BULLETIN SCIENTIFIQUE

DE

L'ÉCOLE POLYTECHNIQUE

DE

TIMIŞOARA

COMPTES RENDUS DES SÉANCES DE LA
„SOCIÉTÉ SCIENTIFIQUE DE TIMIŞOARA"

TOME 3. FASC. 1 — 2.

TIMIŞOARA
„IMPRIMERIE CARTEA ROMÂNEASCA"
1930.

SUR LES INDICATEURS

PAR

T. G. POPOVICIU

ÉLÈVE DE L'ÉCOLE NORMALE SUPÉRIEURE

1. Étant donné un nombre N, on appelle *indicateur* de N et l'on désigne par $\varphi(N)$ le nombre de nombres plus petits que N et premiers avec lui (1 compris).

Connaissant la décomposition en facteurs premiers du nombre N:

$$N = a^{\alpha} b^{\beta} c^{\gamma} \dots$$

nous avons l'indicateur par la formule:

$$\varphi(N) = a^{\alpha-1} b^{\beta-1} c^{\gamma-1} \dots (a-1)(b-1)(c-1)\dots$$

Il résulte que:

1°. *Tout indicateur est pair, sauf:*

$$\varphi(2) = 1.$$

2°. *On a l'inégalité:*

$$\varphi(N) \leqq N - 1$$

l'égalité n'étant possible que si N *est premier.*

3°. *Si* N, N_1 *sont premiers entre eux, on a:*

$$\varphi(N \cdot N_1) = \varphi(N)\,\varphi(N_1).$$

Prenons:

$$\varphi_1(N) = \varphi(N), \quad \varphi_2(N) = \varphi\big(\varphi_1(N)\big), \quad \varphi_3(N) = \varphi\big(\varphi_2(N)\big), \ \text{. etc.}$$

$\varphi_i(N)$ sera l'indicateur itéré ou simplement *l'indicateur d'ordre* i *de* N.

De 1° et 2° résulte qu'il existe un nombre n dépendant de N tel que:

$$\varphi_n(N) = 1\ ^{1)}$$

$\varphi_n(N)$ est alors le dernier indicateur de N.

1) Nous avons étudié le nombre n dans un petit travail qui paraîtra prochainement dans la „*Gazeta Matematică*".

1. Le problème inverse du calcul de l'indicateur consiste dans la résolution de l'équation:

$$\varphi(N) = A. \tag{1}$$

Remarquons d'abord qu'il suffit de chercher les *nombres pairs* N, satisfaisant à (1). En effet de la propriété 3° résulte que:

$$\varphi(N) = \varphi(2N)$$

si N est impair. Nous utiliserons constamment cette remarque dans la suite.

Mais avant d'aborder la résolution de l'équation (1) il faut examiner si elle est possible ou non. Il est évident que si A est impair différent de 1 l'équation est impossible, mais il est facile de voir qu'elle peut être impossible, même si A est pair. Par exemple la relation:

$$\varphi(N) = 14$$

est impossible.

Plus généralement on pourrait se proposer la résolution de l'équation:

$$\varphi_i(N) = A \tag{2}$$

A étant donné. Il est évident que si l'équation (2) est possible pour $i = m$, toutes les équations (2), où $i = 1, 2, \dots m-1$ seront possibles et si l'équation avec $i = m$ est impossible, toutes les équations avec $i = m+1$, $m+2, \dots$ seront impossibles.

Si, l'équation:

$$\varphi_i(N) = A$$

étant possible, la suivante:

$$\varphi_{i+1}(N) = A$$

est impossible nous dirons que, A *peut être indicateur d'ordre* i.

Si l'équation (2) est possible quelque soit i, A peut être indicateur de n'importe quel ordre.

