Cyclotomic Norm Diophantine Equations

Dissertation

for the award of the degree

"Doctor rerum naturalium"

of the Georg-August Universität Göttingen

within the doctoral program "Mathematical Sciences"

of the Georg-August University School of Science (GAUSS)

submitted by

Han Chen

From Fujian

Göttingen, 2023

Thesis advisory committee

Prof. Dr. Preda Mihăilescu,
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Jörg Brüdern,
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Harald Andrés Helfgott,
Mathematisches Institut, Georg-August-Universität Göttingen

Members of the examination board

Reviewer:

Prof. Dr. Preda Mihăilescu,
Mathematisches Institut, Georg-August-Universität Göttingen

Second reviewer:

Prof. Dr. Jörg Brüdern,
Mathematisches Institut, Georg-August-Universität Göttingen

Further members of the examination board

Prof. Dr. Max Wardetzky,
Institute for Numerical and Applied Mathematics, Georg-August-Universität Göttingen

Prof. Dr. Axel Munk,
Institut für Mathematische Stochastik, Georg-August-Universität Göttingen

Prof. Dr. Chenchang Zhu,
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Thomas Schick,
Mathematisches Institut, Georg-August-Universität Göttingen

Date of oral examination: 28 September 2023

Acknowledgement

First of all, I would like to express my deepest gratitude to my supervisor Preda Mihăilescu. I feel like a Klein bottle in a three-dimensional world, and every time I meet with my supervisor, he always tries to pull me into the four-dimensional space. I thank him for all the endless help he has given me, both in my studies and in my life, also for bearing my disappearance from time to time.

I also want to thank Huilin Zhu, Chang Liu for many interesting discussions during the studies. In particular, I want to thank Haojie Hong for introducing the Diophantine equation $x^2+C = y^p$ to me and the helpful discussion with him.

In addition, special thanks to my family for their unfailing love and unwavering support.

Finally, I would like to acknowledge the financial support by the China Scholarship Council.

Contents

Chapter 1

Introduction

Can a number with n 1's as its digits be an integer power? That is, we consider the following Diophantine equation:

$$\underbrace{11\cdots1}_{n \text{ 1's}} = y^q \quad \text{with} \quad y \in \mathbb{Z}, q \geq 2. \tag{1.1}$$

What if left-hand side is not decimal-based but x-based with $|x| > 1$? In this case we look at the following Diophantine equation

$$\frac{x^n - 1}{x - 1} = y^q \quad \text{with} \quad |x|, |y|, q > 1, n > 2. \tag{1.2}$$

Along with the well-known Fermat's Last Theorem and Catalan's Conjecture, the Nagell-Ljunggren equation (1.2) itself is a classical problem of Diophantine equation. This equation is interesting in itself, and it is also linked to other problems.

Here we give a brief survey on the main contributions towards the Nagell-Ljunggren equation (1.2).

1.1 History notes on the Nagell-Ljunggren equation

We must remind the reader that some mathematicians are only concerned with the *positive* solutions of equation (1.2). That is why we have the exceptions about the negative solutions in our main result (8) in this thesis.

It is easy to see that Diophantine equation (1.2) has the following six solutions

$$(x, y, n, q) \in \mathcal{S} := \{(3, \pm 11, 5, 2), (7, \pm 20, 4, 2), (18, 7, 3, 3), (-19, 7, 3, 3)\} \tag{1.3}$$

These solutions carry the exponents $q = 2$ or $q = 3$.

The story about Diophantine equation (1.2) began when Nagell and Ljunggren first made a contribution to this problem in 1920s and later twenty years.

Theorem 1 (Nagell, Ljunggren 1920, 1921, 1943)**.** *There is no solution outside* $\mathcal{S}$ *if any of the following conditions satisfied:*

1. $q = 2$
2. $3 \mid n$
3. $4 \mid n$
4. $q = 3$ *and* $n \not\equiv 5 (\mathrm{mod} 6)$

Proof. Nag20 Nag21 Lju43 □

Encouraged by Nagell and Ljunggren's results we can formulate a conjecture about all solutions of the Diophantine equations (1.2). The following conjecture states that all solutions in integers with exponents larger than one lie in $\mathcal{S}$.

Conjecture 1. *There is no solution outside* $\mathcal{S}$ *to the equation of (1.2).*

It is widely believed that Conjecture (8.3) is right. In the following we present some results on particular cases regarding Conjecture (8.3).

1.2 The prime case and the connection with Catalan's conjecture

Since the case $4 \mid n$ is solved by Nagell in 1921 Nag21, there is no loss of generality in assuming that $4 \nmid n$. In fact, the general case of equation (1.2) can be reduced to the prime case.

Lemma 1. *If* $n > 3$ *is an integer not divisible by 4,* q *an odd prime. If* l *is an odd prime dividing* n, $n = 2^c l^a d$, $l \nmid d$, *then there exist non-zero integers* $h \geq 1$ *and* $t_0, t_1, \cdots, t_a$ *such that*

$$\frac{(x^{h^i})^l - 1}{(x^{h^{i-1}})^l - 1} = t_i^q \quad \text{for } 0 \leq i \leq a; \tag{1.4}$$

or

$$\frac{x^h - 1}{x - 1} = t_0^q \quad \text{and} \quad \frac{(x^{h^i})^l - 1}{(x^{h^{i-1}})^l - 1} = l t_i^q \quad \text{for } 1 \leq i \leq a. \tag{1.5}$$

Proof. Rib94 □

Therefore Conjecture (8.3) can be reduced to the following set of statements, relative to pairs of odd primed (p, q) with $p > 3, q \geq 3$: the equations

$$\frac{x^p - 1}{x - 1} = p^e y^q; \quad e = \begin{cases} 1 & \text{if } x \equiv 1 \bmod p \text{ and} \\ 0 & \text{otherise,} \end{cases} \tag{1.6}$$

have no solution outside $\mathcal{S}$.

We call the equation (1.6) the prime case of Nagell-Ljunggren equation. The Diophantine equation (1.6) has a strong connection to the famous problem of Catalan. We will see soon below by Cassels' relations that solutions of equation (1.6) would imply the famous conjecture of Catalan.

1.3 Catalan's Conjecture

Because of the close connection between the Nagell-Ljunggren equation and the Catalan's equation, we following the first chapter of [BBM14], briefly review below the history of the Catalan's conjecture, which has a high value in our investigation to the Nagell-Ljunggren equation. For more historic information concerning Catalan's problem one may consult the books of Ribenboim [Rib94] and Schoof [Sch10].

Recall that the Catalan's equation is of the form

$$x^p - y^q = 1, \tag{1.7}$$

where $x, y, p, q \in \mathbb{Z}$ with $xy \neq 0$ and $p, q \geq 2$. In 1842 the Belgian mathematician Catalan asked whether 8 and 9 are the only consecutive pure powers of non-zero integers.

Particular cases

The investigation of equation (1.7) reduced to the cases when $p, q \geq 3$, p, q two odd prime numbers due to the following three results:

1. Euler [EDA12] showed in 1738 that the equation $x^2 - y^3 = 1$ has no nontrivial solution other than $3^2 - 2^3 = 1$;

2. In 1850 Victor A Lebesgue [Leb50] proved that the equation $x^m - y^2 = 1$ has no solution;

3. In 1965 Ko Chao [Ko65] deduced that the equation $x^2 - y^n = 1$ has no solution with $n \geq 5$.

For more particular cases, Genoro [Ger57] showed in 1857 that (1.7) has no further solutions if x, y are prime numbers, Hampel [Ham56] deduced in 1956 that there are no further solutions for (1.7) if $|x - y| = 1$.

1.3.1 Cassels' relations

The modern approach to Catalan's problem began in 1960s by Cassels, who factored the equation (1.7) as

$$(x-1) \cdot \frac{x^p - 1}{x - 1} = y^q.$$

Put $z := x - 1$, then

$$\frac{x^p - 1}{x - 1} = z^{p-1} + \sum_{2 \le i \le p-1} \binom{p}{i} z^{i-1} + p, \tag{1.8}$$

so

$$\gcd(\frac{x^p - 1}{x - 1}, x - 1) = \gcd(p, z) \mid p,$$

that is, the greatest common divisor of $\frac{x^p-1}{x-1}$ and $x - 1$ is 1 or p.

Cassels [Cas60] proved that the former case is impossible, so $\gcd(\frac{x^p-1}{x-1}, x - 1) = p$, in which case we have

$$p^2 \nmid \frac{x^p - 1}{x - 1}$$

because of the identity of (1.8). Thus

$$\frac{x^p - 1}{x - 1} = pa^q, \quad x - 1 = p^{q-1}b^q \quad y = pab \tag{1.9}$$

with some $x, y, a, b \in \mathbb{Z}$. Relations (1.9) are called *Cassel's relations*, which are considered as the beginning of modern approach to Catalan's conjecture. It follows that $p \mid y$ provided (x, y, p, q) is a solution of (1.7). By symmetry we see that $(-y, -x, q, p)$ is also a solution, hence $q \mid x$ also holds.

Linear forms in logarithms

To prove Catalan's conjecture, one approach is to bound the exponents in Catalan's equation. Evertse [Eve83] showed that the number of solutions is bounded by $mn^{\min(m,n)}$. This bound does not involve x and y, Baker's Fields Medal result on linear forms in logarithms, in 1964, which was improved in 1973 by explicit lower bounds for non vanishing linear forms, can derive effective bounds for the solutions of some Diophantine equations, in particular, of Catalan's problem. Tijdeman [Tij76] proved the remarkable result that Catalan's equation has only finitely many positive solutions. Shortly after Tijdeman's result, Lavegin used Baker's effective bounds to gain explicit, albeit large, upper bounds on the solutions. Of course, this imply also upper bounds on the exponents. Indeed Lagevin proved

$$|x^m|, |y^n| \le \exp\exp\exp\exp(730),$$

he also showed in the same paper that the greatest prime divisor of mn is less than $\exp(241)$, which is saying $\max\{p, q\} \le \exp(241)$ in the prime exponent case.

This extremely large bounds $\exp(241)$ has been the subject of continuously work of improvement using special additional results on linear forms in logarithms of rational numbers. They work on the special case of two rational numbers and led to successive improvements of the upper bounds. For example, Glass et al. [GMOS94] showed that $\min\{p, q\} < 5.6 \times 5^{19}$ and

$\max\{p,q\} < 3.42 \times 5^{28}$ in 1992. Independently in the same year, Mignotte [Mig92] improved on estimates for logarithmic forms, he replaced the Lagevin's bound and showed that $\max\{p,q\} < 1.31 \times 10^{18}$.

Another approach is to derive lower bounds for p, q, using algebraic criterion, see below. Glass et al. [GMOS94] in 1994 showed that $\min\{p,q\} \geq 17$. A series of papers of Mignotte and Roy [MR95] [MR97a] [MR97b] using heavy computations deduced that

$$\min\{p,q\} \geq 10^5.$$

1.3.2 Cyclotomic fields

Looking at the Catalan's conjecture from an algebraic point of view, we can also obtain some conditions for non-trivial solutions, linear forms in logarithms provided upper bounds on the exponents, while algebraic approaches provided complementary bounds and conditions.

We now consider the algebraic track, the algebraic conditions for Catalan, this track was start by Inkeri, who proved the following two criteria:

Lemma 2 (Inkeri 1964)**.** *If $p \equiv 3(\mathrm{mod}4)$, Catalan's equation has no solution when the following two relations hold*

$$p^{q-1} \not\equiv 1(\mathrm{mod}q^2) \quad \textit{and} \quad q \nmid h(-p),$$

where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Proof. [Ink64] □

Lemma 3 (Inkeri 1990)**.** *Catalan's equation has no solution when we both have*

$$p^{q-1} \not\equiv 1(\mathrm{mod}q^2) \quad \textit{and} \quad q \nmid h_p,$$

where h_p is the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$.

Proof. [Ink90] □

Note that this is a conjunction of two types of conditions, condition one is the so-called *double Wieferich condition*, the second condition is a certain *class number condition*. Inkeri showed two things for the class number condition, one is a small condition for quadratic imaginary fields and it holds for $p \equiv 3(\mathrm{\ mod\ }4)$. The other one is a non-divisibility condition set for large fields which always holds. Mignotte [MR95] improved the special case $p \equiv 3(\mathrm{mod}4)$ of Inkeri and showed it holds for arbitrary p. He replaced the imaginary quadratic extension with the smallest imaginary subextension in $\mathbb{Q}(\zeta_p)$. Then Schwarz proved in 1995 [Sch95] a similar result by replacing the field of Mignotte with an arbitrary field. This is not an improvement of Mignotte but is useful, since the relative class number h_p^- is much more easy to compute than the full class number h_p.

Bugeaud and Hanrot made a breakthrough by separating the conditions in [BH00], they proved that a solution (x, y, p, q) of Catalan's equation satisfies

either $q \leq p$ or $q \mid h_p^-$. So they removed the Wieferich condition, but with a size relation between p and q. Shortly after, Mihăilescu [Mih03] came, he used stronger class field methods, invoking the Stickelberger ideal. He showed that the *double Wieferich condition*: $p^{q-1} \equiv 1 \bmod q^2$ and $q^{p-1} \equiv 1 \bmod p^2$ must hold unconditionally between p and q. This result is very strong, in fact, there are only 7 double Wieferich pairs with $\min\{p, q\} \leq 3.2 \times 10^8$. While both papers appeared later, the result of Bugeaud and Hanrot was made public in spring 1999 and the one of Mihăilescu followed in fall the same year. Based on these results, Mignotte and Roy managed to show the following result by intensive computer computations:

$$\min\{p, q\} \geq 10^7.$$

Both upper and lower bounds on p, q were improved by various authors. By 2001, it was deduced that $10^7 \leq \min\{p, q\} \leq 7.2 \times 10^{11}$ and $\max\{p, q\} \leq 7.8 \times 10^{16}$ [Mig01]; later on, Grantham and Wheeler using heavy computations showed that $\min\{p, q\} \geq 3.2 \times 10^8$. The gap between the upper and lower worlds remains unbridgeable on a computer.

Mihăilescu [Mih04] in 2002 introduced the so-called Runge method – in conjunction with approximation by class field theory and an application of Thaine's result [Tha88]. He showed that if (x, y, p, q) is a solution of Catalan's equation, then $p \equiv 1 \bmod q$ or $q \equiv 1 \bmod p$. In combination with certain estimates from the theory of linear forms in logarithms and a computer calculation, it led to a complete proof of Catalan conjecture in 2002. In a result communicated in 2003 and published in 2006, Mihăilescu [Mih06] used the theory of cyclomic fields and was able to avoid the linear forms in logarithms to prove the conjecture of Catalan.

1.4 On the finiteness of the number of solutions of Nagell-Ljunggren equation

From now on we return to Nagell-Ljunggren equation, but keep in mind the path of history to solve the problem of Catalan.

Some partial conclusions can be drawn by assuming conditions on the indeterminants in the Catalan's equation. In 1986 Shorey and Tijdeman [Tij86] obtained the finiteness of the solutions with conditions imposed on the variables x, y, or m.

Theorem 2 (Shorey, Tijdeman 1986)**.** *The Diophantine equation (1.2) has only finitely many positive solutions if any of the following condition holds:*

1. *x is fixed*
2. *m has a fixed prime factor*
3. *y has a fixed prime factor*

Proof. [ST86] □

Unlike Catalan's conjecture, it is worth mentioning that the equation (1.2) whether has only finitely many solutions (x, y, n, q) is still an open problem. In 1999 Shorey [Sho00] showed that the generalized ABC conjecture implies the finiteness of the positive solutions to the equation (1.2). In 1980, Masser and Oesterlé formulated the following conjecture.

Conjecture 2 (ABC conjecture)**.** *Suppose we have three mutually coprime integers A, B, C satisfying $A + B = C$. Given any $\epsilon > 0$, it is conjectured that there is a constant $k(\epsilon)$ such that*

$$\max\{|A|, |B|, |C|\} \leq k(\epsilon) \left(\mathrm{rad}(ABC)\right)^{1+\epsilon},$$

where rad(n) denotes the he product of the distinct prime factors of the rational integer n. For exmaple, if $n = \prod_{1\leq i\leq m} p_i^{k_i}$, then $\mathrm{rad}(n) = \prod_{1\leq i\leq m} p_i$.

Following we refine this conclusion of Shorey under the condition of ABC conjecture (2).

Lemma 4. *Assume that ABC conjecture holds, then equation (1.2) has only finitely many positive integer solutions.*

Proof. In view of Theorem (1) we may assume that $q \geq 3$ and $n \geq 5$.

Write equation (1.2) as $1 + (x-1)y^q = x^n$, obviously $1, (x-1)y^q, x^n$ are three mutually coprime integers, hence the condition of ABC conjecture holds. Therefore for any $\epsilon > 0$, there is a constant $k(\epsilon) > 0$ such that

$$\max\{1, |(x-1)y^q|, |x^n|\} \leq k(\epsilon) \cdot \mathrm{rad}((x-1)xy)^{1+\epsilon}. \tag{1.10}$$

- If $|(x-1)y^q| \leq |x^n|$, so $|y|^q \leq 2|x|^{n-1}$. Then by (1.10) we have

  $$|x^n| \leq k(\epsilon)\mathrm{rad}\left((x-1)xy\right)^{1+\epsilon} < k(\epsilon)|x^2y|^{1+\epsilon} \leq k(\epsilon)2^{\frac{1+\epsilon}{3}}|x^2 \cdot x^{\frac{n-1}{3}}|^{1+\epsilon},$$

  where $k(\epsilon) > 0$ is a constant depending only on ϵ. Put $\epsilon = \frac{1}{10}$, we see that there are only finitely many possibilities for x, we obtain the desire result because of Theorem (2).

