in \mathbf{Z}$ so $t^q \equiv t$ (mod q) , which results in $-\zeta(t - \zeta) \equiv [-\zeta^{\frac{1}{q}}(t - \zeta^{\frac{1}{q}})]^q$ (mod q).

Thus we have

$$N(x - \zeta)^\phi \equiv [-\zeta(t - \zeta)]^\phi \pmod{q},$$

and both $N(x-\zeta)^{\phi}$ and $[-\zeta(t-\zeta)]^{\phi}$ are q^{th} powers so Lemma 4.2.9 can be applied to obtain

$$N(x-\zeta)^{\phi} \equiv [-\zeta(t-\zeta)]^{\phi} \pmod{q^2}.$$

Now from Theorem 4.3.7 it follows that $N(x-\zeta)^{1-j} \equiv [-\zeta(t-\zeta)]^{1-j} \pmod{q^2}$ which gives $q^2|x\bar{x} - x\bar{x}(\zeta+\bar{\zeta})$. Now using Lemma 4.3.8 it follows that $q^2|x\bar{x}$ from which we get $\mathfrak{q}_1^2|x$ or $q|x$.

As above, we have $-\zeta(t-\zeta)^{\phi} \equiv [-\zeta^{\frac{1}{q}}(t-\zeta^{\frac{1}{q}})]^{q\phi} \pmod{q^2}$
Now using Theorem 4.3.7 we will obtain

$$-\zeta(t-\zeta)^{1-j} \equiv [-\zeta^{\frac{1}{q}}(t-\zeta^{\frac{1}{q}})]^{q(1-j)} \pmod{q^2}.$$

If we write $F(z) = -z(t-z)$ then above expression simply says that

$$F(\zeta)\overline{F(\zeta^{\frac{1}{q}})^q} = \overline{F(\zeta)\overline{F(\zeta^{\frac{1}{q}})^q}} \pmod{q^2}.$$

Thus if we write above expression as $a_0 + a_1\zeta + ... + a_{p-1}\zeta^{p-1} = 0 \pmod{q^2}$, we have $q^2|a_0$, hence by Lemma 4.3.8 we will get $q^2|a_1$. Here
$a_1 = \sum_{s=0}^{m}(-1)^{sp+1}\binom{q}{sp}t^{q-sp} + \sum_{s=0}^{m-1}(-1)^{sp+q_0}\binom{q}{sp+q_0}t^{q-(q_0+sp)} +$
$\sum_{s=1}^{m}(-1)^{sp-q_0}\binom{q}{sp-q_0}t^{q-(sp-q_0)} + \sum_{s=1}^{m}(-1)^{sp+1-2q_0}\binom{q}{sp-2q_0}t^{q-(sp-2q_0)}$,
where $m = [q/p] + 1$ and $-q \equiv q_0 \pmod{q}$. Now all the term in a_1 except first one, which is $-t^q$, are divisible by q. Hence we get, $q|t$. This gives $q|x$ and the theorem is proved.

□

Chapter 5

Catalan Problem over $\mathbb{Z}[i]$

5.1 Introduction

Throughout this chapter we will have $K = \mathbb{Q}(i)$. All abelian groups will be written multiplicatively. We will be assuming that neither p nor q splits in K. In this chapter we intend to define the obstruction group and show that it is part of a short exact sequence, the other objects of which are well known. Let (x, y, p, q) be a Catalan tuple for K. It was observed in chapter 4 that $p \neq q$. Since q is inert in K, so by Proposition 4.3.5 and Theorem 4.3.2 Cassels criteria holds and we have

$$x - 1 = p^{q-1}a^q \qquad \frac{x^p - 1}{x - 1} = pu^q \tag{5.1}$$

$$y + 1 = q^{p-1}b^p \qquad \frac{y^q + 1}{y + 1} = qv^p. \tag{5.2}$$

5.2 The Obstruction Group

We will let $G = Gal(\mathbb{Q}(\zeta_{4p})/\mathbb{Q})$ and σ_{-1} will stand for the complex conjugation. For any positive integer n, μ_n will stand for group of n^{th} roots of unity and ζ_n will denote a primitive n^{th} root of unity. By our assumption the ideal in $\mathbb{Q}(\zeta_{4p})$ above p is principal and is generated by $1 - \zeta_p$.

Using equation (5.1) we have

$$\prod_{\zeta_p \in \mu_p} < (x - \zeta_p) > = < p >< a >^q .$$

Note that $1 - \zeta_p | x - \zeta_p$. Also

$$< \frac{x - \zeta_p}{1 - \zeta_p} > \text{ and } < \frac{x - \zeta_p'}{1 - \zeta_p} >$$

are coprime when $\zeta_p \neq \zeta_p'$. So one obtains;

$$< \frac{x-\zeta_p}{1-\zeta_p} >= \mathfrak{b}^q, \text{ for some integral ideal in } \mathbb{Q}(\zeta_{4p}). \tag{5.3}$$

Now let us define E to be the multiplicative subgroup of $(\mathbb{Q}(\zeta_{4p}))^*$ generated by $(\mathbb{Z}[\zeta_{4p}])^*$ and $1-\zeta_p$ i.e.

$$E =< (\mathbb{Z}[\zeta_{4p}])^*, 1-\zeta_p > .$$

We also consider the subgroup

$$Cl_q[4p] = \{\tilde{\mathbf{b}} : \mathbf{b}^q \text{ is a principal ideal } \}$$

of class group, where $\tilde{\mathbf{b}}$ is the ideal class of $\mathbf{b}$ in the ideal class group of $\mathbb{Q}(\zeta_{4p})$.
The obstruction group is

$$H = \{\alpha \in \mathbb{Q}(\zeta_{4p})^* : ord_\tau(< \alpha >) \equiv o \pmod{q} \text{ if } \tau \neq \wp\}/(\mathbb{Q}(\zeta_{4p})^*)^q,$$

where for prime ideal τ of $\mathbb{Z}[\zeta_{4p}]$ by $ord_\tau(< \alpha >)$ we mean the maximum power of τ dividing $< \alpha >$.
Note that all three groups have $\mathbb{Z}[G]$ module structure. Before mentioning any interconnection among them we shall recall following theorem from appendix of [25];

Theorem 5.2.1. *If Γ is a principal ideal domain and M is a free module of finite rank then for any submodule N of M there is a basis $v_1, \ldots, v_m$ of M and elements $d_1, \ldots, d_n$ of Γ such that $d_1v_1, \ldots, d_nv_n$ is a basis of N and $d_i | d_{i+1}$.*

Now we have following;

Proposition 5.2.2. *We have an exact sequence*

$$0 \longrightarrow E/E^q \longrightarrow H \longrightarrow CL_q[4p] \longrightarrow 0,$$

where the first map is induced from the inclusion of $E \subset \mathbb{Q}(\zeta_{4p})^*$ and the second map is defined as follows;
For any $\tilde{\alpha} \in H$ we have $< \alpha >= \mathbf{b}^q(1-\zeta_p)^r$ for some integer r and ideal $\mathbf{b}$ coprime to $1-\zeta_p$, then we send $\tilde{\alpha} \mapsto \tilde{\mathbf{b}}$.

Proof. (a) injectivity of the first map;
Consider $\epsilon(1-\zeta)^r \in \mathbb{Q}(\zeta_{4p})^{*q}$, for some $\epsilon \in \mathbb{Z}[\zeta_{4p}]^*$. We want to show that $\epsilon(1-\zeta)^r \in E^q$.

First let us assume that $r = 0$. In this case, we have $\epsilon = \xi^q$, for some $\xi \in \mathbb{Q}(\zeta_{4p})^*$. But since $\epsilon \in \mathbb{Z}[\zeta_{4p}]^*$, we get $\xi \in \mathbb{Z}[\zeta_{4p}]^*$.
Now we consider the general case. Again $\epsilon(1-\zeta_p)^r = \xi^q$, for some $\xi \in \mathbb{Q}(\zeta_{4p})^*$. First taking norm for the extension $K(\zeta_p)/\mathbb{Q}(\zeta_p)$ and then comparing the $1-\zeta_p$-adic valuation gives us $q|r$. Thus, eventually, we are left to prove that $\epsilon \in \mathbb{Z}[\zeta_{4p}]^{*q}$ and this is already done.
(b) surjectivity of the last map;
For any $\tilde{\mathbf{b}} \in CL_{4p}[q]$ we have $\mathbf{b}^q =< \alpha >$ for some $\alpha \in \mathbb{Q}(\zeta_{4p})^*$. Clearly $\tilde{\alpha} \in H$. We now write $< \alpha >= \mathbf{b}_1^q(1-\zeta_p)^{qr}$ for some integer r and ideal $\mathbf{b}_1$ coprime to $1-\zeta_p$. Since $\mathbf{b} = \mathbf{b}_1 < 1-\zeta_p >$, we get $\tilde{\mathbf{b}} = \tilde{\mathbf{b}_1}$ and $\tilde{\alpha} \mapsto \tilde{\mathbf{b}_1}$. This proves the surjectivity of the last map.
(c) Exactness at the centre;
One is quick to see that $Im \subset ker$. On the other hand if $\tilde{\alpha} \mapsto 1$ then we have $\alpha = \mathbf{b}^q(1-\zeta_p)^r$ where $\mathfrak{b}$ is a principal ideal. Let $\mathfrak{b} =< \beta >$ for some $\beta \in \mathbb{Q}(\zeta_{4p})^*$. Then $\alpha = \eta\beta^q(1-\zeta_p)^r$, for some unit η. But then $\tilde{\alpha} = \eta\widetilde{(1-\zeta_p)^r}$ and the right side is in the image. This proves that $ker = Im$. □

Lemma 5.2.3. *Let $\sigma_{-1} \in G$ denote the element which maps $\zeta_{4p} \mapsto \zeta_{4p}^{-1}$. Then E/E^q is σ_{-1} invariant.*

Proof. We want to prove that for any element $\varepsilon(1-\zeta_p)^r \in E$ the element $(\varepsilon(1-\zeta)^r)^{1-\sigma_{-1}} \in E^q$. Since $\varepsilon \in \mathbb{Z}[\zeta_{4p}]^*$ so $(\varepsilon)^{1-\sigma_{-1}}$ and all its conjugate have absolute value 1 and hence by the Lemma 4.2.10 it is a root of unity in $\mathbb{Z}[\zeta_{4p}]$. Note that all the roots of unity in $\mathbb{Q}(\zeta_{4p})$ are q^{th} powers. Also we see that $(1-\zeta)^{1-\sigma_{-1}} = -\zeta_p$ is a q^{th} power. This proves the lemma. □

For any abelian group M on which $\mathbb{Z}[G]$ acts we will write $M^+ = M^{1+\sigma_{-1}}$ and $M^- = M^{1-\sigma_{-1}}$, where $M^\theta = \{\theta(m) : m \in M\}$ for any $\theta \in \mathbb{Z}[G]$.

Lemma 5.2.4. *For an abelian group M of odd order, one has $M = M^+M^-$, where the product on right is product of subgroups.*

Proof. For any $m \in M$, we have $m\sigma_{-1}(m) \in M^+$ and $m/\sigma_{-1}(m) \in M^-$ so $m^2 \in M^+M^-$ hence $M^2 \subset M^+M^-$. Since M is of odd order, the map $m \mapsto m^2$ is an automorphism of M. One has $M \subset M^+M^-$. The other way inclusion is obvious as M is G set. □

Lemma 5.2.5. *For an exact sequence*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of abelian groups of odd order on which $\mathbb{Z}[G]$ acts, and the maps involved in the sequence commutes with the action of $\mathbb{Z}[G]$, the sequence

$$0 \longrightarrow (M')^- \longrightarrow M^- \longrightarrow (M'')^- \longrightarrow 0$$

is exact.

Proof. Since the maps involved in the exact sequence commute with the action of $\mathbb{Z}[G]$ so only thing to prove is that ker of the map $M^- \longrightarrow (M^{''})^-$ is contained in the image of the map $(M^{'})^- \longrightarrow M^-$. For this we note that if $(1-\sigma_{-1})(m) \in ker$ then there is $m^{'} \in M^{'}$ whose image is $(1-\sigma_{-1})(m)$. So $(1-\sigma_{-1})(m^{'}) \mapsto (1-\sigma_{-1})^2(m)$, but $(1-\sigma_{-1})^2(m) = (1-\sigma_{-1})(m^2)$ (as $(1-\sigma_{-1})^2 = 2(1-\sigma_{-1})$). Now we use the trick used in Lemma 5.2.4, to conclude the proof. □

Proposition 5.2.6. *We have* $H^- \cong CL_q[4p]^-$.

