universität wien

BACHELORARBEIT

Titel der Bachelorarbeit

Diophantine Equations
and
the Problem of Catalan

Verfasser

Levi Anton Haunschmid

angestrebter akademischer Grad

Bachelor of Science (BSc.)

Wien, im Monat Juli 2018

Studienkennzahl lt. Studienblatt:	A 033621
Studienrichtung lt. Studienblatt:	Mathematik
Betreuer:	Assoz.-Prof. Privatdoz. Dr. Dietrich Burde

Abstract

The Problem of Catalan was a long standing conjecture concerning a diophantine equation, which was recently proved by Preda Mihăilescu using methods from Algebraic Number Theory. After some general remarks on diophantine equations and a brief historical overview this thesis takes a look at several steps of the proof and provides a sketch of the entire proof.

Contents

1 Introduction 1

2 Diophantine Equations 1

3 Historical Overview 3

4 Mathematical Prerequisites 4

4.1 The ring of integers in a number field 4

4.2 Cyclotomic Fields 5

4.3 The Group Ring 7

5 Cassels' Relations 9

6 Results by Inkeri and Mihăilescu 13

6.1 An important algebraic integer 13

6.2 Higher Divisibility 13

7 Sketch of the Proof 16

7.1 The case q divides p-1 16

7.2 The case q does not divide p-1 17

References 23

1 Introduction

Diophantine problems have motivated many advances in number theory. To the recent breakthrough of Wiles, solving the famous Fermat Problem, Mihăilescu added another old Diophantine problem which was finally solved: The Problem of Catalan. This thesis takes a look at the methods used in this proof and gives a partial reproduction.

The brief historical overview in section 3 focuses on the partial results which became a part of the final proof.

Results used from algebra and algebraic number theory which are not covered in the curriculum of the bachelor's degree in mathematics at the University of Vienna are collected in section 4.

In sections 5 and 6 proofs of some results due to Cassels, Inkeri and Mihăilescu are given. In section 7 the proof is sketched. While for some steps proofs are given, others are only described or justified by citations.

Mihăilescu's proof of the problem of Catalan was published in the articles (Mihăilescu 2003) and (Mihăilescu 2004). Major resources also were the book (Bilu et al. 2014) as well as the doctoral thesis (Daems 2003) and the excellent article (Metsänkylä 2003).

2 Diophantine Equations

Diophantine equations are equations, most of the time in several variables, in which one is interested in solutions in the integers or the rationals. That is for a function $f\colon \mathbb{Z}^n \to \mathbb{Z}$ solutions $(x_1, x_2, \ldots, x_n)$ of

$$f(x_1, x_2, \ldots, x_n) = 0$$

are sought.

Sometimes a Diophantine equation in which one of the variables appears in an exponent is called an exponential Diophantine equation.

There are several general questions asked about a given Diophantine equations:

1) Do solutions exist?

2) Is it decidable whether or not solutions exist?

3) How many solutions are there?

4) What structure do the solutions have?

In general 2) has a negative answer. Hilbert's tenth problem asked whether there was an algorithm deciding the solvability of a Diophantine equation (considering only polynomial functions f). In 1970 it was proved in (Matijasevič 1973) that such an algorithm does not generally exists. This result belongs more to the area of logic than to number theory.

One classical example of a Diophantine equation is the equation of Pythagorean triples:
Example 2.1 (Pythagorean Triples).

$$a^2 + b^2 = c^2.$$

Here the answer to questions 1) and 2) is positive and there are infinitely many solutions. The structure is also well understood, as there is a standard parametrization of the Pythagorean triples.

Another example with an infinite number of solution with a less well understood structure are elliptic curves:
Example 2.2 (Elliptic Curves).

$$y^2 = x^3 + ax + b,$$

where a, b are rational constants and rational solutions x, y are considered.

These curves played an important role in Wiles proof of Fermat's Last Theorem and are also very important for number theory in general.

Fermat's Last Theorem is probably the most well known Diophantine Problem. It states that there are no solutions to:
Example 2.3 (Fermat's equation).

$$x^n + y^n = z^n, \text{ where } n \geq 3.$$

Much of the theory used in this thesis was developed by Kummer while working on this problem.

The problem the remainder of this thesis focuses on is a conjecture by Belgian mathematician Catalan in 1842, that the only solution to
Example 2.4 (Catalan's equation).

$$x^m - y^n = 1, \text{ where } m, n \geq 2 \text{ and } x, y \geq 1$$

is $3^2 - 2^3 = 1$. Or put in words: There are no consecutive integers which are pure powers, except 8 and 9. This problem remained unanswered for over 150 years until the conjecture was proved by Preda Mihăilescu in 2002. His proof is the topic of this thesis.

3 Historical Overview

Catalan first stated the problem in 1842 in a list of problems and problems in the first volume of the journal *Nouvelles Annales de Mathématiques*. In 1944 in a letter by Catalan published in the *Journal für reine und angewandte Mathematik*, he wrote that he could not prove it completely so far. It does not seem like he had proved any serious partial results either.

Before taking a look at the further history of Catalan's problem a slight reformulations is necessary: Since m and n are both larger than 1, each has a prime divisor. Denote by p a prime divisor of m and by q a prime divisor of n. Then we have:

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

Thus the existance of a solution of the equation in the previous chapter implies the existance of a solution to the following equation:

Definition 3.1 (Catalan's equation)**.**

$$x^p - y^q = 1, \textit{ where } p, q \textit{ are prime and } x, y \geq 1.$$

If $p = q$ and $x^p - y^q > 1$, then $x^p - y^q > (y+1)^p - y^p > 2^p - 1 > 1$, thus we can also assume p and q to be distinct. This is the equation which will referred to as "Catalan's equation" in the following.

The case $p = 2$ and $q = 3$ was already known before Catalan stated the conjecture. It was proved by Euler (Euler 1915). In fact he proved that the equation $x^2 - y^3 = 1$ has no rational solution except $(0, -1), (\pm 1, 0)$ and $(\pm 3, 2)$. From a modern point of view his result can be interpreted as being about the rational points on the elliptic curve defined by this equation.

The case $q = 2$ was solved by Victor Lebesgue[1], see (Lebesgue 1850).

The case $p = 2$ and $q > 3$ was solved by Ko Chao in (Chao 1964). This completed the even cases (i.e. where either p or q is 2), which is relevant as Mihăilescu's proof does not cover them.

[1] Victor Amédée Lebesgue, not the more famous Henri Léon Lebesgue

In (Tijdeman 1976) Tijdeman proved that there were only finitely many solutions of Catalan's equation using the theory of logarithmic forms, specifically Bakers method. In fact he could even give an explicit bound for the size of the solutions:

$$|x^m|, |y^n| < 10^{10^{10^{10^{320}}}}$$

While this was of course far out of range of calculations, it proved for the first time that Catalan's Problem was decidable.

Refinements of the method gave better bounds, the best of which is an upper bound for $\max\{p, q\}$, which is about $8 \cdot 10^{16}$. However the bounds given by this method were still far beyond of what is possible to check by calculation.

