A CONTINUED FRACTIONS APPROACH TO A RESULT OF FEIT

JOHN P. ROBERTSON AND KEITH R. MATTHEWS

1. INTRODUCTION. For primes that can be written as a sum of integer squares, $p = a^2 + (2b)^2$, Kaplansky [4] asked whether the binary quadratic form $F = x^2 - py^2$ always represents a and $4b$ (that is, are there integer solutions to $x^2 - py^2 = a$ and $x^2 - py^2 = 4b$). Feit [1] and Mollin [4] proved that F does always represent a and $4b$ using the theory of ideals and the class group structure of quadratic orders. In this MONTHLY, Walsh [7] proved a more general result using only elementary methods. He showed that if $D > 1$ is a non-square odd integer, $D = a^2 + (2b)^2$, and $x^2 - Dy^2$ represents -1, then there is a factorization of D into positive integers r and s so that $rx^2 - sy^2$ represents a, and a possibly different factorization so that $rx^2 - sy^2$ represents $4b$.

For any non-square positive integer D, odd or even, for which $x^2 - Dy^2$ represents -1, we use the continued fraction algorithm to generate particular a and b so that $D = a^2 + b^2$, where a is always odd and the parity of b is opposite that of D. We also give *explicit* solutions to $x^2 - Dy^2 = \pm a$ and $x^2 - Dy^2 = \pm 2b$. This shows that standard continued fraction methods give a more elementary answer to Kaplansky's question than the solutions by Feit and Mollin. While this solution is not as elementary as Walsh's, it always uses the trivial factorization of D. We begin with some background.

2. THE CONTINUED FRACTION ALGORITHM. Any irrational real number ξ can be written as an infinite (simple) continued fraction

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

where $a_0 = \lfloor \xi \rfloor$ (with $\lfloor * \rfloor$ denoting the greatest integer function) and the a_i are positive integers for $i > 0$. For D a positive integer, not a square, the following well-known algorithm computes the continued fraction expansion of $\sqrt{D}$ [6, p. 76] [5, p. 358] [3, p. 251] and some related variables. Let $P_0 = 0$, $Q_0 = 1$, and $a_0 = \lfloor\sqrt{D}\rfloor$. For $i \geq 1$, define

(A) $P_i = a_{i-1}Q_{i-1} - P_{i-1}$,
(B) $Q_i = (D - P_i^2)/Q_{i-1}$, and
(C) $a_i = \lfloor(P_i + \sqrt{D})/Q_i\rfloor$.

Also set $A_{-2} = 0$, $A_{-1} = 1$, $A_i = a_iA_{i-1} + A_{i-2}$ for $i \geq 0$, $B_{-2} = 1$, $B_{-1} = 0$, and $B_i = a_iB_{i-1} + B_{i-2}$ for $i \geq 0$. The a_i are the *partial quotients*, the ratios $(P_i + \sqrt{D})/Q_i$ are the *complete quotients*, and the A_i/B_i are the *convergents* related to the continued fraction expansion of $\sqrt{D}$.

The sequences $\{P_i\}$, $\{Q_i\}$, and $\{a_i\}$ are periodic; denote the length of the minimal period by ℓ. For the continued fraction expansion of $\sqrt{D}$, for $i, k > 0$, $P_{i+k\ell} = P_i$ and similarly for $\{Q_i\}$ and $\{a_i\}$. As an example, in Table 1 we give the continued fraction expansion of $\sqrt{58}$, which has $\ell = 7$.

i	-2	-1	0	1	2	3	4	5	6	7	8
P_i			0	7	2	4	3	4	2	7	7
Q_i			1	9	6	7	7	6	9	1	9
a_i			7	1	1	1	1	1	1	14	1
A_i	0	1	7	8	15	23	38	61	99	1447	1546
B_i	1	0	1	1	2	3	5	8	13	190	203

TABLE 1. Continued fraction expansion of $\sqrt{58}$

We will need the following facts:

(i) $x^2 - Dy^2$ represents -1 if and only ℓ is odd [6, p. 93] [5, p. 353] [3, p. 249].
(ii) $A_{i-1}B_i - A_iB_{i-1} = (-1)^i$ for $i \geq 0$ [6, p. 14] [5, p. 330] [3, p. 225]. In particular, $\gcd(A_i, A_{i-1}) = 1$.
(iii) $A_{i-1}^2 - DB_{i-1}^2 = (-1)^iQ_i$ for $i \geq 0$ [6, p. 92] [5, p. 351] [3, p. 246].
(iv) $Q_i = Q_{\ell-i}$ for $0 \leq i \leq \ell$ [6, p. 81] [3, p. 253].
(v) $P_{i+1}B_i = A_i - Q_{i+1}B_{i-1}$ for $i \geq -1$ [6, p. 70].
(vi) $Q_{i+2} = Q_i - a_{i+1}(P_{i+2} - P_{i+1})$ for $i \geq 0$ [6, p. 70] [5, p. 358].
(vii) $DB_{i-1} = A_{i-1}P_i + A_{i-2}Q_i$ for $i \geq 0$ [6, p. 94].

