# ON A THEOREM OF WILSON

Florentin Smarandache, Ph D
Associate Professor
Chair of Department of Math & Sciences
University of New Mexico
200 College Road
Gallup, NM 87301, USA
E-mail:smarand@unm.edu

§1. In 1770 Wilson found the following result in the Number's Theory: "If $p$ is prime, then $(p-1)! \equiv (-1 \bmod p)$".

Did you ever question yourself what happens if the module $m$ is not anymore prime? It's simple, one answers, "if $m$ is not prime and $m \neq 4$ then $(m-1)! \equiv 0 (\bmod m)$"; for the proof see [4].

This is fine, I would continue, but if in the product from the left side of this congruence we consider only numbers that are prime with $m$?

For this reason we'll address this case, and provide a generalization of Wilson's theorem to any modulo, this will conduce to a nice result.

§2. Let $m$ be a whole number. We note $A = \{x \in \mathbf{Z},\ x$ is of the form $\pm p^n,\ \pm 2p^n,\ \pm 2^r$, or $0$, where $p$ is odd prime, $n \in \mathrm{N}$, and $r = 0,1,2\}$.

**Theorem*.** Let $c_1, c_2, ..., c_{\varphi(m)}$ a reduced system of residues modulo $m$. Then $c_1 c_2 \cdot \cdots c_{\varphi(m)} \equiv -1 (\bmod m)$ if $m \in A$, respectively $+1$ if $m \notin A$; where $\varphi$ is Euler's function.

To prove this we'll introduce some lemmas.

**Lemma 1.** $\varphi(m)$ is a multiple of 2.

**Lemma 2.** If $c^2 \equiv 1 (\bmod m)$ then $(m-c)^2 \equiv 1 (\bmod m)$ and $c(m-c) \equiv -1 (\bmod m)$, and $m - c \not\equiv c (\bmod m)$.

Indeed, if $m - c \equiv c (\bmod m)$, we obtain $2c \equiv 0 (\bmod m)$, that is $(c, m) \not\equiv 1$. This is absurd.

Therefore we proved that in any reduced system of residue modulo $m$ it exists an even number of elements $c$ with the property

$$P_1 : c^2 \equiv 1 (\bmod m).$$

If $c_{i_0}$ is part of the system, because $c_{i_0}, m \cong 1$, it results that also $c_1 c_{i_0}, c_2 c_{i_0}, ..., c_{\varphi(m)} c_{i_0}$ constitutes a reduced system of residues $m$. Because

$(1,m)\cong 1$ results that for any $c$ from $c_1,c_2,...,c_{\varphi(m)}$ it exist and it is unique $c'$ from $c_1,c_2,...,c_{\varphi(m)}$ such that

(1) $\quad cc'\equiv 1(\mathrm{mod}\, m)$

and reciprocally: for any $c'$ from $c_1,c_2,...,c_{\varphi(m)}$ it exists an unique $c$ such that

(2) $\quad c'c\equiv 1(\mathrm{mod}\, m)$.

By multiplying these two congruence for all the elements from the system and selecting one of them in the case in which $c\neq c'$ it results that $c_1,c_2,...,c_{\varphi(m)}\cdot b\equiv 1(\mathrm{mod}\, m)$, where $b$ represents the product of all elements $c$ for which $c=c'$, because in this case $c^2\equiv 1(\mathrm{mod}\, m)$. These elements which verify the property $P_1$ can be grouped in pairs as follows: $c$ with $m-c$, and then $c(m-c)\equiv -1(\mathrm{mod}\, m)$. Therefore

$$c_1,c_2,...,c_{\varphi(m)}\equiv \pm 1(\mathrm{mod}\, m),$$

depending of the number of distinct $c$ in the system that have the property $P_1$ is or not a multiple of 4.

If $m\in A$ the equation $x^2\equiv 1(\mathrm{mod}\, m)$ has two solutions (see [1], pp. 38-88), therefore we conclude that $c_1,c_2,...,c_{\varphi(m)}\equiv -1(\mathrm{mod}\, m)$.

