Résolution de certaines équations diophantiennes et propriétés de certains polynômes

Thèse

Jesse Larone

Doctorat en mathématiques
Philosophiæ doctor (Ph. D.)

Québec, Canada

Résolution de certaines équations diophantiennes et propriétés de certains polynômes

Thèse

Jesse Larone

Sous la direction de:

Antonio Lei, directeur de recherche
Claude Levesque et Omar Kihel, codirecteurs de recherche

Résumé

Dans les quatre premiers chapitres de cette thèse, nous abordons quelques équations diophantiennes et leurs solutions. On démontre que l'équation $y^2 = px(Ax^2 + 2)$ n'admet qu'un maximum de six solutions entières où p est nombre premier et $A > 1$ est entier impair ; on démontre que l'équation $\mathrm{Res}_x\big(P(x), x^2 + sx + t\big) = a$ n'admet qu'un nombre fini de solutions (s, t) pour P un polynôme fixe et a un entier autre que zéro ; on résout l'équation $F_n - F_m = y^a$ lorsque $y \in \{6, 11, 12\}$ et on trouve une borne pour les solutions de $F_n + F_m = y^a$ dans le cas général ; et on démontre que si un nombre suffisant d'entiers x consécutifs existent tels que $P(x)$ est sous la forme m^q lorsque $q \geq 2$ est diviseur de $\deg P$, alors $P = R^q$ pour un certain polynôme R, ce qui nous permet de déduire l'existence d'une infinité de solutions à $y^q = P(x)$ à partir d'un nombre fini de telles solutions dans certains cas.

Dans les six derniers chapitres, nous abordons plusieurs sujets reliés à la décomposition d'objects algébriques. Parmi les résultats, on présente quelques conditions sous lesquelles un polynôme ne peut pas être exprimé comme une composition de deux polynômes de degré inférieur ; on présente une nouvelle démonstration du théorème Carltiz-Lutz sur les polynômes de permutations ; on étudie la possibilité d'exprimer un polynôme comme une somme composée ou un produit composé de deux autres polynômes de degré inférieur ; on trouve une borne pour un des plus petits nombres premiers qui se décompose dans un corps imaginaire quadratique donné ; et on étudie la possibilité de recouvrir un anneau avec ses sous-anneaux.

Abstract

The first four chapters of this thesis address some Diophantine equations and their solutions. We prove that the equation $y^2 = px(Ax^2 + 2)$ has at most six integer solutions (x, y) for p a prime and $A > 1$ an odd integer; we prove that the equation $\mathrm{Res}_x\big(P(x), x^2 + sx + t\big) = a$ has only finitely many integer solutions (s, t) for a fixed polynomial P and nonzero integer a; we completely solve the equation $F_n - F_m = y^a$ for $y \in \{6, 11, 12\}$ and bound the solutions for $F_n + F_m = y^a$ in general; and we prove that the existence of sufficiently many consecutive integers x such that $P(x)$ is of the form m^q for $q \geq 2$ dividing $\deg P$ implies that R^q for some polynomial R, providing criteria for deducing the existence of infinitely many solutions to $y^q = P(x)$ from the existence of finitely many solutions in some cases.

In the last six chapters, we address various algebraic decomposition related topics. Among other results, we provide criteria which guarantee a polynomial cannot be written as a composition of two polynomials of smaller degree; we provide a new proof of the Carlitz-Lutz theorem on permutation polynomials; we study the possibility of expressing a polynomial as the composed sum or composed multiplication of two polynomials of smaller degree; we bound from below some of the smallest primes which split in an imaginary quadratic field; and we study the possibility of covering a ring with its subrings.

Contents

Résumé ii

Abstract iii

Contents iv

Acknowledgements vii

Foreword viii

Introduction 1

1 On the equation $\mathbf{Res}_x\big(P(x), x^2 + sx + t\big) = a$ 4
- 1.1 Résumé . . . 4
- 1.2 Abstract . . . 4
- 1.3 Introduction . . . 4
- 1.4 Preliminaries . . . 6
- 1.5 The irreducibility of the polynomial $R(s,t) - a$, for a fixed in $\mathbb{Z} \setminus \{0\}$ . . . 9
- 1.6 Application of Runge method . . . 10
- 1.7 Bibliography . . . 11

2 The number of solutions to $y^2 = px(Ax^2 + 2)$ 13
- 2.1 Résumé . . . 13
- 2.2 Abstract . . . 13
- 2.3 Introduction . . . 14
- 2.4 Preliminary results . . . 16
- 2.5 Main results . . . 17
- 2.6 Bibliography . . . 21

3 Polynomials with values which are powers of integers 23
- 3.1 Résumé . . . 23
- 3.2 Abstract . . . 23
- 3.3 Introduction . . . 23
- 3.4 Preliminaries . . . 25
- 3.5 Proof of Theorem 3.3.1 . . . 29
- 3.6 Bibliography . . . 30

4 On the solutions to equations of the form $F_n \pm F_m = y^a$ 32
- 4.1 Résumé . . . 32

4.2 Abstract . . . 32
4.3 Introduction . . . 32
4.4 Preliminaries . . . 34
4.5 Solutions to $F_n - F_m = 11^a$ . . . 36
4.6 Solutions to $F_n - F_m = y^a$ for $y \in \{6, 12\}$ . . . 40
4.7 On the solutions to $F_n + F_m = y^a$ for fixed y . . . 45
4.8 Bibliography . . . 48

5 A New Proof of the Carlitz-Lutz Theorem **49**
5.1 Résumé . . . 49
5.2 Abstract . . . 49
5.3 Introduction . . . 49
5.4 Proof of Theorem 5.3.3 . . . 51
5.5 Concluding Remarks . . . 53
5.6 Bibliography . . . 53

6 Prime polynomials over Finite Fields **55**
6.1 Résumé . . . 55
6.2 Abstract . . . 55
6.3 Introduction . . . 55
6.4 Functions over $\mathbb{F}_q$ . . . 57
6.5 Decomposition over K . . . 57
6.6 Bibliography . . . 65

7 Composed products of polynomials over unique factorization domains **66**
7.1 Résumé . . . 67
7.2 Abstract . . . 67
7.3 Introduction . . . 67
7.4 Preliminaries . . . 68
7.5 Additive Decompositions . . . 69
7.6 Bibliography . . . 74

8 Multiplicative decompositions of polynomials **75**
8.1 Résumé . . . 75
8.2 Abstract . . . 75
8.3 Introduction . . . 76
8.4 Preliminaries . . . 77
8.5 Composed Product Decompositions . . . 79
8.6 Bibliography . . . 82

9 Least primes which split in imaginary quadratic fields **83**
9.1 Résumé . . . 83
9.2 Abstract . . . 83
9.3 Introduction . . . 83
9.4 Preliminary Results . . . 85
9.5 Main Result . . . 85
9.6 Bibliography . . . 87

10 On the covering of rings by their subrings **89**

10.1 Résumé 89
10.2 Abstract 89
10.3 Introduction 89
10.4 Main Results 90
10.5 Bibliography 94

Conclusion **95**

Acknowledgements

My thanks to professors Antonio Lei and Claude Levesque. It is only thanks to their accommodating nature, their kindness, and their direction that I was able to successfully complete this work. I am fully aware of the time they spent on my behalf. My deepest thanks to professor Omar Kihel for all of his encouragement, time, and support throughout the years, as well as for first introducing me to the beauty of number theory.

I extend my gratitude to the Natural Sciences and Engineering Research Council of Canada for their financial support, allowing me to focus my efforts on research.

Finally, I would like to thank my family for their eternal support. In particular, I would like to thank my mother Hélène, my father Bruce, and my brother Kevin for their unconditional love.

Foreword

This is a thesis collecting research articles. Moreover, all published papers, those submitted, and preprints have been reproduced verbatim within each of their respective chapters. As is traditional within the mathematical community, the names of authors appear in alphabetical order. This being the case, we note that the contributions of each author are proportionally equal.

Chapter 1 reproduces the following published article. Submitted: 12 June 2017. Accepted: 17 July 2017. Published: 2 November 2017.
S. Alkabouss, T. Garici, and J. Larone, *On the equation* $Res_x\big(P(x), x^2 + sx + t\big) = a$, International Journal of Number Theory. 14.4, (2018), 1073–1079.

Chapter 2 reproduces the following published article. Submitted: 6 April 2016. Accepted: 26 May 2017. Published: 9 October 2018.
T. Garici, O. Kihel, and J. Larone, *The number of solutions to* $y^2 = px(Ax^2+2)$, Publications de l'Institut Mathématique. 104.118, (2018), 149–156.

Chapter 3 reproduces the following published article. Submitted: 25 July 2017. Accepted: 5 March 2018. Published: 2018
R. Boumahdi and J. Larone, *Polynomials with values which are powers of integers*, Archivum Mathematicum. 54, (2018), 119–125.

Chapter 4 reproduces the following articles.
The first article; preprint, to be submitted to a mathematical journal.
The second article. Submitted: 19 January 2020. Accepted upon revision: 14 February 2020.
O. Kihel and J. Larone, *The nonnegative integer solutions to the equation* $F_n - F_m = y^p$ *for fixed* $y = 6$, $y = 11$, *or* $y = 12$, (preprint, to be submitted to a mathematical journal)
O. Kihel and J. Larone, *On the nonnegative integer solutions to the equation* $F_n + F_m = y^a$, accepted upon revision (Quaestiones Mathematicae).

Chapter 5 reproduces the following published article. Submitted: 6 April 2019. Accepted: 6 May 2019. Published: 10 July 2019.
R. Boumahdi, O. Kihel, J. Larone, and M. Yadjel, (2019) *A New Proof of the Carlitz-Lutz Theorem*, Bulletin of the Australian Mathematical Society, (2020), 56–60.

Chapter 6 reproduces the following article submitted for publication. Submitted: 30 December 2019.
S. Kebli, O. Kihel, and J. Larone, *Prime Polynomials over Finite Fields*, submitted for publication (Functiones et Approximatio).

Chapter 7 reproduces the following published article. Submitted: 1 May 2019. Accepted: 25 May 2019. Published: 24 July 2019.
L. Benferhat, S. M. E. Benoumhani, R. Boumahdi, and J. Larone, (2019) *Additive decompositions of polynomials over unique factorization domain*, Journal of Algebra and Its Applications, (2019), 24:2050150.

Chapter 8 reproduces the following preprint article
O. Kihel and J. Larone, *Multiplicative decompositions of polynomials over commutative rings*, (preprint, to be submitted to a mathematical journal).

Chapter 9 reproduces the following article submitted for publication. Submitted: 8 March 2020.
S. Alkabouss, B. Bensebaa, O. Kihel, and J. Larone, *Least primes which split in imaginary quadratic fields*, submitted for publication (Mathematica).

Chapter 10 reproduces the following preprint article
O. Kihel and J. Larone, *On the covering of rings by their subrings*, (preprint, to be submitted to a mathematical journal).

Introduction

The entirety of this work lies largely within the broad scopes of number theory and algebra. The topics covered here are varied, although the underlying ideas can be roughly divided into two parts, each with an overall general theme. The first part consists of the search for solutions to some Diophantine equations. The second deals with many different forms of decomposition. In the interest of keeping this work as concise as possible, we attempt to provide the reader with the minimum of required knowledge to fully motivate and understand the provided results.

Diophantine equations

The near ubiquity of Diophantine equations in number theory makes them a consistent source of active research. Here, we concern ourselves with only a few selected from the many.

A Diophantine equation is a polynomial equation in several variables such that only integer solutions to the given equation are desired. Some Diophantine equations have additional variables occurring as exponents, and such equations are called exponential Diophantine equations. One of the most well-known Diophantine equations is $x^n + y^n = z^n$ for $n \geq 3$ whose fame is of course attributed to Fermat's Last Theorem. Using the theories of modular forms and elliptic curves, it was eventually shown to have no integer solutions (x, y, z) with $xyz \neq 0$.

Another well-known example, and one that is perhaps more closely related to and relevant to this work, is Pell's equation $x^2 - ny^2 = \pm 1$. Pell's equation has a fundamental solution which can be obtained by way of continued fraction expansions. From this sole solution, all other solutions can be obtained algebraically through a recurrence relation derived from taking successive powers of the fundamental solution. Over time, interest in related equations of the form $ax^2 - by^4 = c$ has increased, and there have been many papers on the subject. Without delving too deeply into the existing research, we will limit ourselves to simply referencing any such needed results as they are required.

In the first four chapters of this thesis, we recall any relevant knowledge needed, and we present articles containing new research on various Diophantine equations and their solutions. The methods used when discussing these equations vary, and include techniques such as linear

forms in logarithms of algebraic numbers and Runge's method, while also requiring the use of some strong auxiliary results such as one due to Bugeaud, Mignotte, and Siksek.

On Decompositions

A general notion of decomposition exists throughout nearly all branches of mathematics. Relevant and related examples to describe our meaning of the word include the factorization of polynomials over rings and fields, irreducible and prime ring elements (and consequently also groups of units), (internal) direct products of algebraic structures and their substructures, and others.

The last six chapters of this thesis address some of these decomposition related notions. The topics include prime polynomials and rational functions, composite polynomials and rational functions, additive and multiplicative decompositions of polynomials, the splitting of primes in number fields, and the covering of rings by their subrings.

Some motivating concepts

We recall the resultant here for two reasons. First, it will be used throughout many sections of this work, so doing so here is rather convenient. Second, it is an excellent tool to introduce and connect the various ideas discussed within this thesis, motivating some of the research.

Given two polynomials $f = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ and $g = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ over a commutative ring, the resultant of f and g is defined as the determinant of their Sylvester matrix. Specifically,

$$\mathrm{Res}_x(f,g) = \begin{vmatrix} a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\ a_{m-1} & a_m & \cdots & 0 & b_{n-1} & b_n & \cdots & 0 \\ a_{m-2} & a_{m-1} & \ddots & 0 & b_{n-2} & b_{n-1} & \ddots & 0 \\ \vdots & \vdots & \ddots & a_m & \vdots & \vdots & \ddots & b_n \\ a_0 & a_1 & \cdots & \vdots & b_0 & b_1 & \cdots & \vdots \\ 0 & a_0 & \ddots & \vdots & 0 & b_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_1 & \vdots & \vdots & \ddots & b_1 \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{vmatrix}.$$

It is clear from the definition that the expression $\mathrm{Res}_x(f,g)$ is a polynomial in the coefficients of f and of g. Because of this,

$$\mathrm{Res}_x(f,g) = c$$

for an integer c can be viewed as a Diophantine equation. This will be precisely the topic of study in chapter 1.

The discriminant of the polynomial f described above can be stated through the resultant as $\frac{1}{a_m}\mathrm{Res}_x(f, f')$, where f' denotes the formal derivative of f. This implies that the resultant can provide some information related to the critical values of a polynomial. In chapter 6, we consider the problem of writing a polynomial h as the composition of polynomials $f \circ g$, and we provide some criteria (using precisely this connection to critical values) for concluding that such a decomposition cannot be possible excluding some trivial decompositions.

Finally, if for example we define for every $g \in R[x]$ a polynomial $G(x,t)$ in $R[x,t]$ such that $G(x,r) = g(x)$ for some $r \in R$, then the expression $\mathrm{Res}_x(f, G)$ is in fact a polynomial in t. One might then be interested in various properties of a binary operation $\diamond$ defined on $R[x,t]$ by

$$f \diamond g = \mathrm{Res}_x(f, G)\,.$$

The possibility of expressing a polynomial h as $f \diamond g$ in such ways will be addressed in chapters 7 and 8.

Collaborations

I make here an important remark. The new results contained within this work have been obtained from research performed in collaboration with colleagues.

Chapter 1

On the equation $\mathrm{Res}_x\big(P(x), x^2 + sx + t\big) = a$

1.1 Résumé

On montre qu'il n'y a qu'un nombre fini de solutions à $\mathrm{Res}_x\big(P(x), x^2 + sx + t\big) = a$, $a \neq 0$, en utilisant une amélioration de la méthode de Runge présentée par Schinzel.

1.2 Abstract

The number of solutions to the title equation when $a \neq 0$ is shown to be finite. The proof relies on the improvement to Runge's method due to Schinzel.

1.3 Introduction

We briefly recall Runge's method. Suppose that

$$P(X, Y) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{i,j} X^i Y^j$$

is irreducible in $\mathbb{Q}[X, Y]$ with $a_{i,j} \in \mathbb{Z}$ and $m, n > 0$. If there are infinitely many integer solutions (x, y) to $P(X, Y) = 0$, then each of the following statements holds:

i) $a_{i,n} = a_{m,j} = 0$ for $i \neq 0$ and $j \neq 0$;

ii) $ni + mj \leq mn$ for each term $a_{i,j} X^i Y^j$ of P;

iii) the sum of monomials $a_{i,j} X^i Y^j$ of P for which $ni + mj = mn$ is the product of a constant and of a power of an irreducible polynomial in $\mathbb{Z}[X, Y]$;

iv) the algebraic function $y = y(x)$ defined by $P(x, y) = 0$ has but a single system of conjugate Puiseux expansions at infinity.

For details on conjugate Puiseux expansions, we direct the interested reader to [1]. If the last of the above properties fails to hold, we say that P satisfies Runge's condition, and Runge's method consists of showing whether a polynomial P satisfies Runge's condition. Of interest to us will in fact be a refinement of this method due to Schinzel, which for our purposes will also be far simpler to apply, but we leave it for later as a theorem. It will be necessary when applying Schinzel's results to recall that a homogeneous form of degree n is an equation defined by a polynomial

$$P(X_1, \ldots, X_m) = \sum_{i_1+\cdots+i_m=n} a_{i_1,\ldots,i_m} {X_1}^{i_1} \cdots {X_m}^{i_m}.$$

Now let

$$P(x) = a_m(x - \alpha_1) \cdots (x - \alpha_m),$$

where $a_m \in \mathbb{Z}$ and the α_i's are the roots of P lying in $\mathbb{C}$. Set

$$Q(x) = x_n x^n + x_{n-1}x^{n-1} + \cdots + x_0 \in \mathbb{Z}[x],$$

then we have

$$\mathrm{Res}(P, Q) = a_m^n \prod_{i=1}^{m} (x_n \alpha_i^n + x_{n-1}\alpha_i^{n-1} + \cdots + x_0). \tag{1.1}$$

We consider the resultant equation given by

$$\mathrm{Res}(P, Q) = a, \tag{1.2}$$

where a is a given nonzero integer. Notice that a resultant equation can be considered as a polynomial Diophantine equation in coefficients of Q. Many authors studied resultant equations. For examples, one can cite Wirsing [15], Fujiwara [4], Schmidt [14], Schlickewei [13], Pethő [9; 10], Győry [7], Evertse and K. Győry [2], Gaál [5] who proved that the number of polynomials Q satisfying equation (1.2) is finite under the condition $m > n$. In fact, Wirsing [15] proved that if n is a positive integer such that

$$2n\left(1 + \frac{1}{3} + \cdots + \frac{1}{2n-1}\right) < m,$$

then there are only finitely many polynomials $Q \in \mathbb{Z}[x]$ of degree n satisfying equation (1.2). Later, Fujiwara [4] showed that if the polynomial P is irreducible over $\mathbb{Q}$ and $2n < m$ then equation (1.2) has only finitely many solutions in polynomials $Q \in \mathbb{Z}[x]$ of degree n. Moreover, Schmidt [14] proved that the irreducibility of P can be replaced by the condition that P has no nonconstant factor of degree less or equal to n in $\mathbb{Z}[x]$. Let R be a subring of $\mathbb{Q}$ that is a finitely generated extension ring of $\mathbb{Z}$, a be a nonzero element of R, and R^* be the unit group

of R. If m, n are positive integers such that $2n < m$ and $P \in R[x]$ is a polynomial of degree m without multiple zeros that has no nonconstant factor in $R[x]$ of degree less or equal to n, then up to a proportional factor from R^*, Schlickewei [13] proved that there is only a finite number of polynomials $Q \in R[x]$ of degree n satisfying

$$\mathrm{Res}(P, Q) \in a \cdot R^*.$$

Győry [7] proved that if $Q(x)$ is a monic polynomial, then the condition $m \geq 2n$ can replace the condition $m > 2n$. See Theorem 2 in [7]. In 2002, Gaál [5] developed an algorithm based on Baker's method to solve equation (1.2), when $P \in \mathbb{Z}[x]$ is an irreducible polynomial of degree $m \geq 3$ and $Q = x^2 + x_1 x + x_2 \in \mathbb{Z}[x]$. In fact, he transformed equation (1.2) into the inhomogeneous Thue equation

$$a_0^2 N_{F/\mathbb{Q}}(x_2 + x_1\alpha + \alpha^2) = a \quad \text{in } x_1, x_2 \in \mathbb{Z},$$

where α is a root of P and $F = \mathbb{Q}(\alpha)$. More recently, Gaál and Pohst [6] extended the work of Gaál to any monic polynomial Q of degree $n \geq 2$.

In 1887 Runge [11] proved that if $f(x, y)$ is a polynomial with integer coefficients irreducible in the rational field and the equation $f(x, y) = 0$ has infinitely many integer solutions, then the highest homogeneous part $f^+(x, y)$ is up to a constant factor a power of an irreducible form. This result has been improved in 1969 by Schinzel [12] who proved that except for a constant factor $f^+(x, y)$ is a power of a linear form or of an irreducible indefinite quadratic form.

The aim of this paper is to use the improvement of Runge's theorem due to Schinzel [12] to show that the equation in the title has a finite number of solutions.

1.4 Preliminaries

Let

$$P(x) = a_m(x - \alpha_1) \cdots (x - \alpha_m) \in \mathbb{Z}[x],$$

where $a_m \in \mathbb{Z} \setminus \{0\}$ and α_i are the roots of P. We consider the resultant equation

$$R(s, t) = \mathrm{Res}_x(P(x), x^2 + sx + t) = a, \tag{1.3}$$

where a is a given nonzero integer.

Lemma 1.4.1. *Let $A(s, t)$, $B(s, t) \in \mathbb{Z}[s, t]$ such that*

$$P(x) = (x^2 + sx + t)q(s, t, x) + A(s, t)x + B(s, t),$$

then

$$R(s, t) = B^2(s, t) + tA^2(s, t) - sA(s, t)B(s, t).$$

Proof. Let γ, $\beta = -s - \gamma$ be the zeros of $x^2 + sx + t$ in the algebraic closure of $\mathbb{Q}(s,t)$. Then we have

$$\begin{aligned} R(s,t) &= \mathrm{Res}_x\left(x^2 + sx + t, P(x)\right) = P(\gamma)P(\beta) \\ &= (A\gamma + B)(A\beta + B) = tA^2 + B^2 - sAB. \end{aligned}$$

□

From this lemma we can deduce that $R(s,t) \in \mathbb{Z}[s,t]$. So there exist unique polynomials $r_i(s) \in \mathbb{Z}[s]$ such that $R(s,t) = \sum_{i=0}^{n} r_i(s)t^i$. Moreover, by (1.1) we have

$$R(s,t) = a_m^2 \prod_{k=1}^{m} \left(\alpha_k^2 + s\alpha_k + t\right).$$

Then $n = m$ and the two polynomials $R(s,t)$ and $P(x)$ satisfy the following identity:

$$R(s, -x^2 - sx) = P(x)P(-s - x). \tag{1.4}$$

Therefore

$$\begin{aligned} P(x)P(-s-x) &= \sum_{i=0}^{m} (-1)^i r_i(s) \left(x^2 + sx + t - t\right)^i \\ &= \sum_{k=0}^{m} \left(\sum_{i=k}^{m} \binom{i}{k} (-1)^k t^{i-k} r_i(s) \right) \left(x^2 + sx + t\right)^k. \end{aligned}$$

From this we can deduce that there exist polynomials $u_k(s,t) \in \mathbb{Z}[s,t]$ such that

$$P(x)P(-s-x) = u_0(s,t) + u_1(s,t)(x^2 + sx + t) + \cdots + u_m(s,t)(x^2 + sx + t)^m,$$

with $u_0(s,t) = R(s,t)$ and $u_m(s,t) = (-1)^m a_m^2$. More generally, we have the following proposition.

Proposition 1.4.2. *Let s, t, x be 3 variables algebraically independent over $\mathbb{Q}$. If $Q(x)$ is a polynomial with coefficients in $\mathbb{Z}[s,t]$ satisfying $Q(-s-x) = Q(x)$, then:*

1. *There exist unique $v_k(s,t) \in \mathbb{Z}[s,t]$ such that*

$$Q(x) = v_0(s,t) + v_1(s,t)(x^2 + sx + t) + \cdots + v_h(s,t)(x^2 + sx + t)^h.$$

2. *$Res_x\left(Q(x), x^2 + sx + t\right) = \left(v_0(s,t)\right)^2$.*

Proof. The uniqueness is obvious as it is $(x^2 + sx + t)$-adic representation of $Q(x)$. This is a particular representation because the coefficients v_0, $v_1, \ldots, v_h$ depend only on s and t but not on x. Let $q(s,t,x)$, $w(s,t)$ and $v_0(s,t)$ be the unique polynomials with coefficients in $\mathbb{Z}$ such that

$$Q(x) = q(s,t,x)(x^2 + sx + t) + w(s,t)x + v_0(s,t).$$

Then the equality $Q(-s-x)=Q(x)$ and the uniqueness of the polynomials q, w, v_0 imply that $w=0$. Therefore $Q(x)=v_0(s,-x^2-sx)$. Put $v_0(s,t)=\sum_{i=0}^{h} r_i(s)t^i$, then

$$Q(x)=\sum_{k=0}^{h}\left(\sum_{i=k}^{h}\binom{i}{k}(-1)^k t^{i-k} r_i(s)\right)(x^2+sx+t)^k.$$

From this we can deduce that there exist polynomials $v_k(s,t)\in\mathbb{Z}[s,t]$ such that $Q(x)=v_0(s,t)+v_1(s,t)(x^2+sx+t)+\cdots+v_h(s,t)(x^2+sx+t)^h$, where for each k, $v_k(s,t)=\sum_{i=k}^{h}\binom{i}{k}(-1)^k t^{i-k} r_i(s)$. Let γ, β be the zeros of x^2+sx+t in the algebraic closure of $\mathbb{Q}(s,t)$, then $Q(\gamma)=Q(\beta)=v_0(s,t)$. Thus $\mathrm{Res}_x(Q(x),x^2+sx+t)=(v_0(s,t))^2$. □

From this proposition, we can deduce the following result.

Proposition 1.4.3. *Equation (1.3) has a solution $(s^*,t^*)\in\mathbb{Z}^2$ if and only if*

$$P(x)P(-s^*-x)-a\equiv 0 \pmod{x^2+s^*x+t^*}.$$

So we will study the values of $s^*\in\mathbb{Z}$ such that $P(x)P(-s^*-x)-a$ is reducible and possesses a quadratic factor.

We finish this section with a result concerning the polynomial $R(s,t)-a$. By Proposition 1.4.2, one can write $P(X)+P(-s-X)$ into the form

$$P(x)+P(-s-x)=v_0(s,t)+v_1(s,t)(x^2+sx+t)+\cdots+v_h(s,t)(x^2+sx+t)^h.$$

Proposition 1.4.4. *Let $r(s,t)=Res_x\left(P(x)+P(-s-x)-v_0(s,t),P(x)P(-s-x)-a\right)$, then*

$$r(s,t)\equiv 0 \pmod{(R(s,t)-a)^2}.$$

Proof. Consider $V(x,s,t)=v_1(s,t)+\cdots+v_h(s,t)(x^2+sx+t)^{h-1}$ and $R_1(s,t)=\mathrm{Res}_x((x^2+sx+t),P(x)P(-s-x)-a)$. We have $P(x)+P(-s-x)-v_0(s,t)=(x^2+sx+t)V(x,s,t)$ and

$$r(s,t)=\mathrm{Res}_x\left(V(x,s,t),P(x)P(-s-x)-a\right)R_1(s,t). \tag{1.5}$$

Let γ, $\beta=-s-\gamma$ be the zeros of x^2+sx+t in the algebraic closure of $\mathbb{Q}(s,t)$. Then we have

$$R(s,t)=\mathrm{Res}_x\left(x^2+sx+t,P(x)\right)=P(\gamma)P(-s-\gamma)$$

and

$$R_1(s,t)=\left(P(\gamma)P(-s-\gamma)-a\right)^2=(R(s,t)-a)^2.$$

Therefore

$$r(s,t)=\mathrm{Res}_x(V(x,s,t),P(x)P(-s-x)-a)\left(R(s,t)-a\right)^2.$$

We conclude that $r(s,t)\equiv 0 \pmod{(R(s,t)-a)^2}$.

□

1.5 The irreducibility of the polynomial $R(s,t)-a$, for a fixed in $\mathbb{Z}\setminus\{0\}$

In this section, we study the irreducibility of the polynomial $R(s,t)-a$, where a is a fixed nonzero integer.

Theorem 1.5.1. *Let $a\in\mathbb{Z}\setminus\{0\}$, $P(x)\in\mathbb{Z}[x]$ be a separable polynomial of degree m, and $Q(s,x)\in\mathbb{Z}[s,x]$ a polynomial of the form*

$$Q(s,x)=Q_n s^n+Q_{n-1}(x)s^{n-1}+\cdots+Q_0(x),$$

with $n\geq 1$ and $Q_n\in\mathbb{Z}\setminus\{0\}$. Then the polynomial $P(x)Q(s,x)-a$ is absolutely irreducible.

Proof. Let $A(s,x)=A_k(x)s^k+A_{k-1}(x)s^{k-1}+\cdots+A_0(x)$ and $B(s,x)=B_\ell(x)s^\ell+B_{\ell-1}(x)s^{\ell-1}+\cdots+B_0(x)$ be two polynomials in $\overline{\mathbb{Q}}[x,s]$ such that $k\geq\ell$, $k+\ell=n$ and

$$P(x)Q(s,x)-a=A(s,x)B(s,x). \tag{1.6}$$

Suppose now that $\ell\geq 1$ and $k+\ell=n$. By identifying the coefficients of s^j, for $j=0,1,\ldots,n$, we obtain

$$\begin{aligned}
P(x)Q_n &= A_k(x)B_\ell(x),\\
P(x)Q_{n-1}(x) &= A_k(x)B_{\ell-1}(x)+A_{k-1}(x)B_\ell(x),\\
&\cdots\\
P(x)Q_j(x) &= \sum_{\substack{u+v=j\\ u\leq k,\, v\leq\ell}} A_u(x)B_v(x), \quad \text{with} \quad j=n-2,\ldots,1,\\
&\cdots\\
P(x)Q_0(x)-a &= A_0(x)B_0(x).
\end{aligned} \tag{1.7}$$

As $P(x)$ is separable, then $(A_k(x),B_\ell(x))=1$. The second equation in (1.7) shows that $A_k(x)|A_{k-1}(x)$ and $B_\ell(x)|B_{\ell-1}(x)$. The following equations give $A_k(x)|A_j(x)$ and $B_\ell(x)|B_h(x)$, for $j=0,\ldots,k-1$ and $h=0,\ldots,\ell-1$. This contradicts the last equation in (1.7). Therefore, it can be concluded that $\ell=0$, so $B(s,x)=B(x)$ and $k=n\geq 1$. By identifying the coefficients of s^n and s^0 in (1.6), we obtain

$$a=B(x)\left(\frac{1}{Q_n}Q_0(x)A_n(x)-A_0(x)\right).$$

We deduce that $B(x)$ is a constant polynomial. □

We deduce the following results.

