ON A CRITERION FOR CATALAN’S CONJECTURE

JAN-CHRISTOPH SCHLAGE-PUCHTA

Abstract. We give a new proof of a theorem of P. Mihăilescu which states that the equation \( x^p - y^q = 1 \) is unsolvable with \( x, y \) integral and \( p, q \) odd primes, unless the congruences \( p^q \equiv p \pmod{q^2} \) and \( q^p \equiv q \pmod{p^2} \) hold.

MSC-index: 11D61, 11R18

Keywords: Catalan’s conjecture, cyclotomic fields, class group

Improving criterions for Catalan’s equation by Inkeri, Mignotte, Schwarz and Steiner, Mihailescu proved the following theorem.

**Theorem 1.** Let \( p, q \) be odd prime numbers. Assume that \( p^q \not\equiv p \pmod{q^2} \) or \( q^p \not\equiv q \pmod{p^2} \). Then the equation \( x^p - y^q = 1 \) has no nontrivial integer solutions.

Here we will give a different proof of this theorem. More precisely, we will show the following statement.

**Theorem 2.** Let \( p, q \) be odd prime numbers, and assume that the equation \( x^p - y^q = 1 \) has some nontrivial solution. Then we have either \( q^2 | p^q - p \) or the \( q \)-rank of the relative class group of the \( p \)-th cyclotomic field is at least \( (p - 5)/2 \).

Note that different from Mihailescu’s proof of Theorem 1, we have to make use of estimates for the relative size of \( p \) and \( q \) obtained using bounds for linear forms in logarithms, thus the passage from Theorem 2 to Theorem 1 is by no means elementary. However, the proof of Theorem 2 makes much less use of special properties of cyclotomic fields than Mihailescu’s proof of Theorem 1, thus it might be easier to adapt to different situations.

To deduce Theorem 1 from Theorem 3, it suffices to show that the second alternative is impossible. Assume that \( x^p - y^q = 1 \), and that the \( q \)-rank of the relative class group of the \( p \)-th cyclotomic field is at least \( (p - 5)/2 \). This implies \( q^{(p-5)/2} \leq h^{-}(p) \). The class number \( h^{-}(p) \) was estimated by Masley and Montgomery, they showed that for \( p > 200 \)
we have \( h^{-}(p) < (2\pi)^{-p/2}p^{(p+31)/4} \). Thus we get \( q < \sqrt{p} \). On the other hand, Mignotte and Roy\cite{6} proved, that for \( q \geq 3000 \) we have \( p \leq 2.77q \log q (\log p - \log \log q + 2.33)^2 \), combining these inequalities and observing that Mignotte and Roy\cite{7} have shown that \( q > 10^5 \), thus \( \log \log q > 2.33 \), we get \( p \leq 1.92 \log^6 p \), which implies \( p < 6.6 \cdot 10^7 \), thus \( q < \sqrt{p} < 8200 \) contradicting the lower bound \( q > 10^5 \) mentioned above.

To prove theorem 3, we follow the lines of \cite{9}, incorporating an idea of Eichler\cite{2}. \( K \) be the \( p \)-th cyclotomic field, \( \zeta \) a \( p \)-th root of unity, \( I_K \) the group of fractional ideals in \( K \), \( i : K^* \to I_K \) the canonical map \( x \mapsto (x) \), \( K^+ = \mathbb{Q}(\zeta + \zeta^{-1}) \) be the maximal real subfield of \( K \), \( \mathcal{O}_K \) be the ring of integers of \( K \). Denote with \( r \) the \( q \)-rank of the relative class group of \( K \). We begin with a Lemma. \( \mathbb{Q} \) be the set of prime ideals dividing \( q \) in \( K \). Choose a primitive root \( g \) of \( p \) and define \( \sigma \in \text{Gal}(K|\mathbb{Q}) \) by the relation \( \zeta_{\sigma} = \zeta g \).

**Lemma 3.** There is a subgroup \( I_0 \) of \( I_K \) with the following properties:

1. The prime ideals in \( \mathbb{Q} \) do not appear in the factorization of any ideal in \( I_0 \)
2. \( I_K/(i(K^*)I_0) \) has \( q \)-rank \( r \)
3. If \( \epsilon \in K^* \) with \( (\epsilon) \in I_0 \), then \( \epsilon/\overline{\epsilon} \) is a root of unity.

**Proof:** This is Lemma 1 in \cite{9}.

Now assume that \( x \) and \( y \) are nonzero integers with \( x^p - y^q = 1 \). We have \cite{8}

\[
\left( \frac{x - \zeta}{1 - \zeta} \right) = j^q
\]

for some integral ideal \( j \). The ideal classes with \( j^q = (1) \) generate an \( r \)-dimensional vector space over \( \mathbb{F}_q \) in \( I_K/(i(K^*)I_0) \), hence there are integers \( a_0, \ldots, a_r \), not all divisible by \( q \), such that \( j^{a_0+a_1\sigma+\ldots+a_r\sigma^r} \) lies in \( i(K^*)I_0 \). Thus we get

\[
\left( \frac{x - x_{-1}(1 - \zeta)}{1 - \zeta} \right)^{a_0+a_1\sigma+\ldots+a_r\sigma^r} = \epsilon\alpha^q
\]

