LINEAR DIOPHANTINE EQUATIONS WITH NON-NEGATIVE PARAMETERS AND SOLUTIONS

THOMAS M. GREEN
Contra Costa College, San Pablo, California

1. INTRODUCTION

Solving equations, where we are required to find only the integral solutions, has some historical interest. These equations are known as Diophantine equations, after Diophantus of Alexandria, the first to treat these problems in an algebraic manner.

There are innumerable problems that result in first degree equations with two unknowns, where it is required to find integral solutions. Such an equation is called a linear Diophantine equation and is written as

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

It is usually stipulated that the parameters, a, b and n, are also integers. However, if these parameters are rational numbers, (1) can be easily transformed so that each parameter becomes integral.

Equation (1) is indeterminant in that there is an unlimited number of solutions, and if we did not require integral solutions, the problem of finding a solution would be simple. If, however, we restrict the solutions to be integral, the problem of finding these solutions is no longer simple, and in fact there may be no solution. Yet, if a solution does exist, the total number of solutions is still unlimited.

The problem warrants more attention by the added restriction that the solutions be non-negative pairs. If this restriction is imposed upon the parameters as well, then if a solution exists, the number of solutions is finite. The problem of finding these solutions and determining the number of such solutions has occupied much attention throughout the history of number theory [1, Chap. II].

The purpose of this paper is to give an explicit formula for the general solution of (1) and to establish the relationship that exists between the parameters when no solution exists.

(Received December 1966)

2. PRELIMINARY REMARKS

Before developing the relationships above some remarks pertaining to historical developments, topical concepts, and the existence of solutions are in order.

Euler proved that Eq. (1) is solvable in integers when $(a, b) = 1$, i.e., they are relatively prime [1, p. 47], and Gauss proved that the equivalent of (1) is solvable in integers if and only if $(a, b) | n$ [1, p. 54]. In view of these results and the general conditions imposed on (1), i.e., the solutions and parameters are to be non-negative integers, there is no loss of generality by assuming $(a, b) = 1$.

If (x_1, y_1) is a solution of (1) in integers and $(a, b) = 1$, then all other solutions will be given by

$$\begin{aligned} x &= x_1 + bj \\ y &= y_1 - aj \end{aligned} \tag{2}$$

where j is an integer [2, p. 29].

It is for this first solution that we seek an explicit formula. This can be accomplished easily with the Fermat-Euler Theorem applied to the congruence $ax \equiv n \pmod{b}$. Such a result has advantages over other methods of solution, such as, algorithms involving a succession of recursive steps. The Fermat-Euler Theorem involves the concept of Euler's function, denoted $\phi(b)$, which is equal to the number of natural numbers less than b that are coprime with b. An explicit formula for this value is given by

$$\phi(b) = b \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right), \tag{3}$$

where $p_1, p_2, \cdots, p_r$ are the different prime factors of the natural number b [2, p. 24]. The statement of the Fermat-Euler Theorem then becomes [3, p. 63]

$$a^{\phi(b)} \equiv 1 \pmod{b} \tag{4}$$

Assuming that a, b and n are non-negative and $(a,b) = 1$, then if either a or b equals 0 or 1, then the determination of the solution of (1) becomes a simple case. Hence, in what follows we assume that both a and b are greater than 1. This implies that $a \neq b$, since if $a = b$, then $(a,b) = (a,a) = a$, but $(a,b) = 1$, hence $a = b = 1$, a contradiction.

As a final remark we might consider the graphical representation of this problem. Under the imposed restrictions, the graph of equation (1) is confined to the first quadrant. We note that (1) with non-negative parameters represents the family of all line segments whose endpoints are the rational points of the x and y axes. Thus, the line segment determined by the endpoints

$$\left(\frac{p}{q}, 0\right) \quad \text{and} \quad \left(0, \frac{r}{s}\right)$$

has the equation

$$rqx + spy = pr.$$

This is a form of (1) where $rq = a$ and $sp = b$, and $pr = n$. Now we are ready to examine the general solution.

