Effective Methods for Diophantine Equations

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van de Rector Magnificus Dr. D. D. Breimer,
hoogleraar in de faculteit der Wiskunde en
Natuurwetenschappen en die der Geneeskunde,
volgens besluit van het College voor Promoties
te verdedigen op donderdag 27 januari 2005
te klokke 14.15 uur

door

Szabolcs Tengely

geboren te Ózd (Hongarije)
op 13 januari 1976

Samenstelling van de promotiecommissie:

promotor:	Prof. dr. R. Tijdeman
referent:	Dr. L. Hajdu (Universiteit van Debrecen, Hongarije)
overige leden:	Prof. dr. F. Beukers (Universiteit Utrecht) Dr. J. H. Evertse Prof. dr. H. W. Lenstra jr. Prof. dr. P. Stevenhagen Prof. dr. S. M. Verduyn Lunel

Effective Methods for Diophantine Equations

Szabolcs Tengely

THOMAS STIELTJES INSTITUTE
FOR MATHEMATICS

Sok szeretettel édesapámnak, Sándornak és édesanyámnak, Irénnek.

Kölcsey Ferenc: Himnusz (1823)

Isten, áldd meg a magyart,
Jó kedvvel, bőséggel,
Nyújts feléje védő kart,
Ha küzd ellenséggel;
Bal sors akit régen tép,
Hozz rá víg esztendőt,
Megbűnhődte már e nép
A múltat s jövendőt!

Őseinket felhozád
Kárpát szent bércére,
Általad nyert szép hazát
Bendegúznak vére.
S merre zúgnak habjai
Tiszának, Dunának,
Árpád hős magzatjai
Felvirágozának.

Értünk Kunság mezein
Ért kalászt lengettél,
Tokaj szőlővesszein
Nektárt csepegtettél.
Zászlónk gyakran plántálád
Vad török sáncára,
S nyögte Mátyás bús hadát
Bécsnek büszke vára.

Hajh, de bűneink miatt
Gyúlt harag kebledben,
S elsújtád villamidat
Dörgő fellegedben,
Most rabló mongol nyilát
Zúgattad felettünk,
Majd töröktől rabigát
Vállainkra vettünk.

Hányszor zengett ajkain
Ozmán vad népének
Vert hadunk csonthalmain
Győzedelmi ének!
Hányszor támadt tenfiad
Szép hazám, kebledre,
S lettél magzatod miatt
Magzatod hamvvedre!

Bújt az üldözött s felé
Kard nyúl barlangjában,
Szert nézett, s nem lelé
Honját a hazában,
Bércre hág, és völgybe száll,
Bú s kétség mellette,
Vérözön lábainál,
S lángtenger felette.

Vár állott, most kőhalom;
Kedv s öröm röpkedtek,
Halálhörgés, siralom
Zajlik már helyettek.
S ah, szabadság nem virúl
A holtnak véréből,
Kínzó rabság könnye hull
Árvák hő szeméből!

Szánd meg, isten, a magyart
Kit vészek hányának,
Nyújts feléje védő kart
Tengerén kínjának.
Bal sors akit régen tép,
Hozz rá víg esztendőt,
Megbűnhődte már e nép
A múltat s jövendőt!

Contents

1 Introduction **1**

2 Runge-type Diophantine Equations **11**
2.1 Introduction 11
2.2 The case $F(x) = G(y)$ with $\gcd(\deg G, \deg F) > 1$ 13
2.2.1 Description of the algorithm 16
2.2.2 Examples 19

3 Exponential Diophantine Equations **25**
3.1 On the Diophantine equation $x^2 + a^2 = 2y^p$ 25
3.1.1 Equations of the form $x^2 + a^2 = 2y^p$ 26
3.1.2 Resolution of $x^2 + a^2 = by^p$ 36
3.1.3 Remark on the case of fixed p 38
3.2 On the Diophantine equation $x^2 + q^{2m} = 2y^p$ 39
3.2.1 A finiteness result 40
3.2.2 Fixed y 46
3.2.3 Fixed q 47

4 Mixed powers in arithmetic progressions **57**
4.1 Parametrization 58
4.2 The cases $(2, 2, 2, 3)$ and $(3, 2, 2, 2)$ 59
4.3 The cases $(2, 2, 3, 2)$ and $(2, 3, 2, 2)$ 61
4.4 The cases $(3, 2, 3, 2)$ and $(2, 3, 2, 3)$ 63

Bibliography **65**

Samenvatting **73**

Curriculum Vitae **74**

This thesis contains material from the following papers.

Chapter 2 is a modified version of

Sz. Tengely, *On the Diophantine equation* $F(x) = G(y)$,
Acta Arith., **110** (2003), 185-200.

Section 1 in Chapter 3 has, except for some minor modifications, appeared as

Sz. Tengely, *On the Diophantine equation* $x^2 + a^2 = 2y^p$,
Indag. Math. (N.S.), **15** (2004), 291-304.

Chapter 1

Introduction

In the thesis we shall solve Diophantine equations effectively by various methods, more precisely by Runge's method, Baker's method and Chabauty's method. To put our results in the proper context we summarize some of the relevant history.

A Diophantine equation is an equation of the form $f(x_1, x_2, \ldots, x_n) = 0$, where f is a given function and the unknowns $x_1, x_2, \ldots, x_n$ are required to be rational numbers or to be integers. As a generalisation of the concept one may consider rational or integral solutions over a number field. In the study of Diophantine equations there are some natural questions:

- Is the equation solvable?
- Is the number of solutions finite or infinite?
- Is it possible to determine all solutions?

Diophantus was a mathematician who lived in Alexandria around 300 A.D. Six Greek books out of thirteen of Diophantus' Arithmetica have been known for a long time. The most famous Latin translation is due to Bachet in 1621. In 1968 an Arabic manuscript was found in Iran, which is a translation from a Greek text written in Alexandria, but probable it was written by some of Diophantus' commentators. In his works he stated mathematical problems and provided rational solutions. To give an idea of the kind of problems we mention here two of them. The first problem is (problem 20 of book 4) to find four numbers such that the product of any two of them increased by 1 is a perfect square. A set with this property is called a (rational) Diophantine quadruple. The set with this property which Diophantus constructed

is $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. In fact

$$\begin{aligned}
\frac{1}{16}\cdot\frac{33}{16}+1 &= \left(\frac{17}{16}\right)^2,\\
\frac{1}{16}\cdot\frac{17}{4}+1 &= \left(\frac{9}{8}\right)^2,\\
\frac{1}{16}\cdot\frac{105}{16}+1 &= \left(\frac{19}{16}\right)^2,\\
\frac{33}{16}\cdot\frac{17}{4}+1 &= \left(\frac{25}{8}\right)^2,\\
\frac{33}{16}\cdot\frac{105}{16}+1 &= \left(\frac{61}{16}\right)^2,\\
\frac{17}{4}\cdot\frac{105}{16}+1 &= \left(\frac{43}{8}\right)^2.
\end{aligned}$$

The second problem is problem 17 of book 6 of the Arabic manuscript of Arithmetica which comes down to find positive rational solutions to $y^2 = x^6 + x^2 + 1$. Diophantus constructed the solution $x = \frac{1}{2}, y = \frac{9}{8}$.

Fermat's Last Theorem concerns the Diophantine equation

$$x^n + y^n = z^n.$$

Fermat (1601-1665) wrote in the margin of an edition of Diophantus' book that he had proved that there do not exist any positive integer solutions with $n > 2$. His proof was never found and in all likelyhood he did not have it. Using the method of descent, which was introduced by him, Fermat showed that the equation $x^4 + y^4 = z^2$ has no non-trivial solutions. An easy consequence is that Fermat's Last Theorem is true in case of $n = 4$. By means of the method of descent Fermat could solve several Diophantine problems. Fermat claimed that there cannot be four squares in arithmetic progression. If x^2, y^2, z^2, w^2 are consecutive terms of an arithmetic progression, then

$$\begin{aligned}
x^2 + z^2 &= 2y^2,\\
y^2 + w^2 &= 2z^2.
\end{aligned}$$

Besides Fermat found the Diophantine quadruple $\{1, 3, 8, 120\}$ consisting of integers.

Euler (1707-1783) proved Fermat's Last Theorem in case of $n = 3$, that is, he showed that the

equation $x^3+y^3=z^3$ has only trivial solutions. Euler conjectured that for every integer $n>2$, the sum of $n-1$ n-th powers of positive integers cannot be an n-th power. This conjecture is an extension of Fermat's Last Theorem, but it was disproved by Lander and Parkin [47] in 1966. They gave a counterexample,

$$27^5+84^5+110^5+133^5=144^5.$$

Elkies [37] in 1988 found the quartic counterexample

$$2682440^4+15365639^4+18796760^4=20615673^4.$$

Furthermore Euler showed that the only consecutive positive integers among squares and cubes are 8 and 9. That is, he solved the Diophantine equation

$$x^3-y^2=\pm 1,\quad x>0,y>0.$$

In 1844 Catalan conjectured that the Diophantine equation

$$x^m-y^n=1$$

admits only the solution $x=n=3,y=m=2$ in positive integers. So Euler had already solved the special case $m=3,n=2$.

Let

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

where $a_{i,j}\in\mathbb{Z}$ and $m>0,n>0$, which is irreducible in $\mathbb{Q}[X,Y]$. Let $\lambda>0$. Then the λ−leading part of P, $P_\lambda(X,Y)$, is the sum of all terms $a_{i,j}X^iY^j$ of P for which $i+\lambda j$ is maximal. The leading part of P, denoted by $\tilde{P}(X,Y)$, is the sum of all monomials of P which appear in any P_λ as λ varies. Then P satisfies Runge's condition unless there exists a λ so that $\tilde{P}=P_\lambda$ is a constant multiple of a power of an irreducible polynomial in $\mathbb{Q}[X,Y]$. One of the first general results on Diophantine equations is due to Runge [74] who proved the following theorem in 1887.

Theorem. *If P satisfies Runge's condition, then the Diophantine equation $P(x,y)=0$ has only a finite number of integer solutions.*

We present two examples for which the theorem implies the finiteness of integer solutions. The first example is given by

$$P(X,Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

where $P_\lambda(X,Y) = X^2, X^2 - Y^8, -Y^8$ according as $\lambda < \frac{1}{4}, \lambda = \frac{1}{4}, \lambda > \frac{1}{4}$, thus $\tilde{P}(X,Y) = X^2 - Y^8 = (X - Y^4)(X + Y^4)$. The second is

$$P(X,Y) = X(X+1)(X+2)(X+3) - Y(Y+1)\cdots(Y+5),$$

where we obtain that $\tilde{P}(X,Y) = X^4 - Y^6$.

Another general result was given by Thue [89] in 1909 who proved that if $F(X,Y)$ is an irreducible homogeneous polynomial of degree $n \geq 3$ with integer coefficients, and $m \neq 0$ is an integer, then the equation

$$F(x,y) = m \quad \text{in } x, y \in \mathbb{Z}$$

has only finitely many solutions. Siegel [78] in 1926 proved that the hyperelliptic equation

$$y^2 = a_0 x^n + a_1 x^{n-1} + \ldots + a_n =: f(x)$$

has only a finite number of integer solutions if f has at least three simple roots. The same method implies that the equation $y^m = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ with $m > 2$ has only a finite number of integer solutions. In 1929 Siegel [79] classified all irreducible algebraic curves over $\mathbb{Q}$ on which there are infinitely many integral points. These curves must be of genus 0 and have at most 2 infinite valuations. These results are ineffective, that is, their proofs do not provide any algorithm for finding the solutions.

In the 1960's Baker [6], [9] gave explicit lower bounds for linear forms in logarithms of the form

$$\Lambda = \sum_{i=1}^{n} b_i \log \alpha_i \neq 0,$$

where $b_i \in \mathbb{Z}$ for $i = 1, \ldots, n$ and $\alpha_1, \ldots, \alpha_n$ are algebraic numbers ($\neq 0, 1$), and $\log \alpha_i, \ldots, \log \alpha_n$ denote fixed determinations of the logarithms. Using his estimates Baker [7] gave an effective version of Thue's theorem. In [8], [10] he applied the method to the

class of Diophantine equations

$$f(x) = y^m \text{ in } x, y \in \mathbb{Z}, \tag{1.1}$$

where f is an irreducible polynomial of degree $n \geq 3$ with integer coefficients and $m \geq 2$ is a given integer. If $m = 2$, then equation (1.1) is called hyperelliptic equation, otherwise it is called superelliptic equation. Baker's method has been applied for many other types of Diophantine equations, see the papers by Bilu [15],[16], the survey by Győry [42] and the book by Smart [81] and the references given there. In practice Baker's method provides very large upper bounds for the unknowns of a given equation. In 1969 Baker and Davenport [11] proved that the only Diophantine quadruple of the form $\{1, 3, 8, x\}$ is $\{1, 3, 8, 120\}$, the one due to Fermat. They used Baker's method and a reduction algorithm based on continued fractions.

In 1976 Tijdeman [90] proved that Catalan's equation $x^p - y^q = 1$ has only finitely many solutions in integers $p > 1$, $q > 1$, $x > 1$, $y > 1$. He used a refinement of Baker's estimates for linear form in logarithms of algebraic numbers.

Schinzel and Tijdeman [76] in 1976 proved that if a polynomial $P(X)$ with rational coefficients has at least two distinct zeros then the equation $P(x) = y^m$, where $x, y \in \mathbb{Z}$ with $y \neq 0$, implies that $m < c(P)$ where $c(P)$ is a computable constant.

In 1982 Lenstra, Lenstra and Lovász [50] introduced the so-called LLL-basis reduction algorithm which enables one in many cases to reduce the high bounds found by applying Baker's method considerably. See de Weger [93].

In 1983 Faltings [38] proved the following result conjectured by Mordell.

Theorem. *Let K be a number field, and let C/K be a curve of genus $g \geq 2$. Then $C(K)$ is finite.*

It follows from this theorem that for every integer $n \geq 3$ the Fermat equation $x^n + y^n = z^n$ has only finitely many coprime solutions x, y, z.

In 1993 Wiles claimed to have a proof of a large part of the Taniyama-Shimura conjecture on the modularity of elliptic curves and thereby of Fermat's Last Theorem. His proof involved deep results on elliptic curves and modular forms. Some gap was found in the original proof but in 1995 Wiles and Taylor managed to nail it down and to complete the proof of Fermat's Last Theorem, see [94], [86].

In 1997 Darmon and Merel [34] proved following Wiles' approach that Denes' conjecture is true, that is there are no 3-term arithmetic progressions of equal powers greater than two.

A common generalisation of Fermat's equation and Catalan's equation is

$$Ax^r + By^s = Cz^t \tag{1.2}$$

in integers $r, s, t \in \mathbb{N}_{\geq 2}$, $x, y, z \in \mathbb{Z}$ and $A, B, C \in \mathbb{Z}$ given integers with $ABC \neq 0$. In 1995 Darmon and Granville [33] proved the following theorem.

Theorem. *Let $A, B, C \in \mathbb{Z}, ABC \neq 0$ and $r, s, t \in \mathbb{N}_{\geq 2}$ such that $1/r + 1/s + 1/t < 1$. Then the equation* (1.2) *has only finitely many solutions $x, y, z \in \mathbb{Z}$ with* $\gcd(x, y, z) = 1$.

If r, s, t are positive integers with $1/r + 1/s + 1/t > 1$, then there may exist infinitely many coprime integers x, y, z such that (1.2) holds. The following theorem is due to Beukers [13].

Theorem. *Let $A, B, C \in \mathbb{Z}, ABC \neq 0$ and $r, s, t \in \mathbb{N}_{\geq 2}$ such that $1/r + 1/s + 1/t > 1$. Then the equation* (1.2) *has either zero or infinitely many solutions $x, y, z \in \mathbb{Z}$ with* $\gcd(x, y, z) = 1$. *Moreover, there exists a finite set of triples $X, Y, Z \in \mathbb{Q}[U, V]$ with* $\gcd(X, Y, Z) = 1$ *and $AX^r + BY^s = CZ^t$ such that for every primitive integral solution (x, y, z) there is a triple (X, Y, Z) and $u, v \in \mathbb{Q}$ such that $x = X(u, v), y = Y(u, v), z = Z(u, v)$.*

Moreover Beukers [13] in Appendix A gives sets of parametrizations yielding all integer solutions in case of $A = B = C = 1$ for $\{p, q, r\} = \{2, 3, 3\}$ and $\{2, 3, 4\}$. These parametrizations were found by Zagier. Explicit parametrizations in case $x^2 + y^3 = z^5$ have been given by Edwards [36]. In case $1/r + 1/s + 1/t = 1$ we have $(r, s, t) = (3, 3, 3), (4, 4, 2)$ or $(2, 3, 6)$. In all three cases one has to study rational points on curves of genus 1. The following conjecture (also known as the Beal Prize Problem) was made by Tijdeman in a lecture on the Fermat Day in Utrecht in 1993.

Conjecture. *Let x, y, z, r, s, t be positive integers with $r, s, t > 2$. If $x^r + y^s = z^t$ then x, y, z have a factor in common.*

This conjecture was motivated by computations by Beukers and Zagier made for the same occasion. The known positive and primitive solutions to $x^r + y^s = z^t$ with $1/r + 1/s + 1/t < 1$

are as follows:

$$1^r + 2^3 = 3^2 \quad (r > 6),$$
$$2^5 + 7^2 = 3^4,$$
$$7^3 + 13^2 = 2^9,$$
$$2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2,$$
$$17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2,$$
$$33^8 + 1549034^2 = 15613^3.$$

They found the five large solutions. Note that always a square is involved.

Catalan's conjecture was resolved completely in 2002 by Mihăilescu [60]. In his proof he used results and tools from classical algebraic number theory, theory of cyclotomic fields, transcendental number theory and a Runge-type Diophantine argument. Thus 8 and 9 are the only consecutive positive powers indeed.

In the thesis we report on the following research. In Chapter 2 we consider the Runge-type Diophantine equation

$$F(x) = G(y), \tag{1.3}$$

where $F, G \in \mathbb{Z}[X]$ are monic polynomials of degree n and m respectively, such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X, Y]$ and $\gcd(n, m) > 1$. We present an upper bound for the size of the integer solutions to equation (1.3) in case $\gcd(n, m) > 1$. We further give an algorithm to find all integral solutions of equation (1.3). In Section 2.2.2 we make comparisons with previously published computational solutions of Diophantine equations by Runge's method. It turns out that in some cases our algorithm involves considerably fewer calculations. Our algorithm was implemented in Magma [21]. Some examples are given in Table 1.1.

In Chapter 3 exponential Diophantine equations (1.2) of the form $x^2 + a^2 = 2y^p$ are studied.

Equation	# Solutions	CPU time (sec)
$x^2 = y^8 + y^7 + y^2 + 3y - 5$	4	0.16
$x^3 = y^9 + 2y^8 - 5y^7 - 11y^6 - y^5 + 2y^4 + 7y^2 - 2y - 3$	1	0.75
$x^5 = y^{25} + y^{24} + \ldots + y + 7$	1	5.69
$x^2 = y^8 - 7y^7 - 2y^4 - y + 5$	0	4.79
$x^2 = y^4 - 99y^3 - 37y^2 - 51y + 100$	2	1.83
$x^2 - 3x + 5 = y^8 - y^7 + 9y^6 - 7y^5 + 4y^4 - y^3$	6	0.72
$x^3 - 5x^2 + 45x - 713 = y^9 - 3y^8 + 9y^7 - 17y^6 + 38y^5 - 199y^4 - 261y^3 + 789y^2 + 234y$	1	0.38
$x(x+1)(x+2)(x+3) = y(y+1)\cdots(y+5)$	28	0.23

Table 1.1: Results of a run of the procedure Runge.m on an AMD-Athlon 1 GHz PC.

In Section 1 (it is based on [88]) we provide a method to resolve the equation $x^2 + a^2 = 2y^n$ in integers $n > 2, x, y$ for any fixed a. In particular we compute all solutions of the equations $x^2 + a^2 = y^p$ and $x^2 + a^2 = 2y^p$ for odd a with $3 \leq a \leq 501$. In Section 2 we consider the Diophantine equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x, y are integer unknowns with $m > 0$, p and q are odd primes and $\gcd(x, y) = 1$. We prove that there are only finitely many solutions (m, p, q, x, y) for which y is not of the form $2v^2 \pm 2v + 1$. We also study the above equation with fixed y and with fixed q. We completely resolve the equation $x^2 + q^{2m} = 2 \cdot 17^p$. At the end of the section it is proved that if the Diophantine equation $x^2 + 3^{2m} = 2y^p$ with $m > 0$ and p prime admits a coprime integer solution (x, y), then either $p \in \{59, 83, 107, 179, 227, 347, 419, 443, 467, 563, 587, 659, 683, 827, 947\}$ or $(x, y, m, p) \in \{(79, 5, 1, 5), (545, 53, 3, 3)\}$.

