A GENERAL THEOREM FOR THE CHARACTERIZATION OF N PRIME NUMBERS SIMULTANEOUSLY

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. ABSTRACT. This article presents a necessary and sufficient theorem as N numbers, coprime two by two, to be prime simultaneously.

It generalizes V. Popa's theorem [3], as well as I. Cucurezeanu's theorem ([1], p.165), Clement's theorem, S. Patrizio's theorems [2], etc.

Particularly, this General Theorem offers different characterizations for twin primes, for quadruple primes, etc.

§2. INTRODUCTION. It is evident the following:

Lemma 1. Let A, B be nonzero integers. Then:

$$AB \equiv 0 (\mathrm{mod}\, pB) \Leftrightarrow A \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow A / p \text{ is an integer.}$$

Lemma 2.Let $(p,q) \square 1,\ (a,p) \square 1,\ (b,q) \square 1$.

Then:

$$A \equiv 0 (\mathrm{mod}\, p)$$

and

$$B \equiv 0 (\mathrm{mod}\, q) \Leftrightarrow aAq + bBp \equiv 0 (\mathrm{mod}\, pq) \Leftrightarrow aA + bBp / q \equiv 0 (\mathrm{mod}\, p)$$

$$aA / p + bB / q \text{ is an integer.}$$

Proof:

The first equivalence:

We have $A = K_1 p$ and $B = K_2 q$ with $K_1, K_2 \in \mathbf{Z}$ hence

$$aAq + bBp = (aK_1 + bK_2)pq .$$

Reciprocal: $aAq + bBp = Kpq$, with $K \in \mathbf{Z}$ it rezults that $aAq \equiv 0 (\mathrm{mod}\, p)$ and $bBp \equiv 0 (\mathrm{mod}\, q)$, but from our assumption we find $A \equiv 0 (\mathrm{mod}\, p)$ and $B \equiv 0 (\mathrm{mod}\, q)$.

The second and third equivalence results from lemma1.

By induction we extend this lemma to the following:

Lemma 3. Let $p_1, ..., p_n$ be coprime integers two by two, and let $a_1, ..., a_n$ be integer numbers such that $(a_i, p_i) \square 1$ for all i. Then

$$A_1 \equiv 0 (\bmod p_1), \ldots, A_n \equiv 0 (\bmod p_n) \Leftrightarrow$$

$$\Leftrightarrow \sum_{i=1}^{n} a_i A_i \prod_{j \neq i} p_j \equiv 0 (\bmod p_1 \ldots p_n) \Leftrightarrow$$

$$\Leftrightarrow (P / D) \cdot \sum_{i=1}^{n} (a_i A_i / p_i) \equiv 0 (\bmod P / D),$$

where $P = p_1 \ldots p_n$ and D is a divisor of p $\Leftrightarrow \sum_{i=1}^{n} a_i A_i / p_i$ is an integer.

§3. From this last lemma we can find immediately a GENERAL THEOREM:

Let $P_{ij}, 1 \le i \le n, 1 \le j \le m_i$, be coprime integers two by two, and let $r_1, \ldots, r_n, a_1, \ldots, a_n$ be integer numbers such that a_i be coprime with r_i for all i.

The following conditions are considered:

(i) $p_{i_1}, \ldots, p_{in_1}$, are simultaneously prime if and only if $c_i \equiv 0 (\bmod r_i)$, for all i.

Then:

The numbers $p_{ij}, 1 \le i \le n, 1 \le j \le m_i$, are simultaneously prime if and only if

$$(*) \qquad (R / D) \sum_{i=1}^{n} (a_i c_i / r_i) \equiv 0 (\bmod R / D),$$

where $P = \prod_{i=1}^{n} r_i$ and D is a divisor of R.

Remark:

Often in the conditions (i) the module r_i is equal to $\prod_{j=1}^{m_i} p_{ij}$, or to a divisor of it, and in this case the relation of the General Theorem becomes:

$$(P / D) \sum_{i=1}^{n} (a_i c_i / \prod_{j=1}^{m_i} p_{ij}) \equiv 0 (\bmod P / D)$$

where

$$P = \prod_{i,j=1}^{n, m_i} p_{ij} \text{ and } D \text{ is a divisor of } P.$$

Corollaries:

We easily obtain that our last relation is equivalent with:

$$\sum_{i=1}^{n} (a_i c_i (P / \prod_{j=1}^{m_i} p_{ij}) \equiv 0 (\bmod P),$$

and

$$\sum_{i=1}^{n} (a_i c_i / \prod_{j=1}^{m_i} p_{ij}) \text{ is an integer,}$$

etc.

The imposed restrictions for the numbers p_{ij} from the General Theorem are very wide, because if there would be two uncoprime distinct numbers, then at least one from these would not be prime, hence the $m_1 + ... + m_n$ numbers might not be prime.

