On a Question of Kaplansky

P. G. Walsh

1. INTRODUCTION. According to [**1**] and [**4**], Kaplansky asked for a proof of the following: if a prime p has the representation $p = a^2 + (2b)^2$, then the equation $X^2 - pY^2 = a$ is solvable in integers X and Y. As noted in [**1**], this result is implicit in Section 265 of [**2**] and p. 70–71 of [**3**], although the explicit statement does not seem to appear in the literature.

The proof appearing in [**1**] makes use of an array of facts, including the structure of both the unit group and the class group of the ring of integers of the field $Q(\sqrt{p})$, along with unique factorization of ideals in this ring. The proof appearing in [**4**] uses an assortment of facts from algebraic number theory, most of which are taken as references from one of the author's books, and not stated explicitly.

The purpose of this note is to put the original problem in its proper place by providing an elementary, self-contained, and constructive proof. Moreover, our proof lends itself to a generalization of Kaplansky's original question for composite integers in place of p. It does not seem that the methods in [**1**] and [**4**] can be used to establish this generalization. We gratefully acknowledge Walter Feit and Karl Dilcher for their encouragement.

Theorem 1. *Let $n \equiv 1 \pmod 4$ be a nonsquare positive integer such that $n = a^2 + (2b)^2$ for some integers a and b. Assume that the Pell equation $X^2 - nY^2 = -1$ is solvable in integers. Then n admits a (possibly trivial) factorization $n = rs$ such that the equation $rX^2 - sY^2 = a$ is solvable in integers X and Y.*

It is evident that the question of Kaplansky is answered by this theorem, since in the case that n is prime, the Pell equation $X^2 - nY^2 = -1$ is solvable. This last fact is easily deduced from the observation that the ring of integers of the field $\mathbf{Q}(\sqrt{n})$ has a group of units of positive rank.

Proof of theorem. Assume that $n = a^2 + (2b)^2$, and let $T + U\sqrt{n}$ be a solution to $X^2 - nY^2 = -1$. Considering this equation modulo 4, we see that T is even and that U is odd. Let

$$u + v\sqrt{n} = (2b + \sqrt{n})(T + U\sqrt{n}). \tag{1}$$

Then u is odd, v is even, $(u, v) = 1$, and

$$u^2 - nv^2 = a^2. \tag{2}$$

To see that $(u, v) = 1$, simply note using (1) that

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

From (2), using the fact that v is even and $(u, v) = 1$, we see that

$$u \pm a = 2sv_1^2, \quad u \mp a = 2rv_2^2$$

for some integers v_1, v_2 satisfying $2v_1v_2 = v$, and integers r, s satisfying $rs = n$. Therefore,

$$rv_2^2 - sv_1^2 = \pm a,$$

and the result follows upon replacing $v_2\sqrt{r} + v_1\sqrt{s}$ by $(T + U\sqrt{n})(v_2\sqrt{r} + v_1\sqrt{s})$ in the case that $rv_2^2 - sv_1^2 = -a$. ∎

We remark that an argument similar to the one presented shows that, under the same hypotheses, n admits a (possibly different) factorization $n = rs$ for which the equation $rX^2 - sY^2 = 4b$ is solvable in integers. On the other hand, it is not always the case that an equation of the form $rX^2 - sY^2 = 2b$ with $n = rs$ is solvable, as illustrated by the case $n = 5$.

REFERENCES

1. W. Feit, Some Diophantine equations of the form $x^2 - py^2 = z$, *Proc. Amer. Math. Soc.* **129** (2000) 623–625.
2. C. F. Gauss, *Disquisitiones Arithmeticae* (trans. A. A. Clarke), Yale University Press, New Haven, 1966.
3. A.-M. Legendre, *Théorie des Nombres*, Librairie Scientifique et Technique, A. Blanchard, Paris, 1955.
4. R. A. Mollin, Proof of some conjectures by Kaplansky; to appear in *C. R. Math. Rep. Acad. Sci. Canada.*
5. P. G. Walsh, *The Pell Equation and Powerful Numbers*, Master's Thesis, University of Calgary, 1988.

Department of Mathematics, University of Ottawa, 585 King Edward St., Ottawa, Ontario, Canada K1N-6N5
gwalsh@mathstat.uottawa.ca

A Theorem of Touchard on the Form of Odd Perfect Numbers

Judy A. Holdener

A natural number is said to be *perfect* if it is equal to twice the sum of its divisors. That is, n is perfect if and only if

$$\sigma(n) = \sum_{d|n} d = 2n.$$

Mathematicians have been studying such numbers for well over two millennia, yet the mystery surrounding their properties and their existence remains insurmountable. Are there infinitely many perfect numbers? Are there infinitely many even perfect numbers? Are there *any* odd perfect numbers? All of these questions have stood the test of time and remain open. To date, only thirty-nine perfect numbers are known to exist. (See http://www.mersenne.org/status.htm.) All of them are even and most of them were found following the discovery of a new Mersenne prime (any prime of the form $2^p - 1$, where p is itself necessarily prime) using Euclid's characterization of even perfect numbers. Euclid proved that, if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect. Conversely, Euler proved that every even perfect number must be of the form $2^{p-1}(2^p - 1)$ with $2^p - 1$ prime [**1**].