Proof. To prove this first we note that all the three abelian groups in the exact sequence;

$$0 \longrightarrow E/E^q \longrightarrow H \longrightarrow CL_q[4p] \longrightarrow 0$$

are of odd order (the roots of unity in $\mathbb{Z}[\zeta_{4p}]^*$ are q^{th} powers and $(1-\zeta)^r$ is not a q^{th} power for any integer $0 < r < q$. Hence using Dirichlet Unit theorem one gets $|E/E^q| = q^{p+1/2}$. Also $Cl_q[4p]$ is an abelian group with exponent q and hence its order is a power of q. Now we apply $1-\sigma_{-1}$ to above sequence to obtain following exact sequence;

$$0 \longrightarrow (E/E^q)^- \longrightarrow H^- \longrightarrow CL_q[4p]^- \longrightarrow 0.$$

Now Lemma 5.2.3 at once proves the proposition. □

From equation (5.3) it is clear that $(x-\zeta_p) \in H$ hence $(x-\zeta_p)^{1-\sigma_{-1}} \in H^-$. Thus for every Catalan tuple (x, y, p, q) of K we have an element in $CL_q[4p]^-$. We are unable to prove the non triviality of $(x-\zeta_p)^{1-\sigma_{-1}}$. If one can establish the non triviality of $(x-\zeta_p)^{1-\sigma_{-1}}$, then the Inkeri type results [22] follow immediately.

Chapter 6

Inverse problems in Additive Number Theory

6.1 Introduction

For finite set X, by $|X|$ we will denote the number of elements in X. For two subsets A and B of $\mathbb{Z}$ one immediately sees that $|A+B| \geq |A|+|B|-1$, where $A+B = \{a+b : a \in A, b \in B\}$. In what follows, G is an abelian group, written additively. Let X be a subset of an abelian group G, the 'stabilizer' of X is defined to be the subgroup $\{g \in G : g+x \in X, \forall x \in X\}$. Cauchy-Davenport theorem is the following assertion [36];
For subsets A and B of $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number, one has $|A+B| \geq min\{p, |A|+|B|-1\}$.

Chowla proved a 'similar' theorem for any cyclic group [11]. Kneser took a big leap in this direction and proved following beautiful theorem [24].

Theorem 6.1.1. *For finite subsets A and B of an abelian group G with $|A+B| < |A|+|B|$, one has $|A+B| = |A+H|+|B+H|-|H|$, where H is the stabilizer of $A+B$.*

Thus for any finite set A in an abelian group G one 'almost' always has $|A+A| \geq 2|A|-1$.
In the 'Inverse problems in additive number theory' one studies the converse question, i.e. if $|A+A|$ is not too big in comparison with $|A|$ then can we 'describe' A? To be more precise, we define doubling constant of A to be constant c satisfying $|A+A| = c|A|$ [44]. Then one wants to 'describe' the set A when c is 'small'. We mention few well known results along this line. The following two results are for the additive group of integers.

Theorem 6.1.2. *If A is a finite subset of $\mathbb{Z}$ with $|A+A| \leq 2|A|-1$ then A is an arithmetic progression.*

Theorem 6.1.3 (Freiman)**.** *Let A be a subset of integers such that $|A| = k > 2$. If $|A+A| = 2k-1+b \leq 3k-4$, then A is a subset of an arithmetic progression of length $k+b \leq 2k-3$.*

The theorem of Kneser is also a result in this direction for $\mathbb{Z}/n\mathbb{Z}$ with $c < 2$ [36]. Freiman [13] improved the result by allowing $c < 2.4$, when G is of prime order. Deshouillers and Freiman [16] extended Freiman's result for any finite cyclic group, albeit with a smaller c. Their proof 'essentially' proceeds along the following line;
They prove a similar result with some doubling constant c' when A is a subset of $\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ and then they use idea of rectification (what they call 'a partial lift') to obtain the result for $\mathbb{Z}/n\mathbb{Z}$ with the doubling constant c. The proof is quite involved.
Here we give an alternate proof of their result and on our way we make a slight improvement. We stress that the overall structure of our proof is quite similar to that of Deshouillers and Freiman. In the next section we state our theorems and will mention some well known results needed for our proof. Also we will describe the line of proof quite elaborately, making the difference of the two proofs more explicit. In section 3 and section 4 we will present the proof.

6.2 Statements of Theorems

The main result proved in this chapter is the following:

Theorem 6.2.1. *Let n be a positive integer and $\mathcal{A}$ a non-empty subset of $\mathbb{Z}/n\mathbb{Z}$ with $|\mathcal{A}| < c'n$ (with c' a 'small' absolute constant) which satisfies:*

$$|\mathcal{A}+\mathcal{A}| \leq c|\mathcal{A}|.$$

When $c = 2.11$, there is a proper subgroup $\mathcal{H}$ of $\mathbb{Z}/n\mathbb{Z}$ such that one of the following three cases hold;
(1) if the number of the cosets met by $\mathcal{A}$, let us call it s, is different from 1 and 3, then $\mathcal{A}$ is included in an arithmetic progression of l cosets modulo $\mathcal{H}$ such that

$$(l-1)|\mathcal{H}| < |\mathcal{A}+\mathcal{A}| - |\mathcal{A}|;$$

(2) if $\mathcal{A}$ exactly meets 3 cosets, i.e. $s = 3$, then above holds with l being

replaced by $min(l, 4)$*;*
(3) if $\mathcal{A}$ *is included in a single coset then we have*

$$|\mathcal{A}| > c'|\mathcal{H}|.$$

Furthermore, when $l \geq 2$ *then there is a coset of* $\mathcal{H}$ *which contains more than* $\frac{2}{3}|\mathcal{H}|$ *elements from* $\mathcal{A}$*.*

Deshouillers and Freiman [16] proved this theorem for $c = 2.04$. Like Deshouillers and Freiman we will deduce this theorem from following result, which is an analog of above result for $\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$;

Theorem 6.2.2. *For positive integers* $s \geq 6$ *and* d*, consider integers* $a_1 = 0, a_2, \ldots, a_s$ *with gcd of nonzero elements being* 1*, and let* $\mathcal{B}_1, \ldots, \mathcal{B}_s$ *be subsets of* $\mathbb{Z}/d\mathbb{Z}$ *with* $0 \in \mathcal{B}_1$*. We let* $\tilde{\mathcal{B}}_i = a_i \times \mathcal{B}_i$ *and* $\tilde{\mathcal{B}} = \cup_{i=1}^{s} \tilde{\mathcal{B}}_i$*. Under the condition*

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| < 2.5|\tilde{\mathcal{B}}|$$

we have $max\ a_i < (1.5)s$ *and there exists a subgroup* $\tilde{\mathcal{H}}$ *of* $\mathbb{Z}/d\mathbb{Z}$ *and element* $x \in \mathbb{Z}/d\mathbb{Z}$ *such that* $\mathcal{B}_i$ *is included in the coset* $a_i x + \tilde{\mathcal{H}}$ *for each* i *and for some* j *we have* $|\mathcal{B}_j| \geq \frac{2}{3}|\tilde{\mathcal{H}}|$*.*
Moreover, we also have

$$(max\ a_i)|\tilde{\mathcal{H}}| < |\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| - |\tilde{\mathcal{B}}|.$$

In Deshouillers and Freiman [16], a corresponding theorem is proved for $s \geq 5$. The cases $s \leq 4$ are dealt separately. Our proof also works for smaller values of s as well but under the condition $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| < c_1|\tilde{\mathcal{B}}|$, where c_1 is a constant smaller than 2.5 and depends on s. In particular, Theorem 6.2.2 is true with $c_1 = 2.4$ for $s = 5$ and $c_1 = 2.25$ for $s = 4$. We do not elaborate any more on the cases $s \leq 5$ and refer the reader to [16]. In [16] existence of subgroup $\tilde{\mathcal{H}}$ is established under the hypothesis $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| < \frac{5s-2}{2s+1}|\tilde{\mathcal{B}}|$. For the assertion $(max\ a_i)|\tilde{\mathcal{H}}| < |\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| - |\tilde{\mathcal{B}}|$, it is assumed that $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| < 2.04|\tilde{\mathcal{B}}|$.

Remark 6.2.3. *In their proof, Deshouillers and Freiman use the ordering* $a_1 < \ldots < a_s$ *critically, which one can always assume, to obtain a lower bound on* $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}|$*. But we do not restrict our self to this particular ordering and use Hall's marriage problem to get a better lower bound on* $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}|$*.*

6.3 Preliminaries

In this section we mention some known results which will be needed for the proof and develop some preliminary results. Hall's marriage problem states the following;

Theorem 6.3.1. *Given subsets $G_1, \ldots, G_t$ contained in some set G, if for every subset I of $\{1, \ldots, t\}$ we have $|\cup_{i\in I} G_i| \geq |I|$ then there are elements $x_i \in G_i$ such that $x_i \neq x_j$, whenever $i \neq j$.*

In order to verify that the conditions of Hall's marriage problem are satisfied in our case, we need the following proposition which can be found in [43]

Proposition 6.3.2. *Let $\mathcal{U}$ and $\mathcal{V}$ be to non empty set of integers such that*

$$\mathcal{V} = \{v_1 < \ldots < v_t\} \subset \mathcal{U} = \{0 = u_1 < \ldots < u_s\}$$

and $gcd(u_2, \ldots, u_s) = 1$. Then we have $|\mathcal{U} + \mathcal{V}| \geq min(u_s + t, s + 2t - 3)$; moreover, if $\mathcal{U} \neq \mathcal{V}$ and $u_s = s + t - 2$, then $|\mathcal{U} + \mathcal{V}| \geq u_s + t$.

We will also need following result, which is a consequence of Kneser's Theorem;

Proposition 6.3.3. *For two subsets A and B of a finite abelian group G with $|A| \geq |B|$ and $|A + B| < \frac{3}{2}|A|, |B| > \frac{3}{4}|A|$ there is a subgroup H of G with $|H| < \frac{3}{2}|A|$ such that $A + B$ lies in a single coset of H.*

Proof. We have subgroup H of G, from Kneser's theorem, satisfying;

$$|A + B| = |A + H| + |B + H| - |H|. \tag{6.1}$$

One has $|A + H| \geq |A| > \frac{2}{3}|A + B|$ and $|B + H| \geq |B| > \frac{3}{4}|A| > \frac{1}{2}|A + B|$. Hence by equation (2) $|H| > \frac{1}{6}|A + B|$.
Now H is stabilizer of $A + B$ and so $A + B$ is union of cosets of H, say μ cosets. Then one has $\mu < 6$.
Let us assume that A intersects a many cosets of H, then $a|H| \geq |A| > \frac{2}{3}|A + B| \geq \frac{2\mu}{3}|H|$. This gives $a > \frac{2\mu}{3}$. Similarly if b is the number of cosets of H which meets B, then one has $b > \frac{\mu}{2}$. Since $|A + H| = a|H|$ and so on, we also have $\mu|H| \geq a|H| + b|H| - |H|$. This yields a contradiction unless $\mu = 1$, which proves the proposition. □

The following proposition is also a consequence of Kneser's Theorem and the proof run along the same line as of proposition 6.3.3.

Proposition 6.3.4. *Consider two finite subsets A and B of an abelian group G such that, $|A + B| < 2|B|$ and $|B| < 3/4|A|$. Then $A + B$ lies in a single coset modulo some subgroup H with $|H| < 2|B|$.*

Theorem 6.2.1 is deduced from Theorem 6.2.2 and this is achieved using a 'partial lift'. Deshouiller and Freiman are able to 'rectify' more than 85 percentage of elements of $\mathcal{A}$ and then use Theorem 6.2.2 for this part. To complete the proof they use an argument to conclude that whatever is achieved is already enough. In our case we show that once more than 85 percentage of elements of $\mathcal{A}$ are rectified and Theorem 6.2.2 can be appealed then using the structure provided from Theorem 6.2.2 for this part we can conclude that one can rectify all the elements of $\mathcal{A}$.
We will also need the concept of Freiman isomorphism, in order to link Theorem 6.2.1 to Theorem 6.2.2. See [36],
Definition: Let G_1 and G_2 be abelian groups written additively. For $S \subset G_1, T \subset G_2$ a map $f : S \mapsto T$ is called $2-isomorphism$ if f is a bijection and $s_1+s_2 = s_3+s_4$ holds in S if and only if and $f(s_1)+f(s_2) = f(s_3)+f(s_4)$ holds in T.
The following lemma will be of help in the sequel.

