A NUMERICAL FUNCTION IN CONGRUENCE THEORY

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

In this article we define a function L which will allow us to generalize (separately or simultaneously) some theorems from Numbers Theory obtained by Wilson, Fermat, Euler, Gauss, Lagrange, Leibnitz, Moser, Sierpinski.

§1. Let A be the set $m \in \mathbf{Z} \big| m = \pm p^{\beta}, \ \pm 2p^{\beta}$ with p an odd prime, $\beta \in N^{*}$, or $m = \pm 2^{\alpha}$ with $\alpha = 0,1,2$, or $m = 0$.

Let's consider $m = \varepsilon p_1^{\alpha_1} ... p_s^{\alpha_s}$, with $\varepsilon = \pm 1$, all $\alpha_i \in N^{*}$, and $p_1,...,p_s$ distinct positive numbers.

We construct the FUNCTION $L : \mathbf{Z} \to \mathbf{Z}$,

$$L(x,m) = (x + c_1)...(x + c_{\varphi(m)})$$

where $c_1,...,c_{\varphi(m)}$ are all residues modulo m relatively prime to m, and φ is the Euler's function.

If all distinct primes which divide x and m simultaneously are $p_{i_1}...p_{i_r}$ then:

$$L(x,m) \equiv \pm 1 (\operatorname{mod} p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}}),$$

when $m \in A$ respective by $m \notin A$, and

$$L(x,m) \equiv 0 (\operatorname{mod} m / (p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}})).$$

Noting $d = p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}}$ and $m' = m / d$ we find:

$$L(x,m) \equiv \pm 1 + k_1^0 d \equiv k_2^0 m' (\operatorname{mod} m)$$

where k_1^0, k_2^0 constitute a particular integer solution of the Diophantine equation $k_2 m' - k_1 d = \pm 1$ (the signs are chosen in accordance with the affiliation of m to A).

This result generalizes the Gauss' theorem $(c_1,...,c_{\varphi(m)} \equiv \pm 1 (\operatorname{mod} m))$ when $m \in A$ respectively $m \notin A$ (see [1]) which generalized in its turn the Wilson's theorem (if p is prime then $(p-1)! \equiv -1 (\operatorname{mod} m)$).

Proof.

The following two lemmas are trivial:

Lemma 1. If $c_1,...,c_{\varphi(p^{\alpha})}$ are all residues modulo p^{α} relatively prime to p^{α}, with p an integer and $\alpha \in N^{*}$, then for $k \in \mathbf{Z}$ and $\beta \in N^{*}$ we have also that

$kp^{\beta} + c_1, ..., kp^{\beta} + c_{\varphi(p^{\alpha})}$ constitute all residues modulo p^{α} relatively prime to it is sufficient to prove that for $1 \le i \le \varphi(p^{\alpha})$ we have that $kp^{\beta} + c_i$ is relatively prime to p^{α}, but this is obvious.

Lemma 2. If $c_1, ..., c_{\varphi(m)}$ are all residues modulo m relatively prime to m, $p_i^{\alpha_i}$ divides m and $p_i^{\alpha_i+1}$ does not divide m, then $c_1, ..., c_{\varphi(m)}$ constitute $\varphi(m / p_i^{\alpha_i})$ systems of all residues modulo $p_i^{\alpha_i}$ relatively prime to $p_i^{\alpha_i}$.

Lemma 3. If $c_1, ..., c_{\varphi(m)}$ are all residues modulo q relatively prime to q and $(b, q) \square 1$ then $b + c_1, ..., b + c_{\varphi(q)}$ contain a representative of the class $\hat{0}$ modulo q.

Of course, because $(b, q - b) \square 1$ there will be a $c_{i_0} = q - b$ whence $b + c_i = \mathcal{M}_{q}$.

From this we have the following:

Theorem 1. If $x, m / \ p_{i_1}^{\alpha_{i_1}} ... p_{i_s}^{\alpha_{i_s}} \quad \square 1$,

then

$$(x + c_1)...(x + c_{\varphi(m)}) \equiv 0 \mod m / \ p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}} \quad .$$

Lemma 4. Because $c_1, ..., c_{\varphi(m)} \equiv \pm 1 (\mod m)$ it results that $c_1, ..., c_{\varphi(m)} \equiv \pm 1 (\mod p_i^{\alpha_i})$, for all i, when $m \in A$ respectively $m \notin A$.

Lemma 5. If p_i divides x and m simultaneously then:

$$(x + c_1)...(x + c_{\varphi(m)}) \equiv \pm 1 (\mod p_i^{\alpha_i}),$$

when $m \in A$ respectively $m \notin A$. Of course, from the lemmas 1 and 2, respectively 4 we have:

$$(x + c_1)...(x + c_{\varphi(m)}) \equiv c_1, ..., c_{\varphi(m)} \equiv \pm 1 (\mod p_i^{\alpha_i}).$$

From the lemma 5 we obtain the following:

Theorem 2. If $p_{i_1}, ..., p_{i_r}$ are all primes which divide x and m simultaneously then:

$$(x + c_1)...(x + c_{\varphi(m)}) \equiv \pm 1 (\mod p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}}),$$

when $m \in A$ respectively $m \notin A$.

From the theorems 1 and 2 it results:

$$L(x, m) \equiv \pm 1 + k_1 d = k_2 m',$$

where $k_1, k_2 \in \mathbf{Z}$. Because $(d, m') \square 1$ the Diophantine equation $k_2 m' - k_1 d = \pm 1$ admits integer solutions (the unknowns being k_1 and k_2). Hence $k_1 = m't + k_1^0$ and $k_2 = dt + k_2^0$, with $t \in \mathbf{Z}$, and k_1^0, k_2^0 constitute a particular integer solution of our equation. Thus:

$$L(x, m) \equiv \pm 1 + m' dt + k_1^0 d = \pm 1 + k_1^0 (\mod m)$$

or

$L(x,m)=k_2^0 m'(\mathrm{mod}\, m)$.

