ACTA ARITHMETICA
LXXII.3 (1995)

A note on Catalan's equation

by

Wolfgang Schwarz (Saarbrücken)

We give a small, but very useful modification of a criterion of Mignotte ([4]) for Catalan's equation, replacing the class number of a certain abelian field by the relative class number, which is much easier to compute. The proof is the same, apart from the idea to consider the class group modulo the ideals coming from the real subfield.

We use the following notation: K is a CM-field, I_K its group of fractional ideals and $i : K^* \to I_K$ the canonical map $x \mapsto (x)$; j denotes complex conjugation, K^+ the maximal real subfield and $h^-(K)$ the relative class number of K; $\mathcal{O}_K$ is the ring of integral elements of K.

Lemma 1. *Let K be a CM-field and $\mathcal{Q}$ a finite set of prime ideals of K. There is a subgroup I_0 of the ideal group I_K such that*

(i) *the prime ideals in $\mathcal{Q}$ do not appear in the factorization of any ideal in I_0;*
(ii) *$I_K/(i(K^*)I_0)$ has cardinality $h^-(K)$ or $2h^-(K)$;*
(iii) *if $\varepsilon \in K^*$ with $(\varepsilon) \in I_0$, then ε^{1-j} is a root of unity.*

Proof. Let I_0 consist of those ideals which are in the image of the canonical map $I_{K^+} \to I_K$, and which do not contain any prime ideal in $\mathcal{Q}$. If $(\varepsilon) \in I_0$, then $(\varepsilon^j) = (\varepsilon)$, so ε^{1-j} is a unit, hence also a root of unity because all its conjugates have absolute value 1 (cf. [6], Lemma 1.6). It remains to show (ii). It is an easy consequence of the approximation theorem that every ideal class contains an ideal without primes in $\mathcal{Q}$ (see e.g. [3], IV, Corollary 1.4). Therefore $I_K/(i(K^*)I_0)$ = ideal class group of K modulo image of the ideal class group of K^+. By [6], Theorem 10.3, at most 2 ideal classes of K^+ become principal in K, so the statement follows. ∎

Theorem 1. *Let $p \neq q$ be odd prime numbers. Let ζ be a primitive p-th root of unity and K an imaginary subfield of $L := \mathbb{Q}(\zeta)$. Catalan's equation $x^p - y^q = 1$ has no nontrivial integral solution if*

$$q \nmid h^-(K) \quad \text{and} \quad p^{q-1} \not\equiv 1 \bmod q^2.$$

P r o o f. Assume for contradiction that there is a nontrivial solution. According to [2], we have

$$\left(\frac{x-\zeta}{1-\zeta}\right) = \mathbf{a}^q$$

for an integral ideal $\mathbf{a}$ of L. We let $\lambda := N_{L/K}(1-\zeta)$ and multiply $x-\zeta$ by $-\zeta^{-1}$ to get

$$(N_{L/K}(1-x\zeta^{-1})) = (\lambda)N_{L/K}\mathbf{a}^q.$$

Let I_0 be as in Lemma 1, with $\mathcal{Q}$ consisting of all prime divisors of q. Since the order of the group $I_K/(i(K^*)I_0)$ is not divisible by q, there exists an $\alpha \in K^*$ such that $N_{L/K}\mathbf{a} \in (\alpha)I_0$; defining ε by the equation

$$N_{L/K}(1-x\zeta^{-1}) = \varepsilon\lambda\alpha^q,$$

we see that $(\varepsilon) \in I_0$, and hence α is $\mathbf{q}$-integral for all prime divisors $\mathbf{q}$ of q. Now ε^{1-j} is a root of unity, and so is λ^{1-j}, since $(1-\zeta)^{1-j} = -\zeta$. But K contains at most the $2p$th roots of unity, and $2p$ is coprime to q; thus every root of unity is a qth power, and we can write $(\varepsilon\lambda\alpha^q)^j = \varepsilon\lambda\beta^q$, where $\beta \in K^*$, like α, has a denominator prime to q. We consider

$$\gamma := (1-j)N_{L/K}(1-x\zeta^{-1}) = \varepsilon\lambda(\alpha^q - \beta^q).$$

If we show $q \,|\, \gamma$, then $\alpha^q \equiv \beta^q \bmod q$; since q is unramified, $\mathcal{O}_K/(q)$ is a direct product of fields, and the multiplicative group mod q has order prime to q; thus it follows that $\alpha \equiv \beta \bmod q$; writing $\alpha = \beta + tq$ (with $t \in \mathcal{O}_K$), we see that $\alpha^q \equiv \beta^q \bmod q^2$. Thus $q^2 \,|\, \gamma$.

But we have

$$N_{L/K}(1-x\zeta^{-1}) = \prod_\sigma (1-x(\zeta^{-1})^\sigma) \equiv 1 - x\,\mathrm{Tr}_{L/K}(\zeta^{-1}) \bmod x^2,$$

which yields

$$\gamma \equiv x(\mathrm{Tr}_{L/K}(\zeta - \zeta^{-1})) \bmod x^2.$$

By [1], $q \,|\, x$ (hence $q \,|\, \gamma$) and $x \equiv -(p^{q-1}-1) \bmod q^2$, so by our assumption $q^2 \nmid x$. Since $q \,|\, \gamma$ implies $q^2 \,|\, \gamma$, it would follow that $q \,|\, (\mathrm{Tr}_{L/K}(\zeta - \zeta^{-1}))$, which is not true, because K is imaginary, and $\zeta, \ldots, \zeta^{p-1}$ is a $\mathbb{Z}$-basis for the integral elements of L. ∎

Acknowledgements. I want to thank Prof. A. Pethő for calling my attention to this topic.

References

[1] J. W. S. Cassels, *On the equation $a^x - b^y = 1$, II,* Proc. Cambridge Philos. Soc. 56 (1960), 97–103.
[2] K. Inkeri, *On Catalan's conjecture*, J. Number Theory 34 (1990), 142–152.
[3] G. Janusz, *Algebraic Number Fields*, Academic Press, 1973.
[4] M. Mignotte, *A criterion on Catalan's equation*, J. Number Theory, to appear.
[5] M. Mignotte et Y. Roy, *L'équation de Catalan*, Prépublication de l'Institut de Recherche Mathématique Avancée, Strasbourg, 1992.
[6] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, Berlin, 1982.

FACHBEREICH 9 MATHEMATIK
UNIVERSITÄT DES SAARLANDES
D-66041 SAARBRÜCKEN, GERMANY

Received on 28.11.1994
and in revised form on 12.1.1995 (2701)