Corollary 1.5.2. *Let $a\in\mathbb{Z}\setminus\{0\}$ and $P(x)\in\mathbb{Z}[x]$ be a separable polynomial, then the polynomial $P(x)P(-s-x)-a$ is absolutely irreducible.*

Proof. This is a particular case of Theorem 1.5.1 with $Q(s,x) = P(-s-x)$. □

Corollary 1.5.3. *Let $a \in \mathbb{Z} \setminus \{0\}$ and $P(x) \in \mathbb{Z}[x]$ be a separable polynomial. Let $R(s,t) = Res_x(P(x), x^2 + sx + t)$. Then the polynomial $R(s,t) - a$ is absolutely irreducible.*

Proof. By the relation (1.4), $R(s, -x^2 - sx) - a = P(x)P(-s-x) - a$, which is absolutely irreducible by Corollary 1.5.2. Thus, we have that $R(s,t) - a$ is also absolutely irreducible.

□

1.6 Application of Runge method

In this section, we will use Runge method to prove that equation (1.2) has a finite number of solutions.

Lemma 1.6.1. *Let $F(x,y) \in \mathbb{Z}[x,y]$ be a polynomial of degree n which is irreducible over $\mathbb{Q}[x,y]$ and let $F^+(x,y)$ be its homogeneous part of degree n. If $F(x,y) = 0$ has an infinite number of integer solutions then, except for a constant factor, $F^+(x,y)$ is a power of a linear form or of an irreducible indefinite quadratic form.*

Proof. See [12] and Theorem 21, page 276 of [8] □

Lemma 1.6.2. *Let $P(x) \in \mathbb{Z}[x]$, $R(s,t) = Res_x(P(x), x^2 + sx + t)$ and $R^+(s,t)$ its dominant homogeneous form. Then*

$$R^+(s,t) = a_m(-s)^m P(-t/s),$$

where $m = \deg P$ and a_m is the leading coefficient of $P(x)$.

Proof. Let $\alpha_1, \ldots, \alpha_m$ be the roots of $P(x)$. Then we have

$$R(s,t) = \mathrm{Res}_x\left(P(x), x^2 + sx + t\right) = a_m^2 \prod_{i=1}^{m} (\alpha_i^2 + s\alpha_i + t).$$

So

$$\begin{aligned} R^+(s,t) &= a_m^2 \textstyle\prod_{i=1}^m (s\alpha_i + t) = a_m^2 \prod_{i=1}^m (-s)\left(-\alpha_i - \frac{t}{s}\right) \\ &= (-s)^m a_m \cdot a_m \textstyle\prod_{i=1}^m \left(-\alpha_i - \frac{t}{s}\right) = a_m(-s)^m P(-t/s). \end{aligned}$$

□

Theorem 1.6.3. *Let $b \in \mathbb{Z} \setminus \{0\}$ and $f(x) \in \mathbb{Z}[x]$. If $\deg f - \deg(\gcd(f, f')) \geq 3$ then the equation*

$$Res_x\left(f(x), x^2 + sx + t\right) = b \tag{1.8}$$

has a finite number of integer solutions.

Proof. Let $D = \gcd(f, f')$, $P(x) = \frac{f(x)}{D(x)}$. Then $P(x)$ is separable, $\deg P \geq 3$ and

$$\mathrm{Res}_x(f(x), x^2 + sx + t) = R(s,t)\mathrm{Res}_x\left(D(x), x^2 + sx + t\right).$$

Equation (1.8) implies that there exists a divisor a of b such that

$$R(s,t) = a. \tag{1.9}$$

Put $F(s,t) = R(s,t) - a$, then by Corollary 1.5.3, $F(s,t)$ is irreducible and by Lemma 1.6.2, we have

$$F^+(s,t) = R^+(s,t) = a_m(-s)^m P(-t/s).$$

where $m = \deg P$ and a_m is the leading coefficient of $P(x)$. Suppose that, except for a constant factor, $F^+(x,y)$ is a power of a linear form or of an irreducible indefinite quadratic form. Then except for a constant factor, $P(x)$ is a power of a linear or quadratic polynomial which contradicts the fact that P is a separable polynomial of degree $m \geq 3$. The conditions of Lemma 1.6.1 are fulfilled, so equation (1.9) has a finite number of integer solutions. Since there are only a finite number of divisors of b, equation (1.8) has only a finite number of integer solutions. □

Concluding remark

We note that the core of the proof has some room for improvement. Specifically, it seems to only be required that the polynomial $Q(x)$ have two unknown coefficients. It seems within the realm of reason that by replacing the quadratic polynomial $x^2 + sx + t$ with any polynomial with all but exactly two coefficients determined, the proof would only need minor adjustments to accommodate the change. We conjecture here that this is the case: such an equation $\mathrm{Res}_x\big(P(x), Q(x)\big) = a$ has only a finite number of integer solutions (s,t).

1.7 Bibliography

[1] D. Duval, *Rational Puiseux expansions*, Compositio Math. **70** no.2 (1989), 119–154.

[2] J. H. Evertse and K. Győry, *Lower bounds for resultants I*, Compositio Math. **88** (1993), 1–23.

[3] J. H. Evertse and K. Győry, *Lower bounds for resultants II*, In: Number Theory, Diophantine, Computational and Algebraic Aspects, proc. conf. Eger 1996, K. Győy, A. Pethő, V.T. Sós, eds., pp. 181–198. Walter de Gruyter, 1998.

[4] M. Fujiwara, *Some applications of a theorem of W. M. Schmidt*, Michigan Math. J., **19** (1972), 315–319.

[5] I. Gaál, *On the Resolution of Resultant Type Equation*, J. Symbolic Computation **34** (2002), 137–144.

[6] I. Gaál, M. Pohst, *Solving Resultant Form Equations Over Number Fields*, Math. Comp. **77**, no. 264, (2008), 2447–2453.

[7] K. Győry, *Some applications of decomposable form equations to resultant equations*, Colloq. Math., **65** (1993), 267–275.

[8] L. J. Mordell, *Diophantine equations*, Academic Press, London, 1969.

[9] A. Pethő, *Application of Gröbner bases to the resolution of systems of norm equations*, in: Proc. ISSAC **91**, ACM Press, 1991, 144–150.

[10] A. Pethő, *Systems of norm equations over cubic number fields*, Grazer Math. Berichte **318** (1993), 111–120.

[11] C. Runge, *Ueber ganzzahlige lösungen von gleichungen zwischen zwei veränderlichen*, J. Reine Angew. Math **100** (1887), 425–435.

[12] A. Schinzel, *An improvement of Runge's theorem on diophantine equations*, Comment. Pontif. Acad. Sci **2**, no. 20, (1969), 1–9.

[13] H. P. Schlickewei, *Inequalities for decomposable forms*, Astérisque **41-42** (1977), 267–271.

[14] W. M. Schmidt, *Inequalities for resultants and for decomposable forms*, in: Diophantine Approximation and its Applications, Academic Press, New York 1973, 235–253.

[15] E. Wirsing, *On approximations of algebraic numbers by algebraic numbers of bounded degree*, in: Proc. Sympos. Pure Math. **20**, Amer. Math. Soc., Providence 1971, 213–247.

Chapter 2

The number of solutions to $y^2 = px(Ax^2 + 2)$

2.1 Résumé

Togbé a considéré l'équation Diophantienne

$$y^2 = px(Ax^2 + 2)$$

où p est nombre premier et $A > 1$ est entier impair. Il a montré que l'équation n'a pas plus que sept solutions entières (x, y). Il a aussi proposé que le nombre de solutions ne dépasse pas trois et que les valeurs de A et p modulo 8 indiquent si ce nombre est soit un, deux ou trois.

On montre qu'une seule solution existe si $p = 2$ et on vérifie que la conjecture de Togbé est vraie dans sept des seize cas possibles. On améliore toutefois la borne de Togbé dans les autres cas. Nous considérons le cas où A est pair et on trouve une borne pour le nombre de solutions dans certains cas particuliers.

2.2 Abstract

Togbé considered the Diophantine equation

$$y^2 = px(Ax^2 + 2)$$

where p is a prime number and $A > 1$ is an odd integer. He proved that this Diophantine equation has at most seven positive integer solutions (x, y) and conjectured that the number of solutions would not exceed three, and whether this number is one, two, or three depends on the values of A and p modulo 8.

We prove that only one solution exists for $p = 2$, and we prove the conjecture for seven of the sixteen possible cases, while still improving the original bound in Togbé's result in the

remainder of the cases. We furthermore take into consideration the possibility of A even, where we bound the number of solutions in some particular cases.

2.3 Introduction

Cassels [3] was challenged to determine when the sum of three consecutive cubes equals a square. He [3] reduced the problem to finding integral points on the elliptic curve $y^2 = 3x(x^2+2)$. Using the arithmetic of certain quartic number fields, he obtained that the integral points on the above elliptic curve were $(x, y) = (0, 0)$, $(1, 3)$, $(2, 6)$, and $(24, 204)$.

Using the classical work of Ljunggren [7] and its generalizations (see [1], [5], [12], and [13]), Luca and Walsh [8] considered the problem of finding the number of positive integer solutions to the Diophantine equation $y^2 = nx(x^2 + 2)$, where $n > 1$ is a positive integer. They proved that the number of positive integer solutions to $y^2 = nx(x^2+2)$ is at most $3 \cdot 2^{\omega(n)} - 1$, where $\omega(n)$ is the number of distinct prime factors of n. In [4], Chen considered the case where n is a prime number greater than 3. He proved, in particular, that the Diophantine equation $y^2 = nx(x^2 + 2)$ has at most two positive integer solutions.

Recently, Togbé [10] considered the more general Diophantine equation

$$y^2 = px(Ax^2 + 2), \tag{2.1}$$

where p is a prime number and A is an odd integer greater than 1. He proved the following theorem.

Theorem 2.3.1. *For any prime p and any odd positive integer $A > 1$, the Diophantine equation (2.1) has at most seven positive integer solutions (x, y).*

Using results obtained through MAGMA, he then made the following conjecture on sharp bounds for the number of solutions to equation (2.1).

Conjecture 2.3.2. *Let p be a prime and $A > 1$ any odd positive integer.*

1. *If $(A, p) \equiv (1, 1)$, $(1, 5)$, $(1, 7)$, $(3, 1)$, $(3, 3)$, $(3, 7)$, $(5, 1)$, $(5, 5)$, $(5, 7)$, $(7, 3)$, or $(7, 5)$ (mod 8), then Diophantine equation (2.1) has at most one positive integer solution (x, y).*
2. *If $(A, p) \equiv (1, 3)$ or $(7, 1)$, then Diophantine equation (2.1) has at most two positive integer solutions (x, y).*
3. *If $(A, p) \equiv (3, 5)$ or $(7, 7)$, then Diophantine equation (2.1) has at most three positive integer solutions (x, y).*

The aim of this paper is to improve the bound on the number of solutions to the Diophantine equation (2.1) provided in Theorem 2.3.1, and to prove Conjecture 2.3.2 in some cases. The main result of this paper is the following theorem.

Theorem 2.3.3. *Let p be a prime and let $A > 1$ be an odd integer.*

(i) *If $p = 2$, then Diophantine equation (2.1) has at most one positive integer solution (x, y).*

(ii) *Suppose that $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$, where p is odd.*

a) *If $(A, p) \equiv (7, 1)$ or $(7, 7) \pmod 8$, then Diophantine equation (2.1) has at most three positive integer solutions (x, y).*

b) *Diophantine equation (2.1) has at most one positive integer solution (x, y) otherwise.*

(iii) *Suppose that $\left(\frac{-2A}{p}\right) = 1$, where p is odd.*

a) *If $(A, p) \equiv (1, 5)$, $(1, 7)$, $(3, 3)$, $(5, 5)$, $(7, 3)$, or $(7, 5) \pmod 8$, then Diophantine equation (2.1) has at most one positive integer solution (x, y).*

b) *If $(A, p) \equiv (1, 1)$, $(3, 1)$, $(3, 7)$, $(5, 1)$, $(5, 3)$, or $(5, 7) \pmod 8$, then Diophantine equation (2.1) has at most two positive integer solutions (x, y).*

c) *If $(A, p) \equiv (1, 3)$ or $(3, 5) \pmod 8$, then Diophantine equation (2.1) has at most three positive integer solutions (x, y).*

d) *If $(A, p) \equiv (7, 7) \pmod 8$, then Diophantine equation (2.1) has at most four positive integer solutions (x, y).*

e) *If $(A, p) \equiv (7, 1) \pmod 8$, then Diophantine equation (2.1) has at most six positive integer solutions (x, y).*

We will also prove the following result.

Theorem 2.3.4. *Let p be a prime and let $A > 1$ be an even integer.*

(i) *If $p = 2$, then Diophantine equation (2.1) has at most two positive integer solutions (x, y). Moreover, if $A \equiv 0 \pmod 4$ and $A \neq 2^6 \cdot 1785$, then Diophantine equation (2.1) has at most one positive integer solution (x, y).*

(ii) *Suppose that $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$, where p is odd.*

a) *If $A \equiv 0 \pmod 4$, then Diophantine equation (2.1) has at most one positive integer solution (x, y).*

b) *If $A \equiv 2 \pmod 4$, then Diophantine equation (2.1) has at most two positive integer solutions (x, y).*

(iii) Suppose that $\left(\frac{-2A}{p}\right) = 1$*, where* p *is odd.*

a) If $(A, p) \equiv (0, 3) \pmod 4$*, then Diophantine equation (2.1) has at most one positive integer solution* (x, y)*.*

b) If $(A, p) \equiv (0, 1) \pmod 4$*, then Diophantine equation (2.1) has at most two positive integer solutions* (x, y)*.*

c) If $(A, p) \equiv (2, 3) \pmod 4$*, then Diophantine equation (2.1) has at most three positive integer solutions* (x, y)*.*

d) If $(A, p) \equiv (2, 1) \pmod 4$*, then Diophantine equation (2.1) has at most four positive integer solutions* (x, y)*.*

2.4 Preliminary results

We present the results required to prove Theorem 2.3.3 and Theorem 2.3.4. Recall that if q is a prime number, $\nu_q(m)$ denotes the q-adic valuation of m.

Let a and b be odd positive integers for which the equation $aX^2 - bY^2 = 2$ has a solution in positive integers (X, Y). Let

$$\alpha = \frac{a_1\sqrt{a} + b_1\sqrt{b}}{\sqrt{2}}.$$

be the minimal positive solution of this equation, and define a_k and b_k for all odd integers k by

$$\alpha^k = \frac{a_k\sqrt{a} + b_k\sqrt{b}}{\sqrt{2}},$$

which represent all positive integer solutions to $aX^2 - bY^2 = 2$. Luca and Walsh proved the following result in [8] regarding the solutions to the equation

$$aX^2 - bY^4 = 2. \tag{2.2}$$

Theorem 2.4.1.

1. *If* b_1 *is not a square, then equation (2.2) has no integer solution.*
2. *If* b_1 *is a square and* b_3 *is not a square, then* $(X, Y) = (a_1, \sqrt{b_1})$ *is the only integer solution to equation (2.2).*
3. *If* b_1 *and* b_3 *are both squares, then* $(X, Y) = (a_1, \sqrt{b_1})$ *and* $(a_3, \sqrt{b_3})$ *are the only integer solutions to equation (2.2).*

The following result of Ljunggren can be found in [7] and is proved as Theorem 3 in [6].

Theorem 2.4.2. *Let $a > 1$ and b be two positive integers. The equation*

$$aX^2 - bY^4 = 1$$

has at most one solution in positive integers (X, Y).

Let D be a positive non-square integer, and let $\epsilon_D = T_1 + U_1\sqrt{D}$ denote the minimal unit greater than 1, of norm 1, in $\mathbb{Z}[\sqrt{D}]$. Define ${\epsilon_D}^k = T_k + U_k\sqrt{D}$ for $k \geq 1$. Togbé, Voutier, and Walsh proved the following result in [11].

Theorem 2.4.3. *Let D be a positive non-square integer. There are at most two positive integer solutions (X, Y) to the equation $X^2 - DY^4 = 1$.*

1. *If two solutions such that $Y_1 < Y_2$ exist, then ${Y_1}^2 = U_1$ and ${Y_2}^2 = U_2$, except only if $D = 1785$ or $D = 16 \cdot 1785$, in which case ${Y_1}^2 = U_1$ and ${Y_2}^2 = U_4$.*

2. *If only one positive integer solution (X, Y) to the equation $X^2 - DY^4 = 1$ exists, then $Y^2 = U_\ell$ where $U_1 = \ell v^2$ for some square-free integer ℓ, and either $\ell = 1$, $\ell = 2$, or $\ell = p$ for some prime $p \equiv 3 \pmod 4$.*

We will make Theorem 2.3.3 more precise when D is even.

Lemma 2.4.4. *Let D be a positive non-square integer. Suppose that $D = 2d$ where d is a positive integer different from $8 \cdot 1785$. Then the equation $X^2 - DY^4 = 1$ has at most one positive solution (X, Y).*

Proof. Suppose that there exist two solutions to the equation $X^2 - DY^4 = 1$. Then there exist positive integer solutions (X_1, Y_1) and (X_2, Y_2) such that $Y_1 < Y_2$. It follows from Theorem 2.4.3 that ${Y_1}^2 = U_1$, ${Y_2}^2 = U_2$, and $U_2 = 2T_1U_1$, so ${Y_2}^2 = 2T_1{Y_1}^2$. Then

$$2\nu_2(Y_2) = 1 + \nu_2(T_1) + 2\nu_2(Y_1). \tag{2.3}$$

Since $\epsilon_D = T_1 + U_1\sqrt{D}$ is a unit of norm 1 in $\mathbb{Z}[\sqrt{D}]$ and $D = 2d$, we obtain ${T_1}^2 - 2d{U_1}^2 = 1$, so that T_1 is odd. Then $\nu_2(T_1) = 0$, which is a contradiction with (2.3). □

2.5 Main results

Proof of Theorem 2.3.3. Let $p = 2$, and let A be an odd positive integer. Let x, y be positive integers such that $y^2 = 2x(Ax^2 + 2)$. It is not difficult to see that 4 divides x and y. Let $y = 4w$ and $x = 4z$. Then we obtain

$$w^2 = z(8Az^2 + 1).$$

Since $\gcd(z, 8Az^2+1) = 1$, there exist positive integers u and v such that $z = u^2$, $8Az^2+1 = v^2$, and

$$v^2 - 8Au^4 = 1.$$

By Lemma 2.4.4, this equation has at most one positive integer solution (u, v).

Let p be an odd prime, and let A be an odd positive integer. Let x, y be positive integers such that $y^2 = px(Ax^2 + 2)$. We remark that $\gcd(x, Ax^2 + 2) = 1$ or 2, so we consider two cases depending on the parity of x, with each case yielding two equations. Suppose first that x is even, so we let $x = 2z$. Since p is prime, we let $y = 2pw$. Then we obtain

$$pw^2 = z(2Az^2 + 1).$$

Since $\gcd(z, 2Az^2 + 1) = 1$, there exist positive integers u and v such that either $z = pu^2$, $2Az^2 + 1 = v^2$, and

$$v^2 - 2Ap^2u^4 = 1, \tag{2.4}$$

or $z = u^2$, $2Az^2 + 1 = pv^2$, and

$$pv^2 - 2Au^4 = 1. \tag{2.5}$$

Suppose next that x is odd. Since p is prime, we let $y = pw$. Then we obtain

$$pw^2 = x(Ax^2 + 2).$$

Since $\gcd(x, Ax^2+2) = 1$, there exist odd integers u and v such that either $x = pu^2$, $Ax^2+2 = v^2$, and

$$v^2 - Ap^2u^4 = 2, \tag{2.6}$$

or $x = u^2$, $Ax^2 + 2 = pv^2$, and

$$pv^2 - Au^4 = 2. \tag{2.7}$$

We consider each of the above four equations separately to determine the number of positive integer solutions to equation (2.1).

We begin with equation (2.4). Let $D = 2Ap^2$. By Lemma 2.4.4, equation (2.4) has at most one positive integer solution.

We next consider equation (2.5), which has at most one positive integer solution by Theorem 2.4.2. It follows from this equation that v is odd and that u is even if and only if $p \equiv 1 \pmod 8$. If $p \equiv 3, 5$, or $7 \pmod 8$, then u is odd, and we obtain $p - 2A \equiv 1 \pmod 8$. Then equation (2.5) has a solution only if $(A, p) \equiv (1, 1), (3, 1), (5, 1), (7, 1), (1, 3), (5, 3), (3, 7)$, or $(7, 7) \pmod 8$. Furthermore, equation (2.5) has a solution only if $\left(\frac{-2A}{p}\right) = 1$.

Equation (2.6) has at most two positive integer solutions by Theorem 2.4.1. Since u and v are both odd, we have $1 - A \equiv 2 \pmod 8$ so $A \equiv 7 \pmod 8$ and $v^2 \equiv 2 \pmod p$ so $\left(\frac{2}{p}\right) = 1$. Then $p \equiv 1$ or $7 \pmod 8$, and equation (2.6) has at least one solution only if $(A, p) \equiv (7, 1)$ or $(7, 7) \pmod 8$.

Equation (2.7) has at most two positive integer solutions by Theorem 2.4.1. Since u and v are odd, we have $p - A \equiv 2 \pmod 8$ so that equation (2.7) has a solution only if $(A, p) \equiv (1, 3)$, $(3, 5)$, $(5, 7)$, or $(7, 1) \pmod 8$. In particular, suppose that equation (2.7) has two solutions, and let (a_1, b_1) be the minimal positive solution of $pX^2 - AY^2 = 2$, so

$$p{a_1}^2 - A{b_1}^2 = 2.$$

Let

$$\alpha = \frac{a_1\sqrt{p} + b_1\sqrt{A}}{\sqrt{2}},$$

and compute α^3 to obtain

$$b_3 = \frac{3{a_1}^2 p b_1 + {b_1}^3 A}{2}.$$

Since we assume that two solutions exist to equation (2.7), b_1 and b_3 must both be squares by Theorem 2.4.1. It follows that there exist two positive integers B_1 and B_3 such that $b_1 = {B_1}^2$, $b_3 = {B_3}^2$, and

$$3{a_1}^2 p {B_1}^2 + {B_1}^6 A = 2{B_3}^2.$$

This yields $\left(\frac{2}{p}\right) = \left(\frac{A}{p}\right)$. Since $-Au^4 \equiv 2 \pmod p$, we obtain $\left(\frac{-A}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{A}{p}\right)$ so $\left(\frac{-1}{p}\right) = 1$. It follows that $p \equiv 1 \pmod 4$, so $p \equiv 1$ or $5 \pmod 8$. Therefore equation (2.7) has at most two positive integer solutions only if $(A, p) \equiv (3, 5)$ or $(7, 1) \pmod 8$, and it has at most one positive integer solution only if $(A, p) \equiv (1, 3)$ or $(5, 7) \pmod 8$. Furthermore, equation (2.7) has a solution only if $\left(\frac{-2A}{p}\right) = 1$.

Since the number of solutions to equations (2.5) and (2.7) depends on the value of $\left(\frac{-2A}{p}\right)$, we first suppose that $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$, then equations (2.5) and (2.7) have no integer solution, equation (2.4) has at most one solution, and (2.6) has at most two positive integer solutions only if $(A, p) \equiv (7, 1)$, or $(7, 7) \pmod 8$. Therefore when $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$, equation (2.1) has at most three positive integer solutions if $(A, p) \equiv (7, 1)$, or $(7, 7) \pmod 8$, and it has at most one positive integer solution in all other cases.

We next suppose that $\left(\frac{-2A}{p}\right) = 1$. Then equation (2.5) has at most one positive integer solution.

If $A \equiv 1 \pmod 8$, then equation (2.4) has at most one solution, (2.5) has at most one solution and only if $p \equiv 1$ or $3 \pmod 8$, (2.6) has no solution, and (2.7) has at most one solution and only if $p \equiv 3 \pmod 8$.

If $A \equiv 3 \pmod 8$, then equation (2.4) has at most one solution, (2.5) has at most one solution and only if $p \equiv 1$ or $7 \pmod 8$, (2.6) has no solution, and (2.7) has at most two solutions and

only if $p \equiv 5 \pmod 8$.

If $A \equiv 5 \pmod 8$, then equation (2.4) has at most one solution, (2.5) has at most one solution and only if $p \equiv 1$ or $3 \pmod 8$, (2.6) has no solution, and (2.7) has at most one solution and only if $p \equiv 7 \pmod 8$.

If $A \equiv 7 \pmod 8$, then equation (2.4) has at most one solution, (2.5) has at most one solution and only if $p \equiv 1$ or $7 \pmod 8$, (2.6) has at most two solutions and only if $p \equiv 1$ or $7 \pmod 8$, and (2.7) has at most one solution and only if $p \equiv 1 \pmod 8$. □

Proof of Theorem 2.3.4. If A is even and p is odd, we let $A = 2A'$. Then

$$y^2 = 2px(A'x^2 + 1).$$

We let $y = 2pw$, and we obtain

$$2pw^2 = x(A'x^2 + 1).$$

Since $\gcd(x, A'x^2 + 1) = 1$, there exist positive integers u and v such that either $x = 2pu^2$, $A'x^2 + 1 = v^2$, and

$$v^2 - 4A'p^2u^4 = 1, \tag{2.8}$$

or $x = 2u^2$, $A'x^2 + 1 = pv^2$ and

$$pv^2 - 4A'u^4 = 1, \tag{2.9}$$

or $x = u^2$, $A'x^2 + 1 = 2pv^2$ and

$$2pv^2 - A'u^4 = 1, \tag{2.10}$$

or $x = pu^2$, $A'x^2 + 1 = 2v^2$ and

$$2v^2 - A'p^2u^4 = 1. \tag{2.11}$$

If A' is a perfect square, then equation (2.8) has no positive integer solution, otherwise it has at most one positive integer solution by Lemma 2.4.4.
By Theorem 2.4.2, each of equations (2.9), (2.10), and (2.11) has at most one solution. Equation (2.9) has a solution only if $p \equiv 1 \pmod 4$ and $\left(\frac{-A'}{p}\right) = 1$, equation (2.10) has a solution only if A' is odd and $\left(\frac{-A'}{p}\right) = 1$, and equation (2.11) has a solution only if A' is odd. Since the number of solutions to equations (2.9) and (2.10) depends on the value of $\left(\frac{-A'}{p}\right) = \left(\frac{-2A}{p}\right)$, we first suppose that $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$. Then equations (2.9) and (2.10) have no integer solution.

If $A \equiv 0 \pmod 4$, then equation (2.8) has at most one solution, (2.9) has no solution, (2.10) has no solution, and (2.11) has no solution.

If $A \equiv 2 \pmod 4$, then equation (2.8) has at most one solution, (2.9) has no solution, (2.10) has no solution, and (2.11) has at most one solution.

We now suppose that $\left(\frac{-2A}{p}\right) = 1$. Then equations (2.9) and (2.10) have at most one positive integer solution.

If $A \equiv 0 \pmod 4$, then equation (2.8) has at most one solution, (2.9) has at most one solution only if $p \equiv 1 \pmod 4$, (2.10) has no solution, and (2.11) has no solution.

If $A \equiv 2 \pmod 4$, then equation (2.8) has at most one solution, (2.9) has at most one solution only if $p \equiv 1 \pmod 4$, (2.10) has at most one solution, and (2.11) has at most one solution.

If A is even and $p = 2$, we let $A = 2A'$. Then

$$y^2 = 2x(2A'x^2 + 2).$$

We let $y = 2w$, and we obtain

$$w^2 = x(A'x^2 + 1).$$

Since $\gcd(x, A'x^2+1) = 1$, there exist positive integers u and v such that $x = u^2$, $A'x^2+1 = v^2$, and

$$v^2 - A'u^4 = 1, \tag{2.12}$$

which has no solution if A' is a perfect square and at most two solutions by Theorem 2.4.3. Moreover, if A' is even and $A' \neq 2^5 \cdot 1785$, then by Lemma 2.4.4 equation (2.12) has at most one solution. □

Remark 2.5.1. *When we had finished writing the paper, we noticed that a proof of the result stated in Lemma 2.4.4 already existed within the proof of Theorem 1 by Luca and Walsh in [9]. Our proof of Lemma 2.4.4 seems to be different than the proof of the result in [9].*

Remark 2.5.2. *Theorem 2.3.3 implies that Conjecture 2.3.2 is true if* $(A, p) \equiv (1, 5)$, $(1, 7)$, $(3, 3)$, $(3, 5)$, $(5, 3)$, $(7, 3)$, *or* $(7, 5) \pmod 8$.

Remark 2.5.3. *We note that this work was subsequently improved upon by Bencherif, Boumahdi, Garici, and Schedler [2].*

2.6 Bibliography

[1] S. Akhtari, The Diophantine Equation $aX^4 - bY^2 = 1$, J. Reine Angew. Math. **630**, 33–57, 2009.

[2] F. Bencherif, R. Boumahdi, T. Garici, Z. Schedler, Upper bounds for the number of solutions for the Diophantine equation $y^2 = px(Ax^2 - C)$ $(C = 2, \pm 1, \pm 4)$, Colloquium Mathematicum **159**, 243–257, 2020.

[3] J. W. S. Cassels, A Diophantine equation, Glasg. Math. J. **27**, 11–18, 1985.

[4] L. M. Chen, On the Diophantine equation $y^2 = px(x^2 + 2)$, Acta Math. Sinica (Chin. Ser.), **50** (1), 83–86, 2010.

