

CHARACTERIZATION OF N PRIME NUMBERS SIMULTANEOUSLY

F. Smarandache

Abstract.

This article presents a necessary and sufficient condition for 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], and other similar results. In particular, this general result offers different characterizations for twin primes and for quadruple primes.

Introduction.

It is almost evident the following:

Lemma 1. Let A, B be nonzero integers. Then: $AB \equiv 0 \pmod{pB} \Leftrightarrow A \equiv 0 \pmod{p} \Leftrightarrow A/p$ is an integer.

Lemma 2. Let $(p, q) \sim 1, (a, p) \sim 1, (b, q) \sim 1$. Then $A \equiv 0 \pmod{p}$ and $B \equiv 0 \pmod{q} \Leftrightarrow aAq + bBp \equiv 0 \pmod{pq} \Leftrightarrow aA + bBp/q \equiv 0 \pmod{p} \Leftrightarrow aA/p + bB/q$ is an integer.

Proof: The first equivalence: We have $A = K_1p$ and $B = K_2q$, with $K_1, K_2 \in \mathbb{Z}$; therefore, we have $aAq + bBp = (aK_1 + bK_2)pq$.

Conversely, if $aAq + bBp = Kpq$, with $K \in \mathbb{Z}$, it follows that $aAq \equiv 0 \pmod{p}$ and $bBp \equiv 0 \pmod{q}$, but from our assumption we find $A \equiv 0 \pmod{p}$ and $B \equiv 0 \pmod{q}$.

The second and third equivalences result from Lemma 1.

By induction, Lemma 2 can be extended to:

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

$$\begin{aligned} A_1 &\equiv 0 \pmod{p_1}, \dots, A_n \equiv 0 \pmod{p_n} \\ &\Leftrightarrow \sum_{i=1}^n a_i A_i \prod_{j \neq i} p_j \equiv 0 \pmod{p_1 \dots p_n} \\ &\Leftrightarrow (P/D) \cdot \sum_{i=1}^n (a_i A_i / p_i) \equiv 0 \pmod{P/D}, \end{aligned}$$

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

From this last lemma we can derive immediately the GENERAL THEOREM:

Let $P_{ij}, 1 \leq i \leq n, 1 \leq j \leq m_i$, be coprime integers two by two, and let $r_1, \dots, r_n, a_1, \dots, a_n$ be integers such that a_i and r_i are coprime for all i .

The following conditions are considered:

(i) $p_{i_1}, \dots, p_{i_{n_1}}$, are simultaneously prime if and only if $c_i \equiv 0 \pmod{r_i}$, for all i .

Then the numbers $p_{ij}, 1 \leq i \leq n, 1 \leq j \leq m_i$, are simultaneously prime if and only if

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

where

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

Remark. Often, under 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 in the General Theorem becomes:

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

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 to

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

and

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

The imposed restrictions for the numbers p_{ij} from the General Theorem are not so stringent, because if there are two distinct uncoprime numbers, then at least one is not prime; hence the $m_1 + \dots + m_n$ numbers might not be prime.

The General Theorem has many variants in accordance with the choices for the parameters a_1, \dots, a_n , and r_1, \dots, r_m , the parameter D , as well as in accordance with the congruences c_1, \dots, c_n which characterize either a prime number or several 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 Simionov (p is prime if and only if $(p - k!(k-1)! - (-1)^k \equiv 0 \pmod{p}$), when $p \geq k \geq 1$). Here, it is preferable to take $k = \lfloor (p+1)/2 \rfloor$, where $\lfloor x \rfloor$ represents the greatest integer number $\leq x$, in order that the number $(p - k!(k-1)!$ be the smallest possible for obtaining, by means of the General Theorem, conditions c_j' , which characterize several 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 analogously.

Remarks. Let $m_i = 1$ and c_i be the Simionov's theorem, for all i .

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

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

Some Examples:

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

$$(T) \quad \sum_{i=1}^n [p_i - k_i]!(k_i - 1)! - (-1)^{k_i} \cdot \prod_{j \neq i} p_j \equiv 0 \pmod{p_1 p_2 \dots p_n},$$

or

$$(U) \quad \sum_{i=1}^n [p_i - k_i]!(k_i - 1)! - (-1)^{k_i} \prod_{j \neq 1} (p_j) / (p_{s+1} \dots p_n) \equiv 0 \pmod{p_1 \dots p_s},$$

or

$$(V) \quad \sum_{i=1}^n [p_i - k_i]!(k_i - 1)! - (-1)^{k_i} p_j / p_i \equiv 0 \pmod{p_j},$$

or

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

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

$$\sum_{i=1}^n [p_i - 3]! - (p_i - 1)/2 p_i / p_i \equiv 0 \pmod{p_i}.$$

3. The odd numbers p and $p+2$ are twin prime if and only if:

$$(p-1)!(3p+2) + 2p+2 \equiv 0 \pmod{p(p+2)},$$

or

$$(p-1)!(p-2) - 2 \equiv 0 \pmod{p(p+2)},$$

or

$$[(p-1)! + 1]/p + [(p-1)!2 + 1]/(p+2) \text{ is an integer.}$$

These twin prime characterizations differ from Clement's theorem $((p-1)!4 + p + 4 \equiv 0 \pmod{p(p+2)})$.

4. Let $(p, p+k) \sim 1$, then: p and $p+k$ are prime simultaneously if and only if $(p-1)!(p+k) + (p+k-1)!p + 2p+k \equiv 0 \pmod{p(p+k)}$, which differs from I. Cucurezeanu's theorem ([1], p. 165): $k \cdot k![(p-1)! + 1] + [k! - (-1)^k]p \equiv 0 \pmod{p(p+k)}$.

5. Now a characterization of a quadruple of primes $p, p+2, p+6, p+8$: $[(p-1)! + 1]/p + [(p-1)!2! + 1]/(p+2) + [(p-1)!6! + 1]/(p+6) + [(p-1)!8! + 1]/(p+8)$ is an integer.

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

$$(p-1)! + p[(p-3)! + 1]/(p-2) + p[(p+3)! + 1]/(p+4) \equiv -1 \pmod{p},$$

which differ from Patrizio's theorem $(8[(p+3)!/(p+4)] + 4[(p-3)!/(p-2)]) \equiv -11 \pmod{p}$).

References

- [1] I. Cucurezeanu, Probleme de aritmetică și teoria numerelor, Ed. Tehnică, București, 1966.
- [2] Serafino Patrizio, Generalizzazione del teorema di Wilson alle terne prime, Enseignement Math., Vol. 22(2), nr. 3-4, pp. 175-184, 1976.
- [3] Valeriu Popa, Asupra unor generalizări ale teoremei lui Clement, Studii și cercetari matematice, Vol. 24, nr. 9, pp. 1435-1440, 1972.
- [4] Florentin Smarandache, Criterii ca un număr natural să fie prim, Gazeta Matematică, nr. 2, pp. 49-52; 1981; see Mathematical Reviews: 83a: 10007.

[Presented at the 15th American Romanian Academy Annual Convention, which was held in Montréal, Québec, Canada, from June 14-18, 1990, at the École Polytechnique de Montréal.]