2897. On the Equation ax - by = 1

Author(s): R. L. Goodstein

Source: *The Mathematical Gazette*, Vol. 44, No. 348 (May, 1960), pp. 132-134
Published by: The Mathematical Association
Stable URL: https://www.jstor.org/stable/3612572
Accessed: 19-11-2020 13:29 UTC

2897. On the equation $ax - by = 1$

The object of this note is to describe a method of solving the diophantine equation

$$ax - by = 1$$

which is independent of Euclid's algorithm, and continued fractions, and could be used by young children. I start with an application of the method to the numerical example:

$$5x - 11y = 1;$$

we consider the permutation

$$t \to t + 5 \pmod{11}$$

which is conveniently expressed by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 6 & 7 & 8 & 9 & 10 & 11 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

(in which we note that " 5 " is entered beneath " 11 " and the rest is then filled in mechanically). From this permutation we select the cycle which begins with 5 in the first row and ends with 1 in the second, viz.

$$5,\ 10,\ 4,\ 9,\ 3,\ 8,\ 2,\ 7,\ 1.$$

This cycle contains 9 terms, and $x = 9$ is a solution of the equation $5x - 11y = 1$; the corresponding value of y is given by the number of times a term in the cycle is followed by a smaller number, which in this case is 4 (of course $y = (5 \times 9 - 1)/11$ simply). To find a solution of

$$5x - 11y = 3$$

we consider the same permutation and select the cycle which ends with 3, namely

$$5,\ 10,\ 4,\ 9,\ 3$$

which contains 5 terms, and 2 decreases, so that

$$x = 5,\ y = 2 \text{ is a solution.}$$

As another example I consider the equation

$$7x - 5y = 1$$

in which the coefficient of x is now the larger of the two coefficients; this time we use the permutation

$$a \to a - 5 \pmod{7}$$

from which we select the cycle

$$7,\ 2,\ 4,\ 6,\ 1;$$

this cycle contains *five* terms, one more than the value of y, and the terms increase *twice*, once less than the value of x. Of course this second case can always be brought under the first, by writing it in the form

$$2x - 5(y - x) = 1;$$

the cycle now is 2, 4, 1 giving x the value 3, and $y - x$ the value 1, so that $y = 4$.

We consider now the general equation

$$ax - by = c$$

with each two of a, b, c relatively prime and $a > b > c$. The permutation

$$t \to t + a \pmod{b}$$

gives rise to the cycle

$$a, 2a, 3a, \ldots, c$$

provided that there is a natural number k such that $ka \equiv c \pmod{b}$; the b numbers $a, 2a, 3a, \ldots, (b-1)a, ba$ on division by b leave the remainders $0, 1, 2, \ldots, b-1$ in some order, for if ra and sa, $1 \leqslant r < s \leqslant b$, left the same remainder on division by b then $(s-r)a$ would be divisible by b, which is impossible, since a and b have no common factor and $s - r < b$, so that $s - r$ is not divisible by b. Thus there is a value of k between 1 and $b-1$ (inclusive) such that $ka = c$. This value of k gives the number of terms in the cycle

$$a, 2a, \ldots, ka \equiv c \pmod{b},$$

and since by hypothesis $ka - c$ is divisible by b, there is a number l such that

$$ka - c = lb$$

i.e.

$$ka - lb = c$$

showing that $x = k$, $y = l$ is a solution of the equation

$$ax - by = c.$$

It remains to show that l is the number of times a term in the cycle

$$a, 2a, \ldots, c \pmod{b}$$

is followed by a smaller number. Now a term t in the cycle is followed by the larger number $t + a$ if $t + a \leqslant b$ and is followed by a smaller number if $t + a > b$; each term in the cycle has the form $pa - qb$ and the last term is

$$ka - lb = c$$

so that l counts the number of times b has been subtracted, i.e. the number of times a term has decreased. A similar argument applies when $a > b$. To ensure that this treatment of the equation $ax - by = c$ really is independent of Euclid's algorithm, we must check that no step in the proof contains a concealed application of the algorithm. In fact the critical step in the proof which consists in showing that a prime number which divides a product da and does not divide a, necessarily divides d, is generally proved by an application of the algorithm to establish the uniqueness of prime factorisation, but

there are proofs (of the theorem that if p divides da and p does not divide a then p divides d) which do not use the algorithm; a very simple one is given by Davenport in his splendid *Introduction to the Higher Arithmetic* (in the Hutchinson series).

The result may also be obtained very simply as follows. If there is a prime number which divides some product uv without dividing either of the factors u, v, let p be the smallest such prime and let ab be the smallest product which p divides without dividing either of the factors. Necessarily a and b are less than p for if $a>p$ then $(a-p)b$ is a smaller product divisible by p and such that neither of the factors $a-p$, b is divisible by p. Since ab is divisible by p, there is q such that

$$ab=pq$$

Let f be a prime factor of a, then $f<p$ and f divides pq so that f divides q (for p is prime); let a', q' be the quotients when a, q are divided by f, so that

$$fa'b=fpq'$$

and therefore

$$a'b=pq';$$

thus $a'b$ is a smaller product divisible by p and such that neither of the factors a', b is divisible by p. This contradiction proves that there is no prime which divides a product without dividing one of the factors.

By comparison with the standard method of solution of a diophantine equation, finding a cycle of the appropriate permutation may be absurdly long and tiresome. For instance, in the case of the equation

$$79x-101y=1$$

the cycle we require contains 78 terms, whereas, using the algorithm, we obtain the sequence 101, 79, 22, 13, 9, 4, 1, 3, 7, 10, 17, 61, 78 of only 13 terms (and do not in fact need to count the number of terms).

The existence of the cycle ending in unity, furnishes a simpler proof of the existence of a solution, but it must be observed that the existence of a cycle in turn rests upon the existence of a solution of the congruence $az\equiv 1 \pmod{b}$ and the existence of a solution of this congruence provides a direct proof of the existence of the solution $x=z$ of the equation

$$ax-by=1$$

In solving diophantine equations on a digital computer, however, using a permutation leads to a simpler programme than using Euclid's algorithm.

R. L. GOODSTEIN