J. Austral. Math. Soc. (*Series A*) **37** (1984), 39–44

PAIRWISE RELATIVELY PRIME SOLUTIONS OF LINEAR DIOPHANTINE EQUATIONS

R. T. WORLEY

(Received 20 September 1982, revised 21 October 1982)

Communicated by J. H. Loxton

Abstract

It is shown that if $a_1, \ldots, a_m$ are relatively prime integers then for every integer n the equation

$$a_1x_1 + a_2x_2 + \cdots + a_mx_m = n$$

has infinitely many solutions in pairwise relatively prime integers $x_1, \ldots, x_m$.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 10 B 05.

In a recent paper [4] it was shown by an elementary method (a simple sieve using the Moebius function) that if the greatest common divisor $(a, b) = 1$ then the diophantine equation

$$ax + by = n \tag{1}$$

has solutions with $(x, y) = 1$ and $x > y > 0$ provided n is sufficiently large. With little modification the proof shows that for all n, (1) has solutions with $(x, y) = 1$.

More recently, B. H. Neumann asked for an elementary proof that if $(a, b, c) = 1$ then for all integers n

$$ax + by + cz = n$$

has solutions with $(x, y) = (x, z) = (y, z) = 1$, being dissatisfied with the fact that his proof used the infinitude of primes in arithmetical progressions. Since the result appears simple, it would be expected to be in the literature. However I have been unable to find the result mentioned in the obvious places (Dickson [1], LeVeque [3]). It seems that the need for relatively prime solutions has not arisen before.

https://doi.org/10.1017/S144678870002173X Published online by Cambridge University Press

In this note we show by elementary methods:

THEOREM. *If* $(a_1, a_2, \ldots, a_m) = 1$ *then for all integers n the equations*

(2a) $$a_1x_1 + a_2x_2 + \cdots + a_mx_m = n,$$

(2b) $$(x_i, x_j) = 1, \qquad 1 \leqslant i < j \leqslant m,$$

have infinitely many solutions.

This result includes Neumann's case as $m = 3$. The proof is by induction on m, the difficult case being a stronger version of the case $m = 2$.

LEMMA 1. *If* $(a_1, a_2) = 1$, *z is odd and* $(z, n) = 1$ *then for all integers n the equations*

(3a) $$a_1x_1 + a_2x_2 = n,$$

(3a) $$(x_1, x_2) = (x_1, z) = (x_2, z) = 1$$

have infinitely many solutions.

PROOF. Since $(a_1, a_2) = 1$ there is a solution $x_1 = u_0$, $x_2 = v_0$ of (3a). This generates a family

$$x_1 = u_l = u_0 + la_2, \qquad x_2 = v_l = v_0 - la_1, \qquad l \in \mathbf{Z},$$

of solutions of (3a). The aim of the proof is to show that if r is sufficiently large then $x_1 = u_l$, $x_2 = v_l$ satisfies (3b) for some l, $0 \leqslant l \leqslant r$. This is equivalent to showing that N_r is arbitrarily large for sufficiently large r, where

$$N_r = \sum_{0 \leqslant l \leqslant r} \Big(\sum_{d_1 | \nu_l \sigma_l \rho_l} \mu(d_1) \Big)$$

with $\nu_l = (u_l, v_l)$, $\sigma_l = (u_l, z)$, $\rho_l = (v_l, z)$ and μ denoting the Moebius function.

Since $x_1 = u_l$, $x_2 = v_l$ satisfy (3a), and $(z, n) = 1$, it is clear that ν_l, σ_l and ρ_l are pairwise relatively prime, so any divisor d_1 of $\nu_l\sigma_l\rho_l$ can be written uniquely as $d_1 = def$ where $d \mid \nu_l$, $e \mid \sigma_l$ and $f \mid \rho_l$. Thus

$$N_r = \sum_{0 \leqslant l \leqslant r} \sum_{d | \nu_l} \mu(d) \sum_{e | \sigma_l} \mu(e) \sum_{f | \rho_l} \mu(f)$$

which we rearrange as

(4) $$N_r = \sum_{d | n} \mu(d) \Bigg\{ \sum_{\substack{0 \leqslant l \leqslant r \\ d | \nu_l}} \sum_{e | \sigma_l} \mu(e) \sum_{f | \rho_l} \mu(f) \Bigg\}$$

since any divisor of ν_l must divide n. To continue with the proof we need the following result.

LEMMA 2. *With the above notation, the l for which $d \mid \nu_l$ form precisely one congruence class* mod d, *when $d \mid n$.*

PROOF. Plainly if $d \mid \nu_{l_1}$ then $d \mid \nu_l$ for all $l \equiv l_1 \bmod d$. Conversely $d \mid \nu_{l_1}$, $d \mid \nu_{l_2}$ implies d divides $u_{l_1} - u_{l_2} = a_2(l_1 - l_2)$ and d divides $a_1(l_1 - l_2)$. Since $(a_1, a_2) = 1$ it follows that $l_1 \equiv l_2 \bmod d$. It just remains to show that $d \mid \nu_l$ for some l.

Consider the equation $a_1 u_k + a_2 v_k = n$, that is,

$$a_1(u_0 + a_2 k) + a_2(v_0 - a_1 k) = n$$

and let $d \mid n$. Set $\delta = (a_2, d)$: then $(\delta, a_1) = 1$, $\delta \mid a_2$ and $\delta \mid d \mid n = a_1 u_0 + a_2 v_0$. Hence $\delta \mid u_0$, from which it follows that there exists an integer k with $a_2 k \equiv -u_0 \bmod d$. In other words, $a_1 u_k + a_2 v_k = n$ with $d \mid u_k$. Let $d^* = d\delta^{-1}$. Then $u_{k+td^*} = u_k + a_2 t d^* = u_k + a_2^* t d$ where $a_2^* = a_2 \delta^{-1}$, so $d \mid u_{k+td^*}$ for all integers t. On the other hand, $d \mid a_2 v_k = n - a_1 u_k$ means $d^* \mid v_k$. Since $(a_1, \delta) = 1$ there is an integer t such that

$$a_1 t \equiv v_k / d^* \mod \delta.$$

Then $d = d^*\delta$ divides $v_k - a_1 t d^* = v_{k+td^*}$, and so $d \mid \nu_l$ for $l = k + td^*$.

PROOF OF LEMMA 1 (continued). We re-write the inner sum of (4) as

$$\sum_{\substack{0 \leq l \leq r \\ l \equiv l_1 \bmod d}} \sum_{e \mid \sigma_l} \mu(e) \sum_{f \mid \rho_l} \mu(f)$$

and rearrange it as

$$\sum_{e \mid z} \mu(e) \left\{ \sum_{\substack{0 \leq l \leq r \\ l \equiv l_1 \bmod d \\ e \mid u_l}} \sum_{f \mid \rho_l} \mu(f) \right\} \tag{6}$$

where l_1 has the property that $d \mid \nu_{l_1}$. If $e \mid z$ has the property that $(e, a_2) \neq 1$, choose a prime $p \mid (e, a_2)$. Then $p \mid e \mid u_l$, $p \mid a_2$, $a_1 u_l + a_2 v_l = n$ would mean $p \mid (z, n) = 1$, a contradiction. Hence if $(e, a_2) \neq 1$ then the inner sum in (6) is empty as there will be no l for which $e \mid u_l$. We can therefore write the sum in (6) as

$$\sum_{\substack{e \mid z \\ (e, a_2) = 1}} \mu(e) \left\{ \sum_{\substack{0 \leq l \leq r \\ l \equiv l_1 \bmod d \\ e \mid u_l}} \sum_{f \mid \rho_l} \mu(f) \right\}. \tag{7}$$

https://doi.org/10.1017/S144678870002173X Published online by Cambridge University Press

For $l \equiv l_1 \bmod d$, we write

$$u_l = u_{l_1} + kda_2, \qquad k \in \mathbf{Z}.$$

Since $(d, e) \mid (n, z) = 1$ and $(e, a_2) = 1$ it is clear that $e \mid u_l$ for k lying in a unique congruence class mod e; that is, l lying in a unique congruence class mod de. We can therefore write the inner sum in (7) as

$$\sum_{\substack{0 \leq l \leq r \\ l \equiv l_2 \bmod de}} \sum_{f \mid \rho_l} \mu(f)$$

where $e \mid \sigma_{l_2}$ and $d \mid \nu_{l_2}$.

