CONCERNING THE EUCLIDEAN ALGORITHM

R. P. KELISKY
IBM Watson Research Center, Yorktown Heights, New York

In most discussions of the integer solutions of the equation

$$(1) \qquad ax + by = 1, \quad (a, b) = 1,$$

reference is made to the fact that an integer solution of (1) may be obtained by using the Euclidean algorithm. With the restriction that $a > b > 1$ we shall show that in the x-y plane the solution of (1) obtained by the Euclidean algorithm is the lattice point on the line (1) which is nearest the origin. This is probably not a new result, but we cannot find a reference to it in the literature. Dickson [1, pp. 41-52] gives other algorithms for solving (1) for which it is known that the algorithm yields the lattice point on (1) which is nearest the origin.

Suppose $a > b$, $(a, b) = 1$, and $a \not\equiv 1 \pmod b$ and consider the Euclidean algorithm applied to the integers a and b. One obtains the well-known sequence of equations:

$$\begin{aligned}
a &= b\, q_1 + r_1, & 1 < r_1 < b \\
b &= r_1 q_2 + r_2, & 1 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, & 1 < r_3 < r_2 \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, & 1 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n
\end{aligned}$$

with $r_n = 1$. The requirement that $a \not\equiv 1 \pmod b$ is equivalent to $r_1 > 1$, and hence the Euclidean algorithm will require at least a second step. Hence $n \geqq 2$ and $r_{n-1} \geqq 2$.

To obtain a solution of (1) one then derives the following sequence of equations in which, for notational convenience, $a = r_{-1}$ and $b = r_0$:

$$1 = r_n = r_{n-2} - q_n r_{n-1}$$

$$= -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2}$$

$$\vdots$$

(3) $$= P_i r_{n-i-1} + Q_i r_{n-i}$$

$$\vdots$$

$$= P_n r_{-1} + Q_n r_0 \ .$$

The P_i and Q_i are polynomials in the q_i and the solution (P_n, Q_n) will be called the Euclidean algorithm solution of (1). It is determined uniquely by the algorithm described by the equations (2) and (3).

Lemma 1: $|P_n| < \frac{1}{2} b$ and $|Q_n| < \frac{1}{2} a$.

Proof: We first prove by induction

(4) $$|P_i| \leqq \frac{1}{2} r_{n-i}$$

and

(5) $$|Q_i| < \frac{1}{2} r_{n-i-1} \quad \text{for} \quad i = 1, \ldots, n,$$

with equality possible in (4) only if $i = 1$. We have

$$1 = P_i r_{n-i-1} + Q_i r_{n-i} ,$$

and since

$$r_{n-i-2} = r_{n-i-1} q_{n-i} + r_{n-i}$$

it follows that

$$1 = Q_i r_{n-i-2} + (P_i - q_{n-i} Q_i) r_{n-i-1}$$

and we have the recurrence relations

(6) $$P_{i+1} = Q_i$$

and

(7) $$Q_{i+1} = P_i - q_{n-i}Q_i$$

with $P_1 = 1$ and $Q_1 = -q_n$. To prove that $|P_1| = 1 \leqq \frac{1}{2} r_{n-1}$ recall that $r_{n-1} \geqq 2$. Similarly,

$$|Q_1| = q_n = \left[\frac{r_{n-2}}{r_{n-1}}\right] < \frac{r_{n-2}}{r_{n-1}} < \frac{1}{2} r_{n-2} ,$$

From (6) it follows that $|P_2| < \frac{1}{2} r_{n-2}$, and from (7) $|Q_2| < \frac{1}{2} r_{n-3}$ since

$$\begin{aligned} |Q_2| = |P_1 - q_{n-1}Q_1| &\leqq |P_1| + q_{n-1} |Q_1| \\ &< \frac{1}{2} r_{n-1} + q_{n-1} \cdot \frac{1}{2} \cdot r_{n-2} \\ &= \frac{1}{2} r_{n-3} . \end{aligned}$$

Now suppose that

$$|P_k| < \frac{1}{2} r_{n-k} \quad \text{and} \quad |Q_k| < \frac{1}{2} r_{n-k-1}$$

for $k = 2, \ldots, i$. Then from (6)

$$|P_{k+1}| = |Q_k| < \frac{1}{2} r_{n-k-1} ,$$

and

$$\begin{aligned} |Q_{k+1}| = |P_k - q_{n-k}Q_k| &\leqq |P_k| + q_{n-k} |Q_k| \\ &< \frac{1}{2} r_{n-k} + q_{n-k} (\frac{1}{2} r_{n-k-1}) \\ &= \frac{1}{2} r_{n-k-2} . \end{aligned}$$

This completes the induction. Since $r_{-1} = a$ and $r_0 = b$, we have proved the lemma if we take $i = n$ in (4) and (5).