- If $|(x-1)y^q| \geq |x^n|$, so $|x|^{n-1} \leq y^q$. Then by (1.10) we have

  $$|(x-1)y^q| \leq k(\epsilon)|(x-1)xy|^{1+\epsilon},$$

  where $k(\epsilon) > 0$ is a constant depending only on ϵ. We consider the inequality in terms of y^q as follows:

  $$|y|^{q-1-\epsilon} \leq k(\epsilon)x^{1+2\epsilon} \leq k(\epsilon)|y|^{\frac{q(1+2\epsilon)}{4}}$$

  Put $\epsilon = \frac{1}{10}$, we see that there are only finitely many possibilities for $|y|^q$, hence also for $|x|$ since $|x| \leq |x|^n \leq |y|^q$. We finish the proof in this case also because of Theorem (2).

Combining the above two cases together we obtain the lemma. □

1.5 Bounding exponents by linear forms in logarithms

Similar to the Catalan's equation, certain lower bounds on the exponents in the Nagell-Ljunggren equation can be obtained by means of linear forms in logarithms. In 2002, Bugeaud, Hanrot and Mignotte proved the following result:

Lemma 5 (Bugeaud, Hanrot and Mignotte 2002). *If $p \not\equiv 1(\mathrm{mod}8)$ and $q > 64000p(\log p)^2$, then equation (1.2) has no positive solution.*

Proof. [BHM02] □

Later, Han Di and Guan Wenji in 2014 gave a substantial improvement of the constant for $p \equiv 3(\mathrm{mod}\,4)$. More precisely, they proved the following result:

Lemma 6 (Han, Guan 2014). *If $p \equiv 3(\mathrm{mod}4)$ and $q > 220p(\log p)^2$, then equation (1.2) has no positive solutions.*

Proof. [DW14] □

1.5.1 The exclusion of special form of x

Current mathematical techniques are in sufficient for completely solving Conjecture 8.3, but some advance can be obatined in the case where x has some special form. Inkeri excludes the case where x is a certain cubic number.

Lemma 7 (Inkeri 1972). *If $q = 3$, Diophantine equation (1.2) has no solution if x is a cube or $x = z^3 + 1$ with $|z| > 1$.*

Proof. [Ink72] □

This last conclusion about cubes was generalized by Bugeaud and Mignotte as follows

Theorem 3 (Bugeaud, Mignotte 1999). *Diophantine equation (1.2) has no solution if x is a q^{th} power.*

Proof. [BM99] □

1.6 The lower and upper bound for the variables

As in the case of other Diophantine equations, we also study the upper and lower bounds on a variable in the possible solutions of the equation (1.2). We gather the following results about the estimates of the variables in positive solutions.

Bugeaud, Mignotte and Roy deduced an elementary lower bound for y in terms of n and for x in terms of q, which has not been improved.

Lemma 8 (Bugeaud, Mignotte and Roy 2000). *If Diophantine equation (1.2) has a positive solution (x, y, n, q) outside $\mathcal{S}$. Then $y > 2n$, $x > 2q + 1$.*

Proof. [BMR00] □

Also, Bugeaud, Hanrot and Mignotte obtained a lower bound for odd prime divisors of n, with the exception of diagonal case.

Lemma 9 (Bugeaud, Hanrot and Mignotte 2002)**.** *If Diophantine equation (1.2) has a positive solution (x, y, n, q) outside $\mathcal{S}$. Then the least odd prime divisor of n is at least 29 or $(p, q) \in \{(17, 17), (19, 19), (23, 23)\}$.*

Proof. [BHM02] □

Mihăilescu showed an upper bound for x in terms of p and q.

Theorem 4 (Mihăilescu 2007)**.** *If the Diophantine equation (1.6) has a positive solution (x, y, n, q) outside $\mathcal{S}$, with p, q odd prime numbers. Then we have*

1. $x < q^{10p^2}$, *if* $q \leq p$,

2. $x < 2q^{10p^2(p-1)}$, *if* $q \geq p + 2$.

Furthermore, if $p = q$, then $x \leq (2p)^p$.

Proof. [Mih07] □

1.7 The number of prime divisors of n

One approach to attack (1.2) is to decrease upper bounds in the number of factors of the exponent n in (1.2). Related results in this direction are due to Bugeaud and Mihăilescu in 2007.

Lemma 10. *Let (x, y, n, q) be a positive solution of (1.2) not in S. Then, the least prime divisor of n is at least equal to 29 and $\Omega(n) \leq 4$.*

Proof. [BM07] □

Here we denote by $\omega(n)$ and $\Omega(n)$ by the number of distinct prime factors of n and the total number of prime divisors of n, respectively. This result was improved by Bennett and Levin in 2015 via Runge's method (without assuming positive solutions):

Theorem 5 (Bennett, Levin 2015)**.** *Let (x, y, n, q) be a solution of (1.2). Then $1 \leq \omega(n) \leq \Omega(n) \leq 3$.*

Proof. [BL15] □

1.8 Recent results about the Diophantine equation (1.6)

Dupuy treated in 2007 the case of solutions $x \equiv 1 \bmod p$ of equation (1.6) – thus $e = 1$ – elegantly, under the additional assumption $q \nmid h_p^-$, in [Dup07], proving

Theorem 6 (Dupuy 2007)**.** *If $q \nmid h_p^-$, then (1.6) has no solutions with $e = 1$ – or, equivalently, with $x \equiv 1 \bmod p$.*

In 2007, Mihăilescu studied the diagonal case $p = q$ of equation (1.6), which case is considered to be the most difficult case. He gave general class number conditions which are the first known general algebraic necessary conditions for the equation to have solutions. Among others, these lead, based on computer results produced for the investigation of the Fermat Equation, to the conclusion that the equation has no solution for $p < 12\ 000\ 000$. In another paper [Mih07], he considered the case $q \neq p$ and proved the unconditional criterion

Theorem 7 (Mihăilescu 2007)**.** *For $q \neq p$, two distinct odd primes, the equation (1.6) has no solution if $q > (p-1)^2$.*

In this paper [Mih07] Mihăilescu derived a new bound $q > f(p)$ for which there is no solution. For small q the problem is harder and we achieve a conditional result where $q \nmid h_p^-$ for $q < g(p)$ and some additional condition on (p, q) must hold.

This thesis improves on earlier results of Mihăilescu and the aim is to eliminate the case when $q \nmid h_p^-$. This purpose is almost achieved by the result of this thesis.

1.9 The generalized Ramanujan-Nagell equation and its recent results

Another Diophantine equation related to the Catalan equation is to replace the constant 1 with any positive integer C:

$$x^2 + C = y^n, \tag{1.11}$$

where $C > 0$ is a given integer and x, y, n are positive integer unknowns with $\gcd(x, y) = 1$ and $n \geq 3$. We call this equation as *the generalized Ramanujan-Nagell equation.*

The first result concerning the equation (1.11) dates back to Fermat and Euler, they claimed that $(x, y) = (5, 3)$ is the only solution of (1.11) when $(C, n) = (2, 3)$. In 1850 V. A. Lebesgue [Leb50] proved that the above equation has no solutions for $C = 1$.

In 1993, Cohn [Coh93] solved the equation (1.11) for 77 values of C in the range $1 \leq C \leq 100$. The remaining values of C in this range were taken care of in [BMS06] by Bugeaud, Mignotte and Siksek, and in [MdW96] by Mignotte and de Weger.

In the recent years, several authors became interested in the case when $C = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where the p_i are distinct primes and $k \geq 1, a_i \geq 0$ are integers.

The solutions of (1.11) for C is a prime power is completely solved by the combined work of several authors, see [AM02, BP08, BP12, Coh92, HS16, Le02].

When $k = 2$, the solutions of (1.11) for $C = 2^a p^b, p \in \{3, 5, 11, 13, 19\}$ has been investigated in [L$^+$02, LT08, CDST10, LT09]; the cases $C = 5^a p^b, p \in \{11, 13, 17\}$ has been studied in [CDST10, LT08, PR11].

When $k = 3$, the solutions of (1.11) for $C = 2^a 3^b p^c, p \in \{11, 13, 17\}, C = 2^a 13^b p^c, p \in \{5, 17\}$, $C = 2^a 11^b 19^c$ and $C = 2^a 73^b p^c, p \in \{41, 89\}$ have been studied in [CDI$^+$13, GMT16, Gha19, CHS21, Ray22].

1.10 The plan and results of this thesis

This thesis can be seen as a generalization of the above results about the Nagell-Ljunggren equation (1.2) and the generalized Ramanujan-Nagell equation (1.11).

1.10.1 The plan and results about the Nagell-Ljunggren equation:

In Chapter 2-6 we study the case $e = 0$ of (1.6), under the premise that $q \nmid h_p^-$ and $q \neq p$.

In Chapter 2 we introduce the necessary background about the Nagell-Ljunggren equation.

For primes $n \in \mathbb{N}$, we define the following two functions of n:

$$\begin{aligned} M(n) &= \max\left(n, \frac{n(n-12)}{16}\right); \qquad (1.12) \\ M'(n) &= C(n) n \log(n); \quad C(n) = \left(\frac{\log(4)}{1 + \frac{1+\log\log(n)}{\log(n)}} - \frac{4\log(n)}{n-2}\right)^{-1}. \end{aligned}$$

The local approach is based on the following technically involved result on Fermat quotients. Let $t \equiv -y/x \bmod q^2$; a system of equations modulo p in the unknown t is obtained from the property of Fermat quotients. Analysing some of the coefficients of these equations and classifying the magnitude of p, q, in Chapter 3 we will arrive at an important conclusion: there are only three possibilities for t, namely, $t \in \{0, \pm 1\}$.

Proposition 1. *Suppose that (1.6) has non trivial solutions with primes $p \neq q$, $q \nmid h_p^-$. Then $q \in \left[M(p), (p-1)^2\right) \cap \mathbb{N}$ or $q^2 \mid x - t; t \in \{0; \pm 1\}$.*

When $q < M(p), t = 0$, we will consider some special unit and calculate the norm of its q-adic expansion, the condition that this norm equals to ± 1 will be

equivalent to the condition of some trace equation, and in this case considering modulo some higher powers of q would get a contradiction, so in Chapter 4 the following conclusion is obtained:

Proposition 2. *Suppose that (1.6) has non trivial solutions with primes $p \neq q$, $q \nmid h_p^-$ and $q < M(p)$. Then $x \equiv \pm 1 \bmod q^2$.*

Unfortunately, the above approach for $t = 0$ cannot extend to the case $t = \pm 1$, instead the local approximation of the local power series expansions would help, to this end, we use a global bounding approach based on binomial series expansions. For each element $\Theta \in \mathbb{Z}_{\geq 0}[G]$, there exists an associated linear system of equations over $\mathbb{F}_p$, we expect an non-trivial solution with coefficients of the group ring as small as possible, then deduce in Chapter 5 the following result:

Proposition 3. *Suppose that (1.6) has non trivial solutions with primes $p \neq q$, $q \nmid h_p^-$. Then $q < M'(p)$.*

Finally in Chapter 6, we use the condition in Proposition 2 for local developments of the putative solutions, in order to obtain a contradiction to the upper bounds on $|y|$ established in [Mih07]. We thus prove

Proposition 4. *The equation (1.6) has no solution with $q \nmid h_p^-$ if $q < M(p)$.*

and then conclude with the proof of the following main theorem of this thesis, by comparing the results of the last two propositions. The exceptions here is because the result of the lower bound of p we cite is proved under the condition that x is positive.

Theorem 8. *The equation (1.6) has no integers solutions outside $\mathcal{S}$, if $q \nmid h_p^-$ – except possibly for some solutions with $p < 29$ and $x < 0$.*

We do not deal here the case when p is small. Perhaps someone can start in this area later and exclude these cases to get a more complete result.

1.10.2 The plan and results about the generalized Ramanujan-Nagell equation:

In Chapter 7–8 we concern the generalized Ramanujan-Nagell equation (1.11). As we show before, the previous papers considering the equation (1.11) in the case where C is a product of no more than three prime numbers. Below we allow very general positive C in (1.11), at the cost of a small condition, that p does not divide the class number of a certain quadratic extension. The main method we use is the theory of Primitive Divisor Theorem for Lucas sequences, the background of which will be introduced in Chapter 7. Finally in Chapter 8 we will use this method to show our main result about the Diophantine equation (1.11):

Theorem 9. *Let $C \in \mathbb{Z}^+$ and write it in the form of $C = z^2 d$ with d square-free and z positive. Let K be the field $\mathbb{Q}(\sqrt{-d})$ and h_K be the class number of K. Assume $p \geq 5$ is a prime such that $p \nmid h_K$ and for all prime divisors q of z, $p \nmid q \pm 1$. If $d \not\equiv -1 \pmod 8$, then the Diophantine equation*

$$x^2 + C = y^p \tag{1.13}$$

has no positive solution with $\gcd(x, y) = 1$ except that

$$(x, y, C, p) \in \Big\{(401, 11, 250, 5), (22434, 55, 19, 5), (2759646, 377, 341, 5)\Big\}.$$

As an application of Theorem 9, we will prove the following theorem:

Theorem 10. *Let $C = 2^a \cdot 17^b \cdot 41^c$ with $a, b, c \geq 0$. Then the solution of Diophantine equation*

$$x^2 + C = y^p, \quad x, y \geq 1, \quad \gcd(x, y) = 1 \tag{1.14}$$

is given by

$$(x, y, C, p) = (38, 5, 1681, 5) \quad \text{or} \quad p = 7.$$

Chapter 2

Notations and general facts about the Nagell-Ljunggren equation

We assume throughout this paper that $(x, y; p, q) \notin \mathcal{S}$; $q \neq p$ is an unknown solution to (1.6), and $q \nmid h_p^-$. In view of Dupuy's result (6), we know that $e = 0$ and in view of Theorem 7, $q < (p-1)^2$. We let $\mathbb{K} = \mathbb{Q}[\zeta]$ be the $p-$th cyclotomic extension, with ζ a $p-$th primitive root of unity. We shall at places use also a primitive $q-$th root of unity ξ and let $\mathbb{K}' = \mathbb{Q}[\xi], \mathbb{L} = \mathbb{Q}[\zeta, \xi]$.

We let $\Phi_r(x)$ be the $r-$th cyclotomic polynomial and define $P = \{1, 2, \ldots, p-1\}$ and $\sigma_c \in G = \text{ Gal } (\mathbb{Q}(\zeta)/\mathbb{Q})$ be the automorphism of $\mathbb{K}$ with $\zeta \longrightarrow \zeta^c$, for $c \in P$. Complex conjugation is denoted by $\jmath_p \in G$, or simply by $\jmath$ when the group is clear from the context; we may thus write $\overline{\alpha} = \sigma_{p-1}(\alpha) = \jmath_p(\alpha) = \alpha^\jmath$. We let $\lambda = (1-\zeta)$ be an algebraic integer generating the unique ramified prime ideal $\wp$ above p in $\mathbb{K}$.

Cyclotomic Properties of the Equation

Recall that $x \not\equiv 1 \bmod p$ and $e = 0$. We define herewith the *characteristic number* of the equation (1.6) by

$$\alpha = x - \zeta, \quad \text{ and } \alpha_c = \sigma_c(\alpha).$$

The *characteristic ideal* is $\mathfrak{A} = (\alpha, y)$ and one verifies directly that $(\sigma_a(\alpha), \sigma_b(\alpha)) = 1$ for $a, b \in P$, two distinct integers. Indeed, $D(a,b) = (\sigma_a(\alpha), \sigma_b(\alpha))$ contains $\zeta^a - \zeta^b = \sigma_b(\alpha) - \sigma_a(\alpha)$, and thus $D(a,b) | \wp$. However, $x \not\equiv 1 \bmod p$ implies that $\alpha \notin \wp$, so $D(a,b) = 1$. As a consequence, we have

$$\mathfrak{A}^q = (\alpha), \quad \mathbf{N}(\alpha) = y^q; \quad \mathbf{N}(\mathfrak{A}) = (y). \tag{2.1}$$

We proved:

Lemma 11. *Assume that (1.6) has a non trivial solution $(x, y; p, q)$ with $x \not\equiv 1 \bmod p$ and let $\sigma_c(\alpha) = x - \zeta^c$. Then the ideal $\mathfrak{A} = (\alpha, y)$ verifies $\mathfrak{A}^q = (\alpha)$. Moreover $c \neq d \in P$, we have*

$$(\sigma_c(\alpha), \sigma_d(\alpha)) = 1, \quad (\sigma_c(\mathfrak{A}), \sigma_d(\mathfrak{A})) = 1, \quad \mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{A}) = (y).$$

Class number condition

We assumed $q \nmid h_p^-$; then the image of the class $[\mathfrak{A}]$ in the quotient $(\mathcal{C}(\mathbb{K})/\iota(\mathcal{C}(\mathbb{K}^+)))$ is trivial. Since the conjugates of $\mathfrak{A}$ are pairwise coprime, it follows that $\mathfrak{A}$ is divisible by no real prime. It must consequently be a principal ideal, say $\mathfrak{A} = (\rho)$. It follows that $(\alpha) = (\rho^q)$ and by transforming the identity of ideals into one of algebraic numbers, we find:

Lemma 12. *Under the premises above, there is a $\rho \in \mathbb{Z}[\zeta]$ and a unit $\varepsilon \in (\mathcal{O}(\mathbb{K}^+))^\times$ such that*

$$\alpha = \varepsilon \cdot \rho^q. \tag{2.2}$$

Chapter 3

A general result on Fermat quotients

In this chapter we prove a general result on the Fermat quotients of certain binary fractions:

Theorem 11. *Let $p, q, \mathbb{K}$ be like above, and suppose that $x, y \in \mathbb{Z}$ are such that there exists a $\beta \in \mathbb{K}$ such that*

$$\frac{x+\zeta y}{x+\bar{\zeta} y} = \left(\frac{\beta}{\bar{\beta}}\right)^q.$$

If in addition $q < M(p)$ with the function defined in (1.12), then there is an $f \in \{-1, 0, 1\}$ such that

$$x + fy \equiv 0 \bmod q^2.$$

The proof of this theorem requires the rest of this chapter.

