ON A QUESTION OF KAPLANSKY II

P.G. WALSH

(Communicated by F. Luca)

This paper is dedicated to the memory of
Professor Irving Kaplansky

ABSTRACT. There is a question attributed to Irving Kaplansky concerning the solvability of the quadratic equation $x^2 - py^2 = a$ in the case that the prime $p = a^2 + (2b)^2$. This question was answered in the affirmative by Mollin [1], although according to [3], this result is implicit in the work of Gauss and Legendre. The proof appearing in [1] was later simplified in [4], and it was also shown therein that Kaplansky's question was a special case of a more general result. Using the method of proof in [4], Mollin [2] has recently extended the results of [4], but upon further consideration, it appears that there is a more general phenomenon occurring, and also, that one of the assumptions in the main theorem of [2] is unnecessary. In this paper we prove this generalization, and eliminate one of the assumptions stated in the main result of [2]. The proof is again based on the method described in [4].

1. INTRODUCTION

In an earlier article [4], the author generalized a result of Mollin, and at the same time, simplified the method of proof. Recently, Mollin has used this same elementary approach to further the results of [4]. The purpose of this present paper is to extend the results of [2]. The method remains the same as in [4], with the appropriate modifications described in [2] in order to deal with parity issues.

Theorem 1.1. *Let $d \equiv 1 \pmod 4$ be a positive integer, and assume that $n = a^2 + db^2$ for positive integers a, b with a odd and $(n, a) = 1$. Assume further that there is a positive integer c, with $(a, c) = 1$ for which the equation*

$$X^2 n - Y^2 d = c^2$$

is solvable in coprime positive integers X, Y. Then there exists a (possibly trivial) factorization rs of nd, and a divisor f of σc, for which the equation

$$rx^2 - sy^2 = af$$

is solvable in positive integers x, y, where $\sigma = 2$ if n is odd and c is even, and $\sigma = 1$ otherwise.

For simplicity, Theorem 1 only deals with the case $d \equiv 1 \pmod 4$. A similar statement holds for the other cases, which we leave as an exercise for the reader.

We note that Theorem 1 not only extends the result of [2], which dealt with the particular case $d = 1$, but moreover removes an unnecessary assumption contained in the statement of the main theorem in [2]. Specifically, it is assumed therein that the quadratic equation $X^2 - nY^2 = -1$ is solvable. As the conclusion of the main theorem in [2] does not place any restriction on the constructed factors r and s of n, there is no need, during the course of the proof, to multiply by a unit of norm -1. Therefore, we do not need to include an analogous assumption (that the quadratic equation $x^2 n - y^2 d = 1$ be solvable in positive integers x, y) in the statement of Theorem 1 above.

2. Proof of Theorem 1

Let (T, U) be coprime positive integers which satisfy $T^2 n - U^2 d = c^2$, and let α be defined $\alpha = T\sqrt{n} + U\sqrt{d}$. Let $\beta = \sqrt{n} + b\sqrt{d}$, and define integers u, by $u = Tn + Ubd, v = Tb + U$. Then

$$\alpha\beta = (Tn + Ubd) + (Tb + U)\sqrt{nd} = u + v\sqrt{nd}$$

is an element in $\mathbf{Z}[\sqrt{nd}]$ with norm $a^2 c^2$.

Let $g = (u, v)$, then clearly g divides c^2, but in fact, g divides c. We provide the details for this assertion, as the reasoning in [2] appears to be flawed. Suppose that p is a prime dividing g, with p^μ properly dividing g ($\mu > 0$), and such that p^μ does not divide c. Note that p divides c because p^μ divides c^2. It follows that p^μ divides both u and v, hence $p^{2\mu}$ divides $u^2 - v^2 nd = a^2 c^2$. By assumption, $p^{2\mu}$ does not divide c^2, and so p must divide a, contradicting the fact that $(a, c) = 1$. We conclude that g divides c, and from the equation $u^2 - v^2 nd = a^2 c^2$, we deduce that

(1) $\qquad (u/g)^2 - a^2(c/g)^2 = ((u/g) + a(c/g))((u/g) - a(c/g)) = (v/g)^2 nd.$

We now break up the argument into three cases, depending on the relative parities of n and c. We note that n and c cannot both be even, as this would contradict either $(n, a) = 1$ or $(T, U) = 1$.

Case 1: c even, n odd.

In this case, as n, a and d are odd, and $n = a^2 + db^2$, it follows that b is even. Also, the assumption that c is even implies that T and U are odd (as they are coprime), whence it follows that both u and v are odd, which by equation (1) implies that there are integers A, B, r, s, with $v/g = AB$ and $nd = rs$, satisfying

$$(u/g) + a(c/g) = A^2 r, \ (u/g) - a(c/g) = B^2 s,$$

from which it follows that

$$A^2 r - B^2 s = af,$$

with $f = 2(c/g)$.

Case 2: c odd, n even.

In this case, since $d \equiv 1 \pmod 4$ and $(a, b) = 1$, it follows that $n \equiv 2 \pmod 4$, and that b is odd. By considering the equation $T^2 n - U^2 d = c^2$ modulo 4, it is readily verified that both T and U are odd. We conclude that $u = Tn + Ubd$ is odd, and that $v = Tb + U$ is even. Therefore, there are integers A, B, r, s, with $nd = rs$ and $v/g = 2AB$, satisfying

$$(u/g) + a(c/g) = 2A^2 r, \ (u/g) - a(c/g) = 2B^2 s,$$

from which it follows that

$$A^2 r - B^2 s = af,$$

with $f = c/g$.

Case 3: c odd and n odd.

Since $d \equiv 1 \pmod 4$, it follows that $n \equiv 1 \pmod 4$, and again by considering the equation $T^2 n - U^2 d = c^2$ modulo 4 we deduce that T is odd and that U is even. Therefore, in this case we find again that $u = Tn + Ubd$ is odd and that $v = Tb + U$ is even, and the rest of the proof for this case follows as in the previous case.

References

[1] R.A. MOLLIN. *Proof of some conjectures by Kaplansky,* C.R. Math. Rep. Acad. Sci. Canada **23** (2001), 60-64.

[2] R.A. MOLLIN. *On a generalized Kaplansky conjecture,* Int. J. Contemp. Math. Sciences **2** (2007), 411-416.

[3] N. Tzanakis [M.R. 1913340 (2003g:11027)], Reviews of the A.M.S., 2003.

[4] P.G. WALSH, *On a conjecture of Kaplansky,* Amer. Math. Monthly **109** (2002), 60-61.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OTTAWA, 585 KING EDWARD ST., OTTAWA, ONTARIO, CANADA, K1N-6N5

E-mail address: `gwalsh@mathstat.uottawa.ca`