In 1960 Cassels published results now called *Cassels Relations*, which became the starting point of further work (Cassels 1960). These results are presented in section 5.

In 1999 Mihăilescu generalized a result, namely that $q^2|x$, which Inkeri proved in (Inkeri 1990) for regular primes q, to all primes p and q (Mihăilescu 2003). This is the second part of chapter 5.

Mihăilescu finally proved the conjecture in 2002. This proof will be sketched in section 7.

4 Mathematical Prerequisites

4.1 The ring of integers in a number field

In this section important results of algebraic number theory will be presented without proofs. Proofs can be found in most algebraic number theory lecture notes or in (Lang 1965), (Lang 1994) and (Washington 1982).

In algebraic number theory one investigates *algebraic integers*, which are an analogue to the integers in finite field extensions of $\mathbb{Q}$.

Definition 4.1. *A number field is a finite field extension of* $\mathbb{Q}$.

Definition 4.2. *Let $A \subset B$ be an extension of commutative rings. An element $x \in B$ is called* integral *over A if there is a monic polynomial f with coefficients in A such that $f(x) = 0$.*

In the context of this thesis A will always be $\mathbb{Z}$ and B will be a number field. An important result concerning integral elements is:

Theorem 4.3. *Let $A \subset B$ be an extension of commutative rings. Then the elements in B which are integral of A form a ring, called the ring of integers in B over A or the integral closure of A in B.*

There are two proofs commonly found in books and lecture notes on algebraic number theory. On uses elementary symmetric polynomials and the other due to Dedekind uses finitely generated modules.

Definition 4.4. *A ring A is called* integrally closed *if the integral closure of A in the field of fractions of A is A.*

Now we can define algebraic integer:

Definition 4.5. *Let K be a finite field extension of $\mathbb{Q}$. The integral elements in K over $\mathbb{Z}$ are called the ring of algebraic integers in K, denoted by O_K.*

Important properties of O_K are collected in the definition of a Dedekind domain:

Definition 4.6. *A Dedekind domain is an integral domain, which is Noetherian, integrally closed and in which every nonzero prime ideal is maximal.*

Dedekind domain are exactly those in which factorization of ideals into prime ideals works:

Theorem 4.7. *In a Dedekind domain every nonzero Ideal factors uniquely (up to reordering) into prime ideals.*

This is very useful because:

Theorem 4.8. *The ring of integers in a number field is a Dedekind domain.*

This is the main result of algebraic number theory we will be using. - In this context the concept of an ideal is extended to that of an fractional ideal:

Definition 4.9. *A subset I of a commutative ring R is a fractional ideal of R if there is an element $b \in R$ such that bI is an ideal of R.*

The "fractional" is often omitted. With this definition the fractional ideals of a number field form a group. The principal ideals form a subgroup of this group.

Definition 4.10. *The class group of a number field K is the factor group of the group of fractional ideals modulo the principal ideals, it is denoted H_K or simply H.*

Theorem 4.11. *The class group of a number field K is finite, it's size is called the class number of K, sometimes denoted as h_k.*

4.2 Cyclotomic Fields

The number fields used in Mihăilescu's proof are the cyclotomic fields. The are generated by adjoining a n-th root of unity ζ to $\mathbb{Q}$. One can choose $e^{\frac{2\pi i}{n}}$ to get a specific embedding into $\mathbb{C}$.

The minimal polynomial of ζ is called the n-th cyclotomic polynomial and denoted by Φ_n. We have:

$$\Phi_n(x) = \prod_{\substack{1\le i\le n \\ \gcd(n,i)=1}} (x-\zeta^i).$$

For a prime p this simplifies to:

$$\Phi_p(x) = \frac{x^p-1}{x-1} = \sum_{i=0}^{p-1} x^i.$$

From now on we will work mostly in the field $\mathbb{Q}[\zeta]$, where ζ is p-th root of unity and p is prime. The ring of algebraic integers in $\mathbb{Q}[\zeta]$ is exactly what one would expect:

Theorem 4.12. *The ring of algebraic integers in $\mathbb{Q}[\zeta]$ is $\mathbb{Z}[\zeta]$.*

This ring has some special units:

Lemma 4.13. *The elements of the form $\frac{1-\zeta^i}{1-\zeta^j}$ where i and j are integers not divisible by p, are units in $\mathbb{Z}[\zeta]$.*

Proof. It is sufficient to proof that $\frac{1-\zeta^i}{1-\zeta^j}$ is indeed in $\mathbb{Z}[\zeta]$ for general i and j. Then it's inverse $\frac{1-\zeta^j}{1-\zeta^i}$ is also in $\mathbb{Z}[\zeta]$ and thus they are both units.

Now as p does not divide j and they are therefore coprime, there are $m,n\in\mathbb{Z}$ such that $mp+nj=i$. Now:

$$\frac{1-\zeta^i}{1-\zeta^j} = \frac{1-\zeta^{mp+nj}}{1-\zeta^j} = \frac{1-(\zeta^j)^n}{1-\zeta^j} = \sum_{i=0}^{p-1}(\zeta^j)^n \in \mathbb{Z}[\zeta]$$

□

The elements in the subgroup generated by these units are called cyclotomic units. It is denoted by C.

Because of this lemma the ideals $(1-\zeta^i)$ for $i=1,\dots,p-1$ are equal. Because

$$p = \Phi_p(1) = \prod_{i=1}^{p-1}(1-\zeta^i)$$

the ideal (p) decomposes in $\mathbb{Z}[\zeta]$ as $(p) = (1-\zeta)^{p-1}$.

4.3 The Group Ring

Throughout this section p and q are distinct primes larger than 2. As always ζ is a p-th root of unity.

An algebraic object that plays a central role in Mihăilescu's proof is the group ring:

Definition 4.14. *Given a commutative ring R and group G the formal linear combinations*

$$\sum_{\sigma \in G} a_\sigma \sigma$$

with coefficients $a_\sigma \in R$, only finitely of which are nonzero form a ring with component-wise addition and the following multiplication:

$$\left(\sum_{\sigma \in G} a_\sigma \sigma \right) \left(\sum_{\sigma \in G} b_\sigma \sigma \right) = \sum_{\sigma \in G} \sum_{\tau_1 \tau_2 = \sigma} a_{\tau_1} b_{\tau_2} \sigma.$$

This ring is called the group ring and denoted $R[G]$.

Note that the group ring is commutative if and only if the group G is commutative.

In this thesis the group G will always be either the Galois group of the field extension $\mathbb{Q}[\zeta]/\mathbb{Q}$ or the Galois group of $\mathbb{Q}[\zeta + \bar{\zeta}]/\mathbb{Q}$ which will be denoted by G^+. Since both of these groups are abelian, the group rings will be commutative. They are also both finite, therefore the condition that only finitely many a_σ are nonzero is irrelevant here.

The elements of G can be written as $\{\sigma_1, \sigma_2, \dots, \sigma_{p-1}\}$, where σ_i is the Galois reflection which maps ζ to ζ^i. Thus the elements of $R[G]$ can be written as $\sum_{i=0}^{p-1} n_i \sigma_i$. The Galois reflection σ_1 is the identity of R and will also be written as 1. The Galois reflection σ_{p-1} is complex conjugation and will be written as ι.