[5] J. H. Chen and P. M. Voutier, A complete solution of the Diophantine equation $x^2 + 1 = dy^4$ and a related family of quartic Thue equations, J. Number Theory **62**, 71–99, 1997.

[6] W. Ljunggren, Über die unbestimmte Gleichung $Ax^2 - By^4 = C$. Arch. Math. Naturvid **41** (10), 1–18, 1938.

[7] W. Ljunggren, Ein Satz über die Diophantische Gleichung $Ax^2 - By^4 = C(C = 1, 2, 4)$, in: Tolfte Skandinaviska Matematikerkongressen, Lund, 1953, Lunds Universitets Matematiska Inst., Lund, 188–194, 1954.

[8] F. Luca and P. G. Walsh, Squares in Lehmer sequences and some Diophantine applications, Acta Arith. **100**, 47–62, 2001.

[9] F. Luca and P. G. Walsh, On a Diophantine equation of Cassels, Glasg. Math. J. **47**, 303–307, 2005.

[10] A. Togbé, A note on the Diophantine equation $y^2 = px(Ax^2 + 2)$, Afrika Mat. (3) **25**, 739–744, 2014.

[11] A. Togbé, P. M. Voutier, and P. G. Walsh, Solving a family of Thue equations with an application to the equation $x^2 - dy^4 = 1$, Acta Arith. **120**, 39–58, 2005.

[12] P. Yuan, Rational and algebraic approximations of algebraic numbers and their applications, Sci. China Ser. A **40**, 1045–1051. 1997.

[13] P. Yuan and Y. Li, Squares in Lehmer sequences and the Diophantine equation $Ax^4 - By^2 = 2$, Acta Arith. **139**, 275–302., 2009.

Chapter 3

Polynomials with values which are powers of integers

3.1 Résumé

Shapiro a présenté le résultat suivant : si P et Q sont deux polynômes à valeurs entières de degrés p et q respectivement tels que q divise p et $P(n) = Q(m)$ pour une infinité de blocs d'entiers n de longeur $p/q + 2$, alors $P(x) = Q\big(R(x)\big)$ pour un certain polynôme R.

On réduit le nombre de blocs nécessaires lorsque $Q = x^q$ et P est aussi un polynôme à coefficients entiers. Le nombre présenté est fini, mais dépend sur les valeurs de P aux entiers dans un bloc initial. Donc, le résultat n'est pas calculable effectivement.

3.2 Abstract

Shapiro showed that if P and Q are integer-valued polynomials of degrees p and q respectively, such that $P(n) = Q(m)$ for infinitely many $p/q + 2$ length blocks of consecutive integers n, then $P(x) = Q\big(R(x)\big)$ for a polynomial R. We reduce the number of necessary blocks to being only finite in number when $Q(x) = x^q$. While a bound for the number of blocks is provided, the bound depends on the values of P at integers in some initial block. Consequently, the bound given is not effectively computable.

3.3 Introduction

Several authors have studied the integer solutions of the equation

$$y^m = P(x)$$

where $P(x)$ is a polynomial with rational coefficients, and $m \geq 2$ is an integer. If P is an irreducible polynomial of degree at least 3 with integer coefficients, then the above equation

is called a hyperelliptic equation if $m = 2$ and a superelliptic equation otherwise.

In 1969, Baker [1] gave an upper bound on the size of integer solutions of the hyperelliptic equation when $P(x) \in \mathbb{Z}[x]$ has at least three simple zeros, and for the superelliptic equation when $P(x) \in \mathbb{Z}[x]$ has at least two simple zeros.

Using a refinement of Baker's estimates and a criterion of Cassels concerning the shape of a potential integer solution to $x^p - y^q = 1$, Tijdeman [12] proved in 1976 that Catalan's equation $x^p - y^q = 1$ has only finitely many solutions in integers $p > 1$, $q > 1$, $x > 1$, $y > 1$.

Suppose that $y^m - P(x)$ is irreducible in $\mathbb{Q}[x, y]$ where P is monic and $\gcd(m, \deg P) > 1$. Under these conditions, Masser [7] considered the equation $y^m = P(x)$ in the particular case $m = 2$ and $\deg P = 4$. In particular, setting $P(x) = x^4 + ax^3 + bx^2 + cx + d$ where $P(x)$ is not a perfect square, it was shown that for $H \geq 1$ and $X(H)$ defined as the maximum of $|x|$ taken over all integer solutions of all equations $y^2 = P(x)$ with $\max\{|a|, |b|, |c|, |d|\} \leq H$, there are absolute constants $k > 0$ and K such that $kH^3 \leq X(H) \leq KH^3$. Walsh [14] later obtained an effective bound on the integer solutions for the general case. Poulakis [8] described an elementary method for computing the solutions of the equation $y^2 = P(x)$, where P is a monic quartic polynomial which is not a perfect square. Later, Szalay [11] established a generalization for the equation $y^q = P(x)$, where P is a monic polynomial and q divides $\deg P$.

Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_r$ are the roots of $P(x)$ with respective multiplicities $e_1, e_2, \ldots, e_r$. Given an integer $m \geq 3$, we define, for each $i = 1, \ldots, r$,

$$m_i = \frac{m}{(e_i, m)} \in \mathbb{N}.$$

It has been shown by LeVeque [6] that the superelliptic equation $y^m = P(x)$ can have infinitely many solutions in $\mathbb{Q}$ only if $(m_1, m_2, \ldots, m_r)$ is a permutation of either $(2, 2, 1, \ldots, 1)$ or $(t, 1, 1, \ldots, 1)$ with $t \geq 1$. In 1995, Voutier [13] gave improved bounds for the size of solutions (x_0, y_0) to the superelliptic equation with $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Q}$ under the conditions of LeVeque.

Given a polynomial $P(x) \in \mathbb{Z}[x]$ and an integer $q \geq 2$, it is then natural to ask when the equation

$$y^q - P(x) = 0$$

will have infinitely many solutions (x_0, y_0) with $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Q}$. It is clear that this will immediately be the case when $P(x) = \big(R(x)\big)^q$ for some polynomial $R(x) \in \mathbb{Q}[x]$. Indeed, this serves as our motivation.

In 1913, Grösch solved a problem proposed by Jentzsch [5], showing that if a polynomial $P(x)$ with integral coefficients is a square of an integer for all integral values of x, then $P(x)$ is the square of a polynomial with integral coefficients. Kojima [5], Fuchs [2], and Shapiro [10] later proved more general results. In particular, Shapiro proved that if $P(x)$ and $Q(x)$ are

polynomials of degrees p and q respectively, which are integer-valued at the integers, such that $P(n)$ is of the form $Q(m)$ for infinitely many blocks of consecutive integers of length at least $p/q+2$, then there is a polynomial $R(x)$ such that $P(x) = Q\big(R(x)\big)$.

Recall that the height of a polynomial

$$P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$$

is defined by

$$H(P) = \max_{i=0,\ldots,p} |a_i|$$

where $|a_i|$ denotes the modulus of $a_i \in \mathbb{C}$ for each $i = 0, \ldots, p$. We will prove the following result:

Theorem 3.3.1. *Let $P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_0$ be a polynomial with integral coefficients where $a_p > 0$, and let $q \geq 2$ be an integer that divides p. Suppose that there exist integers m_i, $i = 0, 1, \ldots, p/q+1$, such that $P(n_0 + i) = {m_i}^q$ for some consecutive integers*

$$n_0, n_0 + 1, \ldots, n_0 + p/q + 1$$

where

$$n_0 > 1 + (p/q+1)!pq^{p/q+1}H(P)^{p/q+2}\prod_{j=2}^{p/q+2}(jp-j+1)^2.$$

Set

$$M := \sum_{i=0}^{p/q+1}\binom{p/q+1}{i}|m_{p/q+1-i}|.$$

If there exist at least M more blocks of such consecutive integers $n_k + i$, $i = 0, \ldots, p/q+1$, such that $n_k > n_{k-1} + p/q + 1$ for each $k = 1, \ldots, M$ and $P(n_k + i) = m_{k,i}^q$ for all $k = 1, \ldots, M$ and $i = 0, \ldots, p/q+1$ for some integers $m_{k,i}$, then there exists a polynomial $R(x)$ such that $P(x) = \big(R(x)\big)^q$.

3.4 Preliminaries

Let $P(x)$ and $Q(x)$ be non-zero polynomials with integral coefficients of degrees p and q respectively. The following properties are easily verified:

(i) $H(P) \geq 1$

(ii) $H(P') \leq pH(P)$

(iii) $H(P+Q) \leq H(P) + H(Q)$

(iv) $H(PQ) \leq (1+p+q)H(P)H(Q)$

The first and second properties are trivial, while the third follows immediately from the triangle inequality. The last property follows by noting that the coefficient of x^k in the product of $a_p x^p + a_{p-1}x^{p-1} + \cdots + a_0$ and $b^q x^q + b_{q-1}x^{q-1} + \cdots + b_0$ is given by $\sum_{i+j=k} a_i b_j$, where the number of summands is at most $\lceil (p+q)/2 \rceil + 1 \leq 1 + p + q$.

We recall a result which can be found in Rolle [9], or which could also be easily deduced from Cauchy's bound on the roots of a polynomial (see for example the exposition in [3]).

Lemma 3.4.1. *Let $f(x) \in \mathbb{R}[x]$ be a non-zero monic polynomial. If $t \geq 1 + H(f)$, then $f(t) > 0$.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The result follows from writing $f(t)$ as

$$f(t) = t^{n-1}\left(t + \left(a_{n-1} + \frac{a_n - 2}{t} + \cdots + \frac{a_0}{t^{n-1}}\right)\right),$$

since from $t > 1$, we deduce that

$$\left|a_{n-1} + \frac{a_{n-2}}{t} + \cdots + \frac{a_0}{t^{n-1}}\right| \leq \sum_{i=0}^{n-1} |a_i|(1/t)^{n-1-i} \leq H(f)\frac{t}{t-1} < t,$$

and we conclude that $t + \left(a_{n-1} + \frac{a_n - 2}{t} + \cdots + \frac{a_0}{t^{n-1}}\right)$ is positive. □

We will also require the following lemma, which is implicit in the proof of the sole lemma in [10].

Lemma 3.4.2. *Let $f(x)$ be a branch of an algebraic function, real and regular for all $x > x_0$ for some x_0, and satisfying $|f(x)| < Cx^\alpha$ where $C > 0$ and $\alpha > 0$. Then $\lim_{x\to\infty} f^{(r+1)}(x) = 0$, where r is the least integer greater than or equal to α.*

We now establish a bound on the zeros of a particular class of algebraic functions.

Lemma 3.4.3. *Let $P(x)$ be a polynomial of degree p with integral coefficients, and let $f(x)$ be a branch of the algebraic function defined by the equation $y^q = P(x)$ where q is an integer greater than 1. For any integer $k \geq 2$, $R_k(x) = q^k f(x)^{kq-1} f^{(k)}(x)$ is a polynomial with integral coefficients such that $\deg R_k \leq k(p-1)$ and*

$$H(R_k) \leq (k-1)! p q^{k-1} H(P)^k \prod_{j=2}^{k} (jp - j + 1)^2.$$

Proof. Differentiating $f^q = P$ with respect to x, we obtain $q f^{q-1} f' = P'$. We have $\deg P' = p - 1$ and $H(P') \leq pH(P)$. We now consider $R_k = q^k f^{kq-1} f^{(k)}$ and prove the result by induction on k.

For the base case $k = 2$, we differentiate $qf^{q-1}f' = P'$ with respect to x to obtain

$$qf^{q-1}f'' + q(q-1)f^{q-2}f'f' = P''.$$

Multiplying both sides of this equation by qf^q, we obtain

$$\begin{aligned} q^2f^{2q-1}f'' + (q-1)(qf^{q-1}f')(qf^{q-1}f') &= qf^qP'', \\ q^2f^{2q-1}f'' + (q-1)P'P' &= qPP'', \end{aligned}$$

so that

$$R_2 = q^2f^{2q-1}f'' = qPP'' - (q-1)P'P'.$$

We then have

$$\begin{aligned} \deg R_2 &\leq \max\{p + \deg P'', \deg P' + \deg P'\} \\ &= \max\{p + (p-1) - 1, p - 1 + p - 1\} \\ &= 2(p-1), \end{aligned}$$

and

$$\begin{aligned} H(R_2) &\leq qH(PP'') + (q-1)H(P'P') \\ &\leq q(1 + p + \deg P'')H(P)H(P'') + q(1 + \deg P' + \deg P')H(P')H(P') \\ &\leq q(1 + p + p - 2)H(P)[\deg P'H(P')] + q(1 + 2p - 2)[pH(P)]^2 \\ &\leq q(2p-1)H(P)(p-1)[pH(P)] + q(2p-1)[pH(P)]^2 \\ &= pq(2p-1)H(P)^2[(p-1) + p] \\ &= pqH(P)^2(2p-1)^2. \end{aligned}$$

Therefore, the result holds for the base case.

We now assume that the result holds for some integer $k \geq 2$. Differentiating $R_k = q^kf^{kq-1}f^{(k)}$ with respect to x yields

$$q^kf^{kq-1}f^{(k+1)} + q^k(kq-1)f^{kq-2}f'f^{(k)} = {R_k}'.$$

Multiplying both sides of the equation by qf^q, we obtain

$$\begin{aligned} q^{k+1}f^{[k+1]q-1}f^{(k+1)} + (kq-1)[qf^{q-1}f'][q^kf^{kq-1}f^{(k)}] &= qf^q{R_k}', \\ q^{k+1}f^{[k+1]q-1}f^{(k+1)} + (kq-1)P'R_k &= qP{R_k}', \end{aligned}$$

so that

$$R_{k+1} = q^{k+1}f^{[k+1]q-1}f^{(k+1)} = qP{R_k}' - (kq-1)P'R_k.$$

By hypothesis, we have $\deg R_k \leq k(p-1)$. Thus,

$$\begin{aligned}
\deg R_{k+1} &\leq \max\{p + \deg R_k{}', \deg P' + \deg R_k\} \\
&= \max\{p + \deg R_k - 1, p - 1 + \deg R_k\} \\
&= p - 1 + \deg R_k \\
&\leq p - 1 + k(p-1) \\
&= (k+1)(p-1).
\end{aligned}$$

In addition,

$$\begin{aligned}
H(R_{k+1}) &\leq qH(PR_k{}') + (kq-1)H(P'R_k) \\
&\leq kq(1 + p + \deg R_k{}')H(P)H(R_k{}') \\
&\qquad + kq(1 + \deg P' + \deg R_k)H(P')H(R_k) \\
&\leq kq(p + \deg R_k)H(P)[\deg R_k H(R_k)] \\
&\qquad + kq(p + \deg R_k)[pH(P)]H(R_k) \\
&= kq(p + \deg R_k)^2 H(P)H(R_k).
\end{aligned}$$

By hypothesis, we have $\deg R_k \leq k(p-1)$ and

$$H(R_k) \leq (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp - j + 1)^2.$$

Thus,

$$\begin{aligned}
H(R_{k+1}) &\leq kq\big(p + k(p-1)\big)^2 H(P)(k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp - j + 1)^2 \\
&= k!pq^k H(P)^{k+1} \prod_{j=2}^{k+1}(jp - j + 1)^2,
\end{aligned}$$

proving the result. □

Corollary 3.4.4. *Let $P(x)$ be a polynomial of degree p with integral coefficients, and let $f(x)$ be a branch of the algebraic function defined by the equation $y^q = P(x)$ where q is an integer greater than 1. If β is a real zero of $f^{(k)}(x)$ for any integer $k \geq 2$ such that $\beta > 1 + H(P)$, then $\beta \leq 1 + (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp - j + 1)^2$.*

Proof. Let β be a zero of $f^{(k)}(x)$ such that $\beta > 1 + H(P)$. If $f(\beta) = 0$, then $0 = f(\beta)^q = P(\beta)$ and $\beta \leq 1 + H(P)$ by Lemma 3.4.1. We conclude that β is not a zero of $f(x)$.

Since β must be a zero of the polynomial $R_k = q^k f^{kq-1} f^{(k)}$, we conclude from Lemma 3.4.1 and Lemma 3.4.3 that

$$\beta \leq 1 + H(R_k) \leq 1 + (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp - j + 1)^2,$$

as claimed. □

For convenience, we define for all integers $k \geq 2$ the function

$$B(k) = 1 + (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp - j + 1)^2.$$

Defining the difference operator Δ by $\Delta f(x) = f(x+1) - f(x)$ and recursively defining higher order difference operators, we have the following lemma (see page 8 of [4]):

Lemma 3.4.5. *Let $k \geq 1$ be an integer. Then $\Delta^k f(x) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i f(x+k-i)$.*

3.5 Proof of Theorem 3.3.1

Proof. Let $x = \phi(y)$ denote the branch of the algebraic function inverse to the polynomial $y = x^q$, that is, $\phi(y) = y^{1/q}$. Then $\phi(y)$ is positive and free of singularities for all $y \geq 0$.

Set $f(x) = \phi\big(P(x)\big)$. Then $f(x)$ is asymptotically $a_p^{1/q}x^{p/q}$, and $f(n) = \pm m$ for any n such that $P(n) = m^q$.

We show by contradiction that $f(x)$ is a polynomial. Suppose that $f(x)$ is not a polynomial. Then $f^{(p/q+2)}(x)$ is not identically zero. By Corollary 3.4.4, any real zero β of $f^{(p/q+2)}(x)$ satisfying $\beta > 1 + H(P)$ must also satisfy $\beta \leq B(p/q+2)$. Thus, $f^{(p/q+1)}(x)$ is either monotone decreasing or monotone increasing for

$$x > B(p/q+2).$$

Suppose that $f^{(p/q+1)}(x)$ is monotone decreasing for $x > B(p/q+2)$ as described above. It must then be strictly positive for $x > B(p/q+2)$, since $\lim_{x\to\infty} f^{(p/q+1)}(x) = 0$ by Lemma 3.4.2.

Applying the difference operator Δ to $f(x)$ $p/q+1$ times, we find that $\Delta^{p/q+1}f(n_0)$ is an integer. We now apply the Mean Value Theorem repeatedly to obtain a number $c_0 \in (n_0, n_0 + p/q+1)$ such that $f^{(p/q+1)}(c_0) = \Delta^{p/q+1}f(n_0)$ is an integer.

For each $k = 1, \ldots, M$, we repeat the above process with each block of consecutive integers $n_k + i$, $i = 0, \ldots, p/q+1$, to obtain numbers c_k such that $c_k \in (n_k, n_k + p/q+1)$ and $f^{(p/q+1)}(c_k) = \Delta^{p/q+1}f(n_k)$ are integers.

By Lemma 3.4.5, the integer $f^{(p/q+1)}(c_0) = \Delta^{p/q+1} f(n_0)$ is such that

$$\begin{aligned} |f^{(p/q+1)}(c_0)| &= \left| \sum_{i=0}^{p/q+1} \binom{p/q+1}{i} (-1)^i f(n_0 + p/q + 1 - i) \right| \\ &\leq \sum_{i=0}^{p/q+1} \binom{p/q+1}{i} |m_{p/q+1-i}| \\ &= M. \end{aligned}$$

Since $f^{(p/q+1)}(x)$ is monotone decreasing, $f^{(p/q+1)}(c_k) < f^{(p/q+1)}(c_{k-1})$ for each $k = 1, \ldots, M$. Thus $f^{(p/q+1)}(c_j) \leq M - j$ for $j = 0, \ldots, M$. This implies that $f^{(p/q+1)}(c_M) \leq 0$, which contradicts $f^{(p/q+1)}(x)$ being strictly positive at

$$c_M > c_0 > n_0 > B(p/q + 2).$$

Similarly, the case where $f^{(p/q+1)}(x)$ is monotone increasing for $x > B(p/q + 2)$ leads to a contradiction. Therefore, $f(x)$ is a polynomial and $P(x) = f(x)^q$.

3.6 Bibliography

[1] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.*, **65** (1969), 439–444.

[2] W. H. J. Fuchs, A polynomial the square of another polynomial, *Amer. Math. Monthly*, **57** (1950), 114–116.

[3] H. P. Hirst, W. T. Macey, Bounding the Roots of Polynomials, *College Math. J.*< **28** (4), (1997), 292–295.

[4] C. Jordan, *Calculus of finite differences*, 2nd ed, Chelsea Publishing Company, New York, N.Y., 1950.

[5] T. Kojima, Note on number-theoretical properties of algebraic functions, *Tohoku Math. J.*, **8** (1915), 24–27.

[6] W. J. LeVeque, On the equation $y^m = f(x)$, *Acta. Arith.* **IX** (1964), 209–219.

[7] D. W. Masser, Polynomial bounds for Diophantine equations, *Amer. Math. Monthly*, **93** (1980), 486–488.

[8] D. Poulakis, A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, *Elem. Math.*, **54(1)** (1999), 32–36.

[9] M. Rolle, *Traité d'algèbre*, Paris, 1690.

[10] H. S. Shapiro, The range of an integer-valued polynomial, *Amer. Math. Monthly*, **64** (1957), 424–425.

[11] L. Szalay, Superelliptic equations of the form $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$, *Bull. Greek Math. Soc.*, **46** (2002), 23–33.

[12] R. Tijdeman, On the equation of Catalan, *Acta Arith.*, **29(2)** (1976), 197–209.

[13] P. M. Voutier, An upper bound for the size of integral solutions to $Y^m = f(X)$, *J. Number Theory*, **53** (1995), 247–271.

[14] P. G. Walsh, A quantitative version of Runge's theorem on Diophantine equations, *Acta Arith.*, **62(2)** (1992), 157–172.

Chapter 4

On the solutions to equations of the form $F_n \pm F_m = y^a$

4.1 Résumé

On résout l'équation $F_n - F_m = y^a$ pour les valeurs $y \in \{6, 11, 12\}$, ce qui démontre un cas de la conjecture d'Erduvan et Keskin. Les résultats suggèrent aussi une conjecture généralisée. De plus, on borne les solutions de l'équation $F_n + F_m = y^a$ pour $y \geq 3$ fixe en termes de la valeur y choisie.

4.2 Abstract

We solve the equation $F_n - F_m = y^a$ for the fixed values of $y \in \{6, 11, 12\}$, proving one case in the conjecture of Erduvan and Keskin as well as motivating an extended conjecture. Additionally, we consider the general equation $F_n + F_m = y^a$ and show that the number of solutions in non-negative integers (n, m, a) is finite when $y \geq 3$ is a fixed integer. A bound on the number of solutions is given in terms of the fixed value for y.

4.3 Introduction

The sequence of Fibonacci numbers is defined recursively as $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$. The sequence of Lucas numbers is similarly defined as $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for all $n \geq 2$. The negative terms of these sequences are defined by $F_{-n} = (-1)^{n+1} F_n$ and $L_{-n} = (-1)^n L_n$ respectively for $n \geq 1$. Finding all perfect powers in the Fibonacci sequence was a problem completely solved by Bugeaud, Mignotte, and Siksek, who approached it by combining linear forms in logarithms with modularity. Along with Luca, these four authors found all integer solutions to

$$F_n \pm 1 = y^a$$

for $a \geq 2$. Their proof uses a factorization that converts the problem into one of finding solutions of $F_n = y^a$.

Luca and Patel followed by considering the more general equation

$$F_n \pm F_m = y^a$$

for $a \geq 2$. They successfully showed that all integer solutions (n, m, y, a) with $n \equiv m \pmod 2$ satisfy either $y = 0$ and $|n| = |m|$, or $\max\{|n|, |m|\} \leq 36$. The general problem for n and m not congruent modulo 2 remains an open one.

Similar problems and particular cases of the above have been considered. Bravo and Luca solved the equation $F_n + F_m = 2^a$. Bravo, Gómez, and Luca then studied the equation $F_n^{(k)} + F_m^{(k)} = 2^a$ in integers n, m, k, a with $k \geq 2$ and $n \geq m$, where $F_n^{(k)}$ is the nth k-generalized Fibonacci number. This previous work followed after Bravo and Luca's solution to

$$F_n^{(k)} + F_m^{(k)} = d\left(\frac{10^\ell - 1}{9}\right),$$

with $\ell \geq 2$ and $1 \leq d \leq 9$. This was motivated in the context of repdigits: a positive integer that has only a single distinct digit when written in its decimal expansion.

Focusing strictly on non-negative integers n and m, the equation

$$F_n - F_m = y^a \tag{4.1}$$

has been a subject of study. Şiar and Keskin [8] solved this equation for $y = 2$ in non-negative integers (n, m, a), providing each of the solutions.

Erduvan and Keskin [5] provided the exact solutions to the equation for $y = 5$ in positive integers (n, m, a). In the same work, they conjecture that the equation has no solutions in non-negative integers n, m with $a \geq 2$ when $y > 7$ is prime (oddly, there seems to be no explanation on their part as to the omission of $y = 7$).

The aim of this work is to study the solutions in non-negative integers to equation (4.1) for $y \in \{6, 11, 12\}$. Specifically, we prove the following results:

Theorem 4.3.1. *The only solutions in non-negative integers (n, m, a) of*

$$F_n - F_m = 11^a \tag{4.2}$$

are $(n, m, a) \in \{(2, 0, 0), (3, 1, 0), (3, 2, 0), (4, 3, 0), (7, 3, 1)\}$.

Theorem 4.3.2. *The only solutions in non-negative integers (n, m, a) of*

$$F_n - F_m = 6^a \tag{4.3}$$

are $(n, m, a) \in \{(2, 0, 0), (3, 1, 0), (3, 2, 0), (4, 3, 0), (6, 3, 1)\}$.

Theorem 4.3.3. *The only solutions in non-negative integers (n, m, a) of*

$$F_n - F_m = 12^a \tag{4.4}$$

are $(n, m, a) \in \{(2, 0, 0), (3, 1, 0), (3, 2, 0), (4, 3, 0), (13, 11, 2), (14, 13, 2)\}$.

The case $y = 11$ is an obvious choice, since 11 is a prime number and the first open case in the conjecture of Erduvan and Keskin. We briefly justify the few reasons for considering the other two cases. The conjecture of Erduvan and Keskin is a statement for prime y, but composite values for y seem no less reasonable. Moreover, we may freely skip $y = 4 = 2^2$ as it is dealt with in the $y = 2$ case, and the next open case is $y = 6$. Once we allow for such composite y, it can be shown due to a theorem of Bugeaud, Mignotte, and Siksek [2] that there exist solutions when $y = 12$ and $a = 2$. In light of this, we also consider the case $y = 12$.

The related equation

$$F_n + F_m = y^a \tag{4.5}$$

has also seen some progress in this regard. Bravo and Luca [1] found all solutions to the equation when $y = 2$. We prove the following result:

Theorem 4.3.4. *For a fixed integer $y \geq 3$, a solution in non-negative integers (n, m, a) of*

$$F_n + F_m = y^a \tag{4.6}$$

satisfies

$$a < \max\{n, m\} < t^{\frac{\log t}{\log t - 2\log(\log t)}},$$

where

$$t := \frac{6.8C^2(\log y)^2 + (2C\log 20 + 4C\log 2)(\log y) + \log\sqrt{5}}{\log\frac{1+\sqrt{5}}{2}},$$

and $C := 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1 + \log 2)$.

4.4 Preliminaries

If η is an algebraic number of degree d with minimal polynomial

$$\sum_{i=0}^{d} a_i x^{d-i} = a_0 \prod_{i=1}^{d} \left(x - \eta^{(i)}\right) \in \mathbb{Z}[x],$$

where the a_i are relatively prime, a_0 positive, and the $\eta^{(i)}$ are the conjugates of η, then the logarithmic height of η is given by

$$h(\eta) := \frac{1}{d}\left(\log a_0 + \sum_{i=1}^{d} \log\left(\max\left\{|\eta^{(i)}|, 1\right\}\right)\right). \tag{4.7}$$

If $\eta = a/b$ is rational with $b > 1$ and a relatively prime, then $h(\eta) = \log(\max\{|a|, b\})$.

Three well-known properties of the logarithmic height follow.

$$h(\eta \pm \gamma) \leq h(\eta) + h(\gamma) + \log 2, \tag{4.8}$$

$$h(\eta\gamma^{\pm 1}) \leq h(\eta) + h(\gamma), \tag{4.9}$$

$$h(\eta^k) = |k|h(\eta), \quad k \in \mathbb{Q}. \tag{4.10}$$

The nth Fibonacci number can be described in the form

$$F_n = \frac{\alpha^n - \overline{\alpha}^n}{\sqrt{5}} \tag{4.11}$$

where $\alpha = (1 + \sqrt{5})/2$ and $\overline{\alpha}$ its conjugate.

We will require the following well-known identity, which is readily verified by induction:

$$\alpha^{n-2} \leq F_n \leq \alpha^{n-1} \tag{4.12}$$

for $n \geq 1$.

The following theorem is deduced from Corollary 2.3 of Matveev [7]:

Theorem 4.4.1. *Assume that $\gamma_1, \gamma_2, \ldots, \gamma_t$ are positive real algebraic numbers in a real algebraic number field K of degree D, $b_1, b_2, \ldots, b_t$ are rational integers, and*

$$\Lambda := \gamma_1^{b_1} \cdots \gamma_t^{b_t} - 1$$

is not zero. Then

$$|\Lambda| > \exp\left(-1.4 \cdot 30^{t+3} \cdot t^{4.5} \cdot D^2(1 + \log D)(1 + \log B)A_1A_2 \cdots A_t\right),$$

where

$$B \geq \max\{|b_1|, \ldots, |b_t|\}$$

and

$$A_i \geq \max\{Dh(\gamma_i), |\log \gamma_i|, 0.16\}$$

for all $i = 1, \ldots, t$.

The following result is Lemma 5 of Dujella and Pethö [4] provides a variant of Baker-Davenport reduction. For $x \in \mathbb{R}$, $\|x\| := \min\{|x - n| : n \in \mathbb{Z}\}$ denotes the distance from x to the nearest integer.

