

Catalan's Conjecture

Author

Andreas Steiger

A semester project supervised by Prof. E. Kowalski

Fall Semester, 2008

CONTENTS

Contents	i
1 Historical Development and Mihăilescu's Proof	1
2 Advanced Tools	4
2.1 Notation	4
2.2 Group Rings and the Stickelberger Theorem	5
2.3 The $\mathbb{F}_q[G]$ -module H	6
3 Theorem 2: The Wieferich Pair	8
4 Theorem 4: The Lower Bound	9
5 Theorem 3: The Relative Bounds	13
6 Theorem 1: The Plus Argument	16
6.1 Preliminaries on Power Series	16
6.2 Semi-simple Rings and Theorem 1	20
Bibliography	24

HISTORICAL DEVELOPMENT AND MIHĂILESCU'S PROOF

In 1844, Crelle's *Journal für die reine und angewandte Mathematik* published the following note from E. Catalan [3]:

Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement: d'autres seront peut-être plus heureux:

Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes; autrement dit: l'équation $x^m - y^n = 1$, dans laquelle les inconnues sont entières positives, n'admèt qu'une seule solution.

This leads to the following formulation:

Conjecture 1.1 (Catalan). *The only solution to the equation*

$$x^m - y^n = 1 \tag{1}$$

in integers $x, y, m, n > 1$ is $3^2 - 2^3 = 1$.

The first goal is to reduce it to the following conjecture:

Conjecture 1.2 (Catalan). *There are no solutions to the equation*

$$x^p - y^q = 1 \tag{2}$$

in odd primes p, q and non-zero integers x, y .

Remark. Notice that negative integers are allowed in Conjecture 1.2. But since (x, y, p, q) is a solution if and only if $(-y, -x, q, p)$ is a solution, this is a very helpful extension of the problem.

To achieve the reduction to prime power case, we have a look at the history of the problem: It was already known to Euler that for some fixed exponents, there are only a few solutions. By an infinite descent argument, he was able to solve the case $(m, n) = (2, 3)$.

Theorem 1.3 (Euler, 1738). *If $m = 2$ and $n = 3$, the solutions to (1) in rational numbers are $(x, y) \in \{(0, -1), (\pm 1, 0), (\pm 3, 2)\}$.*

But he was not the first to study the problem of consecutive powers: In the 14th century, Levi ben Gerson showed that the only consecutive powers of 2 and 3 are 8 and 9:

Theorem 1.4. *If $3^m \pm 1 = 2^n$, then $m = 2$ and $n = 3$.*

Several years after Catalan's note, Gaussian integers led to a proof of the case $n = 2$:

Theorem 1.5 (Lebesgue 1850, [11]). *If $n = 2$ and $m > 2$, then (1) has no solution in positive integers x, y .*

After that, not much progress was achieved for a long time. Further studies then revealed more results for small exponents, and Nagell resolved the cases $m = 3$ and $n = 3$.

In 1953 and 1961, Cassels published new results [2], that stimulated the problem again.

Theorem 1.6 (Cassels' Relations, 1961). *Solutions to (2) satisfy $p|y$ and $q|x$.*

Other mathematicians were then attracted to the problem by this result. A lot of research was kicked off, and results were found. For our goal, the most important of these results is the case $m = 2$:

Theorem 1.7 (Chao Ko 1960, [8]). *If $m = 2$ and $n > 1$, then there are no solutions to (1) in positive integers except $3^2 - 2^3 = 1$.*

The mentioned results together give the wanted reduction. Thus, from now on Conjecture 1.2 will be meant whenever Catalan's Conjecture is mentioned.

But let us now go on with the little history lesson: After 1960, a lot of different ways were tried to tackle the problem. There were attempts to bound the variables. This resulted in Tijdeman's theorem [17] that there exist computable bound C such that solutions to (1) must satisfy $x, y, m, n < C$. This bound was then computed by Langevin [10]. However, it turned out not to be very useful, for the bounds were

$$\begin{aligned} p, q &< 10^{110}, \\ x, y &< \exp \exp \exp \exp 730. \end{aligned}$$

Further refinements could be accomplished, and around 2000 the best known results [12] were that p and q must lie between 10^7 and 10^{18} , and if further $p < q$ then $p < 7.15 \cdot 10^{11}$ and $q < 7.78 \cdot 10^{16}$.

On the other hand, there were attempts to solve the problem with algebraic approaches. The first notable result was due to Inkeri [6] who showed that solutions to (2) with $p \equiv 3 \pmod{4}$ have to satisfy

$$q|h(\mathbb{Q}(\sqrt{-p})) \quad \text{or} \quad p^{q-1} \equiv 1 \pmod{q^2},$$

and symmetrically in p, q . The second condition is an example of what is called a (double) *Wieferich pair*, i.e. primes p, q such that

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

They are named after Wieferich, who showed that any prime number p that fails to satisfy the First Case of Fermat's Last Theorem has to satisfy $2^{p-1} \equiv 1 \pmod{p^2}$. Nowadays, one calls primes satisfying this condition *Wieferich primes*. Wieferich pairs are supposed to be very rare; There are only 6 examples known, and one conjectures that there exist only finitely many.

The class number approach was strengthened by many results, and in the 90's, mathematicians began to use computers to check conditions similar to those of Inkeri. The approach was successful, since a lot of special cases could be ruled out. But in the end it was not a computer who solved Catalan's Conjecture: In 2002, the Romanian mathematician Preda Mihăilescu found a complete proof. In this text, we show a refined version of the proof, where the major improvement over the initial proof is the independence of a computer calculation, which was required at first.

Theorem 1.8 (Mihăilescu). *If p and q are the exponents of a solution to Catalan's equation, then*

1. $p \equiv 1 \pmod{q}$ or $q \equiv 1 \pmod{p}$,
2. $p^{q-1} \equiv 1 \pmod{q^2}$ and $q^{p-1} \equiv 1 \pmod{p^2}$,
3. $p < 4q^2$ and $q < 4p^2$.

Together these three statements lead to a proof of Catalan's Conjecture.

Theorem 1.9 (Mihăilescu, 2002). *The only solutions of the equation*

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

in integers $p, q \geq 2$ and non-zero integers x, y are given by $(\pm 3)^2 - 2^3 = 1$.

Proof. From the discussion in the first chapter we are left to consider odd primes p, q . Catalan's equation is symmetric in p and q , hence in the first statement we can assume that $p \equiv 1 \pmod{q}$, i.e. there exists $k \in \mathbb{Z}$ such that $p = 1 + kq$. Applying the second statement gives

$$1 \equiv p^{q-1} = (1 + kq)^{q-1} \equiv 1 + kq(q-1) \equiv 1 - kq \pmod{q^2},$$

so $k \equiv 0 \pmod{q}$ and $p \equiv 1 \pmod{q^2}$. Therefore there exists an $l \in \mathbb{Z}_{\geq 1}$ such that $p = 1 + lq^2$. But by the third statement, l can not exceed 3. In the cases $l = 1$ and $l = 3$, the term $1 + lq^2$ is even and hence not prime. By looking at $p = 1 + 2q^2$ modulo 3, we see that $q = 3$ and thus $p = 19$ has to hold. But in this case $3^{18} \not\equiv 1 \pmod{19^2}$, violating the second statement and completing the contradiction. \square

The strategy is as follows: We define a group H (see (4)), for which we can show that it is annihilated by an ideal I (see (3)). This is essentially due to Stickelberger's Theorem 2.1. One can then analyse the properties of the annihilators and since the trivial elements in H are all q th powers of elements in $\mathbb{Q}(\zeta_p)$, even the fraction they are annihilated to can give information. Furthermore, Cassels' Relations 2.3 tell us a lot about the structure of solutions, and will be used throughout the whole article. Equations of the form

$$(x - \zeta_p)^\theta = \alpha^q$$

are the main objects of study, and one can show that the existence of solutions that do not satisfy Mihăilescu's conditions lead to contradictions.

The reader will notice that the proofs for the Theorems 1 and 3 require p and q to be sufficiently large. This is accomplished by Mihăilescu's fourth Theorem:

Theorem 1.10 (Mihăilescu's Theorem 4). *There are no solutions if one of p or q is at most 43.*

For a wider account on the historic development, the reader is suggested to consult the book by Paulo Ribenboim [15] and the article of Mignotte [7]. Furthermore, the articles by Mischler and Boéchat [14], Schoof [16] and Bilu [1] turned out to be very useful.

CHAPTER 2

ADVANCED TOOLS

The reader is assumed to have a working knowledge in algebraic number theory. A good (and free) introduction on this topic can be found in Milne's lecture notes *Algebraic Number Theory* [13]. Furthermore, a little knowledge on p -adic integers is assumed. This can be found in Milne as well. Koblitz' *p -adic Numbers, p -adic Analysis and Zeta-Functions* [9] is another well-written introductory book. As a third ingredient, group rings will be used. Both Mischler & Boéchat's *Le Conjecture de Catalan* [14] and Cohen's *Number Theory* [4] introduce them in the chapters where they are required for the needed results.

With these fundamental tools we can establish results on cyclotomic fields which will constantly be used to proof Mihăilescu's theorems. But first we need to fix some notation.

2.1 Notation

Let x, y, p, q be a fixed non-trivial solution to Catalan's equation

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

where p and q are odd primes.

Let ζ_p denote a p th primitive root of unity. We will often work in the cyclotomic number field $\mathbb{Q}(\zeta_p)$ over \mathbb{Q} , which has the Galois group

$$G := \{\tau_a \mid a \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

, where τ_a acts on ζ_p by raising it to the a -th power. The complex conjugation is an automorphism $\tau_{-1} \in G$, and it will sometimes be written as ι . The fixed field of ι is $\mathbb{Q}(\zeta_p^+)$ where $\zeta_p^+ = \zeta_p + \zeta_p^{-1}$. For the quotient of G by $\langle \iota \rangle$ we will write G^+ .

The class group of the ring of integers $\mathbb{Z}[\zeta_p]$ is denoted by Cl . Similarly, the class group of $\mathbb{Z}[\zeta_p^+]$ is denoted by Cl^+ . This group has a natural image in Cl , and we call the quotient $Cl^- := Cl/Cl^+$. To these three groups, we associate (in the obvious way) the class numbers h_p, h_p^+ and h_p^- . By construction they satisfy $h_p = h_p^+ \cdot h_p^-$.

Let $E := \mathbb{Z}[\zeta_p, \frac{1}{p}]^*$ be the group of p -units. Since $p = u(1 - \zeta_p)^{p-1}$ for some unit $u \in \mathbb{Z}[\zeta_p]^*$, the group E is generated by the unit group $\mathbb{Z}[\zeta_p]^*$ and $1 - \zeta_p$. For an integer b and abelian groups A we set $A^b := \{a^b \mid a \in A\}$ and $A[b] := \{\alpha \in A \mid \alpha^b = 1\}$. Note that if A is a finite group and r is an odd prime, then $A[r]$ has order 1 or is a multiple of r .

2.2 Group Rings and the Stickelberger Theorem

The group ring $\mathbb{Z}[G]$ of the Galois group G acts on the number field in the following way: Let $\lambda = \sum_{\tau \in G} n_\tau \tau \in \mathbb{Z}[G]$ and x an element of the field, then

$$x^\lambda = \prod_{\tau \in G} \tau(x)^{n_\tau}.$$

One verifies easily that the usual rules of exponentiation hold, i.e.

$$(x^\lambda)^\mu = x^{\lambda\mu}, \quad x^\lambda x^\mu = x^{\lambda+\mu}, \quad (xy)^\lambda = x^\lambda y^\lambda.$$

The size of $\theta \in \mathbb{Z}[G]$ is given by $\|\theta\| := \sum_{\tau \in G} |n_\tau|$. The Stickelberger element of $\mathbb{Z}[G]$ is

$$\Theta := \sum_{\tau_a \in G} \frac{a}{m} \tau_a^{-1} \in \mathbb{Q}[G].$$

Note that the Stickelberger element is not in $\mathbb{Z}[G]$, but only in $\mathbb{Q}[G]$. However, one can restrict the $\mathbb{Z}[G]$ -module $\Theta\mathbb{Z}[G]$ to the group ring by intersection, and one defines the Stickelberger ideal to be $I_{st} = \mathbb{Z}[G] \cap \Theta\mathbb{Z}[G]$, which is in fact an ideal of $\mathbb{Z}[G]$. It is generated by the elements $\Theta_b := (\tau_b - b)\Theta$, where b is coprime to p . There is convenient \mathbb{Z} -basis for I_{st} by the elements $f_i := \Theta_i - \Theta_{i+1}$ for $i \in \{1, \dots, \frac{p-1}{2}\}$ together with the G -trace $s(G) := \sum_{\tau \in G} \tau$. Each f_i has size $\frac{p-1}{2}$, since all coefficients n_τ are either 0 or 1. Furthermore, we define $e_i := (1 - \iota)f_i$. The e_i have size $p-1$ and generate the ideal

$$I := (1 - \iota)I_{st}. \quad (3)$$

Finally, the most important fact about the group rings is the following statement:

Theorem 2.1 (Stickelberger's Theorem). *The Stickelberger ideal I_{st} of $\mathbb{Q}(\zeta_p)$ annihilates the class group Cl , i.e. \mathfrak{a}^θ is a principal ideal for all $\theta \in I_{st}$, $\mathfrak{a} \in Cl$.*

As mentioned above, proofs for all these statements can be found in Mischler & Boéchat [14], chapter 5, and Cohen [4], chapter 3.6.

2.3 The $\mathbb{F}_q[G]$ -module H

For a module M of a group ring $R[G]$ containing ι , one defines the M -submodules $M^\pm := \{x \in M \mid \iota x = \pm x\}$. If $\frac{1}{2} \in R$ (which will be the case everywhere), then $M = M^+ \oplus M^-$.

Define $\mathfrak{p} = (1 - \zeta_p)$ to be the unique prime ideal in $\mathbb{Z}[\zeta_p]$ above (p) . One can then consider the $\mathbb{F}_q[G]$ -module

$$H := \{\alpha \in \mathbb{Q}(\zeta_p)^* \mid \text{ord}_\tau(\alpha) \equiv 0 \pmod{q} \text{ for all primes } \tau \neq \mathfrak{p}\} / (\mathbb{Q}(\zeta_p)^{*q}). \quad (4)$$

For any element $\alpha \in H$ there exists a unique fractional ideal \mathfrak{a} in $\mathbb{Q}(\zeta_p)$ and a unique integer k such that $(\alpha) = \mathfrak{a}^q \mathfrak{p}^k$.

Lemma 2.2. The $\mathbb{F}_q[G]$ -module H has the following properties:

- i) The map $\varphi : H \rightarrow Cl[q]$ that sends α to the class of $\mathbb{Z}[\zeta_p]$ -ideals \mathfrak{a} as above induces an exact sequence

$$0 \longrightarrow E/E^q \xrightarrow{j} H \xrightarrow{\varphi} Cl[q] \longrightarrow 0.$$

- ii) The group E/E^q is invariant under the action of ι .

- iii) There is an exact sequence

$$0 \longrightarrow E/E^q \longrightarrow H^+ \longrightarrow Cl^+[q] \longrightarrow 0.$$

- iv) The ideal I (see (3)) annihilates H .

- v) $H^- \simeq Cl^-[q]$.

Proof. The map φ is well-defined by the uniqueness of $(\alpha) = \mathfrak{a}^q \mathfrak{p}^k$. Since $\mathfrak{p} = (1 - \zeta_p)$, the q -th power of \mathfrak{a} satisfies $\mathfrak{a}^q = (\alpha(1 - \zeta_p)^{-k})$ and thus $\mathfrak{a} \in Cl[q]$. The kernel of the j is obviously E^q , and φ is surjective. Let $\alpha = \beta^q \mathfrak{p}^k$ be in the kernel of φ . Then there is a unit $u \in \mathbb{Z}[\zeta_p]^*$ such that $\alpha = u\beta^q(1 - \zeta_p)^k \equiv u(1 - \zeta_p)^k \in E/E^q$. Thus the sequence is exact.

For a unit $u \in \mathbb{Z}[\zeta_p]^*$, the element $u^{1-\iota} = \frac{u}{\bar{u}}$ is a $2p$ -th root of unity and is thus a q -th power. Similarly $(1 - \zeta_p)^{1-\iota} = -\zeta_p$ is still a root of unity, and thus a q -th power. Since E is generated by these elements, all $\varepsilon \in E$ satisfy $\varepsilon^{1-\iota} \equiv 1 \pmod{E^q}$, i.e. E/E^q is ι -invariant.

Now one easily sees that the application of $1 + \iota$ to the exact sequence of i) implies the exact sequence of iii). Since I_{st} annihilates $Cl[q]$ and $1 - \iota$ annihilates E/E^q , the exact sequence of i) tells us that $I = (1 - \iota)I_{st}$ annihilates H and $Cl^-[q] \simeq H^-$. \square

We now turn to results concerning our conjecture. The first statement is a refinement of Cassels' Relations 1.6, still due to Cassels.

Corollary 2.3 (Cassels' Relations). *i) There are $a, v \in \mathbb{Z}$ such that*

$$y = pav, \quad x - 1 = p^{q-1}a^q, \quad \frac{x^p - 1}{x - 1} = pv^q.$$

ii) There are $b, u \in \mathbb{Z}$ such that

$$x = qbu, \quad y + 1 = q^{p-1}b^p, \quad \frac{y^q + 1}{y + 1} = qu^p.$$

iii) We have that

$$|x| \geq \max(p^{q-1} - 1, q^{p-1} + q), \quad |y| \geq \max(q^{p-1} - 1, p^{q-1} + p).$$

A proof for these important statements can be found in [4], pages 444 and 447ff., as well as in [14], pages 11ff.