The ring R will always be $\mathbb{Z}, \mathbb{Q}$ or $\mathbb{F}_q$, where $\mathbb{F}_q$ is the field with q elements.

Let $\mathbb{Z}[G]$ act on $\mathbb{Q}[\zeta]$ in the following way:

For $\theta = \sum_{i=0}^{p-1} n_i \sigma_i$ and $x \in \mathbb{Q}[\zeta]$ define

$$x^\theta := \prod_{i=1}^{p-1} \sigma_i(x)^{n_i}.$$

We write this operation exponentially because it satisfies:

$$x^{\theta_1 + \theta_2} = x^{\theta_1} x^{\theta_2} \text{ and } (x^{\theta_1})^{\theta_2} = x^{\theta_1 \theta_2}, \text{ for } x \in \mathbb{Q}[\zeta], \theta_1, \theta_2 \in \mathbb{Z}[G]$$

Using this group action we can consider multiplicative abelian groups closed under Galois reflections as $\mathbb{Z}[G]$ modules. These include the multiplicative group of $\mathbb{Q}[\zeta]$, the group of units in $\mathbb{Z}[\zeta]$, the group of ideals and the group of principal $\mathbb{Z}[\zeta]$ ideals. Because of the latter two the class group H of $\mathbb{Q}[\zeta]$ is also a $\mathbb{Z}[G]$ module.

We say that an element $\theta \in \mathbb{Z}[G]$ annihilates a $\mathbb{Z}[G]$ module if x^θ is the neutral element for all x in the module. For example $\theta \in Z[G]$ annihilates the H if for every ideal $\mathfrak{a}$ the ideal $\mathfrak{a}^\theta$ is a principal ideal.

Now we can state Stickelberger's theorem. First we define the Stickelberger element and the Stickelberger ideal.

Definition 4.15. *The Stickelberger element $\theta_S \in \mathbb{Q}[G]$ is defined as follows:*

$$\theta_S \coloneqq \sum_{a=1}^{p-1} \frac{a}{p} \sigma_a^{-1}.$$

Definition 4.16. *The Stickelberger ideal is defined as:*

$$I_S \coloneqq \mathbb{Z}[G] \cap \theta_S \mathbb{Z}[G]$$

Theorem 4.17 (Stickelberger)**.** *The Stickelber Ideal is generated by the elements θ_c, where*

$$\theta_c \coloneqq \sum_{a=1}^{p-1} \left\lfloor \frac{ac}{p} \right\rfloor \sigma_a^{-1}$$

and it annihilates the H.

For a proof see (Washington 1982, chapter 6).

This theorem gives us a number of nontrivial annihilators of the class group which will be used in chapter 5.

If we have a $\mathbb{Z}[G]$ module M such that for all $x \in M$ we have $x^q = 1$, i.e. $q \in \mathbb{Z}[G]$ annihilates M, then it is also an $\mathbb{F}_q[G]$ module. To see this take two different elements θ_1 and θ_2 of $\mathbb{Z}[G]$ such that $q | \theta_1 - \theta_2$. Then we have for all $x \in M$:

$$x^{\theta_1} = x^{\theta_2} x^{\theta_1 - \theta_2} = x^{\theta_2} (x^q)^{(\theta_1 - \theta_2)/q} = x^{\theta_2}.$$

Some simple examples of such modules are $\mathbb{Q}[\zeta]^\times / (\mathbb{Q}[\zeta]^\times)^q$ or E/E^q, where E is the group of units in $\mathbb{Z}[\zeta]$.

An important property of $\mathbb{F}_q[G]$ used in Mihăilescu's proof is that $\mathbb{F}_q[G]$ is semisimple if $q \nmid p-1$. For commutative rings semisimplicity is equivalent to being a finite product of fields.

Lemma 4.18. *If $q \nmid p-1$, the group ring $\mathbb{F}[G]$ is a finite product of finite fields.*

Proof. G is isomorphic to the multiplicative group of the ring $\mathbb{Z}/p\mathbb{Z}$ and thus is cyclic. Therefore it has a generator σ, which satisfies $\sigma^{p-1} = 1$ and $\sigma^i \neq 1$ for $1 < i < p-1$. Furthermore the σ^i are linearly independent over $\mathbb{F}_q$. We can write every element of the ring $\mathbb{F}_q[G]$ uniquely as $\sum_{i=1}^{p-1} n_i\sigma^i$.

Thus the map from $\mathbb{F}_q[X]$ to $\mathbb{F}_q[G]$ which maps X to σ is surjective and has kernel $(X^{p-1}-1)$. This induces an isomorphism between $\mathbb{F}_q[X]/(X^{p-1}-1)$ and $\mathbb{F}_q[G]$.

Because $q \nmid p-1$ the derivative of $X^{p-1}-1$, which is $(p-1)X^{p-2}$, does not vanish in $\bar{\mathbb{F}_q}$. Therefore $X^{p-1}-1$ is separable and we get:

$$\mathbb{F}_q[X]/(X^{p-1}-1) \cong \prod_g \mathbb{F}_q[X]/(g(X)),$$

where g are the irreducible polynomials that divide $X^{p-1}-1$. □

This holds in larger generality, it is still true if G is any group of finite order and $\mathbb{F}_q$ is replaced by any field whose characteristic does not divide the order of G, see (Lang 1965, p.666).

Elements of the group ring have *weight* and *size*:

Definition 4.19. *The weight $w(\theta)$ of an element θ of the group ring is defined as:*

$$w(\theta) = w\left(\sum_{i=0}^{p-1} n_i\sigma_i\right) := \sum_{i=0}^{p-1} n_i.$$

Notice that w is a ring homomorphism from $\mathbb{Z}[G]$ to $\mathbb{Z}$. The kernel of this homomorphism is called the augmentation ideal. The elements of an Ideal of weight zero again form an ideal, which is called the augmented part of that ideal.

Definition 4.20. *The size $\|\theta\|$ is defined as:*

$$\|\theta\| = \left\|\sum_{i=0}^{p-1} n_i\sigma_i\right\| := \sum_{i=0}^{p-1} |n_i|.$$

5 Cassels' Relations

The start of the modern analysis of Catalan's Problem was (Cassels 1960). In it he proved what has become known as Cassels' relations In this section a partial proof of these results is given.

First we need some preparations:

Let (x, y, p, q) be a solution of Catalan's equation, where x and y are positive integers and p and q are prime. The primes p and q are distinct, as it is easy to see that $x^n - y^n \neq 1$ for $y \leq 1$.

As mentioned earlier this thesis does not deal with the even cases so from now on p and q are odd. This allows us to symmetrize the problem if we allow all nonzero integer values for x and y: If (x, y, p, q) is a solution so is $(-y, -x, q, p)$. Indeed:

$$(-y)^q - (-x)^p = -y^q + x^p = x^p - y^q = 1.$$

Now the problem is symmetric in p and q.