In Chapter 4 some generalisations of Fermat's problem on arithmetic progressions of length 4 consisting of squares are discussed. All arithmetic progressions are described which satisfy one of the following conditions

$$\begin{aligned} &\text{four consecutive terms are of the form } x_0^2, x_1^2, x_2^2, x_3^3, \\ &\text{four consecutive terms are of the form } x_0^2, x_1^2, x_2^3, x_3^2, \\ &\text{four consecutive terms are of the form } x_0^3, x_1^2, x_2^3, x_3^2. \end{aligned} \tag{1.4}$$

In the first two cases we show that it is sufficient to find all rational points on certain hyperelliptic curves of genus 2 to obtain all progressions with $\gcd(x_0, x_1, x_2, x_3) = 1$. These hyperelliptic curves are given by

$$Y^2 = X^6 + 18X^5 + 75X^4 + 120X^3 + 120X^2 + 72X + 28,$$
$$Y^2 = X^6 - 6X^5 + 15X^4 + 40X^3 - 24X + 12.$$

In both cases the rank of the Jacobian is 1, therefore Chabauty's method can be applied. In the third case one can obtain a genus 2 curve without using any parametrisation, which enable us to get rid of the condition $\gcd(x_0, x_1, x_2, x_3) = 1$. The curve is given by

$$C : Y^2 = -X^6 + 2X^3 + 3.$$

We prove that $C(\mathbb{Q}) = \{(-1, 0), (1, \pm 2)\}$. These rational points gives rise to two families of progressions of the form $x_0^3, x_1^2, x_2^3, x_3^2$ given by

$$x_0 = -2t^2, x_1 = 0, x_2 = 2t^2, x_3 = \pm 4t^3 \text{ for some } t \in \mathbb{Z},$$
$$x_0 = t^2, x_1 = \pm t^3, x_2 = t^2, x_3 = \pm t^3 \text{ for some } t \in \mathbb{Z}.$$

It follows there are no increasing arithmetic progression of integers of the types (1.4).

Chapter 2

Runge-type Diophantine Equations

2.1 Introduction

Consider a polynomial

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

where $a_{i,j} \in \mathbb{Z}$ and $m > 0, n > 0$, which is irreducible in $\mathbb{Q}[X,Y]$. We recall Runge's result [74] on Diophantine equations:

if there are infinitely many $(x,y) \in \mathbb{Z}^2$ *such that* $P(x,y) = 0$ *then the following properties hold:*

- $a_{i,n} = a_{m,j} = 0$ *for all non-zero* i *and* j,
- *for every term* $a_{i,j}X^iY^j$ *of* P *one has* $ni + mj \leq mn$,
- *the sum of all monomials* $a_{i,j}X^iY^j$ *of* P *for which* $ni+mj = mn$ *is up to a constant factor a power of an irreducible polynomial in* $\mathbb{Z}[X,Y]$,
- *there is only one system of conjugate Puiseux expansions at* $x = \infty$ *for the algebraic function* $y = y(x)$ *defined by* $P(x,y) = 0$.

The latter two properties have been sharpened by Schinzel [75] and by Ayad [5]. The fourth property implies the three others. If the fourth statement does not hold, we say that P satisfies Runge's condition. Runge's method of proof is effective, that is, it yields computable upper bounds for the sizes of the integer solutions to these equations provided

Runge's condition is satisfied. Using this method upper bounds were obtained by Hilliker and Straus [45] and by Walsh [92]. Grytczuk and Schinzel [41] applied a method of Skolem [80] based on elimination theory to obtain upper bounds for the solutions. Laurent and Poulakis [48] obtained an effective version of Runge's theorem over number fields by interpolation determinants. Their result extends Walsh's result which holds for the field of rational numbers.

If $P(X,Y) = Y^n - R(X)$ is irreducible in $\mathbb{Q}[X,Y]$, R is monic and $\gcd(n, \deg R) > 1$, then P satisfies Runge's Condition. Masser [58] considered equation $y^n = R(x)$ in the special case $n = 2, \deg R = 4$, and Walsh [92] gave a bound for the general case. In [73] Poulakis described an elementary method for computing the solutions of the equation $y^2 = R(x)$, where R is a monic quartic polynomial which is not a perfect square. Szalay [84] generalized the result of Poulakis by giving an algorithm for solving the equation $y^2 = R(x)$ where R is a monic polynomial of even degree. Recently, Szalay [85] established a generalization to equations $y^p = R(x)$, where R is a monic polynomial and $p|\deg R$.

Several authors (for references see e.g.[14],[20],[35]) have studied the question if the equation $F(x) = G(y)$ has finitely or infinitely many solutions in $x, y \in \mathbb{Z}$, where F, G are polynomials with rational coefficients. Bilu and Tichy [20] completely classified those polynomials $F, G \in \mathbb{Q}[X]$ for which the equation $F(x) = G(y)$ has infinitely many integer solutions. The methods used in [14],[20],[35] are ineffective so they do not lead to algorithms to find all the solutions.

In this chapter we will prove the following theorem.

Theorem. *Let $F, G \in \mathbb{Z}[X]$ be monic polynomials with $\deg F = n \leq \deg G = m$, such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X,Y]$ and $\gcd(n,m) > 1$. Let $d > 1$ be a divisor of $\gcd(n,m)$. If $(x,y) \in \mathbb{Z}^2$ is a solution of the Diophantine equation $F(x) = G(y)$, then*

$$\max\{|x|, |y|\} \leq d^{\frac{2m^2}{d} - m}(m+1)^{\frac{3m}{2d}}\left(\frac{m}{d} + 1\right)^{\frac{3m}{2}}(h+1)^{\frac{m^2+mn+m}{d}+2m},$$

where $h = \max\{H(F), H(G)\}$ and $H(\cdot)$ denotes the classical height, that is the maximal absolute value of the coefficients.

We provide an algorithm to determine all the solutions, and show by examples how it works and compare the results with others on the same equations in the literature.

2.2 The case $F(x) = G(y)$ with $\gcd(\deg G, \deg F) > 1$

We deal with the Diophantine equation

$$F(x) = G(y), \tag{2.1}$$

where $F, G \in \mathbb{Z}[X]$ are monic polynomials with $\deg F = n, \deg G = m$, such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X, Y]$ and $\gcd(n, m) > 1$. Then Runge's condition is satisfied. Let $d > 1$ be a divisor of $\gcd(n, m)$. Without loss of generality we can assume $m \geq n$. By $H(\cdot)$ we denote the classical height, that is the maximal absolute value of the coefficients.
In the following theorem we extend a result of Walsh [92] concerning superelliptic equations for which Runge's condition is satisfied.

Theorem 2.2.1. *If $(x, y) \in \mathbb{Z}^2$ is a solution of* (2.1) *where F and G satisfy the above mentioned conditions then*

$$\max\{|x|, |y|\} \leq d^{\frac{2m^2}{d}-m}(m+1)^{\frac{3m}{2d}}\left(\frac{m}{d}+1\right)^{\frac{3m}{2}}(h+1)^{\frac{m^2+mn+m}{d}+2m},$$

where $h = \max\{H(F), H(G)\}$.

In the special case that $G(Y) = Y^m$ Walsh [92, Theorem 3] obtained a far better result for the integer solutions of (2.1), viz.

$$|x| \leq d^{2n-d}\left(\frac{n}{d}+2\right)^d (h+1)^{n+d}.$$

In the Corollary of Theorem 1 [92] Walsh has shown that if $P(X, Y)$ satisfies Runge's condition, then all integer solutions of the Diophantine equation $P(X, Y) = 0$ satisfy

$$\max\{|x|, |y|\} < (2m)^{18m^7} h^{12m^6},$$

where $m = \deg_Y P$, and $h = H(P)$. Grytczuk and Schinzel [41] have stated in their Corollary that if $P(X, Y)$ satisfies Runge's condition, then

$$\max\{|x|, |y|\} < \begin{cases} (45h)^{250} & \text{if } m = 2, \\ \left((4m^3)^{8m^2} h\right)^{96m^{11}} & \text{if } m > 2. \end{cases}$$

Here we cited corollaries from [41] and from [92] because it is easier to compare these results

with the Theorem. We note that in the special case (2.1) our theorem gives a far better upper bound.

We will need the concept of resultant. The resultant of two polynomials $f, g \in \mathbb{C}[X, Y]$ of degrees r, t in Y, respectively, say $f(X,Y) = a_0(X)Y^r + a_1(X)Y^{r-1} + \ldots + a_r(X)$ with $a_0(X) \not\equiv 0$ and $g(X,Y) = b_0(X)Y^t + b_1(X)Y^{t-1} + \ldots + b_t(X)$ with $b_0(X) \not\equiv 0$ is defined by

$$\mathrm{Res}_Y(f(X,Y), g(X,Y)) = \begin{vmatrix} a_0(X) & \ldots & \ldots & a_r(X) & & \\ & \ddots & & & \ddots & \\ & & a_0(X) & \ldots & \ldots & a_r(X) \\ b_0(X) & \ldots & b_t(X) & & & \\ & \ddots & & \ddots & & \\ & & \ddots & & \ddots & \\ & & & b_0(X) & \ldots & b_t(X) \end{vmatrix}$$

We use the following result in the proof of the Theorem.

Lemma 2.2.1. *There exist Puiseux expansions (in this case even Laurent expansions)*

$$u(X) = \sum_{i=-\frac{n}{d}}^{\infty} f_i X^{-i} \text{ and}$$
$$v(X) = \sum_{i=-\frac{m}{d}}^{\infty} g_i X^{-i}$$

of the algebraic functions U, V defined by $U^d = F(X), V^d = G(X)$, such that $d^{2(n/d+i)-1} f_i \in \mathbb{Z}$ for all $i > -\frac{n}{d}$, similarly $d^{2(m/d+i)-1} g_i \in \mathbb{Z}$ for all $i > -\frac{m}{d}$, and $f_{-\frac{n}{d}} = g_{-\frac{m}{d}} = 1$. Furthermore $|f_i| \le (H(F)+1)^{\frac{n}{d}+i+1}$ for $i \ge -\frac{n}{d}$ and $|g_i| \le (H(G)+1)^{\frac{m}{d}+i+1}$ for $i \ge -\frac{m}{d}$.

Proof. See [92] pp. 169-170. □

Proof of the Theorem. Let (2.1) admit a solution $(x, y) \in \mathbb{Z}^2$. Applying the lemma we write

$$F(X) = \left(\sum_{i=-\frac{n}{d}}^{\infty} f_i X^{-i} \right)^d, \quad G(Y) = \left(\sum_{i=-\frac{m}{d}}^{\infty} g_i Y^{-i} \right)^d,$$

where $|f_i|$ and $|g_i|$ are bounded by expressions given in the lemma. It follows from the lemma that $\left| \frac{d^{\frac{2m}{d}-1} f_k}{t^k} \right| < \frac{1}{2^{k+1}}$ for $|t| > 4d^{\frac{2m}{d}-1}(H(F)+1)^{\frac{n}{d}+2} =: x_0$. Thus we have $|\sum_{i=1}^{\infty} d^{\frac{2m}{d}-1} f_i t^{-i}| < \frac{1}{2}$. Similarly if $|t| > 4d^{\frac{2m}{d}-1}(H(G)+1)^{\frac{m}{d}+2} =: y_0$ then $|\sum_{i=1}^{\infty} d^{\frac{2m}{d}-1} g_i t^{-i}| < \frac{1}{2}$. Since $F(x) = G(y)$,

we have $u(x)^d - v(y)^d = 0$, that is

$$(u(x) - v(y))\left(u(x)^{d-1} + u(x)^{d-2}v(y) + \ldots + v(y)^{d-1}\right) = 0, \quad \text{if } d \text{ is odd,}$$
$$\left(u(x)^2 - v(y)^2\right)\left(u(x)^{d-2} + u(x)^{d-4}v(y)^2 + \ldots + v(y)^{d-2}\right) = 0, \quad \text{if } d \text{ is even.}$$

First assume that d is odd and

$$u(x)^{d-1} + u(x)^{d-2}v(y) + \ldots + v(y)^{d-1} = 0. \tag{2.2}$$

Suppose $v(y) \neq 0$. In this case we can divide (2.2) by $v(y)^{d-1}$, and we get

$$\left(\frac{u(x)}{v(y)}\right)^{d-1} + \left(\frac{u(x)}{v(y)}\right)^{d-2} + \ldots + \left(\frac{u(x)}{v(y)}\right) + 1 = 0.$$

It suffices to observe that $\frac{t^k-1}{t-1}$ has no real root if k is odd. Thus $v(y) = 0$ and $u(x) = 0$.

Now assume that d is even. Note that

$$u(x)^{d-2} + u(x)^{d-4}v(y)^2 + \ldots + v(y)^{d-2} = 0$$

can only happen if $u(x) = v(y) = 0$. By the above considerations we have

$$u(x) = v(y) \text{ if } d \text{ is odd, and}$$
$$u(x) = \pm v(y) \text{ if } d \text{ is even.}$$

Let $|x| > x_0, |y| > y_0$. Then we obtain from

$$0 = |u(x) \pm v(y)| = \left|\sum_{i=-\frac{n}{d}}^{\infty} f_i x^{-i} \pm \sum_{i=-\frac{m}{d}}^{\infty} g_i y^{-i}\right|$$

that

$$\left|\sum_{i=-\frac{n}{d}}^{0} d^{\frac{2m}{d}-1} f_i x^{-i} \pm \sum_{i=-\frac{m}{d}}^{0} d^{\frac{2m}{d}-1} g_i y^{-i}\right| < 1.$$

Since $d^{\frac{2m}{d}-1} f_i \in \mathbb{Z}$ for $i = -\frac{n}{d}, \ldots, 0$ and $d^{\frac{2m}{d}-1} g_i \in \mathbb{Z}$ for $i = -\frac{m}{d}, \ldots, 0$ we have

$$Q(x, y) := \sum_{i=0}^{\frac{n}{d}} d^{\frac{2m}{d}-1} f_{-i} x^i \pm \sum_{i=0}^{\frac{m}{d}} d^{\frac{2m}{d}-1} g_{-i} y^i = 0.$$

Hence x satisfies $\mathrm{Res}_Y(F(X) - G(Y), Q(X, Y)) = 0$ and y satisfies

$\mathrm{Res}_X(F(X) - G(Y), Q(X,Y)) = 0$. We note that these resultants are non-zero polynomials since $F(X) - G(Y)$ is irreducible over $\mathbb{Q}[X,Y]$ of degree n in X and of degree m in Y, whereas $\deg_X Q(X,Y) = \frac{n}{d}$, and $\deg_Y Q(X,Y) = \frac{m}{d}$. By applying Lemma 1 of Grytczuk and Schinzel [41] we obtain the following bounds for $|x|$ and $|y|$:

$$\begin{aligned} |x| &\leq \left(h(n+1)\sqrt{m+1}\right)^{\frac{m}{d}} \left(d^{\frac{2m}{d}-1}(h+1)^{\frac{n+m}{d}+2}(\frac{n}{d}+1)\sqrt{\frac{m}{d}+1}\right)^{m}, \\ |y| &\leq \left(h(m+1)\sqrt{n+1}\right)^{\frac{n}{d}} \left(d^{\frac{2m}{d}-1}(h+1)^{\frac{n+m}{d}+2}(\frac{m}{d}+1)\sqrt{\frac{n}{d}+1}\right)^{n}. \end{aligned} \tag{2.3}$$

By combining the bounds x_0, y_0 and (2.3) obtained for $|x|, |y|$ we get the bound given in the theorem. □

2.2.1 Description of the algorithm

In this section we give an algorithm to find all integral solutions of concrete Diophantine equations of the form (2.1) by adapting the proof of the theorem. Let p be the smallest prime divisor of $\gcd(m,n)$. Let $u(X) = \sum_{i=-\frac{n}{p}}^{0} f_i X^{-i}$ and $v(X) = \sum_{i=-\frac{m}{p}}^{0} g_i X^{-i}$ be the polynomial part of the Puiseux expansions at ∞ of $u(X)^p = F(X), v(X)^p = G(X)$, respectively, with $f_{-\frac{n}{p}} = g_{-\frac{m}{p}} = 1$. Denote by D the least common multiple of both the non-zero denominators of f_i for $i \in \{-\frac{n}{p}, \ldots, -1\}$ and of g_i for $i \in \{-\frac{m}{p}, \ldots, -1\}$ and of $f_0 - g_0$. Let t be a positive real number. The leading coefficients of $F(X) - (u(X) - t)^p$ and $F(X) - (u(X) + t)^p$ have opposite signs, similarly in the case of the polynomials $G(X) - (v(X) - t)^p$ and $G(X) - (v(X) + t)^p$. Hence we have that either

$$(u(x) - t)^p < F(x) < (u(x) + t)^p \text{ or } (u(x) + t)^p < F(x) < (u(x) - t)^p,$$

if $|x|$ is large enough. Similarly we have that either

$$(v(x) - t)^p < G(x) < (v(x) + t)^p \text{ or } (v(x) + t)^p < G(x) < (v(x) - t)^p,$$

if $|x|$ is large enough. We note that if $p \neq 2$, then the degree of the polynomials $F(X) - (u(X) - t)^p$ and $F(X) - (u(X) + t)^p$ is even, so only the case $(u(x) - t)^p < F(x) < (u(x) + t)^p$ occurs.

The same holds for $G(X) - (v(X) - t)^p$ and $G(X) - (v(X) + t)^p$. Let

$$\begin{aligned}
x_t^- &= \min\{\{0\} \cup \{x \in \mathbb{R} : F(x) - (u(x) - t)^p = 0 \text{ or } F(x) - (u(x) + t)^p = 0\}\},\\
x_t^+ &= \max\{\{0\} \cup \{x \in \mathbb{R} : F(x) - (u(x) - t)^p = 0 \text{ or } F(x) - (u(x) + t)^p = 0\}\},\\
y_t^- &= \min\{\{0\} \cup \{x \in \mathbb{R} : G(x) - (v(x) - t)^p = 0 \text{ or } G(x) - (v(x) + t)^p = 0\}\},\\
y_t^+ &= \max\{\{0\} \cup \{x \in \mathbb{R} : G(x) - (v(x) - t)^p = 0 \text{ or } G(x) - (v(x) + t)^p = 0\}\}.
\end{aligned}$$

Suppose that p is odd. Then we have

$$\begin{aligned}
(u(x) - t)^p < F(x) < (u(x) + t)^p \text{ for } x \notin [x_t^-, x_t^+],\\
(v(y) - t)^p < G(y) < (v(y) + t)^p \text{ for } y \notin [y_t^-, y_t^+].
\end{aligned}$$

If (x, y) is a solution (2.1) such that $x \notin [x_t^-, x_t^+]$ and $y \notin [y_t^-, y_t^+]$, then

$$(u(x) - t)^p - (v(y) + t)^p < F(x) - G(y) < (u(x) + t)^p - (v(y) - t)^p.$$

Thus

$$(u(x) - v(y) - 2t)\left(\sum_{k=0}^{p-1}(u(x) - t)^{p-1-k}(v(y) + t)^k\right) < 0, \tag{2.4}$$

$$(u(x) - v(y) + 2t)\left(\sum_{k=0}^{p-1}(u(x) + t)^{p-1-k}(v(y) - t)^k\right) > 0. \tag{2.5}$$

Either $u(x) - t \neq 0$ or $v(y) + t \neq 0$ since otherwise $u(x) - v(y) - 2t = 0$, a contradiction. Similarly, either $u(x) + t \neq 0$ or $v(y) - t \neq 0$ since otherwise $u(x) - v(y) + 2t = 0$, a contradiction. Without loss of generality we may assume that $v(x) - t \neq 0$ and $v(x) + t \neq 0$. We rewrite (2.4) and (2.5) as follows

$$\begin{aligned}
(u(x) - v(y) - 2t)\frac{1}{(v(y) + t)^{p-1}}\left(\sum_{k=0}^{p-1}\left(\frac{u(x) - t}{v(y) + t}\right)^k\right) < 0,\\
(u(x) - v(y) + 2t)\frac{1}{(v(y) - t)^{p-1}}\left(\sum_{k=0}^{p-1}\left(\frac{u(x) + t}{v(y) - t}\right)^k\right) > 0.
\end{aligned}$$

Since $p - 1$ is even and $\sum_{k=0}^{p-1} s^k \geq \frac{1}{2}$ for $s \in \mathbb{R}$ we obtain that

$$-2t < u(x) - v(y) < 2t.$$

There are only finitely many rational numbers with bounded denominator between $-2t$ and $2t$. It follows from Lemma 2.2.1 that the denominator of $u(x) - v(y)$ divides $p^{\frac{2m}{p}-1}$, so $D \mid p^{\frac{2m}{p}-1}$. Hence x is a solution of $\mathrm{Res}_Y(F(X) - G(Y), u(X) - v(Y) - T)$ for some rational number $-2t < T < 2t$ with denominator dividing D. To resolve a concrete equation of the form (2.1) it is sufficient to find all integral solutions of the following equations

$$\begin{aligned} &F(x) = G(k) \text{ for some } k \in [y_t^-, y_t^+], \\ &G(y) = F(k) \text{ for some } k \in [x_t^-, x_t^+], \\ &\mathrm{Res}_Y(F(X) - G(Y), u(X) - v(Y) - T) = 0 \text{ for some } T \in \mathbb{Q}, |T| < 2t \\ &\text{with denominator dividing } D. \end{aligned} \tag{2.6}$$

The number of equations to be solved depends on t, a good choice can reduce the time of the computation.