Lemma 13. *Let p, q be odd primes and let x and y be coprime integers with $q \nmid x, y$ and such that there is a $\beta \in \mathbb{Q}(\zeta)$ with*

$$\frac{x+\zeta^q \cdot y}{x+\overline{\zeta}^q \cdot y} = \pm \left(\frac{\beta}{\overline{\beta}}\right)^q. \tag{3.1}$$

Then

$$-(\zeta^q - \overline{\zeta}^q)\varphi(t) \equiv \sum_{k=1}^{q-1} \frac{t^k - t^{2-k}}{k} \cdot (\zeta^k - \overline{\zeta}^k) \bmod q, \tag{3.2}$$

where $\varphi(a) \equiv \frac{a^q - a}{q} \bmod q$ for $a \in \mathbb{Z}/(q^2\mathbb{Z})$ is the Fermat quotient function and $t :\equiv -y/x \bmod q^2$.

Proof. We have

$$\frac{x+\zeta^q \cdot y}{x+\overline{\zeta}^q \cdot y} \equiv \left(\frac{x+\zeta \cdot y}{x+\overline{\zeta} \cdot y}\right)^q \bmod q\mathbb{Z}[\zeta],$$

and thus, from (3.1):

$$\pm\frac{\beta}{\overline{\beta}} = \frac{x+\zeta\cdot y}{x+\overline{\zeta}\cdot y} + q\cdot\mu,$$

with $\mu\in\mathbb{Q}(\zeta)$ being a q-integer. By raising to the power q, it follows again from (3.1), that

$$\frac{x+\zeta^q\cdot y}{x+\overline{\zeta}^q\cdot y} \equiv \pm\left(\frac{x+\zeta\cdot y}{x+\overline{\zeta}\cdot y}\right)^q \bmod q^2\mathbb{Z}[\zeta]. \tag{3.3}$$

Note that $\varphi(a)\equiv\frac{a^q-a}{q} \bmod q$, for $(a,q)=1$ and $t\equiv -y/x \bmod q^2$, so $-(y/x)^q\equiv t+q\varphi(t) \mod q^2$. Now

$$\begin{aligned}(x+\zeta\cdot y)^q &\equiv x^q\cdot(1-t\cdot\zeta)^q \equiv (x+q\varphi(x))\cdot(1-t\zeta)^q\\ &\equiv (x+q\varphi(x))\cdot(1-t\zeta^q+qf(\zeta)) \bmod q^2\end{aligned}$$

where

$$f(\zeta) = -\zeta^q\cdot\varphi(t)+\frac{1}{q}\cdot\sum_{k=1}^{q-1}\binom{q}{k}(-t\zeta)^k \equiv -\left(\zeta^q\cdot\varphi(t)+\sum_{k=1}^{q-1}\frac{t^k\zeta^k}{k}\right) \bmod q.$$

Writing $\alpha = 1+\frac{y}{x}\zeta^q = 1-t\zeta^q+q^2z$ for some $z\in\mathbb{Z}[\zeta]$ and eliminating denominators in (3.3) we find that

$$\alpha\cdot(x+q\varphi(x))\left(\overline{\alpha}+q\cdot f(\overline{\zeta})\right)\equiv\overline{\alpha}\cdot(x+q\varphi(x))\cdot(\alpha+q\cdot f(\zeta)) \bmod q^2$$

and

$$\alpha\cdot f(\overline{\zeta})\equiv\overline{\alpha}\cdot f(\zeta) \bmod q.$$

We let $S=\sum_{k=1}^{q-1}\frac{t^k\zeta^k}{k}$. Regrouping the terms, we find:

$$(1-t\overline{\zeta}^q)\cdot(\varphi(t)\cdot\zeta^q+S)\equiv(1-t\zeta^q)\cdot(\varphi(t)\cdot\overline{\zeta}^q+\overline{S}) \bmod q,$$

hence

$$-(\zeta^q-\overline{\zeta}^q)\varphi(t)\equiv(1-t\overline{\zeta}^q)S-(1-t\zeta^q)\overline{S} \bmod q,$$

and

$$-(\zeta^q-\overline{\zeta}^q)\varphi(t)\equiv\sum\frac{t^k}{k}\left(\zeta^k-\overline{\zeta}^k\right)-\sum\frac{t^{k+1}}{k}\left(\zeta^{k-q}-\overline{\zeta}^{k-q}\right) \bmod q.$$

We regroup the powers of ζ using $q-k\equiv -k \bmod q$, thus $\zeta^{k-q}/k\equiv-\overline{\zeta}^{q-k}/(q-k)$, which can be applied in the above for $k=1,2,\ldots,q-1$:

$$-(\zeta^q-\overline{\zeta}^q)\varphi(t)\equiv\sum_{k=1}^{q-1}\frac{t^k-t^{2-k}}{k}\cdot\left(\zeta^k-\overline{\zeta}^k\right) \bmod q,$$

which is the statement of (3.2). □

The Lemma 13 essentially yields a system of equations modulo q in the unknown t. It turns out that under some additional conditions on p and q, there are only three possible values for t (one of which is $t = 0$). This reflects the main ideas which will subsequently lead, by a more in depth study of the system (3.2), to a sharper inequality between p and q. The *light* result is the following:

Proposition 5. *Assume that $p > q$ are odd primes and there is a $\beta \in \mathbb{Q}(\zeta)$ such that (3.1) holds. Then*

$$x + f \cdot y \equiv 0 \bmod q^2 \tag{3.4}$$

for some $f \in \{-1, 0, 1\}$.

Proof. Assume first that $x \equiv 0 \bmod q$ and $x = qu$ with $(u, q) = 1$. Since $(x, y) = 1$ and $p \neq q$, it follows that $(x + \zeta^a y, q) = 1$, so the right hand side of (3.1) is a q-integer. The equation is Galois-invariant, so we can replace ζ by ζ^q. Thus (3.1) becomes

$$\frac{y + q\overline{\zeta}^q u}{y + q\zeta^q u} = \gamma^q,$$

with $\gamma = \pm\zeta^{-2} \cdot \beta/\overline{\beta}$. From the definition, we see that $\gamma^q \equiv 1 \bmod q\mathbb{Z}[\zeta]$. Let $\mathfrak{Q} \subset \mathbb{Z}[\zeta]$ be a prime above q, and f be its height. We have a fortiori $\gamma^q \equiv 1 \bmod \mathfrak{Q}$ and raising the identity to the power q^{f-1}, we obtain

$$\gamma \equiv \gamma^{q \cdot q^{f-1}} \equiv 1 \bmod \mathfrak{Q}.$$

This holds for all primes of $\mathbb{Z}[\zeta]$ above q, so $\gamma \equiv 1 \bmod q$. Consequently, $\gamma = 1 + qw$ for some $w \in \mathbb{Z}[\zeta]$, and thus $\gamma^q = (1 + qw)^q \equiv 1 \bmod q^2$, and $y + qu\zeta^q \equiv y + qu\overline{\zeta}^q \mod q^2$. Thus $u \cdot (\zeta^2 - \overline{\zeta}^2) \equiv 0 \bmod q$. Since p is odd, this is only possible if $u \equiv 0 \bmod q$ and thus $x \equiv 0 \mod q^2$. We can interchange x and y, so this proves that if x or y is divisible by q, then it is divisible by q^2, which takes care of $f = 0$ in this case.

We may now assume that $q \nmid x, y$ and use the previous lemma, which implies that (3.2) holds under the given premises. Since the set $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ builds a base of the algebra $\mathbb{Z}[\zeta]/(q \cdot \mathbb{Z}[\zeta])$, the coefficients of the single powers in the above identity must all vanish and $p > q + 1$ implies that the coefficient of ζ is $a_1 = t(1 - t^{-4})$ and thus

$$t^4 \equiv 1 \bmod q$$

must hold. Furthermore, if $q + 2 < p$, then the coefficient of ζ^2 is

$$2 \cdot a_2 = (t^2 - t^{-4}) \equiv 0 \quad \text{hence} \quad t^6 - 1 \equiv 0 \bmod q.$$

The last two congruences in t have the only common solution $t^2 = 1 \bmod q$. One easily verifies that if this holds, then the right hand side in (3.2) vanishes and thus $\varphi(t) \equiv 0 \bmod q$. This leads to the possible solution $x \pm y \equiv 0 \bmod q^2$. Inserting the value back shows that this is indeed a solution of (3.1). If $p = q+2$,

then we still have $a_1 = t^{-3}(t^4-1)$ so $t^4 \equiv 1 \bmod q$. If $t^2 - 1 \equiv 0 \bmod q$, we find the previous solution. So let us assume that $t^2 \equiv -1 \bmod q$ and consider the second coefficient: but $\varphi(t)\overline{\zeta}^q = \varphi(t)\zeta^2$ has in this case a contribution to a_2. We estimate this coefficient by using $t^2 \equiv -1 \bmod q$:

$$\begin{aligned} 2 \cdot a_2 &\equiv t^2 - t^{-4} - 2\varphi(t) \equiv -t^{-4}\left(t^6 - t^2 + t^2 - 1 + 2t^4\varphi(t)\right) \\ &\equiv t^2 - 1 + 2\varphi(t) \equiv 2(\varphi(t) - 1) \bmod q, \end{aligned}$$

a congruence which is satisfied by $\varphi(t) \equiv 1 \bmod q$. We have to consider also

$$\begin{aligned} 3 \cdot a_3 = (t^3 - t^{-5}) - (t^{q-1} - t^{-q-1}) \equiv 0 \bmod q \quad \Leftrightarrow \\ 0 \equiv t^{-5}(t^8 - 1) - (1 - t^{-2}) \bmod q. \end{aligned}$$

If $t^2 \equiv -1 \bmod q$, then the first term vanishes while the second is $-2 \not\equiv 0 \bmod q$, so $t^2 \equiv -1 \bmod q$ is not possible. This takes care of the case $p = q + 2$ as well, thus completing the proof of the proposition. □

It follows from Lemma 13 that

Corollary 1. *If $p > q > 3$ are odd primes for which (1.6) has nontrivial solutions and such that $q \nmid h_p^-$, then (3.4) holds.*

Proof. The premises of Lemma 13 are given and thus (3.2) holds. By setting $\beta = \rho_1$ in this equation, we find that the hypotheses of Proposition 5 also hold, and by its proof it follows that (3.4) must be true. □

3.1 Sharpening

In order to gain more information from (3.2), also in cases when $q > p$, we need to introduce first some operations on sequences. Let k be a field and $\mathcal{T}$ be the space of sequences on $k(t)$. We define the following operators on $\mathcal{T}$: For $a = (a_n)_{n\in\mathbb{N}} \in \mathcal{T}$, the maps $\theta_+, \theta_-, \Theta : \mathcal{T} \to \mathcal{T}$ produce the following sequences:

$$\begin{aligned} \theta_+(a)_n &= a_n - t \cdot a_{n-1}, \\ \theta_-(a)_n &= t \cdot a_n - a_{n-1}, \\ \Theta(a)_n &= \theta_+(\theta_-(a))_n. \end{aligned} \tag{3.5}$$

Furthermore we let Δ be the classical forward difference operator

$$\Delta a_n \;=\; a_n - a_{n-1}$$

and

$$n^{\underline{k}} = n \cdot (n-1) \ldots (n-k+1)$$

be the k-th falling power of n, so $\Delta n^{\underline{k}} = k \cdot (n-1)^{\underline{k-1}}$. The main properties of the operators in (3.5) are given by the following lemma.

Lemma 14. *The operators θ_+ and θ_- are linear and they commute:*

$$\Theta = \theta_+ \circ \theta_- = \theta_- \circ \theta_+.$$

Furthermore,

$$\begin{aligned} \theta_+(t^n) &= 0, & \theta_+(t^{-n}) &= (1-t^2)t^{-n}, \\ \theta_-(t^{-n}) &= 0, & \theta_-(t^n) &= -(1-t^2)t^{n-1}, \end{aligned} \tag{3.6}$$

and

$$\begin{aligned} \theta_+^l(n^{\underline{k}} \cdot t^n) &= \frac{k!}{l!} \cdot (n-l)^{\underline{k-l}} \cdot t^n, \\ \theta_-^l(n^{\underline{k}} \cdot t^{-n}) &= \frac{k!}{l!} \cdot (n-l)^{\underline{k-l}} \cdot t^{-(n-l)}, \end{aligned} \tag{3.7}$$

where we set $a^{\underline{k-l}} = 0$ if $k < l$. In particular, we have:

$$\begin{aligned} \theta_+^k(n^{\underline{k}} \cdot t^n) &= k! \cdot t^n, \\ \theta_-^k(n^{\underline{k}} \cdot t^{-n}) &= k! \cdot t^{-(n-k)}, \\ \Theta^k(n^{\underline{k}} \cdot t^n) &= k! \cdot (t^2-1)^k \cdot t^{n-k}, \\ \Theta^k(n^{\underline{k}} \cdot t^{-n}) &= k! \cdot (-1)^k \cdot (t^2-1)^k \cdot t^{-(n-k)}. \end{aligned} \tag{3.8}$$

Proof. Commutativity follows by a straightforward computation from

$$\theta_+ \circ \theta_-(a_n) = \theta_- \circ \theta_+(a_n) = t \cdot (a_n + a_{n-2}) - (t^2+1)a_{n-1}.$$

The rules (3.6) are also easily verified and they yield (3.7) by induction on k. Finally, the first two actions in (3.8) are obtained by setting $l = k$ in (3.7), while the action of Θ is obtained due to commutativity, by setting $\Theta^k = \theta_-^k \circ \theta_+^k$ or $\Theta^k = \theta_+^k \circ \theta_-^k$, depending whether the operand is t^n or t^{-n}. □

Remark 1. *Note that $k+1$ consecutive values of a_n are necessary for applying $\theta_\pm^k$, while Θ^k requires $2k+1$ consecutive values.*

We shall call the set $\{-1, 0, 1\}$ the *admissible solutions*. The task we pursue is to improve our estimates on pairs p, q for which the system (3.2) has no other solutions except (3.4). In particular, we are concerned with $p < q$, since Proposition 5 deals already with $p > q$. We shall use the fact on which the proof of Proposition 5 relies: $(\zeta^k)_{k=1}^{p-1}$ forms a base of the algebra $\mathbb{Z}[\zeta]/(q\mathbb{Z}[\zeta])$ and this allows us to consider (3.2) as a linear system modulo q. Concretely, the coefficients of $\zeta^k - \overline{\zeta}^k$ in that equation must vanish, for $k = 1, 2, \ldots, \frac{p-1}{2}$. Let $0 < \nu < \frac{p-1}{2}$ be the value for which $\nu \equiv q \bmod p$ or $\nu \equiv -q \bmod p$. Then, with δ_{ij} the Kronecker δ, the previous observation yields the equations:

$$\begin{aligned} -\delta_{\nu,k} \cdot \varphi(t) \equiv & \sum_{j \geq 0; jp+k<q} \frac{t^{k+pj} - t^{2-(k+pj)}}{pj+k} \\ & - \sum_{j \geq 0; jp+(p-k)<q} \frac{t^{p-k+pj} - t^{2-(p-k+pj)}}{p-k+jp} \bmod q. \end{aligned} \tag{3.9}$$

The index value ν plays a singular role in the equations above: first, it is the only index for which the equations are not homogeneous. Second the number of terms in the sums in the right hand side changes between $0 < k < \nu$ and $p/2 > k > \nu$. In these two intervals, (3.9) yields homogeneous equations which manifests itself in the vanishing of polynomials of fixed degree in k. This suggests the use of the difference operators defined above. Let $5 \leq p < q$ be primes. We shall take the approach of choosing either the interval $0 < k < \nu$ or $\nu < k < p/2$, whichever has more elements: in that interval; (3.9) translates into polynomial equations of the type $f_q(k;t) = 0$. Having a contiguous interval on which this equation holds, one can use the iteration of Θ in order to reduce the degree in k of the polynomial f_q. We have thus to distinguish the cases $\nu < p/4$ and $\nu > p/4$.[1]

Proposition 6. *Let $5 \leq p < q$ be primes such that (3.2) holds and ν be defined above. Suppose that $\nu > p/4$. If in addition, $q < \frac{p(p-12)}{16}$, then (3.4) holds.*