Lemma 6.3.5. *Let G be a subset of $[0, s-1]$ with $|G| \geq 2s/3+1$, then for any $d \leq s/3$ there are elements $g_1, g_2 \in G$ such that $d = g_1 - g_2$.*

Proof. Suppose there are no solution of $d = g_1 - g_2$. Then observe that, for $a \in G$, $a + d$ is not in G. Thus every interval of length less than or equal to $2d$ can have at most d elements in G. Hence by breaking the interval $[1, s]$ into sub intervals of length $2d$ and one sub interval of length less than or equal to $2d$, we see that $|G| \leq \frac{2s}{3}$; the proposition follows.

□

For any subset G of $[0, s-1]$, we will define $G^{(1)}$ to be set of those elements d of $[0, s-1]$ which satisfy a relation of the form $d = b+c-a$ for $a, b, c \in G$, not necessarily distinct. $G^{(i+1)}$ is defined from $G^{(i)}$ inductively. We will define $G^{good} = \cup_{i\geq 0} G^{(i)}$, with $G^{(0)} = G$. In case we have a subset $A \subset [0, s-1]$ at hand and $G \subset A$, then G^{good} shall be obtained by intersecting $G^{(i)}$ with A at each step. The phrase 'A misses an element a' will be used in the sense that a is not in A. We have following useful proposition.

Proposition 6.3.6. *For an integer $s > 3$, consider $A \subset [0, s-1]$ with $|A| \geq 2s/3+1$ then we can choose a set G of two elements a_i, a_j from A such that $G^{good} = A$ and $a_j - a_i = 1$.*

Proof. We use induction on s. Let $t = [s/2]$, be the integral part of $s/2$. Let $A' = A \cap [0, t-1]$ or $A' = A \cap [t, s-1]$ depending upon if A has more elements in $[0, t-1]$ or in the other half. Let us consider the first case, Now by induction hypothesis we can choose a G' such that $G'^{good} \cap A' = A'$ (in second case we translate by t). Now we see that the distance between maximum from

A' and minimum of $A \cap [t, s-1]$ is not more than $s/3$, hence by Lemma 6.3.5, this difference is also achieved as difference of two elements from G'^{good}. This shows that minimum of $A \cap [t, s-1]$ is in G'^{good}. Similar reasoning shows that $G'^{good} \cap A = A$. Take G=G', this proves the proposition. □

The following theorem is an important result in itself and is essential for the proof of Theorem 6.2.2. Here we will use some notations and bounds from the next section (Lemma 6.4.1).

Theorem 6.3.7. *Let $s \geq 6$ and $A = \{0 = a_1, \ldots, a_s\} \subset [0, N-1]$, with $gvd(a_2, \ldots, a_s) = 1$. Also consider integers $x_1, \ldots, x_s$ satisfying*

$$a_j - a_i = a_k - a_l = t \Longrightarrow x_j - x_i = x_k - x_l,$$

whenever $t \leq \frac{s}{2}$. If $|A + A| < \frac{5}{2}s$, then there exist x, y such that $x_i = a_i x + y$ for each i.

Our strategy to prove this theorem is to produce two elements $a_i, a_j \in A$ with $a_j - a_i = 1$ such that for $G = \{a_i, a_j\}$ we have $G^{good} = A$. Once we have two elements a_i, a_j like this, then we can solve for x, y satisfying

$$x_i = a_i x + y \text{ and } x_j = a_j x + y.$$

By the definition of G^{good} it is clear that for every $x_k \in G^{good}$ we have $x_k = a_k x + y$.
Let R be as defined in the beginning of section 6.4, then we can assume $N = s+R-2$. By Lemma 6.4.1 we have $R < \frac{s}{2}+3$. Also if $s \geq \frac{2}{3}(s+R-2)+1$, i.e. $2R \leq s+1$, then by Proposition 6.3.6 we succeed. So we assume $s + 2 \leq 2R \leq s + 5$.
Let a be the largest integer such that A misses a elements from the interval $[0, 2a-1]$ (in case there are no a satisfying this then we take $a = 0$) and let b be the largest integer such that A misses b elements from $[s+R-2b-2, s+R-3]$. Finally let c be the number of elements A misses from $[2a, s + R - 2b - 3]$. We have the following;
Claim: $|A + A| \geq 2s + R - 4 + c$.
To prove the claim, we make the following observation;
for any $n \leq s + R - 3$, if number of elements A misses from $[0, n]$ is strictly less than $\frac{n+1}{2}$, then $n \in A + A$.
Using this we conclude that every element of the interval $[2a, s + R - 3]$ is in $A + A$. Considering $\{s + R - 3 - a_i : a_i \in A\}$, we see that every element of the interval $[s + R - 3 + 2b, 2(s + R - 3)]$ appears in $A + A$. Also there are a elements from $[0, 2a - 1]$ and b elements from $[s + R - 3, s + R - 3 + 2b]$ appearing in $A + A$. But from the b elements of $[s + R - 3, s + R - 3 + 2b]$,

the element $s+R-3$ is already considered. Hence $|A+A| \geq [(s+R-3)-2a+1]+[2(s+R-3)-(s+R-3+2b)+1]+a+b = 2s+R-3+c$, as $a+b+c = R-2$. The claim is established.
Since $|A+A| < \frac{5}{2}s$, we obtain $c \leq 1$. We discuss the case $c=1$, the case $c=0$ being similar. A misses one element from the interval $I = [2a, s+R-2b-3]$, hence for the set $A' = A \cap I$ Proposition 6.3.6 is applicable provided $2s-12 \geq 2R$. Thus, for $s \geq 17$ we can chose two elements $a_i, a_j \in A'$ with $a_j - a_i = 1$ and for $G' = \{a_i, a_j\}$ we have $G'^{good} = A'$. Even though A' misses one element from I but the set $A'+A'-A'$ coincides with the set $I+I-I$. The latter is $[4a-s-R+2b+3, 2s+R-2a-4b-6]$. Now we consider two cases $a \leq b$ and $a > b$.
case 1- $a \leq b$.
Let k be an integer such that $G'^{good} = G'^{(k)}$, then from above it is clear that for $G = G' \in A$, we have $G^{(k+1)} = a \cap [0, s+R-2b-3]$. Also since any element of $A \cap [s+R-2b-3, s+R-3]$ is at most at a distance of $R-2-a-1$ from $s+R-2b-3$, hence using arguments as in Lemma 6.3.5 show that $G^{(k+2)} = A$.
case 2- $a > b$
Here the proof is similar, so we do not give the details.
This finishes proof of the Theorem 6.3.7 for $s \geq 17$. For smaller values of s it is possible to check case by case and we omit the proof.

6.4 Proof of Theorem 6.2.2

For $A' = \{a_1, \ldots, a_s\} \subset \mathbb{Z}$ with $0 \in A'$ and *gcd* of nonzero elements being 1, we shall define $R = min\{max\ a_i - s + 3, s\}$. Clearly $2 \leq R \leq s$. We have the following;

Lemma 6.4.1. $|A'+A'| \geq 2s+R-3$.

Proof. We will consider sets
$G_{1,1} = \ldots = G_{1,s-1} = a_1 + A'$,
$G_{2,1} = G_{2,2} = a_2 + A', G_{3,1} = G_{3,2} = a_3 + A', \ldots, G_{R,1} = G_{R,2} = a_R + A'$,
$G_{R+1} = a_{R+1} + A', \ldots G_s = a_s + A'$.

It is easy to verify that the conditions of Hall's marriage problem are satisfied for the family G_{ij}, which yields $|A'+A'| \geq (s-1)+2(R-1)+(s-R) = 2s+R-3$. The above proof also shows that there are distinct $s-1$ elements in $A'+A'$ with a_1 as a summand, 2 elements with a_i as a summand, for each $2 \leq i \leq R$ and one elements with a_i, for $i > R$, as a summand. □

Now we will assume the setup as in Theorem 6.2.2. Just considering the first co-ordinate, for us the above lemma gives $|\pi_1(\tilde{\mathcal{B}}+\tilde{\mathcal{B}})| \geq 2s+R-3$, where $\pi_1(\tilde{\mathcal{B}}+\tilde{\mathcal{B}})$ denotes the first co-ordinate of $\tilde{\mathcal{B}}+\tilde{\mathcal{B}}$. By considering the second coordinates, we give a lower bound on $|\tilde{\mathcal{B}}+\tilde{\mathcal{B}}|$.

Proposition 6.4.2. *We have the following lower bound,*

$$\begin{aligned}|\tilde{\mathcal{B}}+\tilde{\mathcal{B}}| \;\geq\; & \sum_{j=1}^{s-1}|\mathcal{B}_1+\mathcal{B}_{1,j}|+\sum_{j=s}^{s+1}|\mathcal{B}_2+\mathcal{B}_{2,j}|+\ldots+\sum_{j=s+2R-4}^{s+2R-3}|\mathcal{B}_R+\mathcal{B}_{R,j}| \\ & +|\mathcal{B}_{R+1}+\mathcal{B}_{R+1,j}|+\ldots+|\mathcal{B}_s+\mathcal{B}_{s,j}| \qquad (6.2)\end{aligned}$$

where $\mathcal{B}_{i,j} \in \{\mathcal{B}_1,\ldots,\mathcal{B}_s\}$ and for a fixed i the $\mathcal{B}'_{i,j}s$ are distinct.

Proof. In the proof of Lemma 6.4.1 we have produced $2s+R-3$ elements in $\Pi_1(\tilde{\mathcal{B}}+\tilde{\mathcal{B}})$. There are $s-1$ elements of the form a_1+a_j, 2 elements of the form a_i+a_j for $i=2,\ldots,R$, and 1 elemet of the form a_i+a_j for $i>R$.

This gives us;

$$\begin{aligned}\tilde{\mathcal{B}}+\tilde{\mathcal{B}} \supset\; & \{(a_1+a_i,\mathcal{B}_1+\mathcal{B}_i) \text{ for some } s-1 \text{ values of } i, 1\leq i\leq s\}\cup \\ & \{(a_2+a_i,\mathcal{B}_2+\mathcal{B}_i) \text{ for some 2 values of } i, 1\leq i\leq s\}\cup \\ & \ldots\cup\{(a_R+a_i,\mathcal{B}_R+\mathcal{B}_i) \text{ for some 2 values of } i, 1\leq i\leq s\}\cup \\ & \{(a_{R+1}+a_i,\mathcal{B}_{R+1}+\mathcal{B}_i) \text{ for some } 1\leq i\leq s\}\cup\ldots\cup \\ & \{(a_s+a_i,\mathcal{B}_s+\mathcal{B}_i) \text{ for some } 1\leq i\leq s\}\end{aligned}$$

This way of listing elements of $\tilde{\mathcal{B}}+\tilde{\mathcal{B}}$ plays a critical role in the proof. As a consequence the proposition follows.

□

Mostly we will be assuming $|\mathcal{B}_1|\geq\ldots\geq|\mathcal{B}_s|$ so that the lower bound obtained in the Proposition 6.4.2 is the best by this method, but at times we will be assuming different ordering too.Since $|\mathcal{B}_i+\mathcal{B}_j|\geq max\{|\mathcal{B}_i|,|\mathcal{B}_j|\}$, we obtain the following,

Corollary 6.4.3. $|\tilde{\mathcal{B}}+\tilde{\mathcal{B}}|-|\tilde{\mathcal{B}}|\geq(s-2)|\mathcal{B}_1|+|\mathcal{B}_2|+\ldots+|\mathcal{B}_R|$.

