

Je ne fais pourtant de tort a personne,
 En suivant les ch'mins qui n' mèn'nt pas à Rome,
 Mais les brav's gens n'aiment pas que
 L'on suive une autre route qu'eux... ¹

To Emma, the child who will grow

PRIMARY CYCLOTOMIC UNITS AND A PROOF OF CATALAN'S CONJECTURE. DRAFT

PREDA MIHĂILESCU

ABSTRACT. Catalan's conjecture states that the equation $x^p - y^q = 1$ has no other integer solutions but $3^2 - 2^3 = 1$. A classical result of Cassels and our recent consequence establish that p, q must verify a *double Wieferich condition* if the equation has integer solutions with p, q odd. If $p \equiv 1 \pmod q$, then a contradiction to the above follows from Baker's methods in transcendence theory. If $p \not\equiv 1 \pmod q$, then the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ has order coprime to q . We show that the existence of solutions to Catalan's equation produces an excess of q - *primary cyclotomic* units in this case. This fact leads to a contradiction which proves Catalan's conjecture.

1. INTRODUCTION

Journal de Crelle published the following small note of E. Catalan in its volume **27** of 1844 (Fig. 1): *"Sir, please state the following theorem in your journal; I believe it to be true, although I could not prove it completely so far: others might be luckier. 'Two consecutive integers, other than 8 and 9, cannot be exact powers. In other words, the equation $x^m - y^n = 1$ admits no solution in the positive integers' ". The young *répétiteur* had made a reputation with his elegant solution to the problem of dissecting a polygon into triangles by means of non-intersecting diagonals, but had a career which was strongly handicapped by his extreme left wing views and activities. Whether correlated to this or only coincidentally, the published note appears as lost in an attic, among the errata to the last volumes of Crelle.*

Briefly, Catalan conjectured that the equation $X^U - Y^V = 1$ has no other solution in *positive* integers except $3^2 - 2^3 = 1$. If such a solution would exist and $p|U$ and $q|V$ are primes, it is clear by setting $x = X^{U/p}$ and $y = Y^{V/q}$, that a solution exists to the equation:

$$(1) \quad x^p - y^q = 1 \text{ with } p, q \text{ distinct primes}$$

¹"La mauvaise réputation", by Georges Brassens

Date: Version 10.0 July 10, 2002.

If x, y are coprime integers and $n > 1$, an elementary calculation shows that

$$\left(\frac{x^n \pm y^n}{x \pm y}, x \pm y \right) \mid n$$

One writes $x = (x \pm y) \mp y$ and then expands. This fact (see e.g. [36] P1.2) was known at Catalan's time and had been used to distinguish the two cases of Fermat's Last Theorem. Applying it to (1), one obtains the following alternatives, which were obvious for Catalan:

Case I If $\left(p, \frac{x^p-1}{x-1} \right) = 1$ then:

$$(x-1) = r^q, \quad \frac{x^p-1}{x-1} = s^q \quad \text{and} \quad y = rs.$$

Case II $\left(p, \frac{x^p-1}{x-1} \right) = p$ then:

$$(x-1) = p^{q-1} \cdot a^q, \quad \frac{x^p-1}{x-1} = p \cdot v^q \quad \text{and} \quad y = pav.$$

The analogous cases distinction hold for $y^q + 1$.

In 1850, Lebesgue proved [22] that the equation $x^p = y^2 + 1$ has no positive integer solutions. He thus solved (1) for the case $q = 2$.

The note from 1844 seems to have been forgotten for almost hundred years. The question regained actuality in the post World War II years with Cassels' fundamental proof of the fact that the Case I of Catalan's equation with odd exponents had no solutions. Considering more generally the *integer* solutions of (1) with *odd* exponents, Cassels notes that if (x, y, p, q) fulfill (1), then so does $(-y, -x, q, p)$; certainly, if the equation has no solution in the integers, it has none in the natural numbers. Using the above simple symmetry, Cassels proved: for any non trivial solution (x, y, p, q) of (1), with p, q odd primes, the following relations hold:

$$(2) \quad \begin{aligned} x-1 &= p^{q-1}a^q & \text{and} & \quad \frac{x^p-1}{x-1} = pv^q, & y &= pav \\ y+1 &= q^{p-1}b^p & \text{and} & \quad \frac{y^q+1}{y+1} = qu^p, & x &= qbu, \end{aligned}$$

where a, b and u, v are integers for which $(pa, u) = (qb, v) = 1$.

Like a long aged wine which had gained in flavor and mystery, Catalan's conjecture now attracted a varied line of researchers. The case $p = 2$ was finally solved in 1960 by Ko Chao [18] and his solution was made available to the western readers in 1964, [19]. Together with Lebesgue's result and Cassels' milestone, it was here-with known that any solutions of (1) other then $3^2 - 2^3 = 1$ had to verify (2). In particular, if Catalan's equation has a solution, then

$$(3) \quad \frac{x^p-1}{x-1} = pv^q,$$

for some $v \in \mathbb{Z}$. This equation allows the investigation of Catalan's equation in cyclotomic fields, since it is equivalent to

$$(4) \quad \mathbf{N} \left(\frac{x-\zeta}{1-\zeta} \right) = v^q, \quad \text{with} \quad \zeta^p = 1, \quad \zeta \neq 1.$$

Hyrrö and Inkeri exploited various consequences of Cassels' work in a series of ingenious, elementary papers, thus finding bounds on $|x|, |y|$ and relations between these unknowns and Fermat quotients of $p \bmod q$ and $q \bmod p$. In 1964, Inkeri used several of these results and applied to the equation (4) a loesly related idea to

the one Eichler had used in his celebrated theorem [9] on the First Case of Fermat's Last Theorem.

He found the following criterion: if (1) has a solution with odd p, q , and $p \equiv 3 \pmod{4}$, then

$$(5) \quad q|h(\mathbb{Q}(\sqrt{-p})) \quad \text{or} \quad p^{q-1} \equiv 1 \pmod{q^2},$$

and symmetrically in p, q . Here $h(\mathbb{Q}(\sqrt{-p}))$ is the class number of the quadratic subfield of the cyclotomic field $\mathbb{Q}(\zeta)$. Primes p, q verifying $p^{q-1} \equiv 1 \pmod{q^2}$ and $q^{p-1} \equiv 1 \pmod{p^2}$ arising in Inkeri's condition were subsequently called *double Wieferich prime pairs*, an evident analogy to the famous condition $2^{p-1} \equiv 1 \pmod{p^2}$, which Wieferich had shown at the beginning of the 20-th century to be necessary for primes for which the First Case of Fermat's Last Theorem would fail. We shall refer to ulterior developments of Inkeri's work as *the algebraic track*.

Baker's fundamental results (1964) on linear forms in logarithms had soon a major impact on the study of Catalan's equation. Using A. Baker's great "Sharpening" papers for linear forms in the logarithms of algebraic numbers [2], R. Tijdeman [45] showed in 1976 by an ingenious argument that there is an effectively computable bound on the size of p and q satisfying (1). Thus Tijdeman proved that the number of solutions of (1) is finite. Although he did not give explicit bounds himself, it is possible to obtain them from [45]; in fact Langevin proved [20] in the same year that $p, q < 10^{110}$. There has been a long series of developments of this analytic approach, the *transcendence track*; it started with Glass et. al. [10] (1994) bringing Langevin's bound down to the order of 10^{26} . Further development including the works of [3], [4], [30], [31] continually improved the upper bounds for p and q . The best upper bounds proved up to date are $p < 7.15 \cdot 10^{11}$, $q < 7.78 \cdot 10^{16}$, [31].

While the goal of the transcendence track was to reduce the upper bounds on the exponents, improving (5) and eventually uncoupling the criteria in that relation was the algebraic goal. Works of Inkeri [15], Mignotte [26], Schwarz [39] and Steiner [42] consequently strengthened the class number part in (5).

In the 90'es computational efforts have been made for obtaining *lower* bounds on the exponents, by verifying the Inkeri type conditions on a computer. This third, *computational* track was most actively represented by M. Bennett and M. Mignotte, who added several ingenious elementary criteria in order to rule out isolated cases that would not contradict the current Inkeri type criteria.

On the algebraic track a major advance was achieved in spring 1999, when Bugeaud and Hanrot first succeeded to uncouple the class number condition from (5) and prove that $q|h_p^-$ if $q > \frac{p}{2} \cdot \left(1 + \frac{1}{\log q}\right)$. With their result, two *double Wieferich pairs*, (2903, 18787) and (911, 318917), which resisted both the Inkeri criteria and a special condition found by Mignotte, were ruled out and, based on the computer results of the latter, the lower bound $p, q > 10^6$ were proved [31].

In the fall of the same year, the second relation in (5) was shown [33] to hold unconditionally too. Furthermore, using results of Hyrö on the Fermat quotients of p, q , one proved that (x, y, p, q) verify (2), then also $q^2|x$ and $p^2|y$. The independent double Wieferich criterion highly simplified computer verifications and Mignotte could announce in March 2000 the lower bound $p, q > 10^7$. It appears [11] that ulterior computations led also by J. Grantham pushed these bounds as far as $p, q > 3 \cdot 10^8$. It was however evident that in order to reach a cross over point of the lower and upper bounds, computer efforts would not suffice for a long time, unless

the upper bounds could still be improved. It was a spread expectation [11], that a breakthrough could happen this way.

An important consequence of the double Wieferich criterion is the fact that if $p \equiv 1 \pmod q$ then $p \equiv 1 \pmod{q^2}$ and a fortiori, $p > q^2$. It does not take the utmost sophistication of the linear forms in logarithm apparatus which has been developed since Tijdeman for gaining upper bounds on p, q , in order to prove that $p > q^2$ is impossible. We provide in Appendix B a simple proof thereof, which is based directly on Tijdeman's arguments and was kindly provided by A. Glass. As mentioned above, Hyyrö also ingeniously worked out lower bounds on $|x|, |y|$ from Cassels' relations. For the self containment of this paper, we add in Appendix A a proof of a slightly stronger bound, which we shall use in this paper. It should however be mentioned, that the older bounds proved by Hyyrö [13] are also sufficient for the present proof.