Proof. Let $n = \lfloor q/p \rfloor$. The equation (3.9) yields on the interval $0 < k < \nu$:

$$\sum_{0 \leq j \leq n} \frac{t^{k+pj} - t^{2-(k+pj)}}{pj+k} \equiv \sum_{0 \leq j < n} \frac{t^{p-k+pj} - t^{2-(p-k+pj)}}{p-k+jp} \bmod q. \tag{3.10}$$

After eliminating denominators, this yields a polynomial equation:

$$(-1)^n k^{2n} \cdot \sum_{0 \leq j \leq n} \left(t^{k+pj} - t^{2-(k+pj)} \right) + O(k^{2n-1}) \equiv$$
$$(-1)^{n-1} k^{2n} \cdot \sum_{0 \leq j < n} \left(t^{p-k+pj} - t^{2-(p-k+pj)} \right) + O(k^{2n-1}) \bmod q.$$

In order to eliminate the lower order terms in k, we may take Θ^{2n} on both sides of the congruence. This requires at least $2(2n)+1$ contiguous points, so $1 \leq k - 2n < k + 2n < p/4$, which means $2(2n)+1 < p/4$. If this is provided, the equation reduces, after simplifying by $(-1)^n \cdot (2n)! \cdot (1-t^2)^{2n}$, to:

$$\sum_{0 \leq j \leq n} \left(t^{k+pj-2n} - t^{2-(k+pj-2n)} \right)$$
$$+ \sum_{0 \leq j < n} \left(t^{p-k+2n+pj} - t^{2-(p+2n-k+pj)} \right) \equiv 0 \bmod q. \tag{3.11}$$

If $t \notin \{-1, 0, 1\}$ then we can apply θ_+ and θ_- independently to the above congruence. This yields:

$$0 \equiv \sum_{0 \leq j \leq n} t^{2-(k+pj-2n)} - \sum_{0 \leq j < n} t^{p-k+2n+pj} \bmod q,$$

[1] One may also take the approach of considering the whole interval $0 < k < p/2$. In this case the polynomials $f_q(k;t)$ change the degree and shape when k passes the "singular" value $k = \nu$. The computations become more intricate, for a gain of a factor at most 2. We choose to analyze here the simpler approach.

and

$$0 \equiv \sum_{0 \le j \le n} t^{k+pj-2n} - \sum_{0 \le j < n} t^{2-(p+2n-k+pj)} \bmod q.$$

Upon multiplication by the lowest power of t, we obtain

$$\begin{aligned} 0 &\equiv \sum_{0 \le j \le n} t^{pj} - \sum_{0 \le j < n} t^{p(n+1)-2+pj} \bmod q \quad \text{and} \\ 0 &\equiv \sum_{0 \le j \le n} t^{pn+pj-2} - \sum_{0 \le j < n} t^{pj} \bmod q. \end{aligned} \tag{3.12}$$

Adding the two congruences, we obtain $t^{pn} \equiv -t^{pn-2} \bmod q$ with the solutions $t \equiv 0$ and $t^2 \equiv -1 \bmod q$. The first solution is admissible. We reinsert $t^2 \equiv -1 \bmod q$ in (3.11), using the fact that $t^m \equiv (-1)^m t^{-m} \bmod q$ for all m. This yields, after some computations,

$$(t^k + t^{-k}) \cdot \left(1 + \sum_{j=1}^{n} t^{pj} (1 + (-1)^j) \right) 0 \bmod q.$$

The inner sum is

$$1 + 2 \sum_{0 < 2l \le n} (-1)^l = 1 + 2(-1 + 1 - 1 \ldots + (-1)^{[n/2]}) = \begin{cases} 1 & \text{if } [n/2] \equiv 0 \bmod 2 \\ -1 & \text{otherwise,} \end{cases}$$

and the previous condition thus becomes $\pm(t^k + t^{-k}) \equiv 0 \bmod q$, and since $t \not\equiv 0$, it follows that $(-1)^k + 1 \equiv 0 \bmod q$. It suffices to take k even, to obtain $t \equiv 0 \bmod q$, again, an admissible solution.

We now verify the conditions necessary for our derivation. For the final application of $\theta_\pm$ and the condition that k be even, we need:

$$2n + 1 \le k \le p/4 - (2n + 1),$$

which is satisfied by the even value $k = 2(n + 1)$, provided that $4n + 3 < p/4$. On the other hand, we find from the definition of ν and the fact that $\nu > p/4$, that $p(4n + 3) > 4q$, and thus

$$p^2/4 > p(4n + 3) > 4q,$$

as claimed. On the other hand, we find from the definition of n that if $q < \frac{p(p-12)}{16}$, then

$$4n + 3 \le 4\lfloor q/p \rfloor + 3 < 4\frac{p - 12}{16} + 3 = p/4.$$

as claimed. □

Proposition 7. *Let $5 \le p < q$ be primes such that (3.2) holds and ν be defined above. Suppose that $\nu < p/4$ and $q < \frac{p(p-12)}{16}$. Then (3.4) holds.*

Proof. The proof of this proposition follows the same line as the previous one, but encounters a few particular obstructions. We shall let

$$n = \begin{cases} \lfloor q/p \rfloor - 1 & \text{if } (q \bmod p) < p/4, \\ \lfloor q/p \rfloor & \text{if } (q \bmod p) > 3p/4. \end{cases}$$

The equation (3.9) yields now on the interval $\nu < k < p/4$:

$$\sum_{0 \le j \le n} \frac{t^{k+pj} - t^{2-(k+pj)}}{pj+k} \equiv \sum_{0 \le j \le n} \frac{t^{p-k+pj} - t^{2-(p-k+pj)}}{p-k+jp} \bmod q. \tag{3.13}$$

Note that there are equally many terms in the sums of both sides of the above congruences, unlike the case of the previous proposition. If $t \notin \{-1, 0, 1\}$, this perpetuates down to the analogue of (3.12), in which the two congruences become identical:

$$0 \equiv \sum_{0 \le j \le n} t^{pj} + \sum_{0 \le j \le n} t^{p(n+1)+pj-2} \bmod q. \tag{3.14}$$

If $t^p \equiv 1 \bmod q$, we get $(n+1)(t^2+1) \equiv 0 \bmod q$ and $t^2 \equiv -1 \bmod q$, hence $1 \equiv t^p \equiv (-1)^{(p-1)/2} t \bmod q$, showing that t is admissible; so we can assume $t^p \not\equiv 1 \bmod p$. Then

$$t^{p(n+1)} \equiv 1 \bmod q \qquad \text{or} \qquad t^{p(n+1)} \equiv -t^2 \bmod q. \tag{3.15}$$

Note that this condition is equivalent to applying any of $\theta_+ \Theta^{2n+1}$ or $\theta_- \Theta^{2n+1}$ to the original system (3.9).

In order to arrive at a contradiction we shall have to consider lower order terms in k. Let

$$\sigma_j = t^{k+pj} - t^{2-(k+pj)} \qquad \text{and} \qquad \tau_j = t^{p-k+pj} - t^{2-(p-k+pj)}.$$

With some additional work, the first congruence yields, after elimination of denominators:

$$\begin{aligned} &\sum_{0 \le j \le n} \sigma_j \cdot \left(k^{\underline{2n+1}} - ((n+j+1)p - (2n+1)n) \cdot k^{\underline{2n}} \right) \\ &+ \sum_{0 \le j \le n} \tau_j \cdot \left(k^{\underline{2n+1}} - ((n-j)p - (2n+1)n) \cdot k^{\underline{2n}} \right) + O(k^{2n-1}) \equiv 0 \bmod q. \end{aligned} \tag{3.16}$$

We assume that the first congruence of (3.15) satisfied. Then

$$\sum_{0 \le j \le n} t^j = \frac{1 - t^{p(n+1)}}{1 - t^p} \equiv 0 \bmod q$$

and

$$\sum_{0 \le j \le n} t^{-j} = \frac{1 - t^{-p(n+1)}}{1 - t^{-p}} \equiv 0 \bmod q.$$

Herewith, (3.16) reduces to

$$\sum_{0\le j\le n}(t^{k+pj}-t^{2-(k+pj)})\cdot(-jp)\cdot k^{\underline{2n}} + \sum_{0\le j\le n}(t^{p-k+pj}-t^{2-p+k-pj})\cdot(jp)\cdot k^{\underline{2n}}+O(k^{2n-1})\equiv 0 \bmod q$$

We apply Θ^{2n} to the above and after simplifying by $(2n)!\cdot(1-t^2)^{2n}$, get

$$\sum_{0\le j\le n}(t^{k-2n+pj}-t^{2-k+2n-pj})\cdot(-jp) + \sum_{0\le j\le n}(t^{p-k+2n+pj}-t^{2-p+k-2n-pj})\cdot(jp)\equiv 0 \bmod q.$$

Then we have

$$(t^{k-2n}-t^{p-k+2n})\cdot\sum_{0\le j\le n}t^{pj}j\equiv(t^{2-k+2n}-t^{2-p+k-2n})\cdot\sum_{0\le j\le n}t^{-pj}j \bmod q,$$

hence

$$\begin{aligned}(t^{k-2n}-t^{p-k+2n}) \quad &\cdot \quad \frac{1+n}{t^p-1}\equiv(t^{k-2n}-t^{p-k+2n})\cdot(-t^{2-p})\cdot\frac{1+n}{t^{-p}-1} \bmod q,\\ t^{k-2n}-t^{p-(k-2n)} \quad &\equiv \quad t^2(t^{k-2n}-t^{p-k+2n}) \bmod q\end{aligned}$$

Since $t^2\equiv 1 \bmod q$ leads to admissible solutions, it remains that $t^p\equiv t^{2(k-2n)} \bmod q$, which must hold for instance for two successive values of k. Hence, by dividing the corresponding congruences, we get $t^2\equiv 1 \bmod q$, which has only admissible solutions.

Now we claim that

$$t^{p(n+1)}\not\equiv -t^2 \bmod q. \tag{3.17}$$

If not, we have

$$\sum_{0\le j\le n}t^{pj}\equiv\frac{1-t^{p(n+1)}}{1-t^p}\equiv\frac{1+t^2}{1-t^p} \bmod q$$

and

$$\sum_{0\le j\le n}t^{-pj}=\frac{1-t^{-p(n+1)}}{1-t^{-p}}\equiv\frac{1+t^{-2}}{1-t^{-p}} \bmod q.$$

This time, (3.16) is reduced to

$$\left(t^k\cdot\sum_{0\le j\le n}t^{pj}-t^{2-k}\sum_{0\le j\le n}t^{-pj}\right)\cdot k^{\underline{2n+1}} + \left(t^{p-k}\cdot\sum_{0\le j\le n}t^{pj}-t^{2-p+k}\sum_{0\le j\le n}t^{-pj}\right)\cdot k^{\underline{2n+1}}+O(k^{2n})\equiv 0 \bmod q.$$

Then we have

$$\left(t^k \cdot \frac{1+t^2}{1-t^p} - t^{2-k}\frac{1+t^{-2}}{1-t^{-p}}\right) \cdot \underline{k^{2n+1}} \\ + \left(t^{p-k} \cdot \frac{1+t^2}{1-t^p}\frac{1+t^{-2}}{1-t^{-p}}\right) \cdot \underline{k^{2n+1}} + O(k^{2n}) \equiv 0 \bmod q.$$

It follows that

$$\left(\frac{t^2+1}{1-t^p}\right) \cdot (t^k + t^{p-k}) \cdot 2 \cdot \underline{k^{2n+1}} + O(k^{2n}) \equiv 0 \bmod q.$$

We apply Θ^{2n+1} to the above and get

$$\left(\frac{t^2+1}{1-t^p}\right) \cdot \left(t^{k-2n-1} + t^{p-k+2n+1}\right) \cdot 2 \cdot (2n+1)! \cdot (t^2-1)^{2n+1} \equiv 0 \bmod q.$$

We have excluded $t^2 \equiv -1 \bmod q$ and the vanishing of the second factor leads to $t^p \equiv t^{2(k-2n-1)}$, which implies like before, that $t^2 - 1 \equiv 0 \bmod q$, thus only admissible solutions are possible. This confirms the claim (3.17).

We finally have to derive the inequality between p and q, for which the proof above holds. The condition is that the interval $(p/4, p/2)$ contains sufficient contiguous points for applying both $\theta_\pm \Theta^{2n+1}$ and $\theta_+^2 \Theta^{2n}$. This requires at least $2(2n+1)+1$ contiguous points, so we need $p/4 < k-2(n+1) < k+2(n+1)+1 < p/2$, which means $4n+3 < p/4$. Note that by definition of n, if $q < \frac{p(p-12)}{16}$, then

$$4n + 3 \leq 4\lfloor q/p \rfloor + 3 < p/4.$$

This completes the proof of the Proposition 1. □

Chapter 4

The local approach

We consider the cases when a solution to (1.6) has $x \equiv f \bmod q^2$, with $f \in \{-1, 0, 1\}$. Let $\mu := \rho/\bar{\rho}$ and note that $\delta := \overline{\alpha} \cdot \left(\frac{\mu-1}{1-\zeta^2}\right)^q \in \mathcal{O}(\mathbb{K})^\times$, as follows by the following computations:

$$\delta = \bar{\alpha} \cdot \left(\frac{\mu-1}{1-\zeta^2}\right)^q = -\zeta^q \bar{\alpha} \left(\frac{\rho-\overline{\rho}}{(\zeta-\bar{\zeta})\overline{\rho}}\right)^q = -\zeta^q \frac{\bar{\alpha}}{\overline{\rho}^q} \cdot \left(\frac{\rho-\bar{\rho}}{\zeta-\bar{\zeta}}\right)^q = -\zeta^q \bar{\varepsilon} \cdot \left(\frac{\rho-\bar{\rho}}{\zeta-\bar{\zeta}}\right)^q.$$

We note that $A - \overline{A} \equiv 0 \bmod (\zeta - \bar{\zeta})$ for arbitrary $A \in \mathbb{Z}[\zeta]$, so consequently $\frac{\rho-\bar{\rho}}{\zeta-\bar{\zeta}} \in \mathbb{Z}[\zeta]$. In view of Lemma 12, we have:

$$\begin{aligned} \alpha - \bar{\alpha} &= \zeta - \bar{\zeta} = \varepsilon \cdot (\rho - \overline{\rho}) \cdot \left(\frac{\rho^q - \bar{\rho}^q}{\rho - \bar{\rho}}\right), \quad \text{hence} \\ \varepsilon^{-1} &= \left(\frac{\rho-\bar{\rho}}{\zeta-\bar{\zeta}}\right) \cdot \left(\frac{\rho^q - \bar{\rho}^q}{\rho - \bar{\rho}}\right); \end{aligned} \tag{4.1}$$

the two factors on the right hand side are integral, and their product is a unit, so both must be units, individually[1]. We note also that $\overline{\alpha} \cdot \left(\frac{\mu-1}{\pi}\right)^q \in \mathcal{O}(\mathbb{K})^\times$ for every $\pi \in \wp$ that generates the prime above p. We shall adapt various values for π to the different values of f. We may write $\delta(1-\zeta^2)$ in the above case, to indicate that the unit is defined with respect to the choice $\pi = 1 - \zeta^2$.

We shall compute a q-adic developments of δ and its norm, and compare this to 1, which should be the result, since we have seen that δ is a unit.

4.1 The case $f = 0$

Let $x = q^l z$ with $z \in \mathbb{Z}$, $p \nmid z$ and $l \geq 2$; we have

$$\mu^q = \zeta^{2q} \frac{1 - \overline{\zeta}^q x}{1 - \zeta^q x},$$

[1] We mention for later use, that the decomposition so far is independent of the value of x

so

$$\mu = \zeta^2 \cdot \frac{1-\bar{\zeta}^q q^{l-1} z}{1-\zeta^q q^{l-1} z} + O(q^{2(l-1)}) = \zeta^2 \cdot \left(1 + q^{l-1} z \cdot (\zeta^q - \bar{\zeta}^q)\right) + O(q^{2(l-1)}),$$

hence

$$\begin{aligned} \frac{\mu - 1}{\zeta^2 - 1} &= 1 + \frac{x}{q} \cdot \frac{\zeta^q (1 - \bar{\zeta}^{2q})}{1 - \bar{\zeta}^2} + O(q^{2(l-1)}), \\ \delta &= 1 + x \cdot \left(\frac{\zeta^q (1 - \bar{\zeta}^{2q})}{1 - \bar{\zeta}^2} + \bar{\zeta}^q \right) + O(q^{2(l-1)}); \end{aligned}$$

by defining $B = \frac{\zeta^q (1-\bar{\zeta}^{2q})}{1-\bar{\zeta}^2}$, and taking the norm of $\delta(\zeta^2 - 1)\bar{\zeta}$, we see that $\mathbf{N}(\delta) = 1$ implies $\mathbf{Tr}(B - \bar{\zeta}^q) \equiv 0 \bmod q$ and so $\mathbf{Tr}(B) \equiv -1 \bmod q$. Let $q \equiv r \bmod p$, where $1 \leq r \leq p-1$; since

$$\bar{B} = \bar{\zeta}^r (1 + \zeta^2 + \ldots + \zeta^{2(r-1)}) = \zeta^{-r} + \zeta^{2-r} + \ldots + \zeta^{r-2},$$

we see that for odd r, none of the terms in this sum carries the exponent zero. There are r terms in the sum B, so

$$\mathbf{Tr}(B - \zeta^{-q}) = \begin{cases} -r+1 & \text{if } r \text{ is odd} \\ -r+1+p & \text{otherwise.} \end{cases} \tag{4.2}$$

If r is even, which only happens when $q > p$, then $0 < -r+1+p < q$ and hence $q \nmid (-r+1+p)$. If r is odd, the vanishing condition requires $r = 1$ so $q \equiv 1 \bmod p$.