Even though Proposition 6.4.2 holds for all values of R, for $R=2,3$ we will need different consideration at times. For $R=3$ we see that $A'=$

$\{0, 1, \ldots, s\}$ with one element $i_0 \neq 0$ omitted . Here we claim that;

$$\begin{aligned}
\tilde{\mathcal{B}} + \tilde{\mathcal{B}} \supset \quad & \{(a_1 + a_i, \mathcal{B}_1 + \mathcal{B}_i) \text{ for some } s \text{ values of } i, 1 \leq i \leq s\} \cup \\
& \{(a_2 + a_i, \mathcal{B}_2 + \mathcal{B}_i) \text{ for some 2 values of } i, 1 \leq i \leq s\} \cup \\
& \cup\{(a_3 + a_i, \mathcal{B}_3 + \mathcal{B}_i) \text{ for some values of } i, 1 \leq i \leq s\} \cup \\
& \{(a_4 + a_i, \mathcal{B}_4 + \mathcal{B}_i) \text{ for some } 1 \leq i \leq s\} \cup \ldots \cup \\
& \{(a_s + a_i, \mathcal{B}_s + \mathcal{B}_i) \text{ for some } 1 \leq i \leq s\}.
\end{aligned}$$

This is achieved by considering the family of sets
$G_{1,1} = \ldots = G_{1,s} = a_1 + A'$,
$G_{2,1} = G_{2,2} = a_2 + A', G_3 = a_3 + A', \ldots, G_s = a_s + A'$,
and then applying the Hall's marriage theorem. This immediately yields,

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| \geq \sum_{j=1}^{s} |\mathcal{B}_1 + \mathcal{B}_{1,j}| + \sum_{j=s+1}^{s+2} |\mathcal{B}_2 + \mathcal{B}_{2,j}| + |\mathcal{B}_3 + \mathcal{B}_{3,j}| + \ldots + |\mathcal{B}_s + \mathcal{B}_{s,j}|. \quad (6.3)$$

For $R = 2$ a similar consideration yields,

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| \geq \sum_{j=1}^{s} |\mathcal{B}_1 + \mathcal{B}_{1,j}| + |\mathcal{B}_2 + \mathcal{B}_{2,j}| + \ldots + |\mathcal{B}_s + \mathcal{B}_{s,j}|. \quad (6.4)$$

Proposition 6.4.4. *Under the assumption of Theorem 6.2.2 one has max* $a_i < 1.5s$.

Proof. Using the trivial lower bound on $|\mathcal{B}_i + \mathcal{B}_j|$ in equation (6.2) we obtain,

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| \geq (s-1)|\mathcal{B}_1| + 2|\mathcal{B}_2| + \ldots + 2|\mathcal{B}_R| + |\mathcal{B}_{R+1}| + \ldots + |\mathcal{B}_s|.$$

Since $|\tilde{A}| = \sum_i |\mathcal{B}_i|$, from above we obtain

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| - |\tilde{\mathcal{B}}| \geq ((s-2)|\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_R|) \cdot \frac{s+R-3}{s+R-3}.$$

Now

$$\frac{(s-2)|\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_R|}{s+R-3},$$

being average of $|\mathcal{B}_1|$, $s-2$ times, and $|\mathcal{B}_2|, \ldots, |\mathcal{B}_R|$, is greater than the average of $|\mathcal{B}_1|, \ldots, |\mathcal{B}_s|$, namely

$$\frac{\sum_i |\mathcal{B}_i|}{s}$$

(as $|\mathcal{B}_1| \geq |\mathcal{B}_i|$ and $s + R - 3 \geq s$). This gives

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| - |\tilde{\mathcal{B}}| \geq \frac{\sum_i |\mathcal{B}_i|}{s}(s + R - 3).$$

Now because of the assumption we get $s + R - 3 < 1.5s$. Thus $R \neq s$ and hence $R = max\ a_i - s + 3$, and this gives the proposition. □

Now we intend to exhibit the subgroup $\tilde{\mathcal{H}}$ as sought in Theorem 6.2.2. This will be done through next few lemmas.

Lemma 6.4.5. *There exists a subgroup $\tilde{\mathcal{H}}$ of $\mathbb{Z}/d\mathbb{Z}$ such that $\mathcal{B}_1$ lies in a single coset of $\tilde{\mathcal{H}}$ and $|\tilde{\mathcal{H}}| < 3/2|B_1|$.*

Proof. If $|\mathcal{B}_1 + \mathcal{B}_i| < 3/2|\mathcal{B}_1|$ and $|\mathcal{B}_i| > 3/4|\mathcal{B}_1|$, then from Proposition 6.3.3 we get that $\mathcal{B}_1 + \mathcal{B}_i$ lies in a single coset of the stabilizer and consequently $\mathcal{B}_1$ also lies in a single coset. We will partition $\mathcal{B}_i's$ in three different categories.
$U = \{a_i : |\mathcal{B}_i| > \frac{3}{4}|\mathcal{B}_1|\}$,
$V = \{a_i : \frac{1}{2}|\mathcal{B}_1| < |\mathcal{B}_i| \leq \frac{3}{4}|\mathcal{B}_1|\}$ and
$W = \{a_i : |\mathcal{B}_i| \leq \frac{1}{2}|\mathcal{B}_1|\}$.
We let u, v and w denote the respective cardinality.
If there is no subgroup as claimed in the lemma, then as seen in the Proposition 6.3.3 and Proposition 6.3.4, one has,

$|\mathcal{B}_1 + \mathcal{B}_i| \geq \frac{3}{2}|\mathcal{B}_1|$, if $a_i \in U$,
$|\mathcal{B}_1 + \mathcal{B}_i| \geq 2|\mathcal{B}_i|$, if $a_i \in V$,
$|\mathcal{B}_1 + \mathcal{B}_i| \geq |\mathcal{B}_1|$ otherwise.

Then using equation (6.2) one obtains;

$$|\tilde{\mathcal{B}}+\tilde{\mathcal{B}}| \geq \frac{3(u-1)}{2}|\mathcal{B}_1|+2\sum_{a_i\in V}|\mathcal{B}_i|+w|\mathcal{B}_1|+2(|\mathcal{B}_2|+\ldots+|\mathcal{B}_R|)+|\mathcal{B}_{R+1}|+\ldots+|\mathcal{B}_s|.$$

This gives;

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| - \tilde{\mathcal{B}} \geq \frac{3}{2}(u-1)|\mathcal{B}_1| + 2\sum_i |\mathcal{B}_i| + w|\mathcal{B}_1| - |\mathcal{B}_1| + (|\mathcal{B}_2| + \ldots + |\mathcal{B}_R).$$

But we are given $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| - |\tilde{\mathcal{B}}| < 1.5|\tilde{\mathcal{B}}|$. Comparing the two inequalities we get,

$$1.5|\tilde{\mathcal{B}}| > \frac{3}{2}(u-1)|\mathcal{B}_1| + 2\sum_{a_i\in V} |\mathcal{B}_i| + w|\mathcal{B}_1| - |\mathcal{B}_1| + (|\mathcal{B}_2| + \ldots + |\mathcal{B}_R|).$$

Now we will assume that $R \geq 4$. In case $u + v = 1$, then above inequality already yields a contradiction. So we assume that $u + v > 1$.
Let us put,
$|\mathcal{B}_i|' = |\mathcal{B}_1|$ if $a_i \in U$, $|\mathcal{B}_i|' = \frac{3}{4}|\mathcal{B}_1|$ if $a_i \in V$ and $|\mathcal{B}_i|' = \frac{1}{2}|\mathcal{B}_1|$ if $a_i \in W$.
Also we will write $V = X \cup Y$, where $X = V \cap \{a_2, \ldots, a_4\}$. For $a_i \in V$ we have $|\mathcal{B}_1 + \mathcal{B}_i| \geq max\{2|\mathcal{B}_i|, |\mathcal{B}_1|\}$ so we get $|\mathcal{B}_1 + \mathcal{B}_i| \geq 0.5|\mathcal{B}_i| + 0.75|\mathcal{B}_1|$

and $|\mathcal{B}_1 + \mathcal{B}_i| \geq \frac{3}{2}|\mathcal{B}_i| + \frac{1}{4}|\mathcal{B}_1|$ as well. We will use the first inequality when $a_i \in X$ and the second one when $a_i \in Y$. Then proceeding as above, from equation (6.2) we obtain

$$\begin{aligned} 1.5|\tilde{\mathcal{B}}| \quad &\geq 1.5(u-1)|\mathcal{B}_1| + 0.5\sum_{a_i \in X}|\mathcal{B}_i| + 0.75x|\mathcal{B}_1| + 1.5\sum_{a_i \in Y}|\mathcal{B}_i| \\ &\quad +0.25y|\mathcal{B}_1| + w|\mathcal{B}_1| - |\mathcal{B}_1| + (|\mathcal{B}_2| + \ldots + |\mathcal{B}_4|), \end{aligned}$$

with $x = |X|$ and $y = |Y|$.

Since coefficient of each $|\mathcal{B}_i|, i > 1$ in above inequality (after shifting everything to the left) is non negative so we can replace each $|\mathcal{B}_i|$ by $|\mathcal{B}_i|'$. This argument leads to

$$0 > -2.5|\mathcal{B}_1| + 0.25y|\mathcal{B}_1| + 0.25w|\mathcal{B}_1| + (|\mathcal{B}_2|' + \ldots + |\mathcal{B}_4|').$$

Note that $u+x+y+w = s \geq 5$ and $x \leq 3$. Using this in the above inequality we obtain a contradiction.

The same argument works for $R = 3$ by taking $X = V \cap \{a_2\}$ and using equation (6.3).

We give the sketch of the proof for $R = 2$. Equation (6.4) leads to,

$$(1.5)u|\mathcal{B}_1| + 2\sum_{j \in V}|\mathcal{B}_j| + w|\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_s| \leq |\tilde{\mathcal{B}} + \tilde{\mathcal{B}}|. \tag{6.5}$$

Since $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| < 2.5|\tilde{\mathcal{B}}|$, the above inequality yields a contradiction whenever $w \geq 4$ or $v \geq 2$. Also when $v = 1$ and $w = 3$, the above inequality leads to a contradiction. Thus we can assume $v + w \leq 3$.

Observe that for $a_i, a_j \in U$, we always have
$(|B_1| + |\mathcal{B}_i|) + (|\mathcal{B}_i| + |\mathcal{B}_j|) \geq 3|\mathcal{B}_i|$. (For this we use, if $\mathcal{B}_i$ is in a single coset then $|B_1| + |\mathcal{B}_i| \geq 2|\mathcal{B}_i|$ and otherwise $|B_i| + |\mathcal{B}_j| \geq \frac{3}{2}|\mathcal{B}_i|$). For any i let $A_i = \{a_j : j \leq i\}$, then $A_i + A_i \subset A' + A'$, and has at least $2i - 1$ elements. Further, when there are $2i - 1$ elements in $A_i + A_i$, there is some $j \leq i$ such that $A_{i+1} + A_{i+1} = A_i + A_i \cup \{a_{i+1} + a_{i+1}, a_{i+1} + a_j\}$. This gives us the lower bound

$$(1.5)|\mathcal{B}_1| + 3|\mathcal{B}_2| + \ldots + 3|\mathcal{B}_u| + 2|\mathcal{B}_{u+1}| + \ldots + 2|\mathcal{B}_{u+3}| < 2.5|\tilde{\mathcal{B}}|. \tag{6.6}$$

Since $v + w \leq 3$, above yields a contradiction when $u \geq 7$. So we assume $u < 7, v + w < 4$. These cases can be worked out using the techniques developed so far, but for the sake of completeness we will sketch the proof.

Now we shall consider four cases;

Case (1)- $v + w = 3$.

