AN APPLICATION OF UNIMODULAR TRANSFORMATIONS

DMITRI THORO
San Jose State College, San Jose, California

1. INTRODUCTION

The purpose of this paper is to investigate the Diophantine equation

$$(1) \qquad f(x, y) = x^2 - xy - y^2 = A .$$

In particular, we will prove the following [1]

Theorem. Equation (1) has a solution in relatively prime integers x and y if and only if

(i) $A = 5^e A' \neq 0$, where $e = 0$ or 1 and

(ii) if p is a prime factor of A', then $p \equiv 1$ or $-1 \pmod{10}$.

An application to Fibonacci numbers may be found in [2].

2. TECHNIQUES

Our primary tool will be unimodular transformations

$$\begin{cases} x = \alpha X + \beta Y \\ y = \gamma X + \delta Y \end{cases}$$

with determinant $\alpha\delta - \beta\gamma = \pm 1$.

If we define the product of two transformations in the customary manner, it is a straightforward procedure to verify that the set of all unimodular transformations forms a non-abelian group. We shall make tacit use of this fact.

For convenience, let us designate the binary quadratic form

$$ax^2 + bxy + cy^2 \text{ by } [a, b, c] .$$

Note that the discriminant $b^2 - 4ac$ is invariant under a unimodular transformation (cf. analytic geometry: rotation of axes).

First we observe that

$$\text{(iii)} \quad \text{if } (\alpha, \gamma) = 1, \text{ then } f(\alpha, \gamma) \neq 0$$

since $(\alpha, \gamma) = 1$ implies α and γ are both odd or of opposite parity, hence $f(\alpha, \gamma)$ is odd;

$$\text{(iv)} \quad f(1, 0) = 1;$$

$$\text{(v)} \quad \text{if } f(\alpha, \gamma) = A, \text{ then } f(\gamma, -\alpha) = -A.$$

Thus in the following discussion we may, whenever it is convenient, assume $A > 2$.

3. THE PROOF: PART I

Suppose the Diophantine equation (1) has a solution in relatively prime integers α and γ : $f(\alpha, \gamma) = A$, $(\alpha, \gamma) = 1$. Since the g.c.d. of any two integers α and γ (not both zero) may be expressed as a linear combination of α and γ, there exist integers β and δ such that $\alpha\delta - \beta\gamma = 1$.

Applying the unimodular transformation whose coefficient matrix is

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

to $f(x, y) \equiv [1, -1, -1]$ yields a new binary quadratic form $[A, B, C]$. But the discriminants are invariant under this transformation; thus $B^2 - 4AC = 5$.

Putting it another way, $f(\alpha, \gamma) = A$, where $(\alpha, \gamma) = 1$ implies the congruence

$$(2) \qquad x^2 \equiv 5 \pmod{4A}$$

is solvable. However, this congruence has a solution if and only if conditions (i) and (ii) are satisfied. For any x, $x^2 \equiv 0$, 1, or 4 (mod 8). Therefore (2) has no solution if A is even. If $A = 25A'$, $x^2 \equiv 5$ (mod 100), whence $x = 5t$, which leads to the contradiction $5t^2 \equiv 1$ (mod 5).

To complete this discussion, the reader should use the quadratic reciprocity theorem (first proved by Gauss at the age of 18). In particular, we note that $x^2 \equiv 5 \pmod p$ has a solution if and only if $x^2 \equiv p \pmod 5$ has a solution.

4. THE PROOF: PART II

To establish the sufficiency of conditions (i) and (ii), we will show that there exist unimodular transformations $T_1, T_2, \ldots, T_k$, H, and L such that

$$[A_1, B_1, C_1] \xrightarrow{T_1} [A_2, B_2, C_2] \xrightarrow{T_2} [A_3, B_3, C_3] \xrightarrow{T_3} \cdots$$

$$\xrightarrow{T_k} [A_{k+1}, B_{k+1}, C_{k+1}] \xrightarrow{H} [A_{k+2}, B_{k+2}, C_{k+2}] \xrightarrow{L} [1, -1, -1]$$

where $A_1 = A$ (cf. (1)), $B_1 = B$ (a solution of the congruence (2)), $A_{k+1} = \pm 1$ is the first A_i numerically equal to unity, $|B_{k+2}| = 1$, and the C_i are determined by the invariance of the discriminant.