In this case we consider some higher order terms:

$$\mu = \zeta^2 (1 - q^l z \bar{\zeta}^q)^{1/q} (1 - q^l z \zeta^q)^{-1/q}. \tag{4.3}$$

By expanding (4.3) under the condition $\zeta^q = \zeta$, we obtain

$$\begin{aligned} \mu &= \zeta^2 \left(1 - q^{l-1} z \bar{\zeta} + q^{2l-2} z^2 \frac{1-q}{2} \bar{\zeta}^2\right) \cdot \left(1 + q^{l-1} z \zeta + q^{2l-2} z^2 \frac{1+q}{2} \zeta^2\right) + O(q^{3l-3}) \\ &= \zeta^2 \left(1 + q^{l-1} z (\zeta - \bar{\zeta}) + q^{2l-2} z^2 \frac{\bar{\zeta}^2 (1-q) - 2 + \zeta^2 (1+q)}{2}\right) + O(q^{3l-3}), \\ \frac{\mu - 1}{1 - \bar{\zeta}^2} &= -\left(1 + q^{l-1} z \frac{\zeta - \bar{\zeta}}{1 - \bar{\zeta}^2} + q^{2l-2} z^2 \frac{\bar{\zeta}^2 \frac{1-q}{2} - 1 + \frac{q+1}{2} \zeta^2}{1 - \bar{\zeta}^2}\right) + O(q^{3l-3}), \end{aligned}$$

implying that

$$-\left(\frac{\mu - 1}{1 - \zeta^2}\right)^q = 1 + q^l z \frac{\zeta - \bar{\zeta}}{1 - \bar{\zeta}^2} + q^{2l-1} z^2 \left(\frac{\bar{\zeta}^2 \frac{1-q}{2} - 1 + \frac{q+1}{2} \zeta^2}{1 - \bar{\zeta}^2} + \left(\frac{\zeta - \bar{\zeta}}{1 - \bar{\zeta}^2}\right)^2 \frac{q-1}{2} \right) + O(q^{2l}).$$

Hence

$$\delta = 1 + q^{2l-1}z^2\left(\frac{\overline{\zeta}^2\frac{1-q}{2} - 1 + \frac{q+1}{2}\zeta^2}{1-\overline{\zeta}^2} + \zeta^2\frac{q-1}{2}\right) + O(q^{2l}).$$

Taking the norm of the last equality, we obtain

$$\mathbf{N}(\delta) = 1 + q^{2l-1}z^2 \cdot \mathbf{Tr}\left(\frac{\overline{\zeta}^2\frac{1-q}{2} - 1 + \frac{q+1}{2}\zeta^2}{1-\overline{\zeta}^2} + \zeta^2\frac{q-1}{2}\right) + O(q^{2l})$$

$$= 1 + q^{2l-1}z^2\left(-\frac{p-1}{2}\cdot\frac{1-q}{2} - \frac{p-1}{2} + \frac{q+1}{2}\cdot\frac{p-3}{2} + \frac{1-q}{2}\right) + O(q^{2l})$$

$$= 1 + q^{2l-1}z^2\frac{1-p}{2} + O(q^{2l}) \not\equiv \pm 1 \bmod q^{2l}.$$

We assumed that $q \equiv 1 \bmod p$, so the factor $\frac{1-p}{2} \not\equiv 0 \bmod q$ and consequently $\mathbf{N}(\delta) = 1 + Cq^{2l-1} + O(q^{2l})$, for an integer constant $C = z^2\frac{1-p}{2} \not\equiv 0 \bmod q$. This is inconsistent with the fact that δ is a unit, which completes the proof of case $f = 0$ in Proposition 2.

Chapter 5

Diophantine approximation

- $\Theta = \sum_{c\in P} m_c\sigma_c \in \mathbb{Z}_{\geq 0}\,[G]$; weight $w(\Theta) = \sum_{c\in P} n_c$.
- Formal binomial series:

$$\begin{aligned} F_{n\sigma_c}(T) &= (1+\zeta^c T)^{n/q} = 1 + \sum_{k=1}^{\infty} \binom{n/q}{k} (\zeta^c T)^k; \quad \text{and} \quad (5.1)\\ F_\Theta(T) &= \prod_{c=1}^{p-1} F_{m_c\sigma_c}(T) := 1 + \sum_{k=1}^{\infty} a_k(\Theta) T^k \in \mathbb{K}[[T]]. \end{aligned}$$

where the coefficients $a_k(\Theta)$ are obtained by multiplying out the elementary series and rearranging in ascending order of the powers of the indeterminate T.

Alternatively, we may fix $g \in P$ a generator of $\mathbb{F}_p^\times$ and fix $\sigma = \sigma_g \in G$, which is then a generator of the cyclic galois group. We then write our generic group ring element as

$$\Theta = \sum_{j\in P} n_j \sigma^j = \sum_{j\in P} n_j \sigma_{g^j},$$

and the formal power series $F_\Theta(T) := \prod_{j\in P} F_{n_j\sigma_{g^j}}(T)$.

The series $F_\Theta(-1/x)$ are absolutely convergent in $\mathbb{C}$, for $|x| > 1$, and in particular for integers $x \in \mathbb{Z}\setminus\{-1,0,1\}$ and

$$(F_{\sigma^d}(-1/x))^q = \mu^q,$$

so there exist exponents $a(d), a(d,\Theta) \in \mathbb{Z} \cap [-\frac{q-1}{2}, \frac{q-1}{2}]$ such that

$$\sigma^d(\rho/\overline{\rho}) = \xi^{a(d)} \cdot F_{(1-j)\sigma^d}(-1/x), \quad \text{and} \quad \sigma^d(\rho/\overline{\rho})^\Theta = \xi^{a(d,\Theta)} F_{\sigma^d(1-j)\Theta}(-1/x);$$

we may also write $a(\Theta) = a(1,\Theta)$. We may estimate the power series by appealing to Lemma 7 of [Mih06], which leads to

$$W(\sigma^d\Theta) := \left|F_{(1-j)\sigma^d\Theta}(-1/x) - 1\right| < 3\frac{w(\Theta)}{q|x|}. \quad (5.2)$$

By considering the action of Θ on $\sigma^d(\rho/\overline{\rho})$, one verifies the following:

$$a(d,\Theta) \equiv \sum_{i=1}^{p-1} n_i a(d+i) \bmod p. \tag{5.3}$$

Recall that $\sigma^{\frac{p-1}{2}}$ is the complex conjugation, hence $a(i+\frac{p-1}{2},\Theta) = -a(i,\Theta)$ for $1 \le i \le \frac{p-1}{2}$. Let $\nu_i = n_i - n_{i+\frac{p-1}{2}}$; by inserting in (5.3) we obtain

$$a(d,\Theta) \equiv \sum_{i=1}^{\frac{p-1}{2}} \nu_i a(d+i) \bmod p, \quad d = 1,2,\ldots,p-1. \tag{5.4}$$

We call the system of equations (5.4) over $\mathbb{F}_p$, the *associated linear system of* $\Theta \in \mathbb{Z}_{\ge 0}[G]$. Above considerations show that we may interpret the vector $\vec{A} := (a(d))_{d=1}^{\frac{p-1}{2}}$ as given and consider the ν_i as unknowns for a given constant vector $\vec{X}$. We shall impose certain conditions on the vector $\vec{X}$, which will determine n_i and herewith, a $\Theta \in \mathbb{Z}[G]$. For some $\tau \in \mathbb{N}$ with $1 \le \tau \le (p-1)/2$, we let the entries $X_j = 0; j \le \tau$ in the right hand side vector of the system (5.4), meaning that we wish to find Θ, such that the exponents $a(\sigma^d\Theta) = 0$ for $d \le \tau$. The remaining entries in $\vec{X}$ are free. We shall maximize τ subject to the condition that the homogenous system built from the first τ equations in (5.4) has a non trivial integer solution $\vec{\nu}$ with $||\vec{\nu}||_1 < 2$. The values $X_d; d > \tau$ will be determined by this solution.

Focusing herewith on the first τ equations we consider the linear map with matrix $M = (a(d,i))_{d,i=1}^{\tau,(p-1)/2}$ and its action on the vectors in $V_2 = \{0,1\}^{(p-1)/2}$. For $v \in V_2$ we consider the image $w = Mv \in (\mathbb{Z}/(q\cdot\mathbb{Z}))^\tau$. By an application of the pigeon hole principle, we see that as soon as

$$2^{(p-1)/2} > q^\tau \quad \Leftrightarrow \quad \tau < \frac{p-1}{2\log_2(q)}, \tag{5.5}$$

there are two different vectors $v_1, v_2 \in V_2$ with identical image, so letting $v = v_1 - v_2$, we obtain an integer vector with entries in $\{-1,0,1\}$ and such that $Mv \equiv 0 \bmod q$. We may thus choose the value

$$\tau = \left[\frac{p-1}{2\log_2(q)}\right],$$

and the previous reasoning implies there is a vector $\vec{\nu}$ with entries in $\{-1,0,1\}$ which annihilates modulo q the first τ equations in (5.4). This vector defines a group ring element $\theta = \sum_{i=1}^{(p-1)/2} \nu_i \sigma^i \in \mathbb{Z}[G]$. It can be transformed into a positive element $\Theta \in \mathbb{Z}_{\ge 0}[G]$ as follows: we observe that in θ, the coefficients $\nu_i = 0$ for $i > p/2$. We derive the $\Theta = \sum_{c\in P} n_c\sigma^c$ as follows: set all $n_j = 0$ and then, for $c = 1,2,\ldots,\frac{p-1}{2}$, let $n_j = \nu_j$ if $\nu_j \ge 0$ and $n_{p-j} = -\nu_j$ otherwise. This defines Θ uniquely, and by the above, we know that $a(\sigma_d\Theta) = a(\sigma_d\theta) = 0$ for all $d \le \tau$. The weight verifies $w(\Theta) = \sum_1^{(p-1)/2} |\nu_i| \le \frac{p-1}{2}$.

5.1 The norm of $(\rho/\overline{\rho})^{\Theta}-1$

We move on to compute the norm of $(\rho/\overline{\rho})^{\Theta}-1$:

$$\mathbf{N}\big((\rho/\overline{\rho})^{\Theta}-1\big)=\prod_{c\in P}\big((\sigma^{c}(\rho/\overline{\rho}))^{\Theta}-1\big)=\prod_{c\in P}\Big(\xi^{a(c,\Theta)}\cdot F_{\sigma^{d}(1-\jmath)\Theta}(-1/x)-1\Big)=:P_1\cdot P_2,$$

where P_1 denotes the products of the factors with $a(c,\Theta)\neq 0$ and P_2 denotes the one with $a(c,\Theta)=0$. Let the number of factors appearing in P_2 be $t(\Theta)$, so by construction, $2\tau\leq t(\Theta)$.

Then by (5.2), for each factor $\phi_c:=\big(\xi^{a(c,\Theta)}\cdot F_{\sigma^{d}(1-\jmath)\Theta}(-1/x)-1\big)$ appearing in P_1, we have that

$$\begin{aligned}\Big|\xi^{a(c,\Theta)}\cdot F_{\sigma^{d}(1-\jmath)\Theta}(-1/x)-1\Big|&\leq\big|F_{\sigma^{d}(1-\jmath)\Theta}(-1/x)-1\big|+1\\&\leq 3\frac{w(\Theta)}{q|x|}+2\leq 2\left(1+\frac{3(p-1)}{4q|x|}\right);\end{aligned}\tag{5.6}$$

similarly, for each factor ϕ_c occurring in P_2, we have

$$\big|F_{\sigma^{d}(1-\jmath)\Theta}(-1/x)-1\big|\leq 3\frac{w(\Theta)}{q|x|}\leq\frac{3(p-1)}{2q|x|}.\tag{5.7}$$

Let $q=cp\log(p)$, for some $c>1$; we search a minimal value for c, such that the existence of a solution to (1.6) to which we apply Θ derived here, leads to a contradiction. If $p>29$, then $3(p-1)/2q<1/2$, hence by (5.6), (5.7), we obtain

$$|\mathbf{N}\big((\rho/\overline{\rho})^{\Theta}-1\big)|=|P_1\cdot P_2|<3^{p-1-t(\Theta)}\cdot(1/|x|)^{t(\Theta)}.$$

Therefore

$$|\mathbf{N}\big((\rho-\overline{\rho})^{\Theta}\big)|=|\mathbf{N}(\overline{\rho}^{\Theta})|\cdot|\mathbf{N}\big((\rho/\overline{\rho})^{\Theta}-1\big)|<|y|^{w(\Theta)}\cdot 3^{p-1-t(\Theta)}\cdot(1/|x|)^{t(\Theta)};\tag{5.8}$$

recall that $(\rho-\overline{\rho})$ is associated with $(\zeta-\bar{\zeta})$ by (4.1), hence

$$\mathbf{N}\big((\rho-\overline{\rho})^{\Theta}\big)=p^{w(\Theta)},$$

and (5.8) is equivalent to

$$1<\left(\frac{|y|}{p}\right)^{w(\Theta)}\cdot 3^{p-1-t(\Theta)}\cdot(1/|x|)^{t(\Theta)}.$$

Recall that we have the known result $|y|\geq 2p+1$, $t(\Theta)\geq 2\tau$ and $w(\Theta)\leq(p-1)/2$, hence

$$1<\left(\frac{|y|}{p}\right)^{w(\Theta)}\cdot 3^{p-1-t(\Theta)}\cdot(1/|x|)^{t(\Theta)}\leq\left(\frac{|y|}{p}\right)^{(p-1)/2}\cdot 3^{p-1-2\tau}\cdot(1/|x|)^{2\tau}.\tag{5.9}$$

Note that

$$y^q = \frac{x^p - 1}{x - 1} < \frac{4}{3}|x|^{p-1};$$

if $p > 9$, we obtain from (5.9):

$$1 < \left(\frac{4}{3}\right)^{\frac{p-1}{2q}} \cdot (9/p)^{(p-1)/2} \cdot |x|^{\frac{(p-1)^2}{2q} - 2\tau} \leq \left(|x|^{\frac{p-1}{2q} - \frac{2\tau}{p-1}}\right)^{p-1}, \tag{5.10}$$

which is impossible if

$$\tau \geq \frac{(p-1)^2}{4q}. \tag{5.11}$$

We see that if there is an integer τ with upper bound given by (5.5) and lower bounded by (5.11), then (5.9) leads to a contradiction, derived from the assumption that (1.6) has a solution. In other words, provided that q is sufficiently large for the interval

$$\frac{(p-1)\log 2}{2\log(q)} > \tau \geq \frac{(p-1)^2}{4q}. \tag{5.12}$$

to contain an integer, we may conclude that there are no solutions of (1.6) for such p, q, if $q \nmid h_p^-$. If the simple inequality

$$\frac{(p-1)\log(2)}{2\log(q)} > \frac{(p-1)^2}{4q} + 1 \tag{5.13}$$

holds, then the given interval necessarily contains an integer. Multiplying both sides with $\frac{4q}{(p-1)^2}$, we get the equivalent inequality

$$\frac{q\log(4)}{(p-1)\log(q)} > 1 + \frac{4q}{(p-1)^2}. \tag{5.14}$$

For $c < 2.7$, we use $\log(q) < 1 + \log(p) + \log\log(p)$ and $(4q)/(p-1)^2 \leq c\log(p)/(p-2)$, so

$$\frac{q\log(4)}{(p-1)\log(q)} > \frac{c\log(4)}{1 + \frac{1+\log\log(p)}{\log(p)}}$$

hence the condition is fulfilled if

$$c \cdot \left(\frac{\log(4)}{1 + \frac{1+\log\log(p)}{\log(p)}} - \frac{4\log(p)}{p-2}\right) > 1. \tag{5.15}$$

Defining thus $C(p)$ to be the inverse of the cofactor of c and $M'(p) = C(p)p\log(p)$, we recover the definitions in (1.12), in which $C(p)$ is a function with asymptotic value $\lim_{p\to\infty} M'(p) = 1/\log(4) < 0.75$. Note that for $p = 29$ we have $M(p) < M'(p)$, while asymptotically we obviously have $M(p)/M'(p) \to \infty$. With some elementary analysis, one also verifies that the difference of the two functions only has one zero on $x > 29$. This is determined numerically to be $x \in (113, 127)$, which confirms the last statement of Proposition 3.

Finally, for the $29 \leq p \leq 113$, we need to check if there is any prime $M(p) < q < M'(p)$, such that the pair (p, q) satisfies the previously derived. Note that there always is a loss, when deriving a general condition that excludes all pairs verifying it. For concrete numbers, one may still show that no solution exist, by some concrete verification. We have done this using PARI and the following three conditions:

1. Existence of an integer τ satisfying condition of (5.12);
2. Using the conditions on μ in Proposition (6) and Proposition (7) that provide inequalities between μ and $4n + 3$.
3. Showing that the only possible values of t in (3.10) (if $\mu > p/4$) and (3.13) (if $\mu < p/4$) belong to $\{0, \pm 1\}$.