3. EXPLICIT REPRESENTATIONS. In what follows, D is a positive integer, not a square, $x^2 - Dy^2$ represents -1 (so by (i) ℓ is odd), and $n = (\ell + 1)/2$. We prove the claims made in the second paragraph of the Introduction for $a = Q_n$ and $b = P_n$. The following lemma establishes representations of $\pm Q_n$.

Lemma 1.

$$A_{n-1}^2 - DB_{n-1}^2 = (-1)^n Q_n, \tag{1}$$

$$A_{n-2}^2 - DB_{n-2}^2 = (-1)^{n-1} Q_n, \tag{2}$$

and $\gcd(A_{n-1}, B_{n-1}) = \gcd(A_{n-2}, B_{n-2}) = 1$.

Proof. Equation (1) is an immediate consequence of (iii). Equation (2) follows from (iii) with $i = n-1$ and (iv) which gives $Q_{n-1} = Q_n$. By (ii), $\gcd(A_{n-1}, B_{n-1}) = \gcd(A_{n-2}, B_{n-2}) = 1$. ■

The next theorem shows that D is the sum of the squares of the claimed a and b.

Theorem 1. *$D = Q_n^2 + P_n^2$, where Q_n is odd and* $\gcd(P_n, Q_n) = 1$.

Proof. That $D = Q_n^2 + P_n^2$ is well known [6, p. 83], but the proof is short, so we include it: by (B) $D - P_n^2 = Q_n Q_{n-1}$, by (iv) $Q_n = Q_{n-1}$, and the result follows.

Next we show that two consecutive Q_i cannot both be even. Using (A) we substitute $Q_{i+1}a_{i+1} - P_{i+1}$ for P_{i+2} in (vi) to get

$$Q_i = Q_{i+1}a_{i+1}^2 + Q_{i+2} - 2P_{i+1}a_{i+1}.$$

If Q_{i+1} and Q_{i+2} were both even, Q_i would also be even, and continuing this, all Q_j with $0 \le j \le i+2$ would be even. But $Q_0 = 1$ is odd. It follows that $Q_n = Q_{n-1}$ is odd.

Because $D = Q_n^2 + P_n^2$, if $g = \gcd(Q_n, P_n)$, then g^2 divides D. By (1) and (2) g then divides A_{n-1}^2 and A_{n-2}^2, so by (ii), $g = 1$. ■

Now we can establish a theorem that gives surprisingly simple explicit representations of $\pm 2b$.

Theorem 2. *If $(T_1, U_1) = (A_{n-1} - A_{n-2}, B_{n-1} - B_{n-2})$, then*

$$T_1^2 - DU_1^2 = (-1)^n 2P_n. \tag{3}$$

Similarly if $(T_2, U_2) = (A_{n-1} + A_{n-2}, B_{n-1} + B_{n-2})$, then

$$T_2^2 - DU_2^2 = (-1)^{n-1} 2P_n. \tag{4}$$

Finally, $\gcd(T_1, U_1) = \gcd(T_2, U_2) = 1$.

Proof.

$$\begin{aligned} T_1^2 - DU_1^2 &= (A_{n-1} - A_{n-2})^2 - D(B_{n-1} - B_{n-2})^2 \\ &= (A_{n-1}^2 - DB_{n-1}^2) + (A_{n-2}^2 - DB_{n-2}^2) \\ &\quad - 2A_{n-1}A_{n-2} + 2DB_{n-1}B_{n-2} \\ &= -2A_{n-1}A_{n-2} + 2DB_{n-1}B_{n-2} \text{ by (1) and (2).} \end{aligned} \tag{5}$$