3. THE SOLUTION

The explicit formula involves the concept of the principal remainder modulo m, for which we may use the following notation:

DFN. (PRINCIPAL REMAINDER):

$$[\![\, y \pmod m \,]\!] = x \quad \text{iff} \quad x \equiv y \pmod m \quad \text{and} \quad 0 \leq x \leq m - 1 \tag{5}$$

The following lemma, that is easily verified, though not essential to the derivation of the explicit formula, makes the solution of a specific example feasible.

Lemma.

$$\left[\!\left[\prod_{i=1}^{n} y_i \pmod m \right]\!\right] \equiv \prod_{i=1}^{n} [\![y_i \pmod m]\!] \pmod m \quad . \tag{6}$$

As a special consequence of this lemma we may note that,

$$[\![y^n \pmod m]\!] \equiv [\![y \pmod m]\!]^n \pmod m \quad . \tag{7}$$

Since the number of solutions of (1) will be finite, the method of solution will be to find the minimum positive integral value of x (or y), and then to find the corresponding value of y (or x) which will necessarily be maximum and then to subtract multiples of a (or b) to obtain the set of all possible non-negative solutions of (1). The following formula for the minimum value of x is essentially due to Bouniakowski, and independently, Cauchy [1, pp. 55-56].

Theorem. If the equation, $ax + by = n$, has non-negative parameters, a, b, and n, and $a \geq 1$ and $b \geq 1$, and $(a, b) = 1$, then when non-negative integral solutions exist, the minimum non-negative integral value of x, which satisfies the equation such that y is also a non-negative integer, is given by

$$X_{min} = [\![na^{\phi(b)-1} \pmod b]\!] \quad . \tag{8}$$

Proof. The remarks made in Sec. 2 claim that there is no essential loss of generality by assuming the above conditions. It is important to note that we must assume a value of n such that non-negative solutions do exist. There does exist a finite number of values of n, for a given a and b, such that the equation will not have the non-negative solutions that we are seeking. This is proved in the next section. Formula (8) is independent of this consideration, therefore, we could obtain an erroneous value of X_{min} if used without circumspection, however, we would soon be aware of the error when the attempt to solve for the corresponding value of y was made.

The equation $ax + by = n$ is equivalent to the congruence

$$ax \equiv n \pmod b \quad . \tag{9}$$

Now by the Fermat-Euler Theorem if we multiply both sides of (9) by $a^{\phi(b)-1}$, we obtain

$$x \equiv n \cdot a^{\phi(b)-1} \pmod{b} \quad , \tag{10}$$

whereby, the least value of x is the principal remainder,

$$X_{min} = [\![\, n \cdot a^{\phi(b)-1} \pmod{b}]\!] \qquad \text{Q. E. D.} \tag{11}$$

Using the same principals we may derive a formula for X_{max}.

$$X_{max} = \left[\frac{n}{a}\right] - \left[\!\!\left[-[\![n \pmod{a}]\!] \cdot a^{\phi(b)-1} \pmod{b} \right]\!\!\right] \quad , \tag{12}$$

where $[\ ]$ denotes the greatest integer function.

Proof. Equation (1) is equivalent to the congruence,

$$by \equiv n \pmod{a} \quad . \tag{13}$$

Now if $m = [\![n \pmod{a}]\!]$, then $b \cdot y \equiv m \pmod{a}$. Therefore,

$$by \in \{ m, \ m + a, \ m + 2a, \cdots, m + ka \} \quad . \tag{14}$$

where $k = [n/a]$. We note that $m + ka = n$, hence, this is the maximum value that $b \cdot y$ can achieve. By substituting these values of $b \cdot y$ into (1) we obtain the corresponding values of x, that is,

$$x \in \{ k, \ k - 1, \ k - 2, \cdots, k - k \} \quad , \tag{15}$$

in that order. Therefore, there is an integral solution of (1) when

$$y = \frac{ja + m}{b}$$

is an integer, where $0 \leq j \leq k$. This situation is equivalent to the congruence

$$ja + m \equiv 0 \pmod{b} \quad . \tag{16}$$

The corresponding value of x is

$$x = k - j \quad . \tag{17}$$

Now since $(a, b) = 1$, we can solve (16) for j by using (4), the Fermat-Euler Theorem. This gives

$$j \equiv -ma^{\phi(b)-1} \pmod{b} \quad . \tag{18}$$

Now that j has been found, we can find x from (17). Since k represents the maximum value that x can be, we will have the maximum integral value of x that satisfies (1) by subtracting the least value of j from k as represented in (17). That least value of j is the principal remainder, $[\![j \pmod{b}]\!]$. By substituting for k, j, and m in (17), we arrive at (12). Q. E. D.