Lemma 4.4.2. *Let M be a positive integer, let p/q be a convergent of the continued fraction of the irrational number γ such that $q > 6M$, and let A, B, μ be some real numbers with $A > 0$ and $B > 1$. Let $\epsilon := \|\mu q\| - M\|\gamma q\|$. If $\epsilon > 0$, then there exists no solution to the inequality*

$$0 < |u\gamma - v + \mu| < AB^{-w},$$

in positive integers u, v, and w with $u \leq M$ and

$$w \geq \frac{\log(Aq/\epsilon)}{\log B}.$$

The following result combines Theorems 1 and 2 of Bugeaud, Migonette, and Siksek [2]:

Theorem 4.4.3. *The only perfect powers in the Fibonacci sequence are $F_0 = 0$, $F_1 = F_2 = 1$, $F_6 = 8$, and $F_{12} = 144$. The only perfect powers in the Lucas sequence are $L_1 = 1$ and $L_3 = 4$.*

The following well-known result can be extracted from Lemma 2.1 of Luca and Patel [6]:

Lemma 4.4.4. *Assume that $n \equiv m \pmod 2$. Then*

$$F_n - F_m = \begin{cases} F_{(n-m)/2}L_{(n+m)/2} & \text{if } n \equiv m \pmod 4; \\ F_{(n+m)/2}L_{(n-m)/2} & \text{if } n \equiv m+2 \pmod 4. \end{cases}$$

The following can be extracted from Theorem 1 of Bugeaud, Luca, Mignotte, and Siksek [3]:

Theorem 4.4.5. *If $F_n = 2^s y^b$ for some integers $n \geq 1$, $y \geq 1$, $b \geq 2$, and $s \geq 0$, then $n \in \{1, 2, 3, 6, 12\}$.*

4.5 Solutions to $F_n - F_m = 11^a$

Proof of Theorem 4.3.1. Assume that equation (4.2) holds. By inequality (4.12), we obtain

$$11^a = F_n - F_m < F_n < \alpha^{n-1} < 11^{n-1}. \tag{4.13}$$

This shows that $a < n - 1$.

If $n - m = 1$, then $F_{m-1} = 11^a$. By Theorem 4.4.3, we have solutions $(3, 2, 0)$ and $(4, 3, 0)$. If $n - m = 2$, then $F_{m+1} = 11^a$, and by Theorem 4.4.3 we have $(2, 0, 0)$ and $(3, 1, 0)$. Assume that $m \geq 1$ and $n - m \geq 3$. For $1 \leq m < n \leq 200$, a direct computation in Maple shows that the only solution is $(7, 3, 1)$.

Assume then that $n > 200$, $m \geq 1$, and $n - m \geq 3$. Equation (4.12) can be rewritten as

$$\frac{\alpha^n}{\sqrt{5}} - 11^a = F_m + \frac{\overline{\alpha}^n}{\sqrt{5}}$$

to yield

$$\left|\frac{\alpha^n}{\sqrt{5}} - 11^a\right| = \left|F_m + \frac{\overline{\alpha}^n}{\sqrt{5}}\right| \leq F_m + \frac{|\overline{\alpha}|^n}{\sqrt{5}} < \alpha^m + \frac{1}{2}\,.$$

We obtain

$$\left|1 - 11^a\alpha^{-n}\sqrt{5}\right| < \sqrt{5}\alpha^{m-n} + \frac{\sqrt{5}}{2}\alpha^{-n} = \sqrt{5}\alpha^{m-n}\left(1 + \frac{\alpha^{-m}}{2}\right) < \frac{4}{\alpha^{n-m}}\,. \tag{4.14}$$

We apply Theorem 4.4.1, setting $\gamma_1 := 11$, $\gamma_2 := \alpha$, $\gamma_3 := \sqrt{5}$, $b_1 := a$, $b_2 := -n$, and $b_3 := 1$. Since the γ_i are all positive real numbers lying in the field $K = \mathbb{Q}(\sqrt{5})$, we have $D = 2$. Define

$$\Lambda_1 := 11^a\alpha^{-n}\sqrt{5} - 1\,.$$

Then $\Lambda_1 \neq 0$, else $\alpha^{2n} = 5 \cdot 11^{2a} \in \mathbb{Q}$, which is impossible as α^{2n} is irrational. Since $h(\gamma_1) = \log 11 = 2.397895\ldots$, we take $A_1 := 4.8$. Since

$$h(\gamma_2) = \frac{\log\alpha}{2} = \frac{0.4812\ldots}{2}$$

and

$$h(\gamma_3) = \log\sqrt{5} = 0.8047\ldots$$

we can take $A_2 := 0.5$ and $A_3 := 1.7$. From $a < n - 1$, we deduce that

$$B := \max\{|b_1|, |b_2|, |b_3|\} = \max\{a, n, 1\} = n\,.$$

Inequality (4.14) and Theorem 4.4.1 together imply that

$$\frac{4}{\alpha^{n-m}} > |\Lambda_1| > \exp\Big(-1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1 + \log 2)(1 + \log n)(4.8)(0.5)(1.7)\Big)\,.$$

We obtain

$$(n - m)\log\alpha - \log 4 < 3.95655 \cdot 10^{12}(1 + \log n)\,. \tag{4.15}$$

We again rewrite equation (4.2):

$$\frac{\alpha^n}{\sqrt{5}} - \frac{\alpha^m}{\sqrt{5}} - 11^a = \frac{\overline{\alpha}^n}{\sqrt{5}} - \frac{\overline{\alpha}^m}{\sqrt{5}}\,.$$

Since $|\overline{\alpha}|^n + |\overline{\alpha}|^m < 2/3$ for all $n > 200$, we obtain

$$\left|\frac{\alpha^n(1 - \alpha^{m-n})}{\sqrt{5}} - 11^a\right| = \frac{|\overline{\alpha}|^n + |\overline{\alpha}|^m}{\sqrt{5}} < \frac{1}{3}$$

which yields

$$\left|1 - 11^a\alpha^{-n}\sqrt{5}(1 - \alpha^{m-n})^{-1}\right| < \frac{\sqrt{5}\alpha^{-n}(1 - \alpha^{m-n})^{-1}}{3}\,.$$

That $1 - \alpha^{m-n} > 1/3$ follows immediately from

$$\alpha^{m-n} = \frac{1}{\alpha^{n-m}} < \frac{1}{\alpha} < \frac{2}{3}\,,$$

which in turn implies that $(1-\alpha^{m-n})^{-1} < 3$. Then

$$\left|1 - 11^a \alpha^{-n} \sqrt{5}(1-\alpha^{m-n})^{-1}\right| < \frac{\sqrt{5}}{\alpha^n}\,. \tag{4.16}$$

We apply Theorem 4.4.1 once again. Take $\gamma_1 := 11$, $\gamma_2 := \alpha$, $\gamma_3 := \sqrt{5}(1-\alpha^{m-n})^{-1}$, $b_1 := a$, $b_2 := -n$, and $b_3 := 1$. The positive real numbers γ_1, γ_2, and γ_3 lie in $K = \mathbb{Q}(\sqrt{5})$, so we have $D = 2$. Set

$$\Lambda_2 := 11^a \alpha^{-n} \sqrt{5}(1-\alpha^{m-n})^{-1} - 1\,.$$

Then $\Lambda_2 \neq 0$, else $\overline{\alpha}^m = \overline{\alpha}^n$, which is impossible as $n > m$ by assumption. Since

$$h(\gamma_1) = \log 11 = 2.39789\ldots$$

and

$$h(\gamma_2) = \frac{\log \alpha}{2} = \frac{0.4812\ldots}{2}\,,$$

we take $A_1 := 4.8$ and $A_2 := 0.5$. Since

$$h(\gamma_3) \leq \log 2\sqrt{5} + (n-m)\frac{\log \alpha}{2}$$

by equations (4.8), (4.9), and (4.10), one can show that $|\log \gamma_3| < \log 5 + (n-m)\log \alpha$. As such, we take $A_3 := \log 20 + (n-m)\log \alpha$. It follows again that $B := n$, since $a < n-1$. From inequality (4.16), we then obtain

$$\frac{\sqrt{5}}{\alpha^n} > |\Lambda_2| > \exp\Big(-1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1+\log 2)(1+\log n)(4.8)(0.5)\big(\log 20 + (n-m)\log \alpha\big)\Big)$$

or

$$n \log \alpha - \log \sqrt{5} < 2.32738 \cdot 10^{12}(1+\log n)\big(\log 20 + (n-m)\log \alpha\big)\,. \tag{4.17}$$

We can now substitute inequality (4.15) into the above to obtain

$$n \log \alpha - \log \sqrt{5} < 2.32738 \cdot 10^{12}(1+\log n)\big(\log 20 + 3.95655 \cdot 10^{12}(1+\log n) + \log 4\big) \tag{4.18}$$

or

$$n < 1.91359 \cdot 10^{25} + 3.82717 \cdot 10^{25} \log n + 1.91359 \cdot 10^{25}(\log n)^2\,.$$

Then

$$n < 1.53087 \cdot 10^{26}(\log n)^2\,.$$

A quick computation with Maple yields $n < 7.2367 \cdot 10^{29}$.

Let

$$z_1 := a \log 11 - n \log \alpha + \log \sqrt{5}\,.$$

Then

$$|1 - e^{z_1}| < \frac{4}{\alpha^{n-m}}$$

by inequality (4.14). The inequality

$$\frac{\alpha^n}{\sqrt{5}} = F_n + \frac{\overline{\alpha}^n}{\sqrt{5}} > F_n - 1 \geq F_n - F_m = 11^a$$

implies that $11^a\sqrt{5}\alpha^{-n} < 1$, so that $z_1 < 0$. Since $4\alpha^{-(n-m)} < 0.95$ for $n - m \geq 3$, it follows that $e^{|z_1|} < 20$. Since $x < e^x - 1$ for positive x, we have

$$0 < |z_1| < e^{|z_1|} - 1 = e^{|z_1|}|1 - e^{z-1}| < 80\alpha^{-(n-m)}\,,$$

or

$$0 < \left| n - a\left(\frac{\log 11}{\log \alpha}\right) + \frac{\log\sqrt{5}}{\log\alpha}\right| < \frac{80}{\log\alpha}\alpha^{-(n-m)} \leq 166.3\alpha^{-(n-m)}\,. \tag{4.19}$$

We now look to apply Lemma 4.4.2: set $\gamma := \log 11/\log\alpha \notin \mathbb{Q}$, $\mu := \log\sqrt{5}/\log\alpha$, $A := 166.3$, $B := \alpha$, and $w := n - m$. Let $M := 7.2367 \cdot 10^{29}$. The denominator of the 61st convergent of γ, q_{61}, exceeds $6M$, and

$$\epsilon := \|\mu q_{61}\| - M\|\gamma q_{61}\| = 0.17976\ldots > 0\,.$$

Thus, inequality (4.19) has no solution for

$$n - m \geq \frac{\log(Aq_{61}/\epsilon)}{\log B} = 161.2955\ldots\,.$$

We obtain $n - m \leq 161$, which we now substitute into inequality (4.17) yielding

$$n < 3.89198 \cdot 10^{14}(1 + \log n),$$

which in turn yields $n < 1.4883 \cdot 10^{16}$.

We apply Lemma 4.4.2 again, now to reduce the bound for n. Let

$$z_2 := a\log 11 - n\log\alpha + \log\left(\sqrt{5}(1 - \alpha^{m-n})^{-1}\right).$$

By inequality (4.16),

$$|1 - e^{z_2}| < \frac{\sqrt{5}}{\alpha^n} < 3\alpha^{-n}\,.$$

If $z_2 > 0$, then $0 < z_2 < e^{z_2} - 1 < \sqrt{5}\alpha^{-n} < 1/2$, so that $e^{|z_2|} = e^{z_2} < 1/2 < 2$. If $z_2 < 0$, then $|1 - e^{z_2}| = 1 - e^{z_2} < \sqrt{5}\alpha^{-n} < 1/2$, which implies $e^{z_2} > 1/2$ so that $e^{|z_2|} = e^{-z_2} < 2$. Altogether,

$$0 < |z_2| < e^{|z_2|} - 1 = e^{|z_2|}|1 - e^{z_2}| < 6\alpha^{-n}\,.$$

From $0 < |z_2| < 6\alpha^{-n}$, we obtain

$$0 < \left| a\left(\frac{\log 11}{\log\alpha}\right) - n + \frac{\log\left(\sqrt{5}(1 - \alpha^{m-n})^{-1}\right)}{\log\alpha}\right| < \frac{6}{\log\alpha}\alpha^{-n} \leq 13\alpha^{-n}\,. \tag{4.20}$$

Set $\gamma := \log 11/\log \alpha$,

$$\mu_{n-m} := \frac{\log\left(\sqrt{5}(1-\alpha^{-(n-m)})^{-1}\right)}{\log \alpha},$$

$A := 13$, $B := \alpha$, $w := n$, and $M := 1.4883 \cdot 10^{16}$. The denominator of the 39th convergent of γ, q_{39}, exceeds $6M$, and

$$\epsilon := \|\mu_{n-m} q_{39}\| - M\|\gamma q_{39}\| \in [0.01031\ldots, 0.49629\ldots]$$

for all $n-m \in [3,161] \cap \mathbb{Z}$ with $n-m \neq 4$. We conclude by Lemma 4.4.2 that inequality (4.20) has no solution for

$$n = w \geq \frac{\log(Aq_{39}/\epsilon)}{\log B} \geq \frac{\log(Aq_{39}/0.01)}{\log B} = 103.2442$$

with $n-m \neq 4$. Since we assume that a solution has $n > 200$, we have reached a contradiction. The only possible remaining solutions occur when $n-m=4$, in which case

$$11^a = F_n - F_m = F_{m+4} - F_m = F_{m+3} + F_{m+2} - F_m = F_{m+3} + F_{m+1} = L_{m+2}$$

by the well-known identity $F_{\ell+1} + F_{\ell-1} = L_\ell$. By Theorem 4.4.3, this is impossible. □

Remark 4.5.1. *We note that the bounds for n and m provided by Theorem 4.3.1 also give bounds for the Fibonacci numbers F_n and F_m by inequality (4.12).*

4.6 Solutions to $F_n - F_m = y^a$ for $y \in \{6, 12\}$

Proof of Theorem 4.3.1. Assume that equation (4.3) holds. By inequality (4.12), we obtain

$$6^a = F_n - F_m < F_n < \alpha^{n-1} < 6^{n-1}. \tag{4.21}$$

This shows that $a < n-1$.

If $n-m=1$, then $F_{m-1} = 6^a$. By Theorem 4.4.3, we have solutions $(3,2,0)$ and $(4,3,0)$. If $n-m=2$, then $F_{m+1} = 6^a$, and by Theorem 4.4.3 we have $(2,0,0)$ and $(3,1,0)$. Assume that $m \geq 1$ and $n-m \geq 3$. For $1 \leq m < n \leq 200$, a direct computation in Maple shows that the only solution is $(6,3,1)$.

Assume then that $n > 200$, $m \geq 1$, and $n-m \geq 3$. Equation (4.12) can be rewritten as

$$\frac{\alpha^n}{\sqrt{5}} - 6^a = F_m + \frac{\overline{\alpha}^n}{\sqrt{5}}$$

to yield

$$\left|\frac{\alpha^n}{\sqrt{5}} - 6^a\right| = \left|F_m + \frac{\overline{\alpha}^n}{\sqrt{5}}\right| \leq F_m + \frac{|\overline{\alpha}|^n}{\sqrt{5}} < \alpha^m + \frac{1}{2}.$$

We obtain

$$\left|1 - 6^a \alpha^{-n}\sqrt{5}\right| < \sqrt{5}\alpha^{m-n} + \frac{\sqrt{5}}{2}\alpha^{-n} = \sqrt{5}\alpha^{m-n}\left(1 + \frac{\alpha^{-m}}{2}\right) < \frac{4}{\alpha^{n-m}}. \tag{4.22}$$

We apply Theorem 4.4.1, setting $\gamma_1 := 6$, $\gamma_2 := \alpha$, $\gamma_3 := \sqrt{5}$, $b_1 := a$, $b_2 := -n$, and $b_3 := 1$. Since the γ_i are all positive real numbers lying in the field $K = \mathbb{Q}(\sqrt{5})$, we have $D = 2$. Define

$$\Lambda_1 := 6^a \alpha^{-n} \sqrt{5} - 1 \,.$$

Then $\Lambda_1 \neq 0$, else $\alpha^{2n} = 5 \cdot 6^{2a} \in \mathbb{Q}$, which is impossible as α^{2n} is irrational. Since $h(\gamma_1) = \log 6 = 1.791759\ldots$, we take $A_1 := 3.6$. Since

$$h(\gamma_2) = \frac{\log \alpha}{2} = \frac{0.4812\ldots}{2}$$

and

$$h(\gamma_3) = \log \sqrt{5} = 0.8047\ldots$$

we can take $A_2 := 0.5$ and $A_3 := 1.7$. From $a < n - 1$, we deduce that

$$B := \max\{|b_1|, |b_2|, |b_3|\} = \max\{a, n, 1\} = n \,.$$

Inequality (4.22) and Theorem 4.4.1 together imply that

$$\frac{4}{\alpha^{n-m}} > |\Lambda_1| > \exp\Big(- 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1 + \log 2)(1 + \log n)(3.6)(0.5)(1.7) \Big) \,.$$

We obtain

$$(n - m) \log \alpha - \log 4 < 2.96741 \cdot 10^{12} (1 + \log n) \,. \tag{4.23}$$

We again rewrite equation (4.3):

$$\frac{\alpha^n}{\sqrt{5}} - \frac{\alpha^m}{\sqrt{5}} - 6^a = \frac{\overline{\alpha}^n}{\sqrt{5}} - \frac{\overline{\alpha}^m}{\sqrt{5}} \,.$$

Since $|\overline{\alpha}|^n + |\overline{\alpha}|^m < 2/3$ for all $n > 200$, we obtain

$$\left| \frac{\alpha^n (1 - \alpha^{m-n})}{\sqrt{5}} - 6^a \right| = \frac{|\overline{\alpha}|^n + |\overline{\alpha}|^m}{\sqrt{5}} < \frac{1}{3}$$

which yields

$$\left| 1 - 6^a \alpha^{-n} \sqrt{5} (1 - \alpha^{m-n})^{-1} \right| < \frac{\sqrt{5} \alpha^{-n} (1 - \alpha^{m-n})^{-1}}{3} \,.$$

That $1 - \alpha^{m-n} > 1/3$ follows immediately from

$$\alpha^{m-n} = \frac{1}{\alpha^{n-m}} < \frac{1}{\alpha} < \frac{2}{3} \,,$$

which in turn implies that $(1 - \alpha^{m-n})^{-1} < 3$. Then

$$\left| 1 - 6^a \alpha^{-n} \sqrt{5} (1 - \alpha^{m-n})^{-1} \right| < \frac{\sqrt{5}}{\alpha^n} \,. \tag{4.24}$$

We apply Theorem 4.4.1 once again. Take $\gamma_1 := 6$, $\gamma_2 := \alpha$, $\gamma_3 := \sqrt{5}(1 - \alpha^{m-n})^{-1}$, $b_1 := a$, $b_2 := -n$, and $b_3 := 1$. The positive real numbers γ_1, γ_2, and γ_3 lie in $K = \mathbb{Q}(\sqrt{5})$, so we have $D = 2$. Set

$$\Lambda_2 := 6^a \alpha^{-n} \sqrt{5} (1 - \alpha^{m-n})^{-1} - 1 \,.$$

Then $\Lambda_2 \neq 0$, else $\overline{\alpha}^m = \overline{\alpha}^n$, which is impossible as $n > m$ by assumption. Since

$$h(\gamma_1) = \log 6 = 1.79175\ldots$$

and

$$h(\gamma_2) = \frac{\log \alpha}{2} = \frac{0.4812\ldots}{2}\,,$$

we take $A_1 := 3.6$ and $A_2 := 0.5$. Since

$$h(\gamma_3) \leq \log 2\sqrt{5} + (n-m)\frac{\log \alpha}{2}$$

by equations (4.8), (4.9), and (4.10), one can show that $|\log \gamma_3| < \log 5 + (n-m)\log \alpha$. As such, we take $A_3 := \log 20 + (n-m)\log \alpha$. It follows again that $B := n$, since $a < n-1$. From inequality (4.24), we then obtain

$$\frac{\sqrt{5}}{\alpha^n} > |\Lambda_2| > \exp\Big(-1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1+\log 2)(1+\log n)(3.6)(0.5)\big(\log 20 + (n-m)\log \alpha\big)\Big)$$

or

$$n \log \alpha - \log \sqrt{5} < 1.74554 \cdot 10^{12}(1+\log n)\big(\log 20 + (n-m)\log \alpha\big)\,. \tag{4.25}$$

We can now substitute inequality (4.23) into the above to obtain

$$n \log \alpha - \log \sqrt{5} < 1.74554 \cdot 10^{12}(1+\log n)\big(\log 20 + 2.96741 \cdot 10^{12}(1+\log n) + \log 4\big) \tag{4.26}$$

or

$$n < 1.076394 \cdot 10^{25} + 2.152788 \cdot 10^{25} \log n + 1.076394 \cdot 10^{25}(\log n)^2\,.$$

Then

$$n < 4.305575 \cdot 10^{25}(\log n)^2\,.$$

A quick computation with Maple yields $n < 1.9587 \cdot 10^{29}$.

Let

$$z_1 := a \log 6 - n \log \alpha + \log \sqrt{5}\,.$$

Then

$$|1 - e^{z_1}| < \frac{4}{\alpha^{n-m}}$$

by inequality (4.22). The inequality

$$\frac{\alpha^n}{\sqrt{5}} = F_n + \frac{\overline{\alpha}^n}{\sqrt{5}} > F_n - 1 \geq F_n - F_m = 6^a$$

implies that $6^a\sqrt{5}\alpha^{-n} < 1$, so that $z_1 < 0$. Since $4\alpha^{-(n-m)} < 0.95$ for $n - m \geq 3$, it follows that $e^{|z_1|} < 20$. Since $x < e^x - 1$ for positive x, we have

$$0 < |z_1| < e^{|z_1|} - 1 = e^{|z_1|}|1 - e^{z-1}| < 80\alpha^{-(n-m)}\,,$$

or

$$0 < \left| n - a\left(\frac{\log 6}{\log \alpha}\right) + \frac{\log \sqrt{5}}{\log \alpha} \right| < \frac{80}{\log \alpha}\alpha^{-(n-m)} \leq 166.3\alpha^{-(n-m)}\,. \tag{4.27}$$

We now look to apply Lemma 4.4.2: set $\gamma := \log 6/\log \alpha \notin \mathbb{Q}$, $\mu := \log \sqrt{5}/\log \alpha$, $A := 166.3$, $B := \alpha$, and $w := n - m$. Let $M := 1.9587 \cdot 10^{29}$. The denominator of the 57th convergent of γ, q_{57}, exceeds $6M$, and

$$\epsilon := \|\mu q_{57}\| - M\|\gamma q_{57}\| = 0.01556\ldots > 0\,.$$

Thus, inequality (4.27) has no solution for

$$n - m \geq \frac{\log(Aq_{57}/\epsilon)}{\log B} = 163.6257\ldots\,.$$

We obtain $n - m \leq 163$, which we now substitute into inequality (4.25) yielding

$$n < 2.9539 \cdot 10^{14}(1 + \log n),$$

which in turn yields $n < 1.1212 \cdot 10^{16}$.

We apply Lemma 4.4.2 again, now to reduce the bound for n. Let

$$z_2 := a \log 6 - n \log \alpha + \log\left(\sqrt{5}(1 - \alpha^{m-n})^{-1}\right).$$

By inequality (4.24),

$$|1 - e^{z_2}| < \frac{\sqrt{5}}{\alpha^n} < 3\alpha^{-n}\,.$$

If $z_2 > 0$, then $0 < z_2 < e^{z_2} - 1 < \sqrt{5}\alpha^{-n} < 1/2$, so that $e^{|z_2|} = e^{z_2} < 1/2 < 2$. If $z_2 < 0$, then $|1 - e^{z_2}| = 1 - e^{z_2} < \sqrt{5}\alpha^{-n} < 1/2$, which implies $e^{z_2} > 1/2$ so that $e^{|z_2|} = e^{-z_2} < 2$. Altogether,

$$0 < |z_2| < e^{|z_2|} - 1 = e^{|z_2|}|1 - e^{z_2}| < 6\alpha^{-n}\,.$$

From $0 < |z_2| < 6\alpha^{-n}$, we obtain

$$0 < \left| a\left(\frac{\log 6}{\log \alpha}\right) - n + \frac{\log\left(\sqrt{5}(1 - \alpha^{m-n})^{-1}\right)}{\log \alpha} \right| < \frac{6}{\log \alpha}\alpha^{-n} \leq 13\alpha^{-n}\,. \tag{4.28}$$

Set $\gamma := \log 6/\log \alpha$,

$$\mu_{n-m} := \frac{\log\left(\sqrt{5}(1 - \alpha^{-(n-m)})^{-1}\right)}{\log \alpha},$$

$A := 13$, $B := \alpha$, $w := n$, and $M := 1.4883 \cdot 10^{16}$. The denominator of the 35th convergent of γ, q_{35}, exceeds $6M$, and

$$\epsilon := \|\mu_{n-m} q_{35}\| - M\|\gamma q_{35}\| \in [0.002787\ldots, 0.491883\ldots]$$

for all $n-m \in [3,163] \cap \mathbb{Z}$ with $n-m \neq 4$. We conclude by Lemma 4.4.2 that inequality (4.28) has no solution for

$$n = w \geq \frac{\log(Aq_{35}/\epsilon)}{\log B} \geq \frac{\log(Aq_{35}/0.00278)}{\log B} = 102.5494\ldots$$

with $n-m \neq 4$. Since we assume here that $n > 200$, we conclude that there are no solutions when $n-m \neq 4$. The remaining case yields

$$6^a = F_n - F_m = F_{m+4} - F_m = F_{m+3} + F_{m+2} - F_m = F_{m+3} + F_{m+1} = L_{m+2}$$

by the well-known identity $F_{\ell+1} + F_{\ell-1} = L_\ell$. By Theorem 4.4.3, this is impossible. □

Proof of theorem 4.3.3. The same method used to prove Theorems 4.3.1 and 4.3.2 can be used to show this result. Since the proof follows with only some slight differences in computation, we simply detail these differences here. If $n-m = 1$, then $F_{m-1} = 12^a$. By Theorem 4.4.3, we have solutions $(3,2,0)$, $(4,3,0)$, and $(14,13,2)$. If $n-m = 2$, then $F_{m+1} = 12^a$, and by Theorem 4.4.3 we have $(2,0,0)$, $(3,1,0)$, and $(13,11,2)$. Assume that $m \geq 1$ and $n-m \geq 3$. For $1 \leq m < n \leq 200$, a direct computation in Maple shows that the only solutions are $(7,1,1)$ and $(7,2,1)$.

Assume then that $n > 200$, $m \geq 1$, and $n-m \geq 3$. Proceeding as in the previous section, the first application of Theorem 4.4.1 yields

$$(n-m)\log\alpha - \log 4 < 4.12141 \cdot 10^{12}(1+\log n)\,.$$

The second application yields

$$n < 1.494987 \cdot 10^{25} + 2.989974 \cdot 10^{25}\log n + 1.494987 \cdot 10^{25}(\log n)^2\,.$$

Then

$$n < 5.979947 \cdot 10^{25}(\log n)^2\,.$$

A quick computation with Maple gives $n < 2.74773 \cdot 10^{29}$. Continuing , the first application of Lemma 4.4.2 yields

$$q_{64} > 6M, \epsilon = 0.3193598\ldots > 0\,,$$

so there is no solution for

$$n - m \geq 161.6677955\ldots\,.$$

Then $n-m \leq 161$. By substitution, this bound for $n-m$ gives

$$n < 4.05415 \cdot 10^{14}(1+\log n)\,,$$

and Maple then gives $n < 1.551963 \cdot 10^{16}$. The second application of Lemma 4.4.2 yields $q_{40} > 6M$ and $\epsilon \in [0.0066\ldots, 0.4930\ldots]$ for all $n-m \in [3,161] \cap \mathbb{Z}$ with $n-m \neq 4, 24$. Then

there is no solution for $n \geq 103.506$. Again, there is no solution for $n - m = 4$, so only the case $n - m = 24$ remains. In this final case, we have $12^a = F_n - F_m = F_{12}L_{m+12} = 144L_{m+12}$ by Lemma 4.4.4. Since $12^{a-2} = L_{m+12}$ cannot be satisfied for $a \geq 2$ and non-negative m, this case is impossible. □

4.7 On the solutions to $F_n + F_m = y^a$ for fixed y

We first prove the following lemma:

Lemma 4.7.1. *Let $t > 0$, and set $\varepsilon := 1 - 2\frac{\log(\log t)}{\log t}$. If $t^{1/\varepsilon} > e^e$, then there are no positive integers n such that $t^{1/\varepsilon} \leq n < t(\log n)^2$.*

Proof. Consider the real-valued function

$$g(x) := 1 - 2\frac{\log(\log x)}{\log x}$$

of the real variable x. It is straightforward to show that $g' > 0$ when $\log(\log x) > 1$, that is, $x > e^e$. If $t > e^e$, then $t^{1/\varepsilon} > t > e^e$, and it follows that $\varepsilon = g(t) < g(x)$ for $x > t$. From this, we obtain $\log\left((\log x)^2\right) < (1 - \varepsilon)\log x$ or $(\log x)^2 < x^{1-\varepsilon}$ for all $x > t$. The assumption that $t^{1/\varepsilon} \leq n < t(\log n)^2$ leads to

$$n < t(\log n)^2 < tn^{1-\varepsilon}\,,$$

implying that $n^\varepsilon < t$, which is a contradiction. □

Proof of Theorem 4.3.4. Assume that equation (4.6) holds. We may assume without loss of generality that $m \leq n$. If $n = m$, we obtain $y^a = F_n + F_m = 2F_n$. Solving this equation is equivalent to solving $F_n = 2^{a-1}w^a$, and the result follows by Theorem 4.4.5. We may now assume that $m < n$. By inequality (4.12), we obtain

$$y^a = F_n + F_m \leq F_n + F_{n-1} = F_{n+1} < \alpha^n < y^n\,. \tag{4.29}$$

This shows that $a < n$.

If $n - m = 1$, then $F_{m-1} = y^a$. By Theorem 4.4.3, we have $n \leq 12$. If $n - m = 2$, then $F_{m+1} = y^a$, and by Theorem 4.4.3 we again have $n \leq 12$.

