Generalised Wilson's Theorem

1 Introduction

It is known that if p is a prime then,

$$(p-1)! \equiv -1(mod\ p) \tag{1}$$

This theorem was proposed by John Wilson and published by Waring in 1770, although it was previously known to Leibniz. It was proved by Lagrange in 1773.
In this paper, I prove the generalised version of Wilson's theorem.

2 Main Proof

Theorem 2.1. Let p be any prime and n be any natural number, then the following congruence holds

$$(np-1)! \equiv (-1)^n (n-1)! p^{n-1} (mod\ p^n).$$

Proof: Let us define a set S_n with $p-1$ elements,

$$S_n = \{(n-1)p+1, (n-1)p+2, (n-1)p+3, ..., np-1\}$$

Observe that,

$$(n-1)p+k \equiv k(mod\ p) \tag{2}$$

where $k = 1, 2, 3, ..., p-1$.
Substituting $k = 1, 2, 3, ..., p-1$ in (2) and multiplying all the congruences, we obtain,

$$\prod_{x \in S_n} x \equiv (1 \times 2 \times 3 \times ... \times (p-1)) \equiv (p-1)! \equiv -1(mod\ p)$$

Thus,

$$\prod_{x \in S_n} x \equiv -1(mod\ p) \tag{3}$$

Substituting $n = 1, 2, 3, ..., n-1, n$ in (3) and multiplying all the congruences, we obtain,

$$\prod_{n=1}^{n} \prod_{x \in S_n} x \equiv ((-1) \times (-1) \times (-1) \times ...(-1))(mod\ p)$$

$$\prod_{n=1}^{n} \prod_{x \in S_n} x \equiv (-1)^n (mod\ p) \tag{4}$$

Multiplying both sides of (4) with $(n-1)!p^{n-1}$ we have,

$$(n-1)!p^{n-1} \prod_{n=1}^{n} \prod_{x \in S_n} x \equiv (-1)^n (n-1)!p^{n-1} (mod\ p^n)$$

Finally,

$$(np-1)! \equiv (-1)^n (n-1)!p^{n-1} (mod\ p^n).$$

3 References

[1] R. Andrew Ohana, A Generalization of Wilsons Theorem, 2009.

[2] Miller, G. A. A New Proof of the Generalized Wilson's Theorem. Annals of Mathematics, vol. 4, no. 4, 1903, pp. 188-190.

Romanian Mathematical Magazine
Web: http://www.ssmrmh.ro

ANGAD SINGH
Department of Electronics and Telecommunications, Pune Institute of Computer Technology, Pune, India
email-id: angadsingh1729@gmail.com