*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

# THE PREIMAGE OF THE SMARANDACHE FUNCTION AND CONNECTION WITH THE CRYPTOGRAPHIC PROTECTION OF FINANCIAL INFORMATION (II)

*Tatiana Corina DOSESCU, PhD*

*Faculty of Economics and Business Administration*

*"Dimitrie Cantemir" Christian University, Bucharest, Romania*

*Email tdosescu@yahoo.com*

***Abstract***: Using the results from (Dosescu, 2021) regarding the inverse image $S^{-}$ of the function of Smarandache S, the calculation algorithm for the equivalence classes of the quotient set $\mathbb{N}^*/\sim$ is presented. With the help of a new numerical function, a connection is made with the cryptographic protection of the financial information, through the RSA cryptosystems.

***Keyword***: divisibility of natural numbers, division of modulo m, equivalence classes, algorithm, fixed point of an application, the preimage of a function, RSA cryptosystems.

***JEL Classification: C5, C6.***

## 1. Introduction

This paper is a continuous work research in order to development of mathematical concepts that describes the function of Smarandache.

On $\mathbb{N}^*$, in (Dosescu, 2021), the equivalence relation ~ was defined, as follows: $\forall x,y\in\mathbb{N}^*$, $x\sim y\Leftrightarrow \mathbf{S}(x)=\mathbf{S}(y)$, where **S** is the function of Smarandache (Coman, 2013), (Sandor, 2001), (Sandor, 2003), (Smarandache, 1999).

Because $\mathbf{S}(n!)=n$, the equivalence class of $n\in\mathbb{N}^*$, denoted by $[n]$ or $\hat{n}$, where $\hat{n}=\{x\in\mathbb{N}^*|x\sim n!\}$, i.e. $\hat{n}=\{x\in\mathbb{N}^*|\mathbf{S}(x)=n\}=S_{-}(n)$. It is found, based on Theorem 2 in (Dosescu, 2021), that $S_{-}(n)=\hat{n}$ and $n\neq 1$, if and only if $n$ is a prime number. Also, we can write $S_{-}(n)=\widehat{n!}$, for any $n\in\mathbb{N}^*$. Moreover, $n\notin S_{-}(n)=\hat{n}$, if and only if $n$ is a compound. For example, $6\notin S_{-}(6)$, but $6!\in S_{-}(6)=\hat{6}=\widehat{6!}$. In other words, 6 is not representative of class $\hat{6}$, while 6! is a class representative.

*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

Let the surjective function $f:\mathbb{N}^* \to \mathbb{N}^*$. Then, since the set $\{x \in \mathbb{N}^* | f(x) = n\}$ is non empty for any $n \in \mathbb{N}^*$ , the canonical surjection $f\_$ makes sense, where:

$$f\_ : \mathbb{N}^* \to \mathcal{P}(\mathbb{N}^*), f\_(n) = \{x \in \mathbb{N}^* | f(x) = n\}.$$

Let the equivalence relation is defined on $\mathbb{N}^*$, denoted by ~, as follows:

$$\forall a,b \in \mathbb{N}^*, a \sim b \Leftrightarrow f(a) = f(b).$$

Then the quotient set $\mathbb{N}^*/\sim$ is made up of the equivalence classes of $\mathbb{N}^*$ in relation to the equivalence relation ~. Each equivalence class is determined according to the preimage of a number $n$ by the application $f\_$, being denoted by $\hat{n}$. So $\hat{n} = \{x \in \mathbb{N}^* | f(x) = n\}$. In general, $n \notin \hat{n}$, i.e. the representative of an equivalence class depends on the choice of the function f.

As in any quotient set the equivalence classes form a partition of $\mathbb{N}^*$ or $\mathbb{N}^* = \bigcup_{n \in \mathbb{N}^*} \hat{n}$.

An example of a surjective function defined on $\mathbb{N}^*$ is the function **S**.

If there is, the fixed points of the function $f$ have the following properties, which are easy to justify: i) If $a \in \mathbb{N}^*$ is a fixed point of $f$, then $a$ is a representative of the class $\hat{a}$; ii) If $a,b \in \mathbb{N}^*$ are distinct fixed points of $f$, then $\hat{a} \neq \hat{b}$; iii) Each equivalence class may contain at most one fixed point.