In the special case $p = 2$ if $n - n/d$ and $m - m/d$ are even, then the previous argument works. Otherwise four cases can occur.

1. $$(u(x) - t)^2 < F(x) < (u(x) + t)^2,$$
$$(v(y) - t)^2 < G(y) < (v(y) + t)^2.$$

   In this case it follows that $-2t < u(x) - v(y) < 2t$.

2. $$(u(x) - t)^2 < F(x) < (u(x) + t)^2,$$
$$(v(y) + t)^2 < G(y) < (v(y) - t)^2.$$

   We obtain that $-2t < u(x) + v(y) < 2t$.

3. $$(u(x) + t)^2 < F(x) < (u(x) - t)^2,$$
$$(v(y) - t)^2 < G(y) < (v(y) + t)^2.$$

   In this case we have that $-2t < u(x) + v(y) < 2t$.

4.

$$(u(x) + t)^2 < F(x) < (u(x) - t)^2,$$
$$(v(y) + t)^2 < G(y) < (v(y) - t)^2.$$

In this case it follows that $-2t < u(x) - v(y) < 2t$.

If $p = 2$ then we can apply the above arguments to conclude that each solution $(x, y) \in \mathbb{Z}^2$ of (2.1) satisfies at least one of the following equations:

$$\begin{aligned}
&F(x) = G(k) \text{ for some } k \in [y_t^-, y_t^+],\\
&G(y) = F(k) \text{ for some } k \in [x_t^-, x_t^+],\\
&\mathrm{Res}_Y(F(X) - G(Y), u(X) - v(Y) - T) = 0 \text{ for some } T \in \mathbb{Q}, |T| < 2t\\
&\text{with denominator dividing } D,\\
&\mathrm{Res}_Y(F(X) - G(Y), u(X) + v(Y) - T) = 0 \text{ for some } T \in \mathbb{Q}, |T| < 2t\\
&\text{with denominator dividing } D.
\end{aligned} \tag{2.7}$$

In the algorithm we need to compute the approximate values of the smallest real roots and the largest real roots of certain polynomials. One can apply for example the method of Collins and Akritas [32], based on Descartes' rule of signs, or Schönhage's algorithm [77], which is implemented in Magma [21]. Denote by NumofEq(t) the number of equations corresponding with t. It is $x_t^+ - x_t^- + y_t^+ - y_t^- + 4Dt + 1$ if p is odd and $x_t^+ - x_t^- + y_t^+ - y_t^- + 8Dt$ if $p = 2$. The remaining question is how we should fix the parameter t such that the number of equations to be solved becomes as small as possible. We perform a reduction algorithm as follows. We let $t = \frac{1}{2D}$. In this way if $x \notin [x_t^-, x_t^+], y \notin [y_t^-, y_t^+]$, we have that $-1 < D(u(x) \pm v(y)) < 1$. Since $D(u(x) \pm v(y))$ is an integer the only possibility is $u(x) \pm v(y) = 0$. In this case there is only one resultant equation to be solved if p is odd and two if $p = 2$. Then we compute NumofEq($2t$), if it is smaller than NumofEq(t), then we replace t by $2t$ and proceed, otherwise the procedure returns the actual values of $x_t^+, x_t^-, y_t^+, y_t^-, t$. Finally we compute the integer solutions of the polynomial equations (2.6) if p is odd, and (2.7) if $p = 2$.

2.2.2 Examples

I implemented the algorithm in the computer algebra program package Magma [21]. The program was run on an AMD-K7 550 MHz PC with 128 MB memory.

t	#equations	$[x_t^-, x_t^+, y_t^-, y_t^+]$
1/256	1278	[-350, 353, -253, 318]
1/128	628	[-174, 177, -98, 171]
1/64	311	[-86, 89, -24, 96]
1/32	195	[-42, 45, -20, 56]
1/16	158	[-20, 23, -16, 35]

Table 2.1: Information on the reduction.

Example 1. Consider the Diophantine equation

$$x^2 - 3x + 5 = y^8 - y^7 + 9y^6 - 7y^5 + 4y^4 - y^3.$$

We have

$$\begin{aligned} u(X) &= X - \frac{3}{2}, \\ v(Y) &= Y^4 - \frac{1}{2}Y^3 + \frac{35}{8}Y^2 - \frac{21}{16}Y - \frac{1053}{128}. \end{aligned}$$

In Table 2.1 we collect information on the reduction.

It remains to solve the following equations:

$$\begin{aligned} &\mathrm{Res}_Y(F(X) - G(Y), u(X) - v(Y) - k) = 0, \text{ for } k \in \{-15, \ldots, 15\}, \\ &\mathrm{Res}_Y(F(X) - G(Y), u(X) + v(Y) - k) = 0, \text{ for } k \in \{-15, \ldots, 15\}, \\ &G(y) = F(x), \text{ for } x \in \{-20, \ldots, 23\}, \\ &F(x) = G(y), \text{ for } y \in \{-16, \ldots, 35\}. \end{aligned}$$

The complete list of the integral solutions of these equations turns out to be:

$$\{(-657, 5), (-3, -1), (0, 1), (3, 1), (6, -1), (660, 5)\}.$$

Computation time in seconds: 0.72.

Example 2. We apply the method to the Diophantine equation

$$x^3 - 5x^2 + 45x - 713 = y^9 - 3y^8 + 9y^7 - 17y^6 + 38y^5 - 199y^4 - 261y^3 + 789y^2 + 234y.$$

t	#equations	$[x_t^-, x_t^+, y_t^-, y_t^+]$
1/6	177	[-86, 45, -32, 11]
1/3	95	[-48, 15, -18, 9]
2/3	67	[-27, 13, -10, 8]
4/3	52	[-16, 11, -2, 6]

Table 2.2: Information on the reduction.

We obtain that

$$u(X) = X - \frac{5}{3},$$
$$v(Y) = Y^3 - Y^2 + 2Y - \frac{4}{3}.$$

In Table 2.2 we collect information on the reduction.

In this case we solve the following equations:

$$\mathrm{Res}_Y(F(X) - G(Y), u(X) - v(Y) - k) = 0, \text{ for } k \in \{-7, \ldots, 7\},$$
$$G(y) = F(x), \text{ for } x \in \{-16, \ldots, 11\},$$
$$F(x) = G(y), \text{ for } y \in \{-2, \ldots, 6\},$$

The only integral solution of these equations is $(x, y) = (-11, -2)$.

Computation time in seconds: 0.38.

Example 3. ([43] Theorem 1. a) Consider the Diophantine equation

$$x(x+1)(x+2)(x+3) = y(y+1)\cdots(y+5).$$

There are many results in the literature concerning similar equations (cf. [14], [57]). We compute that

$$u(X) = X^2 + 3X + 1,$$
$$v(Y) = Y^3 + \frac{15}{2}Y^2 + \frac{115}{8}Y + \frac{75}{16}.$$

In Table 2.3 we collect information on the reduction.

t	#equations	$[x_t^-, x_t^+, y_t^-, y_t^+]$
1/32	108	[-6, 3, -50, 45]
1/16	62	[-5, 2, -26, 21]
1/8	46	[-4, 1, -15, 10]

Table 2.3: Information on the reduction.

It remains to solve the following equations:

$$\mathrm{Res}_Y(F(X) - G(Y), u(X) - v(Y) - k) = 0, \text{ for } k \in \{-3, \ldots, 3\},$$

$$\mathrm{Res}_Y(F(X) - G(Y), u(X) + v(Y) - k) = 0, \text{ for } k \in \{-3, \ldots, 3\},$$

$$G(y) = F(x), \text{ for } x \in \{-4, \ldots, 1\},$$

$$F(x) = G(y), \text{ for } y \in \{-15, \ldots, 10\}.$$

The complete list of non-trivial integral solutions of these equations turns out to be: $\{(-10,-7),(-10,2),(7,-7),(7,2)\}$. Computation time in seconds: 0.23.

The following examples are from [85]. The method described in that paper is similar to ours in the sense that one has to find all the integral solutions of polynomial equations $P(x) = 0$, where $P \in \mathbb{Z}[X]$. We compare both methods by comparing the number of equations which have to be solved. We remark that our algorithm works for equations $F(x) = G(y)$, where $F, G \in \mathbb{Z}[X]$ are monic polynomials with $\deg F = n, \deg G = m$, such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X, Y]$ and $\gcd(n, m) > 1$, while Szalay's algorithm can be applied only for the special case $G(y) = y^m$.

Equation 1. $x^2 = y^4 - 99y^3 - 37y^2 - 51y + 100$,

Equation 2. $x^2 = y^8 - 7y^7 - 2y^4 - y + 5$,

Equation 3. $x^2 = y^8 + y^7 + y^2 + 3y - 5$,

Equation 4. $x^3 = y^9 + 2y^8 - 5y^7 - 11y^6 - y^5 + 2y^4 + 7y^2 - 2y - 3$.

Equation 1	985360	5930
Equation 2	118546	1951
Equation 3	16	22
Equation 4	420	85

In the third column the numbers of equations to be solved by applying our method are stated,

and in the second column the numbers of equations to be solved by applying the method described in [85]. In all but the third case one has to solve fewer equations by using our algorithm.

Acknowledgement. I thank Robert Tijdeman and Jan-Hendrik Evertse for their valuable remarks and suggestions and Frits Beukers for his comments on the algorithm which led to a significant improvement.

Chapter 3

Exponential Diophantine Equations

3.1 On the Diophantine equation $x^2 + a^2 = 2y^p$

A common generalisation of Fermat's equation and Catalan's equation is

$$Ax^p + By^q = Cz^r$$

in integers $r, s, t \in \mathbb{N}_{\geq 2}$, $x, y, z \in \mathbb{Z}$ and $A, B, C \in \mathbb{Z}$ given integers with $ABC \neq 0$. Darmon and Granville [33] wrote down a parametrization for each case when $1/p + 1/q + 1/r > 1$ and $A = B = C = 1$. Beukers [13] showed that for any nonzero integers A, B, C, p, q, r for which $1/p + 1/q + 1/r > 1$ all solutions of $Ax^p + By^q = Cz^r$ can be obtained from a finite number of parametrized solutions. The theory of binary quadratic forms (see e.g. [61], Chapter 14) applies to the case $\{p, q, r\} = \{2, 2, k\}$ and a set of parametrizations can be found easily. We will make use of the fact, that in case of the title equation the parametrization is reducible.

It follows from Schinzel and Tijdeman [76] that for given non-zero integers A, B, C the equation $Ax^2 + B = Cy^n$ has only a finite number of integer solutions $x, y, n > 2$, which can be effectively determined. For special values of A, B and C this equation was investigated by several authors see e.g. [12], [28], [31], [46], [51], [53], [54],[67], [83] and the references given there.

There are many results concerning the more general Diophantine equation

$$Ax^2 + p_1^{z_1} \cdots p_s^{z_s} = Cy^n,$$

where p_i is prime for all i and z_i is an unknown non-negative integer, see e.g. [1], [64], [2], [65], [66], [4], [3], [22], [26], [30], [55], [56], [59], [63], [62], [70]. Here the elegant result of Bilu, Hanrot and Voutier [19] on the existence of primitive divisors of Lucas and Lehmer numbers has turned out to be a very powerful tool. In [70] Pink considered the equation $x^2 + (p_1^{z_1} \cdots p_s^{z_s})^2 = 2y^n$, and gave an explicit upper bound for n depending only on $\max p_i$ and s.

In [52] Ljunggren proved that if p is a given prime such that $p^2 - 1$ is exactly divisible by an odd power of 2, then the equation $x^2 + p^2 = y^n$ has only a finite number of solutions in x, y and n with $n > 1$. He provided a method to find all the solutions in this case.

The equation $x^2 + 1 = 2y^n$ was solved by Cohn [29]. Pink and Tengely [71] considered the title equation and they gave an upper bound for the exponent n depending only on a, and they completely resolved the equation with $1 \leq a \leq 1000$ and $3 \leq n \leq 80$. The theorems in the present section provide a method to resolve the equation $x^2 + a^2 = 2y^n$ in integers $n > 2, x, y$ for any fixed a. In particular we compute all solutions for odd a with $3 \leq a \leq 501$.

3.1.1 Equations of the form $x^2 + a^2 = 2y^p$

Consider the Diophantine equation

$$x^2 + a^2 = 2y^p, \tag{3.1}$$

where a is a given positive integer and $x, y \in \mathbb{N}$ such that $\gcd(x, y) = 1$ and $p \geq 3$ a prime. Put

$$\delta = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4, \\ -1 \text{ if } p \equiv 3 \pmod 4. \end{cases} \tag{3.2}$$

After having read the paper [71], Bugeaud suggested to use linear forms in only two logarithms in order to improve the bound for the exponent. Following this approach we get a far better bound than Pink and Tengely did in [71], that is, than $p < 2^{91}5^{27}a^{10}$.

Theorem 3.1.1. *If (x, y, p) is a solution of $x^2 + a^2 = 2y^p$ with $y > 50000$ then*

$$p \leq \max\{1.85 \log a, 4651\}.$$

Since $\mathbb{Z}[i]$ is a unique factorization domain, (3.1) implies the existence of integers u, v with

$y = u^2 + v^2$ such that

$$\begin{aligned} x &= \Re((1+i)(u+iv)^p) =: F_p(u,v), \\ a &= \Im((1+i)(u+iv)^p) =: G_p(u,v). \end{aligned}$$

Here F_p and G_p are homogeneous polynomials in $\mathbb{Z}[X,Y]$.

In the proof we will use the following result of Mignotte [19, Theorem A.1.3]. Let α be an algebraic number, whose minimal polynomial over $\mathbb{Z}$ is $A\prod_{i=1}^{d}(X-\alpha^{(i)})$. The absolute logarithmic height of α is defined by

$$h(\alpha) = \frac{1}{d}\left(\log|A| + \sum_{i=1}^{d}\log\max(1,|\alpha^{(i)}|)\right).$$

Lemma 3.1.1. *Let α be a complex algebraic number with $|\alpha| = 1$, but not a root of unity, and $\log\alpha$ the principal value of the logarithm. Put $D = [\mathbb{Q}(\alpha):\mathbb{Q}]/2$. Consider the linear form*

$$\Lambda = b_1 i\pi - b_2\log\alpha,$$

where b_1, b_2 are positive integers. Let λ be a real number satisfying $1.8 \le \lambda < 4$, and put

$$\begin{aligned} &\rho = e^{\lambda}, \quad K = 0.5\rho\pi + Dh(\alpha), \quad B = \max(13, b_1, b_2), \\ &t = \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1+2\pi\rho/3\lambda)}, \quad T = \left(\frac{1/3+\sqrt{1/9+2\lambda t}}{\lambda}\right)^2, \\ &H = \max\Big\{3\lambda, D\left(\log B + \log\left(\frac{1}{\pi\rho}+\frac{1}{2K}\right) - \log\sqrt{T} + 0.886\right) + \\ &+\frac{3\lambda}{2} + \frac{1}{T}\left(\frac{1}{6\rho\pi}+\frac{1}{3K}\right) + 0.023\Big\}. \end{aligned}$$

Then

$$\log|\Lambda| > -(8\pi T\rho\lambda^{-1}H^2 + 0.23)K - 2H - 2\log H + 0.5\lambda + 2\log\lambda - (D+2)\log 2.$$

We shall use the following statement in the proof of Theorem 3.1.1. The result can be found as Corollary 3.12 at p. 41 of [68].

Lemma 3.1.2. *If $\Theta = 2\pi r$ for some rational number r, then the only rational values of the tangent and the cotangent functions at Θ can be $0, \pm 1$.*

Proof of Theorem 3.1.1. Without loss of generality we assume that $p > 2000, y > 50000$, We

compute an upper bound for $|\frac{x+ai}{x-ai} - 1|$:

$$\left|\frac{x+ai}{x-ai} - 1\right| \leq \frac{\sqrt{2}a}{y^{p/2}}. \tag{3.3}$$

We have

$$\frac{x+ai}{x-ai} = \frac{(1+i)(u+iv)^p}{(1-i)(u-iv)^p} = i\frac{(u+iv)^p}{(u-iv)^p}.$$

If $\left|i\frac{(u+iv)^p}{(u-iv)^p} - 1\right| > \frac{1}{3}$ then $p \leq \frac{4\log 6}{\log 50000} < 2000$, a contradiction. Thus

$$\left|i\frac{(u+iv)^p}{(u-iv)^p} - 1\right| \leq \frac{1}{3}.$$

Since $|\log z| \leq 2|z-1|$ for $|z-1| \leq \frac{1}{3}$, we obtain

$$\left|i\frac{(u+iv)^p}{(u-iv)^p} - 1\right| \geq \frac{1}{2}\left|\log i\frac{(u+iv)^p}{(u-iv)^p}\right|.$$

Consider the corresponding linear form in two logarithms ($\pi i = \log(-1)$)

$$\Lambda = 2k\sigma\pi i - p\log\left(\delta\left(\frac{u-iv}{-v+iu}\right)^{\sigma}\right),$$

where logarithms have their principal values, $|2k| \leq p$ and $\sigma = \text{sign}(k)$. We apply Lemma 3.1.1 with $\alpha = \delta(\frac{u-iv}{-v+iu})^{\sigma}$, $b_1 = 2k\sigma$ and $b_2 = p$.

Suppose α is a root of unity. Then

$$\left(\frac{u-iv}{-v+iu}\right)^{\sigma} = \frac{-2uv}{u^2+v^2} + \frac{\sigma(-u^2+v^2)}{u^2+v^2}i = \exp\left(\frac{2\pi ij}{n}\right),$$

for some integers j, n with $0 \leq j \leq n-1$. Therefore

$$\tan\left(\frac{2\pi j}{n}\right) = \frac{\sigma(-u^2+v^2)}{-2uv} \in \mathbb{Q}.$$

Hence, by Lemma 3.1.2, $\frac{(u^2-v^2)}{2uv} \in \{0, 1, -1\}$. This implies that $uv = 0$ or $|u| = |v|$, but this is excluded by the requirement that the solutions x, y of (3.1) are relatively prime and that $y > 50000$. Therefore α is not a root of unity.

Note that α is irrational, $|\alpha| = 1$, and it is root of the polynomial $(u^2+v^2)X^2 + 4\delta uvX + (u^2+v^2)$.

Therefore $h(\alpha) = \frac{1}{2}\log y$. Set $\lambda = 1.8$. We have $D = 1$ and $B = p$ and

$$\begin{aligned} &14.91265 \leq K < 9.5028 + \frac{1}{2}\log y, \\ &0.008633 < t < 0.008634, \\ &0.155768 < T < 0.155769, \\ &H < \log p + 2.285949, \\ &\log y > 10.819778, \end{aligned} \tag{3.4}$$

By applying (3.3)-(3.4) and Lemma 3.1.1 we obtain

$$\log 2\sqrt{2}a - \frac{p}{2}\log y \geq \log|\Lambda| \geq -(13.16H^2 + 0.23)K - 2H - 2\log H - 0.004. \tag{3.5}$$

This yields by (3.4) an upper bound $C(a, y)$ for p depending only on a and y. If $y^p < a^{20}$, then $p < \frac{20}{\log y}\log a < 1.85\log a$, otherwise we obtain that

$$0.9p \leq 36.32\log(p)^2 + 166.39\log(p) + 0.37\log(\log(p) + 2.29) + 190.96.$$

Hence we conclude that $p \leq 4651$. Thus we obtain the bound $p \leq \max\{1.85\log a, 4651\}$. □

Theorem 3.1.2 gives us a tool to resolve Diophantine equations of type (3.1) for given a completely. We make use of the fact that the parametrization is reducible and one of the factors is linear. This linear factor, $u + \delta v$, is a divisor a_0 of a. If $u + \delta v \neq a$, then we have $p \mid a - a_0$, which provides a bound for p. This case is covered by the set S_1. In the remaining cases we deal with $u + \delta v = a$. The set S_2 contains solutions of $G_p(u, v) = a$ for which p is small. We need to consider these cases separately because the later arguments do not work for $p = 3, 5, 7$. To have a better bound for p we consider the equation $x^2 + a^2 = 2y^p$ for each $y < 50000$ separately. In all cases we obtain a bound for p and we test if $2y^p - a^2$ is a square or not for all primes p up to this bound. The set S_3 covers this case. It remains to deal with the "large" solutions, where $y = u^2 + v^2 \geq 50000$. If there is such a large solution (u, v) with $|v| > 1$ of $G_p(u, v) = a$, then $\frac{a}{v}$ is a convergent of $\beta + \delta$, where β is a root of $G_p(X, 1)$. Therefore we compute the convergents and check whether the numerator is a.

