ACTA ARITHMETICA
126.3 (2007)

Unsolvability of the Pell minus-equation for certain odd discriminants

by

Gerhard A. Bachmaier (Graz)

Introduction. Already Lagrange knew that the negative Pell equation

$$X^2 - DY^2 = -1 \tag{1}$$

is solvable in rational integers *if and only if* the continued fraction expansion of $\sqrt{D}$ has an odd period. Simpler applicable algebraic conditions for discriminants with two or three prime divisors were found by Dirichlet in terms of quadratic and biquadratic characters. But within his framework, the cases where all prime divisors are biquadratic residues to each other, are not decidable. The following theorem yields decidability for a special subcase.

Theorem. *Assume $D = pq$ where $p \equiv q \equiv 1 \bmod 4$ are distinct positive primes. If $(p/q)_4 = (q/p)_4 = 1$, and if $D = pq = a^4 + 4b^2$ with $(a/p) = -1$, then the negative Pell equation* (1) *does not have an integral solution.*

Proof. Assume that $t^2 - Du^2 = -1$ is an integer solution of (1), and put $\varepsilon = t + u\sqrt{D}$. Since $\beta = 2b + \sqrt{D}$ is primitive (i.e., has no rational divisors $\neq \pm 1$) and has norm $-a^4$, the element $\varepsilon\beta$ is primitive and has norm $+a^4$, hence there exist coprime integers r, s such that $r^2 - Ds^2 = a^4$.

We now use the following

Lemma 1. *Assume that $x^2 - Dy^2 = m^2$ for coprime integers x, y and some odd m. Then one of the equations $X^2 - DY^2 = m$ or $X^2 - DY^2 = pm$ has a primitive solution.*

This implies that either $X^2 - DY^2 = a^2$ or $X^2 - DY^2 = pa^2$ is solvable. The second equation does not have solutions by Lemma 2 below. Thus we are left with $X^2 - DY^2 = a^2$. Reapplying Lemma 1 shows that $X^2 - DY^2 = a$ or $X^2 - DY^2 = pa$ is solvable. Both equations imply immediately that $(a/p) = +1$, contrary to our assumptions. ∎

2000 *Mathematics Subject Classification*: Primary 11D09.

Proof of Lemma 1. From $x^2 - Dy^2 = m^2$ we get $(x-m)(x+m) = pqy^2$. It is easily checked that $\gcd(x-m, x+m) = 2$, hence $x+m = 2vr^2$ and $x-m = 2ws^2$ for coprime r, s and $vw = pq$. Subtracting these equations from each other and dividing through by 2 gives $m = vr^2 - ws^2$. Now there are the following cases:

- $v = 1,\ w = pq$: then $r^2 - Ds^2 = m$.
- $v = p,\ w = q$: then $pr^2 - qs^2 = m$, hence $(pr)^2 - Ds^2 = pm$.
- $v = q,\ w = p$: then $Dr^2 - (qs)^2 = pm$, and using the unit ε we find $(qst + Dru)^2 - D(qs + rt)^2 = pm$.
- $v = pq,\ w = 1$: here $Dr^2 - s^2 = m$, and using ε we get what we want.

Primitivity in all cases is easily checked. ∎

LEMMA 2. *The equation $X^2 - DY^2 = pa^2$ does not have a solution.*

Proof. Dividing through by p shows that there are integers r, s with

$$pr^2 - qs^2 = a^2. \tag{2}$$

This implies $(-1/p)_4(q/p)_4(s/p) = (a/p)$. Now $(q/p)_4 = +1$ and $(a/p) = -1$ by assumption; next $(-1/p)_4 = (2/p)$. Thus we find $(2/p)(s/p) = -1$.

Now write $s = 2^\ell v$ for some odd integer v; since s must be even, we have $\ell \geq 1$. Then quadratic reciprocity and (2) show that $(v/p) = (p/v) = 1$, hence $(s/p) = (2/p)^\ell$. If $\ell = 1$, then $-1 = (2/p)(s/p) = (2/p)^2 = +1$, a contradiction. Thus $\ell \geq 2$, hence $p \equiv 1 \bmod 8$ by (2), so we get the same contradiction $-1 = (2/p)(s/p) = +1$. ∎

Acknowledgements. We thank the referee for valuable suggestions to shorten and simplify the proof.

This paper was inspired by a similar theorem for $D = 2p$ (see [1], [2]).

References

[1] E. Brown, *The class number and fundamental unit of $\mathbb{Q}(\sqrt{2p})$ for $p \equiv 1 \pmod{16}$ a prime*, J. Number Theory 16 (1983), 95–99.

[2] H. von Lienen, *The quadratic form $x^2 - 2py^2$*, ibid. 10 (1978), 10–15.

Institute of Medical Informatics, Statistics, and Documentation
Medical University of Graz
Auenbruggerplatz 2
A-8036 Graz, Austria
E-mail: gerhard.bachmaier@meduni-graz.at

Received on 26.4.2006
and in revised form on 9.11.2006 (5191)