To proof Cassels' relations we need the following lemma:
Lemma 5.1. *Let $x \neq 1$ be an integer and p prime larger than 2, then*

$$\gcd\left(\frac{x^p - 1}{x - 1}, x - 1\right) \in \{1, p\}.$$

Moreover if the gcd is p then $p^2 \nmid \frac{x^p-1}{x-1}$.

Proof. We can write $\frac{x^p-1}{x-1}$ as a geometric series:

$$\frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i \equiv \sum_{i=0}^{p-1} 1 \equiv p \pmod{x - 1}.$$

Thus the gcd divides p, which means it must be either p or 1. For the second part of the lemma we use the Binomial Theorem:

$$\frac{x^p - 1}{x - 1} = \frac{(x - 1 + 1)^p - 1}{x - 1} = \sum_{k=1}^{p} \binom{p}{k} (x - 1)^{k-1} \equiv p \pmod{p^2}.$$

In the last step all but the last term vanish because $p|x - 1$ and $p|\binom{p}{2}$. □

To use this lemma we rearrange Catalan's equation:

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

We also need some analytic estimates:
Lemma 5.2. *For $x, \alpha \in \mathbb{R}$ with $|x| < 1$. Then*

$$|(1 + x)^\alpha - 1| \leq \max\{1, (1 + x)^{\alpha-1}\}|x||\alpha|.$$

Proof. We use Taylor's Theorem with the error term given by the intermediate value theorem and expand only to the first term:

$$(1+x)^\alpha = 1 + \alpha(1+\xi)^{\alpha-1}\xi, \text{ for some } \xi \text{ between 0 and } x.$$

Using this we get:

$$|(1+x)^\alpha - 1| = |\alpha(1+\xi)^{\alpha-1}\xi| \leq |(1+\xi)^{\alpha-1}||\xi||\alpha| \leq \max\{1, (1+x)^{\alpha-1}\}|x||\alpha|.$$

□

The max in this lemma is 1 if and only if $x \geq 0$ and $\alpha \leq 1$ or $x \leq 0$ and $\alpha \geq 1$

Now we are ready for Cassels' Theorem:

Theorem 5.3 (Cassel)**.** *Let (x, y, p, q) be a solution of Catalan's equation. Then $p|y$.*

Proof. We follow the proof given in (Bilu et al. 2014). Cassels' original proof uses the same ideas, but different estimates in some places.

Because of Lemma 4.1. we only need to prove that gcd $\left(\frac{x^p-1}{x-1}, x-1\right)$ is never 1. In this case both $x-1$ and $\frac{x^p-1}{x-1}$ must be q-th powers, as they are coprime and their product is y^q. We define $a \in \mathbb{Z}$ such that $x - 1 = a^q$. Because $x = 0$ is not allowed and $x = 1, 2$ can easily be checked to offer no solutions $|a| > 1$ Now we can rewrite Catalan's equation as follows:

$$x^p - y^q = 1 \iff (a^q + 1)^p = y^q + 1$$

From this we see that y and a^p should be close together

Cassels' proof makes a distinction between the cases $p < q$ and $p > q$. We start with the simpler case $p < q$.

To use Lemma 4.2. we rewrite Catalans equation again:

$$(a^q+1)^p = y^q + 1 \Leftrightarrow (a^q+1)^{\frac{p}{q}} = (y^q+1)^{\frac{1}{q}} \Leftrightarrow a^p(1+a^{-q})^{\frac{p}{q}} = y(1+y^{-q})^{\frac{1}{q}}.$$

Now we can use Lemma 4.2.:

$$|1 - (1+a^{-q})^{\frac{p}{q}})| \leq \max\{1, (1+a^{-q})^{\frac{p}{q}-1}\}|a|^{-q}\frac{p}{q} \leq (1-|a|^{-q})^{\frac{p}{q}-1}|a|^{-q}$$

From this we get because of $|a| > 1$, $p - q \leq -2$ (since they are distinct primes larger than 2) and $p < q$:

$$|a^p - a^p(1 + a^{-q})^{\frac{p}{q}}| \leq |a|^{p-q}(1 - |a|^{-q})^{\frac{p}{q}-1} \leq 2^{-2}(1 - 2^{-5})^{-1} < 1/3.$$

Again by Lemma 4.2.:

$$|1 - (1 + y^{-q})^{\frac{1}{q}}| \leq \max\{1, (1 + y^{-q})^{\frac{1}{q}-1}\}|y|^{-q}\frac{1}{q} \leq (1 - |y|^{-q})^{-1}|y|^{-q}1/q,$$

which we use to estimate $|y - y(1 + y^{-q})^{\frac{1}{q}}|$, using $|y| > 1$, which can be easily checked:

$$|y - y(1 + y^{-q})^{\frac{1}{q}}| \leq (1 - |y|^{-q})^{-1}|y|^{1-q}\frac{1}{q} < (1 - 2^{-5})^{-1}2^{-4}\frac{1}{5} < 1/3.$$

Putting together the estimates yields:

$$\begin{aligned}|a^p - y| = |a^p - a^p(1 + a^{-q})^{\frac{p}{q}} + y(1 + y^{-q})^{\frac{1}{q}} - y| \leq \\ \leq |y - y(1 + y^{-q})^{\frac{1}{q}}| + |a^p - a^p(1 + a^{-q})^{\frac{p}{q}}| < 2/3.\end{aligned}$$

Because both a^p and y are integers this implies $a^p = y$ and therefore $x^p - y^q = x^p - a^{pq}$, but as noted before two powers of the same exponent cannot have difference one therefore we have reached a contradiction.

The second case works in a similar way but uses more intricate estimates. The Taylor series expansion with more terms as well as some estimates involving the p-adic value of binomial coefficients are used. For a detailed version see either the article by Cassel or the book (Bilu et al. 2014).

□

From this theorem the Cassels' Relations follow:
Korollar 5.4. *Let (x, y, p, q) be a solution of Catalan's equation. Then there are $a, u \in \mathbb{Z}$, such that:*

$$x - 1 = p^{q-1}a^q, \quad \frac{x^p - 1}{x - 1} = pu^q, \quad \text{and } y = pau,$$

where p does not divide u, but may divide a.

Proof. From the theorem above and the second part of Lemma 4.1. it follows that the multiplicity of p in $\frac{x^p-1}{x-1}$ is 1 and that $\frac{x-1}{p^{q-1}}$ and $\frac{x^p-1}{p(x-1)}$ are coprime and thus q-th powers, respectively called a^q and u^q. Their product y^q is then $p^q a^q u^q$ an thus the last relation follows. □

6 Results by Inkeri and Mihăilescu

6.1 An important algebraic integer

Let (x, y, p, q) be a solution of Catalan's equation. In the previous chapter it was proved that:

$$\frac{x^p - 1}{x - 1} = pu^q,$$

for some $u \in \mathbb{Z}$.