with \((\epsilon) \in I_0 \) and \( \alpha \) is \( q \)-integral for all prime ideals \( q \) dividing \( q \), since the left hand side is \( q \)-integral, and \((\epsilon) \) is not divisible by \( q \) by condition 1 of Lemma 4. We multiply this equation with \((\zeta^{-1}(1 - \zeta))^{a_0+a_1\sigma+\ldots+a_r\sigma^r} \) to get

\[
(1 - x_{-1})^{a_0+a_1\sigma+\ldots+a_r\sigma^r} = \epsilon'\lambda\alpha^q
\]

where \( \lambda \) divides some power of \( p \), and \( \epsilon' \) differs from \( \epsilon \) by some power of \( \zeta \), especially \((\epsilon) = (\epsilon') \).
By [1], we have $q | x$, thus the left hand side of (1) can be simplified $\pmod{q^2}$. We get

$$1 - x \left( a_0 \zeta^{-1} + a_1 \zeta^{-\sigma} + \ldots + a_r \zeta^{-\sigma^r} \right) \equiv \epsilon' \lambda \alpha^q \pmod{q^2} \quad (2)$$

The complex conjugate of the right hand side can be written as $\zeta^k \epsilon' \lambda \alpha^q$, since every $p$-th root of unity is the $q$-th power of some root of unity, this equals $\epsilon' \lambda \beta^q$ for some $\beta \in K^*$. Thus if we subtract the complex conjugate of (2), we get

$$x \left( a_0 \zeta^{-1} + \ldots + a_r \zeta^{-\sigma^r} - a_0 \zeta^{-\sigma} - \ldots - a_r \zeta^{\sigma^r} \right) \equiv \epsilon' \lambda (\alpha^q - \beta^q) \pmod{q^2} \quad (3)$$

The left hand side of (3) is divisible by $q$, since $x$ is divisible by $q$, and the bracket is integral. However, $(\epsilon') \in I_0$, and by construction we have $(\epsilon', q) = (1)$, and $\lambda$ divides some power of $p$, thus we have $(\lambda, q) = (1)$, too. Hence $q | \alpha^q - \beta^q$, and since $q$ is unramified, this implies $q^2 | \alpha^q - \beta^q$. Hence $q^2$ divides the left hand side of (3). But $x$ is rational, thus either $q^2 | x$, or $q$ divides the bracket. By [1], we have $x \equiv -(p^q - 1) \pmod{q^2}$, hence the first possibility implies $q^2 | p^q - p$. Thus to prove our theorem, it suffices to show that the second choice is impossible.

Assume that

$$a_0 \zeta^{-1} + a_1 \zeta^{-\sigma} + \ldots + a_r \zeta^{-\sigma^r} - a_0 \zeta^{-\sigma} - \ldots - a_r \zeta^{\sigma^r} = q \alpha$$

This can be written as

$$a_0 X^{-1} + a_1 X^{-\sigma} + \ldots + a_r X^{-\sigma^r} - a_0 X^{-\sigma} - \ldots - a_r X^{\sigma^r} = q F(X) + G(X) \Phi(x)$$

where $F$ and $G$ are polynomials with rational integer coefficients, $\Phi$ is the $p$-th cyclotomic polynomial, and $\pi$ denotes the least nonnegative residue $\pmod{p}$ of $a$. The left hand side is of degree $\leq p - 1$, and since we may assume that the leading coefficient of $G$ is prime to $q$, this implies that $G$ is constant. Further on the left hand side there are at most $2r + 2 \leq p - 3$ nonvanishing coefficients, thus $G = 0$. This implies that all coefficients on the left hand side vanish $\pmod{q}$. But all the monomials on the left hand side have different exponents, since otherwise we would have $g^{s_1} \equiv \pm g^{s_2} \pmod{p}$, which would imply that the order of $g$ is $\leq 2r \leq p - 5$, but $g$ was chosen to be primitive. Hence all $a_i$ vanish $\pmod{q}$, but this contradicts the choice of the $a_i$ at the very beginning.

References

[1] J. W. S. Cassels, *On the equation $a^x - b^y = 1$* Proc. Camb. Philos. Soc. 56, 97-103 (1960)

[2] M. Eichler, *Eine Bemerkung zur Fermatschen Vermutung*, Acta Arith. 11, 129-131 (1965)
[3] K. Inkeri, *On Catalan’s Conjecture*, J. Number Theory 34, 142-152 (1990)
[4] J. Masley, H. L. Montgomery, *Cyclotomic fields with unique factorization* J. reine angew. Math. 286/287, 248-256 (1976)
[5] M. Mignotte, *A criterion on Catalan’s equation* J. Number Theory 52, 280-283 (1995)
[6] M. Mignotte, Y. Roy *Catalan’s equation has no new solution with either exponent less than 10651* Exp. Math. 4, 259-268 (1995)
[7] M. Mignotte, Y. Roy, *Minorations pour l’équation de Catalan* C. R. Acad. Sci., Paris, Ser. I 324, 377-380 (1997)
[8] P. Mihăilescu, *A class number free criterion for Catalan’s conjecture*, manuscript, Zürich (1999)
[9] W. Schwarz, *A note on Catalan’s equation* Acta Arith. 72, 277-279 (1995).
[10] R. Steiner, *Class number bounds and Catalan’s equation* Math. Comput. 67, 1317-1322 (1998).

Jan-Christoph Puchta
Mathematisches Institut
Eckerstraße 1
79104 Freiburg
Germany
jcp@arcade.mathematik.uni-freiburg.de