Based upon the works of Lebesgue [22], Ko Chao [19], Cassels [7], [8], Tijdeman [45], myself [33] and the two appendixes, the results which will be used subsequently are grouped together in the following:

Theorem 1. *If Catalan's equation has solutions other than $3^2 - 2^3 = 1$, then $p, q > 10^5$,*

$$(6) \quad p \not\equiv 1 \pmod q,$$

$$(7) \quad |x| > (q^{2p-2}/2)^4,$$

Cassels relations (2) and their consequence (4) hold. Also, the double Wieferich condition

$$(8) \quad p^{q-1} \equiv 1 \pmod{q^2} \quad \text{and} \quad q^{p-1} \equiv 1 \pmod{p^2}$$

and the quadratic divisibility

$$(9) \quad q^2 \mid x \quad \text{and} \quad p^2 \mid y.$$

must hold.

Throughout this paper, we assume that (x, y, p, q) verify Catalan's equation (1) and consequently all the conditions of this theorem are fulfilled.

We close this succinct historical overview with the observation that Cassels' ruling out of the First Case of Catalan's equation, suggested by analogy to the more investigated Fermat's Last Theorem, that Catalan's might be a *plus part* problem. The present proof leads this observation to a successful end. We enclose in Appendix C more suggestive motives both relating and distinguishing Catalan's and Fermat's equations.

We refer readers wishing to know more about the subject to Ribenboim's rich historic overview [36] of Catalan's problem and Mignotte's expert [31] review of recent results, for further important information.

2. PREREQUISITES IN CYCLOTOMIC FIELDS

Let $\zeta \in \mathbb{C}$ be a primitive p -th root of unity and $\mathbb{Q}(\zeta)$ the p -th cyclotomic extension. The maximal real subfield of $\mathbb{Q}(\zeta)$ is $\mathbb{K} = \mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \bar{\zeta})$ and its ring of integers is $\mathbb{Z}[\zeta]^+ = \mathbb{Z}[\zeta + \bar{\zeta}]$. We shall let $P = \{1, 2, \dots, p-1\}$ and $P^+ = \{1, 2, \dots, (p-1)/2\} \subset P$ and write σ_c for the automorphism of $\mathbb{Q}(\zeta)$ with $\zeta \mapsto \zeta^c$, for $c \in P$. It induces an automorphism σ'_c of \mathbb{K} , such that $\sigma'_c(\zeta + \bar{\zeta}) = (\zeta^c + \bar{\zeta}^c)$; obviously $\sigma'_c = \sigma'_{p-c}$ and $G^+ = \text{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma'_c : c \in P^+\}$, while $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) =$

$\{\sigma_c : c \in P\}$. If σ generates G , its restriction σ' generates $G^+ = \{\sigma'^c : c \in P^+\}$. The action of the group rings $\mathbb{Z}[G], \mathbb{Z}[G^+]$ is written multiplicatively and *complex conjugation* is an automorphism of $\mathbb{Q}(\zeta)$ and an element of the group ring, which we denote by $j \in \mathbb{Z}[G]$.

2.1. The embedding of G^+ in G . We shall often consider the action of $\theta \in G^+$ on elements $\gamma' = \gamma \cdot \bar{\gamma} = \gamma^{1+j} \in \mathbb{K}$, where $\gamma \in \mathbb{Q}(\zeta)$. It is practical to consider this as an action of $\Theta = (1+j)\theta$ on γ , thus

$$\gamma^\Theta = \gamma^{(1+j)\theta} = (\gamma')^\theta.$$

This action can be considered as the composition of $1+j \in G$, which maps γ into \mathbb{K} , with $\theta \in G^+$. The expression $\Theta = (1+j)\theta$ is understood formally as the composition of $1+j$ with a lift of θ to G . Explicitly $\theta = \sum_{c \in P^+} n_c \sigma'_c \in G^+$ is lifted by lifting σ'_c to σ_c and thus

$$\Theta = (1+j)\theta = \sum_{c \in P^+} n_c (\sigma_c + \sigma_{p-c}) \in G.$$

2.2. Catalan's equation. Consider briefly some consequences in $\mathbb{Q}(\zeta)$ of the existence of solutions to (1). We shall write $\alpha = \frac{x-\zeta}{1-\zeta}$ and $\alpha_c = \sigma_c(\alpha)$. Note that (3) becomes

$$(10) \quad \mathbf{N}(\alpha) = v^q$$

and there is an ideal $\mathfrak{A} = (\alpha, v) \subset \mathbb{Z}[\zeta]$ with $\mathfrak{A}^q = (\alpha)$. Let $\mathfrak{A}' = \mathfrak{A}^{1+j} \subset \mathbb{Z}[\zeta]^+$ and $\alpha' = \alpha \cdot \bar{\alpha} \in \mathbb{Z}[\zeta]^+$. We collect some handy properties of $\alpha, \mathfrak{A}, \mathfrak{A}'$ in the following:

Lemma 1. *The ideals $\sigma_a(\mathfrak{A}), \sigma_b(\mathfrak{A})$ are coprime for distinct $a, b \in P$. Furthermore, if $\theta \in \mathbb{Z}[G]^+$ annihilates \mathfrak{A}' in the class group of \mathbb{K}^+ , then there is a $\rho \in \mathbb{Z}[\zeta]^+$ together with a real unit δ such that*

$$(11) \quad \alpha^\Theta = \alpha^{(1+j)\theta} = \alpha'^\theta = \delta \cdot \rho^q \equiv (1-\zeta)^{-\Theta} \pmod{q^2 \mathbb{Z}[\zeta]^+}.$$

Proof. The ideal containing both $\sigma_a(\mathfrak{A}), \sigma_b(\mathfrak{A})$, also contains the weighted difference $((1-\zeta^a)\alpha_a - (1-\zeta^b)\alpha_b) = \zeta^b - \zeta^a$ and it is thus at most divisible by the ramified prime \wp lying above p . But by (2), $\alpha = 1 + m \cdot p^{nq-1}/(1-\zeta)$ for $(m, p) = 1$ and some $n \geq 2$. It is thus coprime to \wp .

For the proof of (11), we observe that the existence of δ, ρ is a direct consequence of θ annihilating \mathfrak{A}' ; the congruence then follows from (8) and (9). \square

2.3. Units. We let $E \subset \mathbb{Z}[\zeta]^+$ denote the real units of $\mathbb{Q}(\zeta)$ and the cyclotomic units of \mathbb{K} be the multiplicative group C generated by

$$\frac{\zeta^c - \bar{\zeta}^c}{\zeta - \bar{\zeta}}, \quad c \in P.$$

It is also common to write $\tilde{U} = \langle -\zeta \rangle \times U \subset \mathbb{Z}[\zeta]$, with $U = E$ or $U = C$, for the respective units of $\mathbb{Q}(\zeta)$. The cyclotomic units C are of finite index in E and the analytic class number formula [46] states that

$$h(\mathbb{K}) = [E : C].$$

A common notation [43] is $W = E/C$, so $h(\mathbb{K}) = |W|$.

Definition 1. An element $\gamma \in \mathbb{Z}[\zeta]$ is q -primary if there is a $\nu \in \mathbb{Z}[\zeta]$ such that

$$\gamma \equiv \nu^q \pmod{q^2 \cdot \mathbb{Z}[\zeta]}.$$

The q -primary numbers are q -adic q -th powers. In particular, a cyclotomic unit $\varepsilon \in C$ is q -primary, if it is congruent to a q -th power modulo $q^2\mathbb{Z}[\zeta]^+$. We denote the q -primary cyclotomic units by C_q .

Remark 1. It is more usual to encounter p -primary elements in the p -th cyclotomic extension. One can consider the q -primary ones as such of the pq -th extension, which happen to be elements of the subfield $\mathbb{Q}(\zeta)$ of this extension. It is in particular true that q -primary units of \mathbb{K} generate class fields of degree q over $\mathbb{Q}(\zeta_{pq})$. We shall show that the congruence (11) gives naturally rise to q -primary units and the strategy of our proof consists in fact in showing that all cyclotomic units must be q -primary, if Catalan's equation has more than one nontrivial solution.

The double Wieferich relation (8) implies that $p = \mathbf{N}(1 - \zeta)$ is q -primary. The question of generalizing the (8) to the cyclotomic field lays at hand. Let $L = \{(-\zeta)^n \cdot (1 - \zeta)^\Theta : n \in \mathbb{N}, \Theta : \mathbb{Z}[G]\}$ be the multiplicative subgroup of $\mathbb{Q}(\zeta)^\times$ which is generated by $(1 - \zeta)$ and $-\zeta$ and L_q be the subset of q -primary elements in L . Our questions is equivalent to estimating the size of the $\mathbb{F}_q[G]$ -module L/L_q .

The following lemma shows that L/L_q and C/C_q are annihilated by the same module:

Lemma 2. Let g generate $(\mathbb{Z}/p \cdot \mathbb{Z})^\times$ so $\eta = \frac{\zeta^g - \overline{\zeta^g}}{\zeta - \overline{\zeta}}$ generates the cyclotomic units as a $\mathbb{Z}[G]$ -module; then

$$(12) \quad 1 - \zeta = \eta^\tau \cdot p^r \cdot \mu^q, \quad \text{with} \quad \begin{aligned} \tau &\in \mathbb{Z}[G], \\ \mu &\in \mathbb{Q}(\zeta) \quad \text{and} \quad r \cdot (p - 1) \equiv 1 \pmod{q}. \end{aligned}$$

Proof. Let $N(X) = \frac{X^{p-1}-1}{X-1}$. Since $X^{p-1} - 1$ is separable over, the polynomials $\mathbb{F}_q[X]$, $(N(X), (X - 1)) = 1$ over $\mathbb{F}_q[X]$. There is thus a linear combination

$$N(X)u(X) + (X - 1)v(X) = 1 - qh(X).$$

We now substitute the generating automorphism $\sigma_g \in G$ for X and apply the above identity to $(1 - \zeta)$. We obtain

$$(1 - \zeta) = ((1 - \zeta)^{\sigma-1})^{v(\sigma)} \cdot p^{u(\sigma)} \cdot (1 - \zeta)^{qh(\sigma)} = \eta^\tau \cdot p^r \cdot \mu^q,$$

which is essentially (12). Note that $(1 - \zeta)^{\sigma-1} \in \tilde{C}$ and since ζ is a q -th power, we have $(1 - \zeta)^{\sigma-1} = \eta \cdot (q\text{-th power})$. By taking norms on both sides, since $\mathbf{N}(\mu)$ must be a power of p , the equivalence $r \cdot (p - 1) \equiv 1 \pmod{q}$ follows too. \square

Remark 2. Since $p^r \cdot \mu^q$ is q -primary, (12) clearly shows that if θ annihilates C/C_q , then $(1 - \zeta)^{(1+j)\theta}$ is q -primary and thus θ annihilate L/L_q . This lemma is a technical step of our proof. The use of the information it yields can be circumvented; it is most relevant for reflecting the relation between q -primary units and generalized double Wieferich conditions.