The left-hand side of this equation is the p-th cyclotomic polynomial $\Phi_p(x)$, while the p on the right-hand side can be expressed as $\Phi(1)$. Using the standard factorization for Φ we get:

$$\frac{\Phi(x)}{\Phi(1)} = \prod_{i=1}^{p-1} \frac{x - \zeta^i}{1 - \zeta^i} = u^q.$$

Defining $\lambda_i = \frac{x-\zeta^i}{1-\zeta^i}$ this product has the form $\prod_{i=1}^{p-1} \lambda_i = u^q$. The λ_1 is an algebraic integers as $(1 - \zeta)|p|x - 1$ and thus $(1 - \zeta)|(x - 1) - (1 - \zeta)$. The λ_i are all conjugates of each other and thus are algebraic integers too. The λ_i are also pairwise coprime:

$$\frac{1 - \zeta^j}{\zeta^k - \zeta^j}\lambda_j - \frac{1 - \zeta^k}{\zeta^k - \zeta^j}\lambda_k = \frac{(x - \zeta^j) - (x - \zeta^k)}{\zeta^k - \zeta^j} = 1, \text{ for } i \neq j.$$

This is a valid linear combination in $\mathbb{Z}[\zeta]$, as the coefficients on the left are cyclotomic units and therefore in $\mathbb{Z}[\zeta]$, as proved in the Prerequisites section.

Since $\mathbb{Z}[\zeta]$ is not always a unique factorization domain, this does not mean that the λ_i are q-th powers, but because it is a Dedekind domain it does mean that the ideals (λ_i) are q-th powers of ideals.

6.2 Higher Divisibility

In his first paper (Mihăilescu 2003) on the Catalan equation Mihăilescu showed that $q^2|x$ for any solution (x, y, p, q) (and by symmetry $p^2|y$). This was already proved by Inkeri in (Inkeri 1990), for regular primes, i.e. for primes p such that the class number of $\mathbb{Q}[\zeta]$ is not divisible by p. In Mihăilescu paper there is no such class number conditions.

First we need the following lemma to go from divisibility by q to divisibility by q^2.

Lemma 6.1 (Lifting the Exponent)**.** *The ring $\mathbb{Z}[\zeta]/(q)$ contains no nilpotent elements. Further if $\alpha, \beta \in \mathbb{Z}[\zeta]$ satisfy $\alpha^q - \beta^q \equiv 0 \pmod q$ they also satisfy $\alpha^q - \beta^q \equiv 0 \pmod{q^2}$*

Proof. Because p is the only ramified prime in $\mathbb{Q}[\zeta]$ the ideal (q) factorises as $\mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdots \mathfrak{q}_r$, for some distinct prime ideals $\mathfrak{q}_1, \mathfrak{q}_2, \dots \mathfrak{q}_r$. Now by the chinese remainder theorem we get:

$$\mathbb{Z}[\zeta]/(q) \cong \mathbb{Z}[\zeta]/\mathfrak{q}_1 \times \mathbb{Z}[\zeta]/\mathfrak{q}_2 \times \cdots \times \mathbb{Z}[\zeta]/\mathfrak{q}_r.$$

Because the $\mathfrak{q}_i$ are prime none of the $\mathbb{Z}[\zeta]/\mathfrak{q}_i$ contain nilpotent elements as they are integral domains. Thus their product also contains no nilpotent elements.

Let $\alpha, \beta \in \mathbb{Z}[\zeta]$ satisfy $\alpha^q - \beta^q \equiv 0 \pmod q$. Then we have, by the Frobenius endomorphism:

$$(\alpha - \beta)^q \equiv \alpha^q - \beta^q \equiv 0 \pmod q.$$

And thus $\alpha = \beta + kq$ for some $\in \mathbb{Z}[\zeta]$. Now we can expand α^q:

$$\alpha^q = (\beta + kq)^q = \sum_{i=0}^{q} \binom{q}{i} \beta^{q-i} (kq)^i \equiv \beta^q \pmod{q^2}.$$

This concludes the proof of the lemma.

□

The second part of the lemma is a special case of the "Lifting the Exponent Lemma", a variation of which we already used when proving Cassels' Relations.

We need another small preparatory lemma:

Lemma 6.2. *Let $\alpha \in \mathbb{Z}[\zeta]$ be such that all conjugates of α have absolute value* 1*. Then α is a root of unity.*

Proof. Consider the polynomials

$$f_m(x) := \prod_{\sigma \in G} (x - \sigma(\alpha^m).$$

Their coefficients are integers bounded by $\binom{n}{k} \leq 2^n$ and thus these are finitely many polynomials f_m. This implies that there are only finitely many powers of α which can only be the case if α is a root of unity. □

The proof uses the non-trivial annihaltors given by Stickelbergers Theorem. Define $I_S^- := (1-\iota)I_S$, called the relative part of Stickelberger's Ideal.
Lemma 6.3. *For every $\theta \in I_S^-$, $(x-\zeta)^\theta$ is a q-th power.*

Proof. Let $\theta = (1-\iota)\theta'$ and $\lambda = \frac{x-\zeta}{1-\zeta}$ as in the previous section. Then

$$(x-\zeta)^{(1-\iota)\theta'} = \left(\frac{x-\zeta}{x-\overline{\zeta}}\right)^{\theta'} = \left(\frac{1-\zeta}{1-\overline{\zeta}}\right)^{\theta'} \left(\frac{\lambda}{\overline{\lambda}}\right)^{\theta'}.$$

As θ' annihilates the class group and (λ) is a q-th power of an ideal, $\lambda^{\theta'} = \epsilon\alpha^q$ for some unit ϵ and some $\alpha \in \mathbb{Q}[\zeta]$. Using this we get:

$$(x-\zeta)^{(1-\iota)\theta'} = \left(\frac{1-\zeta}{1-\overline{\zeta}}\right)^{\theta'} \frac{\epsilon}{\overline{\epsilon}} \left(\frac{\alpha}{\overline{\alpha}}\right)^q.$$

Both $\left(\frac{1-\zeta}{1-\overline{\zeta}}\right)$ and $\frac{\epsilon}{\overline{\epsilon}}$ are q-th powers. The first one is $-\zeta$, which is a q-th power because -1 is and all p-th roots of unity are q-th powers. The second one is a root of unity because of the second preparatory lemma.

Thus $(x-\zeta)^\theta$ is a q-th power. □

Now we can proof Mihăilescu's result:
Theorem 6.4. *Let (x,y,p,q) be a solution of Catalan's problem with p and q odd primes. Then $q^2|x$ (and by symmetry $p^2|y$).*

Proof. Let θ be in I_S^-. Since $(1-\overline{\zeta})^\theta$ is equal to $((-\overline{\zeta})(x-\zeta))^\theta$ it is equalt to $(x-\zeta)^\theta$ times a root of unity and therefore also a q-th power. Let us say $(x-\zeta)^\theta = a^q$.