## 2. Numerical function θ

A function that has the domain and codomain included in $\mathbb{N}^*$ is **a numerical function** (Cucurezeanu, 1976). Such a numerical function is further introduced.

For $n \in \mathbb{N}^* - \{1\}$ denote by $\theta(n) = \max\{p \in \text{Prim} | p \leq n\}$. If $n$ is prime, $\theta(n)=n$, that is, $n$ is a fixed point. If $n$ is a compound number, $\theta(n)$ is the largest prime number less than $n$. In this way the numerical function has been defined $\theta:\mathbb{N}^* - \{1\} \to \text{Prim}$, which is a surjective function, having Prim the set of prime numbers. Of θ is attached the inverse image $\theta^-$, where $\theta^-: \mathcal{P}(\text{Prim}) \to \mathcal{P}(\mathbb{N}^* - \{1\})$, and the canonical surjection makes sense: $\theta\_: \text{Prim} \to \mathcal{P}(\mathbb{N}^* - \{1\})$, where $\theta\_(p) = \{x | \theta(x) = p\}$ is **the preimage of** $p$, for any $p \in$ Prim.

*Observation*. The function θ is the restriction to $\mathbb{N}^* - \{1\}$ of the function $M\Pi:[0,\infty) \to \text{Prim}$, where $\Pi: (0,\infty) \to \mathcal{P}(\text{Prim})$, $\Pi(x)$ is the set of smaller prime numbers or equal to $x>0$, and $M\Pi(x) = \max\Pi(x)$ (Coman, 2013). Also, the function is known $\pi:(0,\infty) \to \mathbb{N}$, $\pi(x) = \text{card}\Pi(x)$, with the property: $\lim_{x \to \infty} \frac{\pi(x)}{x/lnx} = 1$ . Then the approximation makes sense: $\pi(x) \approx \frac{x}{\ln x}$, $x \in (1,\infty)$. The approximation error tends to zero, when $x$ tends to ∞.

$\theta\_(p)$ is the set of natural numbers between the prime number $p$, including $p$, and the smallest prime number strictly greater than $p$. For example, $\theta(11) = 11$ and $\theta\_(7) = \{7,8,9,10\}$, i.e. $\theta\_(7)$ is the set of natural numbers between 7, including 7, and 11.

The following properties can be check:

p1) For $n \in \mathbb{N}^* - \{1\}$ , $2 \leq \theta(n) \leq n$;

*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

p2) For $a,b \in \mathbb{N}^* - \{1\}$, $\theta(a \cdot b) \neq \theta(a) \cdot \theta(b)$;

p3) For $p,q \in$Prim, $\theta(p \cdot q) < \theta(p) \cdot \theta(q)$;

p4) There are compound numbers $a$ and $b$ such that $\theta(a \cdot b) > \theta(a) \cdot \theta(b)$. For example:

$$\theta(4 \cdot 10) = 37 > 21 = \theta(4) \cdot \theta(10).$$

p5) For $n \in \mathbb{N}^* - \{1\}$, $\phi\big(\theta(n)\big) = \theta(n) - 1$, where $\phi$ is Euler's function.

*Lemma* 1.

For any $a \in \mathbb{N}^* - \{1\}$ there exists $\acute{\theta}(a) = \max\theta\_\big(\theta(a)\big) + 1 \in$ Prim and we have $\theta(a) \leq a < \acute{\theta}(a)$, $\theta\left[\phi\left(\acute{\theta}(a)\right)\right] = \theta(a)$, $a < \acute{\theta}(a) < 2a$ according to Bertrand $-$ Chebyshev's theorem (Coman, 2013).