At this point, one could ask whether Cassels would have been able to find the theorems of Mihăilescu, if he had tried harder. However, Cassels' approach uses only elementary number theory, in contrast to Mihăilescu, who used the full power of cyclotomy. The proof of Mihăilescu is dependent on deep arithmetic facts which were not known at the time when Cassels worked on the problem.

The following proposition tells us that $x - \zeta_p$ is contained in H , so its class modulo q th powers is annihilated by the ideal I . This annihilation will be used and analysed thoroughly to prove Mihăilescu's Theorems.

Proposition 2.4. *i) There exists a non-zero ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta_p]$ such that*

$$\left(\frac{x - \zeta_p}{1 - \zeta_p} \right) = \mathfrak{a}^q,$$

ii) The class of $x - \zeta_p$ modulo q -th powers is contained in H .

Proof. By Cassels' Relations 2.3, we know that there exists a positive integer v such that

$$\prod_{\substack{\zeta \in \mu_p \\ \zeta \neq 1}} \left(\frac{x - \zeta}{1 - \zeta} \right) = v^q.$$

Since $p|x - 1$ we have $x - \zeta = x - 1 + 1 - \zeta \in (1 - \zeta)$ for all $1 \neq \zeta \in \mu_p$. However, for all non-trivial p -th roots of unity $\zeta \neq \zeta'$ the principal ideals satisfy $(1 - \zeta) = (1 - \zeta_p) = (\zeta - \zeta')$ in $\mathbb{Z}[\zeta_p]$, thus there is a unit $u_\zeta := \frac{1 - \zeta}{1 - \zeta_p}$. Then we have

$$u_\zeta \left(\frac{x - \zeta}{1 - \zeta} \right) - u_{\zeta'} \left(\frac{x - \zeta'}{1 - \zeta'} \right) = \frac{\zeta' - \zeta}{1 - \zeta_p}.$$

This is a unit, thus all the factors in the product are coprime. Hence, each factor has to be the q -th power of an ideal in $\mathbb{Z}[\zeta_p]$ and the first part of the proposition is proven. The second part is then evident by multiplying with $(1 - \zeta_p)$. \square

THEOREM 2: THE WIEFERICH PAIR

We first prove Mihăilescu's second Theorem, stating that p and q have to be a Wieferich pair. As mentioned in the beginning, Wieferich pairs are supposed to be rare and large. This was the first theorem that Mihăilescu proved, and it was a strong indicator for the truth of Catalan's conjecture.

Theorem 3.1 (Mihăilescu's Theorem 2, 2000). *We have*

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

The proof is based on a subtle but beautiful improvement of Cassels' Relations. By using Stickelberger's theorem, one can show that not only q , but also q^2 has to divide x .

Lemma 3.2. Let R be a commutative ring and let q be a prime number such that the principal ideal (q) is radical. Then for any $a, b \in R$ such that $a^q \equiv b^q \pmod{q}$, they also satisfy $a^q \equiv b^q \pmod{q^2}$.

Proof. We have $(a - b)^q \equiv a^q - b^q \equiv 0 \pmod{q}$. The ideal (q) is radical, hence even $a - b \equiv 0 \pmod{q}$, which yields $a^q \equiv b^q \pmod{q^2}$. \square

Remark. In particular, the lemma holds in the case where K is a number field, $S \subset \mathcal{O}_K$ is a subset consisting of elements coprime to q and $R = S^{-1}\mathcal{O}_K$.

Proposition 3.3. q^2 divides x .

Proof. Let $\theta \in I$. By lemma 2.2 we know that I annihilates H , i.e. there is an $\alpha \in \mathbb{Q}(\zeta_p)^*$ such that $(x - \zeta_p)^\theta = \alpha^q$. Multiply this equation by $(-\zeta_p^{-1})^\theta$ (which is a q -th power of another $2p$ -th root of unity, since $(2p, q) = 1$) and apply complex conjugation ι . Then there exists $\beta \in \mathbb{Q}(\zeta_p)^*$ such that

$$(1 - x\zeta_p)^\theta = \beta^q.$$

Since $q|x$ by Cassels' Relations 2.3, we have $1 \equiv \beta^q \pmod{q}$, and by Lemma 3.2 we even get $1 \equiv \beta^q \pmod{q^2}$.

By definition, we have

$$(1 - x\zeta_p)^\theta = \prod_{\tau \in G} (1 - x\tau(\zeta_p))^{n_\tau}.$$

Expanding the product and reducing modulo q^2 gives

$$1 - x \sum_{\tau \in G} n_\tau \tau(\zeta_p) \equiv 1 \pmod{q^2}.$$

Assume that q^2 does not divide x . Then $\sum_{\tau \in G} n_\tau \tau(\zeta_p) \equiv 0 \pmod{q}$ is required for this equivalence to be true. This is only possible if q divides all n_τ , i.e.

the image of the ideal I in $\mathbb{F}_q[G]$ is zero. But this is not true, since the generating elements e_i of I have all their coefficients equal to ± 1 . Thus $q^2|x$ must hold. \square

We are now able to prove Theorem 3.1.

Proof of Mihăilescu's Theorem 2. By Cassels' Relations 2.3 above we have

$$x - 1 = p^{q-1}a^q$$

for some nonzero $a \in \mathbb{Z}$. By applying Fermat's little Theorem to this equation and using $q|x$, we have $-1 \equiv a^q \pmod{q}$, and lemma 3.2 tell us that the equivalence also holds modulo q^2 . Since $q^2|x$ by proposition 3.3, we have that

$$-1 \equiv x - 1 = p^{q-1}a^q \equiv -(p^{q-1}) \pmod{q^2}.$$

Thus the first congruence is proven. The second follows by symmetry. \square

To conclude this chapter we state a corollary to proposition 3.3 which will be used in the proof of Mihăilescu's Theorem 1. Consider the subgroup $H' := \{\alpha \in H \mid \alpha \text{ is a } q\text{-th power modulo } q^2\}$ of H .

Corollary 3.4. *The image of $x - \zeta_p$ is contained in H' .*

Proof. Since $q^2|x$, we have $x - \zeta_p \equiv -\zeta_p \pmod{q^2}$, which is a q -th power modulo q^2 . \square

CHAPTER 4

THEOREM 4: THE LOWER BOUND

The next theorem rules out small values of p and q .

Theorem 4.1 (Mihăilescu's Theorem 4, 2002). *p and q are larger than 43.*

The proof is based on the following proposition that eventually relates the exponents of a solution with their minus class numbers.

Proposition 4.2. *$(x - \zeta_p)^{1-t}$ is not trivial in H .*

The proof is based on a lengthy p -adic argument on $(x - \zeta_p)^{1-t}$. We first state the consequences:

Corollary 4.3. *$p \mid h_q^-$ and $q \mid h_p^-$ must hold.*

Proof. By symmetry it suffices to assume $q \nmid h_p^-$. By definition $h_p^- = |Cl^-|$, and lemma 2.2 states that $H^- \simeq Cl^-[q]$. The cardinality of the subgroup $Cl^-[q]$ is either 1 or a multiple of q . Thus H^- is trivial, contradicting proposition 4.2. \square

Minus class numbers are not hard to calculate: For an odd prime p , choose a generator γ of \mathbb{F}_p^* . Then choose positive integers γ_i not exceeding $p-1$, such that $\gamma_i \equiv \gamma^i \pmod{p}$ for $i = 1, \dots, p-1$. Write $F_p(X) = \sum_{1 \leq i \leq p-1} \gamma_i X^i$. Then

$$h_p^- = \frac{\left| \prod_{1 \leq k \leq \frac{p-1}{2}} F_p(\zeta_{p-1}^{2k-1}) \right|}{(2p)^{\frac{p-3}{2}}}.$$

A proof for this statement can be found in [5], page 225. With these results, we are now able to complete the proof for Theorem 4.

Proof of Mihăilescu's Theorem 4. For $p \leq 19$ the minus class number is always 1. For $p = 23, 29, 31, 37$, and 41, the respective minus class numbers are 3, 8, 9, 37, 11^2 and q has to divide them, which gives no non-trivial solutions in each case. Finally we have $h_{43}^- = 211$. But then one checks that 43 does not divide h_{211}^- , thus the corollary tells us that there are no non-trivial solutions. \square

For $p = 47$ and $q = 137$, the argument does not work since $p|h_q^-$ and $q|h_p^-$. However, one could use Mihăilescu's Theorem 2 to rule out this case.