We now use (vii) with $i = n$ to substitute $DB_{n-1} = A_{n-1}P_n + A_{n-2}Q_n$ into (5) and get:

$$\begin{aligned}
T_1^2 - DU_1^2 &= 2(-A_{n-1}A_{n-2} + B_{n-2}(A_{n-1}P_n + A_{n-2}Q_n)) \\
&= 2(B_{n-2}A_{n-1}P_n + A_{n-2}(-A_{n-1} + Q_nB_{n-2})) \\
&= 2(B_{n-2}A_{n-1}P_n + A_{n-2}(-P_nB_{n-1})) \text{ by (v)} \\
&= 2(B_{n-2}A_{n-1} - A_{n-2}B_{n-1})P_n \\
&= 2(-1)^nP_n \text{ by (ii).}
\end{aligned}$$

There is a similar proof for (4), or alternatively one can use

$$(T_2 + U_2\sqrt{D}) = (T_1 + U_1\sqrt{D})(Q_n + \sqrt{D})/P_n$$

and take norms of both sides.

Finally, let $g = \gcd(T_1, U_1) = \gcd(A_{n-1} - A_{n-2}, B_{n-1} - B_{n-2})$. Then

$$A_{n-2} \equiv A_{n-1} \pmod{g} \text{ and } B_{n-1} \equiv B_{n-2} \pmod{g},$$

so g divides $A_{n-2}B_{n-1} - A_{n-1}B_{n-2}$. By (ii):

$$A_{n-2}B_{n-1} - A_{n-1}B_{n-2} = (-1)^{n-1},$$

so g divides 1 and hence $g = 1$.

The proof that $\gcd(T_2, U_2) = 1$ is similar. ■

Examples for Lemma 1 and Theorems 1 and 2 can be drawn from Table 1, which gives the continued fraction expansion of $\sqrt{58}$. Here $\ell = 7$ and $n = 4$. Lemma 1 then says that $23^2 - 58 \cdot 3^2 = (-1)^4 \cdot 7$ and $15^2 - 58 \cdot 2^2 = (-1)^3 \cdot 7$, both of which can be verified by direct computation. Theorem 1 says that $58 = 7^2 + 3^2$. Equation (3) says that $(23 - 15)^2 - 58(3 - 2)^2 = (-1)^4 \cdot 2 \cdot 3$, or $8^2 - 58 \cdot 1^2 = 6$, and (4) says that $(23 + 15)^2 - 58(3 + 2)^2 = (-1)^3 \cdot 2 \cdot 3$, or $38^2 - 58 \cdot 5^2 = -6$.

For primes $p > 0$ it is well known that $x^2 - py^2$ represents -1 (and so the lemma and theorems above apply) if and only if $p = 2$ or $p \equiv 1 \pmod 4$ [5, p. 357]. The fifteen smallest composite D so that $x^2 - Dy^2$ represents -1 are $D = 10$, 26, 50, 58, 65, 74, 82, 85, 106, 122, 125, 130, 145, 170, and 185.

An apparently open problem is to characterize those D that are a sum of two relatively prime squares but $x^2 - Dy^2$ does not represent -1. Such D include 34, 146, 178, 194, 205, 221, 305, 377, 386, and 410. Grytczuk, Luca, and Wojtowicz [2] prove that $x^2 - Dy^2 = -1$ has a solution if and only if there is a primitive Pythagorean triple (A, B, C) and positive integers a, b so that $D = a^2 + b^2$ and $|aA - bB| = 1$. In this case, $x = |aB + bA|$ and $y = C$ give a solution.

References

[1] W. Feit, Some Diophantine equations of the form $x^2 - py^2 = z$, *Proc. Amer. Math. Soc.* **129** (2000) 623–625.
[2] A. Grytczuk, F. Luca, and M. Wojtowicz, The negative Pell equation and Pythagorean triples, *Proc. Japan Acad. Ser. A Math. Sci.* **76** (2000) 91–94.
[3] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998.
[4] R. A. Mollin, Proof of some conjectures by Kaplansky, *C. R. Math. Acad. Sci. Soc. R. Can.* **23** (2001) 60–64.
[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, New York, 1991.
[6] O. Perron, *Die Lehre von den Kettenbrüchen*, vol. 1, 3rd ed., Teubner, Stuttgart, 1954.
[7] P. G. Walsh, On a question of Kaplansky, this Monthly **109** (2002) 660–661.

Actuarial and Economic Services Division, National Council on Compensation Insurance, Boca Raton, FL 33487
E-mail address: jpr2718@aol.com

Department of Mathematics, University of Queensland, St. Lucia, Brisbane, QLD 4072, AUSTRALIA, and Centre for Mathematics and its Applications, Australian National University, Canberra, ACT 0200, AUSTRALIA
E-mail address: keithmatt@gmail.com