Indeed, the combination of the three criteria helped eliminate all remaining cases. It turns out that 3. is the most powerful condition. We herewith know that the only possible cases remaining verify $x \equiv \pm 1 \bmod q^2$. In order to complete the proof of Theorem 8 we shall eliminate these cases by using a local power series development method.

Chapter 6

Local approximation in the cases $x \equiv \pm 1 \bmod q^2$

In this chapter we use local approximation for eliminating these two remaining cases. Using local power series expansions, we prove

Proposition 8. *The equation (1.6) has no solutions with $x \equiv f \bmod q^{l+1}$, for $p > 29$ and $f \in \{-1, 1\}; l \geq 1$.*

The proof of the proposition covers the rest of this section. We give first a brief description of our approach, which starts from the assumption that $(x, y; p, q)$ is a solution with odd primes p, q and $x \equiv \pm 1 \bmod q^2$.

The μ-map

Let

$$D_G = \left\{ t \in \mathbb{Z}[G]^\times : t = \sum_{c \in P} n_c \sigma_c \text{ with } n_c \in \{0, 1\};\ n_c + n_{p-c} \leq 1;\ n_c \cdot n_{p-c} = 0 \right\}.$$

Note that the set D_G is G-stable, since for $t \in D_G$, the conjugates σt will also fulfill the defining conditions of D_G.

Then, for $t \in D_G$, the product $Z(t) := y \cdot (\rho/\overline{\rho})^t \in \mathbb{Z}[\zeta]$, as follows from the definition of D_G together with the fact that the conjugates of ρ are pairwise coprime and have norm y. We note that the map

$$\Delta : D_G \hookrightarrow \mathcal{O}^\times(\mathbb{K}); \quad t \mapsto Z(t) \tag{6.1}$$

is indeed injective. This follows, for instance, by induction on the weight of t, from the coprimality of the conjugates of ρ.

Moreover, in the cases of interest, when $x \equiv \pm 1 \bmod q^{l+1}$, there is a converging q-adic binomial series

$$\mu(t) \quad = \quad (\rho/\bar{\rho})^t = 1 + \sum_{n=1}^{\infty} a_n(t) q^{ln}; \quad a_n(t) \in \mathbb{Z}[\zeta] \quad \text{and} \tag{6.2}$$

$$\sigma(a_n(t)) \quad = \quad a_n(\sigma t), \quad \forall \sigma \in G. \tag{6.3}$$

Here we assume that the coefficients $a_n(t)$ are elements of the minimal set of representatives $W = \left\{ \sum_{c \in P} w_c \zeta^c \ : \ -\frac{q^l-1}{2} \leq w_c \leq \frac{q^l-1}{2} \right\}$ for $\mathbb{Z}[\zeta]/q^l\mathbb{Z}[\zeta]$; thus, the binomial power series has been reordered in order for the coefficients to match this condition. Thus, $Z(t) = y \cdot \mu(t)$ and the coefficients of the power series are galois covariant, by (6.3). Note also that $\mu(t) \notin \mathbb{Z}[\zeta]$ and herewith, the power series (6.2) has infinitely many non vanishing coefficienty.

We fix a $\theta \in D_G$ such that $\sigma_a \theta \neq \sigma_b \theta$ for $a \neq b$, so $|G\theta| = p-1$. Let $Q = q^N$ for some large N, such that

$$Q > |py|^3.$$

The series (6.2) can be regrouped in terms of powers of Q, with some cofficients $b_m = b_m(\theta) \in W_Q$, where

$$W_Q = \left\{ \sum_{c \in P} w_c \zeta^c \ : \ -\frac{Q-1}{2} \leq w_c \leq \frac{Q-1}{2} \right\}$$

is a set of representatives for $\mathbb{Z}[\zeta]/Q\mathbb{Z}[\zeta]$:

$$\mu(\theta) \quad = \quad (\rho/\bar{\rho})^{\theta} = 1 + \sum_{n=1}^{\infty} b_n Q^n; \quad b_n \in W_Q. \tag{6.4}$$

The coefficients are also galois covariant, so $b_n(\sigma\theta) = \sigma(b_n(\theta))$. Moreover, $||b_n||_1 \leq (Q-1)/2$.

Scalar products and various representations of field elements

Let $\sigma = \sigma_g \in G$ be a generator of this cyclic group. We endow the number field $\mathbb{K} = \mathbb{Q}[\zeta]$ with the base $\mathcal{Z} = \{e_c = \sigma^c(\zeta) \ : \ c \in P\}$, as a $\mathbb{Q}$-vector space; this is at the same time the power normal base of the integers in $\mathbb{Z}[\zeta]$ and a fortiori, integral numbers are represented by vectors of rational integer coefficients with respect to this base. We let $V = \mathbb{Q}^{p-1}$ and denote the coefficient map of linear algebra by

$$\kappa : \mathbb{K} \to V, \quad \alpha = \sum_{c=1}^{p-1} a_c \sigma^c(\zeta) \mapsto \vec{a} = (a_1, a_2, \ldots, a_{p-1}) \in V.$$

It will also be convenient to introduce a notation for the vectors of conjugate elements of $\mathbb{K}$, so let

$$\mathbb{K}_G = \{(\sigma^c(x))_{c \in P} \in \mathbb{K}^{p-1} \ : \ x \in \mathbb{K}\} \subset \mathbb{K}^{p-1},$$

and let $\nu : x \mapsto (\sigma^c(x))_{c\in P}$ be the associated embedding of $\mathbb{K}$ in $\mathbb{K}_G$.

Let $x = \sum_{i=1}^{p-1} x_c\zeta^c, y = \sum_{i=1}^{p-1} y_c\zeta^c \in \mathbb{K}$. Then

$$\mathbf{Tr}(x\cdot y) = \mathbf{Tr}\left(\sum_{j=1}^{p-1} x_j y_{p-j} + \sum_{m=1}^{p-1}\zeta^m \sum_{j+k\equiv m \bmod p-1}\right) = p\cdot\sum_{j=1}^{p-1} x_j y_{p-j} - \mathbf{Tr}(x)\cdot\mathbf{Tr}(y).$$

We observe that the trace has a particularly simple form, if for instance $\mathbf{Tr}(y) = 0$. Thus

Lemma 15. *Notations being like above, let $x, y \in \mathbb{K}$ and assume that $\mathbf{Tr}(y) = 0$. Then*

$$\mathbf{Tr}(x\cdot\bar{y}) = p\cdot\langle\kappa(x),\kappa(y)\rangle,$$

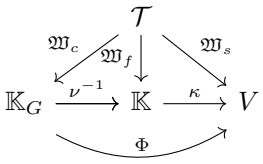
where $\langle\cdot,\cdot\rangle$ is the standard scalar product on $\mathbb{Q}^{p-1}$. The right hand side does not depend upon simultaneous permutations of the coefficients, so the coefficient map may also be κ.

We note that in the above trace we had to take the complex conjugate of y, in order to obtain the standard scalar product on the right hand side. At the same time, the left hand side becomes a non-degenerate hermitian bilinear form.

Let θ be fixed like above and $\mathcal{T} = G\theta$ be its orbit. We map the elements of $\mathcal{T}$ in the following way: A D-vector $\mathfrak{W}$ is a triple of maps

$$\begin{array}{rcl} \mathfrak{W}_c & = & G\to\mathbb{K}_G^{N'};\quad \mathfrak{W}_s = G\to V;\quad \mathfrak{W}_f = G\to\mathbb{K},\\ \nu^{-1} & : & \mathbb{K}_G\to\mathbb{K};\quad \kappa:\mathbb{K}\to V;\quad \Phi = \kappa\circ\nu^{-1}:\mathbb{K}_G\to V\\ & & (Gx)\mapsto x\mapsto(\kappa(x)),\end{array}\qquad (6.5)$$

such that the diagram commutes, as illustrated in the diagram below.



Thus the vector can be given by any of its three presentations, and the other two follow. We give some examples of D-vectors that we shall intensively use:

Examples 1.

a) The coefficients $b_n(t)$ in (6.4) give raise to a D-vector $\mathfrak{W}(b_n)$ presented in $\mathbb{K}$ by the map $\mathfrak{W}_f : t\in\mathcal{T}\mapsto b_n(t)$. We denote the image $(\mathfrak{W}(b_n)) =: \mathbf{b}_n \in V$.

b) We present here the standard base of V as a set of D-vectors

$$\Delta \quad = \quad \{\mathfrak{D}(i)\ :\ i = 1,2,\ldots,p-1\},\quad \textit{given by } \mathfrak{D}(i)_f :\mapsto \sigma^i(\zeta).$$

The standard base of V arises also as

$$\mathcal{E} = \{e_i\ :\ i\in P\} = (\mathfrak{D}(i)_c(\mathcal{T}))_{i=1}^{p-1}\subset V.$$

c) Let $\ell \in \mathbb{Z}[\zeta]$ be an indeterminate. It will be useful to impose the condition $\mathbf{Tr}(\ell) = 0$. For this we define the D-vector $\mathfrak{U}$ induced by $\mathfrak{W}_s(\mathfrak{U}) = U := (1, 1, \ldots, 1)$. The scalar product $\langle U, \kappa(\ell)\rangle = \mathbf{Tr}(\ell)$ and thus $\mathbf{Tr}(\ell) = 0$ iff $\kappa(\ell) \perp U$.

For $\vec{v} \in V$ we define the norm to be the one norm $||\vec{v}|| = ||\vec{v}||_1 = \max_{c\in P}(|v_c|)$ and for $w \in \mathbb{K}_G$ we define $||w|| = ||\Phi(w)||_1$.

Strategy of proof

The principle of our proof is the following: for the unknown ℓ we impose the conditions $\ell \perp U$ and $\ell \perp b_0$ and define

$$\mathfrak{d} := y \cdot \mathbf{Tr}(\mu(\theta) \cdot \bar{\ell}) \in \mathbb{Z}. \tag{6.6}$$

The choice of ℓ should assure that $\mathfrak{d} \neq 0$. Since the complex absolute value $|\mu(\sigma_c\theta)| = 1$ for all $c \in P$, assuming that $||\ell|| \leq L$ for some $L \in \mathbb{R}_{>0}$, we have the upper bound:

$$|\delta| < (p-1)|y|L < Q, \quad \text{if } L \leq Q^{1/2}. \tag{6.7}$$

It will suffice to let $L \leq Q^{1/2}$, in order to reach a contradiction. For this, we use

The Siegel box principle

This is a simple estimate for short non vanishing solutions of homogenous integer linear systems. The question being related to the one of successive minima in lattices, it has known since Siegel's original use – about hundred years ago – numerous developments in various heights and different number fields, the one of Bombieri and Vaaler [BV87] being the most frequently used. Due to the rational scalar product introduced above, we shall be able to apply here the original version of Siegel, which is related to the pigeon hole principle application we used in (5.5). It claims:

Lemma 16. *Let $A = (a_{i,j})_{i,j=1}^{r,s}$ be an integer matrix, with $r < s$ and entries bounded by $B = ||A||_1$. Then there is a solution $X = (X_1, X_2, \ldots, X_s) \in \mathbb{Z}^s \setminus \{0\}$, with norm*

$$||X||_1 \leq (sB)^{r/(s-r)}. \tag{6.8}$$

Under the same condition, Bombieri and Vaaler also prove

$$||X||_1 \leq \left(\sqrt{\det(AA^T)}\right)^{1/(s-r)}.$$

Finding ℓ

Let $\Lambda = \mathbb{Z}^{p-1} \subset V$ and $\mathbf{B} = \{x \in \Lambda \ : \ ||x|| \leq Q^{1/2}\}$. In view of the result of Bugeaud, Hanrot and Mignotte [BHM02], we may assume that $p \geq 29$. If A is an $r \times (p-1)$ matrix with $||A||_1 < Q$, and $r \leq 8$, then (6.8) implies that the system $AX = 0$ has at least one non trivial solution in Λ, with

$$||X|| < ((p-1)Q)^{8/20} < Q^{1/2}.$$

Here is how we use these degrees of freedom. First we impose the conditions $X \perp \mathcal{V}_0 := [U, \mathbf{b}_1(\theta)]_{\mathbb{Q}}$. The coefficients are clearly dominated by Q, so we let $X_1 \in \mathbf{B}$ be a non trivial solution. With this we let $\mathcal{V}_1 = \mathcal{V}_0 \oplus \mathbb{Q}X_1$, and find a further solution $X_2 \in \mathbf{B}^*$, which is in addition perpendicular to X_1. We may this way find at least six vectors $X_i \in \mathbf{B}^*$ which are mutually orthogonal and all orthogonal to $\mathcal{V}_0$. We shall use these degrees of freedom in order to find $\ell \in \mathbf{B}$, such that $\mathfrak{d} \neq 0$ in (6.6).

We note the following substitution, which leaves the sum invariant. For $\nu \in \Lambda$ we define

$$T_\nu(b_n, b_{n+1}) = (b_n + Q\nu, b_{n+1} - \nu). \tag{6.9}$$

The substitution replaces a pair of successive terms in the sequence of coefficients of the series, by leaving the sum in (6.4) unchanged. This follows immediately by considering the contribution of these terms:

$$Q^n \cdot (b_n + Qb_{n+1}) = Q^n(b_n + Q\nu + Q(b_{n+1} - \nu)).$$

In practice, $\nu \in \mathcal{E}$, the standard basis of V. Then, the modified coefficient $T_\nu(b_n)$ still verifies $|T_\nu(b_n)|_1 < 3/2Q$, while $|T_\nu(b_{n+1})|_1 < Q$.

The choice of ν uses the following

Lemma 17. *Let $\mathcal{E} = \{e_j : j = 1, \dots, p-1\}$ be the standard base of $V = \mathbb{Q}^{(p-1)}$ and let $x = (x_1, x_2, \dots, x_{p-1}) \in V$ have trace $\tau = \sum_{i=1}^{p-1} x_i$. Let $t \in \mathbb{Z} \setminus \{-\tau, 0\}$ and*

$$\mathcal{F}(t) := x + t\mathcal{E} := \{x + te_i \ : \ i = 1, 2, \dots, p-1\} \subset V$$

has span $F = [\mathcal{F}(t)]_{\mathbb{Q}}$ of dimension $\dim(F) = p - 1$.

Proof. Since the $p-2$ linearly independent vectors $t(e_1 - e_i) \in F; i = 2, 3, \dots, p-1$, it follows that $\dim(F) \geq p - 2$. Suppose that there is a vanishing linear combination $\sum_{i=1}^{p-1} \lambda_i(x + te_i) = 0$ and let $L := \sum_{i=1}^{p-1} \lambda_i$ be the "trace" of $\vec{\lambda} := \sum_{i \in P^*} \lambda_i e_i$. Unfolding the vanishing condition, we have

$$t\vec{\lambda} + Lx = \vec{0}.$$

If $L = 0$, then $t = 0$, which was excluded, or $\vec{\lambda} = \vec{0}$, so the linear combination was trivial to start with. If $L \neq 0$, we take traces again in the previous identity, and get $L(t + \tau) = 0$. Since $t \neq -\tau$, we obtain a contradiction, showing that the $\dim(F) = p - 1$ indeed. □

Let $S_0 = \mathbf{B}^* \cap \mathcal{V}_0^\perp$. We show that we may modify $\mathbf{b}_2$ by a substitution (6.9) in such a way, that $\mathbf{b}_2 \notin \mathcal{V}_0$ and there is at least one vector $z_0 \in S_0$ such that $z_0 \not\perp \mathbf{b}_2$. In view of Lemma 17 and since $\dim(S_0) > 4$, there is at least one translation of $\mathbf{b}_2$ by some base element $\nu \in Q\mathcal{E}$, which is not perpendicular to S_0. We assume thus that the condition is fulfilled, and use no new notation for the possibly modified coefficients $\mathbf{b}_2, \mathbf{b}_3$.

Let $\tau = \mathbf{Tr}(\mathbf{b}_2)$ and $t = 1$ if $\tau \leq 0$ and $t = -1$ otherwise. We define $w_j = \mathbf{b}_2 + te_j$ and $S^{(j)} = S_0 \cap w_j^\perp$. By Lemma 17, the w_j span V, and it follows that

$$\mathbb{Q} \cdot \left(\sum_{j \in P^*} S^{(j)} \right) \supset \mathbb{Q}S_0,$$

There is a set

$$\emptyset \neq J = \Big\{ j \in P^* \ : \ \mathbb{Q}(w_j^\perp \cap S_0) \not\subset \mathbb{Q}(\mathbf{b}_2^\perp \cap S_0) \Big\}.$$

A fortiori, there is a $j \in P^*$ such that $w_j^\perp \cap S_0 \not\subset (\mathbf{b}_2^\perp \cap S_0)$. For such j, we may choose $w \in S_0$ with $w \perp w_j$ but $w \not\perp \mathbf{b}_2$. We claim that $\ell = w$ satisfies our needs. Indeed, we have

$$\langle \mathbf{b}_2, \ell \rangle = \langle w_j, \ell \rangle - t\langle e_j, \ell \rangle = -t\ell_j \neq 0.$$

Consequently,

$$\mathfrak{d} \equiv Q^2(-pty\ell_j + O(Q)).$$

But $||pty\ell_j|| \leq |y|Q^{1/2} < Q$, and since the choice of ℓ_j ascertains that $\ell_j \neq 0$, it follows that $\mathfrak{d} \not\equiv 0 \bmod Q^3$ and a fortiori, $\mathfrak{d} \neq 0$. But $\mathfrak{d} \equiv 0 \bmod Q^2$ implies $|\mathfrak{d}| \geq Q^2$, which contradicts the upper bound (6.7).