Based on lemma 1, there is the numerical function:

$$\acute{\theta}: \mathbb{N}^* - \{1\} \to \text{Prim}, \acute{\theta}(a) = \max\theta\_\big(\theta(a)\big) + 1.$$

For the number $a \in \mathbb{N}^* - \{1\}$, $\acute{\theta}(a) = \min\{x \in \text{Prim} | x > a\}$, that is $\acute{\theta}(a)$ is the smallest prime number strictly greater than $a$. If $a \in$Prim, $\acute{\theta}(a)$ is the first prime number, successor of $a$. For example, for $a$=8 we have: $\theta(a) = 7 < a = 8 < \acute{\theta}(8) = \max\theta\_\big(\theta(8)\big) + 1 = 10 + 1 = 11$.

Let the prime numbers $p < q$. If $q = \min\{x \in \text{Prim} | x \geq p\}$, in this case, $p$ and $q$ are **successive** and we will denote by $l(p,q)$ **the number of compound numbers** what lie between $p$ and $q$, i.e.:

$$l(p,q) = \text{card}\theta\_(p) - 1,$$

where $\text{card}\theta\_(p) = p\text{-}q$.

Returning to application 3 of (Dosescu, 2021) we have:

$\theta(a) = 100895598163$, where $a$=100895598169 (Câmpan, 1978), $\theta\_(100895598163)$={10089598163,100895598164,100895598165, …,100895598186} and $l(100895598163,100895598187) = \text{card}\theta\_(100895598163) - 1 = 24\text{-}1 = 23$.

Since Prim and $\mathbb{N}^* - \{1\}$ are subsets of $\mathbb{N}^*$, the results of paragraph 1 can be applied. Thus, let the equivalence relation defined on $\mathbb{N}^* - \{1\}$, denoted by ~, as follows:

$$\forall a,b \in \mathbb{N}^* - \{1\}, a \sim b \Leftrightarrow \theta(a) = \theta(b).$$

Then the quotient set $\mathbb{N}^* - \{1\}/\sim$ is made up of the equivalence classes of $\mathbb{N}^* - \{1\}$ in relation to the equivalence relation ~. Since the fixed points of the function $\theta$ are prime numbers, each equivalence class is determined according to the preimage of a prime number $p$ by the application $\theta\_$, being denoted by $\hat{p}$.

Then $\hat{p} = \theta\_(p) = \{x \in \mathbb{N}^* - \{1\} | \theta(x) = p\}$. At the same time, $p$ is a representative of the class $\hat{p}$, because $p \in \hat{p}$, hence Prim is a system of representatives of the equivalence classes. Another system of equivalence class representatives is $\{p + 1 | p \in \text{Prim} - \{2\}\} \cup \{2\}$, because $p+1 \in \hat{p}$ and $\theta(p+1) = p$. For example, $\hat{7} = \{7,8,9,10\}$, because $\theta(7) = \theta(8) = \theta(9) = \theta(10) = 7$. Furthermore $l(7,11) = 3 = \text{card}\hat{7} - 1$.

In general, $l(p,q) = \text{card}\hat{p} - 1$, if $p$ and $q$ are successive prime numbers, $p<q$.

*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

Based on the above, you can write: $\mathbb{N}^* - \{1\} = \bigcup_{p\in \mathrm{Prim}} \hat{p}$.

A characterization of elements in the same equivalence class is:

p6) $a \in \hat{p}$, $p$ prime, if and only if $\acute{\theta}(a) = \acute{\theta}(p)$.

It is observed that (Prim, ≤) is totally ordered and 2 is the first element.

### 3. Algorithm for determining of $S_{\_}$

Based on the results from (Dosescu, 2021), the algorithm for determining the preimage $S_{\_}(n)$, $n\in\mathbb{N}^*$, comprises the following steps: I. Determine the canonical decomposition of $n!$; II. Determine the canonical decomposition of $n$; III. It determines the maximal factors of $n!$, and if $n$ is a compound it also determines the quasi-maximal factors corresponding to the maximal factors;