Assume that $m \geq 1$ and $n - m \geq 3$. Equation (4.6) can be rewritten as

$$\frac{\alpha^n}{\sqrt{5}} - y^a = \frac{\overline{\alpha}^n}{\sqrt{5}} - F_m$$

to yield

$$\left|\frac{\alpha^n}{\sqrt{5}} - y^a\right| = \left|\frac{\overline{\alpha}^n}{\sqrt{5}} - F_m\right| \leq F_m + \frac{|\overline{\alpha}|^n}{\sqrt{5}} < \alpha^m + \frac{1}{2}\,.$$

We obtain

$$\left|1 - y^a \alpha^{-n} \sqrt{5}\right| < \sqrt{5}\alpha^{m-n} + \frac{\sqrt{5}}{2}\alpha^{-n} = \sqrt{5}\alpha^{m-n}\left(1 + \frac{\alpha^{-m}}{2}\right) < \frac{4}{\alpha^{n-m}}\,. \tag{4.30}$$

We apply Theorem 4.4.1, setting $\gamma_1 := y$, $\gamma_2 := \alpha$, $\gamma_3 := \sqrt{5}$, $b_1 := a$, $b_2 := -n$, and $b_3 := 1$. Since the γ_i are all positive real numbers lying in the field $K = \mathbb{Q}(\sqrt{5})$, we have $D = 2$. Define

$$\Lambda_1 := y^a \alpha^{-n}\sqrt{5} - 1\,.$$

Then $\Lambda_1 \neq 0$, else $\alpha^{2n} = 5 \cdot y^{2a} \in \mathbb{Q}$, which is impossible as α^{2n} is irrational. Since $h(\gamma_1) = \log y$, we take $A_1 := 2\log y$. Since

$$h(\gamma_2) = \frac{\log \alpha}{2} = \frac{0.4812\ldots}{2}$$

and

$$h(\gamma_3) = \log\sqrt{5} = 0.8047\ldots$$

we can take $A_2 := 0.5$ and $A_3 := 1.7$. From $a < n$, we deduce that

$$B := \max\{|b_1|, |b_2|, |b_3|\} = \max\{a, n, 1\} = n\,.$$

Inequality (4.30) and Theorem 4.4.1 together imply that

$$\frac{4}{\alpha^{n-m}} > |\Lambda_1| > \exp\Big(-1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1+\log 2)(1+\log n)(2\log y)(0.5)(1.7)\Big)\,.$$

Set $C := 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1+\log 2)$. We obtain

$$(n-m)\log\alpha - \log 4 < 1.7C(\log y)(1+\log n)\,. \tag{4.31}$$

We again rewrite equation (4.6):

$$\frac{\alpha^n}{\sqrt{5}} + \frac{\alpha^m}{\sqrt{5}} - y^a = \frac{\overline{\alpha}^n}{\sqrt{5}} + \frac{\overline{\alpha}^m}{\sqrt{5}}\,.$$

Since $|\overline{\alpha}|^n + |\overline{\alpha}|^m \leq |\overline{\alpha}|^4 + |\overline{\alpha}| < 1$, we obtain

$$\left|\frac{\alpha^n(1+\alpha^{m-n})}{\sqrt{5}} - y^a\right| \leq \frac{|\overline{\alpha}|^n + |\overline{\alpha}|^m}{\sqrt{5}} < \frac{1}{\sqrt{5}}$$

which yields

$$\left|1 - y^a\alpha^{-n}\sqrt{5}(1+\alpha^{m-n})^{-1}\right| < \alpha^{-n}(1+\alpha^{m-n})^{-1}\,.$$

It follows immediately from $\alpha^{m-n} > 0$ that $1 + \alpha^{m-n} > 1$, which in turn implies that $(1 - \alpha^{m-n})^{-1} < 1$. Then

$$\left|1 - y^a\alpha^{-n}\sqrt{5}(1+\alpha^{m-n})^{-1}\right| < \frac{1}{\alpha^n}\,. \tag{4.32}$$

We apply Theorem 4.4.1 once again. Take $\gamma_1 := y$, $\gamma_2 := \alpha$, $\gamma_3 := \sqrt{5}(1+\alpha^{m-n})^{-1}$, $b_1 := a$, $b_2 := -n$, and $b_3 := 1$. The positive real numbers γ_1, γ_2, and γ_3 lie in $K = \mathbb{Q}(\sqrt{5})$, so we have $D = 2$. Set

$$\Lambda_2 := y^a\alpha^{-n}\sqrt{5}(1+\alpha^{m-n})^{-1} - 1\,.$$

Then $\Lambda_2 \neq 0$, else $|\overline{\alpha}|^m = |\overline{\alpha}|^n$, which is impossible as $n > m$ by assumption. Since

$$h(\gamma_1) = \log y$$

and

$$h(\gamma_2) = \frac{\log \alpha}{2} = \frac{0.4812\ldots}{2},$$

we take $A_1 := 2\log y$ and $A_2 := 0.5$. Since

$$h(\gamma_3) \leq \log 2\sqrt{5} + (n-m)\frac{\log \alpha}{2}$$

by equations (4.8), (4.9), and (4.10), one can show that $|\log \gamma_3| < \log 5 + (n-m)\log \alpha$. As such, we take $A_3 := \log 20 + (n-m)\log \alpha$. It follows again that $B := n$, since $a < n$. From inequality (4.32), we then obtain

$$\frac{1}{\alpha^n} > |\Lambda_2| > \exp\Big(- C(1+\log n)(2\log y)(0.5)\big(\log 20 + (n-m)\log \alpha\big)\Big)$$

or

$$n\log \alpha < C(\log y)(1+\log n)\big(\log 20 + (n-m)\log \alpha\big). \tag{4.33}$$

We can now substitute inequality (4.31) into the above to obtain

$$n\log \alpha < C(\log y)(1+\log n)\big(\log 20 + 1.7C(\log y)(1+\log n) + \log 4\big). \tag{4.34}$$

With the inequality $1 \leq \log n \leq (\log n)^2$, we then have

$$n \leq \frac{6.8C^2(\log y)^2 + (2C\log 20 + 4C\log 2)(\log y)}{\log \alpha}(\log n)^2.$$

Setting

$$t := \frac{6.8C^2(\log y)^2 + (2C\log 20 + 4C\log 2)(\log y)}{\log \alpha},$$

application of Lemma 4.7.1 implies that

$$n < t^{\frac{\log t}{\log t - 2\log(\log t)}},$$

since $t > e^e$. □

Remark 4.7.2. *We note that the bounds for n and m provided by Theorems 4.3.1 4.3.2, 4.3.3, and 4.3.4 also give corresponding bounds for the Fibonacci numbers F_n and F_m by inequality (4.12).*

Remark 4.7.3. *Based on the results from completely solving the listed equations in non-negative integers (n, m, a), it seems reasonable to extend the conjecture of Erduvan and Keskin to composite $y \neq 12$ as well.*

4.8 Bibliography

[1] J.J. Bravo and F. Luca, On the Diophantine equation $F_n + F_m = 2^a$. *Quaest. Math.* **39** (3), 391–400, (2016).

[2] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers, *Annals of Mathematics*, **163** (3), 969–1018, (2006).

[3] Y. Bugeaud, F. Luca, M. Mignotte, S. Siksek, Perfect powers from products of terms in Lucas sequences. *J. Reine Angew. Math.* **661**, 109–129, (2007).

[4] A. Dujella and A. Pethö, A generalization of a theorem of Baker and Davenport, *Quarterly Journal of Mathematics*, **49** (3), 291–206, (1998).

[5] F. Erduvan and R. Keskin, non-negative integer solutions of the equation $F_n - F_m = 5^a$, *Turk J Math*, **43**, 1115–1123, (2019).

[6] F. Luca and V. Patel, On perfect powers that are sums of two Fibonacci numbers, *Journal of Number Theory*, **189**, 90–98, (2018).

[7] E.M. Matveev, An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II, *Izvestiya Akademii Nauk Series Mathematics*, **64** (6), 125–180, (2000) (in Russian).

[8] Z. Şiar and R. Keskin, On the equation $F_n - F_m = 2^a$, *Colloq. Math.*, **159** (1), 119–126, (2020).

Chapter 5

A New Proof of the Carlitz-Lutz Theorem

5.1 Résumé

On améliore le résultat de Carlitz et Lutz, présentant des conditions suffisantes et nécessaires qu'un polynôme soit polynôme de permutation.

5.2 Abstract

We refine the result of Carlitz and Lutz, providing necessary and sufficient conditions for a polynomial to be a permutation polynomial.

5.3 Introduction

Let $\mathbb{F}_q$ be the finite field of q elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a permutation polynomial if the induced map from $\mathbb{F}_q$ to $\mathbb{F}_q$ is bijective. Permutation polynomials form an active area of research, and one can find many open problems and conjectures relating to them (see [4] for many such examples).

Denote the unique representative of $f(x)$ modulo $x^q - x$ with degree less than q by $\overline{f(x)}$. The most well-known criterion for classifying permutation polynomials is described by Hermite's criterion (see page 59 of [3]):

Theorem 5.3.1. *Let $f(x) \in \mathbb{F}_q[x]$. Then $f(x)$ is a permutation polynomial if and only if*

(i) $\deg \overline{f(x)^\ell} \leq q-2$ *for* $1 \leq \ell \leq q-2$;

(ii) $f(x)$ *has a unique root in* $\mathbb{F}_q$.

Ayad, Belghaba, and Kihel [1] improved this criterion for binomials ax^n+x^m, showing that one need only check those ℓ in (i) that are divisible by $\gcd(n-m, q-1)$. Carlitz and Lutz [2] gave a variant of the Hermite-Dickson theorem, providing sufficient conditions for a polynomial to be a permutation polynomial:

Theorem 5.3.2. *Let $f(x) \in \mathbb{F}_q[x]$. Suppose that*

(i) $\deg \overline{f(x)^\ell} \leq q-2$ *for* $1 \leq \ell \leq q-2$;

(ii) $\deg \overline{f(x)^{q-1}} = q-1$.

Then $f(x)$ is a permutation polynomial.

In this paper, we refine Theorem 5.3.2, proving the following result:

Theorem 5.3.3. *Let $f(x) \in \mathbb{F}_q[x]$. Then the following conditions are equivalent:*

(i) $\deg \overline{f(x)^\ell} \leq q-2$ *for* $1 \leq \ell \leq q-2$, *and* $\deg \overline{f(x)^{q-1}} = q-1$.

(ii) $\deg \overline{f(x)^\ell} \leq q-2$ *for each* $1 \leq \ell \leq q-2$ *relatively prime to char*$(\mathbb{F}_q)$, *and* $\deg \overline{f(x)^{q-1}} = q-1$.

(iii) $f(x)$ is a permutation polynomial.

5.3.1 Preliminary Results

Let $x_1, \ldots, x_n$ be n variables. For each $k \in \{1, \ldots, n\}$, let

$$s_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k}$$

be the elementary symmetric polynomial of degree k in n variables, and let

$$\sigma_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k$$

be the power sum symmetric polynomial of degree k in n variables, with the conventional definition $\sigma_0(x_1, \ldots, x_n) = n$. The polynomials s_k and σ_k satisfy the relation

$$\sigma_k - s_1\sigma_{k-1} + \cdots + (-1)^k k s_k = 0 \qquad \text{for} \quad 1 \leq k \leq n, \tag{5.1}$$

the validity of which is demonstrated in [6].

A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if $f(\mathbb{F}_q) = \mathbb{F}_q$, which is equivalent to

$$\prod_{c \in \mathbb{F}_q} \big(x - f(c)\big) = \prod_{c \in \mathbb{F}_q} \big(x - c\big) = x^q - x. \tag{5.2}$$

Let $c_1, \ldots, c_q$ be the distinct elements of $\mathbb{F}_q$. By expanding the left-hand side of equation 5.2 and identifying its coefficients with those of $x^q - x$, we deduce that $f(x)$ is a permutation polynomial if and only if

$$s_k\big(f(c_1), \ldots, f(c_q)\big) = 0$$

for each $k \in \{1, \ldots, q-2\}$ and

$$s_{q-1}\big(f(c_1), \ldots, f(c_q)\big) = -1.$$

Consider any map $\tau : \mathbb{F}_q \to \mathbb{F}_q$. There exists a unique polynomial $g(x) \in \mathbb{F}_q[x]$ of degree less than q such that $g(c) = \tau(c)$ for all $c \in \mathbb{F}_q$, and the well-known formula [5]

$$g(x) = \sum_{c \in \mathbb{F}_q} \big(1 - (x-c)^{q-1}\big)\tau(c)$$

provides an expression for $g(x)$. This expression implies that $\deg g \leq q-2$ if and only if

$$\sum_{c \in \mathbb{F}_q} \tau(c) = \sum_{c \in \mathbb{F}_q} g(c) = 0.$$

5.4 Proof of Theorem 5.3.3

Proof of Theorem 5.3.3. The implication $(i) \Rightarrow (ii)$ is clear.

To prove the implication $(ii) \Rightarrow (iii)$, let $p = \mathrm{char}(\mathbb{F}_q)$, and suppose that $\deg \overline{f(x)^\ell} \leq q-2$ for each $\ell \in \{1, \ldots, q-2\}$ such that $\gcd(p, \ell) = 1$ and $\deg \overline{f(x)^{q-1}} = q-1$. Set $a := \sigma_{q-1}\big(f(c_1), \ldots, f(c_q)\big)$. Then $a \neq 0$, and

$$\sigma_\ell\big(f(c_1), \ldots, f(c_q)\big) = 0 \tag{5.3}$$

for each $\ell \in \{1, \ldots, q-2\}$ not divisible by p. We show that

$$s_\ell\big(f(c_1), \ldots, f(c_q)\big) = \sigma_\ell\big(f(c_1), \ldots, f(c_q)\big) \tag{5.4}$$

for all $\ell \in \{1, \ldots, q-1\}$ not divisible by p.

The statement is clear for $\ell = 1$, so let $e \in \{2, \ldots, q-1\}$ be such that p does not divide e and assume that equation 5.4 holds for all $\ell \in \{1, \ldots, e-1\}$ such that p does not divide ℓ. We write equation 5.1 in the form

$$\sigma_e\big(f(c_1), \ldots, f(c_q)\big) + \sum (-1)^u s_u\big(f(c_1), \ldots, f(c_q)\big)\sigma_v\big(f(c_1), \ldots, f(c_q)\big) + (-1)^e e s_e\big(f(c_q), \ldots, f(c_q)\big) = 0 \tag{5.5}$$

where the sum runs over all pairs (u, v) such that $u + v = e$ and $u, v \in \{1, \ldots, e-1\}$. Letting (u, v) be any such pair, if p does not divide u, then $s_u\big(f(c_1), \ldots, f(c_q)\big) = 0$ by hypothesis. If

p does divide u, then p does not divide v, so that $\sigma_v\big(f(c_1),\ldots,f(c_q)\big)=0$. Equation (5.5) is then reduced to

$$\sigma_e\big(f(c_1),\ldots,f(c_q)\big)=(-1)^{e+1}es_e\big(f(c_1),\ldots,f(c_q)\big),$$

and equation 5.3 implies that

$$s_e\big(f(c_1),\ldots,f(c_q)\big)=\sigma_e\big(f(c_q),\ldots,f(c_q)\big)=0$$

for each $e\in\{2,\ldots,q-2\}$ not divisible by p and

$$s_{q-1}\big(f(c_1),\ldots,f(c_q)\big)=\sigma_{q-1}\big(f(c_1),\ldots,f(c_q)\big)=a.$$

Let

$$h(x)=\prod_{c\in\mathbb{F}_q}\big(x-f(c)\big).$$

Expanding $h(x)$ yields an expression of the form

$$h(x)=x^q+ax+\sum_{p|i}a_ix^i,$$

from which it is apparent that $h'(x)=a\neq 0$. Thus, $h(x)$ is separable, implying that $f(x)$ is a permutation polynomial.

To prove the implication $(iii)\Rightarrow(i)$, we suppose that $f(x)$ is a permutation polynomial. Then

$$s_\ell\big(f(c_1),\ldots,f(c_q)\big)=0$$

for $\ell\in\{1,\ldots,q-2\}$ and $s_{q-1}\big(f(c_1),\ldots,f(c_q)\big)=-1$. Equation 5.1 immediately implies that

$$\sigma_\ell\big(f(c_1),\ldots,f(c_q)\big)=0$$

for $\ell\in\{1,\ldots,q-2\}$ and $\sigma_{q-1}\big(f(c_1),\ldots,f(c_q)\big)=-1$. It follows that

$$\sum_{c\in\mathbb{F}_q}f(c)^\ell=0$$

for $\ell\in\{1,\ldots,q-2\}$ and

$$\sum_{c\in\mathbb{F}_q}f(c)^{q-1}=-1.$$

Therefore, $\deg\overline{f(x)^\ell}\leq q-2$ for $\ell\in\{1,\ldots,q-2\}$ and $\deg\overline{f(x)^{q-1}}=q-1$. □

We state and prove an immediate consequence of Theorem 5.3.3:

Corollary 5.4.1. *Let $f(x)\in\mathbb{F}_q[x]$. Then the following are equivalent:*

(i) $f(x)$ *is a permutation polynomial.*

(ii) For any polynomial $u(x) \in \mathbb{F}_q[x]$, $\deg \overline{u(x)} = q-1$ *if and only if* $\deg \overline{u\big(f(x)\big)} = q-1$.

Proof. Suppose that $f(x)$ is a permutation polynomial, and let $u(x) \in \mathbb{F}_q[x]$ be such that $\deg \overline{u(x)} = q-1$. By Theorem 5.3.3, we then have $\deg \overline{u\big(f(x)\big)} = q-1$.

Conversely, let $u_i(x) = x^i$ for each $i \in \{1, \ldots, q-1\}$. Then $\overline{u_i\big(f(x)\big)} = \overline{f(x)^i}$. By Theorem 5.3.3, we have $\deg \overline{u_i\big(f(x)\big)} = q-1$ if and only if $i = q-1$. Therefore, $f(x)$ is a permutation polynomial. □

5.5 Concluding Remarks

The theorems presented can be interpreted as properties of the composition on the left of $f(x)$ with each of the basis elements $\{x^i \mid i = 0, \ldots, q-1\}$ of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[x]/(x^q - x)$. Changing this basis to another will allow one to prove similar results.

Remark 5.5.1. *Let* $f(x)$ *be a permutation polynomial over* $\mathbb{F}_q$*, and consider the map* $\varphi : \{1, \ldots, q-1\} \to \{1, \ldots, q-1\}$ *given by* $\varphi(e) = \deg \overline{f(x)^e}$*. Theorem 5.3.3 shows that* $\varphi^{-1}(q-1) = \{q-1\}$.

In the particular case $f(x) = x^n$*, where* n *is an integer relatively prime to* $q-1$*,* $f(x)$ *is a permutation polynomial ([5]), and it is straightforward to show that the corresponding map* φ *is injective; however, this is not always the case. For example, suppose that* $q = p^r$ *for an odd prime* p*, and let* $f(x) = ax^{q-2} + b$ *with* $a, b \in \mathbb{F}_q^*$*. One can verify that* $\varphi(1) = \varphi(2) = \varphi(3) = q-2$.

Remark 5.5.2. *If* $d > 1$ *is a divisor of* $q-1$*, then there is no permutation polynomial over* $\mathbb{F}_q$ *of degree* d *([5]). This introduces the following problem: for each* $k \in \{1, \ldots, q-2\}$*, let* a_k *be an element of* $\{1, \ldots, q-2\}$ *such that* a_k *does not divide* $q-1$ *whenever* $\gcd(k, q-1) = 1$*. Does there exist a permutation polynomial* $f(x) \in \mathbb{F}_q[x]$ *such that the corresponding map* φ *satisfies* $\varphi(k) = a_k$ *for each* $k \in \{1, \ldots, q-2\}$ *and* $\varphi(q-1) = q-1$*?*

5.6 Bibliography

[1] M. Ayad, K. Belghaba, O. Kihel, On permutation binomials over finite fields, *Bull. Austral. Math. Soc.* **89**(1) (2014), 112–124.

[2] L. Carlitz, J. A. Lutz, A characterization of permutation polynomials over a finite field, *The American Math. Monthly* **85** (1978), 746–748.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York (1958).

[4] R. Lidl, G. L. Mullen, Does a polynomial permute the elements of the field?, *The American Math. Monthly* **95** (1988), 243–246.

[5] R. Lidl, H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and its Applications)*, Cambridge Univeristy Press (2008).

[6] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, Oxford (1998).

Chapter 6

Prime polynomials over Finite Fields

6.1 Résumé

On étudie la possibilité d'écrire une fonction rationelle comme la composition de deux fonctions de degrés inférieurs. Les résultats sont directement influencés par ceux d'Ayad et utilisent des outils généralisés pour nos besoins, tel que le résultant.

6.2 Abstract

We discuss the possibility of decomposing a rational function over a field K into others of smaller degree. The work is motivated by the results of Ayad and follows by employing similar tools and techniques such as the resultant, which is appropriately generalized to two rational functions for our purposes.

6.3 Introduction

A polynomial which can be written as a composition of polynomials of lesser degree are called *composite*, while those polynomials which admit no such decomposition other than trivial ones are called *prime*, where a trivial decomposition is one in which one of the two decomposition factors is necessarily linear. The problem of decomposing a polynomial f into indecomposables was studied extensively by Ritt [4]. Ritt's polynomial decomposition theorem states that if

$$g_1 \circ \cdots \circ g_m = f = h_1 \circ \cdots \circ h_n$$

are two decompositions of f into prime polynomials, then $m = n$ and the degrees of the components are identical but possibly in different order. This shows that the set of degrees of the composition factors of f are uniquely determined by f.

Following this, Beardon [2] proved that the vector of degrees determines the composition factors uniquely. He further showed that the critical values of a complex polynomial f play a

role in its decomposition, where the critical values of f are the images under f of its critical points. Ayad later elaborated on this idea [1]. He provided some classes of prime polynomials, and also provides an algorithm for decomposing a composite polynomial using the valencies of its critical values.

We note that knowledge of a polynomial's decomposition can significantly reduce the number of computational steps needed to find its roots or to evaluate it. This technique is widely used in many computer algebra systems. The study of prime polynomials in this regard identifies those polynomials which are problematic with respect to this desired simplification.

We note a difference in nonzero characteristic when considering Beardon's result on the vector of degrees. Ritt provided a list of the only three cases wherein two polynomials in $\mathbb{C}[x]$ commute with respect to composition. Beardon's result then states that over $\mathbb{C}$, if one fixes the degree of the composition factor h in $f = g \circ h$, then h is uniquely determined up to composition with linear factors. In nonzero characteristic, this general statement immediately fails, as demonstrated by the simple example polynomial $f = x^{p^2} + x^{2p}$, which can be expressed as the compositions

$$(x^p + x^2) \circ x^p \quad \text{and} \quad x^p \circ (x^p + x^2)\,.$$

The polynomials here do not fit among the three cases set by Ritt's result. From this, we can conclude that not all results pertaining to the characteristic zero case will seamlessly convert to higher characteristic cases. One might then question which results do in fact hold.

Throughout the article, we present many results which parallel those of Ayad on polynomials over $\mathbb{C}$ under the assumption that the degree of the polynomial or rational function being considered is not zero in the field K, that is, if the characteristic of K does not divide the degree of the rational function. This provides some criteria to check if a rational function is prime.

In light of the example $x^{p^2} + x^{2p}$ and the results contained in the article, we conjecture here that this behaviour holds in general. In particular, it seems that the new and more interesting possibilities for decomposition arise when certain quantities such as the degree of a given polynomial over K or its valencies are divisible by the characteristic of the field K. This would be an obvious path for further research.

The aim of this paper is to study when a polynomial or rational expression over a field can be expressed as a composition of two polynomials or rational expressions respectively, with a particular focus on when the underlying field is finite. In section 6.4, we briefly discuss the decomposition of functions over a finite field. In section 6.5, we define and consider prime and composite rational expressions over a field K.

6.4 Functions over $\mathbb{F}_q$

Let q be a power of a prime, and denote by $\mathbb{F}_q$ the finite field of q elements. Any function $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ is equivalent to a polynomial function. Thus, the set of all functions over $\mathbb{F}_q$ can be described exactly as

$$A = \mathbb{F}_q[x]/(x^q - x).$$

The units of A with respect to function composition are called the permutation polynomials of $\mathbb{F}_q$.

Theorem 6.4.1. *Let $\varphi = \alpha \circ \beta$, where $\varphi, \alpha, \beta \in A$. Then φ is a permutation polynomial if and only if both α and β are permutation polynomials.*

Proof. If both α and β are permutation polynomials, then so is φ. Suppose that φ is a permutation polynomial. Then

$$|\mathbb{F}_q| = |\varphi(\mathbb{F}_q)| = |\alpha\big(\beta(\mathbb{F}_q)\big)| \leq |\beta(\mathbb{F}_q)| \leq |\mathbb{F}_q|$$

from which we obtain $|\beta(\mathbb{F}_q)| = |\mathbb{F}_q|$. Since $\beta(\mathbb{F}_q) \subseteq \mathbb{F}_q$, it follows that $\beta(\mathbb{F}_q) = \mathbb{F}_q$, so that β is a permutation polynomial. It immediately follows that $\alpha = \varphi \circ \beta^{-1}$ is also a permutation polynomial. □

Definition 6.4.2. Let $\varphi \in A$. We say that φ is a zero factor if there exists $\psi \in A \setminus \{0\}$ such that $\psi \circ \varphi = 0$.

Theorem 6.4.3. *Every $\varphi \in A$ is either a permutation polynomial or a zero factor.*

Proof. Define the map $C_\varphi : A \to A$ by $\psi \mapsto \psi \circ \varphi$. If C_φ is injective, then it is surjective as well, since A is finite. Thus, there exists $\psi \in A$ such that $(\psi \circ \varphi)(x) = x \in A$. If C_φ is not injective, there exist distinct $\alpha, \beta \in A$ such that $\alpha \circ \varphi = \beta \circ \varphi$. Setting $\psi = \alpha - \beta$ yields $\psi \circ \varphi = \alpha \circ \varphi - \beta \circ \varphi = 0$. □

To consider a meaningful notion of irreducibility, one usually treats units as trivial cases, so here we deal with the zero factors of A. Let $\varphi \in A$ be a zero factor. There exists $\psi \in A \setminus \{0\}$ such that $\psi \circ \varphi = 0$. Then $(\psi + x) \circ \varphi = \varphi$ is a non-trivial decomposition of φ as $\psi + x \neq x$. In this sense, every function over $\mathbb{F}_q$ is either a permutation polynomial or is a composition of polynomial functions.

6.5 Decomposition over K

There are results regarding the decomposition of polynomials and rational expressions into indecomposables, which have been referred to as prime polynomials and prime rational expressions. In this section, we discuss indecomposability of polynomials and rational expressions

through their valencies, which we will define shortly. Ayad [1] studied this problem using valencies for polynomials over $\mathbb{C}$, and Kihel and Larone [3] later considered some rational expressions over $\mathbb{C}$.

Throughout, let R be an integral domain, K its field of fractions, and $\overline{K}$ an algebraic closure of K. For any rational expression $f \in R(X)\setminus\{0\}$, we define as usual $\deg f = \max\{\deg f_1, \deg f_2\}$ where $f = f_1/f_2$ with $f_1, f_2 \in R[X]$ such that $\gcd(f_1, f_2) = 1$. The following result regarding the degree of a composition can be found in [3]:

Theorem 6.5.1. *Let $g, h \in K(X)$. Then $\deg g \circ h = \deg g \cdot \deg h$.*

It is straightforward to show that the rational expressions of degree 1 form the group of units under the operation of composition. This immediately justifies the following definitions of prime and composite rational expressions, as well as provide a simple class of prime rational expressions:

Definition 6.5.2. Let $f \in R(X)$. If $f = g \circ h$ for some $g, h \in L(X)$ with degrees at least 2, then f is said composite over the field L/K. Otherwise, f is said to be prime over L.

Corollary 6.5.3. *Let $f \in R(X)$. If $\deg f$ is a prime number, then f is prime over $\overline{K}$.*

The result follows immediately from Theorem 6.5.1 and the fact that a rational expression of degree 1 is a unit with respect to composition.

A classical result of Ritt [4] states that, over $\mathbb{C}$, given two decompositions $f = g_1 \circ \cdots \circ g_m$ and $f = h_1 \circ \cdots \circ h_n$ of a polynomial in $\mathbb{C}[X]$ into prime polynomials, we must have $m = n$. Moreover, the degrees of these prime polynomials are the same up to permutation. He also showed that the equation $f_1 \circ f_2 = g_1 \circ g_2$ in prime polynomials $f_1, f_2, g_1, g_2 \in \mathbb{C}[X]$, up to composition with linear factors, has only the solutions

$$f_1 \circ f_2 = f_1 \circ f_2,$$

$$X^n \circ X^s h(X^n) = X^s h(X)^n \circ X^n,$$

$$T_n \circ T_m = T_m \circ T_n,$$

where $h \in \mathbb{C}[X]$, $m, n, s \in \mathbb{N}$, and T_n the Chebyshev polynomial. Beardon [2] showed further that, if one fixes the degree of the composition factor h in the decomposition $f = g \circ h$, then h is uniquely determined up to composition with linear polynomials. This is not necessarily the case in non-zero characteristic, as shown immediately by the example

$$f = X^{p^2} + X^{2p}$$

over a field of characteristic p. Indeed, we then have

$$(X^p + X^2) \circ X^p = X^p \circ (X^p + X^2)$$

which are two distinct decompositions into prime polynomials.

We recall the definition of valency used by Ayad:

Definition 6.5.4. Let $a \in \mathbb{C}$ and $f \in \mathbb{C}[X]$. The smallest integer $i \geq 1$ such that $f^{(i)}(a) \neq 0$ is called the valency of f at a and is denoted by $v_f(a)$. If $v_f(a) \geq 2$, a is called a critical point of f. An element $b \in \mathbb{C}$ is called a critical value of f if there exists a critical point a of f such that $f(a) = b$.

Under this definition, he proved the following result among many others:

Theorem 6.5.5. *Let $f \in \mathbb{C}[X]$, and let d be the greatest divisor of $\deg f$. If $v_f(a)$ is a prime number $p > d$, then f is prime.*

This theorem was proved using a relationship between the valencies of f and the degree of its derivative. For completion, we include a general form of this same relationship over the integral domain R.

Lemma 6.5.6. *Let $f \in R[X]$. Then*

$$\deg f - 1 \geq \sum_{a \in \overline{K}} \big(v_f(a) - 1\big).$$

If $\deg f$ is non-zero in R, then $\deg f - 1$ is equal to the sum on the right.

Proof. The only values $v_f(a) - 1$ that contribute to the above sum are those which are at least 1, that is, $v_f(a) \geq 2$. In particular, $v_f(a) - 1$ counts the multiplicity of a as a root of f', so the sum cannot exceed the degree of f' which is itself less than or equal to $\deg f - 1$.