Using Cassels' theorem that $q|x$, we find that $a^q \equiv 1 \pmod{q}$. Because of 6.1 we obtain $a^q \equiv 1 \pmod{q^2}$.

$$\begin{aligned}1 \equiv (1-\overline{\zeta}x)^{\theta} &= \prod_{\sigma\in G}(1-\sigma(\overline{\zeta})x)^{n_\sigma}\\ &\equiv \prod_{\sigma\in G}(1-n_\sigma\sigma(\overline{\zeta})x)\\ &\equiv 1 - x\sum_{\sigma\in G} n_\sigma\sigma\overline{\zeta} \pmod{q^2}.\end{aligned}$$

Thus $x\sum_{\sigma\in G} n_\sigma\sigma\overline{\zeta} \equiv 0 \pmod{q^2}$. Thus either $q^2|x$ or $q|\sum_{\sigma\in G} n_\sigma\sigma\overline{\zeta}$, which would imply $q|n_\sigma$ for all σ. There are however elements of I_S^- which are not divisible by q. For example $(1-\iota)\theta_2 = (1-\iota)\sum_{i=\frac{p-1}{2}}^{p-1}\sigma_i^{-1}$. Using this as θ we get $q^2|x$. □

Revisiting Cassels' Relations now gives further information: From $x-1 = p^{q-1}a^q$ it follows by $q|x$ that $p^{q-1}a^q \equiv -1 \pmod q$. As $p^{q-1} \equiv 1 \pmod q$, we get $a^q \equiv -1 \pmod q$ and by Lifting the Exponent: $a^q \equiv -1 \pmod{q^2}$.

Now that we also have $q^2|x$ from $p^{q-1}a^q \equiv -1 \pmod{q^2}$ and thus $p^{q-1} \equiv 1 \pmod{q^2}$. By symmetry we get:

$$p^{q-1} \equiv 1 \pmod{q^2}, \qquad q^{p-1} \equiv 1 \pmod{p^2}.$$

Primes satisfying these conditions are called double Wieferich pairs, they first appeared in the study of the Fermat Problem. There are only five known double Wieferich pairs and it is known that there are no other double Wieferich primes with $\min\{p,q\} \leq 3.2\times 10^8$. It is an open problem whether or not infinitely many double Wieferich pairs exist.

7 Sketch of the Proof

In this section the remainder of the proof will be outlined. Some partial results will be proved, for a complete presentation of the proof see (Bilu et al. 2014), (Lorenz 2008) or (Daems 2003).

Mihăilescu's proof splits the problem into two cases: $q|p-1$ and $q\nmid p-1$.

7.1 The case q divides p-1

In this case the first proof of Mihăilescu proceeded as follows:

If $q|p-1$ then $p \equiv 1 \pmod{q}$ and by the Lifting the Exponent Lemma $p^q \equiv 1 \pmod{q^2}$. But we also have $p^q \equiv p \pmod{q^2}$ from the Wieferich Conditions and thus $p \equiv 1 \pmod{q^2}$. Because q^2+1 and $3q^2+1$ are even and $2q^2+1$ is divisible by three, it follows that $p > 4q^2$.

From the theory of logarithmic form mentioned in the historic overview however it follows that $p < 4q^2$, whenever $q > 28000$. This reduced this case to a very manageable calculations, carried out easily by a computer. Before Mihăilescu's proof the conjecture had already been checked for much larger exponents (see (Bilu 2002)).

Later Mihăilescu published in (Mihăilescu 2006) a different proof of this case, without logarithmic forms which therefore also needed no computer calculations.

This proof uses Stickelberger's Theorem together with some estimates about Mihăilescu's Ideal, defined as all elements θ of $\mathbb{Z}[G]$ such that $(x-\zeta)^\theta$ is a q-th power, i.e. $(x-\zeta)^\theta \in (\mathbb{Q}[\zeta])^q$. It is denoted by I_M. The augmented part of of Mihăilescu's Ideal is defined as all elements I_M of weight 0 and is denoted by I_M^{aug}.

The relative part of Stickelberger's Ideal $I_S^- := (1-\iota)I_S$ is a subset of Mihăilescu's Ideal because $(x-\zeta)^\theta$ is a q-th power for all $\theta \in I_S^-$, as was shown in the previous section. Further by multiplicativity of the weight function and $w(1-\iota) = 1-1 = 0$, all Elements of I_S^- have weight 0. Thus $I_S^- \subset I_M^{\text{aug}}$.

The contradiction is achieved by estimating the number of elements of I_M^{aug} and I_S^- of or below a certain size r denoted by $I_M^{\text{aug}}(r)$ and $I_S^-(r)$ respectively.

As the structure of Stickelberger's Ideal is relatively well understood lower bounds for $|I_S^-(r)|$ can be obtained by simple combinatorical arguments.

To get an upper bound for $I_M^{\text{aug}}(r)$, the elements $\alpha(\theta)$ such that $\alpha(\theta)^q = (x-\zeta)^\theta$ as well as $\xi(\theta)$, defined as the nearest root of unity to $\alpha(\theta)$ are analyzed. By an application of the pigeonhole principle and some estimates using heights of algebraic numbers, it is shown that for a specific r, dependent on $p, qandx$ there are at most q elements in $I_M^{\text{aug}}(r)$. For large enough, but not very large, p, q and x, this contradicts the lower bounds for $|I_S^-(r)|$. The small cases do not need computer calculation but are instead excluded by the Hyyrö Estimates which follow from Cassels' relations.

7.2 The case q does not divide p-1

An important step in the second case is the following theorem due to Mihăilescu:

Theorem 7.1. *If $\theta = \sum_{i=1}^{p-1} n_i \sigma_i \in \mathbb{Z}[G]$ is divisible by $(1+\iota)$ and $w(\theta)$ is divisible by q and*

$$(x-\zeta)^{\theta} \in (\mathbb{Q}[\zeta])^q,$$

then $\theta \in q\mathbb{Z}[G]$, i.e. $q|n_i$ for all i.

The assumption that $(1+\iota)$ divides θ essentially means that this is a statement about the real part $\mathbb{Q}[\zeta + \overline{\zeta}]$ (Sometimes also called "plus" part) of the cyclotomic field. This is opposed to the first case and Stickelberger's Theorem which belong to the relative (or "minus") part of the cyclotomic theory.

Because $\mathbb{Q}[\zeta]/(\mathbb{Q}[\zeta])^q$ has the structure of a $\mathbb{F}_q[G]$ module, this statement is equivalent to saying that the only $\theta \in \mathbb{F}_q[G]$ in the augmented part of Mihăilescu's ideal divisible by $(1+\iota)$ is 0. Because the proof will use some estimates it is desirable to stay in $\mathbb{Z}[G]$. However this reformulation means that we can assume the n_i to be between 0 and $q-1$. Additionally because the statement is also symmetric in passing from θ to $-\theta$ the weight of θ can be assumed to be less than $\frac{q(p-1)}{2}$. Define m such that $w(\theta) = mq$.