IV. Determine $a\in S_{\_}(n)$ as follows:

- if $n$ is prime, then, using the notations in proposition 4 of (Dosescu, 2021), $a=n\cdot q$, where $q = 1$ or $q=2^{\propto}$ with $1\leq\propto\leq g(n,2)$ or $q=3^{\beta}$ with $1\leq\beta\leq g(n,3)$ or $q=2^{\propto}\cdot 3^{\beta}$ with $1\leq\propto\leq g(n,2)$ and $1\leq\beta\leq g(n,3)$ or … or $q=2^{\propto}\cdot 3^{\beta}\cdot \ldots \cdot p^{\omega}$ with $1\leq\propto\leq g(n,2)$, $1\leq\beta\leq g(n,3)$ , … and $1\leq\omega\leq g(n,p)$, $p=\theta(n)$;

- if $n$ is compound, then, using the notations in proposition 4 of (Dosescu, 2021) and taking into account F, the set of maximal factors together with the corresponding quasi-maximal factors, $a=f\cdot q$, where:

- $f$ is a maximum factor, a quasi-maximum factor, a finite product of distinct maximum or quasi-maximum factors and not having the same base, all of F;

- $q$ is 1 or a product of different factors, from the canonical decomposition of $n!$, which are neither maximal nor quasi-maximal.

*Observation*. $F=\bigcup_{i=1}^{m}\left\{{p_i}^{g(n,p_i)-k_i+1}, \ldots, {p_i}^{g(n,p_i)}\right\}$, where $k_i$ corresponds to $p_i$ as in proposition 4c) of (Dosescu, 2021).

### 4. Algorithm for determining of card$S_{_}(n)$

Let $n\in\mathbb{N}^*$ and $n! = {q_1}^{\beta_1}\cdot {q_2}^{\beta_2}\cdot \ldots \cdot {q_r}^{\beta_r}$, the canonical decomposition of $n!$, where $r$ is the number of factors in the canonical decomposition of $n!$. Obviously $q_1 = 2, q_2 = 3$, ..., and:

- if $n$ is prime, then $q_r = n$ and $\beta_r = 1$;

- if $n$ is compound, then $q_r = \theta(n)$ and $\beta_r = 1$.

For $n$ prime we consider F = $\{n\}$ and for $n$ compound we consider F as in the above observation. Let G be the set of factors in the canonical decomposition of $n!$.

For $f\in F$ and ${a_1}^{i_1}, \ldots, {a_k}^{i_k} \in G$ the notation $f*{a_1}^{i_1} * \ldots * {a_k}^{i_k}$ is used for the set of elements in $S_{\_}(n)$ which are the product of $k$+1 factors $f\cdot {a_1}^{l_1}\cdot \ldots \cdot {a_k}^{l_k}$, $k=\overline{1,r-1}$, and each $l_j$ takes all the

*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

values from 1 to $i_j, j=\overline{1,k}$. It is found that the number of those elements is equal to the product $i_1 \cdot \ldots \cdot i_k$, i.e.:$\text{card}\left(f * {a_1}^{i_1} * \ldots * {a_k}^{i_k}\right) = i_1 \cdot \ldots \cdot i_k$.

***Caution***. If cardF> 1 those factors can be avoided, which have already been taken into account, so that there are no elements common to several sets.

With this precaution it can be written:

$$\text{cardS\_}(n) = \text{cardF} + \sum_{k=1}^{r-1} \sum_{f \in \text{F}} \text{card}\left(f * {a_1}^{i_1} * \ldots * {a_k}^{i_k}\right).$$

The algorithm for determining cardS_$(n)$, $n \in \mathbb{N}^*$, comprises the following steps:

I. Determine the canonical decomposition of *n*!;

II. Determine G and *r*=cardG;

III. Determine F and cardF, using where *n* is composed step III of the calculation algorithm for S_$(n)$;

IV. For each *k*, $k=\overline{1, r-1}$ and each $f \in$F, taking into account the mentioned precaution, it is determined $\text{card}\left(f * {a_1}^{i_1} * \ldots * {a_k}^{i_k}\right)$, where ${a_1}^{i_1}, \ldots, {a_k}^{i_k} \in$ G.

V. Calculate $\text{cardS\_}(n) = \text{cardF} + \sum_{k=1}^{r-1} \sum_{f \in \text{F}} \text{card}\left(f * {a_1}^{i_1} * \ldots * {a_k}^{i_k}\right)$.