Theorem 3.1.2. *Let*

$$\mathcal{A}(C) = \bigcup_{p \le C} \left\{ \tan \frac{(4k+3)\pi}{4p} : 0 \le k \le p-1 \right\},$$

$$T = \begin{cases} \operatorname{lcm}(\operatorname{ord}_u(v), \operatorname{ord}_v(u)) \text{ if } \min\{|u|, |v|\} \ge 2, \\ \max\{|u|, |v|\} \text{ otherwise}, \end{cases}$$

and δ is defined by (3.2)*. If (x, y, p) is a solution of $x^2 + a^2 = 2y^p$ such that* $\gcd(x, y) = 1$*, then there exist integers u, v satisfying $(u, v, p) \in S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5$ where*

$$\begin{aligned}
S_1 &= \left\{(u,v,p) : u + \delta v = a_0, a_0 \ne a, a_0 | a, p | a - a_0, G_p(-\delta v + a_0, v) = a\right\}, \\
S_2 &= \left\{(u,v,p) : u + \delta v = a, p \in \{3,5,7\}, G_p(-\delta v + a, v) = a\right\}, \\
S_3 &= \Big\{(u,v,p) : u + \delta v = a, u^2 + v^2 \le 50000, 11 \le p \le C(a, u^2 + v^2), \\
&\quad p \equiv \pm 1 \bmod T\Big\}, \\
S_4 &= \Big\{(u,v,p) : u + \delta v = a, |u| > 223, |v| = 1, 11 \le p \le C(a, 50000), \\
&\quad p \equiv \pm 1 \bmod T\Big\}, \\
S_5 &= \Big\{(u,v,p) : u + \delta v = a, u^2 + v^2 > 50000, |v| \ge 2, 11 \le p \le C(a, 50000), \\
&\quad \frac{a}{v} \textit{ is a convergent of } \beta + \delta \textit{ for some } \beta \in \mathcal{A}(C(a, 50000))\Big\}.
\end{aligned}$$

To prove Theorem 3.1.2 we need the following lemmas.

Lemma 3.1.3. *If l is an odd positive integer, then*

$$\begin{aligned}
(u - \delta v) &\mid F_l(u, v), \\
(u + \delta v) &\mid G_l(u, v).
\end{aligned}$$

Proof. If $l \equiv 1 \pmod 4$ then

$$F_l(u, u) = \frac{u^l}{2}((1+i)^{l+1} + (1-i)^{l+1}) = 0,$$

and also

$$G_l(u, -u) = \frac{u^l}{2i}((1-i)^{l-1} - (1+i)^{l-1}) = 0.$$

The proof of the other case is similar. □

Lemma 3.1.4. *We have*

$$G_p(X,1) = \prod_{k=0}^{p-1}\left(X - \tan\frac{(4k+3)\pi}{4p}\right).$$

Proof. By definition $G_p(X,1) = \Im((1+i)(X+i)^p)$. We have

$$2i\left(\cos\frac{(4k+3)\pi}{4p}\right)^p G_p(\tan\frac{(4k+3)\pi}{4p},1) = \\ = i^p(1+i)(-1)^k\left(\exp\left(\frac{-3i\pi}{4}\right) - i\exp\left(\frac{3i\pi}{4}\right)\right) = 0.$$

Hence $G_p(\tan\frac{(4k+3)\pi}{4p},1) = 0$ for $0 \le k \le p-1$. Since $G_p(X,1)$ has degree p and G_p is monic, the lemma follows. □

Proof of Theorem 3.1.2. We have seen that $a = \Im((1+i)(u+iv)^p) =: G_p(u,v)$. Hence Lemma 3.1.3 implies that $u + \delta v | a$, that is, there exists an integer a_0 such that $a_0|a$ and $u + \delta v = a_0$. Define a function $s : \mathbb{N} \to \{\pm 1\}$ as follows:

$$s(k) = \begin{cases} 1 \text{ if } k \equiv 0,1 \pmod 4, \\ -1 \text{ if } k \equiv 2,3 \pmod 4. \end{cases}$$

It follows that

$$a = G_p(-\delta v + a_0, v) = \sum_{k=0}^{p} s(k)\binom{p}{k}(-\delta v + a_0)^{p-k}v^k,$$

hence

$$a \equiv (-\delta v + a_0)^p + \delta v^p \equiv a_0 \pmod p.$$

If $a_0 \neq a$ then it remains to solve the polynomial equations

$$G_p(-\delta v + a_0, v) = a, \qquad \text{for } a_0|a, a_0 \neq a \text{ and } p|a - a_0. \tag{3.6}$$

That is the first instance mentioned in Theorem 3.1.2.

From now on we assume that $a_0 = a = u + \delta v$. We claim $p \equiv \pm 1 \bmod T$. We note that

$$1 \equiv \frac{G_p(u,v)}{u+\delta v} \equiv u^{p-1} + (p-\delta)u^{p-2}v \bmod v^2,$$
$$1 \equiv \frac{G_p(u,v)}{u+\delta v} \equiv v^{p-1} + (p-\delta)v^{p-2}u \bmod u^2.$$

Suppose that $|u| = 1$. Then either $v = 0$ or $(p - \delta)v \equiv 0 \bmod v^2$, that is $p \equiv \delta \bmod v$ and the claim is proved. The case $|v| = 1$ is similar. Now assume that $\min\{|u|, |v|\} \geq 2$. In this case we obtain that

$$u^{p-1} \equiv 1 \bmod v,$$
$$v^{p-1} \equiv 1 \bmod u,$$

and therefore $\mathrm{ord}_v(u)|p - 1$ and $\mathrm{ord}_u(v)|p - 1$. Hence

$$T = \mathrm{lcm}(\mathrm{ord}_u(v), \mathrm{ord}_v(u))|p - 1.$$

If $y \leq 50000$ then we have $|u| \leq 224, |v| \leq 224$, therefore a belongs to the finite set $\{u + \delta v : |u| \leq 224, |v| \leq 224, u^2 + v^2 \leq 50000\}$. For all possible pairs (u, v) we have $p \leq C(a, u^2 + v^2)$ and $p \equiv \pm 1 \bmod T$. Thus $(u, v, p) \in S_3$.

Consider the case $y > 50000$. Let $\beta_i, i = 1, \ldots, p$ be the roots of the polynomial $G_p(X, 1)$, such that $\beta_1 < \beta_2 < \ldots < \beta_p$. Let $\gamma_i = u - \beta_i v$, and $\gamma_{i_1} = \min_i |\gamma_i|$. From Lemma 3.1.3 it follows that there is an index i_0 such that $|\beta_{i_0}| = 1$. From $G_p(u, v) = a$ we obtain

$$\prod_{\substack{i=1 \\ i \neq i_0}}^{p} (u - \beta_i v) = 1. \tag{3.7}$$

Using the mean-value theorem one can easily prove that

$$\left| \tan \frac{(4k_1 + 3)\pi}{4p} - \tan \frac{(4k_2 + 3)\pi}{4p} \right| \geq |k_1 - k_2| \frac{\pi}{p}.$$

Hence, by Lemma 3.1.4

$$|\gamma_i - \gamma_j| = |(\beta_i - \beta_j)v| \geq \frac{|i - j|\pi}{p} |v|.$$

If γ_{i_1} and γ_{i_1+k} have the same sign then we obtain that

$$|\gamma_{i_1+k}| \geq \frac{|k|\pi}{p} |v|,$$

otherwise

$$|\gamma_{i_1+k}| \geq \frac{(2|k| - 1)\pi}{2p} |v|.$$

Hence, from (3.7) we get

$$1 = \prod_{\substack{i=1 \\ i \neq i_0}}^{p} |u - \beta_i v| = \prod_{\substack{i=1 \\ i \neq i_0}}^{p} |\gamma_i| \geq (p-2)! |\gamma_{i_1}| \left(\frac{\pi |v|}{2p} \right)^{p-2}.$$

If $|\gamma_{i_1}| < \frac{1}{2|v|}$, then $|\frac{a}{v} - (\beta_{i_1} + \delta)| < \frac{1}{2v^2}$, hence $\frac{a}{v}$ is a convergent of $\beta_{i_1} + \delta$. If $|\gamma_{i_1}| \geq \frac{1}{2|v|}$, then

$$1 \geq \frac{1}{2|v|}(p-2)! \left(\frac{\pi |v|}{2p} \right)^{p-2} > \frac{\sqrt{2\pi}}{2|v|} \left(\frac{\pi (p-2)|v|}{2ep} \right)^{p-2}, \tag{3.8}$$

where we used the inequality $(p-2)! > \sqrt{2\pi}(\frac{p-2}{e})^{p-2}$. From (3.8) it follows that

$$|v| \leq \left(\frac{\sqrt{2}}{\sqrt{\pi}} \left(\frac{2e}{\pi} + \frac{4e}{\pi(p-2)} \right) \right)^{\frac{1}{p-3}} \left(\frac{2e}{\pi} + \frac{4e}{\pi(p-2)} \right),$$

it is easy to see that the right-hand side is a strictly decreasing function of p and that $|v| < 2$ for $p \geq 19$. We get the same conclusion for $p \in \{11, 13, 17\}$ from (3.8). Now, if $p \in \{3, 5, 7\}$, then it remains to solve $G_p(-\delta v + a, v) = a$. If $|v| < 2$, then we have to check only the cases $v = \pm 1$, because in case of $v = 0$ we do not obtain any relatively prime solution. Hence $(u, v, p) \in S_4$. If $|v| > 2$, then $|\gamma_{i_1}| < \frac{1}{2|v|}$, that is $\frac{a}{v}$ is a convergent of $\beta_{i_1} + \delta$. We conclude that $(u, v, p) \in S_5$, and the theorem is proved. □

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

We recall that Ljunggren proved that if a is a given prime such that $a^2 - 1$ is exactly divisible by an odd power of 2, then the equation $x^2 + a^2 = y^n$ has only a finite number of solutions in x, y and n with $n > 1$. He provided a method to find all the solutions in this case. We shall only require that $a \neq 0$. In this case we get the following parametrization

$$\begin{aligned} x &= \Re((u + iv)^p) =: f_p(u, v), \\ a &= \Im((u + iv)^p) =: g_p(u, v). \end{aligned}$$

Here f_p and g_p are homogeneous polynomials in $\mathbb{Z}[X, Y]$.

Theorem 3.1.3. *If (x, y, p) is a solution of $x^2 + a^2 = y^p$ with $y > 50000$ then*

$$p \leq \max\{1.85 \log a, 4651\}.$$

Proof. The proof goes in the same way as that of Theorem 3.1.1, so we indicate a few steps

only. Without loss of generality we assume that $p > 2000, y > 50000$. We have

$$\left|\frac{x+ai}{x-ai} - 1\right| \leq \frac{2a}{y^{p/2}} \tag{3.9}$$

Consider the corresponding linear form in two logarithms

$$\Lambda = 2k\sigma\pi i - p\log\left(\left(\frac{u-iv}{u+iv}\right)^{\sigma}\right),$$

the where logarithms have their principal values, $|2k| \leq p$ and $\sigma = \text{sign}(k)$. We apply Lemma 3.1.1 with $\alpha = \delta(\frac{u-iv}{u+iv})^{\sigma}, b_1 = 2k\sigma$ and $b_2 = p$. As in the proof of Theorem 3.1.1 we find that α is not a root of unity. It is a root of the polynomial $(u^2+v^2)X^2 - 2(u^2-v^2)X + (u^2+v^2)$. Therefore $h(\alpha) = \frac{1}{2}\log y$. Set $\lambda = 1.8$. We have $D = 1$ and $B = p$ and $K \leq 9.503 + \frac{1}{2}\log y$. By applying Lemma 3.1.1 we obtain

$$\log 4a - \frac{p}{2}\log y \geq \log|\Lambda| \geq -(13.16H^2 + 0.23)K - 2H - 2\log H - 0.004. \tag{3.10}$$

We have the bound (3.4) for H, this yields an upper bound $C_1(a,y)$ for p depending only on a and y which is decreasing with respect to y. If $y^p < a^{20}$, then $p < \frac{20}{\log y}\log a < 1.85\log a$, otherwise we obtain that

$$0.9p \leq 36.32\log(p)^2 + 166.39\log(p) + 0.37\log(\log(p) + 2.29) + 191.02.$$

From the above inequality we conclude that $p \leq 4651$. Thus we obtain the bound $p \leq \max\{1.85\log a, 4651\}$. □

Theorem 3.1.4. *If (x,y,p) is a solution of $x^2 + a^2 = y^p$ such that $\gcd(x,y) = 1, a \neq 0$, then there exist integers u, v satisfying $(u,v,p) \in S_1 \cup S_2 \cup S_3$ where*

$$\begin{aligned}
S_1 &= \left\{(u,v,p) : v = a_0, a_0 \neq \delta a, a_0|a, p|a - \delta a_0, g_p(u,a_0) = a\right\},\\
S_2 &= \left\{(u,v,p) : v = \delta a, u^2 + a^2 \leq 50000, 3 \leq p \leq C(a, u^2+a^2), a^{p-1} \equiv 1 \bmod u^2\right\},\\
S_3 &= \left\{(u,v,p) : v = \delta a, |u| \leq \cot\left(\frac{\pi}{p}\right)a + 1 \text{ and } 3 \leq p \leq C_1(a, 50000)\right\}.
\end{aligned}$$

We have similar lemmas as we applied to prove Theorem 3.1.2.

Lemma 3.1.5. *If l is an odd positive integer, then*

$$\begin{aligned} u &\mid f_l(u,v), \\ v &\mid g_l(u,v). \end{aligned}$$

Proof. By definition $g_l(u,v) = \Im((u+iv)^l) = \frac{(u+iv)^l-(u-iv)^l}{2i}$, therefore $g_l(u,0) = 0$. Similarly for f_p. □

Lemma 3.1.6. *We have*

$$g_p(X,1) = p\prod_{k=1}^{p-1}\left(X - \cot\frac{k\pi}{p}\right).$$

Proof. We have

$$2i\left(\sin\frac{k\pi}{p}\right)^p g_p(\cot\frac{k\pi}{p},1) = \exp(ik\pi) - \exp(-ik\pi) = 0.$$

Hence $g_p(\cot\frac{k\pi}{p},1) = 0$ for $1 \le k \le p-1$. □

In the proof of Theorem 3.1.1 it is clear from (3.7) that there exists an index j such that $|u - \beta_j v| \le 1$. Since $u + \delta v = a$ it follows that

$$|v| \le \frac{a+1}{|\beta_j + \delta|}.$$

The denominator can be quite small, therefore we do not get a useful bound for $|v|$. In the present case we are lucky, since we can use the equation

$$p\prod_{k=1}^{p-1}\left(u - \delta a\cot\frac{k\pi}{p}\right) = 1 \tag{3.11}$$

to get a bound for $|u|$ and resolve $x^2 + a^2 = y^p$ completely.

Proof of Theorem 3.1.4. From Lemma 3.1.5 we obtain that $v \mid a$, therefore there exists an integer a_0 such that $a_0 \mid a$ and $a_0 = v$. Thus

$$g_p(u,a_0) = a,$$

which implies that $p \mid a - \delta a_0$. If $a_0 \ne \delta a$ then we get $(u,v,p) \in S_1$. Consider the case $a_0 = \delta a$. If $y \le 50000$ then we have $u^2 + a^2 \le 50000$ and (3.10) provides a bound $C_1(a, u^2+a^2)$ for p. Now we prove the congruence condition on p using the equation $g_p(u,\delta a) = a$. Hence, by

$\delta^2 = 1$,

$$1 = a^{-1}g_p(u, \delta a) = \sum_{k=1}^{\frac{p+1}{2}} s(2k-1)\binom{p}{2k-1}u^{p-2k+1}\delta a^{2k-2}.$$

This implies that

$$s(p)\delta a^{p-1} \equiv 1 \bmod u^2.$$

Thus $(u, v, p) \in S_2$. If $y > 50000$ then from (3.10) we obtain that $p < C_1(a, 50000)$. By (3.11) there is an integer $1 \leq j \leq p-1$ such that $|u - \delta a \cot \frac{j\pi}{p}| < 1$. Hence

$$|u| < a \cot \frac{\pi}{p} + 1,$$

so $(u, v, p) \in S_3$. □

Remark. We note that the method that we apply in this paper works for some equations of the type

$$x^2 + a^2 = cy^p$$

with $a \neq 0, c \neq 1, 2$ an even integer, as well.

3.1.2 Resolution of $x^2 + a^2 = by^p$

Applying Theorem 3.1.2 we obtain the following result.

Corollary. *Let a be an odd integer with $3 \leq a \leq 501$. If $(x, y) \in \mathbb{N}^2$ is a positive solution of $x^2 + a^2 = 2y^p$ such that $x \geq a^2, \gcd(x, y) = 1$ then*

$$(a, x, y, p) \in \{(3, 79, 5, 5), (5, 99, 17, 3), (19, 5291, 241, 3), (71, 275561, 3361, 3)$$
$$(99, 27607, 725, 3), (265, 14325849, 46817, 3), (369, 1432283, 10085, 3)\}.$$

Proof. Finding the elements of the five sets in Theorem 3.1.2 provides the solutions of (3.1). We describe successively how to find the elements of these sets.

I. For a given a one has to resolve (3.6), that means several polynomial equations. One can perform this job either by factoring the polynomial or by testing the divisors of the constant term of the polynomial. Nowadays the computer algebra programs contain procedures to find all integral solutions of polynomial equations. We used Magma [21] to do so. The total CPU time for step I was about 44 minutes. For example when $a = 249$ then $a_0 \in \{-249, -83, -3, -1, 1, 3, 83\}$, therefore $p \in \{3, 5, 7, 31, 41, 83\}$. There is only one solution:

$(x, y, p) = (307, 5, 7)$. It took 0.4 sec to solve this case completely. In the list only the last solution is derived from this part.

II. The cases $p = 3$, $p = 5$ and $p = 7$. If $p = 3$ then we have only to solve quadratic equations of the form

$$6v^2 + 6av + a^2 - 1 = 0.$$

We obtained the following solutions indicated in the list
$(5, 99, 17, 3), (19, 5291, 241, 3), (71, 275561, 3361, 3), (265, 14325849, 46817, 3)$.
If $p = 5$ then we get the Thue equation

$$\frac{G_5(X, Y)}{X + Y} = X^4 + 4X^3Y - 14X^2Y^2 + 4XY^3 + Y^4 = 1$$

which has only the solutions $(\pm 1, \pm 2), (\pm 2, \pm 1), (\pm 1, 0), (0, \pm 1)$. Therefore the solutions of (3.1) with $p = 5$ and $u + v = a$ are given by $(a, x, y) \in \{(1, 1, 1), (3, 79, 5)\}$. If $p = 7$ then the corresponding Thue equation has only trivial solutions, hence the only solution of (3.1) with $p = 7, u - v = a$ is $(a, x, y) = (1, 1, 1)$. The total CPU time for step II was about 1.8 seconds.

III. If (u, v, p) belongs to S_3, then $|u| \leq 224$ and $|v| \leq 224$. Since we are interested only in relatively prime solutions of (3.1), we have to check only those pairs (u, v) for which $u + \delta v = a$, $\gcd(u, v) = 1, 2 \nmid u - v$ and $u^2 + v^2 \leq 50000$. For such a pair (u, v) one can compute T easily, and from (3.5) one gets $C(a, u^2 + v^2)$. So we obtain the set S_3. It remains to check which triples yield a solution of (3.1). To do so we compute $y = u^2 + v^2$ and we examine whether $2y^p - a^2$ is a square. This last step can be done efficiently, see [25], pp. 39-41. We used the appropriate procedure of Magma [21]. We did not obtain any solution in this case with $p \geq 11$. The total CPU time for step III was about 24.4 hours.