By assumption there is an α such that $(x-\zeta)^{\theta} = \alpha^q$. We have $\alpha \in \mathbb{Z}[\zeta]$ because we assumed that all n_i to be nonnegative. Now since $w(\theta) = mq$:

$$\left(1 - \frac{\zeta}{x}\right)^{\theta} = \left(\frac{1}{x}\right)^{\theta} (x-\zeta)^{\theta} = \left(\frac{1}{x^{mq}}\right) \alpha^q = \left(\frac{\alpha}{x^m}\right)^q.$$

The technique used to solve the Theorem is known as Runge's method. It consists of showing that a partial sum of a power series is already so close to the result that they must be equal. The power series used will be:

$$F(T) = (1-\zeta T)^{\frac{\theta}{q}} = \prod_{\sigma \in G} (1-\zeta^{\sigma} T)^{\frac{n_\sigma}{q}},$$

where $(1-\zeta^{\sigma}T)^{\frac{n_\sigma}{q}}$ is defined as $\sum_{k \geq 0} \binom{\frac{n_\sigma}{q}}{k} (-\zeta^{\sigma} T)^k$. Because $(1+\iota)$ divides θ this power series has coefficients in $\mathbb{Q}[\zeta + \overline{\zeta}]$ and can be regarded as a real power series. This power series will be used for $T = 1/x$. For this purpose one again needs Hyyrö's estimates to show that $|x|$ is large enough.

Some calculations show that $F(T)$ has the form:

$$F(T) = \sum_{k \geq 0} \frac{a_k}{k! q^k} T^k,$$

where $a_k \equiv (-\sum_{i=1}^{p-1} n_i \zeta^i)^k$.

After using estimates about binomial power series as well as Hyyrö's estimates and

$m \leq \frac{p-1}{2}$ the Runge method is successful: $q^{m+\mathrm{ord}_q(m!)}x^m F_m(1/x) - q^{m+\mathrm{ord}_q(m!)}\alpha$, where F_m is the m-th partial sum of F, is an algebraic integer all of whose conjugates have absolute value less than 1 and therefore is 0.

If $m = 0$ then $\theta = 0$ and we are done. Otherwise we can expand the partial sum:

$$q^{m+\mathrm{ord}_q(m!)}\alpha = \sum_{k=0}^{m} q^{m+\mathrm{ord}_q(m!)} \frac{a_k}{k!q^k} x^{m-k}.$$

The left hand side as well as the first m terms of the sum are algebraic integers divisible by q and therefore the last one $q^{\mathrm{ord}_q(m!)}\frac{a_m}{m!}$ is as well. Thus $(\sum_{i=1}^{p-1} n_i \zeta^i \equiv 0 \pmod q)^m$ and this means because of the first part of 6.1 and the linear independence of the ζ^i, that $n_i \equiv 0 \pmod q$ for all i. This theorem is a major step in Mihăilescu's proof.

We need the following definition to analyze units of $\mathbb{Z}[\zeta]$.

Definition 7.2. *An element $\alpha \in \mathbb{Z}[\zeta]$ is called q-primary if there is an $\beta \in \mathbb{Z}[\zeta]$ such that:*

$$\alpha \equiv \beta^q \pmod q.$$

Let E denote the group of units, C the cyclotomic units and C_q, the q-primary cyclotomic units. To use this we look at the following modules and their annihilators:

Lemma 7.3. *The $\mathbb{F}_q[G]$ modules*

$$E/CE^q, \qquad C/C_q, \qquad C_q/(C_q \cap E^q)$$

are cyclic. Their Annihilators, called I_1, I_2 and I_3 respectively, are pairwise coprime and further satisfy

$$I_1 I_2 I_3 = (\mathcal{N}, 1 - \iota),$$

where $\mathcal{N}$ is the norm element in $\mathbb{F}_q[G]$ (i.e. $\sum_{i=1}^{p-1} \sigma_i$) and ι is complex conjugation.

Because factor modules of cyclic modules are cyclic and $C/C_q \cong CE^q/C_qE^q$ and $C_q/(C_q \cap E^q) \cong C_qE^q/E^q$, it suffices to show that E/E^q is cyclic and that $\mathrm{ann}_{\mathbb{F}_q[G]}(E/E^q) = (\mathcal{N}, 1 - \iota)$. For a proof of this see [].

Now we want to use 7.1 to show that $I_1 I_3 \subset (\mathcal{N}, 1 - \iota)$. For this purpose we need Thaine's theorem, a tool from the "plus" part of cyclotomic theory. For an abelian group A denote by $[A]_q$ the group consisting elements the order of which is a q-th power, i.e. the q-torsion subgroup.

The special case of Thaine's theorem we need is:
Theorem 7.4 (Thaine)**.** *Let q be a prime not dividing $p-1$. Then any $\theta \in \mathbb{Z}[G]$ divisible by $(1+\iota)$ that annihilates $[E/C]_q$ also annihilates the $[H]_q$ the q-torsion subgroup of H.*

Again limiting us to elements divisible by $(1+\iota)$ means that this is essentially a statement about $\mathbb{Z}[G^+]$. For a proof see chapter 12 of (Bilu et al. 2014) or (Washington 1982).

A first use of Thaine's theorem is showing:
Lemma 7.5. *Every $\theta \in I_1$ divisible by $(1+\iota)$ annihilates $[H]_q$.*

Proof. We will use an important property of ideals of $\mathbb{Z}[G]$: Because of 4.18 every ideal is idempotent: Because $\mathbb{Z}[G]$ is a product of fields, every ideal is just the product of ideals of fields, but fields only have the 0 ideal and the the non proper ideal, which are both idempotent. Thus all ideals in $\mathbb{Z}[G]$ are idempotent specifically I_1, I_2 and I_3.

Thus there are $\theta_1, \dots, \theta_m \in I_1$ such that $\theta = \theta_1 \dots \theta_m$, where m is chosen such that $|[E/C]_q| = q^m$. Because $I_1 = \operatorname{ann}_{\mathbb{F}_q[G]}(E/CE^q)$, we have $E^{\theta_1} \subset CE^q$ and thus

$$E^{\theta_1\theta_2} \subset (CE^q)^{\theta_2} \subset C_2^{\theta}(CE^q)^q \subset CE^{q^2}.$$

Inductively we get $E^{\theta} \subset E^{q^m}$. Now let $\epsilon C \in [E/C]_q$. As shown above $\epsilon^{\theta} = \eta\epsilon_1^{q^m}$ for some cyclotomic unit η and some unit ϵ_1 with $\epsilon_1 C \in [E/C]_q$. Thus $(\epsilon C)^{\theta} = (\epsilon_1 C)^{q^m} = C$ which means that θ annihilates $[E/C]_q$. As a consequence of Thaine's theorem θ annihilates $[H]_q$. □

Similarly to 6.3 we now get information about $(x-\zeta)^{\theta}$:
Lemma 7.6. *For any element $\theta \in I_1$ divisible by $(1+\iota)$ of weight 0:*

$$(x-\zeta)^{\theta} \in E(\mathbb{Q}[\zeta])^q$$

Proof. As we saw in section 6 $(\lambda) = \left(\frac{x-\zeta}{1-\zeta}\right)$ is the q-th power of an ideal A. As A^q is a principal ideal, the coset of A in H belongs to $[H]_q$. Therefore A^{θ} is also principal by the previous lemma and thus (λ^{θ}) is the q-th power of a principal ideal. Because $w(\theta) = 0$, $(1-\zeta)^{\theta}$ is a product of terms of the form $\frac{1-\zeta^i}{1-\zeta^j}$ and therefore a cyclotomic unit.