**5. Aplication**

Using the above algorithms, determine: card S_$(12)$ and indicate 10 elements of S_$(12)$.

*Solution.*

Applying the above algorithm we obtain:

I. $12!=2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$; II. G=$\{2^{10}, 3^5, 5^2, 7, 11\}$ and *r*=5; III. F=$\{2^{10}, 2^9, 3^5\}$ and cardF=3; IV. For *k* = 1 and

- $f=2^{10}$ the sum has $C_4^1 = 4$ terms, namely:

card$f*3^5$= 5, card$f*5^2 = 2$, card$f*7$=1, card$f*11$=1;

- $f=2^9$ the sum has $C_4^1 = 4$ terms, namely:

card$f*3^5 = 5$, card$f*5^2$= 2, card$f*7$= 1, card$f*11$=1;

- $f=3^5$ the sum has $C_4^1 = 4$ terms, namely:

card$f*2^8$=8 (instead of the factors $2^{10}$ and $2^9$, which were previously considered, must $2^8$ because the terms $2^{10} \cdot 3^5$ and $2^9 \cdot 3^5$ are already considered in $2^{10}*3^5$ and $2^9 * 3^5$, respectively), card$f*5^2$= 2, card$f*7$= 1, card$f*11$=1.

For *k* = 2 and

- $f=2^{10}$ the sum has $C_4^2 = 6$ terms, namely:

card$f*3^5 * 5^2 = 10$, card$f*3^5 * 7 = 5$, card$f* 3^5 * 11 = 5$, card$f*5^2 * 7 = 2$, card$f*5^2 * 11 = 2$, card$f * 7 * 11 = 1$;

- $f=2^9$ the sum has $C_4^2 = 6$ terms, namely:

*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

$\text{card}f*3^5*5^2=10$, $\text{card}f*3^5*7=5$, $\text{card}f*3^5*11=5$, $\text{card}f*5^2*7=2$, $\text{card}f*5^2*11=2$, $\text{card}f*7*11=1$;

- $f$=$3^5$ the sum has $C_4^2=6$ terms, namely:

$\text{card}f*2^8*5^2=16$, car $df*2^8*7=8$, $\text{card}f*2^8*11=8$ (instead of the factors $2^{10}$ and $2^9$, which were previously considered, $2^8$ must be used, in order to avoid terms common to the other sets), $\text{card}f*5^2*7=2$, $\text{card}f*5^2*11=2$, $\text{card}f*7*11=1$.

For $k$ = 3 and

- $f$=$2^{10}$ the sum has $C_4^3=4$ terms, namely:

$\text{card}f*3^5*5^2*7=10$, $\text{card}f*3^5*5^2*11=10$, $\text{card}f*3^5*7*11=5$, $\text{card}f*5^2*7*11=2$;

- $f$=$2^9$ the sum has $C_4^3=4$ terms, namely:

$\text{card}f*3^5*5^2*7=10$, $\text{card}f*3^5*5^2*11=10$, $\text{card}f*3^5*7*11=5$, $\text{card}f*5^2*7*11=2$;

- $f$=$3^5$ the sum has $C_4^3=4$ terms, namely:

$\text{card}f*2^8*5^2*7=16$, $\text{card}f*2^8*5^2*11=16$, $\text{card}f*2^8*7*11=8$ (instead of the factors $2^{10}$ and $2^9$, which were previously considered, $2^8$ must be used, in order to avoid terms common to the other sets), $\text{card}f*5^2*7*11=2$.

For $k$ = 4 and

- $f$=$2^{10}$ the sum has $C_4^4=1$ terms, namely:

$\text{card}f*3^5*5^2*7*11=10$;

- $f$=$2^9$ the sum has $C_4^4=1$ terms, namely:

$\text{card}f*3^5*5^2*7*11=10$;

- $f$=$3^5$ the sum has $C_4^4=1$ terms, namely:

$\text{card}f*2^8*5^2*7*11=16$ (instead of the factors $2^{10}$ and $2^9$, which were previously considered, $2^8$ must be used, in order to avoid terms common to the other sets).

V.