Proof of proposition 4.2. Write $\pi = \zeta_p - 1$ and suppose that $(x - \zeta_p)^{1-l}$ is trivial in H , i.e. there exists $\alpha \in \mathbb{Q}(\zeta_p)^*$ such that

$$(x - \zeta_p)^{1-l} = \frac{x - \zeta_p}{x - \bar{\zeta}_p} = \alpha^q.$$

By Cassels' Relations 2.3 we know that $x \equiv 1 \pmod{p^{q-1}}$. Therefore α is equivalent to $-1 \pmod{\pi}$. Put $\mu = \frac{x-1}{1-\zeta_p} \in \mathbb{Z}[\zeta_p]$. Then the π -adic valuation of μ is $\text{ord}_\pi(\mu) \geq (p-1)(q-1) - 1 \geq 4$. One easily verifies that $\frac{x-\zeta_p}{1-\zeta_p} = 1 + \mu$ and

$$\frac{1 + \mu}{1 + \bar{\mu}} = -\zeta_p^{-1} \alpha^q,$$

which is again a q -th power. Fix q -th roots of $1 + \mu$ and $1 + \bar{\mu}$ such that

$$\frac{\sqrt[q]{1 + \mu}}{\sqrt[q]{1 + \bar{\mu}}} = -\zeta_p^{-1/q} \alpha.$$

Since $\alpha \equiv -1 \pmod{\pi}$, this implies that $\sqrt[q]{1 + \mu}$ is congruent to $\sqrt[q]{1 + \bar{\mu}}$ modulo π . Write

$$\eta = \left(\sqrt[q]{1 + \mu} + \zeta_p^{-1/q} \sqrt[q]{1 + \bar{\mu}} \right)^q.$$

η is a unit in the ring $\mathbb{Z}[\zeta_p]$: Indeed, η is integral since μ and $\bar{\mu}$ are integral and roots of integral numbers are integral as well. On the other hand, a quick calculation shows that

$$\eta = \left(\sqrt[q]{1 + \bar{\mu}} \right)^q \left(-\alpha \zeta_p^{-1/q} + \zeta_p^{-1/q} \right)^q = (1 + \bar{\mu})(1 - \alpha)^q \zeta_p^{-1} \in \mathbb{Q}(\zeta_p).$$

Since $\sqrt[q]{1+\mu} + \zeta_p^{-1/q} \sqrt[q]{1+\bar{\mu}}$ divides the unit

$$1 + \mu + \zeta_p^{-1}(1 + \bar{\mu}) = \frac{x - \zeta_p}{1 - \zeta_p} + \frac{x - \bar{\zeta}_p}{\zeta_p - 1} = \frac{\bar{\zeta}_p - \zeta_p}{1 - \zeta_p},$$

its q -th power η has to be a unit as well.

This implies that η satisfies

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\eta) = 1.$$

The degree of $\mathbb{Q}(\zeta_p)$ over \mathbb{Q} is the same as the degree of $\mathbb{Q}_p(\zeta_p)$ over \mathbb{Q}_p , hence we can compute the norm in $\mathbb{Q}_p(\zeta_p)$. The ring $\mathbb{Z}_p[\zeta_p]$ is local, and its unique maximal ideal is generated by π . Both $1 + \mu$ and $1 + \bar{\mu}$ are contained in the pro- p -group $1 + \pi\mathbb{Z}_p[\zeta_p]$, hence they have q -th roots, and the element $u = \sqrt[q]{1+\mu} + \zeta_p^{-1/q} \sqrt[q]{1+\bar{\mu}}$ is contained in $\mathbb{Z}_p[\zeta_p]$, having η as q -th power.

Let's have a look at the Taylor series of $\sqrt[q]{1+\mu}$: It converges to a number that is congruent to 1 modulo π up to a q -th root of unity, since μ is a high power of π . Now, if $p \not\equiv 1 \pmod{q}$, then the only q -th root of unity in $\mathbb{Q}_p(\zeta_p)$ is 1. Otherwise there are other q -th roots of unity besides 1. But then we can multiply η with a suitable root of unity without changing its norm, such that the q -th root of $1 + \mu$ is actually congruent to 1 modulo π . Choose $r \in \mathbb{Z}$ to be congruent to $-1/q$ in \mathbb{F}_p . Then we get

$$\begin{aligned} u &= \sqrt[q]{1+\mu} + \zeta_p^{-1/q} \sqrt[q]{1+\bar{\mu}} \\ &= 1 + \frac{\mu}{q} + \zeta_p^r \left(1 + \frac{\bar{\mu}}{q}\right) + O(\mu^2) \\ &= (1 + \zeta_p^r) \left(1 + \frac{x-1}{q} \frac{1 - \zeta_p^{r+1}}{(1 - \zeta_p)(1 + \zeta_p^r)}\right) + O(\mu^2). \end{aligned}$$

The norm of $1 + \zeta_p^r = \frac{1 - \zeta_p^{2r}}{1 - \zeta_p^r}$ is 1, thus we can compute the norm

$$\begin{aligned} N(u) &= \prod_{\substack{\zeta \in \mu_p \\ \zeta \neq 1}} \left(1 + \frac{x-1}{q} \frac{1 - \zeta^{r+1}}{(1 - \zeta)(1 + \zeta^r)}\right) + O(\mu^2) \\ &= 1 + \frac{x-1}{q} \sum_{\substack{\zeta \in \mu_p \\ \zeta \neq 1}} \frac{1 - \zeta^{1+r}}{(1 - \zeta)(1 + \zeta^r)} + O(\mu^2). \end{aligned}$$

Put $\pi' = \zeta - 1$ for any root of unity $\zeta \in \mu_p \setminus \{1\}$. Then π' is associated to π and the terms in the sums can be written independently of ζ as follows:

$$\begin{aligned} \frac{1 - \zeta^{1+r}}{(1 - \zeta)(1 + \zeta^r)} &= \frac{1 - (1 + \pi')^{r+1}}{-\pi'(1 + (1 + \pi')^r)} = \frac{-(r+1)\pi' + O(\pi^2)}{-\pi'(2 + r\pi') + O(\pi^3)} \\ &= \frac{r+1}{2} + O(\pi). \end{aligned}$$

The last equality is due to the geometric series for $\frac{1}{1+O(\pi)}$.

Recall that $\text{ord}_\pi(\mu) \geq 4$, hence $\mu^2 = \left(\frac{x-1}{\pi}\right)^2$ is divisible by $\pi(x-1)$. Thus

$$N(u) = 1 + \frac{x-1}{q} \frac{(r+1)(p-1)}{2} + O(\pi(x-1)).$$

But remember that $\eta = u^q$ has norm 1, thus $1 = N(\eta) = N(u)^q$ resulting in

$$1 = N(u) = 1 + (x-1) \frac{(r+1)(p-1)}{2} + O(\pi(x-1)).$$

This implies that $\pi(x-1)$ divides $\frac{(x-1)(r+1)(p-1)}{2}$. The only possibility is $\pi|r+1$ in \mathbb{Z}_p . i.e. $r \equiv -1 \pmod{p}$. But we already set r to be equivalent to $-1/q$ in \mathbb{F}_p , which is only possible if $q \equiv 1 \pmod{p}$.

The same argument is now repeated under the assumption $q \equiv 1 \pmod{p}$, but this time we throw away third powers of μ in the Taylor expansion. We now know that $\zeta_p^{-1} = \zeta_p^{-1/q}$, and thus $\mu = -\zeta_p^{-1/q} \bar{\mu}$. This time, $p \equiv 1 \pmod{q}$ can not happen and the obstacle of different q -th roots of unity does not appear. So we get

$$\begin{aligned} u &= 1 + \binom{1/q}{2} \mu^2 + \zeta_p^{-1} \left(1 + \binom{1/q}{2} \bar{\mu}^2\right) + O(\mu^3) \\ &= (1 + \zeta_p^{-1}) \left(1 + \frac{1-q}{2q^2} \mu^2 \zeta_p\right) + O(\mu^3) \\ &= (1 + \zeta_p^{-1}) \left(1 + \frac{1-q}{2q^2} (x-1)^2 \frac{\zeta_p}{(1-\zeta_p)^2}\right) + O(\mu^3). \end{aligned}$$

Again, we take the norm and get

$$N(u) = 1 + \frac{1-q}{2q^2} (x-1)^2 \underbrace{\sum_{\substack{\zeta \in \mu_p \\ \zeta \neq 1}} \frac{\zeta}{(1-\zeta)^2}}_{=:s_p} + O(\mu^3).$$

It is well known that the sum s_p has the value $\frac{1-p^2}{12}$. This time the condition $N(u) = 1$ tells us that $\mu^3 = \frac{(x-1)^3}{\pi^3}$ divides $\frac{(1-q)(x-1)^2(p^2-1)}{24q^2}$ in \mathbb{Z}_p and furthermore that $x-1$ divides $\frac{(1-q)(p^2-1)\pi^3}{24q^2}$. Recall that p^{q-1} divides $x-1$, thus it has to divide $\frac{(1-q)\pi^3}{3}$ as well. This implies $p^{q-1}|q-1$ in \mathbb{Z}_p and thus in \mathbb{Z} , which is absurd since p^{q-1} is much larger than $q-1$. Finally we arrived at a contradiction, thus the initial assumption that $(x-\zeta_p)^{1-t}$ was trivial in H is wrong. \square

THEOREM 3: THE RELATIVE BOUNDS

In this chapter, we prove Mihăilescu's third theorem. This is the point where we leave Mihăilescu's original path to prove the conjecture. His first proof was a similar, but asymmetric condition for p and q , and it could be checked by a computer calculation that no such p and q exist. However, a little later he found a way to avoid this computation, by proving the following theorem:

Theorem 5.1 (Mihăilescu's Theorem 3, 2004). *We have*

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

It is based on the fact that x and y have to be quite large in absolute value, which is the case by Cassels' Relations.