If T is the product of these transformations,

$$[A, B_1, C_1] \xrightarrow{T} [1, -1, -1] \quad \text{or} \quad [1, -1, -1] \xrightarrow{T^{-1}} [A, B_1, C_1]$$
$$\equiv F(x, y).$$

Thus if the coefficient matrix of T^{-1} is

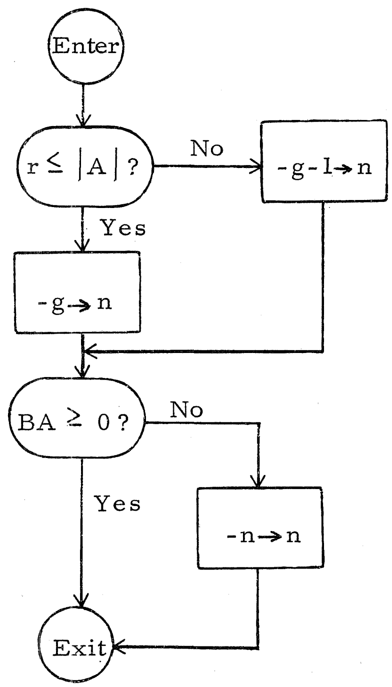
$$\begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} ,$$

$F(1, 0) = A$ implies $f(t_1, t_3) = A$. I.e., the desired solution of (1) is simply $x = t_1$, $y = t_3$. Moreover, since T^{-1} is unimodular, $t_1t_4 - t_3t_2 = \pm 1$ forces $(t_1, t_3) = 1$.

A Useful Lemma. Given any two integers B and $A \neq 0$, there exists an integer n such that

$$|B + 2nA| \leq |A| .$$

Proof. If we define $g = [|B|/2|A|]$ and $r = |B| - 2|A|g$, then the following flow chart exhibits n. (As usual "$s \rightarrow t$" means "replace s by t".)



We may now define the (matrices of the) required transformations. Let

$$T_i = \begin{pmatrix} n_i & 1 \\ -1 & 0 \end{pmatrix} ,$$

where n_i satisfies the inequality

$$|-B_i + 2n_iA_i| \leq |A_i| \quad .$$

Then it turns out that $B_{i+1} = -B_i + 2n_iA_i$, $A_{i+1} = (B_{i+1}^2 - 5)/4A_i$. As previously mentioned, $A_1 = A$ (given) and $B_1 = B$ (a solution of (2)). Note that B must be odd; hence all the B_i are odd. Similarly, all the A_i are odd.

Choose

$$H = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$$

so that h satisfies

$$|B_{k+1} + 2h\, A_{k+1}| \le |A_{k+1}| \ .$$

Then $B_{k+2} = B_{k+1} + 2h\, A_{k+1}$. Note that $B_{k+2} \ne 0$ (since B_{k+1} is odd); but $A_{k+1} = \pm 1$ (by definition), hence $|B_{k+2}| = 1$.

The reader may quickly establish the inequality

$$|A_{i+1}| < |A_i|/4, \quad i = 1, 2, \ldots, k \ .$$

Since the A_i can be shown to be odd, this establishes the existence of A_{k+1}.

Finally, L is chosen to be

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ or } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

according as the penultimate form is

$$[1, -1, -1], \quad [1, 1, -1], \quad [-1, 1, 1], \quad \text{or} \quad [-1, -1, 1],$$

respectively.

Thus we have established the existence of the transformations $T_1, T_2, \ldots, T_{k+1}$, H, L and hence the desired solution of (1).

5. REMARKS

We have, however, more than an existence proof. The procedures developed in Part II of the proof constitute an efficient algorithm. The algorithm was programmed in FORTRAN successfully. For $|A| \le 4^k$, no more than k+2 unimodular transformations are required to obtain a solution.

REFERENCES

1. D. E. Thoro, "A Diophantine Algorithm," (Abstract) Am. Math. Monthly, Vol. 71, No. 3, June-July 1964, pp. 716-717.

2. Brother U. Alfred, "On the Ordering of the Fibonacci Sequence," Fibonacci Quarterly, Vol. 1, No. 4, December 1963, pp. 43-46.

XXXXXXXXXXXXXXX