$\text{CardS}_-(12)$ =3+18+12+25+25+37+27+27+42+10+10+16=3+30+87+96+36=156+96= 252<479001600=12!.

Applying the calculation algorithm for determining $S_-$ we obtain:

I. $12!=2^{10}\cdot 3^5\cdot 5^2\cdot 7\cdot 11$; II. $12=2^2\cdot 3$; III. Maximal factors corresponding to 12! can be: $2^{10}$ and $3^5$. The verification is as follows:

- from $g(12,2)=\left[\frac{12}{2}\right]+\left[\frac{12}{4}\right]+\left[\frac{12}{8}\right]+\left[\frac{12}{16}\right]=6+3+1=10$ and $g(11,2)=\left[\frac{11}{2}\right]+\left[\frac{11}{4}\right]+\left[\frac{11}{8}\right]+\left[\frac{11}{16}\right]=8$ it obtain A = {12,13,…}, the set of solutions of the inequality g (x, 2) ≥10, which implies $\mathbf{S}(2^{10})=\min A=12$ and therefore $2^{10}$ is the maximal factor, in addition $2^{10}\in S_-(12)$. Since 12 is a compound number, it makes sense to determine the quasimaximal factors corresponding to $2^{10}$. Because $g(11,2)=g(12,2)-k$, where $k$=2≥2, there is only one quasi-

*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

maximal factor $2^9$. Indeed, since $g(11,2) = 8 < 9 < 10 = g(12,2)$ the set of solutions of the inequality $g(x,2) \geq 9$ is A={12,13, ... }, of where $\mathbf{S}(2^9) = 12$ and $2^9 \in S\_(12)$. In addition, $2^9$ is also the minimum quasi-maximal factor corresponding to $2^{10}$.

- from $g(12,3) = \left[\frac{12}{3}\right] + \left[\frac{12}{9}\right] + \left[\frac{12}{27}\right] = 5$ and $g(11,3) = \left[\frac{11}{3}\right] + \left[\frac{11}{9}\right] + \left[\frac{11}{27}\right] = 4$ it obtain A={12,13, ... }, the set of solutions of the inequality $g(x,3) \geq 5$, which implies $\mathbf{S}(3^5) = \min A = 12$ and therefore $3^5$ is the maximal factor, in addition $3^5 \in S\_(12)$. Since 12 is a compound number, it makes sense to determine the quasi-maximal factors corresponding to $3^5$. Because $g(11,3) = g(12,3) - k$, where *k*=1<2, there is no quasi-maximal factor corresponding to $3^5$.

IV. Determine the set $S\_(12)$, taking into account that 12 is a compound number, F={$2^{10}, 2^9, 3^5$} and that any element of the set is of the form $f \cdot q$, where *f* is a maximal factor, a quasimaximal factor, a finite product of distinct maximal or quasimaximal factors, all of *F*, and *q* is 1 or a product of distinct factors, from the canonical decomposition of $n!$, which are neither maximal nor quasimaximal. It follows that $S\_(12)$ also contains the following 10 terms:

$$S\_(12) = \{2^{10}, 2^9, 3^5, \dots, 3^5 \cdot 2 \cdot 5, 3^5 \cdot 2 \cdot 5^2, 3^5 \cdot 2^2 \cdot 5, \dots, 3^5 \cdot 2^7 \cdot 5 \cdot 7 \cdot 11,$$
$$3^5 \cdot 2^7 \cdot 5^2 \cdot 7 \cdot 11, 3^5 \cdot 2^8 \cdot 5 \cdot 7 \cdot 11, \dots, 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \} =$$
$$= \{243, 512, 1024, ..., 2430, 4860, 12150, ..., 11975040, 23950080, 59875200, ..., 479001600\}.$$

## 6. Connection with cryptosystems

The algorithms in paragraphs 4 and 5 use number factoring. The issue of factoring large numbers is considered a difficult issue. Cryptosystems use such a problem to ensure their security (***), a problem that falls within the scope of cryptographic protection of financial information.