This first part of the theorem could have been proved also using the following reasoning:

If $m\in A$ then it exist primitive roots modulo $m$ (see [1], pp. 65-68-72); let $d$ be such a root; then we could represent the system reduced to residues modulo $m$, $c_1,c_2,...,c_{\varphi(m)}$ as $d^1,d^2,...,d^{\varphi(m)}$ after rearranging, from were

$$c_1,c_2,...,c_{\varphi(m)}\equiv \left(d^{\frac{\varphi(m)}{2}}\right)^{1+\varphi(m} \equiv -1(\mathrm{mod}\, m),$$

because from $d^{\varphi(m}\equiv 1(\mathrm{mod}\, m)$ we have that

$$\left(d^{\frac{\varphi(m)}{2}}-1\right)\left(d^{\frac{\varphi(m)}{2}}+1\right)\equiv 0(\mathrm{mod}\, m)$$

therefore

$$d^{\frac{\varphi(m)}{2}}\equiv -1(\mathrm{mod}\, m);$$

contrary would have been implied that $d$ is not a primitive root modulo $m$.

For the second part of the proof we shall present some other lemmas.

**Lemma 3.** Let's consider the integer numbers nonzero, non-unitary $m_1$ and $m_2$ with $(m_1,m_2)\cong 1$. Then

(3) $\quad x^2\equiv 1(\mathrm{mod}\, m_1)$ admits the solution $x_1$

and

(4) $\quad x^2\equiv 1(\mathrm{mod}\, m_2)$ admits the solution $x_2$

if and only if

(5) $x^2 \equiv 1(\mathrm{mod}\, m_1 m_2)$ admits the solution

(5') $x_3 \equiv (x_2 - x_1) m_1^{'} m_1 + x_1 (\mathrm{mod}\, m_1 m_2)$,

where $m_1^{'}$ is the inverse of $m_1$ in rapport with modulo $m_2$.

*Proof.*

From (3) it results

$x = m_1 h + x_1$, $h \in \mathbf{Z}$,

and from (4) we find

$x = m_2 k + x_2$, $k \in \mathbf{Z}$.

Therefore

(6) $m_1 h - m_2 k = x_2 - x_1$

this Diophantine equation has integer solutions because

(7) $(m_1, m_2) \cong 1$

From (6) results $h \equiv \ x_2 - x_1 \ \ m_1^{'} (\mathrm{mod}\, m_2)$.

Therefore

$h \equiv \ x_2 - x_1 \ \ m_1^{'} + m_2 t, \ \ t \in \mathbf{Z}$

and

$x \equiv \ x_2 - x_1 \ \ m_1^{'} m_1 + x_1 + m_1 m_2 t$

or

$x \equiv (x_2 - x_1) m_1^{'} m_1 + x_1 \bmod(m_1 m_2)$.

(The rationale would have been analog if we would have determined $k$ by finding

$x \equiv (x_1 - x_2) m_2^{'} m_2 + x_2 \bmod(m_1 m_2)$,

but this solution is congruent modulo $m_1 m_2$ with the one found anterior; $m_2^{'}$ being the reciprocal of $m_2$ modulo $m_1$.)

**Reciprocal.** Immediately, results that

$x_3 \equiv x_1 (\mathrm{mod}\, m_1)$ and $x_3 \equiv x_2 (\mathrm{mod}\, m_2)$.

**Lemma 4.** Let $x_1, x_2, x_3$ be the solutions for congruencies (3), (4) respective (5) such that

$x_3 \equiv (x_2 - x_1) m_1^{'} m_1 + x_1 (\mathrm{mod}\, m_1 m_2)$

Analogue for $x_1^{'}, x_2^{'}, x_3^{'}$.

(O) Will consider from now on every time the classes of residue modulo $m$ that have represents in the system $0, 1, 2, ..., |m| - 1$ .

Then if $(x_1, x_2) \neq (x_1^{'}, x_2^{'})$ it results that $x_3 \not\equiv x_3^{'} (\mathrm{mod}\, m)$.

*Proof.* By absurd.

Let $x_1 \neq x_1^{'}$ (analogue it can be shown for $x_2 \neq x_2^{'}$).

From $x_3 \equiv x_3^{'} (\mathrm{mod}\, m_1 m_2)$ it would result that $x_3 \equiv x_3^{'} (\mathrm{mod}\, m_1)$,

that is

$(x_2 - x_1) m_1^{'} m_1 + x_1 \equiv (x_2^{'} - x_1^{'}) m_1^{'} m_1 + x_1^{'} (\mathrm{mod}\, m_1)$,

Thus

$$x_1 \equiv x_1^{'} (\mathrm{mod}\, m_1).$$

Since $x_1$ and $x_1^{'}$ are from $0,1,2,...,|m|-1$ it results that $x_1 = x_1^{'}$, which is absurd.

**Lemma 5.** The congruence $x^2 \equiv 1(\mathrm{mod}\, m)$ has an even number of distinct solutions**.**

This results from lemma 2.