Altogether we obtain:

$$(x-\zeta)^{\theta} = (1-\zeta)^{\theta}\lambda^{\theta} \in E(\mathbb{Q}[\zeta])^q.$$

□

Now the divisibility also proofed in section 6 can be used to strengthen this result:

Lemma 7.7. *For any element $\theta \in I_1$ divisible by $(1+\iota)$ of weight 0:*

$$(x-\zeta)^\theta \in C_q(\mathbb{Q}[\zeta])^q$$

Proof. First we again use that I_1 is idempotent: There are $\theta_1, \theta_2 \in I_1$ such that $\theta = \theta_1\theta_2$. Thus:

$$(x-\zeta)^{\theta_1\theta_2} \in (E(\mathbb{Q}[\zeta])^q)^{\theta_2} = E^{\theta_2}(\mathbb{Q}[\zeta])^q) \subset C(\mathbb{Q}[\zeta])^q.$$

This means there is an $\eta \in C$ and an $\alpha \in \mathbb{Q}[\zeta]$ such that: $(x-\zeta)^\theta = \eta\alpha^q$. Using 6.4 we get $\eta\alpha^q \equiv (-\zeta)^\theta \pmod{q^2}$. Because $(-\zeta)$ is a root of unity so is $(-\zeta)^\theta$ and thus it is a q-th power and thus η is q-primary. □

By the definition of I_3 we get the following result:

Lemma 7.8. *For any element $\theta \in I_1I_3$ divisible by $(1+\iota)$ of weight 0:*

$$(x-\zeta)^\theta \in (\mathbb{Q}[\zeta])^q$$

Proof. Writing $\theta = \theta_1\theta_3$ with $\theta_1 \in I_1$ and $\theta_3 \in I_3$:

$$(x-\zeta)^\theta = (x-\zeta)^{\theta_1\theta_3} \in C_q^{\theta_3}(\mathbb{Q}[\zeta])^q \subset (\mathbb{Q}[\zeta])^q.$$

□

But this tells us that $\theta = 0$ by 7.1 and thus there are no nontrivial elements in I_1I_3 of weight 0, which are divisible by $(1+\iota)$. Some simple calculation with ideals of $\mathbb{F}[G]$ show that having a trivial intersection with the ideal $(1+\iota)\mathbb{F}[G]^{\text{aug}}$ of elements divisible by $(1+\iota)$ of weight 0, means being contained in the ideal $(1-\iota, \mathcal{N})$. This means $I_1I_3 \subset (1-\iota, \mathcal{N}) = I_1I_2I_3$. Thus $I_2 = (1)$, which means, as $I_2 = \mathrm{ann}_{\mathbb{F}_{\shortparallel}[\mathbb{G}]}(C/C_q)$, that $C = C_q$, i.e. all cyclotomic units are q-primary. This cannot happen:

Lemma 7.9. *If $p > q$, not all cyclotomic units in $\mathbb{Z}[\zeta]$ are q-primary.*

Proof. If all cyclotomic units are q-primary so is in particular $1+\zeta^q = \frac{1-\zeta^{(}2q)}{1-\zeta^{(}q)}$. Thus $1+\zeta^q \equiv \beta^q \pmod{q^2}$, for some $\beta \in \mathbb{Z}[\zeta]$. Thus $(1+\zeta)^q \equiv 1+\zeta^q \equiv \beta^q \pmod{q}$ and by the Lifting the Exponent Lemma we get:

$$(1+\zeta)^q \equiv (1+\zeta^q) \pmod{q^2}$$

Thus the polynomial $f := \frac{1}{q}((1+T)^q - (1+T^q)) \in \mathbb{Z}[T]$ has ζ as a root modulo q and hence also all of it's $p-1$ conjugates ζ^i. Consider a prime ideal $\mathfrak{q}$ in $\mathbb{Z}[\zeta]$ which divides (q). All roots of f modulo q are also roots modulo $\mathfrak{q}$. They are also all distinct because otherwise we would have, since $(\zeta^i - \zeta^j) = (1-\zeta)$:

$$\mathfrak{q} | (\zeta^i - \zeta^j) | (p),$$

but (p) and (q) are coprime. Thus we have $p-1$ distinct roots of f in the field $\mathbb{Q}[\zeta]/\mathfrak{q}$. But the degree of f is $q-1$ which by assumptions is less than $p-1$. $\square$

The assumption that $p > q$ is no problem: If either $p|q-1$ or $q|p-1$ we can proceed as in the previous subsection. Otherwise the problem is symmetric in p and q as discussed in the beginning of section 5 and we can assume $p > q$.

This finishes Mihăilescu's proof of the Problem of Catalan!

References

Bilu, Y. (2002), ‘Catalan’s conjecture after mihăilescu’, *Sém. Bourbaki* **55**.

Bilu, Y., Bugeaud, Y. & Mignotte, M. (2014), *The Problem of Catalan*, Springer.

Cassels, J. (1960), ‘On the equation $a^x - b^y = 1$’, *Mathematical Proceedings of the Cambridge Philosophical Society* **56**.

Chao, K. (1964), ‘On the diophantine equation $x^2 = y^n + 1, xy \neq 0$’, *Sci. Sinica (Notes)* **14**.

Daems, J. (2003), A cyclotomic proof of Catalan’s Conjecture, PhD thesis, Universität Leiden.

Euler, L. (1915), ‘Theorematum quorundam arithmeticorum demonstrationes.’, *Comm. Acad. Sci. Petrop.* **10**.

Inkeri, K. (1990), ‘On catalan’s problem’, *J. Number Theory* **34**.

Lang, S. (1965), *Algebra*, Springer, New York.

Lang, S. (1994), *Algebraic Number Theory*, Springer, New York.

Lebesgue, V. (1850), ‘Sur l’impossibilité en nombres entiers de l’equation $x^m = y^2 + 1$’, *Nouv. Ann. Math.* **9**.

Lorenz, T. (2008), Die Catalan’sche Vermutung, PhD thesis, Technische Universität Wien.

Matijasevič, Y. V. (1973), ‘On recursive unsolvability of hilbert’s tenth problem’, *Studies in Logic and the Foundations of Mathematics* **74**.

Metsänkylä, T. (2003), ‘Catalan’s conjecture: Another old diophantine problem solved’, *Bulletin of the American Mathematical Society* **41**.

Mihăilescu, P. (2003), ‘A class number free criterion for catalan’s conjecture’, *J. Number Theory* **99**.

Mihăilescu, P. (2004), ‘Primary cyclotomic units and a proof of catalan’s conjecture’, *J. für die reine und angewandte Mathematik* **572**.

Mihăilescu, P. (2006), ‘On the class groups of cyclotomic extensions in the presence of a solution to catalan’s equation.’, *J. Number Theory* **118**.

Tijdeman, R. (1976), ‘On the equation of catalan’, *Acta Arith.* **29**.

Washington, L. C. (1982), *Introduction to cyclotomic fields*, Springer.