Corollary. If a non-negative integral solution of (1) exists and $(a, b) = 1$, then there are at least

$$\left[\frac{n}{ab}\right]$$

and at most

$$\left[\frac{n}{ab}\right] + 1$$

solutions.

Proof. We note that (13) has just one solution such that $0 \leq y < a$ [3, p. 51]. Therefore, from (14) we also note that there are at least $[k/b]$ and at most $[k/b] + 1$ solutions. Also, since $k = [n/a]$, the corollary is proved.

4. THE NON-EXISTENCE OF SOLUTIONS

Even when a and b are relatively prime, in deference to Sec. 2, there will be cases when (1) has no solutions, due to the restriction that they be non-

negative. Naturally, we would wish to know just what cases have no solutions, therefore, it is necessary to state the following.

Theorem. The equation $ax + by = n$, where a, b, and n are non-negative integers and $ab \neq 0$ and $(a,b) = 1$, will not have integral solutions ≥ 0 when $n = ab - (ja + kb)$, where $j,k = 1, 2, 3, \cdots$.

Proof. Assume (1) has a non-negative integral solution and that $n = ab - (ja + kb)$ for some j and k. Then

$$ax + by = ab - ja - kb \tag{19}$$

$$a(x + j) + b(y + k) = ab \tag{20}$$

Let $X = x + j$ and $Y = y + k$; then,

$$aX + bY = ab. \tag{21}$$

It is important to note that X, Y, a, and b are all greater than or equal to one. From (21) we obtain

$$b = X + \frac{bY}{a} \quad \text{or} \quad b - X = \frac{bY}{a} \ . \tag{22}$$

Now $b \equiv X$ is an integer, therefore a divides Y, since a and b are relatively prime. Suppose $Y/a = r$, then $b - X = br$, but this is impossible since all the quantities are positive integers, therefore, there is a contradiction. Q. E. D.

It was proved by E. Lucas [1, p. 68] that there are $\frac{1}{2}(a - 1)(b - 1)$ such values of n which afford no solutions. He also gave a method to determine if a given case was solvable, but it involved long computations.

5. AN EXAMPLE

Find all the non-negative integral solutions of $20x + 14y = 410$. $(20, 14) = 2$, therefore, by dividing through by 2 we have the parameters 10, 7, and 205. Now since $205 \geq 10 \cdot 7$ and $(10,7) = 1$ we can solve for X_{min}.

$$X_{min} = [\![n \cdot a^{\phi(b)-1} \bmod b)]\!]$$
$$= [\![205 \cdot 10^{\phi(7)-1} (\bmod 7)]\!]$$
$$= [\![205 \cdot 10^{5} (\bmod 7)]\!]$$

By using the Lemma, this simplifies to

$$X_{min} = [\![2 \cdot 3^{5} \ (\bmod 7)]\!]$$
$$= [\![2 \cdot 3 \cdot 9 \cdot 9 \ (\bmod 7)]\!]$$
$$= [\![2 \cdot 3 \cdot 2 \cdot 2 \ (\bmod 7)]\!]$$
$$= [\![3 \ (\bmod 7)]\!]$$
$$= 3 \ .$$

By substituting X_{min} into the original equation we obtain Y_{max}.

$$10 \cdot 3 + 7y = 205$$
$$y = 25$$

Now subtract multiples of a, (10). In this case $y \in \{25, 15, 5\}$. The corresponding values of x are found by adding multiples of b, (7). In this case $x \in \{3, 10, 17\}$. The three pairs of non-negative integral solutions of the original equation are (3, 25), (10, 15) and (17, 5).

REFERENCES

1. L. Dickson, History of the Theory of Numbers, Vol. 2, Chelsea, New York, 1952.
2. T. Nagell, Introduction to Number Theory, Wiley and Sons, New York, 1951.
3. G. Hardy and E. Wright, An Introduction to the Theory of Numbers, Oxford University Press, London, 1954.

★ ★ ★ ★ ★