IV. In case of S_4 and S_5 we have a common bound for p which can be obtained from (3.5). It turns out that this bound is 4079. Since $v = \pm 1$ we have $y = a^2 \pm 2a + 2$. We check whether $2(a^2 \pm 2a + 2)^p - a^2$ is a square for all primes $p \leq 4079$, $p \equiv \pm 1 \bmod T$. There is no solution. The total CPU time was about 3.6 minutes.

V. To get S_5 we have to compute approximate values of some real numbers of the form

$$\tan \frac{(4k + 3)\pi}{4p}.$$

We note that we do not need very high precision, since the numerators of the convergents are bounded by a, in our case at most 501. We computed all convergents of the real numbers

contained in $\mathcal{A}(C(a, 50000))$ with numerator at most 501. From the triples (u, v, p) of S_5 we got the solutions of (3.1) as in the previous cases. For example, for $a = 501$ we obtained several convergents, one of them being

$$\frac{501}{45848} \approx 0.010927412319,$$

which is a convergent of

$$\tan \frac{(4 \cdot 993 + 3)\pi}{4 \cdot 4003} \approx 0.010927412156.$$

We did not get any solution of (3.1) from this part. The total CPU time for step IV was about 4.5 days. □

Applying Theorem 3.1.4 we obtain the following result in case y^p has coefficient 1.

Corollary. *Let a be an odd integer with $3 \leq a \leq 501$. If $(x, y) \in \mathbb{N}^2$ is a positive solution of $x^2 + a^2 = y^p$ such that $x \geq a^2, \gcd(x, y) = 1$ then*

$$(a, x, y, p) \in \{(7, 524, 65, 3), (97, 1405096, 12545, 3), (135, 140374, 2701, 3)\}.$$

3.1.3 Remark on the case of fixed p

Let $I(N)$ denote the set of odd integers less than or equal to N. To resolve (3.1) completely for a fixed prime p and $a \in I(N)$ an obvious method is to find all integral solution of the polynomial equations

$$G_p(-\delta v + a_0, v) = a, \quad \text{for } a_0 | a \text{ and } a_0 \equiv a \bmod p.$$

We will refer to this method as method I. Method II will mean that we solve the polynomial equations (3.6) and determine all integral solutions of the Thue equation

$$\frac{G_p(X, Y)}{X + \delta Y} = 1.$$

Solving Thue equations of high degree is a difficult task, but in certain cases it is possible (see [17],[18],[19],[44]). In the following table in the first row we indicate the run times needed to resolve (3.1) for $p = 5, 7$ and 11, and for odd integers $a \in \{1, \ldots, 5001\}$ using method I. The second row contains the run times in case of method II. We note that in case of $p = 3$

method II does not apply, since the degree of the polynomial $\frac{G_p(X,Y)}{X+\delta Y}$ is 2.

$1 \le a \le 5001$	$p = 5$	$p = 7$	$p = 11$
method I.	7.26 sec	52 sec	310 sec
method II.	3.34 sec	8.34 sec	100 sec

The complete lists of solutions in these cases are given by:

- $p = 5$:

$$(a,x,y) \in \{(3,79,5),(79,3,5),(475,719,13),(475,11767,37),(717,1525,17),$$
$$(2807,5757,29),(2879,3353,25),(3353,2879,25)\},$$

- $p = 7$:

$$(a,x,y) \in \{(249,307,5),(307,249,5),(2105,11003,13)\},$$

- $p = 11$:

$$(a,x,y) \in \{(3827,9111,5)\}.$$

3.2 On the Diophantine equation $x^2 + q^{2m} = 2y^p$

There are many results in the literature concerning the Diophantine equation

$$Ax^2 + p_1^{z_1} \cdots p_s^{z_s} = By^n,$$

where A, B are given non-zero integers, $p_1, \ldots, p_s$ are given primes and $n, x, y, z_1, \ldots, z_s$ are integer unknowns with $n > 2$, x and y coprime and non-negative, and $z_1, \ldots, z_s$ non-negative, see e.g. [1], [64], [2], [65], [66], [4], [3], [22], [26], [30], [55], [56], [59], [63], [62], [70]. Here the elegant result of Bilu, Hanrot and Voutier [19] on the existence of primitive divisors of Lucas and Lehmer numbers has turned out to be a very powerful tool. Using this result Luca [56] solved completely the Diophantine equation $x^2 + 2^a 3^b = y^n$. Le [49] obtained necessary conditions for the solutions of the equation $x^2 + p^2 = y^n$ in positive integers x, y, n with $\gcd(x, y) = 1$ and $n > 2$. He also determined all solutions of this equation for $p < 100$. In [70] Pink considered the equation $x^2 + (p_1^{z_1} \cdots p_s^{z_s})^2 = 2y^n$, and gave an explicit upper bound for n depending only on $\max p_i$ and s. The equation $x^2 + 1 = 2y^n$ was solved by Cohn [29]. Pink and Tengely [71] considered the equation $x^2 + a^2 = 2y^n$. They gave an upper bound for

the exponent n depending only on a, and completely resolved the equation with $1 \le a \le 1000$ and $3 \le n \le 80$. In the present section we study the equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x, y are integer unknowns with $m > 0$, p and q odd primes and x and y coprime. In Theorem 3.2.1 we show that all but finitely many solutions are of a special type. Theorem 3.2.2 provides bounds for p. Theorem 3.2.3 deals with the case of fixed y, Theorem 3.2.5 with the case of fixed q.

3.2.1 A finiteness result

Consider the Diophantine equation

$$x^2 + q^{2m} = 2y^p, \tag{3.12}$$

where $x, y \in \mathbb{N}$ with $\gcd(x, y) = 1, m \in \mathbb{N}$ and p, q are odd primes and $\mathbb{N}$ denotes the set of positive integers. Since the case $m = 0$ was solved by Cohn [29] (he proved that the equation has only the solution $x = y = 1$ in positive integers) we may assume without loss of generality that $m > 0$. If $q = 2$, then it follows from $m > 0$ that $\gcd(x, y) > 1$, therefore we may further assume that q is odd.

Theorem 3.2.1. *There are only finitely many solutions* (x, y, m, q, p) *of* (3.12) *with* $\gcd(x, y) = 1, x, y \in \mathbb{N}$, *such that* y *is not of the form* $2v^2 \pm 2v + 1, m \in \mathbb{N}$ *and* $p > 3, q$ *odd primes.*

Remark. The question of finiteness in case of $y = 2v^2 \pm 2v + 1$ is interesting. The following examples show that very large solutions can exist.

y	p	q
5	5	79
5	7	307
5	13	42641
5	29	1811852719
5	97	22993575370363230255945284717663 99
13	7	11003
13	13	13394159
13	101	22480363734265533023633690933103706711211958360218401 7999
25	11	69049993
25	47	37829305586052202725400160492 2967
41	31	40103338450160604152604 41

In these examples $m = 1$.

All solutions of (3.12) with small q^m have been determined in [88].

Lemma 3.2.1. *Let q be an odd prime and $m \in \mathbb{N} \cup \{0\}$ such that $3 \leq q^m \leq 501$. If there exist $(x, y) \in \mathbb{N}^2$ with $\gcd(x, y) = 1$ and an odd prime p such that (3.12) holds, then*

$$(x, y, q, m, p) \in \{(3, 5, 79, 1, 5), (9, 5, 13, 1, 3), (55, 13, 37, 1, 3), (79, 5, 3, 1, 5),$$
$$(99, 17, 5, 1, 3), (161, 25, 73, 1, 3), (249, 5, 307, 1, 7), (351, 41, 11, 2, 3),$$
$$(545, 53, 3, 3, 3), (649, 61, 181, 1, 3), (1665, 113, 337, 1, 3), (2431, 145, 433, 1, 3),$$
$$(5291, 241, 19, 1, 3), (275561, 3361, 71, 1, 3)\}.$$

Proof. This result follows from Corollary 1 in [88]. □

For $q^m > 501$ we shall derive a good bound for p by Baker's method.
We introduce some notation. Put

$$\delta_4 = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4, \\ -1 \text{ if } p \equiv 3 \pmod 4. \end{cases} \tag{3.13}$$

and

$$\delta_8 = \begin{cases} 1 \text{ if } p \equiv 1 \text{ or } 3 \pmod 8, \\ -1 \text{ if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases} \tag{3.14}$$

Since $\mathbb{Z}[i]$ is a unique factorization domain, (3.12) implies the existence of integers u, v with $y = u^2 + v^2$ such that

$$\begin{aligned} x &= \Re((1 + i)(u + iv)^p) =: F_p(u, v), \\ q^m &= \Im((1 + i)(u + iv)^p) =: G_p(u, v). \end{aligned} \tag{3.15}$$

Here F_p and G_p are homogeneous polynomials in $\mathbb{Z}[X, Y]$.

Lemma 3.2.2. *Let F_p, G_p be the polynomials defined by (3.15). We have*

$$\begin{aligned} (u - \delta_4 v) &\mid F_p(u, v), \\ (u + \delta_4 v) &\mid G_p(u, v). \end{aligned}$$

Proof. This is Lemma 3 in [88]. □

Lemma 3.2.2 and (3.15) imply that there exists a $k \in \{0, 1, \ldots, m\}$ such that either

$$\begin{aligned} u + \delta_4 v &= q^k, \\ H_p(u, v) &= q^{m-k}, \end{aligned} \tag{3.16}$$

or

$$\begin{aligned} u + \delta_4 v &= -q^k, \\ H_p(u, v) &= -q^{m-k}, \end{aligned} \tag{3.17}$$

where $H_p(u, v) = \frac{G_p(u,v)}{u+\delta_4 v}$.

For all solutions with large q^m we derive an upper bound for p in case of $k = m$ in (3.16) or (3.17) and in case of $q = p$.

Theorem 3.2.2. *If* (3.12) *admits a relatively prime solution* $(x, y) \in \mathbb{N}^2$ *then we have*

$$\begin{aligned} &p \leq 3803 \text{ if } u + \delta_4 v = \pm q^m, q^m \geq 503, \\ &p \leq 3089 \text{ if } p = q, \\ &p \leq 1309 \text{ if } u + \delta_4 v = \pm q^m, m \geq 40, \\ &p \leq 1093 \text{ if } u + \delta_4 v = \pm q^m, m \geq 100, \\ &p \leq 1009 \text{ if } u + \delta_4 v = \pm q^m, m \geq 250. \end{aligned}$$

We shall use the following lemmas in the proof of Theorem 3.2.2. The first result is due to Mignotte [19, Theorem A.1.3]. Let α be an algebraic number, whose minimal polynomial over $\mathbb{Z}$ is $A \prod_{i=1}^{d} (X - \alpha^{(i)})$. The absolute logarithmic height of α is defined by

$$h(\alpha) = \frac{1}{d} \left(\log |A| + \sum_{i=1}^{d} \log \max(1, |\alpha^{(i)}|) \right).$$

Lemma 3.2.3. *Let* α *be a complex algebraic number with* $|\alpha| = 1$, *but not a root of unity, and* $\log \alpha$ *the principal value of the logarithm. Put* $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]/2$. *Consider the linear form*

$$\Lambda = b_1 i\pi - b_2 \log \alpha,$$

where b_1, b_2 are positive integers. Let λ be a real number satisfying $1.8 \le \lambda < 4$, and put

$$\rho = e^{\lambda}, \quad K = 0.5\rho\pi + Dh(\alpha), \quad B = \max(13, b_1, b_2),$$
$$t = \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1 + 2\pi\rho/3\lambda)}, \quad T = \left(\frac{1/3 + \sqrt{1/9 + 2\lambda t}}{\lambda}\right)^2,$$
$$H = \max\Big\{3\lambda, D\left(\log B + \log\left(\frac{1}{\pi\rho} + \frac{1}{2K}\right) - \log\sqrt{T} + 0.886\right) +$$
$$+ \frac{3\lambda}{2} + \frac{1}{T}\left(\frac{1}{6\rho\pi} + \frac{1}{3K}\right) + 0.023\Big\}.$$

Then

$$\log|\Lambda| > -(8\pi T\rho\lambda^{-1}H^2 + 0.23)K - 2H - 2\log H + 0.5\lambda + 2\log\lambda - (D+2)\log 2.$$

The next result can be found as Corollary 3.12 at p. 41 of [68].

Lemma 3.2.4. *If $\Theta \in 2\pi\mathbb{Q}$, then the only rational values of the tangent and the cotangent functions at Θ can be $0, \pm 1$.*

Proof of Theorem 3.2.2. Without loss of generality we assume that $p > 1000$ and $q^m \ge 503$. We give the proof of Theorem 3.2.2 in the case $u + \delta_4 v = \pm q^m, q^m \ge 503$, the proofs of the remaining four cases being analogous. From $u + \delta_4 v = \pm q^m$ we get

$$\frac{503}{2} \le \frac{q^m}{2} \le \frac{|u| + |v|}{2} \le \sqrt{\frac{u^2 + v^2}{2}} = \sqrt{\frac{y}{2}},$$

which yields that $y \ge \frac{q^{2m}}{2} > 126504$. Hence

$$\left|\frac{x + q^m i}{x - q^m i} - 1\right| = \frac{2 \cdot q^m}{\sqrt{x^2 + q^{2m}}} \le \frac{2\sqrt{y}}{y^{p/2}} = \frac{2}{y^{\frac{p-1}{2}}}. \tag{3.18}$$

We have

$$\frac{x + q^m i}{x - q^m i} = \frac{(1+i)(u+iv)^p}{(1-i)(u-iv)^p} = i\left(\frac{u+iv}{u-iv}\right)^p. \tag{3.19}$$

If $\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| > \frac{1}{3}$ then $6 > y^{\frac{p-1}{2}}$, which yields a contradiction with $p > 1000$ and $y > 126504$. Thus $\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| \le \frac{1}{3}$. Since $|\log z| \le 2|z-1|$ for $|z-1| \le \frac{1}{3}$, we obtain

$$\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| \ge \frac{1}{2}\left|\log i\left(\frac{u+iv}{u-iv}\right)^p\right|. \tag{3.20}$$

Suppose first that $\alpha := \delta_4 \left(\frac{u-iv}{-v+iu}\right)^\sigma$ is a root of unity for some $\sigma \in \{-1, 1\}$. Then

$$\left(\frac{u-iv}{-v+iu}\right)^\sigma = \frac{-2uv}{u^2+v^2} + \frac{\sigma(-u^2+v^2)}{u^2+v^2}i = \pm\alpha = \exp\left(\frac{2\pi i j}{n}\right),$$

for some integers j, n with $0 \le j \le n-1$. Therefore

$$\tan\left(\frac{2\pi j}{n}\right) = \frac{\sigma(-u^2+v^2)}{-2uv} \in \mathbb{Q} \text{ or } (u,v) = (0,0).$$

The latter case is excluded. Hence, by Lemma 3.2.4, $\frac{u^2-v^2}{2uv} \in \{0, 1, -1\}$. This implies that $|u| = |v|$, but this is excluded by the requirement that the solutions x, y of (3.12) are relatively prime, but $y > 126504$. Therefore α is not a root of unity.

Note that α is irrational, $|\alpha| = 1$, and it is a root of the polynomial $(u^2+v^2)X^2 + 4\delta_4 uvX + (u^2+v^2)$. Therefore $h(\alpha) = \frac{1}{2}\log y$.

Choose $l \in \mathbb{Z}$ such that $|p\log(i^{\delta_4}\frac{u+iv}{u-iv}) + 2l\pi i|$ is minimal, where logarithms have their principal values. Then $|2l| \le p$. Consider the linear form in two logarithms ($\pi i = \log(-1)$)

$$\Lambda = 2|l|\pi i - p\log\alpha. \tag{3.21}$$

If $l = 0$ then by Liouville's inequality and Lemma 1 of [91],

$$|\Lambda| \ge |p\log\alpha| \ge |\log\alpha| \ge 2^{-2}\exp(-2h(\alpha)) \ge \exp(-8(\log 6)^3 h(\alpha)). \tag{3.22}$$

From (3.18) and (3.22) we obtain

$$\log 4 - \frac{p-1}{2}\log y \ge \log|\Lambda| \ge -4(\log 6)^3 \log y.$$

Hence $p \le 47$. Thus we may assume without loss of generality that $l \ne 0$.

We apply Lemma 3.2.3 with $\sigma = \text{sign}(l), \alpha = \delta_4(\frac{u-iv}{-v+iu})^\sigma, b_1 = 2|l|$ and $b_2 = p$. Set $\lambda = 1.8$. We have $D = 1$ and $B = p$. By applying (3.18)-(3.21) and Lemma 3.2.3 we obtain

$$\log 4 - \frac{p-1}{2}\log y \ge \log|\Lambda| \ge -(13.16H^2 + 0.23)K - 2H - 2\log H - 0.004.$$

We have

$$15.37677 \le K < 9.5028 + \frac{1}{2}\log y,$$
$$0.008633 < t < 0.008634,$$
$$0.155768 < T < 0.155769,$$
$$H < \log p + 2.270616,$$
$$\log y > 11.74803,$$

From the above inequalities we conclude that $p \le 3803$. □

The following lemma gives a more precise description of the polynomial H_p.

Lemma 3.2.5. *The polynomial $H_p(\pm q^k - \delta_4 v, v)$ has degree $p-1$ and*

$$H_p(\pm q^k - \delta_4 v, v) = \pm\delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^k p\widehat{H}_p(v) + q^{k(p-1)},$$

where $\widehat{H}_p \in \mathbb{Z}[X]$ has degree $< p-1$. The polynomial $H_p(X,1) \in \mathbb{Z}[X]$ is irreducible and

$$H_p(X,1) = \prod_{\substack{k=0\\k\neq k_0}}^{p-1}\left(X - \tan\frac{(4k+3)\pi}{4p}\right),$$

where $k_0 = \left\lfloor \frac{p}{4} \right\rfloor (p \mod 4)$.

Proof. By definition we have

$$H_p(u,v) = \frac{G_p(u,v)}{u+\delta_4 v} = \frac{(1+i)(u+iv)^p - (1-i)(u-iv)^p}{2i(u+\delta_4 v)}. \tag{3.23}$$

Hence

$$H_p(\pm q^k - \delta_4 v, v) = \frac{(1+i)(\pm q^k + (i-\delta_4)v)^p - (1-i)(\pm q^k + (-i-\delta_4)v)^p}{\pm 2iq^k}.$$

Therefore the coefficient of v^p is $(1+i)(-\delta_4+i)^p + (1-i)(\delta_4+i)^p$. If $\delta_4 = 1$, then it equals $-2(-1+i)^{p-1} + 2(1+i)^{p-1} = -2(-4)^{\frac{p-1}{4}} + 2(-4)^{\frac{p-1}{4}} = 0$, since $p \equiv 1 \pmod 4$. If $\delta_4 = -1$, then it equals $(1+i)^{p+1} - (-1+i)^{p+1} = (-4)^{\frac{p+1}{4}} - (-4)^{\frac{p+1}{4}} = 0$. Similarly the coefficient of v^{p-1} is $\pm\frac{(1+i)(\delta_4-i)^{p-1} - (1-i)(\delta_4+i)^{p-1}}{2i} p = \pm\delta_8 2^{\frac{p-1}{2}} p$. It is easy to see that the constant is $q^{k(p-1)}$. The coefficient of v^t for $t = 1, \ldots, p-2$ is $\pm\binom{p}{t}(q^k)^{p-t-1}c_t$, where c_t is a power of 2. The irreducibility of $H_p(X,1)$ follows from the fact that $H_p(X-\delta_4, 1)$ satisfies Eisenstein's

irreducibility criterion. The last statement of the lemma is a direct consequence of Lemma 4 from [88]. □

Lemma 3.2.6. *If there exists a* $k \in \{0, 1, \ldots, m\}$ *such that* (3.16) *or* (3.17) *has a solution* $(u, v) \in \mathbb{Z}^2$ *with* $\gcd(u, v) = 1$*, then either* $k = 0$ *or* $k = m$*,* $p \neq q$ *or* $(k = m - 1, p = q)$.

Proof. Suppose $0 < k < m$. It follows from Lemma 3.2.5 that q divides $\pm\delta_8 2^{\frac{p-1}{2}} p v^{p-1}$. If $q \neq p$, we obtain that $q \mid v$ and $q \mid u$, which is a contradiction with $\gcd(u, v) = 1$. Thus $k = 0$ or $k = m$. If $p = q$, then from Lemma 3.2.5 and (3.16),(3.17) we get

$$\pm\delta_8 2^{\frac{p-1}{2}} v^{p-1} + p^k \widehat{H}_p(v) + p^{k(p-1)-1} = \pm p^{m-k-1}.$$

Therefore $k = 0$ or $k = m - 1$. □

Now we are in the position to prove Theorem 3.2.1.