The General Theorem has many variants in accordance with the assigned values for the parameters $a_1, ..., a_n$ and $r_1, ..., r_m$, the parameter D, as well as in accordance with the congruences $c_1, ..., c_n$ which characterize either a prime number or many other prime numbers simultaneously. We can start from the theorems (conditions c_i) which characterize a single prime number (see Wilson, Leibnitz, F. Smarandache [4], or Siminov (p is prime if and only if $(p-k)!(k-1)! - (-1)^k \equiv 0 (\bmod p)$, when $p \geq k \geq 1$; here, it is preferable to take $k = [(p+1)/2]$, where $[x]$ represents the gratest integer number $\leq x$, in order that the number $(p-k)!(k-1)!$ be the smallest possibly) for obtaining, by means of the General Theorem, conditions $c_j^{'}$, which characterize many prime numbers simultaneously. Afterwards, from the conditions $c_i, c_j^{'}$, using the General Theorem again, we find new conditions $c_h^{''}$ which characterize prime numbers simultaneously. And this method can be continued analogically.

Remarks

Let $m_i = 1$ and c_i represent the Simionov's theorem for all i

(a) If $D = 1$ it results in V. Popa's theorem, which generalizes in the Cucurezeanu's theorem and the last one generalizes in its turn Clement's theorem!

(b) If $D = P / p_2$ and choosing convenintly the parameters a_i, k_i for $i = 1, 2, 3$, it results in S. Patrizio's theorem.

Several Examples:

1. Let $p_1, p_2, ..., p_n$ be positive integers >1, coprime integers two by two, and $1 \leq k_i \leq p_i$ for all i. Then $p_1, p_2, ..., p_n$ are simultaneously prime if and only if:

(T) $$\sum_{i=1}^{n} \left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i} \right] \cdot \prod_{j \neq i} p_i \equiv 0 (\bmod p_1 p_2 ... p_n)$$

or

(U) $$\sum_{i=1}^{n} \left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i} \right] \cdot \prod_{j \neq i} p_i / (p_{s+1} ... p_n) \equiv 0 (\bmod p_1 ... p_s)$$

or

(V) $$\sum_{i=1}^{n} \left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i} \right] \cdot p_j / p_i \equiv 0 (\bmod p_j)$$

or

(W) $$\sum_{i=1}^{n} \left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i} \right] \cdot p_j / p_i \text{ is an integer.}$$

2. Another relation example (using the first theorem form [4]: p is a prime positive integer if and only if $(p-3)! - (p-1)/2 \equiv 0 (\mathrm{mod}\, p)$

$$\sum_{i=1}^{n} \left[(p_i - 3)! - (p_i - 1)/2 \right] \cdot p_1 / p_i \equiv 0 (\mathrm{mod}\, p_1)$$

3. The odd numbers … and … are twin prime if and only if:
$(p-1)!(3p+2) + 2p + 2 \equiv 0 (\mathrm{mod}\, p(p+2))$
or
$(p-1)!(p+2) - 2 \equiv 0 (\mathrm{mod}\, p(p+2))$
or
$\left[(p-1)! + 1 \right] / p + \left[(p-1)! 2 + 1 \right] / (p+2)$ is an integer.
These twin prime characterzations differ from Clement's theorem $((p-1)! 4 + p + 4 \equiv 0 (\mathrm{mod}\, p(p+2)))$

4. Let $(p, p+k) \square 1$ then: p and $p+k$ are prime simultaneously if and only if

$$(p-1)!(p+k) + (p+k-1)! p + 2p + k \equiv 0 (\mathrm{mod}\, p(p+k)),$$

which differs from I. Cucurezeanu's theorem ([1], p. 165):

$$k \cdot k! \left[(p-1)! + 1 \right] + \left[K! - (-1)^k \right] p \equiv 0 (\mathrm{mod}\, p(p+k))$$

5. Look at a characterization of a quadruple of primes for $p, p+2, p+6, p+8$:

$$\left[(p-1)! + 1 \right] / p + \left[(p-1)! 2! + 1 \right] / (p+2) + \left[(p-1)! 6! + 1 \right] / (p+6) + \left[(p-1)! 8! + 1 \right] / (p+8)$$

be an integer.

6. For $p-2, p, p+4$ coprime integers tw by two, we find the relation:

$$(p-1)! + p\left[(p-3)! + 1 \right] / (p-2) + p\left[(p+3)! + 1 \right] / (p+4) \equiv -1 (\mathrm{mod}\, p),$$

which differ from S. Patrizio's theorem

$$\left(8\left[(p+3)! / (p+4) \right] + 4\left[(p-3)! / (p-2) \right] \equiv -11 (\mathrm{mod}\, p) \right).$$

References

[1] Cucuruzeanu, I – Probleme de aritmetică şi teoria numerelor, Ed. Tehnică, Bucharest, 1966.

[2] Patrizio, Serafino – Generalizzazione del teorema di Wilson alle terne prime - Enseignement Math., Vol. 22(2), nr. 3-4, pp. 175-184, 1976.

[3] Popa, Valeriu – Asupra unor generalizări ale teoremei lui Clement - Studii şi Cercetări matematice, Vol. 24, nr. 9, pp. 1435-1440, 1972.

[4] Smarandache, Florentin – Criterii ca un număr natural să fie prim - Gazeta Matematică, nr. 2, pp. 49-52; 1981; see Mathematical Reviews (USA): 83a:10007.

[Presented at the 15th American Romanian Academy Annual Convention, which was held in Montréal, Québec, Canada, from June 14-18, 1990, at École Polytechnique de Montréal. Published in ”Libertas Mathemaica”, University of Texas, Alington, Vol. XI, 1991, pp. 151-5]