If $\deg f$ is non-zero in R, then either $\mathrm{char}(R) = 0$ or $\gcd(\deg f, \mathrm{char}(R)) = 1$. In either case, $\deg f' = \deg f - 1$, so the sum of the multiplicities of the roots of f' is exactly $\deg f - 1$, and the sum of $v_f(a) - 1$ over all $x \in \overline{K}$ must equal $\deg f' = \deg f - 1$. □

We can refine Theorem 6.5.5 by extending the definition of valency to rational expressions. As it stands, the notion of valency is related to the valuation of a Puiseux series and to the annihilation degree of a rational function at a point.

Lemma 6.5.7. *Let $f \in R[X]$, and let $a \in \overline{K}$. Then $v_f(a)$ is the smallest integer i such that the coefficient a_i of the series expansion*

$$f(X) - f(a) = \sum_{j=0}^{\deg f} a_j (X - a)^j$$

of $f - f(a)$ about a is non-zero.

Proof. Let ν be the smallest integer as described in the statement of the lemma. Then

$$f(X) - f(a) = \sum_{j=\nu}^{\deg f} a_j (X-a)^j.$$

We first note that $\nu > 0$: if we suppose that $\nu = 0$, then $f(X) - f(a)$ evaluated at $X = a$ yields $0 = f(a) - f(a) = a_0 = a_\nu$, which contradicts the definition of ν. Then $f^{(i)}(a) = 0$ for all $0 \leq i \leq \nu - 1$, and $f^{(\nu)}(a) = \nu! a_\nu \neq 0$. Thus, $v_f(a) = \nu$. □

Given $f \in R(X)$ and $a \in \overline{K}$, there is a unique $c_f(a) \in \overline{K}$ such that $f - c_f(a)$ has a zero or pole at a. In particular, $c_f(a) = 0$ if a is a pole of f, and $c_f(a) = f(a)$ otherwise.

Definition 6.5.8. Let $f \in R(X)$ and $a \in \overline{K}$. We define the valency of f at a, denoted $v_f(a)$, as the smallest integer i such that the coefficient a_i of the series expansion of $f - c_f(a)$ about a is non-zero.

We call $a \in \overline{K}$ with $v_f(a) \neq 0$ a critical point of f. If $v_f(a) > 1$, then a is not a pole of f, and we call $f(a)$ a critical value of f.

With this definition of valency, a relationship similar to that of Lemma 6.5.6 holds. The relationship lies between the valencies and the quantity described in the following definition:

Definition 6.5.9. Let $f \in R(X) \setminus 0$ with $f = f_1/f_2$. We define

$$\deg_* f = \deg f_1 - \deg f_2 \,.$$

We note that this quantity remains unchanged when simplifying the ratio f_1/f_2. Theorem 6.5.1 states that the map $\deg : \big(K[X] \setminus \{0\}, \circ\big) \to \big(\mathbb{Z}, \cdot\big)$ is a homomorphism of monoids. The map $\deg_* : K(X) \setminus \{0\} \to \mathbb{Z}$ is not strictly a homomorphism, but it behaves rather similarly to one. First, if $f = g \circ h$, then there exists a decomposition $f = G \circ H$ such that $\deg_* H > 0$. Indeed, if $\deg_* h \leq 0$, writing $h = h_1/h_2$ and dividing h_1 by h_2 in $K[X]$ yields $a \in K$ and $r \in K[x]$ with $h_1 = ah_2 + r$, and either $r = 0$ or $\deg r < \deg h_2$. Then $h = h_1/h_2 = a + r/h_2$, and we define $\mu(x) = 1/(x-a)$. This yields $f = (g \circ \mu^{-1}) \circ (\mu \circ h)$, where $\deg_*(\mu \circ h) = \deg_* h_2/r = \deg h_2 - \deg r > 0$. Next, we have the following result regarding the behaviour of $\deg_*$:

Lemma 6.5.10. *Let $f \in K(X)$. If $f = g \circ h$ with $\deg_* h > 0$, then $\deg_* f = \deg_* g \cdot \deg_* h$.*

Proof. Writing $h = h_1/h_2$ and

$$g(X) = b \frac{\prod_{i=1}^{m_1}(X - \alpha_i)}{\prod_{j=1}^{m_2}(X - \beta_j)}$$

yields

$$g\big(h(X)\big) = \frac{bh_2(X)^{\deg g - m_1} \prod_{i=1}^{m_1} \big(h_1(X) - \alpha_i h_2(X)\big)}{h_2(X)^{\deg g - m_2} \prod_{j=1}^{m_2} \big(h_1(X) - \beta_j h_2(X)\big)}.$$

Since $\deg_* h > 0$ by assumption, we have

$$\begin{aligned} \deg_* f &= \big((\deg g - m_1)\deg h_2 + m_1 \deg h_1\big) - \big((\deg g - m_2)\deg h_2 - m_2 \deg h_1\big) \\ &= (m_1 - m_2)(\deg h_1 - \deg h_2) \\ &= \deg_* g \cdot \deg_* h, \end{aligned}$$

as claimed. □

For polynomials, the two maps $\deg_*, \deg : K[X] \setminus \{0\} \to \mathbb{Z}$ are equal. While deg retains some of its properties over $K[X]$ when extended to $K(X)$, such as the one given in Theorem 6.5.1, the map $\deg_*$ retains others.

Theorem 6.5.11. *Let $f \in K(X)$. If $\deg_* f$ is non-zero in K, then $\deg_* f' = \deg_* f - 1$.*

Proof. We may write

$$f(X) = \frac{aX^{n_1} + f_1(X)}{X^{n_2} + f_2(X)}$$

where $a \neq 0$ and $\deg f_1 < n_1, \deg f_2 < n_2$. The expression for the derivative of f can be obtained by simplifying

$$\frac{\big(an_1X^{n_1-1} + f_1'(X)\big)\big(X^{n_2} + f_2(X)\big) - \big(aX^{n_1} + f_1(X)\big)\big(n_2X^{n_2-1} + f_2'(X)\big)}{\big(X^{n_2} + f_2(X)\big)^2}$$

which we may write concisely as

$$\frac{a \deg_* f X^{n_1+n_2-1} + F_1(X)}{X^{2n_2} + F_2(X)}$$

where $\deg F_1 < n_1 + n_2 - 1$ and $\deg F_2 < 2n_2$. Then $\deg_* f' = (n_1 + n_2 - 1) - (2n_2) = n_1 - n_2 - 1 = \deg_* f - 1$ whenever $\deg_* f = n_1 - n_2$ is non-zero in K. □

We have now the generalization of Lemma 6.5.6, which shows the relationship between the valencies of f and $\deg_* f$.

Proposition 6.5.12. *Let $f \in K(X)$. If $\deg_* f$ is non-zero in K, then*

$$\deg_* f - 1 = \sum_{a \in \overline{K}} \big(v_f(a) - 1\big).$$

Proof. The values $v_f(a)-1$ contributing to the sum are those which are non-zero. If $v_f(a)-1 > 0$, then $v_f(a)-1$ counts the multiplicity of a as a zero of f'. If $v_f(a)-1 < 0$, it instead counts the negative of the multiplicity of a as a pole of f'. Together, we have

$$\sum_{a\in\overline{K}} \big(v_f(a)-1\big) = \deg_* f' = \deg_* f - 1$$

by Theorem 6.5.11. □

Theorem 6.5.13. *Let $f \in K[X]$, and let d be the greatest proper divisor of $\deg f$. If $\deg_* f$ is divisible by a prime number $p > d$, then f is prime over $\overline{K}$.*

Proof. Suppose that f is composite. Then there exist $g, h \in \overline{K}[X]$ such that $f = g \circ h$ with $\deg_* h > 0$. Either $\deg_* h$ or $\deg_* g$ is divisible by $p > d$, so that $|\deg_* h| \geq p > d$ or $|\deg_* g| \geq p > d$; however, each also satisfies $|\deg_* h| \leq \deg h \leq d$ or $|\deg_* g| \leq \deg g \leq d$, which is a contradiction in either case. □

Ayad's result, stated above as Theorem 6.5.5, is a particular case of the following corollary:

Corollary 6.5.14. *Let $f \in K(X)$ be such that $\deg f$ and $\deg_* f$ are non-zero in K, and let d be the greatest divisor of $\deg f$. If $v_f(a)$ non-zero in K is divisible by a prime number $p > d$ for some $a \in \overline{K}$, then f is prime over $\overline{K}$.*

Proof. Suppose that $v_f(a) > 0$. Since $f - f(a)$ has a zero of order $v_f(a)$ at a, defining the unit $\mu(X) = (aX+1)/X$ gives a rational expression $\big(f-f(a)\big)\circ\mu$ with $\deg_*\big(f-f(a)\big)\circ\mu = v_f(a)$ divisible by $p > d$. Thus, both $\big(f-f(a)\big)\circ\mu$ and f are prime over $\overline{K}$. If $\nu := v_f(a) < 0$, then $1/f$ has a zero of order $-v_f(a)$ at a. The previous argument shows that $1/f \circ \mu$ is prime, so f is as well. □

As Ayad [1] did over $\mathbb{C}$, we introduce the resultant of two polynomials. After we present a theorem for the polynomial case, we then generalize the notion to two elements of $R(X)$ and prove a similar result. The resultant of the two polynomials $f = a_n X^n + \cdots + a_0$ and $g = b_m X^m + \cdots + b_0$ in $R[X]$ is defined as

$$\mathrm{Res}_X(f,g) = {a_n}^m {b_m}^n \prod_{\alpha,\beta}(\alpha-\beta)$$

where α and β run over all of the roots of f and g respectively in $\overline{K}$. Some well-known properties of the resultant are as follows:

1. For an additional polynomial $h \in R[X]$, we have $\mathrm{Res}_X(f,gh) = \mathrm{Res}_X(f,g)\mathrm{Res}_X(f,h)$;
2. $\mathrm{Res}_X(f,g) \in R$;

3. f and g have a common root in $\overline{K}$ if and only if their resultant is zero.

The discriminant of f is given by

$$D[f] = \frac{(-1)^{n(n-1)/2}}{a_n}\mathrm{Res}_X(f, f')\,.$$

The discriminant is an integral polynomial in the coefficients of f, so it lies in R. Letting T be a new variable, $b \in \overline{K}$ is a critical value of f if and only if it is a root of $D[f-T]$. The multiplicity of a critical value is defined as its multiplicity as a root of $D[f-T]$, and we call a critical value with multiplicity 1 a simple critical value.

Theorem 6.5.15. *Let $f = g \circ h$, and let $D(t) = Res_x\big(f(x)-t, f'(x)\big)$. There exists $a \in K$ such that*

$$D(t) = aD[g-t]^{\deg h}\, Res_x\big(f(x)-t, h'(x)\big)\,.$$

Proof. Let n and a_n be the degree and leading coefficient of f respectively. We have

$$\begin{aligned} D(t) &= \frac{(-1)^{n(n-1)/2}}{a_n}\mathrm{Res}_x\big(f(x)-t, f'(x)\big) \\ &= \frac{(-1)^{n(n-1)/2}}{a_n}\mathrm{Res}_x\Big(g\big(h(x)\big)-t, g'\big(h(x)\big)\Big)\mathrm{Res}_x\Big(g\big(h(x)\big)-t, h'(x)\Big)\,. \end{aligned}$$

Write $g'(x) = (\deg g)b\prod_\beta (x-\beta)$ where β runs over all roots of g' in an algebraic closure of K, and b is the leading coefficient of g. Then

$$\begin{aligned} \mathrm{Res}_x\Big(g\big(h(x)\big)-t, g'\big(h(x)\big)\Big) &= \mathrm{Res}_x\Big(g\big(h(x)\big)-t, (\deg g)b\prod_\beta \big(h(x)-\beta\big)\Big) \\ &= [(\deg g)b]^{\deg f}\mathrm{Res}_x\Big(g\big(h(x)\big)-t, \prod_\beta \big(h(x)-\beta\big)\Big) \\ &= [(\deg g)b]^{\deg f}\prod_\beta \mathrm{Res}_x\Big(g\big(h(x)\big)-t, \big(h(x)-\beta\big)\Big) \\ &= [(\deg g)b]^{\deg g \deg h}\prod_\beta \big(g(\beta)-t\big)^{\deg h} \\ &= \left([(\deg g)b]^{\deg g}\prod_\beta \big(g(\beta)-t\big)\right)^{\deg h} \\ &= \Big(\mathrm{Res}_x\big(g'(x), g(x)-t\big)\Big)^{\deg h} \\ &= (-1)^{\deg f \deg g'}\Big(\mathrm{Res}_x\big(g(x)-t, g'(x)\big)\Big)^{\deg h} \\ &= (-1)^{\deg f \deg g'} D[g-t]^{\deg h}\,. \end{aligned}$$

Thus,

$$D(t) = \frac{(-1)^{n(n-1)/2+n\deg g'}}{a_n} D[g-t]^{\deg h} \mathrm{Res}_x\Big(g\big(h(x)\big) - t, h'(x)\Big).$$

Setting $a = \dfrac{(-1)^{n(n-1)/2+n\deg g'}}{a_n}$ yields the result. □

Corollary 6.5.16. *Let $f \in R[x]$ have degree n, and let $D(t)$ be the discriminant of $f - t$. If $f(x)$ is composite with a right composition factor of degree k, then there exist polynomials $A, B \in R[t]$ such that $D(t) = A(t)^k B(t)$ and $\deg B \leq k-1$. Moreover, if $\deg f$ is non-zero in R, then $\deg B = k-1$.*

Proof. It follows immediately from Theorem 6.5.15, by setting $B(t) = a\mathrm{Res}_x\Big(g\big(h(x)\big) - t, h'(x)\Big)$ and $A(t) = D[g-t]$, that we have $A \in R[t]$ and $B \in K[t]$. Since $A(t), D(t) \in R[t]$, it follows that $B(t) \in R(t)$, and we conclude that $B(t) \in R[t]$ as well.

If $\deg f$ is non-zero in R, then $k = \deg h \leq \deg f$ implies that $\deg h' = \deg h - 1 = k-1$. Consequently, $\deg B = k-1$. □

Theorem 6.5.17. *Let $f \in K[x]$ have degree n, and let d be the greatest proper divisor of n. If f has at least d simple critical values, then f is prime over K.*

Proof. Suppose that f is composite with a right composition factor of degree k. Then $2 \leq k \leq d$, and we write $D(t) = A(t)^k B(t)$ for some polynomials $A, B \in K[t]$. Since f has at least d simple critical values, and each simple critical value is necessarily a root of $B(t)$, we have $k - 1 \geq \deg B \geq d \geq k$, which is a contradiction. Thus, f is prime. □

Kihel and Larone [3] studied the resultant of the two rational functions $f, g \in \mathbb{C}(X)$, which they defined as the resultant of their numerators. Let $f \in K[X]$ be composite such that $\deg_* f > 1$ is non-zero in K. Then there exist $g, h \in \overline{K}[X]$ such that $f = g \circ h$ with $\deg_* h > 0$. Since $\deg_* f = \deg_* g \cdot \deg_* h$, we have $\deg_* g$ non-zero in K, which in turn implies that $\deg_* g' = \deg_* g - 1 > 0$. The proofs of Lemma 4.6 and Corollary 4.5 [3] deal with only $\mathbb{C}$, although they immediately translate to $\overline{K}$ under the assumptions made here, yielding the following result analogous to Theorem 6.5.15:

Theorem 6.5.18. *Let $f \in K(X)$ satisfy $\deg_* f > 1$ and $\deg_* f$ non-zero in K. If $f = g \circ h$ for some $g, h \in \overline{K}[X]$ with $\deg_* h > 0$, then the polynomial $r_f(T) := Res_X(f - T, f')$ can be written in the form*

$$r_f(T) = A(T)^{\deg h} B(T)$$

with $A, B \in K[T]$ such that $\deg B \leq 2\deg h - 1$.

The polynomial $r_f(T)$ is for rational expressions an analogue to the discriminant in the sense that $b \in \overline{K}$ is a critical value of f if and only if b is a root of $r_f(T)$. We call a critical value with multiplicity 1 as a root of $r_f(T)$ a simple critical value of f.

Corollary 6.5.19. *Let $f \in K(X)$ satisfy $\deg_* f > 1$ and $\deg_* f$ non-zero in K, and let d be the greatest proper divisor of $\deg f$. If f has at least $2d$ simple critical values, then f is prime over $\overline{K}$.*

Proof. The proof is similar to that of Theorem 6.5.17 with instead the inequality

$$2\deg h - 1 \geq \deg B \geq 2d \geq 2\deg h$$

yielding the contradiction. □

6.6 Bibliography

[1] M. Ayad, Critical points, critical values of a prime polynomial, *Complex Variables and Elliptic Equations: An International Journal*, **51**(2), (2006), 143–160.

[2] A. F. Beardon, Composition factors of polynomials, *Complex Variables and Elliptic Equations: An International Journal*, **43**, (2001), 225–239.

[3] O. Kihel and J. Larone, Prime rational functions, *Acta Arithmetica*, **169**(1) (2015), 29–46.

[4] J. F. Ritt, Prime and composite polynomials, *Trans. Amer. Math. Soc.*, **23**, (1992), 51–66.

Chapter 7

Composed products of polynomials over unique factorization domains

Let $\mathbb{F}_q$ be a finite field with algebraic closure Γ, and denote by σ the Frobenius automorphism of Γ. If G is a non-empty σ-invariant subset of Γ, then there is a binary operation $\diamond$ on G such that σ is an endomorphism of $(G, \diamond)$. Suppose now that $(G, \diamond)$ is an abelian group. If $f, g \in \mathbb{F}_q[x]$ have roots lying in G, then the operation $\diamond$ induces an operation on polynomials by

$$f \diamond g = \prod_{\alpha,\beta} (x - \alpha \diamond \beta),$$

where the product runs over all roots α and β of f and g respectively. Whether an irreducible monic polynomial $h \in \mathbb{F}_q[x]$ can be expressed as $f \diamond g$ was studied by Brawley and Carlitz, who proved among other results that $h = f \diamond g$ is irreducible over $\mathbb{F}_q$ if and only if both f and g are also irreducible over $\mathbb{F}_q$ with relatively prime degrees. While much of their work is done in these general terms, they do focus on two particular cases of decomposition with respect to this composed product they have defined: additive decompositions and multiplicative decompositions, respectively occurring when $\diamond$ is field addition and multiplication. While we are not certain as to the reasoning behind their terminology, we do note that it seems rather apt. Indeed, the usual composition of two polynomials can be expressed through the resultant as

$$(f \circ g)(x) = \mathrm{Res}_t\big(f(t), g(x) - t\big),$$

which parallels the extended definition we give to additive compositions below.

Following the notation of Brawley and Carlitz, we extend the definition of additive composition to polynomials over commutative rings instead of only finite fields with the resultant:

$$(f * g)(x) = \mathrm{Res}_t\big(f(t), g(x - t)\big).$$

Ayad considered polynomials of the form

$$\mathrm{Res}_t\big(f(t), g(x - t)\big)$$

where $f, g \in \mathbb{Q}[x]$, showing that in some circumstances they are irreducible polynomials over $\mathbb{Q}$ which are reducible over all finite fields $\mathbb{F}_p$. This suggests that consideration of composed sums of polynomials over $\mathbb{Z}$ could very well be fruitful. Indeed, applying the definition of composed sum through the resultant over a commutative ring R, we can see that the result of Brawley and Carlitz need not hold. For example, over $\mathbb{Z}$, the irreducible polynomial $x^4 - 10x^2 + 1$ can be written $(x^2 - 2) * (x^2 - 3)$. Note that the two polynomials have degrees which are not relatively prime. This is a prototypical example of a polynomial reducible over all $\mathbb{F}_p$, as suggested by the result of Ayad.

7.1 Résumé

On étudie les unités sous l'opération $*$ et la décomposition de polynômes sur un domaine à factorisation unique en polynômes indécomposables.

7.2 Abstract

We describe the units under the operation $*$ and study the decomposition of polynomials over a unique factorisation domain into indecomposables with respect to this operation.

7.3 Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, let f and g be monic polynomials over $\mathbb{F}_q$, and consider the polynomial $f * g$ defined through the additive composition of f and g. Although the roots of f and g may lie outside of $\mathbb{F}_q$, the polynomial $f * g$ has coefficients in $\mathbb{F}_q$. The operation $*$ is a binary operation on the set of monic polynomials over $\mathbb{F}_q$, called composed addition. If a monic polynomial $h \in \mathbb{F}_q[x]$ with $\deg h > 1$ can be expressed as $h = f * g$ where $\deg f > 1$ and $\deg g > 1$, then h is said to be additively decomposable into the additive composition factors f and g.

Additive decompositions over finite fields were extensively studied by Brawley and Carlitz in [1] and [2], who proved a unique decomposition theorem for irreducible monic polynomials with respect to composed addition, and provided a test for additive decomposability of irreducibles, among other results. For convenience, we state here another result from [1].

Theorem 7.3.1. *Let h be a monic irreducible over $\mathbb{F}_q$ with $\deg h > 1$. If h is additively decomposable as $h = f * g$ where $\deg f = m > 1$ and $\deg g = n > 1$, then f and g are both irreducible and $\gcd(m, n) = 1$.*

In this paper, we study the analogous notion of composed addition of two polynomials over a given commutative ring R, in particular over integral domains and unique factorization domains.

7.4 Preliminaries

Let $u(x) = u_m(x-\alpha_1)\cdots(x-\alpha_m)$ be a polynomial over an integral domain R, where $\alpha_1, ..., \alpha_m$ are all of the roots of u in some algebraic closure of the field of fractions of R. Let $v(x)$ be a polynomial over R of degree n. Then the resultant of u and v is given by

$$\mathrm{Res}_x\big(u(x), v(x)\big) = u_m^n \prod_{i=1}^{m} v(\alpha_i).$$

The resultant can also be computed as the determinant of a Sylvester matrix, the entries of which consist of the element 0 and coefficients of u and v. Thus, $\mathrm{Res}_x\big(u(x), v(x)\big)$ is a polynomial in the coefficients of u and v.

To motivate our definition of composed addition over a commutative ring R, we begin with the finite field case. Let $h \in \mathbb{F}_q[x]$ be a monic polynomial that is additively decomposable as $f * g$. Let $\alpha_1, ..., \alpha_m$ and $\beta_1, ..., \beta_n$ be all of the roots of f and g respectively in some algebraic closure of $\mathbb{F}_q$. Noting that

$$(-1)^m f(x-t) = \prod_{i=1}^{m} \big(t - (x - \alpha_i)\big)$$

we deduce that $f * g$ is related to the resultant as follows:

$$\begin{aligned}(f*g)(x) &= \prod_{i=1}^{m}\prod_{j=1}^{n} \big(x - (\alpha_i + \beta_j)\big) \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n} \big((x-\alpha_i) - \beta_j\big) \\ &= \mathrm{Res}_t\big((-1)^m f(x-t), g(t)\big).\end{aligned}$$

Since the resultant of two polynomials over a commutative ring R can be computed, the expression $\mathrm{Res}_t\big((-1)^{\deg f} f(x-t), g(t)\big)$ provides us with a natural way to extend the definition of composed addition to polynomials (not necessarily monic) over a commutative ring R.

If a polynomial $h \in R[x]$ can be expressed as $h = f * g$ where f and g are polynomials over R which are not units with respect to composed addition, then we say that h is additively decomposable over R into the additive composition factors f and g. The group of units of polynomials over R under the operation of composed addition is

$$\mathcal{U} = \{ax + b \mid a, b \in R \text{ and } a^{-1} \in R\}.$$

Indeed, letting $u(x) = x$, then for any $f \in R[x]$ we have

$$(f * u)(x) = (u * f)(x) = \mathrm{Res}_t\big((-1)(x-t), f(t)\big) = \mathrm{Res}_t\big(t - x, f(t)\big) = f(x).$$

Thus, the polynomial x is the identity element with respect to composed addition. If $u \in \mathcal{U}$ and $v \in \mathcal{U}$ is its inverse, then $1 = \deg(u * v) = \deg(u)\deg(v)$ implies that both u and v are linear polynomials.

Let $u = u_1x + u_2, v = v_1x + v_2 \in R[x]$ where u_1 and v_1 are not 0. Then $u * v = (u_1v_1)x + (u_1v_2 + u_2v_1)$ is again a linear polynomial. Moreover, if u_1 and v_1 are units of R, then u_1v_1 is a unit of R. Thus, $\mathcal{U}$ is closed under composed addition. If u, v are as above and v is the inverse of u, then $u * v = (u_1v_1)x + (u_1v_2 + u_2v_1) = x$ implies that $u_1v_1 = 1$ and $u_1v_2 + u_2v_1 = 0$. Solving these equations yields $v_1 = u_1^{-1}$ and $v_2 = -u_2/u_1^2$, so $u \in \mathcal{U}$ has an inverse if and only if its leading coefficient is a unit of R.

It remains to show that composed addition of linear polynomials is associative. Let $u = u_1x + u_2, v = v_1x + v_2, w = w_1x + w_2 \in \mathcal{U}$. Then

$$\begin{aligned}(u * v) * w &= \big((u_1v_1)x + (u_1v_2 + u_2v_1)\big) * (w_1x + w_2)\\ &= (u_1v_1w_1)x + (u_1v_1w_2 + u_2v_2w_1 + u_2v_1w_1)\\ &= (u_1x + u_2) * \big((v_1w_1)x + (v_1w_2 + v_2w_1)\big)\\ &= u * (v * w).\end{aligned}$$

We quickly note that if G is the subset $\{ax + b + \langle x^2\rangle : a^{-1} \in R\}$ of $R[x]/\langle x^2\rangle$, then the mapping $\psi : \mathcal{U} \to G$ given by $ax + b \mapsto ax + b + \langle x^2\rangle$ is a group isomorphism from $\mathcal{U}$ with the operation of composed addition to G with the usual multiplication operation.

7.5 Additive Decompositions

We present first a lemma which follows directly from the definition of the resultant.

Lemma 7.5.1. *Let R be an integral domain and K its field of fractions. Let $h, f, g \in R[x]$, and let $h = ch_1$, $f = af_1$, and $g = bg_1$ where $c, a, b \in R$ and $h_1, f_1, g_1 \in K[x]$ are monic. Then $h = f * g$ over R if and only if $h_1 = f_1 * g_1$ over K and $c = a^{\deg g}b^{\deg f}$.*

Proof. Let

$$f = a\prod_{i=1}^{m}(x - \alpha_i) \qquad \text{and} \qquad g = b\prod_{j=1}^{n}(x - \beta_j).$$

If $h_1 = f_1 * g_1$ and $c = a^nb^m$, then we may write

$$h = ch_1 = a^nb^m\prod_{i=1}^{m}\prod_{j=1}^{n}\big(x - (\alpha_i + \beta_j)\big) = f * g.$$

Conversely, if $h = f * g$, then

$$h_1 = \prod_{i=1}^{m}\prod_{j=1}^{n}\big(x - (\alpha_i + \beta_j)\big) = f_1 * g_1$$

and the leading coefficient of h is a^nb^m. □

We now present some classes of polynomials which are not additively decomposable.

Theorem 7.5.2. *Let R be an integral domain. If $h \in R[x]$ has leading coefficient p where p is prime, then h is not additively decomposable over R.*

Proof. Suppose that h is additively decomposable over R. There exist $f, g \in R[x]$ with $\deg f = m \geq 1$ and $\deg g = n \geq 1$ such that $p = a^n b^m$, where $a, b \in R$ are the leading coefficients of f and g respectively. We show that one of f and g is a unit with respect to composed addition.

Since $p = a^n b^m$, we can assume without loss of generality that $p = a^n$ and $b^m = 1$. Then $a = p$, $n = 1$ and $b^m = 1$, so that g is a polynomial of degree 1 with leading coefficient a unit of R. Therefore, g is a unit with respect to composed addition. □

If R is a unique factorization domain, then the proof of the previous theorem can be modified to give a more general result.

Theorem 7.5.3. *Let R be a unique factorization domain. If $h \in R[x]$ with $\deg h > 1$ has leading coefficient that is square-free and not a unit of R, then h is not additively decomposable over R.*

Proof. Let c be the leading coefficient of h, and suppose that h is additively decomposable over R. There exist $f, g \in R[x]$ with $\deg f = m \geq 1$ and $\deg g = n \geq 1$ such that $c = a^n b^m$, where $a, b \in R$ are the leading coefficients of f and g respectively. Since c is square-free, we may write $c = p_1 p_2 \cdots p_r$, where $p_1, p_2, ..., p_r$ are distinct prime elements of R. Without loss of generality, we assume that $p_1 \cdots p_t = a^n$ where $1 \leq t \leq r$.

Suppose for contradiction that $n \geq 2$. Since $a \in R$, it follows that the primitive polynomial $x^n - p_1 \cdots p_t \in R[x]$ is reducible over R. The ideal $\mathfrak{P} = \langle p_1 \rangle$ is a prime ideal of R since p_1 is prime. Moreover, $1 \notin \mathfrak{P}$, $p_1 \cdots p_t \in \mathfrak{P}$, and $p_1 \cdots p_t \notin \mathfrak{P}^2$. Thus $x^n - p_1 \cdots p_t$ is irreducible over R by Eisenstein's Criterion, which is a contradiction.

Since $\deg g = n = 1$, we have $\deg f = m = \deg h$. If $t < r$, then the same argument as above applied to the polynomial $x^m - p_{t+1} \cdots p_r \in R[x]$ yields a contradiction. Thus, we conclude that $a = a^n = p_1 \cdots p_r$ and $b^m = 1$. Thus b, the leading coefficient of g, is a unit of R, so g is a unit with respect to composed addition. □

Let $\sigma : R \to S$ be a unit-preserving ring homomorphism from an integral domain R to an integral domain S. This homomorphism can naturally be extended to a homomorphism $\bar{\sigma} : R[x] \to S[x]$ by $c_n x^n + \cdots + c_0 \mapsto \sigma(c_n)x^n + \cdots + \sigma(c_0)$. For simplicity, we denote $\bar{\sigma}$ by σ as well. Since $\mathrm{Res}_x(f, g)$ is a polynomial in the coefficients of f and of g, we have $\sigma\big(\mathrm{Res}_x(f, g)\big) = \mathrm{Res}_x\big(\sigma(f), \sigma(g)\big)$.

Let $h = f * g$, and let $a, b, c \in R$ be the leading coefficients of f, g, h respectively. Then $c = a^n b^m$ where $m, n \geq 1$. If $\deg \sigma(h) = \deg h$ for a unit-preserving homomorphism σ, then $\sigma(a)^n \sigma(b)^m = \sigma(c) \neq 0$, so that $\sigma(a) \neq 0$ and $\sigma(b) \neq 0$.