Proof of Theorem 3.2.1. By Lemma 3.2.6 we have that $k = 0, m - 1$ or $k = m$. If $k = 0$, then $u + \delta_4 v = \pm 1$ and $y = 2v^2 \pm 2v + 1$. If $k = m - 1$, then $p = q$. Hence $u + \delta_4 v = \pm p^{m-1}$ which implies that $y \geq \frac{p^{2(m-1)}}{2} \geq \frac{p^2}{2}$. From Theorem 3.2.2 we obtain that $p \leq 3089$. We recall that $H_p(u, v)$ is an irreducible polynomial of degree $p - 1$. Thus we have only finitely many Thue equations (if $p > 3$)

$$H_p(u, v) = \pm p.$$

By a result of Thue [89] we know that for each p there are only finitely many integer solutions, which proves the statement.

Let $k = m$. Here we have $u + \delta_4 v = \pm q^m$ and $H_p(\pm q^m - \delta_4 v, v) = \pm 1$. If $q^m \leq 501$ then there are only finitely many solutions which are given in Lemma 3.2.1. We have computed an upper bound for p in Lemma 3.2.2 when $q^m \geq 503$. This leads to finitely many Thue equations

$$H_p(u, v) = \pm 1.$$

From Thue's result [89] follows that there are only finitely many integral solutions (u, v) for any fixed p, which implies the remaining part of the theorem. □

3.2.2 Fixed y

First we consider (3.12) with given y which is not of the form $2v^2 \pm 2v + 1$. Since $y = u^2 + v^2$ there are only finitely many possible pairs $(u, v) \in \mathbb{Z}^2$. Among these pairs we have to select

those for which $u \pm v = \pm q^{m_0}$, for some prime q and for some integer m_0. Thus there are only finitely many pairs (q, m_0). The method of [88] makes it possible to compute (at least for moderate q and m_0) all solutions of $x^2 + q^{2m_0} = 2y^p$ even without knowing y. Let us consider the concrete example $y = 17$.

Theorem 3.2.3. *The only solution (m, p, q, x) in positive integers m, p, q, x with p and q odd primes of the equation $x^2 + q^{2m} = 2 \cdot 17^p$ is $(1, 3, 5, 99)$.*

Proof. Note that 17 is not of the form $2v^2 \pm 2v + 1$. From $y = u^2 + v^2$ we obtain that q is 3 or 5 and $m = 1$. This implies that 17 does not divide x. We are left with the equations

$$x^2 + 3^2 = 2 \cdot 17^p,$$
$$x^2 + 5^2 = 2 \cdot 17^p.$$

From Lemma 3.2.1 we see that there is no solution with $q = 3, m = 1, y = 17$ and the only solution in case of the second equation is $(x, y, q, m, p) = (99, 17, 5, 1, 3)$. □

3.2.3 Fixed q

If m is small, then one can apply the method of [88] to obtain all solutions. Theorem 3.2.2 provides an upper bound for p in case $u + \delta_4 v = \pm q^m$. Therefore it is sufficient to resolve the Thue equations

$$H_p(u, v) = 1$$

for primes less than the bound. In practice this is a difficult job but in some special cases there exist methods which work, see [17], [18], [19], [44]. Lemma 3.2.7 shows that we have a cyclotomic field in the background just as in [19]. Probably the result of the following lemma is in the literature, but we have not found a reference. We thank Prof. Stevenhagen for the short proof.

Lemma 3.2.7. *For any positive integer M denote by ζ_M a primitive Mth root of unity. If α is a root of $H_p(X, 1)$ for some odd prime p, then $\mathbb{Q}(\zeta_p + \overline{\zeta}_p) \subset \mathbb{Q}(\alpha) \cong \mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p})$.*

Proof. Since $\tan z = \frac{1}{i} \frac{\exp(iz) - \exp(-iz)}{\exp(iz) + \exp(-iz)}$, we can write $\alpha = \tan(\frac{(4k+3)\pi}{4p})$ as

$$\frac{1}{i} \frac{\zeta_{8p}^{4k+3} - \zeta_{8p}^{-4k-3}}{\zeta_{8p}^{4k+3} + \zeta_{8p}^{-4k-3}} = -\zeta_4 \frac{\zeta_{4p}^{4k+3} - 1}{\zeta_{4p}^{4k+3} + 1} \in \mathbb{Q}(\zeta_{4p}).$$

Since it is invariant under complex conjugation, α is an element of $\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p})$. We also know that $[\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = p - 1$, thus $\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p}) \cong \mathbb{Q}(\alpha)$. The claimed inclusion follows from the fact that $\zeta_p + \overline{\zeta}_p$ can be expressed easily in terms of $\zeta_{4p} + \overline{\zeta}_{4p}$. □

It is important to remark that the Thue equations $H_p(u, v) = \pm 1$ do not depend on q. Therefore after resolving them it becomes easier to resolve equation (3.12). By combining the methods of composite fields [18] and non-fundamental units [44] for Thue equations we may rule out some cases completely. If the method applies it remains to consider the cases $u + \delta_4 v = \pm 1$ and $p = q$. The problem is that the bound for p is still large, and the computation may take several months. One possibility to improve the bound is applying the method of [88] and resolve equation (3.12) for values of q^m larger than 501, but this is more and more time consuming as q^m increases. If q is fixed one can follow a strategy to eliminate large primes p. Here we use the fact that when considering the Thue equation

$$H_p(q^m - \delta_4 v, v) = 1, \tag{3.24}$$

we are looking for integer solutions (u, v) for which $u + \delta_4 v$ is a power of q. Let w be a positive integer relatively prime to q, then the set $S(q, w) = \{q^m \mod w : m \in \mathbb{N}\}$ has $\mathrm{ord}_w(q)$ elements. Let

$$L(p, q, w) = \\ \left\{ s \in \{0, 1, \ldots, \mathrm{ord}_w(q)\} : H_p(q^s - \delta_4 v, v) = 1 \text{ has a solution modulo } w \right\}.$$

We search for numbers $w_1, \ldots, w_N$ such that $\mathrm{ord}_{w_1}(q) = \ldots = \mathrm{ord}_{w_N}(q) =: w$, say. Then

$$m_0 \mod w \in L(p, q, w_1) \cap \ldots \cap L(p, q, w_N),$$

where $m_0 \mod w$ denotes the smallest non-negative integer congruent to m modulo w. Hopefully this will lead to some restrictions on m. As we saw before the special case $p = q$ leads to a Thue equation $H_p(u, v) = \pm p$ and the previously mentioned techniques may apply even for large primes. In case of $u + \delta_4 v = \pm 1$ one encounters a family of superelliptic equations $H_p(\pm 1 - \delta_4 v, v) = \pm q^m$. We will see that sometimes it is possible to solve these equations completely using congruence conditions only.

From now on we consider (3.12) with $q = 3$, that is

$$x^2 + 3^{2m} = 2y^p. \tag{3.25}$$

The equation $x^2 + 3 = y^n$ was completely resolved by Cohn [27]. Arif and Muriefah [2] found all solutions of the equation $x^2 + 3^{2m+1} = y^n$. There is one family of solutions, given by $(x, y, m, n) = (10 \cdot 3^{3t}, 7 \cdot 3^{2t}, 5 + 6t, 3)$. Luca [55] proved that all solutions of the equation $x^2 + 3^{2m} = y^n$ are of the form $x = 46 \cdot 3^{3t}, y = 13 \cdot 3^{2t}, m = 4 + 6t, n = 3$.

Remark. We note that equation (3.25) with odd powers of 3 is easily solvable. From $x^2 + 3^{2m+1} = 2y^p$ we get

$$4 \equiv 2y^p \pmod 8,$$

hence $p = 1$.

Let us first treat the special case $p = q = 3$. By (3.15) and Lemma 3.2.2 we have

$$\begin{aligned} x &= F_3(u, v) = (u + v)(u^2 - 4uv + v^2), \\ 3^m &= G_3(u, v) = (u - v)(u^2 + 4uv + v^2). \end{aligned}$$

Therefore there exists an integer k with $0 \le k \le m$, such that

$$\begin{aligned} u - v &= \pm 3^k, \\ u^2 + 4uv + v^2 &= \pm 3^{m-k}. \end{aligned}$$

Hence we have

$$6v^2 \pm 6(3^k)v + 3^{2k} = \pm 3^{m-k}.$$

Both from $k = m$ and from $k = 0$ it follows easily that $k = m = 0$. This yields the solutions $(x, y) = (\pm 1, 1)$. If $k = m - 1 > 0$, then $3 \mid 2v^2 \pm 1$. Thus one has to resolve the system of equations

$$\begin{aligned} u - v &= -3^{m-1}, \\ u^2 + 4uv + v^2 &= -3. \end{aligned}$$

As we mentioned, sometimes it is possible to handle the case $k = 0$ using congruences only. In case of $q = 3$ it works.

Lemma 3.2.8. *There is no solution of* (3.16) *and* (3.17) *with* $k = 0$.

Proof. We give a proof for (3.16) which also works for (3.17). In case of (3.16) if $k = 0$, then $u = 1 - \delta_4 v$. Observe that by (3.23)

- if $v \equiv 0 \pmod 3$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$,
- if $v \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$,
- if $v \equiv 1 \pmod 3$ and $p \equiv 3 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv \pm 1 \pmod 3$,
- if $v \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv \pm 1 \pmod 3$,
- if $v \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$.

Thus $H_p(1 - \delta_4 v, v) \not\equiv 0 \pmod 3$. Therefore there is no $v \in \mathbb{Z}$ such that $H_p(1 - \delta_4 v, v) = 3^m$, as should be the case by (3.16) and (3.17). □

Finally we investigate the remaining case, that is $u + \delta_4 v = q^m$. We remark that $u + \delta_4 v = -q^m$ is not possible because from (3.17) and Lemma 3.2.5 we obtain $-1 \equiv H_p(-q^m - \delta_4 v, v) \equiv q^{k(p-1)} \equiv 1 \pmod p$.

Lemma 3.2.9. *If there is a coprime solution* $(u, v) \in \mathbb{Z}^2$ *of* (3.16) *with* $k = m$, *then* $p \equiv 5$ *or* $11 \pmod{24}$.

Proof. In case of $k = m$ we have, by (3.16) and Lemma 3.2.5,

$$H_p(3^m - \delta_4 v, v) = \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + 3^m p \widehat{H}_p(v) + 3^{m(p-1)} = 1. \tag{3.26}$$

Therefore

$$\delta_8 2^{\frac{p-1}{2}} p \equiv 1 \pmod 3$$

and we get that $p \equiv 1, 5, 7, 11 \pmod{24}$. Since by Lemma 3.2.1 the only solution of the equation $x^2 + 3^{2m} = 2y^p$ with $1 \le m \le 5$ is given by $(x, y, m, p) \in \{(79, 5, 1, 5), (545, 53, 3, 3)\}$, we may assume without loss of generality that $m \ge 6$. To get rid of the classes 1 and 7 we work modulo 243. If $p = 8t + 1$, then from (3.26) we have

$$2^{4t}(8t + 1)v^{8t} \equiv 1 \pmod{243}.$$

It follows that $243 | t$ and the first prime of the appropriate form is 3889 which is larger than

the bound we have for p. If $p = 8t + 7$, then

$$-2^{4t+3}(8t + 7)v^{8t+6} \equiv 1 \pmod{243}.$$

It follows that $t \equiv 60 \pmod{243}$ and it turns out that $p = 487$ is in this class, so we work modulo 3^6 to show that the smallest possible prime is larger than the bound we have for p. Here we have to resolve the case $m = 6$ using the method from [88]. This value of m is not too large so the method worked. We did not get any new solution. Thus $p \equiv 5$ or $11 \pmod{24}$. □

Theorem 3.2.4. *There exists no coprime integer solution (x, y) of $x^2 + 3^{2m} = 2y^p$ with $m > 0$ and $p < 1000, p \equiv 5 \pmod{24}$ or $p \in \{131, 251, 491, 971\}$ prime.*

Proof. To prove the theorem we resolve the Thue equations

$$H_p(u, v) = 1$$

for the given primes. In each case there is a small subfield, hence we can apply the method of [18]. We wrote a PARI [69] script to handle the computation. To get c_1 one has to compute

$$\min_k \left| \prod_{\substack{l=0 \\ l \neq k, k_0}}^{p-1} \left(\tan \frac{(4k + 3)\pi}{4p}) - \tan \frac{(4l + 3)\pi}{4p} \right) \right|,$$

$k_0 = \left\lfloor \frac{p}{4} \right\rfloor (p \mod 4)$. Using the mean-value theorem one can easily prove that

$$\left| \tan \frac{(4k_1 + 3)\pi}{4p} - \tan \frac{(4k_2 + 3)\pi}{4p} \right| \geq |k_1 - k_2| \frac{\pi}{p}.$$

Hence $c_2 \geq |k_1 - k_2| \frac{\pi}{p}$, and it is easy to see that the minimum is $|\tan \frac{\pi}{4p} + \tan \frac{3\pi}{4p}|$. Using Gaussian periods one can compute a defining equation of the subfield, see [18, Lemma 7.1.1]. In Table 3.1 we indicate defining equations for primes $p < 1000, p \equiv 5 \pmod{24}$ or $p \in \{131, 251, 491, 971\}$. The PARI [69] procedure *bnfinit* produces, in particular, a full system of independent units of the small subfield. One has to use the procedure *bnfcertify* to ensure that that the system of units is fundamental. We note that if $p = 659$ or $p = 827$, then there is a degree 7 subfield, but the regulator is too large to get unconditional result, the same holds for $p = 419, 683, 947$, in these cases there is a degree 11 subfield. In the computation we followed the paper [18], but at the end we skipped the enumeration step. Instead we used the

Table 3.1: Defining equations

p	polynomial
29	$x^4 - 29x^2 + 29$
53	$x^4 - 53x^2 + 53$
101	$x^4 - 101x^2 + 2525$
131	$x^5 + x^4 - 52x^3 - 89x^2 + 109x + 193$
149	$x^4 - 149x^2 + 3725$
173	$x^4 - 173x^2 + 173$
197	$x^4 - 197x^2 + 9653$
251	$x^5 + x^4 - 100x^3 - 20x^2 + 1504x + 1024$
269	$x^4 - 269x^2 + 6725$
293	$x^4 - 293x^2 + 293$
317	$x^4 - 317x^2 + 15533$
389	$x^4 - 389x^2 + 9725$
461	$x^4 - 461x^2 + 11525$
491	$x^5 + x^4 - 196x^3 + 59x^2 + 2019x + 1377$
509	$x^4 - 509x^2 + 61589$
557	$x^4 - 557x^2 + 27293$
653	$x^4 - 653x^2 + 79013$
677	$x^4 - 677x^2 + 114413$
701	$x^4 - 701x^2 + 118469$
773	$x^4 - 773x^2 + 93533$
797	$x^4 - 797x^2 + 134693$
821	$x^4 - 821x^2 + 40229$
941	$x^4 - 941x^2 + 23525$
971	$x^5 + x^4 - 388x^3 + 1476x^2 + 8304x + 7168$

bound for $|x|$ given by the formula (34) at page 318. We collect the value of some constants in Table 3.2, the time is in seconds. We obtained small bounds for $|u|$ in each case. It remains to find the integer solutions of the polynomial equations $H_p(u_0, v) = 1$ for the given primes with $|u_0| \leq X_3$. There is no solution for which $u + \delta v = 3^m, m > 0$, and the statement follows. □

We recall that Cohn [29] showed that the only positive integer solution of $x^2 + 1 = 2y^p$ is given by $x = y = 1$.

Theorem 3.2.5. *If the Diophantine equation $x^2 + 3^m = 2y^p$ with $m > 0$ and p prime admits a coprime integer solution (x, y), then either*

$$p \in \{3, 59, 83, 107, 179, 227, 347, 419, 443, 467, 563, 587, 659, 683, 827, 947\}$$

or $(x, y, m, p) = (79, 5, 2, 5)$.

Proof. We will provide lower bounds for m which contradict the bound for p provided by Theorem 3.2.2. By Theorem 3.2.2 we have $p \leq 3803$ and by Lemma 3.2.9 we have

Table 3.2: Summary of the computation

p	c_6	B_0	B_0^{red}	X_3	time
29	$7.36 \cdot 10^8$	$1.33 \cdot 10^{31}$	21	4	1.2
53	$2.04 \cdot 10^{16}$	$8.31 \cdot 10^{32}$	40	3	1.9
101	$4.94 \cdot 10^{30}$	$4.75 \cdot 10^{35}$	38	2	3.4
149	$1.5 \cdot 10^{45}$	$7.35 \cdot 10^{36}$	44	2	7.3
131	$2.25 \cdot 10^{40}$	$2.15 \cdot 10^{42}$	115	2	5.9
173	$7.37 \cdot 10^{52}$	$2.18 \cdot 10^{36}$	134	2	5.7
197	$6.91 \cdot 10^{59}$	$5.87 \cdot 10^{37}$	76	2	6.5
251	$1.03 \cdot 10^{76}$	$1.19 \cdot 10^{46}$	34	2	13.6
269	$2.92 \cdot 10^{81}$	$6.91 \cdot 10^{38}$	72	2	14.3
293	$1.54 \cdot 10^{89}$	$6.88 \cdot 10^{37}$	230	2	10.3
317	$1.1 \cdot 10^{96}$	$7.19 \cdot 10^{38}$	99	2	12.9
389	$3.65 \cdot 10^{117}$	$1.02 \cdot 10^{40}$	72	2	25.2
461	$2.72 \cdot 10^{139}$	$1.67 \cdot 10^{40}$	117	2	22.2
491	$5.97 \cdot 10^{148}$	$8.5 \cdot 10^{47}$	214	2	24.9
509	$8.17 \cdot 10^{153}$	$2.28 \cdot 10^{40}$	127	2	23.4
557	$2.81 \cdot 10^{168}$	$7.87 \cdot 10^{40}$	157	2	26.5
653	$2.02 \cdot 10^{197}$	$1.35 \cdot 10^{41}$	146	2	32.6
677	$6.29 \cdot 10^{204}$	$4.14 \cdot 10^{41}$	272	2	27.8
701	$6.52 \cdot 10^{211}$	$2.76 \cdot 10^{41}$	169	2	37.1
773	$4.55 \cdot 10^{233}$	$1.08 \cdot 10^{42}$	254	2	44.2
797	$6.58 \cdot 10^{240}$	$6.67 \cdot 10^{41}$	220	2	45.4
821	$6.93 \cdot 10^{247}$	$1.19 \cdot 10^{42}$	138	2	55.5
941	$1.45 \cdot 10^{284}$	$4.22 \cdot 10^{42}$	224	2	62.4
971	$1.26 \cdot 10^{293}$	$2.53 \cdot 10^{51}$	93	2	75.1

p	mod	p	mod	p	mod	p	mod	p	mod
1013	16,27	1571	5,22	1973	16,22	2357	16,22	3011	5,22
1109	16,22	1613	16,22	1979	16,22	2459	16,22	3203	16,22
1181	16,22	1619	16,22	2003	16,22	2477	16,22	3221	16,22
1187	16,22	1667	16,22	2027	16,22	2531	5,22	3323	16,22
1229	16,22	1709	16,22	2069	16,22	2579	16,22	3347	16,22
1259	16,22	1733	16,22	2099	16,22	2693	16,22	3371	5,22
1277	16,22	1787	16,22	2141	16,22	2741	16,27	3413	16,22
1283	16,22	1811	5,22	2237	16,22	2861	16,22	3533	16,22
1307	16,22	1877	16,27	2243	16,22	2909	16,22	3677	16,22
1493	16,22	1931	5,22	2309	16,27	2957	16,22	3701	16,22
1523	16,22	1949	16,22	2333	16,22	2963	16,22		

Table 3.3: Excluding some primes using congruences.

