

On a Generalized Kaplansky Conjecture

R. A. Mollin

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta, Canada, T2N 1N4
<http://www.math.ucalgary.ca/~ramollin/>
ramollin@math.ucalgary.ca

Abstract

A conjecture was related to this author in correspondence, some years ago, with Irving Kaplansky, which according to Professor Kaplansky, was inspired by the proof of [4, Theorem 6.5.9, p. 348]. It asserts that if p is a prime with representation $p = a^2 + (2b)^2$, then the equation $x^2 - py^2 = a$ is solvable in integers x, y . In [5], we proved this conjecture along with several others by him. Subsequently, Walsh in [6], gave a slight extension of the above proof: if $n \equiv 1 \pmod{4}$ is a nonsquare integer with representation $n = a^2 + (2b)^2$ for integers a and b , and if $X^2 - nY^2 = -1$ has solutions in integers X, Y , then n has a factorization $n = rs$ such that the equation $ru^2 - sv^2 = a$ is solvable in integers u, v . It is the purpose of this work to generalize the latter to a much wider range of cases as given in Theorem 1.1 below. We illustrate with several examples to show the wide applicability of the result.

Mathematics Subject Classification: 11A51, 11D09, 11R11

Keywords: Diophantine equations

1 Generalized Conjecture of Kaplansky

In [1], Feit noted that the aforementioned conjecture of Kaplansky is actually implicit in work of Gauss [2, Section 265, pp. 290–291], and work of Legendre [3, pp. 70–71]. However, it does not seem to have been explicitly

proven before the work in [1], [5], and [6]. The following result has no analogue in the literature.

The following generalizes [6] which in turn generalized [5].

Theorem 1.1 *Let $n \in \mathbb{N}$, where n is not a perfect square, and $n = a^2 + b^2$ for some $a, b \in \mathbb{N}$, where a is odd. Suppose that there exist primitive solutions to both*

$$x^2 - ny^2 = -1, \quad (1.1)$$

and

$$X^2 - nY^2 = -c^2, \text{ where } c \in \mathbb{N} \text{ with } \gcd(a, c) = 1. \quad (1.2)$$

Then there exists a factorization $n = rs$, possibly trivial, with $r, s \in \mathbb{N}$ such that $rw^2 - sz^2 = ad$ has a solution where d is a positive divisor of σc where $\sigma = 2$ if n is odd and c is even, and $\sigma = 1$ otherwise.

Proof. Let $T + U\sqrt{n}$ be a primitive integral solution of $X^2 - nY^2 = -c^2$, and set

$$u + v\sqrt{n} = (b + \sqrt{n})(T + U\sqrt{n}) \quad (1.3)$$

so

$$u^2 - v^2n = (ac)^2. \quad (1.4)$$

Using Equation (1.3), we see that if $\gcd(u, v) = g$ then $g \mid c^2$ since

$$(u + v\sqrt{n})(T - U\sqrt{n}) = -c^2(b + \sqrt{n}).$$

If g does not divide c , then there must exist a prime p such that p^{2j} divides g for some $j \in \mathbb{N}$ so that p^{2j} divides c^2 but p^j does not divide c . Hence, by Equation (1.4), we must have that $\gcd(c, a) > 1$ contradicting the hypothesis. Therefore, $g \mid c$. Thus by Equation (1.4),

$$\left(\frac{u}{g}\right)^2 - a^2 \left(\frac{c}{g}\right)^2 = \left(\frac{v}{g}\right)^2 n. \quad (1.5)$$

Now we consider three cases that depend upon the relative parities of n and c .