We now show that all cyclotomic units cannot be q -primary, at least if $p > q$:

Proposition 1. If $C_q = C$ then $q > p$.

Proof. Suppose that all cyclotomic units are q -primary, i.e. $C_q = C$. Since ζ is a q -th power, then \tilde{C} will be primary too. In particular, $\eta_c = 1 + \zeta^c$, $c \in P$ are q -primary, i.e. $1 + \zeta^c \equiv \nu^q \pmod{q^2 \cdot \mathbb{Z}[\zeta]}$. If $q \cdot r' \equiv 1 \pmod{p}$, the congruence modulo q shows that we must have plainly $\nu \equiv 1 + \zeta^{cr'} \pmod{q \cdot \mathbb{Z}[\zeta]}$. Writing $\nu = 1 + \zeta^{cr'} + q \cdot \gamma$, with $\gamma \in \mathbb{Z}[\zeta]$ and raising to the q -th power, we find $\nu^q = 1 + \zeta^c + O(q^2)$, so:

$$(13) \quad 1 + \zeta^c \equiv (1 + \zeta^{cr'})^q \pmod{q^2 \cdot \mathbb{Z}[\zeta]}.$$

Consider now the polynomial

$$F(X) = \left(\frac{(1+X)^q - (1+X^q)}{q \cdot X} \pmod{q} \right) = \sum_{k=1}^{q-1} (-1)^k \cdot X^{k-1}/k \in \mathbb{F}_q[X].$$

Let Ω be some maximal ideal of $\mathbb{Z}[\zeta]$ above q and $\mathbb{L} = \mathbb{Z}[\zeta]/\Omega \subset \overline{\mathbb{F}}_q$, a field of characteristic q . By (13), it follows that $X_c = \zeta^{cr'} \pmod{\Omega} \in \mathbb{L}$ are zeroes of F , for all $c \in P$. But $(\zeta^c - \zeta^d) = \wp$, the ramified prime above p and since p, q are distinct primes, the powers of ζ are all distinct modulo Ω and F has at least $p-1$ zeroes in \mathbb{L} . Since \mathbb{L} is a field, F cannot have more than $q-2$ distinct roots in \mathbb{L} , so $q-2 \geq p-1$ and $q > p$, as claimed. \square

2.4. Group ring representations. In this subsection we consider representations of group rings acting on \mathbb{K} ; we write these actions multiplicatively, while the module structures are written, as usually, additively.

Let S be one of $\mathbb{Z}_q, \mathbb{Z}/(q^N \cdot \mathbb{Z}), \mathbb{F}_q$. Since $q \nmid (p-1)$, the polynomial $X^{p-1} - 1$ is separable over S and there is some extension $S' \supset S$ in which this polynomial splits in linear factors. Let $\mathfrak{X}(S')$ be the set of Dirichlet characters on G^+ with images in S' . The representation of G in S' is semi simple and we have the usual idempotents

$$\varepsilon_\chi(S) = 2/(p-1) \sum_{a \in P^+} \chi(\sigma_a) \cdot \sigma_a^{-1}.$$

2.4.1. Irreducible modules, annihilators and supports. These idempotents depend on S . In fact, any character $\chi \in \mathfrak{X}(\mathbb{Z}'_q)$ maps to $\chi \pmod{q^N \cdot \mathbb{Z}'_q} \in \mathfrak{X}(\mathbb{Z}/(q^N \cdot \mathbb{Z}))'$ and, conversely, there is a unique lift from $\mathfrak{X}(\mathbb{Z}/(q^N \cdot \mathbb{Z}))$ to $\mathfrak{X}(\mathbb{Z}'_q)$.

If $\langle \chi \rangle$ is the S -orbit of $\chi \in \mathfrak{X}(S')$, then the traces

$$\rho(\chi) = \sum_{\chi' \in \langle \chi \rangle} \chi' = \mathbf{Tr}_{S'/S}(\chi)$$

are S -valued. We let $\mathfrak{R}(S) = \{\rho(\chi) : \chi \in \mathfrak{X}(S')\}$, the S -irreducible characters of G^+ , [24], **Chap. 9**. If σ' generates G^+ , we have the following:

Lemma 3. *For each irreducible character $\rho \in \mathfrak{R}(S)$ there is an irreducible factor $f_\rho(X)$ of $X^{(p-1)/2} - 1$ over S for which*

$$\rho \cdot S[G^+] \cong S[G^+]/(f_\rho(\sigma')),$$

the isomorphic modules being irreducible over S . In particular, $S[G^+]$ is a direct sum of irreducible modules:

$$(14) \quad S[G^+] = \bigoplus_{\rho \in \mathfrak{R}(S)} \rho S[G^+] = \bigoplus_{\rho \in \mathfrak{R}(S)} S[G^+]/(f_\rho(\sigma)).$$

Furthermore, if M is an $S[G^+]$ - module, then there is a subset $\mathfrak{S}(M) \subset \mathfrak{R}(S)$ such that:

$$(15) \quad M = \bigoplus_{\rho \in \mathfrak{S}(M)} \rho \cdot M \quad \text{and} \quad \rho M \neq 0, \quad \forall \rho \in \mathfrak{S}(M).$$

Proof. Note that the map $X \bmod (X^{(p-1)/2} - 1) \mapsto \sigma'$ induces an isomorphism of the S - algebra $S[X]/(X^{(p-1)/2} - 1)$ in $S[G^+]$. The proof of (14) follows by use of this isomorphism and common facts on irreducible representations of group rings [24], [46]. The direct sum (14) induces the representation (15) of M as a direct sum. We obtain $\mathfrak{S}(M)$ by removing the trivial terms from this sum. \square

Definition 2. Let S be as above. If M is an $S[G^+]$ - module and $\mathfrak{S}(M)$ is the set defined by (15), the cyclic module

$$M^\perp = \bigoplus_{\rho \in \mathfrak{S}(M)} \rho \cdot S[G^+] \subset S[G^+]$$

is called the support of M in $S[G^+]$; if M is cyclic, then $M \cong M^\perp$. Also

$$M^\top = \bigoplus_{\rho \in (\mathfrak{R} \setminus \mathfrak{S}(M))} \rho \cdot S[G^+] \subset S[G^+]$$

is the annihilator of M and if M is cyclic, then $M \cong S[G^+]/M^\top$. Furthermore, the generators $\Omega(T)$ of the cyclic modules $T = M^\perp$ and $T = M^\top$ are called the effective support and the minimal annihilator of M , respectively.

Any element $\gamma \in K^\times$ generates a $\mathbb{Z}/(q^N \cdot \mathbb{Z})$ - module

$$M_N(\gamma) = \{\gamma^\theta \bmod (\mathbb{K}^\times)^{q^N} : \theta \in \mathbb{Z}[G^+]\}.$$

The notions of support and annihilator of γ apply to this module.

We list now some important properties of supports and annihilators.

Lemma 4. Let M be an $S[G^+]$ - module. We have

$$(16) \quad (M^\top)^\top = M^\perp$$

and equivalently,

$$(17) \quad \Omega(M^\perp) \cdot \Omega(M^\top) = 0,$$

as elements of $S[G^+]$.

Suppose that M is a finite Abelian q - group on which G^+ acts, making it into a $\mathbb{Z}/(q^N \cdot \mathbb{Z})$ - module, for some $N > 0$.

Then, for any $\rho \in \mathfrak{R}(\mathbb{Z}/(q^N \cdot \mathbb{Z}))$ and $\tilde{\rho} = \rho \bmod q \cdot \mathbb{Z}/(q^N \cdot \mathbb{Z}) \in \mathfrak{R}(\mathbb{F}_q)$ we have:

$$(18) \quad \rho \cdot M \neq 0 \Leftrightarrow \tilde{\rho} \cdot (M/(qM)) \neq 0$$

and $\mathfrak{S}(M) = \mathfrak{S}(M/qM)$.

Proof. The relations (16) and (17) are consequences of the complementarity of support and annihilator, as reflected, for instance, by the following relation, that reformulates the definitions:

$$\mathfrak{S}(M) \oplus \mathfrak{S}(M^\top) = S.$$

Suppose that M is a finite Abelian q - group; if $\tilde{\rho}(M/qM) \neq 0$, there is a $x \in \rho M \setminus q \cdot (\rho M)$ and thus $\rho M \neq 0$. Conversely, let $0 < n \leq N$ be the height of ρM , so $q^n(\rho M) = 0$ but $q^{n-1}(\rho M) \neq 0$. If x generates ρM , it has order q^n and the

order of qx is $n - 1$. It follows that $x_1 = (x \bmod qM) \in (\tilde{\rho})(M/qM)$ and $x_1 \neq 0$, so $\tilde{\rho}(M/qM) \neq 0$, which completes the proof of (18). \square

Applied to units, the lemmata and definitions of this subsection yield the capital **Proposition 2**. *Let $D = C_q/C^q$, a cyclic $\mathbb{F}_q[G^+]$ -module. If $\varepsilon \in E$ is annihilated modulo E^q by the module D^\perp , then $\varepsilon \in C \cdot E^q$. Furthermore, if ε is q -primary, then $\varepsilon \in E^q$.*

Proof. Note first that C being cyclic, so are C^q and C_q , as $\mathbb{Z}[G]$ -modules. It follows that C_q/C^q is cyclic as an $\mathbb{F}_q[G^+]$ -module.