$p \equiv 5$ or $11 \pmod{24}$. We compute the following sets for each prime p with $1000 \leq p \leq 3803$, $p \equiv 5$ or $11 \pmod{24}$:

$$A5 = L(p, 3, 242),$$

$$A16 = L(p, 3, 136) \cap L(p, 3, 193) \cap L(p, 3, 320) \cap L(p, 3, 697),$$

$$A22 = L(p, 3, 92) \cap L(p, 3, 134) \cap L(p, 3, 661),$$

$$A27 = L(p, 3, 866) \cap L(p, 3, 1417),$$

$$A34 = L(p, 3, 103) \cap L(p, 3, 307) \cap L(p, 3, 1021),$$

$$A39 = L(p, 3, 169) \cap L(p, 3, 313),$$

$$A69 = L(p, 3, 554) \cap L(p, 3, 611).$$

In case of $A5$ we have $\mathrm{ord}_{242}3 = 5$, hence this set contains those congruence classes modulo 5 for which (3.25) is solvable, similarly in case of the other sets. How can we use this information? Suppose it turns out that for a prime $A5 = \{0\}$ and $A16 = \{0\}$. Then we know that $m \equiv 0 \pmod{5 \cdot 16}$ and Theorem 3.2.2 implies $p \leq 1309$. If the prime is larger than this bound, then we have a contradiction. In Table 3.3 we included those primes for which we obtained a contradiction in this way. In the columns mod the numbers n are stated for which sets An were used for the given prime. It turned out that only 4 sets were needed. In case of $5, 22$ we have $m \geq 110$, $p \leq 1093$, in case of $16, 22$ we have $m \geq 176$, $p \leq 1093$ and in the case $16, 27$ we have $m \geq 432$, $p \leq 1009$. We could not exclude all primes using the previous argument, but there is an other way to use the computed sets. We can combine the available information by means of the Chinese remainder theorem. Let $CRT([a5, a16, a39], [5, 16, 39])$

p	r_m	CRT	p	r_m	CRT	p	r_m	CRT
1019	384	5,16,27	2267	448	5,16,69	3389	170	5,27,34
1061	176	5,16,39	2339	208	5,16,39	3461	116	5,16,39
1091	580	5,16,27	2381	44	5,27,34	3467	336	5,16,27
1163	586	5,27,34	2411	180	5,16,27	3491	850	5,27,34
1301	416	5,16,39	2549	320	5,16,27	3539	112	5,16,39
1427	270	5,27,34	2699	640	5,16,69	3557	176	5,16,39
1451	340	5,16,27	2789	204	5,27,34	3581	150	5,27,34
1499	112	5,16,39	2819	352	5,16,27	3659	112	5,16,39
1637	121	5,27,34	2837	131	5,27,34	3779	72	5,27,34
1901	304	5,16,39	2843	136	5,27,34	3797	416	5,16,39
1907	102	5,27,34	3083	340	5,27,34	3803	136	5,27,34
1997	170	5,27,34	3251	580	5,16,27			
2213	170	5,27,34	3299	64	5,16,39			

Table 3.4: Excluding some primes using CRT.

be the smallest non-negative solution of the system of congruences

$$m \equiv a5 \pmod 5$$
$$m \equiv a16 \pmod{16}$$
$$m \equiv a39 \pmod{39},$$

where $a5 \in A5, a16 \in A16$ and $a39 \in A39$. Let r_m be the smallest non-zero element of the set $\{CRT([a5, a16, a39], [5, 16, 39]) : a5 \in A5, a16 \in A16, a39 \in A39\}$, In Table 3.4 we included the values of r_m and the numbers related to the sets $A5 - A69$. We see that $m \geq r_m$ in all cases. For example, if $p = 1019$ then $m \geq 384$, and Theorem 3.2.2 implies $p \leq 1009$, which is a contradiction. For $p = 2381$ we used $A5, A27$ and $A34$, given by $A5 = \{0, 1, 4\}, A27 = \{0, 14, 15, 17\}, A34 = \{0, 10\}$. Hence

$$\{CRT([a5, a27, a34], [5, 27, 34]) : a5 \in A5, a16 \in A16, a39 \in A39\} =$$
$$= \{0, 44, 204, 476, 486, 554, 690, 986, 1394, 1404, 1836, 1880, 1904,$$
$$2040, 2390, 2526, 2754, 3230, 3240, 3444, 3716, 3740, 3876, 4226\}.$$

The smallest non-zero element is 44 (which comes from $[a5, a27, a34] = [4, 17, 10]$), therefore $m \geq 44$ and $p \leq 1309$, a contradiction. In this way all remaining primes > 1000 can be handled. We are left with the primes $p < 1000, p \equiv 5 \pmod{24}$ and with $p \in \{131, 251, 491, 971\}$ prime. They are mentioned in Theorem 3.2.4. □

Acknowledgement. I would like to thank Robert Tijdeman for his valuable remarks and suggestions, Peter Stevenhagen for the useful discussions on algebraic number theory, and

for the proof of Lemma 3.2.7. Furthermore, Guillaume Hanrot provided the Pari code which was used in [19] and gave some hints how to modify it.

Chapter 4

Mixed powers in arithmetic progressions

In this chapter some extensions of Fermat's problem on arithmetic progressions of squares are discussed. All arithmetic progressions are described which satisfy one of the following conditions

four consecutive terms are of the form $x_0^2, x_1^2, x_2^2, x_3^3$ or $x_0^3, x_1^2, x_2^2, x_3^2$,

four consecutive terms are of the form $x_0^2, x_1^2, x_2^3, x_3^2$ or $x_0^2, x_1^3, x_2^2, x_3^2$,

four consecutive terms are of the form $x_0^3, x_1^2, x_2^3, x_3^2$ or $x_0^2, x_1^3, x_2^2, x_3^3$.

We shall prove that in the first two cases the only coprime solutions are the trivial ones and in the third instance the complete solution is given by

$$(x_0, x_1, x_2, x_3) \in \{(-2t^2, 0, 2t^2, \pm 4t^3), (t^2, \pm t^3, t^2, \pm t^3)\}$$

for some $t \in \mathbb{Z}$ or

$$(x_0, x_1, x_2, x_3) \in \{(\pm 4t^3, 2t^2, 0, -2t^2), (\pm t^3, t^2, \pm t^3, t^2)\}$$

for some $t \in \mathbb{Z}$, respectively.

4.1 Parametrization

The next lemma provides a parametrization of the solutions of certain ternary Diophantine equations. The lemma and the proof are due to Lajos Hajdu.

Lemma 4.1.1. *All solutions of the equations*

$$i)\ 2b^2 - a^2 = c^3, \quad ii)\ a^2 + 2b^2 = 3c^3,$$

in integers a, b and c with $gcd(a, b, c) = 1$ are given by the following parametrizations:

i) $a = \pm(x^3 + 6xy^2)$, $b = \pm(3x^2y + 2y^3)$,
or $a = \pm(x^3 + 6x^2y + 6xy^2 + 4y^3)$, $b = \pm(x^3 + 3x^2y + 6xy^2 + 2y^3)$,

ii) $a = \pm(x^3 - 6x^2y - 6xy^2 + 4y^3)$, $b = \pm(x^3 + 3x^2y - 6xy^2 - 2y^3)$.

Here x and y are coprime integers and the $\pm$ signs can be chosen independently.

Proof. The statement can be proved by factorizing the appropriate expressions in the appropriate number fields. We handle each case separately.

i) We note that the ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$ and this is a principal ideal domain. In $\mathbb{Q}(\sqrt{2})$ we have

$$(a + \sqrt{2}b)(a - \sqrt{2}b) = (-c)^3.$$

Using $\gcd(a, b) = 1$, a simple calculation gives that

$$\gcd(a + \sqrt{2}b, a - \sqrt{2}b) \mid 2\sqrt{2}$$

in $\mathbb{Q}(\sqrt{2})$. Hence, as $1 + \sqrt{2}$ is a fundamental unit of $\mathbb{Q}(\sqrt{2})$, we have

$$a + \sqrt{2}b = (1 + \sqrt{2})^{\alpha}(\sqrt{2})^{\beta}(x + \sqrt{2}y)^3, \tag{4.1}$$

where $\alpha \in \{-1, 0, 1\}$, $\beta \in \{0, 1, 2\}$ and x, y are some integers. By taking norms, we immediately obtain that $\beta = 0$. If $\alpha = 0$, then expanding the right hand side of (4.1) we get

$$a = x^3 + 6xy^2, \quad b = 3x^2y + 2y^3.$$

Otherwise, when $\alpha = \pm 1$ then (4.1) yields

$$a = x^3 \pm 6x^2y + 6xy^2 \pm 4y^3, \quad b = \pm x^3 + 3x^2y \pm 6xy^2 + 2y^3.$$

Substituting $-x$ and $-y$ in place of x and y, respectively, we obtain the parametrizations given in the statement. Observe that the coprimality of a and b implies $\gcd(x,y) = 1$.

ii) We note that the ring of integers of $\mathbb{Q}(\sqrt{-2})$ is $\mathbb{Z}[\sqrt{-2}]$ and this is a principal ideal domain. In $\mathbb{Q}(\sqrt{-2})$ we obtain

$$(a + \sqrt{-2}b)(a - \sqrt{-2}b) = 3c^3.$$

Observe that $\gcd(a,b) = 1$. Indeed, as $\gcd(a,b,c) = 1$, the only possible proper common divisor of a and b could be 3. However, $3 \mid a$ and $3 \mid b$ implies $3 \mid c$, a contradiction. Hence

$$\gcd(a + \sqrt{-2}b, a - \sqrt{-2}b) \mid 2\sqrt{-2}$$

in $\mathbb{Q}(\sqrt{-2})$. As $\mathbb{Q}(\sqrt{-2})$ has no other units than ± 1, using $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$, we can write

$$a + \sqrt{-2}b = (1 + \sqrt{-2})^{\alpha}(1 - \sqrt{-2})^{\beta}(\sqrt{-2})^{\gamma}(x + \sqrt{-2}y)^3, \tag{4.2}$$

where $\alpha, \beta, \gamma \in \{0,1,2\}$ and x, y are some integers. By taking norms, we immediately obtain that $\gamma = 0$ and $\alpha + \beta \equiv 1 \pmod 3$. If $\alpha = \beta = 2$, then writing out (4.2) we get that $3 \mid a$, $3 \mid b$, a contradiction. In case of $\alpha = 0, \beta = 1$ or $\alpha = 1, \beta = 0$ by expanding the right hand side of (4.2) we obtain

$$a = x^3 \pm 6x^2y - 6xy^2 \pm 4y^3, \quad b = \pm x^3 + 3x^2y \mp 6xy^2 - 2y^3.$$

Substituting $-x$ and $-y$ in place of x and y, respectively, we get the parametrizations indicated in the statement. As a consequence of $\gcd(a,b) = 1$, we deduce $\gcd(x,y) = 1$ once again.

□

4.2 The cases $(2,2,2,3)$ and $(3,2,2,2)$

Let $x_0^2, x_1^2, x_2^2, x_3^3$ be consecutive terms of an arithmetic progression with $\gcd(x_0, x_1, x_2, x_3) = 1$. Applying part i) of Lemma 4.1.1 to the last three terms of the progression, we get that

either

$$x_1 = \pm(x^3 + 6xy^2), \quad x_2 = \pm(3x^2y + 2y^3)$$

or

$$x_1 = \pm(x^3 + 6x^2y + 6xy^2 + 4y^3), \quad x_2 = \pm(x^3 + 3x^2y + 6xy^2 + 2y^3)$$

where x, y are some coprime integers in both cases.

In the first case from $x_0^2 = 2x_1^2 - x_2^2$ we get

$$x_0^2 = 2x^6 + 15x^4y^2 + 60x^2y^4 - 4y^6.$$

If $x = 0$ then $\gcd(x, y) = 1$ gives that $y = \pm 1$, which is a contradiction. Otherwise, by putting $Y = x_0/x^3$ and $X = y^2/x^2$ we obtain the elliptic equation

$$Y^2 = -4X^3 + 60X^2 + 15X + 2.$$

One can check with MAGMA [21] or another suitable program that this elliptic curve has no affine rational points.

In the second case by the same assertion we obtain

$$x_0^2 = x^6 + 18x^5y + 75x^4y^2 + 120x^3y^3 + 120x^2y^4 + 72xy^5 + 28y^6.$$

If $y = 0$, then the coprimality of x and y yields $x = \pm 1$, and we get the trivial progression $1, 1, 1, 1$. So assume that $y \neq 0$ and let $Y = x_0/y^3$, $X = x/y$. By these substitutions we are led to the hyperelliptic equation

$$Y^2 = X^6 + 18X^5 + 75X^4 + 120X^3 + 120X^2 + 72X + 28.$$

Theorem 4.2.1. *Let C be the curve given by*

$$Y^2 = X^6 + 18X^5 + 75X^4 + 120X^3 + 120X^2 + 72X + 28.$$

Then $C(\mathbb{Q})$ consists only of the points ∞^+ and ∞^-.

Proof. One can get an upper bound for the rank of the Jacobian using M. Stoll's [82] algorithm implemented in MAGMA [21]. In the present case it turns out to be 1. The order of $\mathcal{J}_{\text{tors}}(\mathbb{Q})$ is a divisor of $\gcd(\#\mathcal{J}(\mathbb{F}_5), \#\mathcal{J}(\mathbb{F}_7)) = \gcd(21, 52) = 1$. Therefore the torsion

subgroup is trivial. The divisor $D = [\infty^+ - \infty^-]$ has infinite order, so the rank equals 1. Since the rank is less than the genus, we can apply Chabauty's method [24] to obtain a bound for the number of rational points on C. Other examples are worked out in [23],[39],[40],[72].

The rank of the Jacobian is 1, hence $\mathcal{J}(\mathbb{Q}) = \langle D_0 \rangle$ for some $D_0 \in \mathcal{J}(\mathbb{Q})$ of infinite order. A finite computation $\pmod{13}$ shows that $D \notin 5\mathcal{J}(\mathbb{Q})$, a similar computation $\pmod{139}$ yields that $D \notin 29\mathcal{J}(\mathbb{Q})$. Hence $D = kD_0$ with $5 \nmid k, 29 \nmid k$. The reduction of C over $\mathbb{F}_p$ is a curve of genus 2 for any prime $p \neq 2, 3$. We will use $p = 29$. We used Chabauty's method as implemented in MAGMA [21] by Stoll to bound the number of rational solutions.

$> Qx\langle x\rangle := PolynomialRing(Rationals());$

$> f := x^6 + 18 * x^5 + 75 * x^4 + 120 * x^3 + 120 * x^2 + 72 * x + 28;$

$> C := HyperellipticCurve(f);$

$> pts := Points(C : Bound := 100);$

$> J := Jacobian(C);$

$> D := J![pts[1], pts[2]];$

$> TwoSelmerGroupData(J);$

$> Chabauty(D, 29);$

We found that there are at most 2 rational points on C. Therefore we conclude that $C(\mathbb{Q}) = \{\infty^+, \infty^-\}$. □

Corollary. *There is no increasing arithmetic progression of integers of the type* $x_0^2, x_1^2, x_2^2, x_3^3$.

Proof. From the previous theorem and from the preceding discussion we obtained that the only progression is the trivial 1,1,1,1. □

Corollary. *There is no increasing arithmetic progression of integers of the type* $x_0^3, x_1^2, x_2^2, x_3^2$.

Proof. In this case we apply part i) of Lemma 4.1.1 to the first three terms of the progression. Then we use the equation $x_3^2 = 2x_2^2 - x_1^2$. From this point on the reasoning is similar to the previous case. It turns out that only the trivial arithmetic progression can occur. □

4.3 The cases $(2,2,3,2)$ and $(2,3,2,2)$

Let $x_0^2, x_1^2, x_2^3, x_3^2$ be consecutive terms of an arithmetic progression with $\gcd(x_0, x_1, x_2, x_3) = 1$. Now from part ii) of Lemma 4.1.1, applied to terms with indices $0, 2, 3$

of the progression, we get

$$x_0 = \pm(x^3 - 6x^2y - 6xy^2 + 4y^3), \quad x_3 = \pm(x^3 + 3x^2y - 6xy^2 - 2y^3)$$

where x, y are some coprime integers. Using $x_1^2 = (2x_0^2 + x_3^2)/3$ we obtain

$$x_1^2 = x^6 - 6x^5y + 15x^4y^2 + 40x^3y^3 - 24xy^5 + 12y^6.$$

If $y = 0$, then in the same way as before we deduce that the only possibility is given by the progression $1, 1, 1, 1$. Otherwise, if $y \neq 0$ set $Y = x_1/y^3$, $X = x/y$ to get the hyperelliptic equation

$$Y^2 = X^6 - 6X^5 + 15X^4 + 40X^3 - 24X + 12.$$

Theorem 4.3.1. *Let C be the curve given by*

$$Y^2 = X^6 - 6X^5 + 15X^4 + 40X^3 - 24X + 12.$$

Then $C(\mathbb{Q})$ consists only of the points ∞^+ and ∞^-.

Proof. One can get an upper bound for the rank of the Jacobian using M. Stoll's [82] algorithm implemented in MAGMA [21]. In this case it is 1. The torsion subgroup is trivial. The divisor $D = [\infty^+ - \infty^-]$ has infinite order, hence the rank is 1. We can apply Chabauty's method [24] to obtain a bound for the number of rational points on C.

Since the rank of the Jacobian is 1, we have $\mathcal{J}(\mathbb{Q}) = \langle D_0 \rangle$, for some $D_0 \in \mathcal{J}(\mathbb{Q})$ of infinite order. A finite computation $\pmod{13}$ shows that $D \notin 5\mathcal{J}(\mathbb{Q})$, a similar computation $\pmod{131}$ yields that $D \notin 11\mathcal{J}(\mathbb{Q})$. Hence $D = kD_0$ with $5 \nmid k, 11 \nmid k$. The reduction of C over $\mathbb{F}_p$ is a curve of genus 2 for any prime $p \neq 2, 3$. We will use $p = 11$.

```
> Qx<x> := PolynomialRing(Rationals());
> f := x^6 - 6 * x^5 + 15 * x^4 + 40 * x^3 - 24 * x + 12;
> C := HyperellipticCurve(f);
> pts := Points(C : Bound := 100);
> J := Jacobian(C);
> D := J![pts[1], pts[2]];
> TwoSelmerGroupData(J);
> Chabauty(D, 11);
```

We obtained that there are at most 2 rational points on C. Therefore we conclude that $C(\mathbb{Q}) = \{\infty^+, \infty^-\}$. □

Corollary. *There exists no increasing arithmetic progression of integers of the type* $x_0^2, x_1^2, x_2^3, x_3^2$.

Corollary. *There exists no increasing arithmetic progression of integers of the type* $x_0^2, x_1^3, x_2^2, x_3^2$.

Proof. From part ii) of Lemma 4.1.1, applied to terms with indices $0, 1, 3$ of the progression, we get the parametrizations. Then we use the equation $x_2^2 = (x_0^2 + 2x_3^2)/3$. It turns out that only the trivial arithmetic progression can occur. □

4.4 The cases $(3,2,3,2)$ and $(2,3,2,3)$

Let $x_0^3, x_1^2, x_2^3, x_3^2$ be consecutive terms of an arithmetic progression with $\gcd(x_0, x_1, x_2, x_3) = 1$. We have

$$\begin{aligned} x_1^2 &= \frac{x_0^3 + x_2^3}{2}, \\ x_3^2 &= \frac{-x_0^3 + 3x_2^3}{2}. \end{aligned} \tag{4.3}$$

We note that $x_2 = 0$ implies $x_0 = x_1 = x_2 = x_3 = 0$. Assume $x_2 \neq 0$. Then we obtain from (4.3) that

$$\left(\frac{2x_1x_3}{x_2^3}\right)^2 = -\left(\frac{x_0}{x_2}\right)^6 + 2\left(\frac{x_0}{x_2}\right)^3 + 3.$$

Thus it is sufficient to find all rational points on the curve $Y^2 = -X^6 + 2X^3 + 3$.

Theorem 4.4.1. *Let C be the curve given by*

$$Y^2 = -X^6 + 2X^3 + 3.$$

Then $C(\mathbb{Q}) = \{(-1, 0), (1, \pm 2)\}$.