Next we refer to the RSA cryptosystem with public key, often used, whose algorithm involves the choice of two large prime numbers, *p* and *q*, with which we calculate $n = p \cdot q$, called **the module**. The numbers used as the module are also called **RSA numbers** (***).

We discuss the case where *p* and *q* are chosen as "approximately equal / close" large prime numbers.

In this case $n = p \cdot q$. Assuming fixed *p*, we will choose *q* as a function of *p*, so that it is as "close" to *p* as possible, using the numerical function θ. So: i) if $l\left(p, \acute{\theta}(p)\right) < l\left(p, \theta(p-1)\right)$, it choose $q=\acute{\theta}(p)$; ii) if $l\left(p, \acute{\theta}(p)\right) > l\left(p, \theta(p-1)\right)$, it choose $q=\theta(p-1)$; iii) if $l\left(p, \acute{\theta}(p)\right) = l\left(p, \theta(p-1)\right)$, it choose $q=\acute{\theta}(p)$ or $q=\theta(p-1)$.

In situation i), $p<q=\acute{\theta}(p)$. Then $\mathbf{S}(n) = \acute{\theta}(p)$, $\phi(n) = (p-1)\left(\acute{\theta}(p) - 1\right)$, where ϕ is Euler's function. In situation ii) $p>q=\theta(p-1)$. Then $\mathbf{S}(n) = p$, $\phi(n) = (p-1)(\theta(p-1) - 1)$ and $S\_(n) = \hat{n} = \theta(\widehat{p-1})$, $\theta(n) < n < \acute{\theta}(n)$ and $\theta\_\left(\theta(n)\right) = \hat{n} = \widehat{\theta(n)}$ . For situation iii) it is useful to calculate θ [ϕ (n)] in situations i) and ii).

*Social Economic Debates*
*Volume 11, Issue 1, 2022*
*ISSN 2360-1973; ISSN-L 2248-3837*

In situation i) it obtain: $\theta[\phi(n)]_{i)} = \theta\left[(p-1)\left(\acute{\theta}(p)-1\right)\right]$, where$(p-1)\left(\acute{\theta}(p)-1\right) = (p-1)\cdot \max\theta_(p) > p(p-1)$. (*)

In situation ii) it obtain:$\theta[\phi(n)]_{ii)} = \theta[(p-1)(\theta(p-1)-1)]$, where$(p-1)(\theta(p-1)-1) < (p-1)\theta(p-1) < (p-1)p$. (**)

From (*) and (**) it obtain: $\theta[\phi(n)]_{i)} \geq \mu[\phi(n)]_{ii)}$.

**Conclusion**. In situation iii), in order to increase the difficulty of factorizing *n*, we choose $q$=$\acute{\theta}(p)$. Moreover, even in situation ii) it is advisable to choose $q$=$\acute{\theta}(p)$, in order to increase the difficulty of factorizing *n*, although "close" is sacrificed.

**References**

Câmpan Fl. T., 1978, *Old and new in mathematics*, (Translation from Romanian). Ion Creangă Publiching House, Bucharest

Coman M., 2013, *Mathematical encyclopedia of classes of integer numbers*, (Translation from Romanian). Education Publishing Chesapeake Avenue Columbus, Ohio 43212 USA.

Cucurezeanu I., 1976, *Problems of arithmetic and number theory*, (Translation from Romanian). Tehnică Publishing House, Bucharest

Dosescu T. C., 2021, *The preimage of the Smarandache function and connection with the cryptographic protection of financial information*, Social Economic Debates, Volume 10, Issue 1.

Sandor J., 2001, *The Smarandache function introduced more than 80 years ago*!, Octogon Mathematical Magazine, 9, no.2, 920-921.

Sandor J., 2003, *On Additive Analogues of Certain Arithmetic Functions*, Notes on Number Theory and Discrete Mathematics, volume 9, Number 2, pp.29.

Smarandache Fl., 1999, *About some new functions in number theory*, (Translation from Romanian). http://fs.unm.edu/AUNFITN.pdf.

*** *Introduction in cryptography*,
http://staff.fmi.uvt.ro/~stelian.mihalas/cri_sin/cursuri/crisin.pdf.