§2. APPLICATIONS

1) Lagrange extended Wilson's theorem in the following way: "If p is prime then

$$x^{p-1}-1\equiv(x+1)(x+2)...(x+p-1)(\mathrm{mod}\, p)\text{''}.$$

We shall extend this result as follows: whichever are $m\neq 0,\pm 4$, we have for $x^2+s^2\neq 0$ that

$$x^{\varphi(m_s)+s}-x^s\equiv(x+1)(x+2)...(x+|m|-1)(\mathrm{mod}\, m)$$

where m_s and s are obtained from the algorithm:

$$(0)\qquad \begin{cases} x=x_0d_0;\;\;(x_0,m_0)\square 1 \\ m=m_0d_0;\; d_0\neq 1 \end{cases}$$

$$(1)\qquad \begin{cases} d_0=d_0^1d_1;\;\;(d_0^1,m_1)\square 1 \\ m_0=m_1d_1;\; d_1\neq 1 \end{cases}$$

……………………………………..

$$(\text{s-1})\qquad \begin{cases} d_{s-2}=d_{s-2}^1d_{s-1};\;\;(d_{s-2}^1,m_{s-1})\square 1 \\ m_{s-2}=m_{s-1}d_{s-1};\; d_{s-1}\neq 1 \end{cases}$$

$$(\text{s})\qquad \begin{cases} d_{s-1}=d_{s-1}^1d_s;\;\;(d_{s-1}^1,m_s)\square 1 \\ m_{s-1}=m_sd_s;\;\; d_s\neq 1 \end{cases}$$

(see [3] or [4]). For m positive prime we have $m_s=m$, $s=0$, and $\varphi(m)=m-1$, that is Lagrange.

2) L. Moser enunciated the following theorem: If p is prime then $(p-1)!a^p+a=\mathbf{M}\, p$", and Sierpinski (see [2], p. 57): if p is prime then $a^p+(p-1)!a=\mathbf{M}\, p$" which merge the Wilson's and Fermat's theorems in a single one.

The function L and the algorithm from §2 will help us to generalize that if "a" and m are integers $m\neq 0$ and $c_1,...,c_{\varphi(m)}$ are all residues modulo m relatively prime to m then

$$c_1,...,c_{\varphi(m)}a^{\varphi(m_s)+s}-L(0,m)a^s=\mathbf{M}\, m,$$

respectively

$$-L(0,m)a^{\varphi(m_s)+s}+c_1,...,c_{\varphi(m)}a^s=\mathbf{M}\, m$$

or more:

$$(x+c_1)...(x+c_{\varphi(m)})a^{\varphi(m_s)+s}-L(x,m)a^s=\mathbf{M}\, m$$

respectively

$$-L(x,m)a^{\varphi(m_s)+s} + (x+c_1)...(x+c_{\varphi(m)})a^s = \mathbf{M}\ m$$

which reunite Fermat, Euler, Wilson, Lagrange and Moser (respectively Sierpinski).

3) A partial spreading of Moser's and Sierpinski's results, the author also obtained (see [6], problem 7.140, pp. 173-174), the following: if m is a positive integer, $m \neq 0$,4. and "a" is an integer, then $(a^m - a)(m-1)! = \mathbf{M}\ m$, reuniting Fermat and Wilson in another way.

4) Leibnitz enunciated that: "If p is prime then $(p-2)! \equiv 1(\bmod p)$"";

We consider "$c_i < c_{i+1}(\bmod m)$" if $c_i^{'} < c_{i+1}^{'}$ where $0 \leq c_i^{'} < |m|$, $0 \leq c_{i+1}^{'} < |m|$, and $c_i \equiv c_i^{'}(\bmod m)$, $c_{i+1} \equiv c_{i+1}^{'}(\bmod m)$ it seems simply that $c_1, c_2, ..., c_{\varphi(m)}$ are all residues modulo m relatively prime to $m(c_i < c_{i+1}(\bmod m))$ for all $i, m \neq 0$, then $c_1, c_2, ..., c_{\varphi(m)-1} \equiv \pm(\bmod m)$ if $m \in A$ respectively $m \notin A$, because $c_{\varphi(m)} \equiv -1(\bmod m)$.

REFERENCES:

[1] Lejeune-Dirichlet - Vorlesungen über Zahlentheorie" - 4te Auflage, Braunschweig, 1894, §38.

[2] Sierpinski, Waclaw, - Ce ştim şi ce nu ştim despre numerele prime - Ed. Stiințifică, Bucharest, 1966.

[3] Smarandache, Florentin, - O generalizare a teoremei lui Euler referitoare la congruență - Bulet. Univ. Braşov, seria C, Vol. XXIII, pp. 7-12, 1981; see Mathematical Reviews: 84J:10006.

[4] Smarandache, Florentin - Généralisations et généralités - Ed. Nouvelle, Fés, Morocco, pp. 9-13, 1984.

[5] Smarandache, Florentin - A function in the number theory – An. Univ. Timişoara, seria şt. mat., Vol. XVIII, fasc. 1, pp. 79-88, 1980; see M. R.: 83c:10008.

[6] Smarandache, Florentin - Problèmes avec et sans…problèmes! - Somipress, Fés, Morocco, 1983; see M. R.: 84K:00003.

[Published in "Libertas Mathematica», University of Texas, Arlington, Vol. XII, 1992, pp. 181-185]