La formule:

$$\varphi(2^{\alpha+1}) = 2^{\alpha}, \qquad \alpha = 0, 1, 2, \dots \tag{3}$$

nous montre que *les puissances de 2 peuvent être indicateurs de n'importe quel ordre.* De même l'égalité:

$$\varphi(2^{\alpha} 3^{\beta+1}) = 2^{\alpha} 3^{\beta}, \tag{4}$$

nous prouve que *les nombres de la forme* $2^{\alpha} 3^{\beta}$ $(\alpha \neq 0)$ *peuvent être indicateurs de n'importe quel ordre.*

Nous nous proposons de démontrer que:

Les seuls nombres pouvant être indicateurs de n'importe quel ordre sont les nombres de la forme:

$$2^{\alpha}, \quad \text{ou} \quad 2^{\alpha} 3^{\beta}, \quad \text{avec} \quad \alpha \neq 0. \tag{5}$$

Il suffit d'examiner les nombres pairs qui ne sont pas de la forme (5).
Avant de continuer remarquons que si :

$$\varphi(\mathrm{N}) = 2^{\alpha}\,\mathrm{A}$$

A étant impair non puissance de 3 ($\mathrm{A} = 1 = 3^0$ est puissance de 3), le nombre N ne peut pas être de l'une des formes (5). Nous auront toujours en vue cette remarque.

3. *Lemme. p étant un nombre entier positif, dans la suite :*

$$p_1 = 2\,p + 1, \qquad p_2 = 2\,p_1 + 1, \qquad p_3 = 2\,p_2 + 1, \ldots$$

il y a au moins un nombre non premier.

En effet :

1°. Si :

$$p \equiv 0 \qquad (\text{mod. } 3).$$

on a :

$$p_1 \equiv 1 \qquad (\text{mod. } 3).$$

et :

$$p_2 \equiv 0 \qquad (\text{mod. } 3).$$

et il est evident que $p_2 > 3$.

2°. Si :

$$p \equiv 1 \qquad (\text{mod. } 3),$$

on a :

$$p_1 \equiv 0 \qquad (\text{mod. } 3),$$

à moins que p ne soit pas égal à 1. Dans ce cas $p_1 = 3$ et :

$$p_3 \equiv 0 \qquad (\text{mod. } 3).$$

3°. Si :

$$p \equiv -1 \qquad (\text{mod. } 3)$$

nous pouvons poser :

$$p = 3\,k - 1$$

et alors :

$$p_1 = 2\,.\,3\,.\,k - 1$$
$$p_2 = 2^2\,.\,3\,.\,k - 1$$
$$p_3 = 2^3\,.\,3\,.\,k - 1$$
$$\cdots\cdots$$

Posons :

$$3\,k - 1 = 2^m\,.\,k_1$$

k_1 étant impair, alors de la congruence :

$$2^{\varphi(k_1)} \equiv 1 \qquad (\text{mod. } k_1)$$

nous déduisons :

$$2^{\varphi(k_1)}\,3\,.\,k \equiv 2^m\,k_1 + 1 \equiv 1 \qquad (\text{mod. } k_1)$$

donc $p_{\varphi(k_1)}$ est divisible par k_1 qui est certainement plus petit que lui. Le raisonnement est en défaut si $k_1 = 1$. Dans ce cas :

$$3\,k - 1 = 2^m = 2^{2n+1}$$

et on a :

$$2^{2n}\,.\,3\,k \equiv 1 \qquad (\text{mod. } 5) \qquad n \text{ impair}$$
$$2^{2n+5}\,.\,3\,k \equiv 1 \qquad (\text{mod. } 5) \qquad n \text{ pair.}$$

Le lemme est donc démontré.

4. Nous allons démontrer la propriété en vue d'abord pour le cas d'un nombre de la forme :

$$2\,\mathrm{A} \qquad (\mathrm{A} \text{ impair} \neq 3^{\beta}).$$

Nous divisons la démonstration en trois parties.

I. *Un nombre de la forme :*

$$2\,p$$

p étant premier > 3 ne peut pas être indicateur de n'importe quel ordre.

De l'équation :

$$\varphi(\mathrm{N}) = 2\,p$$

on déduit :

$$\mathrm{N} = 2\,q^m \qquad (q \text{ premier})$$

d'où :

$$\varphi(2\,q^m) = q^{m-1}(q-1) = 2\,p$$

donc :

1°. $m = 2, \quad q = p = 3$ impossible par hypothèse.

2°. $m = 1, \quad q = 2\,p + 1 = p_1$.