If some $\mathcal{B}_i$ with $a_1 \neq a_i \in U$ lies in a single coset, then $|\mathcal{B}_1 + \mathcal{B}_i| \geq 2|\mathcal{B}_i|$, and

we obtain

$$\frac{3}{2}(u-1)|\mathcal{B}_1| + 2|\mathcal{B}_i| + 2\sum_{a_j \in V} |\mathcal{B}_j| + w|\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_s| \leq \tilde{\mathcal{B}} + \tilde{\mathcal{B}}.$$

This immediately yields a contradiction.
In case all $\mathcal{B}_i$ with $a_i \in U$ lies in more than one coset (for any such subgroup), then we break $A' + A'$ in $U + U, U + V \cup W$ and $V \cup W + V \cup W$. We note that in $A' + A'$, we can consider 3 elements from $V \cup W + V \cup W$, 3 elements from $U + V \cup W$ and rest from $U + U$. This consideration yields,

$$3|\mathcal{B}_1| + \ldots + 3|\mathcal{B}_{u-1}| + \frac{3}{2}|\mathcal{B}_u| + |\mathcal{B}_u + \mathcal{B}_{u+1}| + 2|\mathcal{B}_u + \mathcal{B}_{u+3}| + 2|\mathcal{B}_{u+2}| + |\mathcal{B}_{u+3}|) < 2.5|\tilde{\mathcal{B}}|. \tag{6.7}$$

Adding equation (6.6) and (6.7) we obtain

$$(1.5)u|\mathcal{B}_1| - 0.5|\mathcal{B}_u| + |\mathcal{B}_u + \mathcal{B}_{u+1}| + |\mathcal{B}_u + \mathcal{B}_{u+3}| + |\mathcal{B}_{u+2}| - |\mathcal{B}_{u+1}| < \sum_i |\mathcal{B}_i|,$$

i.e.

$$\frac{1}{2}(u-1)|\mathcal{B}_1| + |\mathcal{B}_u + \mathcal{B}_{u+1}| + |\mathcal{B}_u + \mathcal{B}_{u+3}| < 2|\mathcal{B}_{u+1}| + |\mathcal{B}_{u+3}|,$$

this gives a contradiction.
Case (2)- $v + w = 2$.
If there are two or more $\mathcal{B}_i$ with $a_1 \neq a_i \in U$ which lie in a single coset, then we are through as in earlier case (these two $\mathcal{B}_i$ contributing $0.5|\mathcal{B}_i|$ each and $0.5|\mathcal{B}_1|$, coming from $V \cup W$).
If there is only one such $\mathcal{B}_i$ which lies in a single coset. Let $a_j \neq a_1, a_i \in U$, then $a_j + U \neq a_1 + U$ and hence we obtain

$$\frac{3}{2}(u-1)|\mathcal{B}_1| + 2|\mathcal{B}_i| + \frac{3}{2}|\mathcal{B}_j| + |\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_s| \leq \tilde{\mathcal{B}} + \tilde{\mathcal{B}}.$$

(One $|\mathcal{B}_1 + \mathcal{B}_j|$ coming at the expense of one $|\mathcal{B}_1 + \mathcal{B}_t|$ with $t \in V \cup W$ or $|\mathcal{B}_m + \mathcal{B}_t|$ for $m > 1$).
This yields a contradiction if $1.5|\mathcal{B}_1| + .5|\mathcal{B}_i| > 1.5(|\mathcal{B}_{u+1}| + |\mathcal{B}_{u+2}|)$. If this inequality does not hold then we have $v = 2, w = 0$ and from

$$\frac{3}{2}(u-1)|\mathcal{B}_1| + 2|\mathcal{B}_i| + 2\sum_{a_j \in V} |\mathcal{B}_j| + w|\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_s| \leq \tilde{\mathcal{B}} + \tilde{\mathcal{B}}$$

we get $0.5(|\mathcal{B}_i| + |\mathcal{B}_{u+1}| + |\mathcal{B}_{u+2}|) < |\mathcal{B}_1|$, this is not possible given that $1.5|\mathcal{B}_1| + 0.5|\mathcal{B}_i| \leq 1.5(|\mathcal{B}_{u+1}| + |\mathcal{B}_{u+2}|)$.
If there are no $\mathcal{B}_i$ with $a_i \in U$ which lies in a single coset, then by considering

the contribution of $U+U, U+V\cup W$ and $V\cup W+V\cup W$ separately in descending order we obtain

$$3|\mathcal{B}_1|+\ldots+3|\mathcal{B}_{u-1}|+\frac{3}{2}|\mathcal{B}_u|+\frac{5}{2}(|\mathcal{B}_{u+1}|+|\mathcal{B}_{u+2}|)<2.5|\tilde{\mathcal{B}}|,$$

which in turn gives $0.5(|\mathcal{B}_1|+\ldots+|\mathcal{B}_{u-1}|)<|\mathcal{B}_u|$, a contradiction as $u\geq 3$.
case (3)- $v+w=1$.
If two or more $\mathcal{B}_i$ with $a_1\neq a_i\in U$ lie in a single coset then we are through.
If there is only one $\mathcal{B}_i$ which lies in a single coset then we can obtain

$$\frac{3}{2}(u-1)|\mathcal{B}_1|+2|\mathcal{B}_i|+\frac{3}{2}\sum_{a_j\neq a_1,a_u\in U}|\mathcal{B}_j|+|\mathcal{B}_u|+2|\mathcal{B}_{u+1}|\leq\tilde{\mathcal{B}}+\tilde{\mathcal{B}},$$

this gives a contradiction as $u\geq 4$.
case (4)- $v+w=0$.
If three or more $\mathcal{B}_i$ with $a_1\neq a_i\in U$ lie in a single coset then we are through.
If only two of $\mathcal{B}_i$ with $a_i\neq a_1$ lie in a single coset, say $\mathcal{B}_{u-1},\mathcal{B}_u$. Among the rest $u-2$ let us consider the ordering $|\mathcal{B}_1|\geq\ldots\geq|\mathcal{B}_{u-2}|$. We can obtain

$$3(|\mathcal{B}_1|+\ldots+|\mathcal{B}_{u-3}|)+\frac{3}{2}|\mathcal{B}_{u-2}|+2|\mathcal{B}_{u-1}|+|\mathcal{B}_{u-1}|+|\mathcal{B}_u|+|\mathcal{B}_u|<2.5|\tilde{\mathcal{B}}|,$$

since $u\geq 5$ we have a contradiction.
The cases when one or none of $\mathcal{B}_i$ with $a_1\neq a_i$ lie in a single coset are very similar to the calculation done earlier. □

Next we shall show that each of the $\mathcal{B}_i$ lies in a single coset of $\tilde{\mathcal{H}}$ for some subgroup $\tilde{\mathcal{H}}$ of $\mathbb{Z}/d\mathbb{Z}$ with $|\tilde{\mathcal{H}}|<3/2|\mathcal{B}_1|$. This is content of Lemma 6.4.6.

Lemma 6.4.6. *There is a subgroup $\tilde{\mathcal{H}}$ of $\mathbb{Z}/d\mathbb{Z}$ with $|\tilde{\mathcal{H}}|<3/2|\mathcal{B}_1|$ such that each of the $\mathcal{B}_i$ is contained in a single coset of $\tilde{\mathcal{H}}$.*

Proof. For a clear exposition we shall give the proof when $R\geq 4$. The cases $R=2,3$ can be handled with a bit more careful working. Here we shall consider $\tilde{\mathcal{B}}$ in various different ordering. Let us write

$$\begin{aligned}\tilde{\mathcal{B}} &= \{(a_i,C_i):1\leq i\leq r;|C_1|\geq|C_2|\geq\ldots\}\cup\\ &\quad\{(a_{r+j},D_j):1\leq j\leq t;|D_1|\geq|D_2|\geq\ldots\},\end{aligned}$$

where C_i lies in a singel coset modulo H for the subgroup H of lemma 3 and D_j does not lie in a singel coset modulo H.
By Lemma 6.4.5, we have $C_1=\mathcal{B}_1$ and one immediately has $|C_1+C_i|\geq|C_1|$

and $|C_1 + D_j| \geq 2|C_1|$. Now using the description of $\tilde{\mathcal{B}} + \tilde{\mathcal{B}}$, we obtain;

$$|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| \geq (r + 2t - 2)|\mathcal{B}_1| + 2|\mathcal{B}_2| + \ldots + 2|\mathcal{B}_R| + |\mathcal{B}_{R+1} + \ldots + |\mathcal{B}_s|.$$

Next let us write (after a rearrangement),
$\tilde{\mathcal{B}} = \{(a_i, \mathcal{B}_i) : \mathcal{B}_i = D_i \text{ for } 1 \leq i \leq t \text{ and } B_{t+i} = C_i \text{ for } 1 \leq i \leq r\}$.
Proceeding in the same way for this listing of $\tilde{\mathcal{B}}$, as we had done to obtain equation (6.2), we get

$$\begin{aligned} |\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| \quad \geq \quad & t|D_1| + 2|C_2| + \ldots + 2|C_r| + 2|D_2| + \ldots + 2|D_4| + |D_5| + \ldots + |D_t| \\ & + |C_1| + \ldots + |C_r|, \end{aligned}$$

assuming $R \geq 4$ and $t \geq 4$. When $t \leq 3$ then also the method works with appropriate changes. Now we assume $c' < 2.5$ and add the two lower bounds on $|\tilde{\mathcal{B}} + \tilde{\mathcal{B}}|$ to obtain,

$$\begin{aligned} & (r + 2t - 2)|\mathcal{B}_1| + 2|\mathcal{B}_2| + \ldots + 2|\mathcal{B}_R| + |\mathcal{B}_{R+1} + \ldots + |\mathcal{B}_s| \\ 5|\tilde{\mathcal{B}}| \quad > \quad & + t|D_1| + 2|C_2| + \ldots + 2|C_r| + 2|D_2| + \ldots + 2|D_4| + |D_5| + \ldots + |D_t| \\ & + |C_1| + \ldots + |C_r|. \end{aligned}$$

We note that

$$|\tilde{\mathcal{B}}| = \sum_{i=1}^{s} |\mathcal{B}_i| = \sum_{i} |A_i| = \sum_{i=1}^{r} |C_i| + \sum_{i=1}^{t} |D_i|.$$

Also $|\mathcal{B}_1| = |C_1|$, this immediately yields,

$$3|\tilde{\mathcal{B}}| > (r+2t-3)|\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_R| + (t-1)|D_1| + 2|C_2| + \ldots + 2|C_r| + |D_2| + \ldots + |D_4|.$$

Further we have $s = r + t$ and $(s-3)|\mathcal{B}_1| + |\mathcal{B}_2| + \ldots + |\mathcal{B}_R| \geq |\tilde{\mathcal{B}}|$, so we get,

$$2|\tilde{\mathcal{B}}| > t|\mathcal{B}_1| + (t-1)|D_1| + 2|C_2| + \ldots + 2|C_r| + |D_2| + \ldots + |D_4|.$$

Since $(t-2)|\mathcal{B}_1| + |D_3| + |D_4| \geq \sum_i |D_i|$ and $(t-1)|D_1| + |D_2| \geq \sum_i |D_i|$, the above yields $2|\tilde{\mathcal{B}}| > 2|\tilde{\mathcal{B}}|$, a contradiction. □

Let $x_i \in \mathbb{Z}/d\mathbb{Z}$ be such that $\mathcal{B}_i \subset x_i + \tilde{\mathcal{H}}$. Next we shall prove the existence of $x \in \mathbb{Z}/d\mathbb{Z}$ such that $\mathcal{B}_i \subset a_i x + \tilde{\mathcal{H}}$. Actually we shall exhibit $x, y \in \mathbb{Z}/d\mathbb{Z}$ satisfying $\mathcal{B}_i \subset a_i x + y + \tilde{\mathcal{H}}$, but this is sufficient as translation by a fixed element is a $2-isomorphism$. We shall give the proof for $R \geq 4$. The basic idea is to show that if such an x and y can not be obtained then it will result in more terms on right side of equation (2), which will exceed the limit. This is made precise below.