Define $X := \text{Ann}_{\mathbb{F}_q[G]}(x - \zeta_p)$ to be the annihilator of $x - \zeta_p$, i.e. the ideal in $\mathbb{F}_q[G]$ consisting of the elements θ such that $(x - \zeta_p)^\theta$ is a q -th power.

Lemma 5.2. There is an injective homomorphism

$$X \longrightarrow \mathbb{Q}(\zeta_p)^* / (\mathbb{Q}(\zeta_p)^*)^q,$$

sending an annihilator θ to the element $\alpha \in \mathbb{Q}(\zeta_p)^*$ for which $(x - \zeta_p)^\theta = \alpha^q$.

Proof. Since $\mathbb{Q}(\zeta_p)^*$ does not contain any primitive q -th roots of unity, the image α is well-defined. In the proof of proposition 2.4 we have already seen that the conjugates of $\frac{x - \zeta_p}{1 - \zeta_p}$ are multiplicatively independent. By Cassels' Relations, we know that $|x| \geq q^{p-1} - 1 \geq 3$, and hence the norms of the conjugates are strictly larger than 1 and they can not be units:

$$N\left(\frac{x - \zeta}{1 - \zeta}\right) = \frac{|\prod_{1 \leq i \leq p-1} (x - \zeta^i)|}{p} \geq \frac{(|x| - 1)^{p-1}}{p} > 1.$$

Hence they are divisible by distinct prime ideals of $\mathbb{Z}[\zeta_p]$. □

Proposition 5.3. *Suppose $p, q \geq 11$. If θ is a non-zero element in $X \cap (1 - \iota)\mathbb{Z}[G] \subset \mathbb{Z}[G]$ such that $\|\theta\| \leq \frac{3q}{p-1}$ and $\alpha \in \mathbb{Q}(\zeta_p)^*$ is such that $(x - \zeta_p)^\theta = \alpha^q$, then for any $\sigma \in G$*

$$|\arg(\sigma(\alpha))| > \frac{\pi}{q}.$$

Proof. The proof consists of a contradiction involving the norm of the denominator of $\alpha - 1$, very similar to diophantine approximations.

Suppose $0 \neq \theta = \sum_{\tau \in G} n_\tau \tau$ satisfies the conditions of the proposition and assume there is a σ such that $|\arg(\sigma(\alpha))| \leq \frac{\pi}{q}$. The element θ is in $(1 - \iota)$, hence $\iota\theta = -\theta$ and

$$|\sigma(\alpha)|^{2q} = |(x - \zeta_p)^{\sigma\theta}|^2 = (x - \zeta_p)^{\sigma\theta + \sigma\iota\theta} = (x - \zeta_p)^{\sigma\theta - \sigma\theta} = 1,$$

and so we get $|\sigma(\alpha)| = 1$. For the same reason we get $n_{\iota\tau} = -n_\tau$, hence $s = \sum_\tau n_\tau = 0$ and we can write

$$\alpha^q = (x - \zeta_p)^\theta = \prod_\tau (x - \tau(\zeta_p))^{n_\tau} = \underbrace{x^s}_{=1} \prod_\tau \left(1 - \frac{\tau(\zeta_p)}{x}\right)^{n_\tau}.$$

Recall that $|x| \geq q^{p-1} + q$ is very large, so the following Taylor expansion of the principal branch of the complex logarithm is justified:

$$\begin{aligned} |\arg(\sigma(\alpha)^q)| = |\log(\sigma(\alpha)^q)| &= \sum_\tau \left| n_\tau \log \left(1 - \frac{\tau(\zeta_p)}{x}\right) \right| \\ &\leq \sum_\tau \left| n_\tau \sum_{k \geq 1} \frac{\tau(\zeta_p)^k}{kx^k} \right| \leq \frac{\|\theta\|}{|x| - 1}. \end{aligned}$$

By our assumption that $|\arg(\sigma(\alpha))| < \frac{\pi}{q}$ it is clear that

$$\arg(\sigma(\alpha)^q) = q \arg(\sigma(\alpha)).$$

Using this and the bound on the size of θ we even have

$$\arg(\sigma(\alpha)) \leq \frac{\|\theta\|}{q(|x| - 1)} < \frac{1}{q^{p-1}}.$$

Thus α has to be very close to 1, and since $\sigma(\alpha) = e^{i \arg(\sigma(\alpha))}$ we can use the Taylor expansion of the exponential to estimate

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

Obviously, the same is true for the complex conjugate of $\sigma(\alpha)$. For the other conjugates of α we have $|\tau(\alpha) - 1| \leq |\tau(\alpha)| + 1 = 2$. Knowing bounds for all conjugates of $\alpha - 1$ we can bound its norm

$$|N(\alpha - 1)| \leq \left(\frac{2\|\theta\|}{q(|x| - 1)} \right)^2 2^{p-3}.$$

By lemma 5.2, α is non-zero as well. The denominator J of $\alpha - 1 \in \mathbb{Z}[\zeta_p]$ is equal to the denominator of α , and since all the functions used are multiplicative we can even use α^q to get useful bounds. We have already seen that $n_{\iota\tau} = -n_\tau$, therefore the numerator and the denominator of $\alpha^q = (x - \zeta_p)^\theta$ have the same norm. Hence we can square the norm of α^q to get rid of the signs and get the bound

$$N(J)^{2q} = N(\alpha^q)^2 \leq N \left(\prod_\tau (x - \zeta_p)^{|n_\tau|} \right) \leq (|x| + 1)^{(p-1)\|\theta\|}.$$

Therefore we have the inequality

$$(|x| + 1)^{-\frac{(p-1)}{2q} \|\theta\|} \leq \frac{1}{N(J)} \leq |N(\alpha - 1)| \leq \left(\frac{2\|\theta\|}{q(|x| - 1)} \right)^2 2^{p-3}.$$

Now $|x|$ is large enough to satisfy $(|x| + 1)^2 \leq 2(|x| - 1)^2$ and hence

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

Using the bound of the size of θ we get $2 - \frac{(p-1)}{2q} \|\theta\| \geq 2 - 3/2 \geq 1/2$ and $\|\theta\|/q \leq 3/p$, and hence

$$(\sqrt{q})^{p-1} \leq \sqrt{|x| + 1} \leq 2^p \left(\frac{3}{p} \right)^2 \leq 2^{p-1}.$$

This contradicts $q \geq 11$ by far, and the proposition holds even for $q \geq 5$. \square

The next proposition states that if $q > 4p^2$, then the proposition just proven can not hold, leading to a contradiction. But first, we need two little lemmas:

Lemma 5.4. Let $k \geq 2$ and $s \geq 6$ be integers satisfying $s + 2k \geq 13$. Then

$$\binom{s+k}{s} > \frac{4}{3}(s+1)k^2 + 1.$$

Proof. If the pair (s, k) satisfies the inequality and $s' \geq s, k' \geq k$, then the pair (s', k') satisfies the inequality as well. The smallest pairs that satisfy all conditions for s and k are $(6, 4)$, $(7, 3)$ and $(9, 2)$, and in each case the inequality holds. \square

Lemma 5.5. Assume $q > 4p^2$ and $p, q \geq 11$. Then there exist at least $q + 1$ elements $\theta \in I$ such that $\|\theta\| \leq \frac{3}{2} \frac{q}{p-1}$.