Case 1.1 *c is even and n is odd.*

Since n is a sum of two squares then it follows that $n \equiv 1 \pmod{4}$, so b is even in Equation (1.3). Also, it follows from congruence conditions modulo 4 that T, U are both odd. Hence u, v are both odd. Since $\gcd(u/g, v/g) = 1$, then by

Equation (1.5), there exist $r, s \in \mathbb{N}$ such that $n = rs$, and $v_1, v_2 \in \mathbb{N}$ such that $v/g = v_1v_2$ with

$$\frac{u}{g} \pm \frac{ca}{g} = sv_1^2, \tag{1.6}$$

and

$$\frac{u}{g} \mp \frac{ca}{g} = rv_2^2. \tag{1.7}$$

Therefore,

$$rv_2^2 - sv_1^2 = \mp 2ca/g = \mp ad,$$

where $d = 2c/g \mid 2c$. In the event that the minus sign holds, we invoke a solution $T_1 + U_1\sqrt{n}$ to Equation (1.1). Then we replace $v_2\sqrt{r} + v_1\sqrt{s}$ by $(T_1 + U_1\sqrt{n})(v_2\sqrt{r} + v_1\sqrt{s})$.

Case 1.2 c is odd and n is even.

In this case, $n \equiv 2 \pmod{4}$ since n is a sum of two squares, so a, b are both odd. Thus, $T^2 - 2U^2 \equiv -1 \pmod{4}$ so if U is even, $T^2 \equiv -1 \pmod{4}$, a contradiction, so U and T are both odd. Therefore, $u = bT + Un$ is odd and $v = bU + T$ is even. Since $\gcd(u/g, v/g) = 1$, there exist $r, s \in \mathbb{N}$ such that $n = rs$, and $v_1, v_2 \in \mathbb{N}$ such that $v/g = 2v_1v_2$ with

$$\frac{u}{g} \pm \frac{ca}{g} = 2sv_1^2, \tag{1.8}$$

and

$$\frac{u}{g} \mp \frac{ca}{g} = 2rv_2^2. \tag{1.9}$$

Therefore,

$$rv_2^2 - sv_1^2 = \mp ca/g = \mp ad,$$

where $d = c/g \mid c$. If the minus sign holds, we deal with this as in with case 1.1.

Case 1.3 c and n are both odd.

In this case, $n \equiv 1 \pmod{4}$ since it is a sum of two squares. Again by congruence conditions modulo 4, T is even and U is odd. Therefore, b is even in Equation (1.3) so we must have that u/g is odd and v/g is even. Therefore, there exist $v_1, v_2 \in \mathbb{N}$ such that $2v_1v_2 = v/g$ and by Equation (1.5), there exist $r, s \in \mathbb{N}$ such that $n = rs$, and $v_1, v_2 \in \mathbb{N}$ such that $v/g = 2v_1v_2$ with

$$\frac{u}{g} \pm \frac{ca}{g} = 2sv_1^2, \tag{1.10}$$

and

$$\frac{u}{g} \mp \frac{ca}{g} = 2rv_2^2. \tag{1.11}$$

Therefore,

$$rv_2^2 - sv_1^2 = \mp ca/g = \mp de,$$

where $d = c/g \mid c$ and $e = a$ is odd. In the event that the minus sign holds, we invoke a solution $T_1 + U_1\sqrt{n}$ to Equation (1.1). Then we replace $r\sqrt{v_2} + v_1\sqrt{s}$ by $(T_1 + U_1\sqrt{n})(v_2\sqrt{r} + v_1\sqrt{s})$.

Cases (1.1)–(1.3) complete the proof. □

The following is immediate from the above, since when a prime p is a sum of two squares, then Equation (1.1) is necessarily solvable.

Corollary 1.1 (Mollin [5])

If p is a prime with representation $p = a^2 + (2b)^2$, then the equation $x^2 - py^2 = a$ is solvable in integers x, y

The following is immediate from Theorem 1.1 since it is the case where $c = 1 = \sigma$.

Corollary 1.2 (Walsh [6])

If $n \equiv 1 \pmod{4}$ is a nonsquare integer with representation $n = a^2 + (2b)^2$ for integers a and b , and if $X^2 - nY^2 = -1$ has solutions in integers X, Y , then n has a factorization, possibly trivial, $n = rs$ such that the equation $ru^2 - sv^2 = a$ is solvable in integers u, v .

The following is an illustration of Case 1.1 in the proof of Theorem 1.1.