Si p_1 n'est pas premier, $2\,p$ ne peut pas être indicateur. Dans le cas contraire :

$$\varphi(2\,p_1) = 2\,p.$$

Si $p_2 = 2\,p_1 + 1$ n'est pas premier, $2\,p_1$ ne peut pas être indicateur donc $2\,p$ peut pas être indicateur d'ordre 2. Dans le cas contraire.

$$\varphi_2(2\,p_2) = \varphi_1(2\,p_1) = 2\,p.$$

On voit finalement que pour que $2\,p$ soit un indicateur d'ordre i et non pas d'ordre $i+1$ il faut que les nombres :

$$p_1 = 2\,p + 1, \qquad p_2 = 2\,p_1 + 1, \ldots \qquad p_i = 2\,p_{i-1} + 1$$

soient premiers et que $2\,p_i + 1$ ne soit pas premier. La propriété en vue résulte alors du lemme démontré.

II. *Un nombre de la forme :*

$$2\,p^{\alpha} \qquad (\alpha > 1)$$

p étant premier > 3 ne peut pas être indicateur de n'importe quel ordre.

L'équation :

$$\varphi(\mathrm{N}) = 2\,p^{\alpha},$$

donne encore :

$$\mathrm{N} = 2\,q^{m} \qquad (q \text{ premier})$$

et :

$$q^{m-1}(q-1) = 2\,p^{\alpha},$$

donc.

1° $m = \alpha + 1$, $\quad q = p = 3$ impossible par hypothèse.

2° $m = 1$, $\quad q = 2\,p^{\alpha} + 1 = p_1$.

Si p_1 n'est pas premier, $2\,p^{\alpha}$ ne peut être indicateur. Dans le cas contraire :

$$\varphi(2\,p_1) = 2\,p^{\alpha}$$

et le nombre $2\,p_1$ est d'une forme déjà étudiée. La propriété II résulte alors de la propriété I.

III *Un nombre de la forme :*

$$2\,p_1^{\alpha_1} p_2^{\alpha_2} \dots p_v^{\alpha_v} \qquad (p_1 < p_2 < \dots < p_v,\ v > 1)$$

$p_1, p_2, \dots p_v$ étant premiers, ne peut pas être indicateur de n'importe quel ordre.

On doit avoir toujours :

$$\mathrm{N} = 2\,q^{m} \qquad (q \text{ premier})$$

(car si N contenait plusieurs facteurs premiers impairs, $\varphi(\mathrm{N})$ serait divisible au moins pur 2^2).

On a donc :

$$q^{m-1}(q-1) = 2\,p_1^{\alpha_1} p_2^{\alpha_2} \dots p_v^{\alpha_v}$$

1°. il est evident qu'on ne peut jamais avoir $q = p_1, p_2, \dots$ on p_{v-1}.

2°. $\quad m = \alpha_v + 1 \quad q = p_v = 2\,p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{v-1}^{\alpha_{v-1}} + 1.$

Alors ou bien cette égalité n'a pas lieu, on bien on a :

$$\varphi(2\,p_v^{\alpha_v + 1}) = 2\,p_1^{\alpha_1} p_2^{\alpha_2} \dots p_v^{\alpha_v}$$

et le nombre $2\,p_v^{\alpha_v+1}$ est d'une forme déjà étudiée. La propriété III résulte de la propriété II.

3°. $\quad m = 1, \quad q = 2\,p_1^{\alpha_1} p_2^{\alpha_2} \dots p_v^{\alpha_v} + 1 = p'.$

Si p' n'est pas premier l'égalité est impossible. Dans le cas contraire :

$$\varphi(2\,p') = 2\,p_1^{\alpha_1} p_2^{\alpha_2} \dots p_v^{\alpha_v}$$

et la propriété III résulte alors de la propriété I.

Nous pouvons donc énoncer la proposition suivante :

Un nombre de la forme :

$$2\,\mathrm{A}$$

A étant impair non puissance de 3, ne peut pas être indicateur de n'importe quel ordre.