Proof. Recall that I has a \mathbb{Z} -basis $\{e_i\}$ for $1 \leq i \leq (p-1)/2$ such that all e_i have size $p-1$. Now one can choose non-negative integers λ_i such that $\sum_i \lambda_i \leq s := \left\lfloor \frac{3q}{2(p-1)^2} \right\rfloor$ and define $\theta := \sum_i \lambda_i e_i$. For such a θ we have

$$\|\theta\| \leq (p-1) \sum_i \lambda_i \leq (p-1)s \leq \frac{3q}{2(p-1)}.$$

There are $\binom{s + \frac{p-1}{2}}{s}$ such elements θ . Since $\|-\theta\| = \|\theta\|$, there are $2 \binom{s + \frac{p-1}{2}}{s} - 1$ elements in I of size at most $\frac{3q}{2(p-1)}$. Now we apply lemma 5.4 with $k = \frac{p-1}{2}$ and get that there are at least

$$2 \cdot \frac{4}{3}(s+1) \frac{(p-1)^2}{4} + 1 > 2 \cdot \frac{1}{3} \frac{3q}{2(p-1)^2} (p-1)^2 + 1 = q + 1$$

such elements. We are allowed to use the lemma since $k = \frac{p-1}{2} \geq 5$ and $s = \left\lfloor \frac{3q}{2(p-1)^2} \right\rfloor > \left\lfloor \frac{3 \cdot 4}{2} \right\rfloor = 6$. \square

Proposition 5.6. *Assume $q > 4p^2$ and $p, q \geq 11$. Then for all $\sigma \in G$ there exists a nonzero θ in $I \subset \mathbb{Z}[G]$ with $\|\theta\| \leq \frac{3q}{p-1}$, such that $|\arg(\sigma(\alpha))| \leq \pi/q$, where α is the unique element in $\mathbb{Q}(\zeta_p)^*$ satisfying $(x - \zeta_p)^\theta = \alpha^q$.*

Proof. Fix $\sigma : \mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C}$. By lemma 5.5 we can find at least $q + 1$ elements $\theta_0, \dots, \theta_q \in I$ having $\|\theta_i\| \leq \frac{3}{2} \frac{q}{p-1}$, and each of them annihilates $x - \zeta_p \in H$. As in the proof for Proposition 5.3, we find a bound on the absolute value of the argument of $\sigma(\alpha_i)$, but this time we find that there exist integers $k_i \in \mathbb{Z}$ such that

$$\left| \arg(\sigma(\alpha_i)) - \frac{2\pi k_i}{q} \right| \leq \frac{\|\theta_i\|}{q(|x| - 1)}.$$

By the pigeon hole principle, at least 2 of these k_i differ by a multiple of q , say k_0 and k_1 . Choose $\theta := \theta_0 - \theta_1$. Then the associated α satisfies

$$|\arg(\sigma(\alpha))| \leq \frac{\|\theta\|}{q(|x| - 1)} \leq \frac{3}{(p-1)q^{p-1}} < \frac{\pi}{q}.$$

□

The proof for Mihăilescu's third Theorem is now immediate:

Proof of Mihăilescu's Theorem 3. By Mihăilescu's Theorem 4, the lower bounds for p, q are much larger than 11. By symmetry assume that $q > 4p^2$. Then both proposition 5.3 and 5.6 apply. Since $I \subset X \cap (1 - \iota)\mathbb{Z}[G]$, this is a contradiction. □

CHAPTER 6

THEOREM 1: THE PLUS ARGUMENT

Theorem 1 is the main result of Mihăilescu and is proven, in contrast to his other theorems, by using the plus part of the class group, which is invariant under complex conjugation.

6.1 Preliminaries on Power Series

As usual, let p, q be odd primes. For $\theta = \sum_{\tau \in G} n_\tau \tau \in \mathbb{Z}[G]$, let

$$(1 - \tau(\zeta_p)T)^{n_\tau/q} = \sum_{k \geq 0} \binom{n_\tau/q}{k} (-\tau(\zeta_p)T)^k \in \mathbb{Q}(\zeta_p)[[T]],$$

and define

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

For $\sigma \in G$, let $F^\sigma(T)$ denote the power series obtained by applying σ to the coefficients of F .

Lemma 6.1. Let R be a commutative domain of characteristic 0 and let $I \subset R$ be an ideal. Suppose the two power series $\sum_{k \geq 0} \frac{a_k}{k!} T^k$ and $\sum_{k \geq 0} \frac{b_k}{k!} T^k$ in $R[[T]]$ have the property that there exist $a, b \in R$ such that

$$\forall k \geq 0: \quad a_k \equiv a^k \pmod{I}, \quad b_k \equiv b^k \pmod{I}.$$

Then the product of the two power series is $\sum_{k \geq 0} \frac{c_k}{k!} T^k$ where $c_k \equiv (a + b)^k \pmod{I}$.

Proof.

$$\begin{aligned} \frac{c_k}{k!} &= \sum_{l+m=k} \frac{a_l}{l!} \frac{b_m}{m!} = \frac{1}{k!} \sum_{l+m=k} a_l b_m, \\ c_k &\equiv \sum_{l+m=k} \binom{k}{m} a^l b^m = (a + b)^k \pmod{qR}. \end{aligned}$$

□

Proposition 6.2. The power series F has the following properties:

- (i) Its coefficients are integral outside of q .
- (ii) There exist $a_k \in \mathbb{Z}[\zeta_p]$ having $a_k \equiv (-\sum_{\tau} n_{\tau} \tau(\zeta_p))^k \pmod{q}$, such that

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

- (iii) For all $\sigma \in G$ and all $t \in (-1, 1)$, we obtain a converging series when evaluating F^σ at t . Call its value $F^\sigma(t)$. Denote by $F_k^\sigma(T)$ the sum of the terms of degree up to k , and write $m = \frac{1}{q} \sum_{\tau} n_{\tau}$. If furthermore $0 \leq n_{\tau} \leq q$, then we have for any $k \geq 0$

$$|F^\sigma(t) - F_k^\sigma(t)| \leq \binom{-m}{k+1} \frac{|t|^{k+1}}{(1-|t|)^{m+k}}.$$

Proof. Part (i) comes from the fact that for $x \in \mathbb{Q}^*$ the binomial coefficient $\binom{x}{n}$ is integral outside the prime divisors of the denominator of x .

For the second part, consider the power series

$$(1 - \tau(\zeta_p)qT)^{n_{\tau}/q} = \sum_{k \geq 0} \frac{n_{\tau}(n_{\tau} - q) \dots (n_{\tau} - (k-1)q)}{k!} (-\tau(\zeta_p)T)^k.$$

This power series has coefficients of the form $\frac{a_k}{k!}$ having $a_k \equiv (-\tau(\zeta_p)n_{\tau})^k \pmod{q}$. Thus we can apply lemma 6.1 to get the product

$$F(qT) = \sum_{k \geq 0} \frac{c_k}{k!} T^k, \quad \text{with } c_k \equiv \left(-\sum_{\tau} \tau(\zeta_p) n_{\tau} \right)^k \pmod{q}.$$

For the third part, observe that

$$\left| \binom{n_\tau/q}{k} \right| \leq \left| \binom{-n_\tau/q}{k} \right|,$$

so the absolute values of the coefficients of the series $\sum_{k \geq 0} \binom{n_\tau/q}{k} (-\tau(\zeta_p)T)^k$ are smaller than those of the series $\sum_{k \geq 0} \binom{-n_\tau/q}{k} (-T)^k = (1-T)^{-n_\tau/q}$, whose coefficients are all positive. Therefore, when we apply σ , we get that the coefficients of $F^\sigma(T)$ are bounded by those of

$$\begin{aligned} \prod_{\tau \in G} (1-T)^{-n_\tau/q} &= (1-T)^{-1/q \sum_{\tau} n_\tau} = (1-T)^{-m} \\ &= \sum_{k \geq 0} \binom{-m}{k} (-1)^k T^k =: S(T). \end{aligned}$$

Hence we find for all complex $|t| < 1$

$$\begin{aligned} |F^\sigma(t) - F_k^\sigma(t)| &\leq |S(|t|) - S_k(|t|)| \leq \frac{|S^{(k+1)}(|t|)|}{(k+1)!} |t|^{k+1} \\ &\leq \left| \binom{-m}{k+1} \right| \frac{|t|^{k+1}}{(1-|t|)^{m+k+1}}. \end{aligned}$$

□

Proposition 6.3. *If θ is contained in the ideal $(1 + \iota) \subset \mathbb{Z}[G]$, then*

- i) *the power series $F(T)$ is contained in the subring $\mathbb{Q}(\zeta_p^+) [[T]]$,*
- ii) *if $t \in \mathbb{Q}$ satisfies $|t| < 1$ and $(1 - t\zeta_p)^\theta = \beta^q$ for some $\beta \in \mathbb{Q}(\zeta_p^+)$, then $F^\sigma(t) = \sigma(\beta)$ for all $\sigma \in G$.*

Proof. For the first part, observe that since $\theta \in (1 + \iota)\mathbb{Z}[G]$, its coefficients satisfy $n_\tau = n_{\iota\tau}$ for all $\tau \in G$. But then the products can be partitioned into two parts that are equal up to complex conjugation, so the product of these two parts is real. Since $\mathbb{R} \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p^+)$, this proves i).

For the second part, we have

$$\sigma(\beta)^q = \sigma((1 - t\zeta_p)^\theta) = \prod_{\tau} (1 - t\sigma(\tau(\zeta_p)))^{n_\tau} \in \mathbb{R}.$$

Since this product is finite, we can take the unique real q -th root and get $F^\sigma(t) = \sigma(\beta)$. □

Recall that $G^+ = G/\langle \iota \rangle$ and that H^+ is the subgroup of H containing the elements which are invariant under complex conjugation.