First we note that, from Proposition 6.4.4, $R < s/2 + 3$. Also this gives us $max\{a_i\} < 1.5s$. For $1 \leq k \leq R-2$ we will consider,

$$S_k = \{(a_i, a_j) \in A' \times A' : a_j - a_i = k\}.$$

Note that $|S_k| \geq s - R - k + 1$. To see this we form pairs (a_i, a_j) with all choices of $0 \leq a_i, a_j \leq max\{a_i\}$ satisfying $a_j - a_i = k$, there are exactly $s + R - 3 - k$ many such pairs. Of these, at most $2(R-2)$ of them can have either a_i or a_j not in A'. Now for (a_i, a_j) and $(a_u, a_v) \in S_k$ we will define $(a_i, a_j) \backsim (a_u, a_v)$ if $x_j - x_i = x_v - x_u \pmod{\tilde{\mathcal{H}}}$. We contend that under this equivalence S_1 has only one equivalence class. Let $S_1 = \sqcup_{j=1}^{t} S_{1j}$ be the decomposition of S_1 in disjoint equivalence classes. We want to show that $t = 1$. Let us assume $t > 1$. For $j \neq j'$ and $(a_u, a_v) \in S_{1j}, (a_w, a_z) \in S_{1j'}$ we have $a_v + a_w = a_u + a_z$, where as $\mathcal{B}_u + \mathcal{B}_z \cap \mathcal{B}_v + \mathcal{B}_w = \emptyset$. For the lower bound on $|2\tilde{\mathcal{B}}|$ in equation (6.2) we had considered at most one of $\mathcal{B}_j + \mathcal{B}_v$ and $\mathcal{B}_i + \mathcal{B}_u$, corresponding to the first co-ordinate $a_v + a_w = a_u + a_z$. This reasoning shows that, if S_1 has more than one equivalence class then we can improve upon equation (6.2) to obtain a better lower bound.
Let S_{1j_0} have maximum cardinality among all equivalence classes, j_0 need not be unique and if there are more choices we fix any one. We arrange elements of S_{1j_0} with first co-ordinate in increasing order, and consider them as a row. Also we can arrange the elements of S_1 which are not in S_{1j_0} with first co-ordinate in increasing order, and consider them as a column. For every (a_u, a_v) in the row and every (a_w, a_z) in the column we have an element $a_v + a_w = a_u + a_z$ in $A' + A'$, and all such elements are distinct. Corresponding to the first co-ordinate $a_v + a_w = a_u + a_z$, at most one of $\mathcal{B}_j + \mathcal{B}_v$ and $\mathcal{B}_i + \mathcal{B}_u$ was considered in equation (6.2). But $\mathcal{B}_j + \mathcal{B}_v$ and $\mathcal{B}_i + \mathcal{B}_u$ are disjoint. Thus we get at least $s - R - 1$ many more summands in equation (6.2). Note that these summands are different because of the condition $\mathcal{B}_u + \mathcal{B}_z \cap \mathcal{B}_v + \mathcal{B}_w = \emptyset$. We obtain

$$\begin{aligned} |\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| \quad \geq \quad & \sum_{j=1}^{s-1} |\mathcal{B}_1 + \mathcal{B}_{1,j}| + \sum_{j=s}^{s+1} |\mathcal{B}_2 + \mathcal{B}_{2,j}| + \ldots + \sum_{j=s+2R-4}^{s+2R-3} |\mathcal{B}_R + \mathcal{B}_{R,j}| \\ & + |\mathcal{B}_{R+1} + \mathcal{B}_{R+1,j}| + \ldots + |\mathcal{B}_s + \mathcal{B}_{s,j}| \\ & + (|\mathcal{B}_s| + \ldots + |\mathcal{B}_{s-(s-R)}|). \end{aligned}$$

This lower bound leads to a contradiction, by noticing that each $|\mathcal{B}_i|$ can be replaced by $|\mathcal{B}_1|$ and there are at least $\frac{5s}{2}$ terms on the right side. This proves that S_1 shall have only one equivalence class. Similar analysis shows that S_k has only one equivalence class.

Thus for $t \leq R-2$, we have

$$a_j - a_i = a_k - a_l = t \Longrightarrow x_j - x_i = x_k - x_l.$$

Also it is easy to obtain $|A' + A'| < \frac{5s}{2}$. Now we can appeal Theorem 6.3.7 to prove the existence of x and y as claimed. Next we intend to prove the last assertion of the Theorem 6.2.2, namely;

$$max\ a_i|\tilde{\mathcal{H}}| < |\tilde{\mathcal{B}} + \tilde{\mathcal{B}}| - |\tilde{\mathcal{B}}|.$$

Note that $max\ a_i = s + R - 3$. We consider sets,
$U = \{a_i : |A_i| \geq \frac{2}{3}|\tilde{\mathcal{H}}|\}, \quad V = \{a_i : \frac{1}{3}|\tilde{\mathcal{H}}| \leq |A_i| < \frac{2}{3}|\tilde{\mathcal{H}}|\},$
$W = \{a_i : |A_i| < \frac{1}{3}|\tilde{\mathcal{H}}|\}$
A first coordinate of $\tilde{\mathcal{B}} + \tilde{\mathcal{B}}$ will be referred as 'good' if it can be represented in the form $u + v$ with $u \in U, v \in U \cup V$. Every 'good' first coordinate contributes $|\tilde{\mathcal{H}}|$ in equation (6.2). Showing that $|W| \leq 1$ establishes the result with the help of equation (6.2). We shall write u, v, w for the number of elements in U, V, W respectively, also elements of U will be denoted by $u_1 < \ldots < u_u$.

Lemma 6.4.7. *Under the hypothesis of the Theorem 6.2.2 we have* $u \geq w + 2R - 3$.

Proof. First we establish $u \geq R$.
On the contrary if $R > u$, then equation (6.2) gives us the inequality

$$(u+v-1)|\tilde{\mathcal{H}}| + (w+u-2)|\mathcal{B}_1| + 2/3(R-u)|\tilde{\mathcal{H}}| < 1.5u|\mathcal{B}_1| + v|\tilde{\mathcal{H}}| + .75w|\mathcal{B}_1|.$$

This is proved by shifting $\mathcal{B}_2, \ldots \mathcal{B}_R$ on the right side of equation (6.2) and noticing that the coefficient is positive so one can replace them by a bigger quantity, namely $|\mathcal{B}_1|$. Simplifying this yields

$$u|\tilde{\mathcal{H}}| + 0.25w|\mathcal{B}_1| + 2/3(R-u)|\tilde{\mathcal{H}}| < (0.5u + 2)|\mathcal{B}_1| + |\tilde{\mathcal{H}}|,$$

Since $R > u, u \geq 1, w \geq 2$ we obtain a contradiction. Thus we have $u \geq R$. Using this in equation (6.2) yields,

$$(u + v - 1)|\tilde{\mathcal{H}}| + (w + R - 2)|\mathcal{B}_1| < 1.5u|\mathcal{B}_1| + v|\tilde{\mathcal{H}}| + 0.5w|\tilde{\mathcal{H}}|.$$

As $2/3|\tilde{\mathcal{H}}| \leq |\mathcal{B}_1| \leq |\tilde{\mathcal{H}}|$, the above inequality shall be true for one of the extreme value of $|\mathcal{B}_1|$, as the inequality is linear in $|\mathcal{B}_1|$. Putting $|\mathcal{B}_1| = 2/3|\tilde{\mathcal{H}}|$ gives a contradiction and $|\mathcal{B}_1| = |\tilde{\mathcal{H}}|$ gives $u \geq w + 2R - 5$. We need to gain a bit more. Since $R \geq 4$, we have $u \geq R + 1$. Let us partition W in two parts,

$W_1 = \{a_i : |\mathcal{B}_i| \geq |\tilde{\mathcal{H}}| - |\mathcal{B}_R|\}$, $W_2 = \{a_i : |\mathcal{B}_i| < |\tilde{\mathcal{H}}| - |\mathcal{B}_R|\}$ with w_1, w_2 being their cardinality respectively. Again if $w_2 \leq 1$ then equation (6.2) will already prove the assertion of the Theorem. As in this case in equation (6.2) there will be at most s first coordinates with summands from W_2 which will contribute at least $|\tilde{\mathcal{B}}|$ in equation (6.2) and rest will contribute $(s+R-3)|\tilde{\mathcal{H}}|$. Equation (6.2) helps us in having,

$$\left\{ \begin{matrix} (u+v+w_1-1)|\tilde{\mathcal{H}}|+ \\ (w_2+R-3)|\mathcal{B}_1| + |\mathcal{B}_R| \end{matrix} \right\} < \left\{ \begin{matrix} 1.5(R-1)|\mathcal{B}_1| + 1.5(u-R+1)|\mathcal{B}_r|+ \\ v|\tilde{\mathcal{H}}| + 0.5w_1|\tilde{\mathcal{H}}| + 1.5w_2(|\tilde{\mathcal{H}}| - |\mathcal{B}_R|) \end{matrix} \right\},$$

i.e.

$$[u+0.5w_1-1.5w_2-1]|\tilde{\mathcal{H}}|+[w_2-0.5R-1.5]|\mathcal{B}_1|+[1.5(w_2-u+R)-0.5]|\mathcal{B}_R| < 0.$$

Since the last inequality does not hold for $|\mathcal{B}_1| = 2/3|\tilde{\mathcal{H}}|$ (which in turn will also give $|\mathcal{B}_1| = |\mathcal{B}_R|$), so it shall be true when $|\mathcal{B}_1|$ is replaced by $|\tilde{\mathcal{H}}|$. This gives us,

$$(u + 0.5w_1 - 0.5w_2 - 0.5R - 2.5)|\tilde{\mathcal{H}}| + (1.5w_2 - 1.5u + 1.5R - 0.5)|\mathcal{B}_R| < 0.$$

Again, as $2/3|\tilde{\mathcal{H}}| \leq |\mathcal{B}_R| \leq |\tilde{\mathcal{H}}|$, as done earlier, we obtain $u > w_1 + 2w_2 + 2R - 6$. As $w_2 \geq 2$ we get $u \geq w + 2R - 3$, this proves the lemma. □

We call an element of A' 'desirable' if all the first coordinates (of $\tilde{\mathcal{B}} + \tilde{B}$) it contributes to are 'good' and we say it is 'almost desirable' if all but one coordinates it contributes to are 'good'. Our aim is to show that there is at least one 'desirable' and at least $R-1$ 'almost desirable' elements in A'. Then renaming desirable element as a_1 and almost desirable elements as $a_2, \ldots, a_R$ in equation (6.2) yields the result. Towards this, we take T as complement of A' in $[0, s+R-3]$ and $K = W \cup T$. The cardinality of K is $k = w+R-2$. Let d_1 be the number of elements of K which are smaller than u_{k+1} and d_2 be the number of elements of K which are bigger than u_{k+1}. We first assume that none of d_i is zero and finish the proof.
Claim: When none of d_i is zero then every element of U in the interval (u_{d_1}, u_{u-d_2}) is 'desirable' and u_{d_i} is 'almost desirable'.
Let $u_j \in U \cap (u_{d_1}, u_{u-d_2})$ and $w \in W$ then we wish to show that $u_j + w = u + v$ for some $u \in U, v \in U \cup V$.
case (1)- $u_{c+1} \leq u_j + w < u_{k+1}$.
All elements $u_j + w - u_r, 1 \leq r \leq c+1$ are smaller than u_{k+1} and are in $[0, s+R-3]$, hence can not be in K, proving that u_j is 'desirable'.
case (2)- $u_{k+1} \leq u_j + w \leq s + R - 3$.
Here, the elements $u_j + w - u_r, 1 \leq r \leq k+1$ can not all lie in K, making u_j a 'desirable' element.

case (3)- $u_j + w \leq s + R - 3 + u_{u-k}$.
In this case one of the elements from $u_j + w - u_r, u - k \leq r \leq u$ makes u_j 'desirable'.
case (4)- $u_j + w > s + R - 3 + u_{u-k}$.
Now one of the elements $u_j + w - u_r, u - d_2 \leq r \leq u$ assures that u_j is 'desirable'.
This produces $R - 1$ desirable elements. Similar analysis shows that the elements u_{d_1}, u_{d_2} are 'almost desirable'. In case one of d_1 and d_2 is zero, say $d_2 = 0$. In this case clearly u_j with $u_j + w \geq u_{k+1}$ is 'desirable' and there are $R - 1$ such u_j, namely u_r, for $r \geq k + 1$. We claim that u_k is almost desirable. For this we notice that there can be at most one w such that $\{u_k + w - u_j : 1 \leq j \leq k\} = K$ and thus u_k contributes to all but one good coordinate, proving that u_k is almost desirable. The case when $d_1 = 0$ is similar.

