General Wilson's Theorem & Primitive Roots

Masum Billal

March 4, 2013

Abstract

In this paper, we generalize *Wilson's theorem* in number theory along with some other theorems related to primitive root and orders. For this purpose, we denote the set of co-prime numbers less than or equal to n by $\mathbb{H}$, and let $g_1, g_2, \ldots, g_{\varphi(n)}$ be those $\varphi(n)$ numbers and T_n be the product of them. $ord_n(a)$ denotes the order of a modulo n i.e. the smallest positive integer such that

$$a^{ord_n(a)} \equiv 1 \pmod n$$

Moreover, for $d|\varphi(n)$, $H(d)$ denotes the number of positive integers a for which $ord_n(a) = d$ and $a \perp n$ means $\gcd(a, n) = 1$. For brevity, we assume $w = \varphi(n)$ and $P(A) = \prod_{a \in \mathbb{A}} a$ for a set A.

1. Generalization Of Wilson's Theorem

We already know that,

Theorem 1. *$2, 4, p^k, 2p^k$ are the only numbers having a primitive root, where p is an odd prime.*

Theorem 2. *If n has a primitive root, then*

$$a^{\frac{\varphi(n)}{2}} \equiv -1 \pmod n$$

for $a \perp n$.

Proof. We just need to consider $n = p^k$. $w = \varphi(p^k) = p^{k-1}(p-1)$.

$$a^w \equiv 1 \pmod{p^k}$$

Alternatively, we can write

$$p^k | a^w - 1 = \left(a^{\frac{w}{2}} + 1\right)\left(a^{\frac{w}{2}} - 1\right)$$

Since p is odd, it divides only one of $a^{\frac{w}{2}} + 1$ or $a^{\frac{w}{2}} - 1$, otherwise it would lead to $p | a^{\frac{w}{2}} + 1 - (a^{\frac{w}{2}} - 1) = 2$. Again, $p^k | a^{\frac{w}{2}} - 1$ can't hold for the smallest w. $\square$

Theorem 3 (Generalized Wilson's Theorem)**.**

$$T_n \equiv -1 \pmod{n}$$

for any n.

Proof. Let g be any primitive root of n. Then, $g_1, \ldots, g_w$ can be generated by g i.e. $g_1 \equiv g^i \pmod{n}$ for a unique i, which follows from the primitivity of n. Therefore, using theorem **??**,

$$\begin{aligned} g_1 \cdots g_w &\equiv g^1 \cdots g^w \pmod{n} \\ &\equiv g^{\frac{w(w+1)}{2}} \pmod{n} \\ &\equiv \left(g^{\frac{w}{2}}\right)^{w+1} \pmod{n} \\ &\equiv (-1)^{w+1} \pmod{n} \\ &\equiv -1 \pmod{n} \end{aligned}$$

□

Remark. We get Wilson's theorem if we set $n = p$ a prime.

A more general version of this theorem can be proven considering a quadratic non-residue $a \perp n$.

Theorem 4.

$$T_n \equiv \pm 1 \pmod{n}$$

with $T_n \equiv -1$ if n has a primitive root, and vice-versa.

Outline Of Proof. For each $g \in \mathbb{H}$ there is a unique $h \in \mathbb{H}$ so that $gh \equiv a \pmod{n}$. So we pair up them and get $\frac{w}{2}$ pairs. □

Theorem 5 (Converse Of The General Wilson)**.** *If $\mathbb{G} = \{a_1, ..., a_k\}$ such that*

$$P(G) \equiv \pm 1 \pmod{n}$$

then a_i must be co-prime to n and $k \leq w$.

Proof.

$$n | P(G) \pm 1$$

Let $g_i = \gcd(a_i, n)$. Then $g_i | a_i | a_1 \cdots a_k$. Also

$$g_i | n | a_1 \cdots a_k \pm 1$$

which implies $g_i | 1 \Rightarrow g_i = 1$. This assures that a_i must be relatively prime to n. And there can be at most w numbers less than or equal to n. Hence, $k \leq w$ must also hold. □

Theorem 6. *If $\mathbb{G} = \{a_1, ..., a_w\}$ are pairwise distinct positive integers less than or equal to n such that*

$$n | P(G) \pm 1$$

then $\{a_1, ..., a_w\}$ is a permutation of $\mathbb{H}$.

The proof follows from the theorem above.

2. Primitive Roots

Theorem 7. *If g is a primitive root of p such that $p^{\alpha}|g^{p-1}-1$ but $p^{\alpha+1} \not| g^{p-1}-1$, $g^{p^{k-\alpha}(p-1)}$ is a primitive root of p^k for $k \geq \alpha$.*

Proof. This actually needs nothing but the application of *Lifting The Exponent Lemma.* $\square$

Theorem 8. *If n has a primitive root, then*

$$\sum_{d|w} H(d) = w$$

Proof. Say, a has order d. Then $a^i; i = 1, ..., d-1$ has order $\frac{d}{\gcd(i, d)}$. We have $ord_n(a^i) = d$ if $d \perp i$ i.e. there are $\varphi(d)$ such numbers. Hence, $H(d) = \varphi(d)$. Since for any a, if $ord_n(a) = d, d|w$, for any $d|w$, the total number of primitive roots modulo n is $\sum_{d|w} H(d)$. $\square$

Theorem 9. *If n has a primitive root, then it has $\varphi(w)$ primitive roots.*

Proof. n has $H(w)$ primitive roots with order w. From the previous theorem's discussion, $H(w) = \varphi(w)$. $\square$

Theorem 10. *If $x^n \equiv a \pmod n$ with n having a primitive root, then a^k is a primitive $n-th$ root if $n \perp k$.*

Proof. Clearly $ord_n(a^k) = \frac{n}{\gcd(n, k)}$. Therefore, the theorem follows. $\square$

Theorem 11.

$$\left(g_1 \cdots g_{\frac{w}{2}}\right)^2 \equiv \pm 1 \pmod n$$

Proof. $\gcd(a, n) = 1 \Rightarrow \gcd(a, n-a) = 1$ implies $g_i = g_{w-i}$ if we consider $\mathbb{H}$ in a sorted manner. Then this is straight. $\square$

Corollary. Setting $n = p \equiv 1 \pmod 4$, a prime

$$\left(g_1 \cdots g_{\frac{w}{2}}\right)^2 \equiv -1 \pmod p$$

implies -1 is a quadratic residue of p. Because $\frac{p-1}{2}$ is even. As a result, we can infer *Fermat-Euler's 4n+1 theorem* from here.

Masum Billal
University Of Dhaka, Bangladesh
E-mail: billalmasum93@gmail.com