Let $W = E/C$ and $W(q) = W/W^q$. Then the cyclotomic units $\eta \in E^q \setminus C^q$ which are q -th powers of cyclotomic units in E , lay in $W(q)^\perp \cdot C$. A fortiori $W(q)^\perp \subset D^\perp$, since the q -th powers are also q -primary – hence $W(q)^\top \supset D^\top$, by (16). The hypothesis implies, by (16), that the support ε is in D^\top . Consequently, $\varepsilon \in W(q)^\top E$ and by definition of annihilators,

$$W(q)^\top \cdot E \subset W(q)^\top \cdot (CE^q),$$

which proves the first assertion.

For the second statement, let $\varepsilon = \eta \cdot \delta^q$, with $\eta \in C$ and $\delta \in E$. Since ε is q -primary and is annihilated by D^\perp , it follows that η is a q -th power, which completes the proof. \square

2.4.2. Lifts and weights.

Definition 3. *If $\Psi = \sum_{c \in P^+} t_c \cdot \sigma_c \in \mathbb{F}_q[G^+]$, its **canonical lift** to $\mathbb{Z}[G^+]$ is*

$$\widehat{\Psi} = \sum_{c \in P^+} n_c \cdot \sigma_c \quad \text{with } 0 \leq n_c < q \quad \text{and } n_c \bmod q = t_c.$$

The augmentation map $\pi_q : \mathbb{F}_q[G] \rightarrow \mathbb{F}_q$ is the homomorphism $\Psi \mapsto \sum_c t_c$; its restriction to $\mathbb{F}_q[G^+]$ is defined similarly. The integer augmentation map will be denoted by $\pi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$. We refer to the values of the augmentation map as **weights**. For $\Psi \in \mathbb{F}_q[G]$ we define its canonical weight to be:

$$\widehat{\pi}(\Psi) := \pi(\widehat{\Psi}) \in \mathbb{N}.$$

Note that the canonical weight is by definition positive. Also, for $\Psi = (1 + j)\psi$, with $\psi \in G^+$, we will have

$$\widehat{\pi}(\Psi) = 2 \cdot \widehat{\pi}(\psi).$$

If $M \subset \mathbb{F}_q[G^+]$, we denote by M_0 the kernel of the augmentation map:

$$M_0 = \{\Psi \in M : \pi_q(\Psi) = 0.\}$$

The action of Ψ on $\mathbb{K}^\times / (\mathbb{K}^\times)^q$ is given by lifting it canonically to $\mathbb{Z}[G^+]$. Thus, for $\gamma \in \mathbb{K}^\times$, we define:

$$\gamma^\Psi := \gamma^{\widehat{\Psi}} \quad \bmod (\mathbb{K}^\times)^q.$$

We let

$$\mathbf{N} = \mathbf{N}_{\mathbb{K}/\mathbb{Q}} = \sum_{c \in P^+} \sigma'_c.$$

The ideal $(\mathbf{N}, q) \subset \mathbb{Z}[G^+]$ is an $\mathbb{F}_q[G^+]$ module; we denote its image modulo q as **norm ideal**:

$$\mathfrak{n} = \mathbf{N} \cdot \mathbb{F}_q[G^+] = \{a \cdot \mathbf{N} : a \in \mathbb{F}_q\} \subset \mathbb{F}_q[G^+].$$

Note the following simple property of $\mathbb{F}_q[G]$ -modules:

Lemma 5. *Let $M \subset \mathbb{F}_q[G^+]$. If $M \neq \mathfrak{N}$, then $M_0 \neq 0$ and there is a $\theta \in M_0$ with $\widehat{\pi}(\theta) = h \cdot q$ and $h \leq (p-1)/4$.*

Proof. Let $\Psi \in M$; then $w_q(\sigma\Psi) = w_q(\Psi)$ for all $\sigma' \in G^+$. Since $M \neq \mathfrak{N}$, there is a $\sigma \in G^+$ and a $\Psi \in M$ such that $\theta' = \Psi(1 - \sigma') \neq 0$. Obviously $w_q(\theta') = 0$ and thus $\widehat{\pi}(\theta') \equiv 0 \pmod{q}$, thus $M_0 \neq 0$. Since the coefficients of the lift are $n_c < q$, we have

$$w(\widehat{\theta}') = \sum_{c \in P^+} n_c = a \cdot q < (p-1)/2 \cdot q.$$

Consider also $\theta'' = -\theta'$. Then $n_c(\theta) + n_c(-\theta) \in \{0, q\}$ and $\widehat{\pi}(\theta') + \widehat{\pi}(\theta'') \leq q \cdot \frac{p-1}{2}$. By choosing θ among θ' and θ'' such that $\widehat{\pi}(\theta)$ is minimal, the estimate for h follows and this completes the proof of the lemma. \square

2.5. Units and the plus part of the class group. We have already mentioned that the *analytic class number formula* relates the class number $h(\mathbb{K})$ to the order of the group $W = E/C$. In 1988, Thaine succeeded to prove the most powerful result [43], [46], §15.2, relating the local irreducible submodules of $\mathcal{C}(\mathbb{K})$ and W . The theorem of Thaine holds for general real Abelian extensions $\mathbb{L} \supset \mathbb{Q}$ and localizations at primes q with $q \nmid [\mathbb{L} : \mathbb{Q}]$.

We state its restriction to $\mathbb{L} = \mathbb{K} = \mathbb{Q}(\zeta_p)^+$ and $q \nmid p-1$ an odd prime:

Theorem 2 (Thaine). *If $q \nmid p-1$ and $\theta \in \mathbb{Z}[G^+]$ annihilates the q -Sylow group of W then θ also annihilates the q -Sylow group of the class group of \mathbb{K} .*

We need for the purposes of our proof the related result:

Corollary 1. *If $\theta \in \mathbb{F}_q[G^+]$ annihilates $W(q) = W/W^q$, then it also annihilates $A(q) = \mathcal{C}(\mathbb{K})/(\mathcal{C}(\mathbb{K}))^q$. In particular, it annihilates \mathfrak{A}' .*

Proof. Thaine's theorem states that $\mathfrak{S}(W) \supset \mathfrak{A}$; the relation (18) states that $W(q)$ and W have, up to lift, the same support, and the same holds for A . This proves the first statement. The second is a consequence of $\mathfrak{A}^q = (\alpha)$ and thus $\mathfrak{A}' \in A(q)$. \square

3. THE MODULE C/C_q

Keeping the notations of the previous section, we can now relate the annihilation of C/C_q to algebraic numbers generated by solutions of Catalan's equation.

Theorem 3 (Bumira Camar). *Let $D = C_q/C^q$ and $\Omega = \Omega(D^\top)$ be the minimal annihilator. If $r \cdot (p-1) \equiv 1 \pmod{q}$, then there is a $\mu \in \mathbb{K}$ such that:*

$$(19) \quad \left(\frac{(x-\zeta)(x-\bar{\zeta})}{p^r} \right)^\Omega = \mu^q.$$

Furthermore, if $\theta \in D_0^\top$, then

$$(20) \quad ((x-\zeta)(x-\bar{\zeta}))^\theta = \nu^q \quad \text{with } \nu \in \mathbb{Z}[\zeta]^+.$$

Proof. The module D is cyclic and thus $D = D^\perp = \mathbb{F}_q[G^+]/(\Omega)$. Since the q -th powers in C/C^q are necessarily q -primary, it follows that Ω also annihilates W/W^q . The corollary 1 to Thaine's theorem implies then that Ω annihilates \mathfrak{A}' . There is thus a unit $\varepsilon \in E$ and $\mu_0 \in \mathbb{Z}[\zeta]^+$, such that

$$\left(\frac{(x-\zeta)(x-\bar{\zeta})}{(1-\zeta)(1-\bar{\zeta})} \right)^\Omega = \varepsilon \cdot \mu_0^q.$$

Then the relation (12) allows replacing the denominator of the left hand side by a power of p and proposition 2 shows that the resulting unit on the right hand side is cyclotomic:

$$\left(\frac{(x - \zeta)(x - \bar{\zeta})}{p^r}\right)^\Omega = \eta \cdot \mu_1^q.$$

But the double Wieferich relations (8) and (9) imply that the left hand side is q -primary, and so must be η . Raising this equation at $\Gamma = \Omega(D^\perp)$ (notice that $\Gamma \cdot \Omega = 0$ by (17)), we find it annihilates η and we can apply the second part of proposition 2. It follows that η is a q -th power, and this proves (19).

Assume now that $\theta \in D_0^\top$, a fortiori a multiple of Ω . Since $w_q(\theta) = 0$,

$$(21) \quad ((1 - \zeta)(1 - \bar{\zeta}))^\theta = \eta \cdot \delta^q, \quad \text{with } \eta \in C, \delta \in \tilde{C}.$$

Thus

$$\begin{aligned} \left(\frac{(x - \zeta)(x - \bar{\zeta})}{(1 - \zeta)(1 - \bar{\zeta})}\right)^\theta &= \varepsilon_1 \cdot \nu_1^q \quad \text{and, using (21)} \\ ((x - \zeta)(x - \bar{\zeta}))^\theta &= \varepsilon_2 \cdot \nu_2^q. \end{aligned}$$

Applying proposition 2 like before, we find that $\varepsilon_2 \in E^q$, thus confirming (20). \square

Remark 3. *Note that we did not need lemma 2 for proving (20), which is the relation on which the sequel of our proof builds. As mentioned in remark 1, the more general statement (19) can be circumvented in the sequel of the proof.*

Buturuga mică răstoarnă carul mare translates to "the small branch turns over the large chariot", whence **Bumira Camar**. Indeed, the tiny primary cyclotomic units are annihilated by θ and this makes, via (1), the huge $((x - \zeta)(x - \bar{\zeta}))^\theta$ to become a q -th power. We consider this to be a good idiosyncratic image of the core strategy of this proof.

Annihilation of the primary units was applied by Thaine in [44] to the Second Case of Fermat Last theorem, obtaining a close relation to (19). We explain in Appendix C why in the case of Fermat's equation, this cannot lead to a contradiction of the kind we develop subsequently for Catalan.

This theorem gives a powerful tool for estimating the size of Ω by using analytical methods. Note that by (16), $C/C_q \oplus (\Omega) \cong \mathbb{F}_q[G^+]/(\mathfrak{N})$. We shall show that if Catalan's conjecture is false, then $\Omega = \mathbf{N}$ and all cyclotomic units are q -primary.