The contradiction confirms the Proposition 8, hence completes the proof of the Theorem (8).

Chapter 7

General results about the primitive divisors for Lucas sequences

A *Lucas pair* is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity.

Given a Lucas pair (α, β), one defines the corresponding sequence of Lucas numbers by

$$\mathcal{L}_n := \mathcal{L}_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n \geq 0. \tag{7.1}$$

Two Lucas pairs (α, β), (α_1, β_1) are *equivalent* if $\alpha/\alpha_1 = \beta/\beta_1 = \pm 1$. For equivalent Lucas pairs we have $\mathcal{L}_n(\alpha, \beta) = \pm\mathcal{L}_n(\alpha_1, \beta_1)$. Therefore one of them has a primitive divisor if and only if the other has. Below we briefly review the history of this problem.

Let α, β be a Lucas pair. A prime number q is a *primitive divisor* of $\mathcal{L}_n$ if q divides $\mathcal{L}_n$ but does not divide $(\alpha - \beta)^2\mathcal{L}_1 \cdots \mathcal{L}_{n-1}$. In this case we call (α, β) as *n-defective Lucas*.

One of the oldest and important problems about Lucas pairs is the *existence of primitive divisor*.

The first result about the existence of primitive divisor problem goes back to 1892, Zsigmondy [Zsi92] proved that $\mathcal{L}_n(\alpha, \beta)$ has a primitive divisor for $n > 6$ provided that $\alpha, \beta \in \mathbb{Z}$ (6 is optimal here). In 1913 Carmichael [Car13] generalized Zsigmondy's result to real cases, he proved that if $\alpha, \beta \in \mathbb{R}$ is a real Lucas pair, then $\mathcal{L}_n(\alpha, \beta)$ has a primitive divisor for $n > 12$. For non-real Lucas pair the situation is much more complicated, in 1974 Schinzel [Sch74] prove the Lucas pair $\mathcal{L}_n(\alpha, \beta)$ has a primitive divisor for n exceeding an effectively computable absolute constant n_0. Shortly after, in 1977 Stewart [Ste77], compared with Schinzel's conclusion, gave an explicit solution. He showed that $n_0 = e^{452}4^{67}$ would work. The constant n_0 later was improved by Voutier to $2 \cdot 10^{10}$ in 1996 [Vou96] and to 30030 in 1998 [Vou98].

In 1995 Voutier [Vou95] showed the following useful result for $n \leq 30$.

Theorem 12 (Voutier 1995)**.** *Let $n \neq 6$ satisfy $4 < n \leq 30$. Then, up to equivalence, all n-defective Lucas pairs are of the form $\left((a-\sqrt{b})/2, (a+\sqrt{b})/2\right)$, where a, b are given in the following Table.*

n	(a,b)						
5	(1, 5)	(1, -7)	(2, -40)	(1, -11)	(1, -15)	(12, -76)	(12, -1364)
7	(1, -7)	(1, -19)					
8	(2, -24)	(1, -7)					
10	(2, -8)	(5, -3)	(5, -47)				
12	(1, 5)	(1, -7)	(1, -11)	(2, -56)	(1, -15)	(1, -19)	
13	(1, -7)						
18	(1, -7)						
30	(1, -7)						

In 2001, Bilu, Hanrot and Voutier [BHV01] made an outstanding contribution to the problem of existence of primitive divisor, they showed the following theorem.

Theorem 13 (Bilu, Hanrot and Voutier 2001)**.** *Every integer $n > 30$ is totally non-defective.*

Combining Theorem (12) with Theorem (13), one can obtain

Theorem 14. *Let p is prime and suppose that $p \notin \{2, 3, 5, 7, 13\}$. Then $\mathcal{L}_p$ has a primitive divisor.*

The following statement is well-known, but we give a short proof here for the reader's convenience.

Proposition 9. *A primitive divisor q of $\mathcal{L}_n$ satisfies $q \equiv \pm 1 \pmod{n}$.*

Proof. If $\alpha, \beta \in \mathbb{Z}$, since q does not divide either α or β, the order of α/β in the group $\mathbb{F}_q^\times$ is exactly n. So $n \mid q-1$.

Now assume $M := \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ is a quadratic field. If q ramifies in $\mathcal{O}_M$, then $q \mid (\alpha - \beta)^2$ By definition of primitive divisor, this can not happen. Let $\overline{\alpha/\beta}$ be the image of α/β in the residue fields appearing below. If q splits in $\mathcal{O}_M$, say $q = \mathfrak{p}_1\mathfrak{p}_2$, then $\mathfrak{p}_1 \mid \mathcal{L}_n$ but $\mathfrak{p}_1 \nmid \mathcal{L}_t$ for $t < n$. The order of $\overline{\alpha/\beta}$ in the group $(\mathcal{O}_M/\mathfrak{p}_1)^\times \cong \mathbb{F}_q^\times$ is again n and so $n \mid q-1$. If q is inert in $\mathcal{O}_M$, the order of $\overline{\alpha/\beta}$ in the group $(\mathcal{O}_M/q)^\times \cong \mathbb{F}_{q^2}^\times$ is n, we have $n \mid q^2 - 1$. The subgroup

$$\left\{ s \in \mathbb{F}_{q^2}^\times : \mathcal{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(s) = 1 \right\}$$

is of order $(q^2-1)/(q-1) = q+1$ because this norm map is surjective. $\overline{\alpha/\beta}$ is in this subgroup, we must have $n \mid q+1$. □

Remark 2. *If Lucas pair* $(\alpha, \beta) \notin \mathbb{Z}^2$ *and assume that* $\mathcal{L}_n$ *has a primitive divisor* q*. Let* $M = \mathbb{Q}(\alpha)$*. Then from the proof of Proposition 9 we see that* q *is not ramified in* M *and*

$$\begin{cases} q \equiv 1 \bmod n & \text{if } q \text{ splits in } M \\ q \equiv -1 \bmod n & \text{if } q \text{ is inert in } M. \end{cases} \tag{7.2}$$

Chapter 8

The Diophantine equation $x^2 + C = y^p$

8.1 Background

In this section we assume that $(x, y) \in \mathbb{N}^2$ is a solution of (1.13), where $\gcd(x, y) = 1$. We prove in this section two results that we will use to associate with a Lucas sequence in the proof of our main result in the next section.

Proposition 10. *As notations in Theorem 9. The ideals* $\mathfrak{a} := (x + z\sqrt{-d})$ *and* $\overline{\mathfrak{a}} := (x - z\sqrt{-d})$ *are coprime in* $\mathcal{O}_K$.

Proof. We factorize (1.13) in $\mathcal{O}_K$ as

$$(x + z\sqrt{-d}) \cdot (x - z\sqrt{-d}) = y^p \tag{8.1}$$

By our assumption that $d \not\equiv -1 \bmod 8$, we must have $2 \nmid y$. For if $2 \mid y$, we get $2 \nmid x$ and $C = y^p - x^2 \equiv -1 \bmod 8$, then $d \equiv -1 \bmod 8$.

Note the ideal $\mathfrak{a} + \overline{\mathfrak{a}}$ contains elements $2x$ and y^p. Since $2 \nmid y$, we have $\gcd(2x, y^p) = 1$, thus $\mathfrak{a} + \overline{\mathfrak{a}} = \mathcal{O}_K$. □

Proposition 11. *As notations in Theorem 9. Let* $\alpha \in \mathcal{O}_K$ *such that* $\alpha^p = x + z\sqrt{-d}$ *with* $x, z > 0$. *Then* $\alpha/\overline{\alpha}$ *is not a root of unity in* K.

Proof. By Dirichlet's unit theorem we have $\mathcal{O}_K^\times = W_K$, where W_K is the set of roots of unity in K. More precisely,

$$W_K = \begin{cases} \{\pm 1, \pm i\} & \text{if} \quad d = -1 \\ \{\pm 1, (\pm 1 \pm \sqrt{-3})/2\} & \text{if} \quad d = -3 \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

As $\alpha^p = x + z\sqrt{-d}$ with $x, z > 0$, write $\alpha^p = r\exp(i\varphi)$ with $r > 0$ and $0 < \varphi < \pi/2$, then $\overline{\alpha}^p = r\exp(-i\varphi)$. It is easy to see that $\zeta \in W_K$ satisfying $\zeta \cdot \overline{\alpha}^p = \alpha^p$ must belong to the set $\{\exp(i\theta), \theta = \pi/3, \pi/2, 2\pi/3\}$.

We show all these cases are impossible.

- $\theta = \pi/3$, $\alpha^p = \frac{1+\sqrt{-3}}{2} \cdot \overline{\alpha}^p$, so $z\sqrt{d} \cdot \sqrt{3} = x$, we must have $d = 3$. Then $x = 3z$. Note that $\gcd(x, y) = 1$, by equation (8.1) we have $z = 1$. Thus $x = 3$ and $y^p = 12$, impossible.
- $\theta = \pi/2$, $\alpha^p = i\overline{\alpha}^p$, that is, $x + z\sqrt{-d} = z\sqrt{d} + xi$, so $x = z\sqrt{d}$. Then d must be 1. By (8.1), we get $x = 1$ and $y^p = 2$, impossible.
- $\theta = 2\pi/3$, $\alpha^p = \frac{-1+\sqrt{-3}}{2} \cdot \overline{\alpha}^p$, we get $z\sqrt{d} = x \cdot \sqrt{3}$, so $d = 3$. By (8.1), we must have $x = 1$. This yields $y^p = 4$, which is impossible since $p \geq 5$.

□

8.2 Proof of Theorem 9

In the following, we assume that $(x, y) \in \mathbb{N}^2$ is a solution of equation (1.13), where $\gcd(x, y) = 1$. We factorize (1.13) in $\mathcal{O}_K$ as

$$(x + z\sqrt{-d}) \cdot (x - z\sqrt{-d}) = y^p \tag{8.2}$$

Proposition 10 shows that $\mathfrak{a} := (x + z\sqrt{-d})$ and $\overline{\mathfrak{a}} := (x - z\sqrt{-d})$ are coprime in $\mathcal{O}_K$. Therefore by the unique factorization of ideals, $x + z\sqrt{-d}$ can be expressed as a p-th power of some ideal $\mathfrak{I} \subseteq \mathcal{O}_K$. Because $p \nmid h_K$, such $\mathfrak{I}$ is principal. Since $|\mathcal{O}_K^\times| \in \{2, 4, 6\}$ is coprime with p, any unit of $\mathcal{O}_K$ can be written as a p-th power in $\mathcal{O}$. It follows that

$$x + z\sqrt{-d} = \alpha^p, \quad x - z\sqrt{-d} = \overline{\alpha}^p, \quad \alpha\overline{\alpha} = y \tag{8.3}$$

for some $\alpha \in \mathcal{O}_K$. Further note that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}[(1 + \sqrt{-d})/2] & \text{if} \quad -d \equiv 1 \bmod 4 \\ \mathbb{Z} + \mathbb{Z}[\sqrt{-d}] & \text{if} \quad -d \equiv 2, 3 \bmod 4. \end{cases}$$

Therefore there exist $u, v \in \mathbb{Z}$ such that

$$\alpha = \begin{cases} (u + v\sqrt{-d})/2 & \text{if} \quad -d \equiv 1 \bmod 4 \\ u + v\sqrt{-d} & \text{if} \quad -d \equiv 2, 3 \bmod 4. \end{cases} \tag{8.4}$$

Then

- If $-d \equiv 1 \bmod 4$, we have $\alpha + \overline{\alpha} = u$, $\alpha - \overline{\alpha} = v\sqrt{-d}$.
- If $-d \equiv 2, 3 \bmod 4$, we have $\alpha + \overline{\alpha} = 2u$, $\alpha - \overline{\alpha} = 2v\sqrt{-d}$.

In both cases $\alpha^p - \overline{\alpha}^p = 2z\sqrt{-d}$, $\alpha^p + \overline{\alpha}^p = 2x$ hold and we have the following claims.

Obviously $\gcd(\alpha + \overline{\alpha}, \alpha\overline{\alpha}) = 1$. This is because $\gcd(\alpha + \overline{\alpha}, \alpha\overline{\alpha}) \mid \gcd(\alpha^p + \overline{\alpha}^p, \alpha\overline{\alpha}) = \gcd(2x, y) = 1$.

This fact and Proposition 11 together show that $(\alpha, \overline{\alpha})$ is a Lucas pair, the Lucas sequences $\mathcal{L}_n$ associated with $(\alpha, \overline{\alpha})$ is defined by

$$\mathcal{L}_n := \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}}. \tag{8.5}$$

In particular, when $n = p$,

$$\mathcal{L}_p := \frac{\alpha^p - \overline{\alpha}^p}{\alpha - \overline{\alpha}} = \begin{cases} (2z)/v & \text{if} \quad -d \equiv 1 \bmod 4 \\ z/v & \text{if} \quad -d \equiv 2, 3 \bmod 4. \end{cases} \tag{8.6}$$

Hence $(2z)/v \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$.

[BHV01] confirms the existence of primitive divisors of $\mathcal{L}_p$ when $p \notin \{5, 7, 13\}$. Hence for $p \notin \{5, 7, 13\}$, we choose a primitive divisor of $\mathcal{L}_p$, denoted by q. In view of Proposition 9 we have

$$p \mid q \pm 1, \quad q \mid 2z. \tag{8.7}$$

There are no such primes p, q satisfying (8.7) by the assumption.

We now turn to remain cases when primitive divisors may not exist.

8.2.1 The case $p = 5$

Let $\alpha = (a + \sqrt{b})/2$, by Theorem (12), $\mathcal{L}_5$ has no primitive divisor if only if

$$\pm(a, \pm b) \in \Big\{(1, 5), (1, -7), (2, -40), (1, -11), (1, -15), (12, -76), (12, -1364)\Big\}.$$

We have plus-minus sign before the brackets since the result of is up to equivalence.

- If $\alpha = \pm(1 \pm \sqrt{5})/2$, then

  $$\alpha^5 = \pm\frac{11 \pm 5\sqrt{5}}{2} = x + z\sqrt{-d}.$$

  This is impossible since 11 is not even.

- If $\alpha = \pm(1 \pm \sqrt{-7})/2$, then

  $$\alpha^5 = \pm\frac{11 \pm \sqrt{-7}}{2} = x + z\sqrt{-d},$$

  impossible.

- If $\alpha = \pm(2 \pm \sqrt{-40})/2$, then

  $$\alpha^5 = \pm 401 \pm 5\sqrt{-10} = x + z\sqrt{-d},$$

  so $x = 401, z = 5, d = 10$ and $C = 250, y = 11$.

  In this case, $(x, y, C, p) = (401, 11, 250, 5)$ and $z = 5, d = 10, K = \mathbb{Q}(\sqrt{-10})$. Therefore $h_K = 2$, C even and $5 \nmid (5 \pm 1)$. Thus the assumptions of Theorem (9) satisfied and we have a solution.

- If $\alpha = \pm(1 \pm \sqrt{-11})/2$, then

$$\alpha^5 = \pm\frac{31 \pm \sqrt{-11}}{2} = x + z\sqrt{-d},$$

impossible.

- If $\alpha = \pm(1 \pm \sqrt{-15})/2$, then

$$\alpha^5 = \pm\frac{61 \pm 5\sqrt{-15}}{2} = x + z\sqrt{-d},$$

impossible.

- If $\alpha = \pm(12 \pm \sqrt{-76})/2$, then

$$\alpha^5 = \pm 22434 \pm \sqrt{-19} = x + z\sqrt{-d},$$

so $x = 22434, z = 1, d = 19$ and $C = 19, y = 55$.

In this case, $(x, y, C, p) = (22434, 55, 19, 5)$ and $z = 1, d = 19, K = \mathbb{Q}(\sqrt{-19})$. Therefore $h_K = 1$, $d \equiv 3 \bmod 8$ and z has no prime divisor. Therefore the assumptions of Theorem (9) satisfied and we get a solution.

- If $\alpha = \pm(12 \pm \sqrt{-1364})/2$, then

$$\alpha^5 = \pm 2759646 \pm \sqrt{-341} = x + z\sqrt{-d},$$

so $x = 2759646, z = 1, d = 341$ and $C = 341, y = 377$.

In this case, $(x, y, C, p) = (2759646, 377, 341, 5)$ and $z = 1, d = 341, K = \mathbb{Q}(\sqrt{-341})$. Therefore $h_K = 28$, $d \equiv 5 \bmod 8$ and z has no prime divisor. The assumptions of Theorem (9) satisfied.

8.2.2 The case $p = 7$

Let $\alpha = (a + \sqrt{b})/2$, in view of Theorem (12), $\mathcal{L}_7$ has no primitive divisor if only if

$$\pm(a, \pm b) \in \Big\{(1, -7)(1, -19)\Big\}.$$

- If $\alpha = \pm(1 \pm \sqrt{-7})/2$, then

$$\alpha^7 = \pm\frac{-13 \pm 7\sqrt{-7}}{2} = x + z\sqrt{-d}.$$

This is impossible again since 13 is not even.

- If $\alpha = \pm(1 \pm \sqrt{-19})/2$, then

$$\alpha^7 = \pm\frac{-559 \pm \sqrt{-19}}{2} = x + z\sqrt{-d},$$

impossible.