Proof. Using MAGMA [21] we obtain an upper bound 1 for the rank of the Jacobian, and the torsion subgroup $\mathcal{T}$ consisting of two elements O and $\{(\frac{1-\sqrt{3}i}{2}, 0), (\frac{1+\sqrt{3}i}{2}, 0)\}$. The divisor $D = [(-1,0) + (1,-2) - \infty^+ - \infty^-]$ has infinite order. So the rank is exactly 1. The only Weierstrass point on C is $(-1, 0)$, so it remains to prove that $(1, \pm 2)$ are the only non-Weierstrass points. We have $\mathcal{J}(\mathbb{Q}) = \langle D_0 \rangle$, for some $D_0 \in \mathcal{J}(\mathbb{Q})$ of infinite order. A finite computation $\pmod{13}$ shows that $D \notin 7\mathcal{J}(\mathbb{Q})$, a similar computation $\pmod{23}$ yields that $D \notin 11\mathcal{J}(\mathbb{Q})$. Hence $D = kD_0$ with $7 \nmid k, 11 \nmid k$. The reduction of C over $\mathbb{F}_p$ is a curve of genus 2 for any prime

$p \neq 2, 3$. We will use $p = 11$. > $Qx\langle x\rangle := PolynomialRing(Rationals());$

> $f := -x^6 + 2 * x^3 + 3;$

> $C := HyperellipticCurve(f);$

> $pts := Points(C : Bound := 100);$

> $J := Jacobian(C);$

> $D := J![pts[1], pts[2]];$

> $TwoSelmerGroupData(J);$

> $Chabauty(D, 11);$

We found that there are at most 2 rational points on C. Therefore we conclude that $(1, -2)$ and $(1, 2)$ are the only two non-Weierstrass points on C. □

Corollary. *If $x_0^3, x_1^2, x_2^3, x_3^2$ are consecutive terms of an arithmetic progression, then $(x_0, x_1, x_2, x_3) \in \{(-2t^2, 0, 2t^2, \pm 4t^3), (t^2, \pm t^3, t^2, \pm t^3)\}$ for some $t \in \mathbb{Z}$.*

Proof. The point $(-1, 0)$ is on the curve $Y^2 = -X^6 + 2X^3 + 3$, hence $\frac{x_0}{x_2} = -1$ and $2x_1x_3 = 0$. It easily follows that $x_0 = -2t^2, x_1 = 0, x_2 = 2t^2, x_3 = \pm 4t^3$ is the only possible solution of the problem. In case of the other two points $(1, \pm 2)$ we have $x_0 = x_2$, which implies $x_0^3 = x_1^2 = x_2^3 = x_3^2$. Thus $x_0 = x_2 = t^2$ and $x_1 = x_3 = \pm t^3$ for some $t \in \mathbb{Z}$. □

Corollary. *If $x_0^2, x_1^3, x_2^2, x_3^3$ are consecutive terms of an arithmetic progression, then $(x_0, x_1, x_2, x_3) \in \{(\pm 4t^3, 2t^2, 0, -2t^2), (\pm t^3, t^2, \pm t^3, t^2)\}$ for some $t \in \mathbb{Z}$.*

Proof. In this case we get the equation

$$\left(\frac{2x_0x_2}{x_1^3}\right)^2 = -\left(\frac{x_3}{x_1}\right)^6 + 2\left(\frac{x_3}{x_1}\right)^3 + 3.$$

By Theorem 4.4.1 the only rational points on the curve $Y^2 = -X^6 + 2X^3 + 3$ are $(-1, 0)$ and $(1, \pm 2)$. In a similar way as in the proof of the previous corollary we obtain the solutions. □

Acknowledgement. I'm grateful to Lajos Hajdu for introducing me to the problem and for the proof of Lemma 4.1.1. I wish to thank Nils Bruin for the useful comments on Chabauty's method.

Bibliography

[1] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2 + 2^k = y^n$. *Internat. J. Math. Math. Sci.*, 20(2):299–304, 1997.

[2] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + 3^m = y^n$. *Internat. J. Math. Math. Sci.*, 21(3):619–620, 1998.

[3] S. A. Arif and F S. A. Muriefah. On the Diophantine equation $x^2 + 2^k = y^n$. II. *Arab J. Math. Sci.*, 7(2):67–71, 2001.

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

[5] M. Ayad. Sur le théorème de Runge. *Acta Arith.*, 58(2):203–209, 1991.

[6] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[7] A. Baker. Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms. *Philos. Trans. Roy. Soc. London Ser. A*, 263:173–191, 1967/1968.

[8] A. Baker. The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. *J. London Math. Soc.*, 43:1–9, 1968.

[9] A. Baker. Linear forms in the logarithms of algebraic numbers. IV. *Mathematika*, 15:204–216, 1968.

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

[11] A. Baker and H. Davenport. The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. *Quart. J. Math. Oxford Ser. (2)*, 20:129–137, 1969.

[12] M. Bauer and M. A. Bennett. Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation. *Ramanujan J.*, 6(2):209–270, 2002.

[13] F. Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91(1):61–88, 1998.

[14] F. Beukers, T. N. Shorey, and R. Tijdeman. Irreducibility of polynomials and arithmetic progressions with equal products of terms. In *Number theory in progress, Vol. 1 (Zakopane-Ko´scielisko, 1997)*, pages 11–26. de Gruyter, Berlin, 1999.

[15] Yu. Bilu. Effective analysis of integral points on algebraic curves. *Israel J. Math.*, 90(1-3):235–252, 1995.

[16] Yu. Bilu. Quantitative Siegel's theorem for Galois coverings. *Compositio Math.*, 106(2):125–158, 1997.

[17] Yu. Bilu and G. Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60(2):373–392, 1996.

[18] Yu. Bilu and G. Hanrot. Thue equations with composite fields. *Acta Arith.*, 88(4):311–326, 1999.

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

[20] Yu. F. Bilu and R. F. Tichy. The Diophantine equation $f(x) = g(y)$. *Acta Arith.*, 95(3):261–288, 2000.

[21] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[22] Y. Bugeaud. On the Diophantine equation $x^2 - p^m = \pm y^n$. *Acta Arith.*, 80(3):213–223, 1997.

[23] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[24] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[25] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[26] J. H. E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. *Arch. Math. (Basel)*, 59(4):341–344, 1992.

[27] J. H. E. Cohn. The Diophantine equation $x^2+3 = y^n$. *Glasgow Math. J.*, 35(2):203–206, 1993.

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

[29] J. H. E. Cohn. Perfect Pell powers. *Glasgow Math. J.*, 38(1):19–20, 1996.

[30] J. H. E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. II. *Int. J. Math. Math. Sci.*, 22(3):459–462, 1999.

[31] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. II. *Acta Arith.*, 109(2):205–206, 2003.

[32] G. Collins and A. Akritas. Polynomial real root isolation using Descartes' rule of signs. In *In Proceedings of the third ACM symposium on Symbolic and Algebraic Computation*, pages 272–275, 1976.

[33] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[34] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[35] H. Davenport, D. J. Lewis, and A. Schinzel. Equations of the form $f(x) = g(y)$. *Quart. J. Math. Oxford Ser. (2)*, 12:304–312, 1961.

[36] J. Edwards. A complete solution to $X^2 + Y^3 + Z^5 = 0$. *J. Reine Angew. Math.*, 571:213–236, 2004.

[37] N. D. Elkies. On $A^4 + B^4 + C^4 = D^4$. *Math. Comp.*, 51(184):825–835, 1988.

[38] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[39] E. V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Math.*, 105(1):79–94, 1997.

[40] E. V. Flynn, B. Poonen, and E. F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90(3):435–463, 1997.

[41] A. Grytczuk and A. Schinzel. On Runge's theorem about Diophantine equations. In *Sets, graphs and numbers (Budapest, 1991)*, volume 60 of *Colloq. Math. Soc. J´anos Bolyai*, pages 329–356. North-Holland, Amsterdam, 1992.

[42] K. Győry. Solving Diophantine equations by Baker's theory. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 38–72. Cambridge Univ. Press, Cambridge, 2002.

[43] L. Hajdu and Á. Pintér. Combinatorial Diophantine equations. *Publ. Math. Debrecen*, 56(3-4):391–403, 2000.

[44] G. Hanrot. Solving Thue equations without the full unit group. *Math. Comp.*, 69(229):395–405, 2000.

[45] D. L. Hilliker and E. G. Straus. Determination of bounds for the solutions to those binary Diophantine equations that satisfy the hypotheses of Runge's theorem. *Trans. Amer. Math. Soc.*, 280(2):637–657, 1983.

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

[47] L. J. Lander and T. R. Parkin. A counterexample to Euler's sum of powers conjecture. *Math. Comp.*, 21:101–103, 1967.

[48] M. Laurent and D. Poulakis. On the global distance between two algebraic points on a curve. *J. Number Theory*, 104(2):210–254, 2004.

[49] Maohua Le. On the Diophantine equation $x^2 + p^2 = y^n$. *Publ. Math. Debrecen*, 63(1-2):67–78, 2003.

[50] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[51] W. Ljunggren. Über die Gleichungen $1 + Dx^2 = 2y^n$ und $1 + Dx^2 = 4y^n$. *Norske Vid. Selsk. Forh., Trondhjem*, 15(30):115–118, 1942.

[52] W. Ljunggren. On the Diophantine equation $x^2 + p^2 = y^n$. *Norske Vid. Selsk. Forh., Trondhjem*, 16(8):27–30, 1943.

[53] W. Ljunggren. On the Diophantine equation $Cx^2 + D = y^n$. *Pacific J. Math.*, 14:585–596, 1964.

[54] W. Ljunggren. On the diophantine equation $Cx^2 + D = 2y^n$. *Math. Scand.*, 18:69–86, 1966.

[55] F. Luca. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 61(2):241–246, 2000.

[56] F. Luca. On the equation $x^2 + 2^a \cdot 3^b = y^n$. *Int. J. Math. Math. Sci.*, 29(4):239–244, 2002.

[57] R. A. MacLeod and I. Barrodale. On equal products of consecutive integers. *Canad. Math. Bull.*, 13:255–259, 1970.

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

[59] M. Mignotte. On the Diophantine equation $D_1x^2 + D_2^m = 4y^n$. *Portugal. Math.*, 54(4):457–460, 1997.

[60] P. Mihailescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.

[61] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[62] F. S. A. Muriefah. On the Diophantine equation $px^2 + 3^n = y^p$. *Tamkang J. Math.*, 31(1):79–84, 2000.

[63] F. S. A. Muriefah. On the Diophantine equation $Ax^2 + 2^{2m} = y^n$. *Int. J. Math. Math. Sci.*, 25(6):373–381, 2001.

[64] F. S. A. Muriefah and S. A. Arif. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 57(2):189–198, 1998.

[65] F. S. A. Muriefah and S. A. Arif. The Diophantine equation $x^2 + 5^{2k+1} = y^n$. *Indian J. Pure Appl. Math.*, 30(3):229–231, 1999.

[66] F. S. A. Muriefah and S. A. Arif. The Diophantine equation $x^2 + q^{2k} = y^n$. *Arab. J. Sci. Eng. Sect. A Sci.*, 26(1):53–62, 2001.

[67] T. Nagell. Verallgemeinerung eines Fermatschen Satzes. *Arch. Math.*, 5:153–159, 1954.

[68] I. Niven. *Irrational numbers*. The Carus Mathematical Monographs, No. 11. The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[69] The PARI Group, Bordeaux. *PARI/GP, version* `2.2.8`, 2004. available from `http://pari.math.u-bordeaux.fr/`.

[70] I. Pink. On the Diophantine equation $x^2 + (p_1^{z_1} \dots p_s^{z_s})^2 = 2y^n$. *Publ. Math. Debrecen*, 65(1-2):205–213, 2004.

[71] I. Pink and Sz. Tengely. Full powers in arithmetic progressions. *Publ. Math. Debrecen*, 57(3-4):535–545, 2000.

[72] B. Poonen. The classification of rational preperiodic points of quadratic polynomials over $\mathbf{Q}$: a refined conjecture. *Math. Z.*, 228(1):11–29, 1998.

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

[74] C. Runge. Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen. *J. Reine Angew. Math.*, 100:425–435, 1887.

[75] A. Schinzel. An improvement of Runge's theorem on Diophantine equations. *Comment. Pontificia Acad. Sci.*, 2(20):1–9, 1969.

[76] A. Schinzel and R. Tijdeman. On the equation $y^m = P(x)$. *Acta Arith.*, 31(2):199–204, 1976.

[77] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. Technical report, Univ. Tübingen, 1982.

[78] C. L. Siegel. The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$. *J. Lond. Math. Soc.*, 1:66–68, 1926.

[79] C. L. Siegel. Über einige Anwendungen diophantischer Approximationen. *Abh. Pr. Akad. Wiss.*, 1:41–69, 1929.

[80] T. Skolem. Über ganzzahlige Lösungen einer Klasse unbestimmten Gleichungen. In *Norsk. Mat. Forenings Skrifter*, number 10 in I. 1922.

[81] N. P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[82] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

[83] B. Sury. On the Diophantine equation $x^2 + 2 = y^n$. *Arch. Math. (Basel)*, 74(5):350–355, 2000.

[84] L. Szalay. Fast algorithm for solving superelliptic equations of certain types. *Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.)*, 27:19–24 (2001), 2000.

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

[86] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[87] Sz. Tengely. On the Diophantine equation $F(x) = G(y)$. *Acta Arith.*, 110(2):185–200, 2003.

[88] Sz. Tengely. On the Diophantine equation $x^2+a^2 = 2y^p$. *Indag. Math. (N.S.)*, 15(2):291–304, 2004.

[89] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew Math.*, 135:284–305, 1909.

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

[91] P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences. II. *J. Th´eor. Nombres Bordeaux*, 8(2):251–274, 1996.

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

[93] B. M. M. de Weger. *Algorithms for Diophantine equations*, volume 65 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[94] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Samenvatting

In dit proefschrift lossen we Diophantische vergelijkingen op met verschillende methoden, namelijk de methoden van Runge, van Baker en van Chabauty.
In Hoofdstuk 2 bekijken we de Runge Diophantische vergelijking

$$F(x) = G(y) \qquad (*)$$

met $F, G \in \mathbb{Z}[X]$ monische veeltermen van respectievelijk graad n en m zodanig dat $F(X) - G(Y)$ irreducibel is in $\mathbb{Q}[X, Y]$ en $\gcd(n, m) > 1$. In het hoofdstuk (dat is gebaseerd op [87]), geven we een bovengrens voor de grootte van de oplossingen in gehele getallen voor vergelijking (*) in het geval dat $\gcd(n, m) > 1$. Verder geven we een algoritme om alle gehele oplossingen te vinden. Het algoritme is geïmplementeerd in Magma. In de onderstaande tabel staan enkele voorbeelden van vergelijkingen, het aantal oplossingen en de benodigde rekentijd op een AMD-Athlon 1 GHz PC.

Vergelijking	# Oplossingen	CPU tijd (sec)
$x^2 = y^8 + y^7 + y^2 + 3y - 5$	4	0.16
$x^3 = y^9 + 2y^8 - 5y^7 - 11y^6 - y^5 + 2y^4 + 7y^2 - 2y - 3$	1	0.75
$x^5 = y^{25} + y^{24} + \ldots + y + 7$	1	5.69
$x^2 = y^8 - 7y^7 - 2y^4 - y + 5$	0	4.79
$x^2 = y^4 - 99y^3 - 37y^2 - 51y + 100$	2	1.83
$x^2 - 3x + 5 = y^8 - y^7 + 9y^6 - 7y^5 + 4y^4 - y^3$	6	0.72
$x^3 - 5x^2 + 45x - 713 = y^9 - 3y^8 + 9y^7 - 17y^6 + 38y^5 - 199y^4 - 261y^3 + 789y^2 + 234y$	1	0.38
$x(x+1)(x+2)(x+3) = y(y+1)\cdots(y+5)$	28	0.23

In Hoofdstuk 3 bestuderen we exponentiële Diophantische vergelijkingen van de vorm $x^2 + a^2 = 2y^p$ met x, y geheel en $p > 2$ priemgetal. In Sectie 3.1 (gebaseerd op [88]) geven we een methode om de vergelijking $x^2 + a^2 = 2y^n$ met n, x en y geheel en $n > 2$ op te lossen voor vaste a. In het bijzonder berekenen we alle oplossingen van de vergelijkingen $x^2 + a^2 = y^p$ en $x^2 + a^2 = 2y^p$ voor oneven a met $3 \leq a \leq 501$. In Sectie 3.2 bekijken we de Diophantische vergelijking $x^2 + q^{2m} = 2y^p$ in onbekende getallen m, p, q, x, y waarbij $m > 0$, p, q oneven priem en $\gcd(x, y) = 1$. We bewijzen dat er slechts eindig veel oplossingen (m, p, q, x, y) bestaan wanneer y niet van de vorm $2v^2 \pm 2v + 1$ is. Ook bekijken we deze vergelijking voor vaste y en voor vaste q. Verder lossen we de vergelijking $x^2 + q^{2m} = 2 \cdot 17^p$ helemaal op. Aan het eind van het hoofdstuk wordt bewezen dat indien de Diophantische vergelijking $x^2 + 3^{2m} = 2y^p$ met $m > 0$ en p priem een oplossing in gehele getallen (x, y) heeft met x en y onderling priem, dat dan is $p \in \{59, 83, 107, 179, 227, 347, 419, 443, 467, 563, 587, 659, 683, 827, 947\}$ of $(x, y, m, p) \in \{(79, 5, 1, 5), (545, 53, 3, 3)\}$.

In Hoofdstuk 4 bespreken we enkele generalisaties van Fermat's resultaat. Fermat bewees dat er geen stijgende rekenkundige rij van lengte 4 is die uit kwadraten van gehele

getallen bestaat. Alle rekenkundige rijen worden beschreven die aan een van de volgende voorwaarden voldoen:

$$\begin{aligned} &\text{vier opeenvolgende termen hebben de vorm } x_0^2, x_1^2, x_2^2, x_3^3, \\ &\text{vier opeenvolgende termen hebben de vorm } x_0^2, x_1^2, x_2^3, x_3^2, \\ &\text{vier opeenvolgende termen hebben de vorm } x_0^3, x_1^2, x_2^3, x_3^2. \end{aligned} \tag{**}$$

In de eerste twee gevallen laten we zien dat om alle rijen met $\gcd(x_0, x_1, x_2, x_3) = 1$ te verkrijgen het voldoende is om alle rationale punten op bepaalde hyperelliptische krommen van geslacht 2 te vinden. Deze hyperelliptische krommen worden gegeven door

$$\begin{aligned} Y^2 &= X^6 + 18X^5 + 75X^4 + 120X^3 + 120X^2 + 72X + 28, \\ Y^2 &= X^6 - 6X^5 + 15X^4 + 40X^3 - 24X + 12. \end{aligned}$$

In beide gevallen is de rang van de Jacobiaan 1, waardoor een methode van Chabauty kan worden toegepast. In het derde geval kan men een kromme van geslacht 2 verkrijgen zonder enige vorm van parametrisatie te gebruiken, waardoor we de voorwaarde $\gcd(x_0, x_1, x_2, x_3) = 1$ kunnen weglaten. Deze kromme is gegeven door

$$C : Y^2 = -X^6 + 2X^3 + 3.$$

We bewijzen dat $C(\mathbb{Q}) = \{(-1, 0), (1, \pm 2)\}$. Deze rationale punten leiden tot twee families van rijen van de vorm $x_0^3, x_1^2, x_2^3, x_3^2$ gegeven door

$$\begin{aligned} &x_0 = -2t^2, x_1 = 0, x_2 = 2t^2, x_3 = \pm 4t^3 \text{ voor } t \in \mathbb{Z}, \\ &x_0 = t^2, x_1 = \pm t^3, x_2 = t^2, x_3 = \pm t^3 \text{ voor } t \in \mathbb{Z}. \end{aligned}$$

Er volgt dat er geen stijgende rekenkundige rij van gehele getallen van de vorm (**) bestaat.

Curriculum Vitae

Name : Szabolcs Tengely
Date of birth : 13 January 1976
Place of birth : Ózd, Hungary

Education:

Csépányi Úti Primary School, Ózd, Hungary, 1982-1990,

József Attila Secondary School, Ózd, Hungary, 1990-1994,

Kossuth Lajos University, Debrecen, Hungary, 1994-1999.

Scientific and teaching activities:

By attending a course of Professor dr. Kálmán Győry in number theory, I became interested in this subject, especially in Diophantine equations. Together with István Pink, in 1998 I started to investigate those arithmetical progressions whose terms are perfect powers or "almost" perfect ones. For our results we won the special award of the jury of the National Scientific Competition for Students in 1999. I completed my Master study in 1999. My Master Thesis was about effective and numerical investigation of the Diophantine equation $D_1(a_0x^2 + a_1x + a_2)^2 - D_2(b_0y^2 + b_1y + b_2) = k$. My supervisors were Professor dr. Kálmán Győry and Dr. Lajos Hajdu.
In the academic year 1997/98 and 1998/99 as a student assistant, and continuing in 1999/2000 as an assistant, I gave classes in algebra, discrete mathematics and linear algebra for first and second year students and in number theory for third year students. In the academic year 1999/2000 I was also a scientific researcher-fellow of the Debrecen Number Theory Research Group of the Hungarian Academy of Sciences.
From 2001 to 2005 I did my Ph.D. research under the supervision of Professor dr. Robert Tijdeman at Leiden University which resulted this thesis.
Starting from 1st February 2005 I return to the University of Debrecen (Hungary) to be employed as a lecturer.