4. ABEL SERIES

Many of the techniques in this section are borrowed with the kind permission of Yuri Bilu from his exposé of this proof.

For $r \in \mathbb{R}$, the series of Abel (or generalized binomial series) is

$$f(z) = \sum_{k \geq 0} \binom{r}{k} z^k;$$

it converges uniformly for $|z| < 1$ and the sum verifies $f(z) = (1 + z)^r$. We want to investigate series expansions of algebraic numbers $\mu \in \mathbb{Z}[\zeta]$ which verify $\mu^q = (1 - \zeta/x)^\Theta$, where $\Theta = (1 + j)\theta \in \mathbb{F}_q[G]$, thus $j\Theta = \Theta$.

We shall first give a formal power series which verifies this condition, and investigate some of its properties. After that we consider the convergence of the series,

when inserting complex numbers in the series and give some useful estimates. Based upon these prerequisites, we finally prove:

Theorem 4. *If Catalan's equation (1) has a solution with $p > q \geq 3$, then $p \equiv 1 \pmod{q}$.*

Since this contradicts proposition 1, the theorem is the last step of the proof of Catalan's conjecture. We finally review the important steps of the proof in the next section.

4.1. Formal power series. We start with some definitions.

Definition 4. *Let $\mathbf{R} = \mathbb{Q}(\zeta)[[T]]$ be the ring of formal powers series over the p -th cyclotomic field and $\mathbf{R}^+ = \mathbb{Q}(\zeta)^+[[T]]$. The elementary q -th root series is defined as:*

$$f(T) = \sum_{k \geq 0} \binom{1/q}{k} \cdot (-\zeta \cdot T)^k = \sum_{k \geq 0} a_k \cdot T^k \in \mathbf{R},$$

where $a_k = \binom{1/q}{k} \cdot (-\zeta)^k$. Let $0 < n < q$ and $\sigma \in G$; then σ acts upon ζ and

$$f^{n\sigma}(T) = \sum_{k \geq 0} \binom{n/q}{k} \cdot (\zeta^\sigma \cdot T)^k = \sum_{k \geq 0} a_k(n\sigma) \cdot T^k \in \mathbf{R},$$

and $a_k(\sigma) = \binom{n/q}{k} (-\zeta)^{k\sigma}$.

For $\Theta \in \mathbb{F}_q[G]$ with $\hat{\Theta} = \sum_{c \in P} n_c \cdot \sigma_c$ we define the additive map $\rho : \mathbb{F}_q[G] \rightarrow \mathbb{Z}[\zeta]$ by

$$\rho : \Theta \mapsto - \sum_{c \in P} n_c \cdot \zeta^c.$$

We note two important properties of the coefficients of these elementary series:

Lemma 6. *For $k \geq 0$, let $E(k) = k + v_q(k!)$. Then $E(k)$ is strictly monotonous and verifies*

$$(22) \quad E(k) < k \cdot \frac{q}{q-1}.$$

Furthermore

$$(23) \quad q^{E(k)} \cdot \binom{1/q}{k} \in \mathbb{Z} \quad \text{and} \quad E(k) = -v_q \left(\binom{1/q}{k} \right).$$

Writing $b_k(n\sigma) = (q^k \cdot k!) \cdot a_k(n\sigma)$, the following congruence holds:

$$(24) \quad b_k(n\sigma) \equiv (-n\zeta^\sigma)^k = \rho(n\sigma)^k \pmod{q \cdot \mathbb{Z}[\zeta]}.$$

Proof. Since $k+1 > k$ and $v_q((k+1)!) \geq v_q(k!)$, the function $E(k)$ is strictly monotonous. Note that $v_q(k!) \leq \sum_{i>0} \lfloor k/q^i \rfloor < k/(q-1)$; this leads to the upper bound for $E(k)$. For $n \not\equiv 0 \pmod{q}$ we have

$$v_q(b_k(n)) = v_q \left(q^k \cdot k! \cdot \binom{n/q}{k} \right) = v_q(n \cdot (n-q) \dots (n-(k-1)q)) = 0.$$

This shows that $v_q(a_k(n\sigma)) = -E(k)$.

We now estimate $v_\ell(b_k(n\sigma))$. The pigeon hole principle shows that the number of multiples of ℓ^i in the above product is $\lfloor k/\ell^i \rfloor$. Since ℓ may divide n to a high power, adding up we find:

$$v_\ell(n \cdot (n-q) \dots (n-(k-1)q)) \geq \sum_{i>0} \lfloor k/\ell^i \rfloor = v_\ell(k!).$$

Together with the estimate of $v_q(b_k(n))$, this yields (23).

We now develop $b_k(n\sigma)$:

$$b_k(n\sigma) = (n \cdot (n-q) \dots (n-(k-1)q)) \cdot (-\zeta)^{k\sigma} \equiv (-n\zeta^\sigma)^k \pmod{q\mathbb{Z}[\zeta]}.$$

This is (24), which completes the proof. \square

Let $\Theta \in \mathbb{F}_q[G]$. If $\widehat{\Theta} = \sum_{c \in P} n_c \sigma_c$, then the previous definition naturally implies that:

$$(25) \quad f^\Theta(T) = \prod_{c \in P} \left(\sum_{k \geq 0} \binom{n_c/q}{k} (\zeta^c \cdot T)^k \right).$$

Since $f^\Theta \in \mathbf{R}$, it also has a development as a simple power series. In consistency with the definition of a_k, b_k in lemma 6, we shall write this development as

$$(26) \quad \begin{aligned} f^\Theta(T) &= \sum_{k \geq 0} a_k(\Theta) \cdot T^k \quad \text{and let} \\ b_k(\Theta) &= a_k(\Theta) \cdot (q^k \cdot k!). \end{aligned}$$

The arithmetic properties of the coefficients a_k, b_k are given by the following:

Lemma 7. *The coefficients $a_k(\Theta), b_k(\Theta)$ of the series $f^\Theta \in \mathbf{R}$ have the properties:*

1. Both a_k, b_k commute with the Galois action, i.e.: $a_k(\sigma\Theta) = (a_k(\Theta))^\sigma$.
2. $a_k(\Theta) \in \mathbb{Z}[\zeta, 1/q]$. More precisely, $q^{E(k)} \cdot a_k(\Theta) \in \mathbb{Z}[\zeta]$.
3. $b_k(\Theta) \in \mathbb{Z}[\zeta]$ and

$$(27) \quad b_k(\Theta) \equiv \rho(\Theta)^k \pmod{q \cdot \mathbb{Z}[\zeta]}.$$

4. If $\Theta = j\Theta$, then $a_k(\Theta) \in \mathbb{R}$.

Proof. Property 1. follows from (25) and the fact that σ acts on ζ but not on the formal parameter T . Suppose that $\Theta = \Theta_1 + \Theta_2$; then the coefficients of f^Θ are derived from the ones of $f^{\Theta_i}, i = 1, 2$ as follows:

$$\begin{aligned} a_k(\Theta) &= a_k(\Theta_1 + \Theta_2) = \sum_{l=0}^k a_l(\Theta_1) \cdot a_{k-l}(\Theta_2) \\ b_k(\Theta) &= b_k(\Theta_1 + \Theta_2) = \sum_{l=0}^k \binom{k}{l} \cdot (b_l(\Theta_1) \cdot b_{k-l}(\Theta_2)). \end{aligned}$$

We have

$$v_q(a_l(\Theta_1) \cdot a_{k-l}(\Theta_2)) = -(E(l) + E(k-l)) = -E(k) + v_q\left(\binom{k}{l}\right) \geq -E(k);$$

thus $v_q(a_k(\Theta)) \geq -E(k)$, by induction on the canonical weights $\widehat{\pi}(\Theta_1), \widehat{\pi}(\Theta_2)$. This proves 2. By (24), we have $b_k(\Theta) \equiv \rho(\Theta)^k \pmod{q\mathbb{Z}[\zeta]}$ for $\Theta = n\sigma, \forall \sigma \in G$. Assume

that (27) holds for $\Theta_i, i = 1, 2$. Then by the previous identity for $b_k(\Theta_1 + \Theta_2)$, we have

$$\begin{aligned} b_k(\Theta_1 + \Theta_2) &= \sum_{l=0}^k \binom{k}{l} \cdot (b_l(\Theta_1) \cdot b_{k-l}(\Theta_2)) \\ &\equiv \sum_{l=0}^k \binom{k}{l} \rho(\Theta_1)^l \cdot \rho(\Theta_2)^{k-l} = \rho(\Theta_1 + \Theta_2)^k \pmod{q\mathbb{Z}[\zeta]}. \end{aligned}$$

The relation (27) follows from this by induction on the weights of Θ_1, Θ_2 .

Finally, if $\Theta = (1+j)\theta$ is real, the case we are mostly interested in, note that

$$a_k(1+j) = \sum_{l=0}^k a_l \cdot \bar{a}_{k-l} = \overline{a_k(1+j)} \in \mathbb{R}.$$

It follows from $f^\Theta = (f^{1+j})^\theta$ that $a_k(\Theta) \in \mathbb{R}$. □

4.2. An estimate. The convergence radius of $f(T)$ being one, it follows by multiplicativity, that the series $f^\Theta(T)$ also have the same domain of convergence, for all $\Theta \in \mathbb{F}_q[G]$. Let

$$S_m(\Theta; T) = \sum_{k=0}^m a_k(\Theta) \cdot T^k$$

be the m -th partial sum of f^Θ and $R_m(\Theta; T) = f^\Theta - S_m(\Theta; T)$ the remainder term. We estimate this remainder, when T is replaced by a complex number inside the domain of convergence.

Lemma 8. *Let $\Theta \in (\mathbb{F}_q[G])_0$ have canonical weight $\widehat{\pi}(\Theta) = hq$. If $z \in \mathbb{C}$, $|z| < 1$, then*

$$(28) \quad |f^\Theta(z) - S_m(\Theta; z)| \leq \binom{h+m}{m+1} \cdot \frac{|z|^{m+1}}{(1-|z|)^{m+1+h}}.$$

Proof. A power series $\sum_{k=0}^{\infty} a_k T^k$ with complex coefficients is *dominated* by the series $\sum_{k=0}^{\infty} A_k T^k$ with non-negative real coefficients if $|a_k| \leq A_k$ for $k = 0, 1, \dots$. The relation of dominance is preserved by addition and multiplication of power series.