It seems intuitively clear that there cannot be two lattice points on (1) which are equidistant from the origin if $a \neq b$. The proof of this is straightforward but for completeness we give it here.

Lemma 2: If $a > b > 0$ and $(a, b) = 1$, there do not exist two distinct lattice points on $ax + by = 1$ which are equidistant from the origin.

Proof: Suppose (α, β) and (ξ, η) are distinct lattice points on the given line which are equidistant from the origin. Then

$$\alpha^2 + \beta^2 = \xi^2 + \eta^2 \tag{8}$$

and $a\alpha + b\beta = a\xi + b\eta = 1$. We solve for β in terms of α, η in terms of ξ, and substitute these in (8) to obtain

$$(\alpha^2 - \xi^2)b^2 = 2a(\alpha - \xi) - a^2(\alpha^2 - \xi^2). \tag{9}$$

Since $\alpha \neq \xi$ by hypothesis,

$$(\alpha + \xi)b^2 = 2a - a^2(\alpha + \xi). \tag{10}$$

But this implies that $a \mid (\alpha + \xi)$ since $(a, b) = 1$, and also that $(\alpha + \xi) \mid 2a$. Hence, $\alpha + \xi = \pm a$, or $\alpha + \xi = \pm 2a$. If $\alpha + \xi = \pm a$, then (10) implies the Diophantine equation $a^2 + b^2 = \pm 2$ which is impossible if $a \neq b$. If $\alpha + \xi = \pm 2a$, then $a^2 + b^2 = \pm 1$. Clearly there is no solution to this equation such that $a > b > 0$ and $(a, b) = 1$.

It is well known that if (x_0, y_0) is any lattice point on (1) then all of the lattice points on (1) are given by the equations

$$x = x_0 - bt$$

$$y = y_0 + at$$

where t runs over the set of all integers. We can now prove our

Theorem. If $a > b > 1$ and $(a, b) = 1$ then the Euclidean algorithm solution of (1) is the lattice point on (1) which is nearest the origin.

Proof. First suppose that $a \not\equiv 1 \pmod b$. Denote the Euclidean algorithm solution of (1) by (P_n, Q_n). Clearly the set, S, of positive integers $(P_n - bt)^2 + (Q_n + at)^2$ has a smallest member. If $P_n^2 + Q_n^2$ is not the smallest number in S then there exists an integer $t \neq 0$ such that

$$P_n^2 + Q_n^2 > (P_n - bt)^2 + (Q_n + at)^2$$

or

$$0 < (a^2 + b^2)\ |t| < 2|P_n b - Q_n a|.$$

But from the lemma we have

$$0 < (a^2+b^2)\ |t| \leqq 2(|P_n|\ b + |Q_n| a) < a^2 + b^2.$$

This is impossible; hence $t = 0$ and (P_n, Q_n) is the smallest number in S.

The only remaining case is if $a \equiv 1 \pmod b$ and $a > b > 1$. Here the Euclidean algorithm is complete in one step and $P_1 = 1$ and $Q_1 = -q_1 = -(a-1)/b$. The expression $S(t) = (P_1 - bt)^2 + (Q_1 + at)^2$ can be rewritten

$$c\left[t - \frac{c-a}{bc}\right]^2 + \frac{1}{b^2}$$

where $c = a^2 + b^2$. Now $S(t)$ is a minimum for $t=t^*=(c-a)/bc$, but $b > 1$ and $c > a$ imply that $c(b-1) + a > 0$, or $0 < t^* < 1$. Therefore, the integer t for which $S(t)$ is a minimum is either 0 or 1. It is easy to show that $S(1) > S(0)$ if $(c-a)/bc < 1/2$. But

$$\frac{c-a}{bc} < \frac{1}{b} \text{ and } b \geqq 1;$$

hence (P_1, Q_1) is the point on $ax + by = 1$ which is nearest the origin. This completes the proof of the theorem.

It is an easy consequence of this theorem that if a and b are consecutive Fibonacci numbers, $a > b > 1$, then the lattice point P on the line $ax + by = 1$ which is nearest the origin has Fibonacci coordinates. In fact, if $a = F_{m+1}$, then P is $(F_{n-1}, -F_n)$ where n is the greatest even integer not exceeding m. This follows readily from the identity

$$F_{m+1} F_{n-1} - F_m F_n = (-1)^n F_{m-n+1}.$$

REFERENCES

1. Dickson, L. E., "History of the Theory of Numbers," Vol. 2, Chelsea, New York (1952).

xxxxxxxxxxxxxx