Theorem 6.4. *Suppose $p, q \geq 7$ and $|x| \geq q^{p-1} + q$. Then the $\mathbb{F}_q[G^+]$ -submodule of H^+ generated by the image of $(x - \zeta_p)^{1+\iota}$ has a trivial annihilator.*

Remark. In other words, the generated submodule is free.

Proof. Suppose that $\bar{\psi} \in \mathbb{F}_q[G^+]$ annihilates $(x - \zeta_p)^{1+\iota}$ in H . This implies that for any lift $\theta = \sum_{\tau} n_{\tau} \tau \in \mathbb{Z}[G]$ of $\pm(1 + \iota)\bar{\psi}$, there exists an $\alpha \in \mathbb{Q}(\zeta_p)^*$ such that $(x - \zeta_p)^{\theta} = \alpha^q$. But since $\pi = 1 - \zeta_p$ divides all conjugates of $x - \zeta_p$ exactly once, this condition means that

$$\sum_{\tau} n_{\tau} = \text{ord}_{\pi}((x - \zeta_p)^{\theta}) \equiv \text{ord}_{\pi}(\alpha^q) \equiv 0 \pmod{q}.$$

We choose a lift θ as follows: Reduce the coefficients n_{τ} modulo q , i.e. $0 \leq n_{\tau} < q$ for all $\tau \in G$. Then the element $\theta' = -\theta + q \sum_{\tau} \tau$ is a lift as well, it has all its coefficients between 1 and q , and its size is a multiple of q as well. The coefficients of their sum $\theta + \theta' = q \sum_{\tau} \tau$ is exactly $q(p-1)$, hence there is one with size at most $q \cdot \frac{p-1}{2}$. Call that one θ from now on. By construction, the size of θ is $m q$ for an integer $0 \leq m \leq \frac{p-1}{2}$. If $m = 0$, we are done, so assume $m \geq 1$. Also, the construction did not change the property that $n_{\tau} = n_{\iota\tau}$, so our chosen θ is still equal to $(1 + \iota)\psi$ for a lift $\psi \in \mathbb{Z}[G^+]$ from $\bar{\psi} \in \mathbb{F}_q[G^+]$.

Since $\theta \in (1 + \iota)\mathbb{Z}[G]$, the number $(x - \zeta_p)^{\theta}$ is not only contained in $\mathbb{Z}[\zeta_p]$, but in $\mathbb{Z}[\zeta_p^+]$ as well, and furthermore totally positive. Write $(x - \zeta_p)^{\theta} = \alpha^q$ for some $\mathbb{Z}[\zeta_p^+]$; It is unique und totally positive as well. Out of this data, we build a power series: Write

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

Then $\alpha = x^m F\left(\frac{1}{x}\right)$ and by proposition 6.3 we even have

$$\sigma(\alpha) = x^m F^{\sigma}\left(\frac{1}{x}\right).$$

As before denote $F_m(T)$ the polynomial that consists of the terms of degree at most m of F . We claim that for every σ , the inequality

$$q^{m + \text{ord}_q(m!)} |\sigma(\alpha) - x^m F_m^{\sigma}(1/x)| < 1$$

holds: To see this, notice that the left hand term

$$q^{m + \text{ord}_q(m!)} |x^m F^{\sigma}(1/x) - x^m F_m^{\sigma}(1/x)|$$

can be bounded by

$$\begin{aligned} q^{m + \frac{m}{q-1}} \left| \frac{1}{x} \binom{-m}{m+1} \right| \left(1 - \frac{1}{|x|}\right)^{-2m} &\leq \frac{1}{|x|} q^{m + \frac{m}{q-1} + m \frac{\log 4}{\log q}} \left(1 - \frac{1}{|x|}\right)^{-2m} \\ &\leq q^{\frac{p-1}{2}(-1 + \frac{1}{q-1} + \frac{\log 4}{\log q})} \left(1 - \frac{1}{q^{p-1}}\right)^{-p}. \end{aligned}$$

In the first inequality, we used $\left| \binom{-m}{m+1} \right| = \binom{2m}{m+1} \leq 4^m$, and in the second we took the properties $m \leq \frac{p-1}{2}$ and $|x| \geq q^{p-1}$.

The logarithm of the expression we got, divided by $\log q$, is

$$\frac{p-1}{2} \left(-1 + \frac{1}{q-1} + \frac{\log 4}{\log q} \right) - p \log \left(1 - \frac{1}{q^{p-1}} \right) / \log q.$$

But $-\log(1 - \frac{1}{q^{p-1}}) \leq 1/(q^{p-1} - 1) \leq 1/(q^2 - 1)$ and $q \geq 7$, hence we can bound the expression further to

$$\frac{p-1}{2} \left(-1 + \frac{1}{6} + \frac{\log 4}{\log 7} \right) + \frac{p}{48 \log 7} < 0$$

for all p . Hence the claim is proven.

The preceding propositions 6.2 and 6.3 tell us that if we multiply $F_m(T)$ by a high enough power of q , then the product will have coefficients in $\mathbb{Z}[\zeta_p^+]$; They even tell us that multiplying with $q^{m+\text{ord}_q(m!)}$ will do. Hence the number $q^{m+\text{ord}_q(m!)}(\alpha - x^m F_m(1/x))$ is even contained in $\mathbb{Z}[\zeta_p^+]$. But by the claim above, all conjugates of this number have absolute values below 1, so the norm is 0 and hence

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

All coefficients of this polynomial are algebraic integers. Furthermore, all of them are divisible by q , except maybe the one of a_m – But the left hand side is divisible by q as well, and so this coefficient has to be divisible by q as well. Now, the second part of proposition 6.2 tells us that

$$0 \equiv a_m \equiv \left(- \sum_{\tau} n_{\tau} \tau(\zeta_p) \right)^m \pmod{q}.$$

But the only nilpotent element in $\mathbb{Z}[\zeta_p]/(q)$ is zero, hence

$$\sum_{\tau} n_{\tau} \tau(\zeta_p) \equiv 0 \pmod{q}.$$

This is only possible if $n_{\tau} \equiv 0 \pmod{q}$ for all $\tau \in G$, which implies that $\psi \equiv 0 \pmod{q}$ in $\mathbb{Z}[G^+]$ as required. \square

6.2 Semi-simple Rings and Theorem 1

Recall that H' is the subgroup of elements of H that are a q -th powers modulo q^2 . To prove Theorem 1, we show that $p \not\equiv 1 \pmod{q}$ gives the existence of an annihilator of $H' \cap H^+$, contradicting Theorem 6.4. This is accomplished by observing that in this case p does not divide $|G^+|$, so $\mathbb{F}_q[G^+]$ is semi-simple, i.e. a product of fields.

Definition 6.5. Let C be the group of cyclotomic p -units, i.e. the multiplicative subgroup of $\mathbb{Q}(\zeta_p)^*$ generated by the roots of unity and $1 - \zeta_p^k$, and let C_q be the subgroup of C consisting of the elements that are q -th roots modulo q^2 .

For this group, we have Thaine's Theorem:

Theorem 6.6 (Thaine, 1988). *Let p be an odd prime and $G = \text{Gal}(\mathbb{Q}(\zeta_p)^+/\mathbb{Q})$. If q is an odd prime such that q does not divide $p(p-1)$, then any annihilator $\theta \in \mathbb{Z}[G]$ of E/CE^q also annihilates Cl/Cl^q .*

Proofs of this theorem can be found in various sources. A high-level version can be found in the appendix of [16], whereas the version in the appendix of [14] takes a rather pedestrian approach.

Before we dive into the proof of Theorem 1, we introduce some more notation and provide useful lemmas.

Lemma 6.7. *If $p \not\equiv 1 \pmod{q}$, then E/E^q is a free $\mathbb{F}_q[G^+]$ -module of rank 1, and $\mathbb{F}_q[G^+]$ is semi-simple.*

Proof. Under the assumption $p \not\equiv 1 \pmod{q}$ we know that q does not divide $|G^+|$, and it is a well-known fact from representation theory that $\mathbb{F}_q[G^+]$ is semi-simple in this case. (cf. Maschke's Theorem)

To see that E/E^q is a free module of rank 1, we observe that E/E^q has just as many elements as $\mathbb{F}_q[G^+]$ by using the isomorphism $E/E^q \simeq U/U^q \times \mathbb{Z}/q\mathbb{Z}$ where U is the unit group of $\mathbb{Z}[\zeta_p]$, and counting the elements via Dirichlet's unit theorem.