Let $r > 0$ be a positive real number, and s a complex number satisfying $|s| \leq 1$. Then the binomial series $(1+sT)^r = \sum_{k=0}^{\infty} \binom{r}{k} s^k T^k$ is dominated by $(1-T)^{-r} = \sum_{k=0}^{\infty} (-1)^k \binom{-r}{k} T^k$. Indeed, the coefficients of the latter series are positive and $\left| \binom{r}{k} \right| \leq \left| \binom{-r}{k} \right|$.

It follows that $f^\Theta(T)$ is dominated by $(1-T)^{-h}$. Denoting by $\bar{S}_m(T)$ the m -th partial sum of the series $(1-T)^{-h}$ and using the common remainder estimates for Taylor series, we obtain the following:

$$\begin{aligned} |f^\Theta(z) - S_m(\Theta; z)| &\leq |(1-|z|)^{-h} - \bar{S}_m(|z|)| \\ &\leq \sup_{0 \leq \xi \leq |z|} \left| \left(\frac{d^{m+1}(1-T)^{-h}}{dT^{m+1}} \Big|_{T=\xi} \right) \right| \frac{|z|^{m+1}}{(m+1)!} \\ &= \binom{h+m}{m+1} \cdot \frac{|z|^{m+1}}{(1-|z|)^{h+m+1}}, \end{aligned}$$

as claimed. □

4.3. The equation $(x - \zeta)^\Theta = \nu^q$ and the proof of theorem 4.

We assume in this subsection the various results about possible solutions of Catalan's equation, which we proved above. As a consequence of (20), we also assume that the equation $(x - \zeta)^\Theta = \nu^q$ has a solution $\nu \in \mathbb{Z}[\zeta]^+$, when $\Theta \in [(C_q/C^q)^\top]_0$ is a weight 0 annihilator of C_q/C^q . By lemma 5, we can choose such a Θ , with canonical weight $\widehat{\pi}(\Theta) = 2\widehat{\pi}(\theta) = h \cdot q$ and $h \leq q \cdot \frac{q-1}{2}$. Finally, $|x|$ is bounded below and we shall use the bound (7) from theorem 1, which is proved in Appendix A.

The series defined previously is related to ν by the following fundamental identity:

Proposition 3. *Let Θ, h, ν be as above. Then*

$$(29) \quad \nu^\sigma = x^h \cdot f^{\sigma\Theta}(1/x), \quad \forall \sigma \in G^+.$$

In particular, the Galois action commutes in this case with the series summation, namely

$$(f^\Theta(1/x))^\sigma = f^{\sigma\Theta}(1/x).$$

Proof. For any $\sigma \in G^+$, the equation

$$(30) \quad X^q = (1 - \zeta/x)^{\sigma\Theta}$$

has the solution $X_0(\sigma) = \nu^\sigma/x^h \in \mathbb{K}$. The other $q-1$ complex solutions of this equation are $X_i = \xi^i \cdot X_0(\sigma)$, $i = 1, 2, \dots, q-1$, where ξ is a primitive q -th root of unity. Since $\xi^i \notin \mathbb{R}$, it follows that $X_0(\sigma)$ is the only solution in \mathbb{K} . On the other hand, $|1/x| < 1$ and the series $f^{\sigma\Theta}(1/x)$ converges; its sum is real and it also verifies (30). But $X_0(\sigma)$ is the only real solution of (30), and this proves (29). The fact that Galois action commutes with the series summation is simply a reformulation of (29): $f^{\sigma\Theta} = X_0(\sigma) (X_0(1))^\sigma = (f^\Theta)^\sigma$. \square

We now let

$$\begin{aligned} \beta &= q^{E(h)} \cdot \nu, \\ S_1 &= q^{E(h)} \cdot \sum_{k=0}^h a_k(\Theta) \cdot x^{h-k} = q^{E(h)} x^h \cdot S_h(\Theta; 1/x) \\ S_2 &= \beta - S_1 = q^{E(h)} x^h \cdot R_h(\Theta; 1/x). \end{aligned}$$

Since $\nu \in \mathbb{Z}[\zeta]^+$, a fortiori $\beta \in \mathbb{Z}[\zeta]^+$. The purpose of multiplying by a power of q is best seen considering the definition of S_1 . Indeed, by points 2. and 4. of lemma 7, $q^h \cdot a_k(\Theta) \in \mathbb{Z}[\zeta]^+$ and thus $S_1, S_2 \in \mathbb{Z}[\zeta]^+$. In fact we have:

Lemma 9. *Let β, S_1, S_2 be as above and assume that $p > q \geq 3$. Then*

$$(31) \quad \beta = S_1 \quad \text{and} \quad S_2 = 0.$$

Proof. Since S_1 is a finite sum and Galois action commutes with the coefficients $a_k(\sigma\Theta)$, we obviously have $S_1(\sigma\Theta) = (S_1(\Theta))^\sigma$ for $\sigma \in G^+$. That the same holds for S_2 is a consequence of $S_2 = \beta - S_1$ and proposition 3.

We estimate $|S_2|$ using (28), (22) and (7).

$$\begin{aligned} |S_2| &= \left| q^{E(h)} x^h \cdot R_h(\Theta; 1/x) \right| \\ &\leq q^{qh/(q-1)} \cdot |x|^h \cdot \binom{2h}{h+1} \frac{|x|^{-(h+1)}}{(1 - 1/|x|)^{2h+1}} = A/|x|. \end{aligned}$$

We now use $\binom{2h}{h+1} < 2^{2h}$, $h \leq (p-1)/2$, $p \geq 5$, $q \geq 3$ and $|x| > 10^{14}$ for bounding A :

$$A \leq q^{\frac{q(p-1)}{2(q-1)}} \cdot 2^{p-1} \cdot (1 + 10^{-10})$$

and

$$|S_2| < 2^4 \cdot (1 + 10^{-10}) \cdot 2^{p-1} \cdot q^{(p-1) \cdot (\frac{q}{2(q-1)} - 8)} < 3^{-5(p-1)} < 1.$$

The Galois action commutes with the sum of the remainder S_2 , as we have shown above, and thus $|S_2^\sigma| < 1$ for all $\sigma \in G^+$, so $|\mathbf{N}(S_2)| < 1$. But S_2 is an algebraic integer, so it must vanish. This completes the proof of (31). \square

We are now prepared to give the

Proof of theorem 4. The point 2. of lemma 7 implies that $q^{E(h)} \cdot a_k(\Theta) \equiv 0 \pmod{q}$ for $k < h$. Since $E(k)$ is strongly monotonous, by (31) and the definition of β , we have

$$q^{E(h)} \cdot \nu = \beta \equiv q^{E(h)} a_h \pmod{q\mathbb{Z}[\zeta]^+}.$$

But ν is an algebraic integer and $h > 0$, so the left hand side is a multiple of q and we must have

$$b_h(\Theta) \equiv \rho(\Theta)^h \equiv 0 \pmod{q \cdot \mathbb{Z}[\zeta]^+}.$$

This implies that $q|\rho(\Theta)$, which again is only possible if $q|n_c$, $\forall c \in P^+$. But this means that $\Theta = 0$, in contradiction with $[(C_q/C^q)^\top]_0 \neq 0$. Finally, all cyclotomic units must be q -primary. This contradicts proposition 1, since we assumed $p > q$ and completes the proof of theorem (4). \square

5. CATALAN'S EQUATION

The truth of Catalan's conjecture follows from the theorems proved above. We review here the major steps of the proof.

Theorem 5. *Catalan's conjecture is true.*

Proof. Assume that Catalan's equation has a non trivial solution for $p, q \geq 3$. Then, by the symmetry of Cassels' relations, there is a solution to $\Phi_p(x) = p \cdot v^q$ with $p > q \geq 3$. Assuming that $p \not\equiv 1 \pmod{q}$, by theorem 3, (20) holds. One then applies estimates involving Abel series to this equation, finding that the cyclotomic units of $\mathbb{Q}(\zeta_p)^+$ must all be q -primary. This contradicts the proposition 1 and establishes the truth of the Catalan conjecture, based on the assumption that $p \not\equiv 1 \pmod{q}$. This assumption is easy to prove by Baker's methods for linear forms in logarithms (see Appendix B), using the double Wieferich relation for eliminating some possible exceptions. \square

Acknowledgments: Hendrik Lenstra's sporadic yet sustained and always encouraging and invigoration discussions were of paramount importance in keeping alive my mathematical preoccupation over one and a half decades. To him goes my humble recognition. Yuri Bilu's generous and involved interest was of great help for polishing the ideas of this proof. I owe to Joachim von zur Gathen and the work group in Paderborn the stimulating and peaceful environment in which this research could mature.

In the final steps of the preparation of this manuscript, I received valuable suggestions and help from various mathematicians. I thank A. Baker, Y. Bilu, J. Coates,

A. Glass, M. Mignotte, F. Pappalardi and F. Thaine for their help in this period; their indications helped improve the quality of this text. This work is dedicated in addition to all those who, over shorter or longer periods of time, offered me their trust, without any prior reason for doing so. Some of them are mathematicians, most are not: but when waters were standing still, always someone was there and hope would walk on !

6. APPENDIX A

We shall give a simple lower bound for $|x|$, which strengthens Hyrö's one

$$(32) \quad \begin{cases} |x| & \geq \max\{ p^{q-1}(q-1)^q + 1, & q(2p+1)(2q^{p-1}+1) & \} \\ |y| & \geq \max\{ q^{p-1}(p+1)^p - 1, & p(q-1)(p^{q-1}(q-1)^q + 1 & \}. \end{cases}$$

in the case $p > q$.