Theorem 7.5.4. *Let $\sigma : R \to S$ be a unit-preserving homomorphism from an integral domain R to an integral domain S, and let $h \in R[x]$. If $\deg \sigma(h) = \deg h$ and $h = f * g$ over R, then $\sigma(h) = \sigma(f) * \sigma(g)$ over S.*

Proof. We naturally extend σ to a homomorphism from $R[x,t]$ to $S[x,t]$. Note that $\sigma(t^n) = t^n$ and $\sigma\big((x-t)^n\big) = \big(\sigma(x-t)\big)^n = (x-t)^n$ since σ is unit-preserving. Since σ does not map the leading coefficients of f and g to 0, σ fixes the degrees of $f, g \in R[x,t] = R[x][t]$. Thus

$$\begin{aligned}
\sigma(h) &= \sigma(f * g) \\
&= \sigma\Big(\mathrm{Res}_t\big((-1)^{\deg f} f(x-t), g(t)\big)\Big) \\
&= \mathrm{Res}_t\Big(\sigma\big((-1)^{\deg f} f(x-t)\big), \sigma\big(g(t)\big)\Big) \\
&= \mathrm{Res}_t\big((-1)^{\deg \sigma(f)} \sigma(f)(x-t), \sigma(g)(t)\big) \\
&= \sigma(f) * \sigma(g).
\end{aligned}$$

□

The following lemma concerning linear polynomials will be used to prove that a polynomial can be additively decomposed into a finite number of indecomposable additive composition factors.

Lemma 7.5.5. *Let R be a unique factorization domain, and let $h = ax + b \in R[x]$ where a is not a unit in R. Then $h = f_1 * \cdots * f_r$ for some linear polynomials $f_1, ..., f_r \in R[x]$ which are not additively decomposable over R.*

Proof. If h is not additively decomposable, then the result holds trivially taking $f_1 = h$, so we suppose that h is additively decomposable. We prove the result by induction on the number of prime divisors of a.

If the number of prime divisors of a is equal to 1, then a is prime, and the result follows from Theorem 7.5.2. Suppose that the result holds when the number of prime divisors of a is less than or equal to $d \geq 1$. We show that the result holds when a has $d+1$ prime divisors.

There exist $f_1, f_2 \in R[x]$ such that $h = f_1 * f_2$ where neither f_1 nor f_2 is a unit with respect to composed addition since h is additively decomposable. It follows that the leading coefficients of both f_1 and f_2 are non-units of R dividing the leading coefficient of h. Thus, the number of prime divisors of the leading coefficient of f_1 is less than or equal to d, and the same is true for the leading coefficient of f_2. By the induction hypothesis, we can write $f_1 = g_1 * \cdots * g_t$ and $f_2 = g_{t+1} * \cdots * g_r$ where each g_i is not additively decomposable. Therefore, $h = g_1 * \cdots * g_r$ where each g_i is not additively decomposable. Clearly, $\deg g_i = 1$ for each g_i. □

Theorem 7.5.6. *Let R be a unique factorization domain, and let $h \in R[x]$ be a non-unit with respect to composed addition. Then $h = f_1 * \cdots * f_r$ for some polynomials $f_1, ...f_r \in R[x]$ which are not additively decomposable over R.*

Proof. The case where h is not additively decomposable is trivial, so suppose that h is additively decomposable. We prove the result by induction on $\deg h$. If $\deg h = 1$, then the result holds by Lemma 7.5.5. Suppose that the result holds for all polynomials of degree less than or equal to k. We show that the result holds when $\deg h = k + 1$.

Since h is additively decomposable, $h = f_1 * f_2$ for some polynomials $f_1, f_2 \in R[x]$ which are not units with respect to composed addition. We consider two cases:

1. If there exist f_1 and f_2 such that $\deg f_1 < \deg h$ and $\deg f_2 < \deg h$, then by the induction hypothesis we write $f_1 = g_1 * \cdots * g_t$ and $f_2 = g_{t+1} * \cdots * g_r$ where each g_i is not additively decomposable. Therefore, $h = g_1 * \cdots * g_r$ where each g_i is not additively decomposable.

2. If the only possible choices for f_1 and f_2 are such that $\deg f_1 = 1$ and $\deg f_2 = \deg h$, then we consider the leading coefficient of f_2. If the leading coefficient of f_2 is a unit, then f_2 is not additively decomposable. Applying Lemma 7.5.5 to f_1 yields the result.

   If the leading coefficient of f_2 is not a unit, then it only has a finite number of prime divisors. The same argument used to prove Lemma 7.5.5 shows that $f_2 = g_1 * \cdots * g_t$ where all but one of the g_i must be linear, since f_2 has no additive composition factors of degree strictly between 1 and $\deg f_2 = \deg h$. Applying Lemma 7.5.5 to f_1 and to each linear g_i yields the result. □

We note that for an irreducible monic polynomial h over a finite field, it was shown in [1] that any two additive decompositions of h are equivalent up to additive compositions with linear polynomials, all of which are units with respect to composed addition. For example, the irreducible polynomial $h = x^6 + x^5 + x^3 + x^2 + 1 \in \mathbb{F}_2$ is decomposable into irreducibles as $(x^2 + x + 1) * (x^3 + x + 1)$ and as $(x^2 + x + 1) * (x^3 + x^2 + 1)$ as demonstrated in [1]. Here, we have $x^3 + x^2 + 1 = (x^3 + x + 1) * (x + 1)$.

This is not the case in general. Over $\mathbb{Z}$, the polynomial $h = 36x^4$ can be decomposed as $(2x^2) * (3x^2)$ and as $(x^2) * (6x^2)$; however, there is no polynomial $ax + b \in \mathbb{Z}[x]$ such that $(x^2) * (ax + b) = (ax + b)^2$ will equal either $2x^2$ or $3x^2$. As such, two decompositions of a reducible non-monic polynomial over a ring R need not be equivalent up to units with respect to composed addition.

Corollary 7.5.7. *Let $\sigma : R \to S$ be a unit-preserving homomorphism from a unique factorization domain R to a unique factorization domain S, and let $h \in R[x]$. If $\deg \sigma(h) = \deg h$*

and $\sigma(h)$ is not additively decomposable over S, then $h = f * \ell$ where $f \in R[x]$ is not additively decomposable over R and $\ell \in R[x]$ is a linear polynomial. Moreover, if the leading coefficient of h is a unit in R, then ℓ is a unit with respect to composed addition, so h is not additively decomposable over R.

Proof. By Theorem 7.5.6, we write $h = f_1 * \cdots * f_r$ where each $f_i \in R[x]$ is not additively decomposable over R. Since $\sigma(h) = \sigma(f_1) * \cdots * \sigma(f_r)$ is not additively decomposable over S, all but one of the $\sigma(f_i)$ are units with respect to composed addition. Assume without loss of generality that $\sigma(f_2), ..., \sigma(f_r)$ are these units. It follows from $\deg f_i = \deg \sigma(f_i) = 1$ that f_i is a linear polynomial for each $i = 2, ..., r$. Letting $\ell = f_2 * \cdots * f_r$ yields $h = f_1 * \ell$, where f_1 is not additively decomposable.

If the leading coefficient of h is a unit in R, then the leading coefficient of ℓ must be a unit in R as well, so that ℓ is a unit with respect to composed addition. Therefore, h is not additively decomposable. □

Let h be a monic irreducible over $\mathbb{F}_q$ with $\deg h > 1$. Theorem 7.3.1 asserts that if $h = f * g$, then f and g are irreducibles and $\gcd(\deg f, \deg g) = 1$. The conclusion on the degrees of the additive composition factors need not be true in general for polynomials over a given ring R. For example, the irreducible polynomial $h = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$ can be decomposed as $(x^2 - 2) * (x^2 - 3)$ over $\mathbb{Z}$. We can, however, always guarantee the irreducibility of the additive composition factors of an irreducible polynomial over an integral domain R.

Theorem 7.5.8. *Let R be an integral domain, and let $h \in R[x]$ be irreducible over R. If $h = f * g$ over R, then f and g are both irreducible over R.*

Proof. We prove that if f or g is reducible over R, then h is reducible over R. Assume without loss of generality that g is reducible over R. Then there exist $g_1, g_2 \in R[x]$ such that $g = g_1 g_2$. Then by the multiplicative property of the resultant, we obtain

$$\begin{aligned} h = f * g &= \operatorname{Res}_t\big((-1)^{\deg f} f(x-t), g_1(t) g_2(t)\big) \\ &= \operatorname{Res}_t\big((-1)^{\deg f} f(x-t), g_1(t)\big) \operatorname{Res}_t\big((-1)^{\deg f} f(x-t), g_2(t)\big) \\ &= (f * g_1)(f * g_2) \end{aligned}$$

so that h is reducible over R. □

The converse is not true in general as $(x^2 + 1) * (x^2 + 1) = x^2(x^2 + 4)$ over $\mathbb{Z}$.

7.6 Bibliography

[1] J.V. Brawley and L. Carlitz, Irreducibles and the composed product for polynomials over a finite field, Discrete Math. 65 (1987) 115–139.

[2] J.V. Brawley and L. Carlitz, A test for additive decomposability of irreducibles over a finite field, Discrete Math. 76 (1989) 61–65.

Chapter 8

Multiplicative decompositions of polynomials

With minor adjustments, one can also study composed multiplication. One can successfully exhibit classes of polynomials irreducible over $\mathbb{Q}$ but reducible over all finite fields $\mathbb{F}_p$. In addition, it is relatively simple to construct classes of polynomials which are irreducible over $\mathbb{Q}$, but reducible over many (but not necessarily all) $\mathbb{F}_p$. For example, suppose that $n \in \mathbb{Z}\setminus\{0\}$ is either odd, or n is even but admits no integer m satisfying the equations $n^2 - 2m^2 = \pm 2$. Then

$$x^4 + 2(n^2 \pm 1)x^2 + 1$$

is irreducible over $\mathbb{Z}$ but reducible over $\mathbb{F}_p$ for $p = 2$ and all primes $p \equiv \pm 1 \pmod 8$, and it is reducible at least over $\mathbb{F}_{p^2}$ for every $p \equiv \pm 3 \pmod 8$. Setting $n = 1$, we obtain $x^4 + 1$, which is another prototypical example of polynomial irreducible over $\mathbb{Q}$ but reducible over all $\mathbb{F}_p$. Thus, at the expense of making a weaker claim about reducibility, we have successfully constructed an entire class of polynomials with a similar property.

8.1 Résumé

On étudie l'opération de produit composé $\diamond$ ainsi que la décomposition de polynômes en polynômes indécomposables.

8.2 Abstract

We discuss the composed multiplication operation $\diamond$ and the decomposition of polynomials under this operation.

8.3 Introduction

Let $f, g \in \mathbb{F}_q[x]$ be two monic polynomials over the finite field of q elements. Brawley and Carlitz [1] studied various forms of composed products of the two polynomials, denoted by $f \diamond g$. Among them are the composed products induced by the field multiplication and field addition on the algebraic closure of $\mathbb{F}_q$. In particular, let $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ be all the roots of f and g respectively in an algebraic closure of $\mathbb{F}_q$. The composed addition of f and g is given by

$$\prod_{i=1}^{m} \prod_{j=1}^{n} \big(x - (\alpha_i + \beta_j)\big)\,,$$

and the composed multiplication of f and g is given by

$$\prod_{i=1}^{m} \prod_{j=1}^{n} (x - \alpha_i \beta_j)\,.$$

Among other results, they prove the following theorem:

Theorem 8.3.1. *Let $f, g \in \mathbb{F}_q[x]$ be monic polynomials with $\deg f = m$ and $\deg g = n$. Then $f \diamond g$ is irreducible if and only if both f and g are irreducible and $\gcd(m, n) = 1$.*

The majority of the remaining results from their paper deal with decomposing polynomials and the properties of such decompositions.

Let R be a commutative ring. We recall that the resultant of two polynomials $f, g \in R[x]$, denoted $\mathrm{Res}_x(f, g)$, is the determinant of their Sylvester matrix. In a paper of Ayad, he shows that if the monic polynomials $f, g \in \mathbb{Z}[x]$ satisfy certain additional properties, then the polynomial

$$\mathrm{Res}_y\big(f(y), g(x - y)\big) \in \mathbb{Z}[x]$$

is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{F}_p$ for all primes p. The above polynomial is related to the composed addition of f and g:

$$\prod_{i=1}^{m} \prod_{j=1}^{n} \big(x - (\alpha_i + \beta_j)\big) = \mathrm{Res}_y\big(f(y), g(x - y)\big)$$

where $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are all the roots of f and of g in $\mathbb{C}$ respectively.

The aim of this paper is to provide integral polynomials irreducible over $\mathbb{Z}$ which are reducible over $\mathbb{F}_p$ for every prime p. In particular, we show that certain composed products of integral polynomials are reducible modulo p for all primes p.

8.4 Preliminaries

Let R be a commutative ring with unity and $g = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in R[x]$. The homogenization of g, denoted ${}^h g(y,x)$, is the polynomial defined by

$$ {}^h g(y,x) := b_n x^n + b_{n-1}x^{n-1}y + \cdots + b_1 x y^{n-1} + b_0 y^n \,,$$

that is, it is a homogeneous polynomial in $R[x,y]$ of degree $n = \deg g$ such that ${}^h g(1,x) = g(x)$. Direct comparison shows that $y^n g(x/y) = b_n x^n + b_{n-1}x^{n-1}y + \cdots + b_1 x y^{n-1} + b_0 y^n = {}^h g(y,x)$.

In the case where R is a field, if $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are all the roots of f and g respectively in an algebraic closure of R, and if c_f and c_g are the leading coefficients of f and g respectively, then we obtain

$$\begin{aligned} c_f^n c_g^m \prod_{i=1}^{m}\prod_{j=1}^{n}(x - \alpha_i\beta_j) &= c_f^n \prod_{i=1}^{m}\left({\alpha_i}^n c_g \prod_{j=1}^{n}\left(x/\alpha_i - \beta_j\right)\right) \\ &= c_f^n \prod_{i=1}^{m}\left({\alpha_i}^n g(x/\alpha_i)\right) \\ &= \mathrm{Res}_y\big(f(y), y^n g(x/y)\big) \\ &= \mathrm{Res}_y\big(f(y), {}^h g(y,x)\big)\,. \end{aligned}$$

This motivates the following definition:

Definition 8.4.1. Let R be a commutative ring with unity and $f, g \in R[x]$. We define the composed product of f and g by

$$(f \diamond g)(x) := \mathrm{Res}_y\big(f(y), {}^h g(y,x)\big)\,.$$

It is clear from the definition that if $f = f_1 \diamond f_2$, then $c_f = c_{f_1}^{\deg f_2} \cdot c_{f_2}^{\deg f_1}$ where c_g denotes the leading coefficient of the polynomial g. This property is paralleled with the constant terms of the polynomials: again letting $g = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in R[x]$ and letting $m = \deg f$, if $b_0 \neq 0$, then

$$\begin{aligned} (f \diamond g)(0) &= \mathrm{Res}_y\big(f(y), {}^h g(y,0)\big) \\ &= \mathrm{Res}_y\big(f(y), b_0 y^n\big) \\ &= (-1)^{mn}\mathrm{Res}_y\big(b_0 y^n, f(y)\big) \\ &= (-1)^{mn} {b_0}^m f(0)^n\,, \end{aligned}$$

and if $b_0 = 0$, then

$$(f \diamond g)(0) = \mathrm{Res}_y\big(f(y), {}^h g(y,0)\big) = \mathrm{Res}_y\big(f(y), 0\big) = 0\,.$$

Thus, $(f \diamond g)(0) = (-1)^{mn} f(0)^n g(0)^m$.

The set $R[x]$ is closed under the composed product binary operation. It is of interest then to determine the units, if any, with respect to this operation. The polynomial $\ell = x - 1 \in R[x]$ is the identity under $\diamond$: for any $f \in R[x]$ we have

$$(\ell \diamond f)(x) = \mathrm{Res}_y\big(\ell(y), {}^h f(y,x)\big) = {}^h f(1,x) = f(x)$$

and

$$(f \diamond \ell)(x) = \mathrm{Res}_y\big(f(y), x - y\big) = (-1)^{2\deg f}\mathrm{Res}_y\big(y - x, f(y)\big) = f(x)\,.$$

If $u, v \in R[x]$ are inverses of one another, then $1 = \deg \ell = \deg(u \diamond v) = \deg u \cdot \deg v$ so that $\deg u = \deg v = 1$. Let $u = u_1 x + u_0$ and $v = v_1 x + v_0$. We have

$$x - 1 = \ell(x) = (u \diamond v)(x) = u_1 v_1 x - u_0 v_0\,,$$

from which we obtain $u_1 v_1 = u_0 v_0 = 1$. That is, u_1 and u_0 are units, and $v = {u_1}^{-1} x + {u_0}^{-1}$. It is readily verified that $\diamond$ is associative on linear polynomials, so we summarize as follows:

Theorem 8.4.2. *Let R be a commutative ring with unity. The group of units of $R[x]$ under $\diamond$ consists exactly of the linear polynomials $u = u_1 x + u_0$ with $u_1, u_0 \in R^\times$, and the inverse of any such u is given by ${u_1}^{-1} x + {u_0}^{-1}$.*

Although it will not be of use to us in this paper, we note the algebraic structure of the group of units:

Proposition 8.4.3. *Let R be a commutative ring with unity, and let $G_\diamond$ be the group of units of $R[x]$ under $\diamond$. Then $G_\diamond \simeq R^\times \oplus R^\times$.*

Proof. Let $(\bar{R}, +, *)$ be induced from the ring $(R, +, \cdot)$ with multiplication instead defined by $x * y := -(x \cdot y)$. The map $\phi : R \to \bar{R}$ defined by $\phi(x) = -x$ is a ring isomorphism. Since $R \simeq \bar{R}$ as rings, we obtain $R^\times \simeq \bar{R}^\times$ as groups. Defining the map $\psi : G_\diamond \to R^\times \oplus \bar{R}^\times$ by $\psi(u_1 x + u_0) = (u_1, u_0)$, we have $G_\diamond \simeq R^\times \oplus \bar{R}^\times \simeq R^\times \oplus R^\times$. □

With the units now known, we make the following definition:

Definition 8.4.4. Let R be a commutative ring with unity and $f \in R[X]$. If there exist $f_1, f_2 \in R[X] \setminus G_\diamond$ such that $f = f_1 \diamond f_2$, then we say that f is *multiplicatively decomposable*. Otherwise, we say that f is multiplicatively indecomposable.

If f only admits decompositions of the form $f = f_1 \diamond f_2$ with either f_1 or f_2 linear, then we will say that f is *near-indecomposable* over A.

The near-indecomposable polynomials will be largely sufficient for the purposes of this paper, but we make here a few comments about indecomposable polynomials. Every indecomposable polynomial is near-indecomposable by definition, and the two notions coincide over a

field. When applicable, the following lemma can be used to determine when certain near-indecomposable polynomials are indecomposable:

Lemma 8.4.5. *Let R be a commutative ring with unity, and let $f \in R[x]$ be near-indecomposable over R. If the leading coefficient and constant term of f both lie in $R^\times$, then f is indecomposable over R.*

Proof. We have that f is near-indecomposable, so we write $f = f_1 \diamond f_2$ with f_1 linear without loss of generality. If the leading coefficient c_f of f and $f(0)$ both lie in $R^\times$, then

$$c_f = c_{f_1}^n c_{f_2}$$

and

$$f(0) = (f_1 \diamond f_2)(0) = (-1)^n f_1(0)^n f_2(0)$$

show that $c_{f_1}, f_1(0) \in R^\times$ as well. Thus $f_1 = c_{f_1} x + f_1(0) \in G$, so f is indecomposable. □

8.5 Composed Product Decompositions

We begin this section by presenting two classes of near-indecomposable polynomials.

Theorem 8.5.1. *Let R be a commutative ring with unity. If $f \in R[x]$ has degree p a prime, then f is near-indecomposable over R.*

Proof. Suppose that $f = f_1 \diamond f_2$ for some $f_1, f_2 \in R[x]$ of degrees m and n respectively. Since $p = \deg f = mn$, it follows that either f_1 or f_2 is linear. □

Theorem 8.5.2. *Let R be a commutative ring with unity. If $f \in R[x]$ with $\deg f > 1$ has leading coefficient p a prime, and if p is not a zero divisor of R, then f is near-indecomposable over R. Moreover, the leading coefficient of any linear decomposition factor lies in $R^\times$.*

Proof. Suppose that $f = f_1 \diamond f_2$ for some $f_1, f_2 \in R[X]$ with respective degrees m and n. We have $p = c_{f_1}^n c_{f_2}^m$. Suppose without loss of generality that p divides $c_{f_1}^n$. Then p divides c_{f_1}, and writing $c_{f_1} = pa$ with $a \in R$ yields $p = p^n a^n c_{f_2}^m$. Since p is not a zero divisor, $0 = p(p^{n-1} a^n c_{f_2}^m - 1)$ implies that $p^{n-1} a^n c_{f_2}^m = 1$. Then p^{n-1} divides 1, which is impossible unless $n = 1$. We conclude that $\deg f_2 = 1$ and $a c_{f_2}^m = 1$. □

If a polynomial is not near-indecomposable, then one might ask about a possible decomposition into some near-indecomposables.

Theorem 8.5.3. *Let R be a commutative ring with unity. If $f \in R[x]$, then $f = f_1 \diamond f_2 \diamond \cdots \diamond f_r$ for some near-indecomposable polynomials $f_i \in R[x]$.*

Proof. The case where f is itself indecomposable is trivial. Let us then suppose that f is decomposable and proceed by induction on $\deg f$. The result clearly holds when $\deg f = 1$ as every linear polynomial is near-indecomposable, and we assume as induction hypothesis that the result also holds for all polynomials of degree less than or equal to $\deg f$.

Since f is assumed decomposable, we may write $f = f_1 \diamond f_2$ for some $f_1, f_2 \in R[x] \setminus G_\diamond$. If $\deg f_1 < \deg f$ and $\deg f_2 < \deg f$, by hypothesis we have $f_1 = g_1 \diamond \cdots g_t$ and $f_2 = g_{t+1} \diamond g_r$ for some near-indecomposable polynomials $g_i \in R[x]$. Then $f = g_1 \diamond \cdots \diamond g_r$ as required. If it is only possible to write $f = f_1 \diamond f_2$ with either f_1 or f_2 linear, then f is near-indecomposable by definition. □

Let R and S be commutative rings with unity. A ring homomorphism $\sigma : R \to S$ can be naturally extended to a ring homomorphism from $R[x]$ to $S[x]$ by $a_m x^m + \cdots + a_0 \mapsto \sigma(a_m)x^m + \cdots + \sigma(a_0)$. If $\sigma : R[x] \to S[x]$ preserves the degrees of $f, g \in R[x]$, then

$$\sigma\big(\mathrm{Res}_x(f,g)\big) = \mathrm{Res}_x\big(\sigma(f), \sigma(g)\big)$$

since $\mathrm{Res}_x(f,g)$ is a polynomial in the coefficients of f and of g. This leads us to the following result:

Theorem 8.5.4. *Let R and S be commutative rings with unity, $\sigma : R \to S$ a ring homomorphism, and $f \in R[x]$ be such that its leading coefficient and constant term are not mapped to 0 by σ. If $f = f_1 \diamond f_2$ over R, then $\sigma f = \sigma f_1 \diamond \sigma f_2$ over S. Moreover, $\deg \sigma f_1 = \deg f_1$ and $\deg \sigma f_2 = \deg f_2$.*

Proof. We naturally extend σ to a ring homomorphism from $R[x,y]$ to $S[x,y]$. By assumption, σ does not map c_f nor $f(0)$ to zero. Denote the degrees of f_1 and f_2 by m and n respectively. Then $c_f = c_{f_1}^n c_{f_2}^m$ implies that

$$0 \neq \sigma(c_f) = \sigma(c_{f_1})^n \sigma(c_{f_2})^m \,,$$

while $f(0) = f_1(0)^n f_2(0)^m$ implies that

$$0 \neq \sigma\big(f_1(0)\big)^n \sigma\big(f_2(0)\big)^n \,.$$

Since σ does not map the leading coefficients nor the constant terms of f_1 and f_2 to zero, it preserves the degrees of these two polynomials as well as those of ${}^h f_1(Y,X)$ and ${}^h f_2(Y,X)$. Thus,

$$\sigma(f_1 \diamond f_2) = \sigma\Big(\mathrm{Res}_y\big(f_1(y), {}^h f_2(y,x)\big)\Big) = \mathrm{Res}_y\big(\sigma f_1(y), {}^h \sigma f_2(y,x)\big) = \sigma f_1 \diamond \sigma f_2 \,. \qquad \square$$

Theorem 8.5.5. *Let R and S be commutative rings with unity, $\sigma : R \to S$ a ring homomorphism, and $f \in R[x]$ be such that its leading coefficient and constant term are not mapped to 0 by σ. If σf is near-indecomposable over S, then f is near-indecomposable over R.*

Proof. By Theorem 8.5.3, we write $f = f_1 \diamond \cdots \diamond f_r$ where each $f_i \in R[x]$ is near-indecomposable over R. Then $\sigma f = \sigma f_1 \diamond \cdots \diamond \sigma f_r$ is near-indecomposable over S, so all but one of the σf_i are linear, say f_t with $k \in \{1, \ldots, r\}$. It follows from $\deg f_i = \deg \sigma f_i = 1$ that f_i is linear for each $i \in \{1, \ldots, r\} \setminus \{t\}$. Setting $\ell_1 := f_1 \diamond \cdots \diamond f_{t-1}$ and $\ell_2 := f_{t+1} \diamond \cdots \diamond f_r$ yields $f = \ell_1 \diamond f_1 \diamond \ell_2$. Thus, f is near-indecomposable. □

The proof of the next theorem requires a lemma, which follows immediately from the definition of composed multiplication:

Lemma 8.5.6. *Let R be an integral domain and K its field of fractions. Let $f, f_1, f_2 \in R[x]$ and let $f = c_f F$, $f_1 = c_{f_1} F_1$, and $f_2 = c_{f_2} F_2$ where $c_f, c_{f_1}, c_{f_2} \in R$ and $F, F_1, F_2 \in K[x]$ are monic. Then $f = f_1 \diamond f_2$ over R if and only if $F = F_1 \diamond F_2$ over K and $c_f = c_{f_1}^{\deg f_2} c_{f_2}^{\deg f_1}$.*

Theorem 8.5.7. *Let R be a commutative ring with unity, $\mathfrak{m}$ a maximal ideal of R such that the residue field $R/\mathfrak{m}$ is finite, and $f \in R[x]$ have degree at least 2. If the image of f modulo $\mathfrak{m}$ is irreducible over $R/\mathfrak{m}$ and its leading coefficient and constant term do not lie in $\mathfrak{m}$, then f is the multiplicative composition of at most $\omega(\deg f)$ near-indecomposable polynomials of degrees at least 2 over R.*

Proof. Suppose that $f = f_1 \diamond \cdots \diamond f_r$ where each $f_i \in R[x]$ is near-indecomposable of degree at least 2 over R. Define $\sigma : R \to R/\mathfrak{m}$ by $a \mapsto a \pmod{\mathfrak{m}}$ and extend it to a polynomial ring homomorphism.

Suppose that $r > \omega(\deg f)$. The leading coefficient and constant term of f are not zero modulo $\mathfrak{m}$, so each $\deg f_i = \deg \sigma f_i$ divides $\deg f = \deg \sigma f$ by Theorem 8.5.4. It follows from the pigeonhole principle that at least two of the $\deg \sigma f_i$ share a prime factor of $\deg \sigma f$, say $\deg \sigma f_1$ and $\deg \sigma f_2$ without loss of generality. Set $\sigma g := \sigma f_2 \diamond \cdots \diamond \sigma f_r$ so that $\sigma f = \sigma f_1 \diamond \sigma g$. We assume that these polynomials are monic, otherwise we simply divide by their leading coefficients and the relationship remains by Lemma 8.5.6. By assumption, σf is irreducible over $R/\mathfrak{m}$, so we must have $\gcd(\deg \sigma f_1, \deg \sigma g) = 1$ by Theorem 8.3.1, which contradicts the two degrees sharing a prime factor. Thus, we conclude that $r \leq \omega(\deg f)$. □

Corollary 8.5.8. *Let $f_1, f_2, \ldots, f_r \in \mathbb{Z}[x]$ have degrees all at least 2. If $\omega(\deg f_1 \cdots \deg f_r) < r$, then $f_1 \diamond \cdots \diamond f_r$ is reducible modulo p for every prime p that does not divide its leading coefficient and constant term.*

Example 8.5.9. The following are irreducible over $\mathbb{Z}$ but reducible over $\mathbb{F}_p$ for all primes p:

(i) $x^{12} - x^{10} + 3x^8 + 4x^6 + 3x^4 + 2x^2 + 1 = (x^2 + 1) \diamond (x^2 + x + 1) \diamond (x^3 + x^2 + 1)$;

(ii) $x^8 + 2x^4 + x^2 + 1 = (x^2 + 1) \diamond (x^4 + x + 1)$;

(iii) $x^4 + 5x^2 + 4 = (x^2 + 1) \diamond (x^2 + x - 2)$;

(iv) $x^4 + (a^2 - 2)x^2 + 1 = (x^2 + 1) \diamond (x^2 + ax + 1)$ when $a \notin \{0, \pm 2\}$;

(v) $x^4 + (a^2 + 2)x^2 + 1 = (x^2 + 1) \diamond (x^2 + ax - 1)$ when $a \neq 0$.

Note that the polynomial $f \diamond g$ will not always be irreducible over $\mathbb{Z}$. The examples given above can all routinely be verified as irreducible over $\mathbb{Z}$ by brute force or by use of a computer algebra system.

Theorem 8.5.7 can also be used to produce some weaker statements about the reducibility of polynomials over finite fields. For example, it is well-known that the polynomial $x^4 + 1$ is irreducible over $\mathbb{Z}$ but reducible over every $\mathbb{F}_p$. Letting $R = \mathbb{Z}[\sqrt{2}]$, we can view the polynomial $f = x^4 + (a^2 \pm 2)x^2 + 1$ from the above example (iv and v) as being polynomials in $R[x]$. The ideal $(\sqrt{2})$ of R is prime with corresponding residue field $\mathbb{F}_2$, and $x^2 - 2$ has a root α modulo p when $p \equiv \pm 1 \pmod 8$, so $(p, \sqrt{2} - \alpha)$ is a prime ideal with corresponding residue field $\mathbb{F}_p$. For primes $p \equiv \pm 3 \pmod 8$, the corresponding residue field is $\mathbb{F}_{p^2}$. It follows that the polynomial f is reducible over $\mathbb{F}_p$ for $p = 2$ and every $p \equiv \pm 1 \pmod 8$, and it is reducible at least over $\mathbb{F}_{p^2}$ for every $p \equiv \pm 3 \pmod 8$.