Example 1.1 *Let $n = 145 = 1^2 + 12^2 = a^2 + b^2$. Since*

$$X^2 - 145Y^2 = 9^2 - 145 \cdot 1^2 = -8^2 = -c^2,$$

and

$$X^2 - nY^2 = 12^2 - 145 \cdot 1^2 = -1,$$

we have that if $r = 5$ and $s = 29$, then

$$rw^2 - sz^2 = ad = 5 \cdot 171^2 - 29 \cdot 71^2 = 16 = 2c = \sigma c. \tag{1.12}$$

Notice that, in the notation of the proof of Theorem 1.1, $u = 253$, $v = 21$, $g = 1$, $v_1 = 3$, $v_2 = 7$, and

$$rv_2^2 - sv_1^2 = 5 \cdot 7^2 - 29 \cdot 3^2 = -16 = -2c,$$

so we invoke the solution $12 + \sqrt{145}$ to Equation (1.1) and calculate

$$(12 + \sqrt{145})(5\sqrt{7} + 3\sqrt{29}) = 171\sqrt{5} + 71\sqrt{29},$$

which is how we get Equation (1.12).

The following is an illustration of Case 1.2 in the proof of Theorem 1.1.

Example 1.2 Let $n = 106 = 5^2 + 9^2 = a^2 + b^2$. We have that

$$\begin{aligned} 4005^2 - 389^2 \cdot 106 &= x^2 - ny^2 = -1, \\ 28035^2 - 2723^2 \cdot 106 &= X^2 - nY^2 = -c^2 = -49, \\ 106 = n = rs &= 2 \cdot 53, \end{aligned}$$

and

$$rw^2 - sz^2 = 2 \cdot 27^2 - 53 \cdot 139^2 = 5 \cdot 1 = ad. \quad (1.13)$$

In the notation of Case 1.2 in the proof of Theorem 1.1, $u = 540953$, $v = 52542$, $v_1 = 27$, $v_2 = 139$, and $g = 7 = c$, whence Equation (1.13).

The last illustration is of Case 1.3 in the proof of Theorem 1.1.

Example 1.3 Let $n = 845 = 5 \cdot 13^2 = 29^2 + 2^2 = a^2 + b^2$, for which we have that

$$\begin{aligned} x^2 - ny^2 &= 12238^2 - 421^2 \cdot 845 = -1, \\ X^2 - nY^2 &= 36714^2 - 1263^2 \cdot 845 = -9 = -c^2, \end{aligned}$$

and

$$rw^2 - sz^2 = 10671943^2 - 367126^2 \cdot 845 = 29 \cdot 1 = a \cdot d. \quad (1.14)$$

In the notation of the proof 1.3 in Theorem 1.1, $u = 1140663$, $v = 39240$, $g = 3 = c$, $v_1 = 15$, $v_2 = 436$, and

$$rv_2^2 - sv_1^2 = 1 \cdot 436^2 - 845 \cdot 15^2 = -29 = -a,$$

so we invoke the solution $12238 + 421\sqrt{845}$ to Equation (1.1) and calculate

$$(12238 + 421\sqrt{845})(436 + 315\sqrt{845}) = 10671943 + 367126\sqrt{845},$$

which is how we get Equation (1.14).

Acknowledgements: The author's research is supported by NSERC Canada grant # A8484.

References

- [1] W. Feit, *Some Diophantine equations of the form $x^2 - py^2 = z$* , Proc. Amer. Math. Soc. **129** (000), 623–625.
- [2] C.F. Gauss, **Disquisitiones Arithmeticae**, English Edition, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo (1966).
- [3] A.-M. Legendre, **Théorie des Nombres**, Librairie Scientifique et Technique, A. Blanchard, Paris (1955).
- [4] R.A. Mollin, **Fundamental Number Theory with Applications**, CRC Press, Boca Raton, New York, London, Tokyo, (1998).
- [5] R.A. Mollin, *Proof of some conjectures by Kaplansky*, C. R. Math. Rep. Acad. Sci. Canada **23** (2001), 60–64.
- [6] P.G. Walsh, *On a question of Kaplansky*, American Math. Monthly, **109** (2002), 60-661.

Received: June 13, 2006