We rearrange this sum as

$$\sum_{f \mid z} \mu(f) \Bigg\{ \sum_{\substack{0 \leq l \leq r \\ l \equiv l_2 \bmod de \\ f \mid v_l}} 1 \Bigg\}. \tag{8}$$

If $f \mid z$ has the property that $(f, a_1) \neq 1$, choose a prime $p \mid (f, a_1)$. Then $p \mid f \mid v_l$, $p \mid a_1$, $a_1 u_l + a_2 v_l = n$ would mean that $p \mid (z, n) = 1$, which is impossible. Thus if $f \mid z$ the inner sum in (8) is empty unless $(f, a_1) = 1$, so we can write (8) as

$$\sum_{\substack{f \mid z \\ (f, a_1) = 1}} \mu(f) \Bigg\{ \sum_{\substack{0 \leq l \leq r \\ l \equiv l_2 \bmod de \\ f \mid v_l}} 1 \Bigg\}. \tag{9}$$

For $l \equiv l_2 \bmod de$ we write

$$v_l = v_{l_2} - k\, dea_1, \qquad k \in \mathbf{Z},$$

If $f \mid z$, $(f, a_1) = 1$ and $(f, e) \neq 1$ then f cannot divide v_l for any l, as $(\rho_l, \sigma_l) = 1$. However if $(f, e) = 1$ then $(de, f) = 1$ and $f \mid v_l$ for k lying in a unique congruence class mod f. We can therefore write (9) as

$$\sum_{\substack{f \mid z \\ (f, a_1 e) = 1}} \sum_{\substack{0 \leq l \leq r \\ l \equiv l_3 \bmod def}} 1 = \sum_{\substack{f \mid z \\ (f, a_1 e) = 1}} \mu(f) \left(\frac{r}{def} + O(1) \right).$$

Let z_e denote the greatest divisor of z prime to e. The above expression becomes

$$\frac{r}{de} \sum_{f \mid z_{a_1 e}} \frac{\mu(f)}{f} + O(\tau(z_{a_1})) = \frac{r}{de} \frac{\phi(z_{a_1 e})}{z_{a_1 e}} + O(\tau(z))$$

where $\tau(n)$ denotes the number of divisors of n and ϕ is the Euler function. Substituting in (7) we obtain the estimate

$$\sum_{e \mid z_{a_2}} \frac{r}{d} \frac{\mu(e)}{e} \frac{\phi(z_{a_1 e})}{z_{a_1 e}} + O\left(\tau(z) \sum_{e \mid z_{a_2}} \mu(e)\right) = \frac{r}{d} \frac{\phi(z^+)}{z^+} \frac{\phi^*(z^-)}{z^-} + O(\tau^2(z))$$

where z^+ denotes the product of primes dividing one but not both z_{a_1} and z_{a_2}, z^- denotes the product of primes dividing both z_{a_1} and z_{a_2}, and $\phi^*(z)/z = \prod_{p \mid z}(1 - 2p^{-1})$.

Finally we obtain the estimate

$$N_r = r\frac{\phi(n)}{n} \frac{\phi(z^+)}{z^+} \frac{\phi^*(z^-)}{z^-} + O(\tau^2(z)\tau(n))$$

which is arbitrarily large for sufficiently large r.

REMARK 1. Note that $\phi^*(z^-)/z^-$ is zero if $2 \mid z^-$. This occurs only when z is even and both a_1, a_2 are odd, so the conclusion of Lemma 1 is valid when z is even, provided $a_1 a_2$ is even.

REMARK 2. J. Loxton has observed that Lemma 1 could be proved using congruences and the Chinese Remainder Theorem. The above proof has the advantage of giving the estimate for N_r, and covering the case z even, $a_1 a_2$ even.