6.5 Proof of Theorem 6.2.1

We continue with the notations of the previous section. To prove the Theorem 6.2.1 we shall use a partial lift of $\mathcal{A}$ to a subset $\tilde{\mathcal{B}} \subset \mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$, which satisfies conditions of the Theorem 6.2.2 and thus has the structures provided from the theorem. Using the structure of $\tilde{\mathcal{B}}$ we shall exhibit that on $\mathcal{A}$. Also we shall give the proof for the case when $\mathcal{A}$ has 5 or more 'layers'. For the definition of 'layers' and the proof of the Theorem 6.4.1 when $\mathcal{A}$ has less than 5 'layers' we refer the reader to [16]. Let us consider the following factorization $n = md$ for some $m \geq 240$. For $\mathbb{Z}/n\mathbb{Z}$ we shall take $\{0, 1, \ldots, n-1\}$ and for any $t \in \mathbb{Z}/n\mathbb{Z}$, let $t = m\eta + \xi$, with $0 \leq \xi < m$, be its representation in Euclidean algorithm for the pair (t, m).
This gives a map $\mathbb{Z}/n\mathbb{Z} \mapsto [0, m] \times \mathbb{Z}/d\mathbb{Z}$.
For any integer u coprime to n we shall compose above map with $\mathbb{Z}/n\mathbb{Z} \xrightarrow{u} \mathbb{Z}/n\mathbb{Z}$ to obtain the map

$$\phi = \phi_u : \mathbb{Z}/n\mathbb{Z} \xrightarrow{u} \mathbb{Z}/n\mathbb{Z} \mapsto \mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}.$$

We will write $\phi = (\phi_1, \phi_2)$ as the comma map, where ϕ_j is obtained after composing with the j^{th} projection. We make the following;
Claim: There exists a u and a k such that for $T = [k, k + m/2]$ we have $|\phi^{-1}(T) \cap \mathcal{A}| \geq 0.844|\mathcal{A}|$.
To establish the claim we shall use the theory of Fourier transform and a result of Freiman [14].

For any integer u the Fourier transform of $\mathcal{A}$ is defined to be (see [44]),

$$\hat{\mathcal{A}}(u) = \sum_{a \in \mathcal{A}} exp(2\pi au/n).$$

The result of Freiman states the following;

Theorem 6.5.1. *(Freiman) If u_0 satisfies $|\hat{\mathcal{A}}(u_0)| \geq l|\mathcal{A}|$. Then $u_0\mathcal{A}$ modulo n has at least $\frac{1+l}{2}|\mathcal{A}|$ elements in some half circle modulo n, that is there exists k, such that at least $\frac{1+l}{2}|\mathcal{A}|$ elements of $u_0\mathcal{A}$ modulo n are contained in $[k, k+n/2]$.*

There are improvements of this result due to Lev [29, 30]. These improvements will be able to give the Theorem 4 for a higher value of c than claimed here. But for our purpose the result of Freiman suffices. The following lemma is already proved in [16], we reproduce the proof for the sake of completeness.

Lemma 6.5.2. *There exists $u \neq 0$ such that $|\hat{\mathcal{A}}(u_0)| \geq 0.6868|\mathcal{A}|$.*

Proof.

$$S_1(u) = \sum_{a \in \mathcal{A}} exp(2\pi au/n), \quad S_2(u) = \sum_{b \in \mathcal{A}+\mathcal{A}} exp(2\pi bu/n),$$

for integers u coprime to n. Next let us put

$$S = \sum_{u=0}^{n-1} S_1^2(u)\bar{S}_2(u).$$

One has,

$$\begin{aligned}
S &= \sum_{u=0}^{n-1} \sum_{\substack{a_1,a_2 \in \mathcal{A}, \\ b \in \mathcal{A}+\mathcal{A}}} exp(2\pi iu(a_1+a_2-b)/n) \\
&= \sum_{a_1 \in \mathcal{A}} \sum_{a_2 \in \mathcal{A}} \sum_{\substack{u=0, \\ b=a_1+a_2}}^{n-1} exp(2\pi iu(a_1+a_2-b)/n) \\
&\quad + \sum_{a_1 \in \mathcal{A}} \sum_{a_2 \in \mathcal{A}} \sum_{\substack{u=0, \\ b \neq a_1+a_2}}^{n-1} exp(2\pi iu(a_1+a_2-b)/n) \\
&= \sum_{a_1 \in \mathcal{A}} \sum_{a_2 \in \mathcal{A}} \sum_{u=0}^{n-1} 1 \\
&= n|\mathcal{A}|^2.
\end{aligned}$$

Let $d(u) = gcd(u, n)$ and $m(u) = \frac{n}{d(u)}$. Then one has,

$$S = \sum_{u,m(u)<240} S_1^2(u)\bar{S}_2(u) + \sum_{u,m(u)\geq 240} S_1^2(u)\bar{S}_2(u) = T_1 + T_2.$$

The trivial bound on T_1 yields

$$|T_1| \leq (240)^2|\mathcal{A}|^2|\mathcal{A}+\mathcal{A}| \leq (240)^2(2.12)10^{-9}n|\mathcal{A}|^2.$$

On the other hand,

$$\begin{aligned}
|T_2| &\leq \max_{u,m(u)\geq 240} |S_1(u)| |\sum_{u,m(u)\geq 240} S_1(u)\bar{S}_2(u)| \\
&\leq \max_{u,m(u)\geq 240} |S_1(u)| \sum_{u,m(u)\geq 240} |S_1(u)\bar{S}_2(u)| \\
&\leq \max_{u,m(u)\geq 240} |S_1(u)| \big(\sum_{u,m(u)\geq 240} |S_1(u)|^2\big)^{1/2} \big(\sum_{u,m(u)\geq 240} |\bar{S}_2(u)|^2\big)^{1/2} \\
&\leq \max_{u,m(u)\geq 240} |S_1(u)| (n|\mathcal{A})^{1/2} (n|\mathcal{A}+\mathcal{A}|)^{1/2} \\
&\leq \max_{u,m(u)\geq 240} |S_1(u)| \sqrt{2.11} n|\mathcal{A}|.
\end{aligned}$$

The third inequality follows from Holder's and the fourth one is an application of Parseval's identity. A comparison of the bounds for $|T_1|$ and $|T_2|$ with the value of S suggests existence of some u with $m(u) \geq 240$ such that $|S_1(u)| > 0.6868|\mathcal{A}|$. This establishes the claim with the help of the Freiman's theorem. We remark that the condition $m(u) \geq 240$ is of no importance to us. □

Now we fix an u and some half circle $T = [k, k+m/2)$ for which $|\phi_1^{-1}(T) \cap \mathcal{A}|$ is maximum. Let us write

$$\phi_1(\mathcal{A}) \cap T = \{\beta_1 < \ldots < \beta_s\}.$$

In case there are many choices of u then we will select the one corresponding to which the β_s is minimal.

Lemma 6.5.3. *$gcd(\beta_1, \ldots, \beta_s, m) > 1$ or $gcd(\beta_1, \ldots, \beta_s) = 1$.*

Proof. Let $gcd(\beta_1, \ldots, \beta_s) = \delta$ and $gcd(\delta, m) = 1$. Choose Δ coprime to d satisfying $\Delta\delta = 1 \pmod m$. Then for $u' = \Delta u$ considering the map ϕ_u gives us

$$\phi_u(\mathcal{A}) \cap T = \{\beta_i/\delta : 1 \leq i \leq s\},$$

which is in contradiction to the minimality of β_s. □

Next we note that, without loss of generality, we can assume that $\mathcal{A}$ is not contained in coset of a proper subgroup of $\mathbb{Z}/n\mathbb{Z}$. Because if it is, let $\mathcal{K}$ be the smallest subgroup with the property that $\mathcal{A}$ is contained in a single coset. Then $\mathcal{A}$ is $2-isomorphic$ to a subset of $\mathbb{Z}/n'\mathbb{Z}$ for $n' = |\mathcal{K}|$. Now the image $\mathcal{A}'$ of $\mathcal{A}$ is not contained in a coset of any proper subgroup of $\mathbb{Z}/n'\mathbb{Z}$ and clearly we also have $|\mathcal{A}'+\mathcal{A}'| < 2.11|\mathcal{A}'|$. It might happen that $|\mathcal{A}'| > cn'$ in which case we have that (3) of Theorem 6.2.1 holds. In case $|\mathcal{A}'| < cn'$, then what we shall prove will show that $\mathcal{A}'$ has a structure given by (1) or (2) in Theorem 6.2.1 and consequently so is the case with $\mathcal{A}$.
We shall write $\phi_1(\mathcal{A}) = B \cup D$ where $B = \{\beta_1 < \ldots < \beta_s\}$ and D has empty intersection with the half circle T. Let us assume that D is non empty. For $d \in \tilde{D}$, where $\tilde{D}$ consist of those elements of $\tilde{\mathcal{A}}$ whose first co-ordinate lies in D, we make the following;
Claim:

$$(d + \tilde{B}) \cap (\tilde{B} + \tilde{B}) \neq \varnothing.$$

Note that $|\tilde{\mathcal{A}} + \tilde{\mathcal{A}}| \geq |\tilde{B} + \tilde{B}|$, where $\tilde{\mathcal{A}} = \phi(\mathcal{A})$ and $\tilde{B} \subset \tilde{\mathcal{A}}$ such that first co-ordinate lies in B. We observe that

$$|\tilde{B} + \tilde{B}| < |\tilde{\mathcal{A}} + \tilde{\mathcal{A}}| < 2.11|\tilde{\mathcal{A}}| \leq 2.5|\tilde{B}|$$

and hence Theorem 6.2.2 can be appealed to give $|\tilde{B} + \tilde{B}| - |\tilde{B}| \geq \beta_s|\tilde{\mathcal{H}}|$. Also if the claim is not true then we have $|\tilde{\mathcal{A}} + \tilde{\mathcal{A}}| \geq |\tilde{B}| + |\tilde{B} + \tilde{B}|$. This put together gives us

$$|\tilde{\mathcal{A}} + \tilde{\mathcal{A}}| \geq |\tilde{B}| + \beta_s|\tilde{\mathcal{H}}| + |\tilde{B}| > 3|\tilde{B}| > 2.53|\tilde{\mathcal{A}}|.$$

This contradiction establishes the claim.
Now we embark on the proof of the Theorem 6.2.1. Those elements of $\tilde{\mathcal{A}}$ of the form $(j, jx + \tilde{\mathcal{H}})$ will be called good elements, where $\tilde{\mathcal{H}}$ is the subgroup of $\mathbb{Z}/d\mathbb{Z}$ obtained by the Theorem 6.2.2 for $\tilde{B}$. Clearly elements of $\tilde{B}$ and of $\tilde{B} + \tilde{B}$ are good elements. Since $(d + \tilde{B}) \cap (\tilde{B} + \tilde{B}) \neq \varnothing$, any element $d \in \tilde{D}$ is of the form $(j_1 + j_2 - j_3, (j_1 + j_2 - j_3)x + h)$, for some $h \in \tilde{\mathcal{H}}$. We find that the elements of $\tilde{D}$ are also good and hence every element of $\tilde{\mathcal{A}}$ is of the form $(j, jx + h)$, for some $h \in \tilde{\mathcal{H}}$. We shall use this to establish the following;
Claim: $\mathcal{A}$ is $2-isomorphic$ to $\tilde{\mathcal{A}}$ via ϕ.
For this we see that,

$$\begin{array}{cccccc}
(m\eta_1 + \xi_1) + (m\eta_2 + \xi_2) & = & (m\eta_3 + \xi_3) + (m\eta_4 + \xi_4) & & & in\ \mathcal{A} \\
\downarrow \phi & & \downarrow \phi & & \downarrow \phi & \\
(\xi_1, \eta_1) & & (\xi_2, \eta_2) & & (\xi_3, \eta_3) & in\ \tilde{\mathcal{A}} \\
\| & & \| & & \| & \\
(j_1, j_1x + h_1) & & (j_2, j_2x + h_2) & & (j_3, j_3x + h_3) & (j_4, j_4x + h_4)
\end{array}$$

Note that $\xi_i = j_i$ and $\eta_i = j_i x + h_i$. We want to prove that $(m\eta_1+\xi_1)+(m\eta_2+\xi_2) = (m\eta_3+\xi_3)+(m\eta_4+\xi_4)$ if and only if $(\xi_1, \eta_1)+(\xi_2, \eta_2) = (\xi_3, \eta_3)+(\xi_4, \eta_4)$. One way (the direct) follows easily, we shall prove the converse. We have $(j_1 + j_2) + mx(j_1 + j_2) + m(h_1 + h_2) = (j_3 + j_4) + mx(j_3 + j_4) + m(h_3 + h_4)$ and we shall establish $(\xi_1, \eta_1) + (\xi_2, \eta_2) = (\xi_3, \eta_3) + (\xi_4, \eta_4)$.
If

$$(j_1 + j_2) < m \text{ and } (j_3 + j_4) < m$$

or

$$(j_1 + j_2) > m \text{ and } (j_3 + j_4) > m,$$

then we immediately get $(\xi_1, \eta_1) + (\xi_2, \eta_2) = (\xi_3, \eta_3) + (\xi_4, \eta_4)$. If we have $j_1 + j_2 > m$ and $j_3 + j_4 < m$ (or $j_1 + j_2 < m$ and $j_3 + j_4 > m$), then $j_1 + j_2 = m + (j_3 + j_4)$. Now using $(j_1 + j_2) + mx(j_1 + j_2) + m(h_1 + h_2) = (j_3 + j_4) + mx(j_3 + j_4) + m(h_3 + h_4)$ we obtain $m(mx + 1) = mh$ for some $h \in \tilde{\mathcal{H}}$. Since $gcd(m, d) = 1$, so m is invertible in $\mathbb{Z}/d\mathbb{Z}$ and hence one obtains $1 + mx \in \tilde{\mathcal{H}}$. But every element of $\mathcal{A}$ is of the form $m(jx + h) + j = j(1 + mx) + mh$ for some $j \in [0, m]$ and $h \in \tilde{\mathcal{H}}$ and so $\mathcal{A} \subset \mathcal{H}$ for $\mathcal{H} \subset \mathbb{Z}/n\mathbb{Z}$ defined by

$$\mathcal{H} = \{t \in \mathbb{Z}/n\mathbb{Z} : t \pmod{d} \in \tilde{\mathcal{H}}\}.$$

But we have assumed no such $\mathcal{H}$ exists. By now the claim is established.

