

A NEW FORMULA TO FIND THE SOLUTIONS OF THE LINEAR DIOPHANTINE EQUATION

Issam H. Kaddoura

Baghdad University, College of Science, Department of Mathematics, Jadiriya, Baghdad, Iraq
 issamhkaddoura@yahoo.com

(Received 24 August 2005 - Accepted 3 February 2006)

ABSTRACT

It is well-known that there are algorithms to solve the Diophantine equation $ax + by = 1$ such as Euclid's algorithm and continued fractions.

In this article we obtain a new formula that gives the complete solutions explicitly in terms of arbitrary parameters.

Keywords: Euler's function, Euclid's algorithm, Linear Diophantine equation

Now, if a and b are integers such that $n > 0$ and $\gcd(a,b)=1$, we have the following well-known theorem obtained by Euler:

$$(a)^{\varphi(n)} \equiv 1 \pmod{n} \text{ where } \varphi \text{ is the Euler's function.}$$

And there is another theorem obtained by Carmichael:

$(a)^{\lambda(n)} \equiv 1 \pmod{n}$ where λ is Carmichael's function (John, 1995; Tattersal, 2005; Yan, 2000).

We will now prove the following theorem:

Theorem 1 : If a and b are integers such that $\gcd(a,b) = 1$, then all the solutions of the linear Diophantine equation $ax + by = 1$ are given parametrically by:

$$X = \frac{nb(a)^{\varphi(ma+nb)-1} + m}{ma+nb} - tb \tag{1}$$

$$Y = \frac{n[1 - (a)^{\varphi(ma+nb)}]}{ma+nb} + ta$$

where m, n, t are arbitrary integers such that $ma + nb > 0$ and $\gcd(ma+nb,a)=1$.

Proof: to prove this, we note that $\gcd(ma + nb, a) = 1$ and $ma + nb > 0$ gives $(a)^{\varphi(ma+nb)} \equiv 1 \pmod{ma+nb}$ by Euler's theorem, but $nb \equiv -ma \pmod{ma+nb}$, we deduce that

$$nb(a)^{\varphi(ma+nb)-1} + m \equiv 0 \pmod{ma+nb}$$

this shows that x is an integer and similarly for y .

It's clear that x and y satisfy the Diophantine equation. This completes the proof of Theorem 1.

Also, we can write a dual form of the solutions x and y in theorem 1 by interchanging a and b , and replacing x by y :

$$\begin{aligned} x &= \frac{n \left[1 - (b)^{\varphi(mb+na)} \right]}{mb+na} - tb \\ y &= \frac{n a (b)^{\varphi(mb+na)-1} + m}{mb+na} + ta \end{aligned} \tag{2}$$

where m, n, t are arbitrary integers such that $mb+na > 0$ and $\gcd(mb+na, b) = 1$.

Moreover, it is evident that we can use Carmichael's function instead of Euler's function in theorem 1 to give the solutions of the linear Diophantine equation explicitly.

Now, we are in a position to solve the linear congruence $ax \equiv b \pmod{n}$ using Theorem 1.

It is well-known that the congruence $ax \equiv b \pmod{n}$ where $\gcd(a, n) = 1$ has a solution $x = ba^{\varphi(n)-1}$ but when n is a large positive integer, it is very difficult to factorize n and using the formula $x = ba^{\varphi(n)-1}$ seems to be useless; so we can use our formula to modify the solution by a parametric one.

Theorem 2. : If a, b, n are integers such that $n > 0$ and $\gcd(a, n) = 1$, then the solution of the linear congruence $ax \equiv b \pmod{n}$ is given by :

$$X = \frac{\left[\text{sn}(a)^{\varphi(ta+sn)-1} + t \right] b}{ta+sn} \tag{3}$$

where t, s are arbitrary integers such that $ta+sn > 0$ and $\gcd(ta+sn, a) = 1$.

Proof : It is an immediate consequence of theorem 1.

Finally, we note that the formulas in theorem 1 and theorem 2 have great flexibility because the choice of arbitrary parameters generates solutions under control so, we can minimize the parametric integer $ma+nb$ as possible as we can by changing the values of m and n which simplify the computation of Euler's function $\varphi(ma+nb)$.

Example:

Solve the congruence $(567)^{100} x \equiv 1 \pmod{(567)^{100} - 23}$.

It is very difficult to factorize the integer $(567)^{100} - 23$ but we can use formula (3) to avoid that factorization *i.e.*, noticing that $\gcd[(567)^{100}, (567)^{100} - 23] = 1$, we can choose $s = -1$, $t = 1$ and $a = (567)^{100}$, $b = 1$, $n = (567)^{100} - 23$ are given.

Substitute in the formula to obtain the solution :

$$X = \frac{(23 - (567)^{100}) \left[(567)^{2100} + 1 \right]}{23}.$$

REFERENCES

- John, A.A. 1995. *Theory of numbers*. W.B. Saunders Co., Philadelphia PA, pp. 259. Reissued Dover, New York.
- Tattersal, J.J. 2005. *Elementary number theory*. Cambridge University Press, 2nd edition.
- Yan, S.Y. 2000. *Number theory for computing*. Springer-Verlag, Berlin, Heidelberg, pp. 42-47.