PROOF OF THE THEOREM. The case $m = 1$ is vacuous (or trivial, depending on your viewpoint). For $m \geqslant 2$ it is convenient to prove a slightly stronger result, namely.

PROPOSITION. *If* $(a_1, \ldots, a_m) = 1$, *and* $a_1, \ldots, a_m$ *are ordered so that if* $i \leqslant j$ *then* a_j *is not divisible by a higher power of* 2 *than* a_i, *then, for all integers* n, *the equations* (2a), (2b) *have infinitely many solutions in which* $x_1, \ldots, x_{m-1}$ *are odd.*

PROOF. The proof is by induction on m. For $m = 2$ we consider cases, noting that a_2 must be odd.

(i) If n is even, apply Lemma 1 with $z = 1$. x_1 must be odd for if x_1 were even then x_2 would have to be odd, so $a_1 x_1 = n - a_2 x_2$ is odd, an impossiblity.

(ii) If n is odd and a_1 is even, apply Lemma 1 with $z = 2$ (note Remark 1).

(iii) If n, a_1 and a_2 are all odd then $(a_1, 2a_2) = 1$ so by Lemma 1 with $z = 1$ there exist x_1, x_2 satisfying $a_1 x_1 + 2a_2 x_2 = n$, $(x_1, x_2) = 1$. In this case x_1 is plainly odd, and $x_1' = x_1$, $x_2' = 2x_2$ satisfy $a_1 x_1' + a_2 x_2' = n$, $(x_1', x_2') = 1$. This proves the proposition when $m = 2$.

https://doi.org/10.1017/S144678870002173X Published online by Cambridge University Press

Now suppose the proposition is true for $m-1$. Let $g=(a_1, a_m)$, which is odd and satisfies $(g, a_2, \ldots, a_{m-1})=1$. By the inductive assumption there exist solutions $x_2, \ldots, x_{m-1}, q$ of

$$\begin{gathered} a_2x_2+\cdots+a_{m-1}x_{m-1}+gq=n, \\ (x_2\cdots x_{m-1}, q)=1, \qquad (x_i, x_j)=1, \qquad 2\leqslant i<j\leqslant m-1, \\ x_2\cdots x_{m-1} \text{ odd}. \end{gathered} \tag{10}$$

Now (2a) is satisfied by any solution of $a_1x_1+a_mx_m=gq$, that is, $a_1'x_1+a_m'x_m=q$ where $a_1'=a_1/g$, $a_m'=a_m/g$. By Lemma 1, since $z=x_2\cdots x_{m-1}$ is odd and prime to q, there are infinitely many solutions of this satisfying x_1 odd and $(x_1, x_m)=(x_1, x_2\cdots x_{m-1})=(x_m, x_2\cdots x_{m-1})=1$. Thus $x_1, \ldots, x_m$ satisfy (2a), (2b) and $x_1, \ldots, x_{m-1}$ are odd. This completes the proof by induction.

Remark 3. For any odd integer z with $(z, n)=1$ the above proof can easily be modified to ensure the solutions $x_1, \ldots, x_m$ are also prime to z. If z is even and $(z, n)=1$, let $z=2^rz_1$ with z_1 odd. The solutions $x_1, \ldots, x_m$ prime to z_1 also have $x_1, \ldots, x_{m-1}$ odd, so they are prime to z. Plainly x_m can (and will) be odd, and therefore prime to z, if $a_1+\cdots+a_{m-1}$ is even.

References

[1] L. E. Dickson, *History of the theory of numbers* (Chelsea, 1952).

[2] B. H. Neumann, *Some finite groups with few defining relations*, ANU Mathematics Research Report 40 (Australian National University, 1982).

[3] W. J. LeVeque, *Reviews in number theory* (Amer. Math. Soc., Providence, R.I., 1974).

[4] R. T. Worley, 'Denominator sequences for continued fractions III', *J. Austral. Math. Soc. Ser. A* **26** (1978), 53–56.

Department of Mathematics
Monash University
Clayton, Victoria 3168
Australia