8.2.3 The case $p = 13$

Let $\alpha = (a + \sqrt{b})/2$, recall Theorem (12), $\mathcal{L}_{13}$ has no primitive divisor if only if

$$\pm(a, \pm b) = (1, -7).$$

Then

$$\alpha^{13} = \pm\frac{-181 \pm \sqrt{-7}}{2} = x + z\sqrt{-d},$$

impossible.

Combine all these cases together we complete the proof of Theorem 9.

8.3 Proof of Theorem 10

Write $C = z^2 \cdot d$ with $d > 0$ square. Then $d \in \{1, 2, 17, 34, 41, 82, 697, 1394\}$ and let $K = \mathbb{Q}(\sqrt{-d})$. Denoted by $h(-d)$ the class number of K. Reading the equation (10) modulo 8 yields y is odd. Now we check the the first two assumptions of Theorem 9.

We have the following table for $h(-d)$.

$h(-1) = h(-2) = 1$
$h(-17) = h(-34) = h(-82) = 4$
$h(-41) = h(-697) = 8$
$h(-1394) = 48$

Therefore we see that $p \nmid h(-d)$ when $p \geq 5$.

Assume that $(x, y) \in \mathbb{N}^2$ is a solution of (10), in view of Theorem 9 and its proof, we separate into two cases, depending whether $\mathcal{L}_p$ has a primitive divisor or not.

If $\mathcal{L}_p$ has no primitive divisor, as in the proof of Theorem 9 we list all the possible solutions and no C of these solution is of the form $2^a \cdot 17^b \cdot 41^c$, hence (10) has no solution in this case.

Now assume $\mathcal{L}_p$ has a primitive divisor q. We have $q \mid 2z$ and $p \mid q \pm 1$. Note that the prime divisor q of $2z$ belongs to $\{2, 17, 41\}$. The only possibilities for p, q are $(p, q) = (5, 41)$ and $(p, q) = (7, 41)$.

8.3.1 The case $p = 5$

We have $(p, q) = (5, 41)$ in this case, $q \equiv 1 \bmod p$. By Remark 2 we see q splits in $K = \mathbb{Q}(\sqrt{-d})$. Therefore $d = 1$ or $d = 2$.

If $d = 1$:

In this case, (8.3) becomes

$$x + z\sqrt{-1} = (u + v\sqrt{-1})^5, u, v \neq 0,$$

and equating the imaginary parts gives

$$v(5u^4 - 10u^2v^2 + v^4) = 2^{a_0} \cdot 17^{b_0} \cdot 41^{c_0}. \tag{8.8}$$

Note that $\gcd(q, (\alpha - \overline{\alpha})^2) = \gcd(q, -4v^2) = 1$ by the definition of primitive divisor. Therefore $\gcd(v, 41) = 1$ and

$$v \mid 2^{a_0} \cdot 17^{b_0}.$$

If $2 \mid v$, then u is odd since $y = u^2 + v^2$ is odd. Hence (8.8) can be reduced to

$$5u^4 - 10u^2v^2 + v^4 = \pm 17^{b_1} \cdot 41^{c_1} \tag{8.9}$$

for some $b_1 \leq b_0, c_1 \leq c_0$. Reading (8.9) modulo 8 it is easy to see that it has no solution.

If $v = \pm 1$, u is even so $a_0 = 0$. We get

$$5u^4 - 10u^2 + 1 = \pm 17^{b_0} \cdot 41^{c_0}. \tag{8.10}$$

The sign on the right hand side is positive if we consider the equation modulo 8.

Using SageMath[The22] one sees that (8.10) has a solutions $\{(u, b_0, c_0) = (\pm 2, 0, 1)\}$, which gives $y = 5$ and $x = 38$. So we get a solution

$$(x, y, C, p) = (38, 5, 1681, 5).$$

If $v = \pm 17^{b_2}$ for some $b_2 \in \mathbb{N}^+$, u is even, (8.8) reduced to

$$5u^4 - 10u^2 \cdot 17^{2b_2} + 17^{4b_2} = \pm 41^{c_2}. \tag{8.11}$$

for some $b_2 \leq b_0, c_2 \leq c_0$. The sign on the right hand side is positive if we consider the equation modulo 4. Now SageMath tells us that (8.11) has a solution $\{(u, b_2, c_2) = (\pm 2, 0, 1)\}$, which would imply the same solution $(x, y, C, p) = (38, 5, 1681, 5)$ as above.

If $d = 2$:

In this case, (8.3) becomes

$$x + z\sqrt{-2} = (u + v\sqrt{-2})^5$$

and equating the imaginary parts gives

$$v(5u^4 - 20u^2v^2 + 4v^4) = 2^{a_0} \cdot 17^{b_0} \cdot 41^{c_0}. \tag{8.12}$$

As in the case of the equation (8.8), $\gcd(v, 41) = 1$ and

$$v \mid 2^{a_0} \cdot 17^{b_0}.$$

If $2 \mid v$, then u is odd since $y = u^2 + v^2$ is odd. Hence (8.12) can be reduced to

$$5u^4 - 20u^2v^2 + 4v^4 = \pm 17^{b_1} \cdot 41^{c_1} \tag{8.13}$$

for some $b_1 \leq b_0, c_1 \leq c_0$. Reading (8.13) modulo 8 it is easy to see that it has no solution.

If $v = \pm 1$, u is even and so $a_0 = 0$. We get

$$5u^4 - 20u^2 + 4 = \pm 2^{a_0} \cdot 17^{b_0} \cdot 41^{c_0}. \tag{8.14}$$

Therefore $a_0 = 2$ and the sign on the right hand side is positive if we consider the equation modulo 4.

Using SageMath we see that (8.14) has solutions $\{(u, b_0, c_0) = (\pm 2, 0, 0)\}$, which gives $y = u^2 + v^2 = 5$ and $C = z^2 \cdot d = 16 \cdot 2 = 32$. But then $y^5 - C$ is not a square, contradiction.

If $v = \pm 17^{b_2}$ for some $b_2 \in \mathbb{N}^+$, u is even, (8.12) reduced to

$$20(u/2)^4 - 5u^2 \cdot 17^{2b_2} + 17^{4b_2} = \pm 41^{c_2}. \tag{8.15}$$

for some $b_2 \leq b_0, c_2 \leq c_0$. The sign on the right hand side is positive if we consider the equation modulo 4. Using SageMath would deduce that (8.15) has no solution.

Therefore we show that there is only one solution $(x, y, C, p) = (38, 5, 1681, 5)$ if $p = 5$.

Thus we also complete the proof of Theorem (10).

Bibliography

[AM02] S.A. Arif and F.S.A. Muriefah. On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *Journal of Number Theory*, 95(1):95–100, 2002.

[BBM14] Y. Bilu, Y. Bugeaud, and M. Mignotte. *The problem of Catalan*, volume 9. Springer, 2014.

[BH00] Y. Bugeaud and G. Hanrot. Un nouveau critère pour l'équation de Catalan. *Mathematika*, 47(1-2):63–73, 2000.

[BHM02] Y. Bugeaud, G. Hanrot, and M. Mignotte. Sur l'équation diophantienne $(x^n - 1)/(x - 1) = y^q$, III. *Proceedings of the London Mathematical Society*, 84(1):59–78, 2002.

[BHV01] Yu. Bilu, G. Hanrot, and P.M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[BL15] M.A. Bennett and A. Levin. The Nagell–Ljunggren equation via Runge's method. *Monatshefte für Mathematik*, 177(1):15–31, 2015.

[BM99] Y. Bugeaud and M. Mignotte. On the Diophantine equation $(x^n - 1)/(x - 1) = y^q$, II. *Comptes Rendus de l'Academie des Sciences Series I Mathematics*, 9(328):741–744, 1999.

[BM07] Y. Bugeaud and P. Mihăilescu. On the Nagell-Ljunggren equation. *Mathematica Scandinavica*, pages 177–183, 2007.

[BMR00] Y. Bugeaud, M. Mignotte, and Y. Roy. On the Diophantine equation $(x^n - 1)/(x - 1) = y^q$. *Pacific journal of mathematics*, 193(2):257–268, 2000.

[BMS06] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential diophantine equations II. the Lebesgue–Nagell equation. *Compositio Mathematica*, 142(1):31–62, 2006.

[BP08] A. Bérczes and I. Pink. On the Diophantine equation $x^2 + p^{2k} = y^n$. *Archiv der Mathematik*, 91(6):505–517, 2008.

[BP12] A. Bérczes and I. Pink. On the Diophantine equation $x^2 + d^{2l+1} = y^n$. *Glasgow Mathematical Journal*, 54(2):415–428, 2012.

[BV87] E. Bombieri and J.D. Vaaler. Polynomials with low height and prescribed vanishing. In *Analytic Number Theory and Diophantine Problems: Proceedings of a Conference at Oklahoma State University, 1984*, pages 53–73. Springer, 1987.

[Car13] R.D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *The Annals of Mathematics*, 15(1/4):49–70, 1913.

[Cas60] J.W.S. Cassels. On the equation $a^x - b^y = 1$. II. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 56, pages 97–103. Cambridge University Press, 1960.

[CDI+13] I. Cangül, M. Demırcı, I. Inam, F. Luca, and G. Soydan. On the Diophantine equation $x^2 + 2^a 3^b 11^c = y^n$. *Mathematica Slovaca*, 63(3):647–659, 2013.

[CDST10] I.N. Cangül, M. Demirci, G. Soydan, and N. Tzanakis. On the Diophantine equation $x^2+5^a 11^b = y^n$. *arXiv preprint arXiv:1001.2525*, 2010.

[CHS21] K. Chakraborty, A. Hoque, and R. Sharma. On the solutions of certain Lebesgue–Ramanujan–Nagell equations. *Rocky Mountain Journal of Mathematics*, 51(2):459–471, 2021.

[Coh92] J.H.E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. *Archiv der Mathematik*, 59:341–344, 1992.

[Coh93] J.H.E. Cohn. The Diophantine equation $x^2 + C = y^n$. *Acta Arithmetica*, 65(4):367–381, 1993.

[Dup07] B. Dupuy. A class number criterion for the equation $(x^p - 1)/(x - 1) = py^q$. *Acta Arithmetica*, 127(4):391–401, 2007.

[DW14] H. Di and G. Wenji. A note on the Diophantine equation $(x^p - 1)/(x-1) = p^e y^q$. *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie*, pages 35–43, 2014.

[EDA12] L. Euler, A. Diener, and A. Aycock. Theorematum quorundam arithmeticorum demonstrationes. *arXiv preprint arXiv:1202.3808*, 2012.

[Eve83] J. Evertse. Upper bounds for the numbers of solutions of Diophantine equations. *MC Tracts*, 1983.

[Ger57] G.C. Gerono. Sur la résolution en nombres entiers et positifs de lâéquation $x^m = y^n + 1$. nouv. *Ann. Math*, 16:394–398, 1857.

[Gha19] A. Ghadermarzi. On the Diophantine equations $x^2 + 2^\alpha 3^\beta 19^\gamma = y^n$ and $x^2 + 2^\alpha 3^\beta 13^\gamma = y^n$. *Mathematica Slovaca*, 69(3):507–520, 2019.

[GMOS94] A.M.W. Glass, D.B. Meronk, T. Okada, and R.P. Steiner. A small contribution to Catalan's equation. *Journal of Number Theory*, 47(2):131–137, 1994.

[GMT16] H. Godinho, D. Marques, and A. Togbé. On the Diophantine equation $x^2 + C = y^n$ for $C = 2^a 3^b 17^c$ and $c = 2^a 13^b 17^c$. *Mathematica Slovaca*, 66(3):565–574, 2016.

[Ham56] R. Hampel. On the solution in natural numbers of the equation $x^m - y^n = 1$. *Ann. Polon. Math*, 3:1–4, 1956.

[HS16] A. Hoque and H.K. Saikia. On the divisibility of class numbers of quadratic fields and the solvability of Diophantine equations. *SeMA Journal*, 73:213–217, 2016.

[Ink64] K. Inkeri. On Catalan's problem. *Acta arithmetica*, 9(3):285–290, 1964.

[Ink72] K. Inkeri. On the Diophantine equation $\alpha(x^n - 1)/(x - 1) = y^m$. *Acta Arithmetica*, 21(1):299–311, 1972.

[Ink90] K. Inkeri. On Catalan's conjecture. *Journal of number theory*, 34(2):142–152, 1990.

[Ko65] C. Ko. On the Diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica*, 14:457–460, 1965.

[L+02] F. Luca et al. On the equation $x^2+2^a 3^b = y^n$. *International Journal of Mathematics and Mathematical Sciences*, 29:239–244, 2002.

[Le02] M. Le. On Cohn's conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$. *Archiv der Mathematik*, 78(1):26–35, 2002.

[Leb50] V.A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, nouv. *Ann. Math*, 9(9):178–181, 1850.

[Lju43] W. Ljunggren. Noen setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$. *Norsk. Mat. Tidsskr*, 25(1):17–20, 1943.

[LT08] F. Luca and A. Togbé. On the Diophantine equation $x^2+2^a 5^b = y^n$. *International Journal of Number Theory*, 4(06):973–979, 2008.

[LT09] F. Luca and A. Togbé. On the diophantine equation $x^2+2^a 13^b = y^n$. In *Colloquium Mathematicum*, volume 116, pages 139–146. Instytut Matematyczny Polskiej Akademii Nauk, 2009.

[MdW96] M. Mignotte and B.M.M de Weger. On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$. *Glasgow Mathematical Journal*, 38(1):77–85, 1996.

[Mig92] M. Mignotte. Sur l'équation de Catalan. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 314(3):165–168, 1992.

[Mig01] Maurice Mignotte. Catalan's equation just before 2000. *Number theory (Turku, 1999)*, pages 247–254, 2001.

[Mih03] P. Mihăilescu. A class number free criterion for Catalan's conjecture. *Journal of Number theory*, 99(2):225–231, 2003.

[Mih04] P. Mihailescu. Primary cyclotomic units and a proof of Catalans conjecture. 2004.

[Mih06] P. Mihăilescu. On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation. *Journal of number theory*, 118(1):123–144, 2006.

[Mih07] P. Mihăilescu. New bounds and conditions for the equation of Nagell–Ljunggren. *Journal of Number Theory*, 124(2):380–395, 2007.

[MR95] M. Mignotte and Y. Roy. Catalan's equation has no new solution with either exponent less than 10651. *Experimental Mathematics*, 4(4):259–268, 1995.

[MR97a] M. Mignotte and Y. Roy. Lower bounds for Catalan's equation. *The Ramanujan Journal*, 1(4):351–356, 1997.

[MR97b] M. Mignotte and Y. Roy. Minorations pour l'équation de Catalan. *Comptes Rendus de l'Académie des Sciences-Series I-Mathematics*, 324(4):377–380, 1997.

[Nag20] T. Nagell. Note sur l'équation indéterminée $(x^n - 1)/(x - 1) = y^q$. *Norsk. Mat. Tidsskr*, 2:75–78, 1920.

[Nag21] T. Nagell. Des équations indéterminées $x^2+x+1 = y^n$ et $x^2+x+1 = 3y^n$. *Norsk matem. forenings skrifter I*, 2:14, 1921.

[PR11] I. Pink and Z. Rábai. On the Diophantine equation $x^2+5^k17^l = y^n$. *Communications in Mathematics*, 19(1):1–9, 2011.

[Ray22] S.G. Rayaguru. On the Diophantine equation $x^2 + C = y^n$. *Indian Journal of Pure and Applied Mathematics*, pages 1–9, 2022.

[Rib94] P. Ribenboim. Catalan's conjecture. *Séminaire de Philosophie et Mathématiques*, (6):1–11, 1994.

[Sch74] A. Schinzel. Primitive divisors of the expression $a^n - b^n$ in algebraic number fields. 1974.

[Sch95] W. Schwarz. A note on Catalan's equation. *Acta Arithmetica*, 72(3):277–279, 1995.

[Sch10] R. Schoof. *Catalan's conjecture*. Springer Science & Business Media, 2010.

[Sho00] T.N. Shorey. Exponential Diophantine equations involving products of consecutive integers and related equations. In *Number theory*, pages 463–495. Springer, 2000.

[ST86] T.N. Shorey and R. Tijdeman. *Exponential Diophantine equations*. Cambridge University Press, 1986.

[Ste77] C.L. Stewart. Primitive divisors of Lucas and Lehmer numbers. *Transcendence theory: advances and applications*, pages 79–92, 1977.

[Tha88] F. Thaine. On the ideal class groups of real abelian number fields. *Annals of mathematics*, 128(1):1–18, 1988.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022. `https://www.sagemath.org`.

[Tij76] R. Tijdeman. On the equation of Catalan. *Acta Arithmetica*, 29:197–209, 1976.

[Tij86] R. Tijdeman. Exponential Diophantine equations. *Number Theory*, page 523, 1986.

[Vou95] P.M. Voutier. Primitive divisors of Lucas and Lehmer sequences. *mathematics of computation*, 64(210):869–888, 1995.

[Vou96] P.M. Voutier. Primitive divisors of Lucas and Lehmer sequences, II. *Journal de théorie des nombres de Bordeaux*, 8(2):251–274, 1996.

[Vou98] P.M. Voutier. Primitive divisors of Lucas and Lehmer sequences, III. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 123, pages 407–419. Cambridge University Press, 1998.

[Zsi92] K. Zsigmondy. Zur theorie der potenzreste. *Monatshefte für Mathematik und Physik*, 3:265–284, 1892.