5. Nous allons montrer maintenant que les nombres :

$$2^{\alpha}\,\mathrm{A} \qquad (\mathrm{A} \text{ impair } \neq 3^{\beta})$$

jouissent de la même propriété. La proposition a été démontrée pour $\alpha = 1$. il suffit donc de prouver qu'elle reste vraie pour $\alpha = k$ en la suposant vraie pour $\alpha = 1, 2, \dots k-1$. Nous décomposons la démonstration comme tout à l'heure pour le cas $\alpha = 1$.

IV. *Un nombre de la forme :*

$$2^{k}\,p \qquad (p \text{ premier } > 3)$$

ne peut pas être indicateur de n'importe quel ordre.

L'équation :

$$\varphi(\mathrm{N}) = 2^{k}\,p$$

nous donne :

(6) $$\mathrm{N} = 2^{i}\,p^{j}\,q_1\,q_2 \dots q_r \qquad (q_1, q_2, \dots q_r \text{ premiers } \neq p)$$

et distincts autre eux
$j = 0, 1, 2$

d'où :

(7)
$$\varphi(\mathrm{N}) = 2^{i-1}\,p^{j-1}(p-1)(q_1-1)(q_2-1)\dots(q_r-1) \qquad j \neq 0$$
$$\varphi(\mathrm{N}) = 2^{i-1}(q_1-1)(q_2-1)\dots(q_r-1) \qquad j = 0$$

et il faut que :

(8)
$$p = 2^{n} + 1$$
$$q_1 = 2^{n_1}\,p^{n'_1} + 1$$
$$q_2 = 2^{n_2}\,p^{n'_2} + 1$$
$$\dots\dots$$
$$q_r = 2^{n_r}\,p^{n'_r} + 1.$$

1°. Si $j \neq 0$ on a :

$$i - 1 + n + n_1 + n_2 + \dots + n_r = k$$

$$j - 1 + n'_1 + n'_2 + \dots + n'_r = 1.$$

On ne peut pas avoir $i > k$. Si $i < k$ le nombre N obtenu entre dans le cas $\alpha < k$ pour lequel la propriété est vraie par hypothèse. Si $i < k$, on doit avoir :

$$n = 1, \qquad n_1 + n_2 + \dots + n_r = 0 \qquad (n_1 = n_2 = \dots = n_r = 0)$$

c'est-à-dire $\mathrm{N} = 2^{k}\,p^{2}$ et $p = 3$ qui est exclu par hypothèse.

2°. Si $j=0$ on a :

$$i-1+n_1+n_2+\ldots+n_r=k$$
$$n'_2+n'_2+\ldots+n'_r=1$$

et le seul cas qui doit être étudié, est $i=k$, alors :

$$n_1=1, \qquad n_2+\ldots+n_r=0, \qquad r=1$$
$$n'_1=1$$

et :

$$\varphi\big(2^k(2p+1)\big)=2^k p.$$

Si $p_1=2p+1$ n'est pas premier l'égalité est impossible. Dans le cas contraire $2^k(2p+1)=2^k p_1$ est de même forme que $2^k p$. On voit facilement que tout revient à montrer que la suite :

$$p_1=2p+1, \quad p_2=2p_1+1, \quad p_3=2p_2+1, \ldots$$

contient au moins un nombre non premier, ce qui résulte du lemme démontré.

V. *Un nombre de la forme :*

$$2^k p^\beta \qquad (p \text{ premier} > 3, \quad \beta>3)$$

ne peut pas être indicateur de n'importe quel ordre.

Nous avons toujours la forme (6) de N avec $j=0, 1, 2, \ldots \beta+1$. Nous écrirons donc les rélations (7) et (8).

1°. Si $j\neq 0$, on a :

$$i-1+n+n_1+\ldots+n_r=k$$
$$j-1+n'_1+n'_2+\ldots+n'_r=\beta.$$

On voit encore que le cas $i>k$ est impossible et que $i<k$ se réduit a un cas supposé démontré. Il reste donc $i=k$ comme dernier cas possible. Mais dans ce cas $n=1$ et $p=3$, ce qui est par hypothèse impossible.

2°. Si $j=0$. Le seul cas a considérer est $i=k$, alors :

$$n_1=1, \qquad n_2+n_3+\ldots+n_r=0, \qquad r=1$$
$$n'_1=\beta$$

et :

$$N=2^k(2p^\alpha+1)$$

en supposant bien entendu que $2p^\alpha+1$ est premier. Mais le nombre $2^k(2p^\alpha+1)$ pris comme indicateur a été déjà étudié et la propriété V résulte de la propriété IV.

