Abstract No: PS-37

A method of obtaining a solution of $a^{px+qy} \equiv b \pmod{m}$ when m is prime and a is a primitive root modulo m

P. A. S. D. Wijerathna*, P. G. R. S. Ranasinghe and S. S. M. A. C. Senavirathna

Department of Mathematics, Faculty of Science, University of Peradeniya, Sri Lanka
shashika.d.pdn@email.com*

The congruence relation modulo a positive integer identifies two integers if and only if their difference is divisible by that positive integer. The modern theory of congruences was developed by Gauss at the beginning of the 19th century. Several formulations are established in solving congruences of various types. In this study, we introduce a method in solving congruences of the form $a^{px+qy} \equiv b \pmod{m}$ for a prime number m and integers $a, b, p,$ and q. Since we do not have a standard generalized method of obtaining a solution for the aforementioned congruence type, some restricted forms of it were studied. In this work, we especially focus on the congruences of prime modulus m and a is a primitive root modulo m: If $\gcd(a, n) = 1$ and $\varphi(n)$ is the order of a modulo n, then a is called a *primitive root* of the integer n. Here $\varphi(n)$ is the Euler's Phi function (totient function) of n, that counts the number of integers less than or equal to n which are relatively prime to n. In or method, first, a solution system for $a^{px+qy} \equiv 1 \pmod{m}$ is obtained. That solution system is used with a transformation to obtain a solution of the congruence $a^{px+qy} \equiv b \pmod{m}$. We prove that a solution of $a^{px+qy} \equiv 1 \pmod{m}$ can be obtained by $(\pm k\varphi(m) + x_0, \pm l\varphi(m) + y_0)$, where k and l are non-negative integers. When (x_o, y_o) is a solution of $a^{px+qy} \equiv 1 \pmod{m}$ with both x_o, y_o are not simultaneously zero, the obtained solution is transformed to a solution of $a^{px+qy} \equiv b \pmod{m}$ when $\gcd(p, q) \mid b$. The former result can be used to obtain a solution for the congruence in the form of $a^{px+qy} \equiv b \pmod{m}$ when m is prime and a is a primitive root modulo m. In future, we hope to generalize this method when m is composite and a is not a primitive root modulo m.

Keywords: Congruence, Primitive root, Modular arithmetic, Modular exponentiation