It is now sufficient to show that E/E^q has a trivial $\mathbb{F}_q[G^+]$ -annihilator. Let U^+ denote the unit group of $\mathbb{Z}[\zeta_p^+]$. Then

$$E/E^q \simeq U/U^q \times \mathbb{Z}/q\mathbb{Z} \simeq (U^+/\{\pm 1\})/(U^+/\{\pm 1\})^q \times \mathbb{Z}/q\mathbb{Z}.$$

Let's have a look at the annihilator of $U^+/\{\pm 1\}$: By imitating the proof of Dirichlet's unit theorem, one can show that any $\sum_{\sigma \in G^+} a_\sigma \sigma$ annihilating that module has to be of the form $a \cdot \sum_{\sigma \in G^+} \sigma$, i.e. we can write $s := \sum_{\sigma \in G^+} \sigma$ and

$$\text{Ann}_{\mathbb{F}_q[G^+]}(U^+/\{\pm 1\}) = s\mathbb{Z}[G^+].$$

This even works modulo q th powers, and we deduce

$$\text{Ann}_{\mathbb{F}_q[G^+]}((U^+/\{\pm 1\})/(U^+/\{\pm 1\})^q) = s\mathbb{F}_q[G^+].$$

Choose an $\alpha = \sum_{\sigma \in G^+} a_\sigma \sigma \in \mathbb{Z}[G^+]$ such that $\alpha \cdot s$ annihilates E/E^q . In particular, $\alpha \cdot s$ annihilates $\pi = 1 - \zeta_p$, i.e. there is a unit u such that $\pi^{\alpha \cdot s} = u \cdot \pi^{\sum_{\sigma \in G^+} a_\sigma \frac{p-1}{2}} \in E^q$. Hence $\sum_{\sigma \in G^+} a_\sigma \frac{p-1}{2} \equiv 0 \pmod{q}$. The condition $p \not\equiv 1 \pmod{q}$ tells us now that $\sum_{\sigma \in G^+} a_\sigma \equiv 0 \pmod{q}$ and finally

$$\alpha \cdot s = \sum_{\tau \in G^+} \left(\sum_{\sigma \in G^+} a_\sigma \right) \sigma \tau \in q\mathbb{Z}[G^+].$$

Hence the annihilator of E/E^q in $\mathbb{F}_q[G^+]$ is trivial. \square

Proposition 6.8. *If $C = C_q$, then $p < q$.*

Proof. Let ζ be a primitive p -th root of unity in $\mathbb{Q}(\zeta_p)$ and assume $C = C_q$. Then there exists a $u \in E$ such that

$$\frac{1 - \zeta^{2q}}{1 - \zeta^q} = 1 + \zeta^q = u^q \pmod{q^2}.$$

Hence $(1 + \zeta)^q \equiv 1 + \zeta^q = u^q \pmod{q}$. Both sides are q -th powers, so we even have $(1 + \zeta)^q \equiv 1 + \zeta^q \pmod{q^2}$. Thus the polynomial

$$W(T) := \frac{(1 + T)^q - T^q - 1}{qT} \in \mathbb{F}_q[T]$$

is zero at every p -th root of unity ζ , implying that the p -th cyclotomic polynomial divides $W(T)$. Hence the degree $q - 2$ of $W(T)$ is at least $p - 1$, so $q > p$ holds. \square

Theorem 6.9. *Suppose that $p > q$ and $p \not\equiv 1 \pmod{q}$. Then the $\mathbb{F}_q[G^+]$ -module $H' \cap H^+$ has a non-zero annihilator.*

Proof. Recall that $E = \mathbb{Z}[\zeta_p, \frac{1}{p}]^*$ is the group of p -units. We denote by E_q its subgroup $\{\alpha \in E \mid \alpha \text{ is a } q\text{-th power modulo } q^2\}$. The exact sequence of lemma 2.2 iii) can then be rewritten to the exact sequence

$$0 \longrightarrow E_q/E^q \longrightarrow H' \cap H^+ \longrightarrow Cl^+[q]. \quad (5)$$

Then we have a filtration

$$0 \subset C_q E^q/E^q \subset CE^q/E^q \subset E/E^q$$

with quotients $E_1 = C_q E^q/E^q$, $E_2 = CE^q/C_q E^q$ and $E_3 = E/CE^q$.

Lemma 6.7 tells us that E/E^q is free of rank 1 and that $\mathbb{F}_q[G^+]$ is semi-simple, so all modules over $\mathbb{F}_q[G^+]$ are semi-simple as well. So we can write

$$E_1 \oplus E_2 \oplus E_3 \simeq \mathbb{F}_q[G^+] \simeq \mathbb{F}_q[X]/(X^{\frac{p-1}{2}} - 1)$$

and there are monic polynomials μ_i such that their principal ideal $(\mu_i) = \text{Ann}(E_i)$ satisfy $E_i \simeq \mathbb{F}_q[X]/\text{Ann}(E_i)$. Their product also satisfies $\mu_1 \mu_2 \mu_3 = X^{\frac{p-1}{2}} - 1$.

We also have $E_q/E^q \simeq E_1 \oplus E_q/C_q E^q$. Furthermore $E_q/C_q E^q \subset E/CE^q = E_3$ since the composition $E_q \hookrightarrow E \rightarrow E/CE^q$ has the kernel $E_q \cap CE^q$. In view of the sequence (5) we get an injection

$$H' \cap H^+ \hookrightarrow E_1 \oplus E_3 \oplus Cl^+[q].$$

Since μ_3 annihilates $E_3 = E/CE^q$, it also annihilates $Cl^+/Cl^{+q} \simeq Cl^+[q]$ by Thaine's Theorem 6.6. So the product $\mu_1 \mu_3$ annihilates $H' \cap H^+$.

Assume the product to be zero in $\mathbb{F}_q[G^+] \simeq \mathbb{F}_q[X]/(X^{\frac{p-1}{2}} - 1)$, leaving μ_2 to be a unit and $E_2 = 0$, i.e. $C = C_q$. Proposition 6.8 then tells us that $p < q$, contradicting the prerequisite $p > q$. Hence $\mu_1 \mu_3$ is a non-zero annihilator of the module $H' \cap H^+$. \square

Theorem 6.10 (Mihăilescu's Theorem 1, 2002). *We have*

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

Proof. By symmetry let $p > q$. Then $q \equiv 1 \pmod{p}$ obviously can not hold. Assume that $p \equiv 1 \pmod{q}$ holds neither. By Mihăilescu's Theorem 4 we can assume that $p, q \geq 7$, so we can use theorem 6.4 and the $\mathbb{F}_q[G^+]$ -submodule generated by $(x - \zeta_p)^{1+i}$ in $H' \cap H^+$ has no trivial annihilator. On the other hand, $(x - \zeta_p)^{1+i}$ is contained in $H' \cap H^+$ by corollary 3.4. But $H' \cap H^+$ has a non-trivial annihilator by Theorem 6.9, contradiction.

Hence one of the two congruences has to hold. □

BIBLIOGRAPHY

- [1] Y. Bilu. Catalan's Conjecture (after Mihăilescu). Séminaire Bourbaki, 2002.
- [2] J. W. S. Cassels. On the equation $a^x + b^y = 1$, ii. *Proc. Cambridge Society*, 56:97–103, 1960.
- [3] E. Catalan. Note extraite d'une lettre adressée à l'éditeur. *J. reine angew. Math.*, 27:192, 1844.
- [4] Henri Cohen. *Number Theory. Volume 1: Tools and Diophantine Equations*. Springer Verlag, 2007.
- [5] H. M. Edwards. *Fermat's Last Theorem*. Springer Verlag, 1977.
- [6] K. Inkeri. On Catalan's problem. *Acta Arith.*, 9:285–290, 1964.
- [7] Matti Jutila and Tauno Metsänkylä. *Number Theory*, pages 247–254. Walter der Gruyter, 2001.
- [8] Chao Ko. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica*, 14:457–460, 1965.
- [9] Neal Koblitz. *p-adic Integers, p-adic Analysis and Zeta-Functions*. Springer Verlag, 1984.
- [10] M. Langevin. Quelques applications de nouveaux résultats de Van der Poorten. *Sém. Delange-Pisot-Poitou*, 17, 1975/1976.
- [11] V. A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. *Nov. Ann. Math*, 9:178–181, 1850.
- [12] Preda Mihăilescu. A class number free criterion for Catalan's conjecture. *Journal of Number Theory*, 99:225–231, 2000.
- [13] J. S. Milne. *Algebraic Number Theory*. Lecture Notes, 1998.
- [14] Maurice Mischler and Jacques Boéchat. La conjecture de Catalan racontée à un ami qui a le temps. arXiv:math/0502350v4 [math.NT], 2005.
- [15] Paulo Ribenboim. *Catalan's Conjecture: Are 8 and 9 the Only Consecutive Powers?* Academic Press, 1994.
- [16] René Schoof. *Catalan's Conjecture*. Springer Verlag, to appear.
- [17] R. Tijdeman. On the equation of Catalan. *Acta Arithm.*, 29:197–209, 1976.