If $a = n\sqrt{2}$ for $n \in \mathbb{Z} \setminus \{0\}$, we have $f = x^4 + 2(n^2 \pm 1)x^2 + 1$. It is clear that f has no integer roots, since $f(x) > 0$ for integer x. Attempting to write f as a product of two quadratic factors leads to an equation of the form $2u - b^2 = 2(n^2 \pm 1)$ for an integer b and $u \in \{\pm 1\}$. This implies that 2 divides b, so we write $b = 2c$ and obtain $u - 2c^2 = n^2 \pm 1$. We deduce from $n^2 - 2c^2 \in \{0, \pm 2\}$ that n is must be even. Letting $n = 2m$, we obtain the Pell equations $c^2 - 2m^2 = \mp 1$. Therefore, f is irreducible over $\mathbb{Z}$ whenever n is odd, or whenever n is even but there is no $c \in \mathbb{Z}$ such that either of the Pell equations $c^2 - 2(n/2)^2 = \pm 1$ has solution $(c, n/2)$. In particular, for $n = 1$, we recover $x^4 + 1$, so this argument leads to a weaker statement about reducibility but for a more general class of polynomials.

8.6 Bibliography

[1] J.V. Brawley and L. Carlitz, Irreducibles and the composed product for polynomials over a finite field, Discrete Math. 65 (1987) 115–139.

[2] J.V. Brawley and L. Carlitz, A test for additive decomposability of irreducibles over a finite field, Discrete Math. 76 (1989) 61–65.

Chapter 9

Least primes which split in imaginary quadratic fields

9.1 Résumé

Soit $D < 0$ un entier libre de facteurs carré tel que D est 0 ou 1 modulo 4, $K = \mathbb{Q}(\sqrt{D})$ et h_K le nombre de classes pour le corps K. On utilise les formes quadratiques binaires afin de borner le $(h_K + 1)$-ième nombre premier qui se décompose dans K.

9.2 Abstract

Let $K = \mathbb{Q}(\sqrt{D})$ where $D < 0$ is congruent to either 0 or 1 modulo 4, and let h_K be the class number of K. We show that the $(k_K + 1)$st least prime that splits in K is bounded below by $\sqrt{\frac{3|D|}{4}}$. The proof relies on the fact that the smallest integers representable by a reduced binary quadratic form $ax^2 + bxy + cy^2$ are among a, c, and $a - |b| + c$.

9.3 Introduction

In the ring $\mathbb{Z}$, the prime numbers are, up to a unit, the irreducible elements of the ring. The fundamental theorem of arithmetic guarantees a unique decomposition, up to a unit, of an integer into a product of primes. While this property does not directly translate to arbitrary rings, we can instead discuss the decomposition of ideals into the product of prime ideals. For our purposes, we will briefly recall the necessary ideas for dealing with extensions of $\mathbb{Q}$.

Let K be a number field, and let O_K be its ring of integers. If p is a prime number, then $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, and pO_K admits a unique decomposition into a product of maximal (so also prime) ideals of the form

$$pO_K = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}.$$

Setting as usual $f_i = [O_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ yields the equality

$$[K : \mathbb{Q}] = \sum_{i=1}^{m} e_i f_i \, .$$

If $f_i = e_i = 1$ for all i, we say that p splits completely in K. If $m = 1$ and $f_1 = 1$, then we say that p ramifies completely in K. If $m = 1$ and $e_1 = 1$, then we say that p is inert in K.

The nonzero fractional ideals of O_K, under a suitable equivalence relation, form an abelian group. The number of these ideals classes comprising this ideal class group is finite, and we call it the class number of K and denote it h_K.

In his treatise Disquistiones Arithmeticae, Gauss presented his class number problem. For a given positive integer n, this problem asks for a list all imaginary quadratic fields with class number n, although the original problem was stated in the language of binary quadratic forms. Gauss conjectured that $h(D)$, the number of classes of primitive positive definite quadratic forms of discriminant D, tends to infinity as $-D$ does.

This problem has a very long history, and it has been the subject in works of many authors. Heilbronn [9] ineffectively resolved the general problem. Gauss's class number one problem, which refers to the case $n = 1$, was proved first by Heegner [8], although the proof contains some minor gaps. It was proved later by Baker [1] and Stark [12], who then jointly solved the problem for $n = 2$ [2].

Goldfeld [6] showed that the problem can be reduced to the existence of an elliptic curve with a Hasse-Weil L-function possessing a zero of order at least 3 at $s = 1$. Gross and Zagier [7] proved the existence of such an elliptic curve, reducing the problem to a finite number of computations. Oesterlé [11] generalized Goldfeld's theorem to the solve the problem for $n = 3$. Watkins [13] then modified Goldfeld's approach by considering Dirichlet L-functions possessing zeroes near the real line with low height, which solved the problem for $n \leq 100$.

Beckwith [3] provided an estimate for the number of negative fundamental discriminants whose corresponding class numbers $h(D)$ are indivisible by a given prime and whose imaginary quadratic fields satisfy a given set of local conditions.

Lamzouri, Li, and Soundararajan [10] proved, among other results, upper and lower bounds for $L(1, \chi)$ and $\zeta(1+it)$. They also deduced explicit bounds for the class number of imaginary quadratic fields assuming the generalized Riemann hypothesis.

The aim of this paper is to provide a lower bound on the least primes that split in an imaginary quadratic field in terms of its class number.

9.4 Preliminary Results

We first recall some terminology regarding quadratic forms. A binary quadratic form is given by

$$f(X,Y) = aX^2 + bXY + cY^2$$

for integers a, b, and c and discriminant $D = b^2 - 4ac$. An integer m is said to be represented by the quadratic form $f(X,Y)$ if and only if there exist integers x and y such that $m = f(x,y)$, and the representation is said to be proper if $\gcd(x,y) = 1$.

We will be interested only in positive definite quadratic forms, that is, those with negative discriminants and which represent only positive integers. Furthermore, we say that the quadratic form is primitive if and only if $\gcd(a,b,c) = 1$. Two forms $f(X,Y)$ and $g(X,Y)$ are said to be equivalent if there exist integers α,β,γ, and δ such that $f(X,Y) = g(\alpha X + \beta Y, \gamma X + \delta Y)$ and $\alpha\delta - \gamma\beta = \pm 1$. It is clear that this is an equivalence relation, that equivalent forms represent the same integers, and that equivalent forms have the same discriminant. The equivalence is said to be proper if $\alpha\delta - \gamma\beta = 1$, and we say that two forms are in the same class if and only if they are properly equivalent. Lastly, we recall that a primitive positive definite quadratic form $aX^2 + bXY + cY^2$ is reduced if $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

We will require the following three results, all of which can be found in Cox [4].

Lemma 9.4.1. *Let $f(X,Y) = aX^2 + bXY + cY^2$ be a reduced primitive positive definite quadratic form. Then for any integers x and y,*

$$f(x,y) \geq (a - |b| + c)\min(x^2, y^2)\,.$$

Lemma 9.4.2. *Let $f(X,Y) = aX^2 + bXY + cY^2$ be a reduced primitive positive definite quadratic form. Then*

$$a \leq \sqrt{\frac{|D|}{3}}\,.$$

Theorem 9.4.3. *Every primitive positive definite quadratic form is properly equivalent to a unique reduced quadratic form.*

Since we will be considering forms which are reduced with a fixed discriminant $D < 0$, we immediately have the following result from Lemma 9.4.2 and Theorem 9.4.3:

Theorem 9.4.4. *Let $D < 0$ be given. Then the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and it is equal to the number of reduced forms of discriminant D.*

9.5 Main Result

We prove the following theorem:

Theorem 9.5.1. *Let $D < 0$ be an integer satisfying $D \equiv 0$ or $1 \pmod 4$, let $K = \mathbb{Q}(\sqrt{D})$, and let h_K the class number of K. If the least $h_K + 1$ odd prime numbers which split in K are denoted by $p_1, p_2, \ldots, p_{h_k+1}$ with $p_1 < p_2 < \cdots < p_{h_K+1}$, then*

$$p_{h_K+1} \geq \frac{1}{4}\sqrt{3|D|}\,.$$

Proof. If p is an odd prime which splits in K, then $\left(\frac{D}{p}\right) = 1$, and p can be represented by a proper quadratic form of discriminant D. Hence, it can be represented by a positive definite quadratic form of discriminant $D < 0$ and, consequently, also by a reduced quadratic form of discriminant $D < 0$.

There exist h_K reduced forms of discriminant D. Of the $h_K + 1$ least prime numbers which do not split in K, at least two of them are then represented by the same reduced quadratic form of discriminant D. We let p_i and p_j be these two primes and $f(X, Y) = aX^2 + bXY + cY^2$ the form which represents them both. We additionally assume without loss of generality that $p_i < p_j$.

The form $f(X, Y)$ satisfies the conditions of Lemma 9.4.1, so for integers x and y we have

$$f(x, y) \geq (a - |b| + c)$$

whenever $xy \neq 0$. Additionally, we have $|b| \leq a$ since $f(X, Y)$ is reduced. Thus, $f(x, y) \geq c$. If $|b| \neq c$, then $f(x, y) > a$. If $|b| = c$, then we have $c = a = 1$. This imposes $|b| = c = 1$, so that

$$D = b^2 - 4ac = -3a^2 = -3\,.$$

The theorem holds trivially when $D = -3$, so we suppose now that $D \neq -3$, in which case we have $f(x, y) \geq c$ and $f(x, y) > a$ whenever $xy \neq 0$. For $xy = 0$, we consider each possibility separately. First, if $x = y = 0$ we have $f(0, 0) = 0$. Next, if $x = 0$ and $y \neq 0$, we have

$$f(0, y) = cy^2 \geq c\,.$$

Finally, if $x \neq 0$ and $y = 0$, we have

$$f(x, 0) = ax^2 \geq a\,.$$

Altogether, we have shown that the smallest positive integer that $f(x, y)$ may take is a, while the second smallest is c.

Since the smallest positive integer representable by $f(X, Y)$ is a, we have $p_i \geq a$. Since the second smallest positive integer representable by $f(X, Y)$ is c, and since $p_j > p_i$ is representable by $f(X, Y)$, we deduce that $p_j \geq c$.

The discriminant of f satisfies

$$D = b^2 - 4ac < 0\,,$$

so we have

$$-D = 4ac - b^2 > 0\,.$$

By Lemma 9.4.2,

$$a \leq \sqrt{\frac{|D|}{3}}\,,$$

so

$$|D| = -D \leq 4c\sqrt{\frac{|D|}{3}}\,.$$

Then

$$\frac{1}{4}\sqrt{3|D|} \leq c \leq p_j \leq p_{h_K+1}\,.$$

□

Example 9.5.2. Consider the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-163})$ which has class number $h_K = 1$. Let p_1 and p_2 be the two least odd prime numbers which split in K. If $p_1 < p_2$, then Theorem 9.5.1 asserts that $p_2 \geq \frac{1}{4}\sqrt{3(163)} \approx 5.528$. It is readily verified that each of the primes 2, 3, and 5 are in fact inert: $\mathcal{O}_K = \mathbb{Z}\left[\frac{-1+\sqrt{-163}}{2}\right]$ and each of the ideals (2), (3), and (5) are prime ideals of $\mathcal{O}_K$.

Remark 9.5.3. *The problem of bounding the smallest rational prime which splits in a number field has been previously explored. For example, Siegel's bound on the size of class numbers implies that* $|D|^{1/2-\epsilon} \ll h(D) \ll |D|^{1/2+\epsilon}$*, as discussed in [5], where* $h(D)$ *denotes the number of classes of primitive positive definite quadratic forms of discriminant* D*. Combined with the prime number theorem, one obtains that the* h_K*-th prime is asymptotically greater than* $|D|^{1/2-\epsilon}\log|D|$*.*

The authors would like to thank an anonymous referee who was kind enough to bring such an expected bound for this type of problem to their attention.

9.6 Bibliography

[1] Baker A, Linear forms in the logarithm of algebraic number I, II, III, *Mathematika* **13** (1966), 204–216; ibid. **14** (1967), 102–107; ibid. **14** (1967), 220–228.

[2] Baker A, Stark H, On a fundamental inequality in number theory, *Ann. of Math.*, (2) **94** (1971), 190–199.

[3] Beckwith O, Indivisibility of class numbers of imaginary quadratic fields, *Res Math Sci.*, **4** (2017), no. 20.

[4] Cox D A, Primes of the form $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New Tork (1989).

[5] Davenport H, Multiplicative number theory, third ed., *Graduate Texts in Mathematics*, vol 74, Springer-Verlag, New York, 2000, Revised and with a preface by Hugh L. Montgomery.

[6] Goldfeld D, Gauss's class number problem of imaginary quadratic fields, *Bull. Amer. Math. Soc.*, (1) **13** (1985), 23–37.

[7] Gross B H and Zagier D, Heegner points and derivatives of L-series, *Invent. Math.*, **84** (1986), 225–320.

[8] Heegner K, Diophantische analysis und modulfunktionen, *Math. Z*, **56** (1952), 227–253.

[9] Heilbronn H, On the class number in imaginary quadratic fields, *Quart. J. Math. Oxford Ser.*, (2) **5** (1934),150–160.

[10] Lamzouri Y, Li X, and Soundararajan K, Conditional bounds for the least quadratic non-residue and related problems, *Math. of Comp.*, **84** (2015), 907–938.

[11] Oesterlé J, Nombres de classes des corps quadratiques imaginaires, Seminaires Nicolas Bourbaki, 1983-1984. Astérisque no. 121-122 (1985), 309–323.

[12] Stark H, A complete determination of the complex quadratic fields of class-number one, *Michigan Math. J.*, **14** (1967), 1–27.

[13] Watkins M., Class number of imaginary quadratic field, *Math. of Comp.*, **73** (2003), 907–938.

Chapter 10

On the covering of rings by their subrings

10.1 Résumé

On étudie la possibilité de recourvrir un anneau avec ses sous-anneaux.

10.2 Abstract

We explore the possibility of covering a ring by its subrings.

10.3 Introduction

It is a well-known result that a group cannot be the union of two of its proper subgroups. Scorza seems to have been the first to show that a group is a union of three proper subgroups if and only if it has a quotient isomorphic to the Klein 4-group $V = {C_2}^2$. For the case of covering by four, five, or six subgroups, a similar result holds by replacing V with some other finite group as needed for each case. The case of seven subgroups is notably different: no group can be written as a union of seven of its proper subgroups.

Werner considered the similar problem of covering a ring by its proper subrings.

We say that a ring R is *coverable* if R is equal to a union of its proper subrings: a definition provided by Werner [1]. If this can be done using a finite number of proper subrings, then $\sigma(R)$ denotes the *covering number* of R, which is the minimum number of subrings required to cover R. If R is not coverable, then we take $\sigma(R) = \infty$. Werner [1] proved the following:

Proposition 10.3.1 (Werner)**.** *Let R be a coverable ring such that $\sigma(R)$ is finite. Then there exists a two-sided ideal I of R such that R/I is finite and $\sigma(R) = \sigma(R/I)$.*

The aim of this paper is to expand on the concept of coverable rings.

10.4 Main Results

We begin by providing an example of rings not coverable by their subrings.

Proposition 10.4.1. *The ring $\mathbb{Z}_p$ of p-adic integers is not coverable by a finite number of its proper subrings.*

Proof. The ring $\mathbb{Z}_p$ is principal, and its only ideals are the principal ideals

$$\{0\} \quad \text{and} \quad I_k = \left(p^k\right),\ k \geq 1\,.$$

Suppose that

$$\mathbb{Z}_p = \bigcup_{i=1}^{n} R_i, \quad R_i \subsetneqq \mathbb{Z}_p\,.$$

There exists $I \subset \bigcap_{i=1}^{n} R_i \neq \{0\}$, from which we deduce that $I = I_k$ for some k. Then $I_k = p^k\mathbb{Z}_p$ and

$$\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}\,,$$

the latter of which is not coverable. □

Remark 10.4.2. *We know that if R is a ring such that $R = \bigcup_{i=1}^{n} R_i$ without redundancies, and each R_i is a proper subring of R, then R_i is of finite index in R for each $i \in \{1, \ldots, n\}$.*

We now provide an example of rings which are coverable with finite covering number.

Proposition 10.4.3. *Suppose that $R = \bigcup_{i=1}^{\infty} R_i$, where the R_i are all subrings of R of finite index. If R is Artinian, then*

$$R = \bigcup_{i=1}^{t} R_i$$

for some t.

Proof. Since R_1 has finite index in R, there exists an ideal I_1 of R such that $I_1 \subseteq R_1$ and I_1 has finite index in R. The same argument implies that there exists an ideal $I_2 \subseteq R_2$ where R_2 is again an ideal of R with finite index. Then

$$R \supseteq I_1 \supseteq I_1 \cap I_2 \supseteq I_1 \cap I_2 \cap I_3 \supseteq \cdots\,.$$

Since R is Artinian, the descending sequence of ideals is stationary. Then

$$\bigcap_{j=1}^{\infty} I_j = I_1 \cap I_2 \cap \cdots \cap I_n$$

for some n.

Let $I = \bigcap_{i=1}^{n} I_i$. We note that

$$I_1 \cdot I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n = \bigcap_{j=1}^{\infty} I_j \, .$$

Then I is an ideal of R contained in R_j for each $j \in \{1, \ldots, \infty\}$. We can now take $I = I_1 \cdot I_2 \cdots I_n$, and we then have

$$R/I = \left(\bigcup_{j=1}^{\infty} R_j \right) /I = \bigcup_{j=1}^{\infty} (R_j/I) \, .$$

This shows that R/I is coverable (infinitely) by the R_j/I. Since R/I is finite, then

$$R/I = \bigcup_{j=1}^{\infty} (R_j/I)$$

is a finite union, so we can extract finitely many of the R_j/I from the infinite union such that

$$R/I = \bigcup_{j=1}^{t} (R_j/I) \, .$$

Then

$$R = \bigcup_{j=1}^{t} R_j \, . \qquad \square$$

Remark 10.4.4. *If R is a monogenic ring of integers, then $R = \mathbb{Z}[\theta]$. If R is not monogenic, then $R = \bigcup_{i=1}^{\infty} \mathbb{Z}[\theta_i]$.*

We pose the two following questions:

Question 10.4.5. Is it possible to write a monogenic ring of integers R in the form

$$R = \bigcup_{i=1}^{\infty} \mathbb{Z}[\theta_i]$$

with $\left[R : \mathbb{Z}[\theta_i]\right]$ finite, that is, θ_i primitive, for all $i \in \{1, \ldots, \infty\}$?

Question 10.4.6. If question 10.4.5 is answered in the affirmative, is it possible to write

$$R = \bigcup_{i=1}^{n} \mathbb{Z}[\theta_i]$$

with θ_i primitive for all $i \in \{1, \ldots, n\}$, i.e., given an algebraic integer $\theta \in R$, does there exist $\theta_i \in R$ with θ_i primitive and $\theta \in \mathbb{Z}[\theta_i]$ for some $i \in \{1, \ldots, n\}$?

Example 10.4.7. Let K be a number field having no intermediate field, i.e., there is no subfield k such that

$$\mathbb{Q} \subsetneqq k \subsetneqq K\,.$$

For instance, when $[K : \mathbb{Q}] = p$ is a prime. If $\alpha \in R \setminus \mathbb{Z}$, where R is the ring of integers, then α is a primitive element. We have

$$R = \bigcup_{\alpha \in R \setminus \mathbb{Z}} \mathbb{Z}[\alpha]$$

where $R \setminus \mathbb{Z}$ is countable. Is is possible to find a field $K \supset \mathbb{Q}$ such that $R \neq \bigcup \mathbb{Z}[\alpha]$ where α a primitive element of K?

Proposition 10.4.8. *Let K be a number field and R its ring of integers. If*

$$R = \bigcup_{i=1}^{n} \mathbb{Z}[\theta_i] = \bigcup_{i=1}^{m} \mathbb{Z}[\alpha_i]\,,$$

where both unions are non-redundant, then $n = m$.

Proof. Since both unions are non-redundant, if $j_0 \in \{1, \ldots, m\}$, then there exists $i_0 \in \{1, \ldots, n\}$ such that $\theta_{i_0} \in \mathbb{Z}[\alpha_{j_0}]$ and $\theta_{i_0} \notin \bigcup_{j \in \{1,\ldots,m\} \setminus \{j_0\}} \mathbb{Z}[\alpha_j]$. This implies that for every $j \in \{1, \ldots, m\}$, there exists an $i \in \{1, \ldots, n\}$ such that $\mathbb{Z}[\theta_j]$ is the only one containing θ_i. Then $n \geq m$, and the same reasoning also implies that $m \geq n$. Thus, $n = m$. □

Theorem 10.4.9. *Let K be a number field and R its ring of integers. If*

$$R = \bigcup_{i=1}^{\ell} \mathbb{Z}[\theta_i]\,,$$

then

$$\ell > \big(\log_2 n - 1\big)\big(\sigma(R) - 1\big)$$

where n is the degree of K over $\mathbb{Q}$.

Proof. Let $R = \mathbb{Z}[w_1, \ldots, w_t]$ with t minimal. Then $w_1 \in \mathbb{Z}[\theta_1]$, $w_2 \in \mathbb{Z}[\theta_2]$, …, $w_t \in \mathbb{Z}[\theta_t]$ where we may change the ordering. If $w_1 \in \mathbb{Z}[\theta_i]$ and $w_2 \in \mathbb{Z}[\theta_j]$, then $i \neq j$, since otherwise

we have $R = \mathbb{Z}[w_1, w_2, \ldots, w_t] = \mathbb{Z}[\theta_i, w_3, \ldots, w_t]$ contradicting the minimality of t. Then $t \leq \ell$ and

$$\begin{aligned} R &= \mathbb{Z}[w_1, w_2, \ldots, w_t] \\ &= \mathbb{Z}[\theta_1, \theta_2, \ldots, \theta_\ell] \\ &= \mathbb{Z}[\theta_1, \ldots, \theta_{t-1}] \cup \mathbb{Z}[\theta_t, \ldots, \theta_{2t-1}] \cup \cdots \cup \mathbb{Z}[\ldots, \theta_\ell]\,. \end{aligned}$$

Since t is minimal,

$$\begin{gathered} \mathbb{Z}[\theta_1, \ldots, \theta_{t-1}] \subsetneqq R, \\ \vdots \\ \mathbb{Z}[\theta_t, \ldots, \theta_{2t-1}] \subsetneqq R, \\ \vdots \end{gathered}$$

are $\left\lceil \dfrac{\ell}{t-1} \right\rceil$ proper subrings in the above union comprising R. Then

$$\left\lceil \frac{\ell}{t-1} \right\rceil \geq \sigma(R)$$

implies that

$$\begin{aligned} \frac{\ell}{t-1} + 1 &> \sigma(R) \\ \ell &> (t-1)\big(\sigma(R) - 1\big) \\ \ell &> \big(\log_2 n - 1\big)\big(\sigma(R) - 1\big)\,. \end{aligned}$$

The quantity $\ell = \ell(K)$ is an invariant of the field K. If $\ell = 1$, K is said to be monogenic. If ℓ is finite, then

$$\ell > \big(\log_2 n - 1\big)\big(\sigma(R) - 1\big)\,. \qquad \square$$

Some Concluding Remarks

One might ask if there exists a ring R such that R is coverable as an additive group but not as a ring. Let K be a number field and R its ring of integers. We know that a group is a union (possibly an infinite one) of its proper subgroups if and only if it is not cyclic. Then $(R, +)$, which is never cyclic, is the union of its proper subgroups; however, it is not always coverable as a ring.

We conclude with a note on finite coverings. Let K be a number field and R its ring of integers with no common factor of indices, not coverable as a ring, and admitting a prime $p > 2$ such that

$$pR = \mathfrak{p}_1\mathfrak{p}_2$$

where $[K : \mathbb{Q}] = n > 2$. Then $R/\langle p \rangle$ is not coverable as a quotient ring. Conversely,

$$R/\langle p \rangle \cong \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \,,$$

where $q_1 = p^{f_1}$ and $q_2 = p^{f_2}$. Then $R/\langle p \rangle$ as a group is not cyclic. Thus,

$$R/\langle p \rangle = G_1 \cup \ldots \cup G_r$$

where the G_i are proper subgroups. Since $R/\langle p \rangle$ is finite, r is finite.

10.5 Bibliography

[1] N. J. Werner, Covering Numbers of Finite Rings, *The American Mathematical Monthly*, **122**(6), (2015), 552–566.

Conclusion

We discussed in this work some Diophantine equations and various other topics. In particular, we used well-known tools to explicitly solve some given Diophantine equations and bound the solutions to others. We also discussed topics such as additive, multiplicative, and usual function decompositions, a criterion for characterizing permutation polynomials, the splitting of primes in imaginary quadratic fields, and the covering of rings by subrings.

In chapter 1, we used a refinement of Runge's method to prove that the number of solutions to the equation $\mathrm{Res}_x\big(P(x), x^2 + sx + t\big) = a$ for $a \neq 0$ is finite. As is typical of Runge's method, we cannot immediately deduce anything about the size of the possible solutions to the equation. As such, finding other techniques to apply in place of Runge's method would be beneficial in finding an computably effective bound for the number of solutions. Moreover, as stated within that chapter, it is reasonable to assume that the method presented allows for replacing $x^2 + sx + t$ with a more general polynomial. The fully general problem remains an open one. Specifically, one could inquire about solutions $(s_0, s_1, \ldots, s_n) \in \mathbb{Z}^{n+1}$ to the equation

$$\mathrm{Res}_x\big(P(x), s_n x^n + \cdots + s_1 x + s_0\big) = a$$

where $a \in \mathbb{Z}$.

In chapter 2, we used some known results about Diophantine equations of the form $aX^2 - bY^4 = c$ with $c \in \{1, 2\}$ to bound the number of integral points to the elliptic curve $y^2 = px(Ax^2 + 2)$. This number is given with respect to the values of A and p modulo 8 when A is odd, and with respect to the values of A and p modulo 4 when A is even. This result successfully proves a conjecture of Togbé in seven cases of the possible sixteen and also improving the general bound for the number of solutions that he initially provided. This work has been expanded upon by Bencherif, Boumahdi, Garici, and Schedler, who considered the equation

$$y^2 = px(Ax^2 - C)$$

where $C \in \{2, \pm 1, \pm 4\}$.

In chapter 3, we discuss the equation $y^m = P(x)$ where m divides $\deg P$. We show that given sufficiently many appropriately long blocks of consecutive integers n such that $P(n)$ are

each of the form m^q, there is a polynomial R such that $P(x) = R(x)^q$. In effect, this shows that given a sufficiently long sequence of consecutive integers n such that $P(n) = m^q$, we can deduce the existence of infinitely many integral solutions to the equation $y^q = P(x)$ when q divides $\deg P$. The bound given is not effectively computable, which leads to a possible area of improvement. Additionally, one could consider the more challenging case where x^q is replaced simply by a polynomial $Q(x)$.

In chapter 4, the method of linear forms in logarithms is used to study the solutions to equations of the form $F_n \pm F_m = y^a$. Applying a variant of Baker-Davenport reduction, we completely solve the equation $F_n - F_m = y^a$ for $y \in \{6, 11, 12\}$. We also provide a bound for the solutions to the equation $F_n + F_m = y^a$ for fixed y. We make a remark. Our methods deal with only a single value of y at a time, and as such, we are unable to verify all cases of the conjecture of Erduvan and Keskin in this way. A different method which does not require fixing the value of y would be beneficial in approaching the problem.

In chapter 5, we refine a criterion of Carlitz and Lutz for identifying permutation polynomials. This allows one to characterize a polynomial over $\mathbb{F}_q$ as a permutation polynomial through the degrees of certain of its powers modulo $x^q - x$. The proof relies on a relationship between permutation polynomials and certain symmetric polynomials evaluated at the images of $\mathbb{F}_q$ induced by the polynomial. Since the study of permutation polynomials remains an active area of research, further improvements and refinements could provide tools to construct practical classes of these polynomials.

In chapter 6, we study the possibility of writing a rational function over a field K as the composition of two (or possibly more) rational functions of lesser degree. We build upon the work of Ayad, and subsequently of Kihel and L., who studied the problem over $\mathbb{C}$. Ayad chose to approach the problem through the valencies of a complex polynomial and through a polynomial generalizing its discriminant. Using an extended definition of the resultant, we approach the problem over K similarly. As discussed in that chapter, the more interesting examples which occur when the degree of the underlying rational function is divisible by the characteristic of the field are not covered. This would be an interesting topic for further research.

In chapters 7 and 8, we study the possibility of expressing a polynomial over a unique factorization domain as the composed product of two polynomials of lesser degree, focusing on the operations of composed addition and composed multiplication respectively. While consideration is made for commutative rings with unity, the primary focus lies in ring extensions of $\mathbb{Z}$. We use the results to construct some examples of polynomials over $\mathbb{Z}$ which are irreducible over $\mathbb{Q}$ but reducible over the finite field $\mathbb{F}_p$ for all primes p.

In chapter 9, we use the properties of binary quadratic forms to bound one of the least primes which splits in an imaginary quadratic field. The bound we find is not necessarily sharp, so

the result could potentially still be improved with further consideration.

In chapter 10, we expand upon the work of Werner, who studied the possibility of covering a ring by its proper subrings. We prove that the ring of p-adic integers is not coverable, that an Artinian ring which is a union of subrings of finite index is coverable, and we pose some questions regarding the possible covering of rings of integers which are not monogenic. These questions remain open, leaving room for further research.

Fairly consistent throughout this work was the appearance of the resultant. We have demonstrated some of its usefulness and interest, including generalizing composed products, constructing and solving a Diophantine equation, and perhaps most interestingly as a tool in the study of the decomposition of polynomials and rational function expressions. Note that the Bilu-Tichy theorem states that if the Diophantine equation $f(x) = g(y)$ has infinitely many solutions (x, y) where $f, g \in \mathbb{Q}[x]$, then f and g both belong to some special families of polynomials up to affine transformations. As such, it is of interest in Diophantine applications to determine if a given polynomial is the composition of other polynomials, and the resultant seems a good tool to naturally relate these concepts.