Enfin nous devons démontrer encore que :

VI. *Un nombre de la forme :*

$$2^k p_1^{\alpha_1} p_2^{\alpha_2}\ldots p_v^{\alpha_v} \qquad (p_1, p_2, \ldots p_v \text{ premiers}, \ v>1)$$

ne peut pas être indicateur de n'importe quel ordre.

On doit avoir :

$$N=2^i p_1^{j_1} p_2^{j_2}\ldots p_v^{j_v} q_1 q_1 \ldots q_r \qquad \begin{pmatrix} q_1, q_2, \ldots q_r \text{ premiers distincts} \\ \text{et distincts de } p_1, p_2, \ldots p_v \\ j_\lambda=0, 1, \ldots \alpha_\lambda+1, \ \lambda=1, 2, \ldots v \end{pmatrix}$$

et on obtient :

$$\varphi(N)=2^{i-1} p_s^{j_s-1} p_{s+1}^{j_{s+1}-1}\ldots p_v^{j_v-1}(p_s-1)(p_{s+1}-1)\ldots(p_v-1)$$
$$(q_1-1)(q_2-1)\ldots(q_v-1)$$
$$(j_1=j_2=\ldots=j_{s-1}=0, \ j_s=j_{s+1}, \ldots j\neq 0$$
$$\varphi(N)=2^{i-1}(q_1-1)(q_2-1)\ldots(q_r-1) \qquad (j_1=j_2=\ldots=j_v=0).$$

Pour satisfaire à ces égalités il faut supposer que :

$$p_\mu=2^{m_\mu}B_\mu+1$$
$$q_\mu=2^{n_\mu}B'_\mu+1$$

pour tous les p_μ qui interviennent dans N comme facteurs, et pour q_μ, $\mu=1, 2, \ldots r$, B_μ, B'_μ sont des nombres de la forme :

$$p_{v_1}^{n'_1} p_{v_2}^{n'_2}\ldots q_{v_s}^{n'_s}$$

$v_1, v_2, \ldots v_s$ étant s nombres de la suite $1, 2, \ldots v$.

1°. Si $j_1=j_2=\ldots=j_{s-1}=0$, $j_s\neq 0$, $j_{s+1}\neq 0, \ldots j_v\neq 0$, nous avons :

$$i-1+\sum_{\mu=s}^{v} m_\mu+\sum_{\mu=1}^{r} n_\mu=k,$$

et le seul cas qui demande une étude est $i=k$. Alors on déduit :

$$s=v, \quad m_v=1, \quad n_1+n_2+\ldots+n_r=0,$$

et :

$$N=2^k P_v^{\alpha_v+1}$$

avec :

$$p_v=2p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{v-1}^{\alpha_{v-1}}+1.$$

Si une telle égalité est possible (en intervertissant au besoin l'ordre des facteurs dans $2^k p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_v^{\alpha_v}$), le nombre N rentre dans une catégorie déjà étudiée et la propriété v_1 résulte de la propriété V :

2°. Si $j_1=j_2=\ldots=j_v=0$, nous avons :

$$i-1+\sum_{\mu=1}^{r} n_\mu=k,$$

donc si $i=k$, $r=1$ et $n_1=1$. Le nombre N est de la forme :

$$2^k q,$$

avec :

$$q=2p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_v^{\alpha_v}+1$$

et quand cette égalité est possible on est ramené à la propriété IV.

Nous pouvons donc énoncer :

Théoreme. Un nombre de la forme :

$$2^k A \qquad (k \neq 0)$$

A *étant impair différent d'une puissance de 3, ne peut pas être indicateur de n'importe quel ordre.*

Il résulte que pour un tel nombre on peut déterminer un i tel que l'équation :

$$\varphi_i(N) = 2^k A$$

soit possible et la suivante :

$$\varphi_{i+1}(N) = 2^k A$$

impossible.

La demonstration donnée pour le théoreme énoncé peut servir comme procédé de calcul pour le nombre i.