Proposition 4. *For (x, y, p, q) verifying (1), the following lower bounds hold:*

$$(33) \quad |y| \geq (p^{2q-2}/2)^4 \quad \text{and} \quad |x| \geq (q^{2p-2}/2)^4.$$

Proof. We shall prove the bound for $y = pav$ (2) by using (10). Let $\psi \in \mathbb{Z}[G]$ be a Fueter element, i.e. an element of Stickelberger ideal, having weight $(p-1)/2$, to fix the ideas:

$$\psi = (\sigma_2 - 2)\vartheta = \sum_{c > (p-1)/2} \sigma_c \in \mathbb{Z}[G].$$

Since \mathfrak{A}^ψ is principal, by raising to the q -th power, we find there is a $\gamma \in \mathbb{Z}[\zeta]$ such that $(\alpha^\psi) = (\gamma^q)$ and $\gamma^{1+j} = v$. Iwasawa proves in [17] (see also [16][p. 226, Ex. 13]) that Jacobi sums J verify

$$(34) \quad J \equiv -1 \pmod{(1-\zeta)^2 \mathbb{Z}[\zeta]}.$$

Since $\alpha \equiv 1 \pmod{p^2}$ it follows from (34) that the implicit unit in the previous equation between ideals is in fact $\delta = -1$ and

$$\alpha^\psi = -\gamma^q.$$

Let $\eta(\psi) = \sum_{c > (p-1)/2} \frac{1}{1-\zeta^c}$, so $\eta + \bar{\eta} = \sum_{c \in P} 1/(1-\zeta^c) = (p-1)/2$. Since $\gamma \equiv -1 \pmod{(1-\zeta)^2}$ as a Jacobi sum (34), the previous equation can be rewritten - using (2) - as:

$$\begin{aligned} -\gamma^q &= \alpha^\psi = \left(1 + \frac{x-1}{1-\zeta}\right)^\psi \\ &= 1 + (p\eta) \cdot (p^{2(q-1)}a^q) + O(p^{4q-2}/(1-\zeta)^2) \end{aligned}$$

The Abel series for $\alpha^{\psi/q}$ converges p -adically, leading to the following expansion for γ :

$$\gamma = -\left(1 + p^{2q-1}\eta a^q/q + o(p^{4q-3})\right),$$

and $\nu = \gamma + \bar{\gamma} = -\left(2 + p^{2q-1} \cdot a^q \cdot \frac{p-1}{2q} + o(p^{4q-3})\right)$. Suppose now that $\sigma_c(\nu) = \nu, \forall c \in P$; since $\gamma \cdot \bar{\gamma} = v \in \mathbb{Z}$, we should then have $\gamma \in \mathbb{Z}$, which contradicts lemma 1. Consequently, $\mu = \nu - \sigma_c(\nu) \neq 0$ for some $c \in P$ and $\mu \equiv 0 \pmod{p^{4q-3}}$. Note

that by $\gamma \cdot \bar{\gamma} = v$ and since $\mu \in \mathbb{Z}[\zeta]$, we also have $|\sigma(\mu)| \leq 4|\gamma| = 4\sqrt{v}$ and $\sigma(\mu) \equiv 0 \pmod{p^{4q-3}}$ for all $\sigma \in G$. Thus, by taking norms,

$$4^{p-1}v^{(p-1)/2} \geq \mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\zeta)}(\mu) > p^{(4q-3)(p-1)},$$

hence $|v| > (p^{2(q-1)}/2)^4$, from which the claim for $|y|$ follows, since $|y| = |pbv| > |v|$. The claim for $|x|$ follows by symmetry – substitute (x, y, p, q) by $(-y, -x, q, p)$. \square

7. APPENDIX B

Tijdeman [45] used the theory of logarithmic forms to establish the existence of upper bounds for the exponents p, q , which were first made explicite by Langevin [20]. The estimates of Langevin were improved by Glass *et al.* [10] and the repeatedly by Mignotte and Roy [29], using the very sharp lower bound for the binary logarithmic forms from [21]. They generalize further refinements due to Bennett *et al.* [3].

In this section we use Tijdeman's argument and some electronic computations to prove that $p \not\equiv 1 \pmod{q^2}$. A reader ready to accept Theorem 6 as granted, may overlook this appendix.

First we prove

Proposition 5. *If $q > 10^5$, then $p < q^2$.*

The simple proof of proposition 5 was kindly provided by A. Glass. We start by showing:

Lemma 10.

$$(35) \quad p < 11(q \log q) \cdot (\log(p/\log q) + 3)^2.$$

Proof. We follow Tijdeman's notation, see [41], p.206 and assume that $p > q > 10^5$; we have $q \leq s$.

Let

$$\Lambda = |q \log q - p \log(s^q/x)|.$$

As shown in [10], p. 134, $2e \log(s^q/x) < \log s^q$ and $\{q, s^q/x\}$ is multiplicatively independent. We may therefore apply [21], Theorem 2 to Λ with $\rho = 5.4$, $\alpha_1 = q$, $\alpha_2 = s^q/x$, $b_1 = q$ and $b_2 = p$.

Then, with the notation of [21], Theorem 2, we have $a_1 = 6.4 \log q$,

$$a_2 \geq \frac{4.4}{2e} \log(s^q) + 2 \log(s^q).$$

Since this latter exceeds $2 \log \log 5.4$ for $q > 10^5$, we can satisfy (4) in [21] with $a_2 = 3q \log s$.

Now

$$\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) \leq \log(p/\log q),$$

so we may take $\log(p/\log q) + 2.1$ for h in (3) of [LMN] (it exceeds $5 \log \log 5.4$).

We now apply [21], Theorem 2 to get

$$\log \Lambda \geq -\frac{\log 5.4}{9}(6.4)3(q \log q \log s)\left(\frac{4}{1.6^2}(\log(p/\log q) + 4)^2 - \text{smaller terms.}\right)$$

Note that

$$\frac{4}{1.6^2} \log(p/\log q) + 4 \leq \frac{4}{1.6^2}(\log(p/\log q) + 3).$$

Using the fact that $s, p \geq q > 10^5$, we see that the smaller terms can be bounded respectively by A , $0.1A$ and $0.1A$ where

$$A = (q \log q \log s) \cdot (\log(p/\log q) + 3)^2.$$

Thus

$$(36) \quad \log \Lambda \geq -(8.8 + 1.2)(q \log q \log s) \cdot (\log(p/\log q) + 3)^2.$$

But $\Lambda \leq 4q^2/s^p$ (see (25) of [41] or [29]), so

$$(37) \quad \log \Lambda \leq \log 4 + 2 \log q - p \log s.$$

By (37) and (36), we get that

$$p \leq [10(q \log q) \cdot (\log(p/\log q) + 3)^2] + [(2 \log 2q)/\log s].$$

Since $s \geq q \geq 10^5$, we deduce the stated result. \square

Now we prove proposition 5. Note that $\log \log q > 2.44$ whence $\log(p/\log q) + 3 < 1 + \log p < 1.1 \log p$.

Combining this with (35) gives

$$(38) \quad p < 11(1.1^2)(q \log q)(\log p)^2 < 14(q \log q)(\log p)^2.$$

Finally, since $\log p \leq (22/e)p^{1/22}$ and $(\log x)/x^{0.8}$ is decreasing for $x \geq 10^5$, we obtain

$$(39) \quad p \leq (14 \cdot (22/e)^2 q \log q)^{1.1} \leq (14 \cdot (22/e)^2 q^{1.8} 10^{-4} \log 10^5)^{1.1} \\ \leq (14 \cdot (22/e)^2 \cdot 10^{-4} \log(10^5))^{1.1} q^{1.98}.$$

But

$$(14 \cdot (22/e)^2 \cdot 10^{-4} \log(10^5))^{1.1} < 1.1 < (10^5)^{0.02} \leq q^{0.02}.$$

From (39) we deduce that $p < q^2$.

The promessed result can now easily be completed by electronic computations:

Theorem 6. *Let (x, y, p, q) be a solution of (1). Then $p \not\equiv 1 \pmod q$.*

Proof. Use a computer for the following: For $q < 100000$ and p verifying (38), search for double Wieferich pairs. If any are found, check that $p \not\equiv 1 \pmod q^2$. \square

Remark 4. *M. Mignotte points out [32] that, since $1+2q^2 \equiv 0 \pmod 3$, the smallest prime $p \equiv 1 \pmod q^2$ is*

$$p \geq 1 + 4q^2.$$

This apparently innocent correction allows him to still reduce the bound $q > 100000$ that we proved above and, using also more involved forms in logarithms, which we shall not display here, he may reduce to about $q > 25000$. This still reduce the time for the computer proof of theorem 6.

8. APPENDIX C

We restrict our comparison of Fermat's and Catalan's equations to Kummerian methods. *What is known on Fermat's equation* will thus refer to Kummerian results, and thus mostly pre-Wiles ones. The problem of successfully adapting the Frey curve method to Catalan's equation and thus taking advantage of Wiles' proof of the Taniyama - Shimura conjecture is considered by experts to be a very difficult one [38].

The Second Case of Fermat's equation

$$x^p + y^p + z^p = 0 \quad \text{with} \quad p \mid z$$

gives rise by Abel's relations [37] to the following cyclotomic norm equation, the analog of (4):

$$(40) \quad \mathbf{N}(\alpha_f) = t^p, \quad \text{with} \quad \alpha_f = \frac{x + \zeta y}{1 - \zeta} = - \left(y - \frac{x + y}{1 - \zeta} \right).$$

The associated ideal $\mathfrak{A}_f = (\alpha_f, t)$ has order dividing p . While Kummer's genial descent method proves that $p \mid h_p^-$, this fact happens by reflection - more precisely by proving the existence of p -primary units. It is however *not known* that \mathfrak{A}_f cannot be a principal ideal. On the contrary, such a result was most - wanted on the cyclotomic track, since it would have reduced the Second Case to solely the truth of Vandiver's conjecture.

The situation appeared to be more simple for Catalan's equation. The analog of \mathfrak{A}_f in this equation is, certainly, $\mathfrak{A} = (\alpha, v)$ (see section 2). Using Case I methods related to Eichler's, Inkeri had found a conjunction of Case I - like conditions: he essentially showed that either \mathfrak{A} is not principal or the double Wieferich condition holds. How *different* (the second case of) Catalan was from Fermat's Second Case was made even more evident by Bugeaud and Hanrot's result. They basically proved that the ideal \mathfrak{A} cannot be principal (the condition $q > p$ in their proof can be easily removed by a local variant of their argument). Compare this to Fermat, where whether or not the corresponding ideal \mathfrak{A} can be principal was a most - wanted result! However, the minus part successes for Catalan seem to end here. More intensive investigations of the $\mathbb{F}_q[G]^-$ module generated by $\mathfrak{A}/\overline{\mathfrak{A}}$ end in quite intricate combinatorial conditions, without producing clear general contradictions [34].