Appendix A

Some Facts from Algebraic Number Theory

In this appendix, we shall recall some results from the Algebraic Number Theory which are used in this thesis. Throughout this thesis, K will denote a number field of degree n, i.e. a subfield of $\mathbb{C}$ which is of dimension n over $\mathbb{Q}$ as a vector space. By $\mathbb{O}_K$ we shall denote the ring of integers of K. Tr will always stand for the trace map from K to $\mathbb{Q}$, i.e. for any $\alpha \in K$ the $Tr(\alpha)$ is the trace of the map obtained by multiplying every element of K by α. For any n elements $\omega_1', \ldots, \omega_n'$ we will define their discriminant to be the determinant of the matrix $(Tr(\omega_i'\omega_j')$ and will be denoted by $d(\omega_1', \ldots, \omega_n')$. Also one notes that if g_i denote all the $\mathbb{Q}-$embeddings of K in $\bar{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$, fixed throughout, then one has $d(\omega_1', \ldots, \omega_n') = (det\ W)^2$ for the matrix $W = (g_i(\omega_j'))$.
Let $\omega_1, \ldots, \omega_n$ be an integral basis of K, i.e. a basis of $\mathbb{O}_K$ as $\mathbb{Z}$ module. The discriminant of k is defined to be $d(\omega_1, \ldots, \omega_n)$ and is denoted by d_K. If A is the matrix satisfying $(\omega_i') = A(\omega_i)$ then one observes immediately that

$$d(\omega_1', \ldots, \omega_n') = (det\ A)^2 d_K.$$

Let M be a $\mathbb{Z}$ module inside K, then its complimentary module is defined by

$$M^* = \{\alpha \in K : Tr(\alpha M) \subset \mathbb{Z}\}.$$

The following fact is immediate to derive,

Fact A.0.4.
1. M^* is a $\mathbb{Z}$ module,
2. If $M_1 \subset M_2$, then $M_2^* \subset M_1^*$,
3. $\mathbb{O}_K \subset \mathbb{O}_K^*$.

Now let l be a prime integer and b be an integer which is l^{th} power free. We consider the case $K = \mathbb{Q}(b^{1/l})$, the field obtained by attaching the real l^{th} root to $\mathbb{Q}$. It is easy to establish that $d(1, b^{1/l}, \ldots, b^{(l-1)/l}) = l^l b^{l-1}$. We put $\delta = d(1, b^{1/l}, \ldots, b^{(l-1)/l})$, then we have the following lemma,

Lemma A.0.5. *For every $\alpha \in \mathbb{O}_K$, we have $\delta\alpha \in \mathbb{Z}[b^{1/l}]$.*

Proof. Let $\alpha \in \mathbb{O}_K$, then we have $\alpha = \sum_{i=0}^{l-1} c_i b^{i/l}$, for rational numbers c_i. Now applying $g_i's$ to this, we obtain l equations and can solve for $c_i's$, to see that the denominator of c_i is a divisor of δ. This proves the lemma. □

Thus we have $\omega_i = (\delta)^{-1} \sum_{j=0}^{l-1} a_{ij} b^{j/l}$. From this we obtain

$$d_K = (det\ A)^2 \delta,$$

where A is the matrix $(\frac{a_{ij}}{\delta})$. Since right side has odd power of δ so it follows that $\delta | d_K$. We recall that a prime q ramifies in K if and only if it divides the discriminant of K. All these we record as,

Theorem A.0.6. *If q is a prime divisor of b, then q ramifies in $\mathbb{Q}(b^{1/l})$.*

Bibliography

[1] R. Balasubramanian, F. Luca, R. Thangadurai, *On the exact degree of* $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})$ *over* $\mathbb{Q}$, *Proceedings of the American Mathematical Society, Volume 138, number 7, July 2010, pages 2283-2288.*

[2] Balasubramanian, R., Prem Prakash Pandey *Catalan Conjecture over Number Fields, in preparation.*

[3] Y.F. Bilu, *Catalan's Conjecture [after Mihăilescu], Sém. Bourbaki, 55éme, année,* n^0*, 909 (2002-2003).*

[4] Y. F. Bilu, *Catalan's Conjecture without logarithmic forms (after Bugeaud, hanrot and Mihăilescu). J. Theore. Nombres Bordeaux 17 (2005), no.1, 69-85.*

[5] B. Brindza, K. Gyory, R. Tijdeman, *On the Catalan Equation over Algebraic Number fields, J. Reine Angew. Math. 367(1986), 90-102.*

[6] Y. Bugeaud, G. hanrot, *Un nouveau critère pour l'équation de Catalan, Mathematika 47 (2000) 63-73.*

[7] Cassels, J.W.S., *On the equation* $a^x - b^y = 1$*. I. American Journal of Mathematics 75, 159-162, 1953.*

[8] Cassels, J.W.S., *On the equation* $a^x - b^y = 1$*. II. Proc. Cambridge Philos. Soc. 56 1960 97–103.*

[9] Cassels, J.W.S., A. Frohlich, *Algebraic Number Theory, Academic Press.*

[10] Ko, Chao. *On the Diophantine equation* $x^2 = y^n + 1, xy \neq 0$*, Sci. Sinica 14(1965), 457-460.*

[11] I. Chowla, *A Theorem on the addition of residue classes: Application to the number* $\Gamma(k)$ *in Waring's problem. Proc. Indian Acad. Sci., Section A, 1:242-243, 1935.*

[12] Cremona, J. E. *Elliptic Curve Data, http://www.warwick.ac.uk/ masgaj/ftp/data/.*

[13] G. Freiman, *'Inverse Problems of the additive theory of numbers. On the addition of sets of residues with respect to a prime modulus', Dokl. Akad. Nauk SSSR 141 (1961) 571-573 (Russian), Soviet Math. Dokl. 2 (1961) 1520-1522 (English).*

[14] G. Freiman, *Foundations of a structural theory of set addition, Translations of Mathematical Monographs 37 (American Mathematical Society, Providence, RI, 1973).*

[15] G. Freiman, *'Structure theory of set addition', Asterisque 258 (1999) 1-33.*

[16] Jean-Marc Deshouillers, Gregory A. Freiman, *A step beyong Kneser's theorem for abelian finite groups, Proc. London Math. Soc. (3) 86 (2003), no. 1, 1-28.*

[17] Dupuy, B., *A class number criterion for the equation* $\frac{x^p-1}{x-1} = py^q$. *Acta Arith. 127(2007), no. 4, 391-401.*

[18] L. Euler, *Theorematum quorundam arithmeticorum demonstrationes, pp. 56-58 in Commentationes Arithmeticae, Opere Omnia, Series 1, Vol. II, Teubner, 1915.*

[19] M. Fried, *Arithmetical properties of value sets of polynomials, Acta Arith., 15 (1968/69) 91-115. MR0244150 (39-5467).*

[20] Farshid, Hajir, *On The Class Numbers of Hilbert Class Fields. Olga Taussky-Todd: in memoriam. Pacific J. Math, 1997, Special Issue, 177-187.*

[21] David Hilbert, *The theory of Algebraic Number Fields, 1991, page 199-205.*

[22] K. Inkeri, *On Catalan's conjecture, J. Number Theory 34 (1990), 142-152.*

[23] Vijay Jha, *Stickelberger Ideals in the spirit of Kummer and some applications, Queen's papers in pure and applied Mathematics, Number-93.*

[24] M. Kneser, *'Abschatzung der asymptotischen Dichte von Summenmengen', Math. Z. 58(1953), 459-484.*

[25] Helmut Koch, *Number Theory-Algebraic Numbers and Functions, Graduate Studies in Mathematics, Volume 24, American Society of Mathematics.*

[26] S. Lang, *Algebraic Number Theory (Graduate Texts in Mathematics), Springer Verlag, 1994.*

[27] S. Lang, *Cyclotomic Fields I and II (Graduate Texts in Mathematics), Springer Verlag, 1990.*

[28] V. Lebesgue, *Sur l'impossibilite nombres entiers de l'equation* $x^m = y^2 + 1$*, Nouv, Ann. Math. ((1850), 178-181.*

[29] Lev, Vsevolod, *Distribution of Points on Arcs, Integers 5 (2005), no. 2, A11, 6pp.*

[30] Lev, Vsevolod, *More on Points and arcs, Combinatorial Number Theory, 347-350, de Gruyter, Berlin, 2007.*

[31] T. Metsänkylä, *Catalan's conjecture: another old Diophantine problem solved. Bull. Amer. math. Soc. (N.S.) 41(2004), no. 1,43-57.*

[32] P. Mihăilescu, *A class number free criterion for Catalan's conjecture, J. Number Theory 99 (2003), 225-231.*

[33] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's Conjecture, J. reine angew. Mathematik 572 (2004), 167-195.*

[34] P. Mihăilescu, *On the class group of cyclotomic extensions in presence of a solution to Catalan's equation, J. Number Theory 118(2006), 123-144.*

[35] M. Ram Murty and Jody Esmonde, *Problems in Algebraic Number Theory, Graduate Text in Mathematics, 1991.*

[36] M. Nathanson, *Additive Number Theory, Inverse Problems and the Geometry of Sumsets, GTM 165, Springer.*

[37] Jurgen Neukirch, *Algebraic Number Theory, Springer 1991.*

[38] P, Ribenboim, *Catalan's Conjecture, Academic Press, Boston, 1994.*

[39] C. Runge, *Ueber ganzzahlige Losungen von Gleichungen zwischen zwei veanderlichen, J. reine angew. Mathematik 100 (1887), 425-435.*

[40] J. W. Sands, *Abelian fields and the Brumer-Stark conjecture, Composition Math. 53, (1984) no. 3, 337-346.*

[41] R. Schoof, *Catalan's Conjecture, Universtext, Springer 2008.*

[42] J. Silverman, *The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer*

[43] J. Steinig . *'On Freiman's theorems concerning the sum of two finite sets of integers, 'Structure theory of set addition', Asterisque 258 (1999), 129-140.*

[44] T. Tao, Van, Vu, *Additive Combinatorics, Cambridge Studies in Mathematics 105, 2006.*

[45] F. Thaine, *On the ideal class groups of real abelian number fields, Ann. math. 128 (1988), 1-18.*

[46] R. Tijdeman, *On the equation of Catalan. Acta arith. 29 (1976), no. 2, 197-209.*

[47] L. C. Washington, *Introduction to Cyclotomic Fields, 2nd edition, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.*

[48] Steven H. Weintraub, *Galois Theory, Springer-Verlag 2006 (Universitext).*

[49] S. Wright, *Patterns of quadratic residues and nonresidues for infinitely many primes, J. Number Theory, 123 (2007), 120-132. MR2295434 (2007:11007).*