**Lemma 6.** In the conditions of lemma 3 we have that the number of distinct solutions for congruence (5) is equal to the product between the number of congruencies' solutions (3) and (4). And, all solutions for congruence (5) are obtained from the solutions of congruencies (3) and (4) by applying formula (5').

Indeed, from lemmas 3, 4 we obtain the assertion.

**Lemma 7.** The congruence

(8) $x^2 \not\equiv 1(\mathrm{mod}\, 2^m)$, has only four distinct solutions:

$\pm 1,\ \pm(2^{n-1}-1)$ modulo $2^n$.

By direct verification it can be shown that these satisfy (8).

Using induction we will show that there don't exist others .

For $n = 3$ it verifies, by tries, analog for $n = 4$.

We consider the affirmation true for values $\le n-1$. Let's prove it for $n$.

We retain observation (O) and the following remark:

(9) if $x_0$ is solution for congruence (8) it will be solution also for congruence $x^2 \equiv 1 \mod 2^i$ , $3 \le i \le n-1$.

By absurdum let $a \not\equiv \pm 1,\ \pm(2^{n-1}-1)$ be a solution for (8). We will show that $(\exists) i \in \{3,4,...,n-1\}$ such that $a^2 \not\equiv 1(\mathrm{mod}\, 2^i)$.

We can consider $2^{\frac{n}{2}} < a < 2^n - 1$; because $a$ is solution for (8) if and only if $-a$ is solution for (8).

We consider the case $n = 2k,\ k \ge 2$, integer. (It will analogously be shown when $n$ is odd). Let $a = 2^k + r$, $1 \le r \le 2^{2k} - 2^k - 2$

(10) $a^2 = 2^{2k} + r \cdot 2^{k+1} + r^2 \equiv 1(\mathrm{mod}\, 2^n)$,

from here $r \ne 1$; it results that

$$r^2 \equiv 1(\mathrm{mod}\, 2^i),\ 3 \le i \le k+1$$

From the induction's hypothesis, for $k+1$ we find $r \equiv 2^k - 1(\mathrm{mod}\, 2^{k+1})$ and substituting in (10) we obtain:

$$-2^{k+2} \equiv 0(\mathrm{mod}\, 2^{2k}),$$

or $k \le 2$ thus $n = 4$, which is a contradiction.

Therefore, it results the lemma's validity.

**Lemma 8.** The congruence $x^2 \equiv 1(\mathrm{mod}\, m)$ has

$$\begin{cases} 2^{s-1}, & \text{if} \quad \alpha_1 = 0,1; \\ 2^{s}, & \text{if} \quad \alpha_1 = 2; \\ 2^{s+1}, & \text{if} \quad \alpha_1 \geq 3 \end{cases}$$

distinct solutions modulo $m = \varepsilon 2^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, where $\varepsilon = \pm 1$, $\alpha_j \in \mathrm{N}^*$, $j = 2,3,...,s$, and $p_j$ are odd prime, different numbers two by two.

Indeed, the congruence $x^2 \equiv 1 \left(\mathrm{mod}\, 2^{\alpha_1}\right)$ has

$$\begin{cases} 1, & \text{if} \quad \alpha_1 = 0,1; \\ 2, & \text{if} \quad \alpha_1 = 2; \\ 4, & \text{if} \quad \alpha_1 \geq 3 \end{cases}$$

distinct solutions, and congruence $x^2 \equiv 1 \bmod p_j^{\alpha_j}$, $2 \leq j \leq s$ have each two distinct solutions (see [1], pp. 85-88). From lemma 6 and 7 it results this lemma too.

*

With these lemmas, it results that the congruence $c^2 \equiv 1 \left(\mathrm{mod}\, m\right)$ with $m \in A$ admits a number of distinct solutions which is a multiple of 4. From where $c_1 c_2 \cdot \cdots c_{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, that completely resolves the generalization of Wilson's theorem.

The reader could generalize lemmas 2, 3, 4, 5, 6, 8 and utilize lemma 7 for the case in which we have the congruence $x^2 \equiv a \left(\mathrm{mod}\, m\right)$, with $\left(a, m\right) \cong 1$.

**REFERENCES**


[1] Francisco Bellot Rosada, Maria Victoria Deban Miguel, Felix Lopez Fernandez – Asenjo – "Olimpiada Matematica Española/Problemas propuestos en el distrito Universitario de Valladolid", Universidad de Valladolid, 1992.

[2] "Introducion a la teoria de numeros primos (Aspectos Algebraicos y Analiticos)", Felix Lopez Fernandez – Asenjo, Juan Tena Ayuso Universidad de Valladolid, 1990.