It is thus worthwhile to consider the Second Case more closely. The double Wieferich conditions (8) and (9) imply that $\alpha/\overline{\alpha}$ is primary singular. It is known from the study of Fermat's Second Case, that primary singular elements of this shape generate class fields of the plus part. Only $\alpha/\overline{\alpha}$ is q -primary singular ... in the p -th cyclotomic extension ! By Leopoldt's reflection theorem [24], it generates a class field of $\mathbb{Q}(\zeta_{pq})^+$. In this case, rather than Vandiver's, one would need the similar flavored conjecture

$$p \nmid h_{pq}^+ \quad \text{if} \quad p \not\equiv 1 \pmod{q},$$

where h_{pq}^+ is the class number of the maximal real subfield of the pq -th cyclotomic field. This conjecture is apparently even more intractable than Vandiver's. However, its truth would imply by itself the truth of Catalan's conjecture: this is an easy, unpublished [34] consequence of (9) and (8).

Finally, the present proof builds upon the consequence of Thaine's theorem, that when annihilating the q -primary units, the (q -part of the) class field will also be

null. This leads to q -th power algebraic integers in our case. It is very instructive to note that Francisco Thaine, an expert of the cyclotomic investigation of Fermat's theorem, applied his own theorem in exactly the same way in [44]. He finds that if $\theta \in \mathbb{Z}[G^+]$ annihilates the p -primary units, then

$$\alpha_f^{(1+j)\theta} = \left(\frac{x^2 + y^2 + 2xy(\zeta + \bar{\zeta})}{2 - (\zeta + \bar{\zeta})} \right)^\theta = \nu^p.$$

This is the Fermat analogue of Theorem *bumira camar*. When trying to use the same kind of approach to the above equation, one meets with two serious obstructions. The first, of algebraic nature, consists in the fact that the norm of $(1 - \zeta)$ is certainly not p -primary, so one cannot eliminate the denominator. The second, analytic in nature, consists in the fact that (even accepting to take p -th roots of $\lambda = (1 - \zeta)^{1+j}$), the power series development which is possible for the left hand side will have $|x/y| < 1$ as ratio (if x, y are chosen accordingly), thus eventually converging very slowly. This appears thus to be a dead end for Fermat.

It is relieving to know that the methods we used for Catalan had been naturally implemented to Fermat earlier by Thaine, and also, that they cannot achieve success in that case. The latter was also previously found by the author of this article, increasing the subjective confidence in the proof.

The impossibility to adapt the present Kummerian solution of Catalan's conjecture to the Fermat equation suggests at a first glance, this might reflect the harder tractable structure of the latter. This would make sense, considering the higher amount of research which was involved in it. On the other hand, Ribet's theorem shows the Frey curve of the Fermat equation cannot be modular; this allowed the proof of Fermat's conjecture due to Wiles' epochal proof of Taniyama - Shimura. On this front, we saw that an analog of Ribet's theorem is not at hand for Catalan's equation, so the very same reason which allows our procedure to lead to a cyclotomic proof of Catalan but not of Fermat, allows for Frey curves to lead to a proof of Fermat but not of Catalan. This *anti-symmetry* remains intriguing and it is very well possible that the last word may not yet have been spoken about these two cyclotomic norm equations.

REFERENCES

- [1] A. Baker: *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Phil. Soc., **65**, (1969), pp. 439-444.
- [2] A. Baker: *A sharpening of the bounds for linear forms in logarithms I & II*, Acta Arith. **21**, (1972), 117-129; *ibid* **24**, (1973), pp. 33-36.
- [3] C. Bennett, J. Blass, A. M. W. Glass, D. Meronk and R. P. Steiner: *Linear Forms in the Logarithms of Three Positive Rational Integers*, J. de Théorie des Nombres de Bordeaux, **9**, (1997), pp. 97-136.
- [4] J. Blass, A.M.W. Glass and W. O'Neil: *Catalan's Conjecture and Linear Forms in Logarithms*, preprint.
- [5] Y. Bugeaud and G. Hanrot: *Un nouveau critère pour l'équation de Catalan*, (1999), Acta Arithmetica, to appear.
- [6] E. Catalan: *Note extraite d'une lettre adressée à l'éditeur*, Journal f. d. reine und angew. Math. **27** (1844), 192.
- [7] J. W. S. Cassels: *On the equation $a^x - b^y = 1$* , Amer. J. Math. **75** (1953) pp. 159-162.
- [8] J. W. S. Cassels: *On the equation $a^x - b^y = 1$, II*, Proc. Cambridge Society bf vol 56 (1960), pp. 97-103.
- [9] M. Eichler: *Eine Bemerkung zur Fermatschen Vermutung*, Acta Arith., **11** (1965), 129-131, err. 261.

- [10] A.M.W. Glass, D.B. Merson, T. Okada and R. Steiner: *A Small Contribution to Catalan's Equation*, J. Number Theory, **47**, (1994), pp. 131-37.
- [11] A. Granville: *The Latest on Catalan's Conjecture*, FOCUS-Newsletter of MAA, May/June 2001, pp. 4-5.
- [12] S. Hyvärinen: *Über das Catalan'sche Problem*, Ann. Univ. Turku Ser. AI **79** (1964), pp. 3-10.
- [13] S. Hyvärinen: *Über die Gleichung $ax^n - by^m = c$ und das Catalan'sche Problem*, Ann. Acad. Sci. Fennicae, Ser. AI, **Nr. 355** (1964).
- [14] K. Inkeri: *On Catalan's problem*, Acta Arithm. **9** (1964), pp. 285-290.
- [15] K. Inkeri: *On Catalan's conjecture*, J. of Number Theory **34** (1990), pp. 142-152.
- [16] K. Ireland and M. Rosen: *A Classical Introduction to Modern Number Theory*, Second Edition, Springer Graduate Texts in Mathematics **84**, (1990).
- [17] K. Iwasawa: *A Note on Jacobi Sums*, Symp. Math., **15**, (1975), pp. 447 - 459.
- [18] Ko Chao: *On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$* , Acta Sci. Natur. Univ. Szechuan **2** (1960), pp. 57-64.
- [19] Ko Chao: *On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$* , Sci. Sinica, **14**, (1965), pp. 457-460.
- [20] M. Langevin: *Quelques applications de nouveaux résultats de van der Poorten*, Sémin. Delange - Pisot - Poitou, Paris, Exp. 4.
- [21] M. Laurent, M. Mignotte and Y. Nesterenko: *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. of Number Theory, **55**, (1995), pp. 285-321.
- [22] V.A. Lebesgue: *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$* , Nouv. Ann. Math., **9**, pp. 178-181, (1850).
- [23] H.W.Lenstra Jr.: *Galois theory and primality testing*, In *Orders and their Applications*, I Reiner and K. W. Roggenkamp, eds., Lecture Notes in Mathematics **1142**, Springer Verlag, pp. 169-189.
- [24] R. Long: *Algebraic number theory*, Marcel Dekker, Monographs in Pure and Applied Mathematics **41**, (1977).
- [25] M. Mignotte: *Sur l'équation de Catalan*, C.R.Acad.Sci. Paris Ser I, **314**, (1992), pp. 165-68.
- [26] M. Mignotte: *A Criterion on Catalan's equation*, J.of Number Theory, **52**, (1995), pp. 280-83.
- [27] M. Mignotte: unpublished, cited by [5]
- [28] M. Mignotte: *Catalan's equation just before 2000*, Proceedings Inkeri Colloquium, Turku (2000), Eds. Jutila and Metsänkylä, to appear.
- [29] M. Mignotte and Y. Roy: *Catalan's equation has no new solution with either exponent less than 10651*, Experimental Mathematics, **4**, (1995), pp. 259-268.
- [30] M. Mignotte and Y. Roy: *Minorations pour l'équation de Catalan*, C.R.Acad.Sci. Paris **324**, (1997), pp. 377-80.
- [31] M. Mignotte: *Catalan's equation just before 2000*, Proceedings Inkeri Colloquium, Turku (2000), Eds. Jutila and Metsänkylä, to appear.
- [32] M. Mignotte: personal communication.
- [33] P. Mihăilescu: *A class number free criterion for Catalan*, to appear, J. of Number Theory.
- [34] P. Mihăilescu: *On the relative class group of cyclotomic extensions in presence of a solution to Catalan's equation*, submitted, J. of Number Theory.
- [35] M. Mignotte and M. Waldschmidt: *Linear forms in two logarithms and Schneider's method, III*, Ann. Fac. Sci. Toulouse (V), special issue (1990), pp. 43-75.
- [36] P. Ribenboim: *Catalan's conjecture*, Academic Press, (1994).
- [37] P. Ribenboim: *13 Lectures on Fermat's Last Theorem*, Springer Verlag (1979).
- [38] K. Ribet: *Private email communication*, (1999).
- [39] W. Schwarz: *A note on Catalan's equation*, Acta Arith. **vol 72**, (1995), pp. 277-279.
- [40] J.-P. Serre: *Local Fields*, Springer (1991), Graduate Texts in Mathematics **67**.
- [41] T.N.Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Maths. **87**, CUP, 1986.
- [42] R. Steiner: *Class Number Bounds on Catalan's Equation*, Math. Comp. **67**, (1998), pp. 1317-1322..

- [43] F. Thaine: *On the ideal class groups of real Abelian number fields*, Ann. of Math. **128** (1988), pp. 1-18.
- [44] F. Thaine: *On Fermat's Last Theorem and the Arithmetic of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$* , J. of Number Theory **29**, Nr. **3** (1988), pp. 297-299.
- [45] R. Tijdeman: *On the equation of Catalan*, Acta Arith. **29**, (1976), pp. 197-209.
- [46] L. Washington: *Introduction to Cyclotomic Fields*, Second Edition, Springer (1996), Graduate Texts in Mathematics **83**.

(P. Mihăilescu) GESAMTHOCHSCHULE PADERBORN
E-mail address, P. Mihăilescu: preda@upb.de