FLORENTIN SMARANDACHE

A Numerical Function in Congruence Theory


[Published in "Libertas Mathematica", University of Texas, Arlington, Vol. XII, 1992, pp. 181-185]
A NUMERICAL FUNCTION IN CONGRUENCE THEORY

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 $\{ m \in \mathbb{Z} | m = \pm p^\beta, \pm 2p^\beta \text{ with } p \text{ an odd prime, } \beta \in \mathbb{N}^*, \text{ or } m = \pm 2^\alpha \text{ with } \alpha = 0,1,2, \text{ or } m = 0 \}$.

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

We construct the FUNCTION $L : \mathbb{Z} \rightarrow \mathbb{Z}$,

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

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

If all distinct primes which divide $x$ and $m$ simultaneously are $p_i$ then:

$L(x,m) \equiv \pm 1 (\text{mod } p_1^{\alpha_1}...p_s^{\alpha_s})$

when $m \in A$ respective by $m \not\in A$, and

$L(x,m) \equiv 0 (\text{mod } m / (p_1^{\alpha_1}...p_s^{\alpha_s}))$.

Noting $d = p_1^{\alpha_1}...p_s^{\alpha_s}$ and $m' = m / d$ we find:

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

where $k_1^0,k_2^0$ constitute a particular integer solution of the Diophantine equation $k_1m' - k_2d = \pm 1$ (the signs are chosen in accordance with the affiliation of $m$ to $A$).

This result generalizes the Gauss’ theorem $(c_1,...,c_{\varphi(m)} \equiv \pm 1 (\text{mod } m))$ when $m \in A$ respectively $m \not\in A$ (see [1]) which generalized in its turn the Wilson’s theorem (if $p$ is prime then $(p-1)! \equiv -1 (\text{mod } m)$).

Proof.

The following two lemmas are trivial:

**Lemma 1.** If $c_1,...,c_{\varphi(p^\alpha)}$ are all residues modulo $p^\alpha$ relatively prime to $p^\alpha$, with $p$ an integer and $\alpha \in \mathbb{N}^*$, then for $k \in \mathbb{Z}$ and $\beta \in \mathbb{N}^*$ we have also that $kp^\beta + c_1,...,kp^\beta + c_{\varphi(p^\alpha)}$ constitute all residues modulo $p^\alpha$ relatively prime to it is sufficient to prove that for $1 \leq i \leq \varphi(p^\alpha)$ we have that $kp^\beta + c_i$ is relatively prime to $p^\alpha$, 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 \( c_1, \ldots, c_{\varphi(m)} \) are all residues modulo \( q \) relatively prime to \( q \) and \((b,q) \sim 1\) then \( b + c_1, \ldots, b + c_{\varphi(q)} \) contain a representative of the class \( \hat{0} \) modulo \( q \).

Of course, because \((b,q - b) \sim 1\) there will be a \( c_i = q - b \) whence \( b + c_i = M_q \).

From this we have the following:

Theorem 1. If \( \left(x, m \div \left(p_1^{\alpha_1} \ldots p_r^{\alpha_r}\right)\right) \sim 1\),

then

\[
(x + c_1) \ldots (x + c_{\varphi(m)}) \equiv 0 \left( \text{mod } m / \left(p_1^{\alpha_1} \ldots p_r^{\alpha_r}\right) \right).
\]

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

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

\[
(x + c_1) \ldots (x + c_{\varphi(m)}) \equiv \pm 1 \pmod{p_i^{\alpha_i}},
\]

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

\[
(x + c_1) \ldots (x + c_{\varphi(m)}) \equiv c_1, \ldots, c_{\varphi(m)} \equiv \pm 1 \pmod{p_i^{\alpha_i}}.
\]

From the lemma 5 we obtain the following:

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

\[
(x + c_1) \ldots (x + c_{\varphi(m)}) \equiv \pm 1 \pmod{p_{i_1}^{\alpha_{i_1}} \ldots p_{i_r}^{\alpha_{i_r}}},
\]

when \( m \in A \) respectively \( m \notin A \).

From the theorems 1 and 2 it results:

\[
L(x,m) \equiv \pm 1 + k_1d = k_2m',
\]

where \( k_1, k_2 \in \mathbb{Z} \). Because \((d, m') \sim 1\) the Diophantine equation \( k_2m' - k_1d = \pm 1\) 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 \( t \in \mathbb{Z} \), and \( k_1^0, k_2^0 \) constitute a particular integer solution of our equation. Thus:

\[
L(x,m) \equiv \pm 1 + m'dt + k_1^0d = \pm 1 + k_1^0 \pmod{m}
\]
or

\[
L(x,m) = k_2^0m'(\text{mod } m).
\]

§2. APPLICATIONS

1) Lagrange extended Wilson’s theorem in the following way: “If \( p \) is prime then

\[
x^{p-1} - 1 \equiv (x + 1)(x + 2) \ldots (x + p - 1)(\text{mod } p).
\]
We shall extend this result as follows: whichever are $m \neq 0, \pm 4$, we have for $x^2 + s^2 \neq 0$ that

$$x^{\varphi(m) + s} - x \equiv (x+1)(x+2)\ldots(x+|m|-1)(\mod m)$$

where $m$ and $s$ are obtained from the algorithm:

- (0) \quad \begin{cases} x = x_0d_0; \quad (x_0, m_0) \sim 1 \\ m = m_0d_0; \quad d_0 \neq 1 \end{cases}
- (1) \quad \begin{cases} d_0 = d_1^0d_1; \quad (d_1^0, m_1) \sim 1 \\ m_0 = m_1d_1; \quad d_1 \neq 1 \end{cases}

\[\text{.................................}\]

- (s-1) \quad \begin{cases} d_{s-2} = d_{s-2}^1d_{s-1}; \quad (d_{s-2}^1, m_{s-1}) \sim 1 \\ m_{s-2} = m_{s-1}d_{s-1}; \quad d_{s-1} \neq 1 \end{cases}
- (s) \quad \begin{cases} d_{s-1} = d_{s-1}^1d_s; \quad (d_{s-1}^1, m_s) \sim 1 \\ m_{s-1} = m_sd_s; \quad 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 $(p-1)!a^p + a = p \mathcal{M} p^n$, and Sierpinski (see [2], p. 57): if $p$ is prime then $a^p + (p-1)!a = p \mathcal{M} p^n$ 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 $c_1, \ldots, c_{\varphi(m)}$ are all residues modulo $m$ relatively prime to $m$ then

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

respectively

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

or more:

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

respectively

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

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 $(a^m - a)(m-1)! = \mathcal{M} m$, reuniting Fermat and Wilson in another way.
4) Leibnitz enunciated that: "If \( p \) is prime then \((p - 2)! \equiv 1 (\text{mod} \ p)"";

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

REFERENCES: