FLORENTIN SMARANDACHE

Une generalisation du theoreme d'Euler

In Florentin Smarandache: "Généralisations et Généralités". Fès (Maroc): Édition Nouvelle, 1984.

UNE GENERALISATION DU THEOREME D' EULER

Dans les paragraphes qui suivent nous allons démontrer un résultat qui remplace le théorème d'Euler :

"Si $(a,m) = 1$, alors $a^{\varphi(m)} \equiv 1 \pmod m$ "

dans le cas où a et m ne sont pas premiers entre eux.

A - Notions introductives.

On suppose $m > 0$. Cette supposition ne nuit pas à la généralité, parce que l'indicatrice d'Euler satisfait l'égalité :

$\varphi(m) = \varphi(-m)$ (cf [1]), et que les congruences vérifient la propriété suivante :

$$a \equiv b \pmod m \iff a \equiv b \pmod{-m} \qquad \text{(cf [1] pp 12-13).}$$

Quant à la relation de congruence modulo 0, c'est la relation d'égalité. On note (a,b) le plus grand commun diviseur de deux nombres entiers a et b, et on choisit $(a,b) > 0$.

B - Lemmes, théorème.

Lemme 1 : Soit a un nombre entier et m un naturel > 0. Il existe d_o, m_o de $\mathbb{N}$ tels que $a = a_o d_o$, $m = m_o d_o$ et $(a_o, m_o) = 1$.

Preuve : il suffit de choisir $d_o = (a,m)$. En conformité avec la définition du PGCD, les quotients a_o et m_o de a et m par leur PGCD sont premiers entre eux (cf [3] pp 25-26).

Lemme 2 : Avec les notations du lemme 1, si $d_o \neq 1$ et si : $d_o = d_o^1 d_1$, $m_o = m_1 d_1$, $(d_o^1, m_1) = 1$ et $d_1 \neq 1$, alors $d_o > d_1$ et $m_o > m_1$, et si $d_o = d_1$, alors après un nombre limité de pas i on a $d_o > d_{i+1} = (d_i, m_i)$.

Preuve :

$$(0) \begin{cases} a = a_o d_o & ; \quad (a_o, m_o) = 1 \\ m = m_o d_o & \quad d_o \neq 1 \end{cases}$$

$$(1) \begin{cases} d_o = d_o^1 d_1 & ; \quad (d_o^1, m_1) = 1 \\ m_o = m_1 d_1 & \quad d_1 \neq 1 \end{cases}$$

De (0) et de (1) il résulte que $a = a_o d_o = a_o d_o^1 d_1$ donc $d_o = d_o^1 d_1$ donc $d_o > d_1$ si $d_o^1 \neq 1$.

De $m_o = m_1 d_1$ on déduit que $m_o > m_1$.

Si $d_o = d_1$ alors $m_o = m_1 d_o = k.d_o^{z}$ ($z \in \mathbb{N}^*$ et $d_o \nmid k$).

Donc $m_1 = k.d_o^{z-1}$; $d_2 = (d_1, m_1) = (d_o, k.d_o^{z-1})$. Après $i=z$ pas il vient $d_{i+1} = (d_o, k) < d_o$.

Lemme 3 : Pour chaque nombre entier a et chaque nombre naturel $m > 0$ on peut construire la séquence suivante des relations :

$$(0)\quad \begin{cases} a = a_o d_o & ;\ (a_o, m_o) = 1 \\ m = m_o d_o & ;\ d_o \neq 1 \end{cases}$$

$$(1)\quad \begin{cases} d_o = d_o^1 d_1 & ;\ (d_o^1, m_1) = 1 \\ m_o = m_1 d_1 & ;\ d_1 \neq 1 \end{cases}$$

....

$$(s-1)\quad \begin{cases} d_{s-2} = d_{s-2}^1\, d_{s-1} & ;\ (d_{s-2}^1, m_{s-1}) = 1 \\ m_{s-2} = m_{s-1} d_{s-1} & ;\ d_{s-1} \neq 1 \end{cases}$$

$$(s)\quad \begin{cases} d_{s-1} = d_{s-1}^1 d_s & ;\ (d_{s-1}^1, m_s) = 1 \\ m_{s-1} = m_s d_s & ;\ d_s = 1 \end{cases}$$

Preuve : On peut construire cette séquence en appliquant le lemme 1. La séquence est limitée, d'après le lemme 2, car après r_1 pas on a : $d_o > d_{r_1}$ et $m_o > m_{r_1}$, et après r_2 pas on a: $d_{r_1} > d_{r_1+r_2}$ et $m_{r_1} > m_{r_1+r_2}$, etc..., et les m_i sont des naturels. On arrive à $d_s = 1$ parce que si $d_s \neq 1$ on va construire de nouveau un nombre limité de relations $(s+1), \ldots, (s+r)$, avec $d_{s+r} < d_s$.

Théorème : Soient $a, m \in \mathbb{Z}$ et $m \neq 0$. Alors $a^{\varphi(m_s)+s} \equiv a^s \pmod m$ où s et m_s sont les mêmes que dans les lemmes ci-dessus.

Preuve : Comme dans ce qui précède on peut supposer $m > 0$ sans nuire à la généralité. De la séquence de relations du lemme 3 il résulte que :

$$a \overset{(o)}{=} a_o d_o \overset{(1)}{=} a_o d_o^1 d_1 \overset{(2)}{=} a_o d_o^1 d_1^1 d_2 \overset{(3)}{=} \ldots \overset{(s)}{=} a_o d_o^1 d_1^1 \ldots d_{s-1}^1 d_s$$

$$\text{et } m \overset{(0)}{=} m_o d_o \overset{(1)}{=} m_1 d_1 d_o \overset{(2)}{=} m_2 d_2 d_1 d_o \overset{(3)}{=} \ldots \overset{(s)}{=} m_s d_s d_{s-1} \ldots d_1 d_o$$

$$\text{et } m_s d_s d_{s-1} \ldots d_1 d_o = d_o d_1 \ldots d_{s-1} d_s m_s ,$$

De (0) il découle que $d_o = (a,m)$, et de (i) que $d_i = (d_{i-1}, m_{i-1})$, ce pour tout i de $\{1, 2, \ldots, s\}$.

$$\begin{aligned} d_o &= d_o^1 d_1^1 d_2^1 \ldots\ldots\ldots\ldots d_{s-1}^1 d_s \\ d_1 &= \quad d_1^1 d_2^1 \ldots\ldots\ldots\ldots d_{s-1}^1 d_s \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ d_{s-1} &= \qquad\qquad\qquad\quad d_{s-1}^1 d_s \\ d_s &= \qquad\qquad\qquad\qquad\quad d_s \end{aligned}$$

Donc $d_o d_1 d_2 \ldots d_{s-1} d_s = (d_o^1)^1 (d_1^1)^2 (d_2^1)^3 \ldots (d_{s-1}^1)^s (d_s)^{s+1}$
$= (d_o^1)^1 (d_1^1)^2 (d_2^1)^3 \ldots (d_{s-1}^1)^s$ car $d_s = 1$.

Donc $m = (d_o^1)^1 (d_1^1)^2 (d_2^1)^3 \ldots (d_{s-1}^1)^s . m_s$; donc $m_s \mid m$;

$(d_s, m_s) \overset{(s)}{=} (1, m_s) = 1$ et $(d_{s-1}^1, m_s) \overset{(s)}{=} 1$

$1 \overset{(s-1)}{=} (d_{s-2}^1, m_{s-1}) = (d_{s-2}^1, m_s d_s)$ donc $(d_{s-2}^1, m_s) = 1$

$1 \overset{(s-2)}{=} (d_{s-3}^1, m_{s-2}) = (d_{s-3}^1, m_{s-1} d_{s-1}) = (d_{s-3}^1, m_s d_s d_{s-1})$,

donc $(d_{s-3}^1, m_s) = 1$

....

$1 \overset{(i+1)}{=} (d_i^1, m_{i+1}) = (d_i^1, m_{i+2} d_{i+2}) = (d_i^1, m_{I+3} d_{i+3} d_{i+2}) = \ldots =$

$= (d_i^1, m_s d_s d_{s-1} \ldots d_{i+2})$ donc $(d_i^1, m_s) = 1$, et ce pour tout i de $\{0,1,\ldots,s-2\}$.

....

$1 \overset{(0)}{=} (a_o, m_o) = (a_o, d_1 \ldots d_{s-1} d_s m_s)$ donc $(a_o, m_s) = 1$.

Du théorème d'Euler il résulte que :

$$(d_i^1)^{\varphi(m_s)} \equiv 1 \pmod{m_s} \quad \text{pour tout i de } \{0,1,\ldots,s\} ,$$

$$a_o^{\varphi(m_s)} \equiv 1 \pmod{m_s}$$

mais $a^{\varphi(m_s)} = a_o^{\varphi(m_s)} (d_o^1)^{\varphi(m_s)} (d_1^1)^{\varphi(m_s)} \ldots (d_{s-1}^1)^{\varphi(m_s)}$

donc $a^{\varphi(m_s)} \equiv \underbrace{1.\ldots\ldots 1}_{s+1 \text{ fois}} \pmod{m_s}$

$a^{\varphi(m_s)} \equiv 1 \pmod{m_s}$.

$a_o^s . (d_o^1)^{s-1} (d_1^1)^{s-2} (d_2^1)^{s-3} \ldots (d_{s-2}^1)^1 . a^{\varphi(m_s)} \equiv$

$\equiv a_o^s . (d_o^1)^{s-1} (d_1^1)^{s-2} \ldots (d_{s-2}^1)^1 . 1 \pmod{m_s}$.

On multiplie par :

$(d_o^1)^1 (d_1^1)^2 (d_2^1)^3 \ldots (d_{s-2}^1)^{s-1} (d_{s-1}^1)^s$ et on obtient :

$$a_o^s (d_o^1)^s (d_1^1)^s \ldots (d_{s-2}^1)^s (d_{s-1}^1)^s a^{\varphi(m_s)} \equiv a_o^s (d_o^1)^s (d_1^1)^s \ldots (d_{s-2}^1)^s (d_{s-1}^1)^s$$

$$\pmod{(d_o^1)^1 \ldots (d_{s-1}^1)^s m_s}$$

mais $a_o^s(d_o^1)^s(d_1^1)^s\dots(d_{s-1}^1)^s.a^{\varphi(m_s)} = a^{\varphi(m_s)+s}$ et

$a_o^s(d_o^1)^s(d_1^1)^s\dots(d_{s-1}^1)^s = a^s$ donc $a^{\varphi(m_s)+s} \equiv a^s \pmod m$,

pour tous a, m de $\mathbb{Z}$ $(m \neq 0)$.

Observations :

(1) Si $(a,m) = 1$ alors $d_o=1$. Donc $s = 0$, et d'après le théorème on a $a^{\varphi(m_o)+0} \equiv a^0 \pmod m$ càd $a^{\varphi(m_o)+0} \equiv 1 \pmod m$.

Mais $m = m_o d_o = m_o.1 = m_o$. Donc :

$a^{\varphi(m)} \equiv 1 \pmod m$, et on obtient le théorème d'Euler.

(2) Soient a et m deux nombres entiers, $m \neq 0$ et $(a,m) = d_o \neq 1$, et $m = m_o d_o$. Si $(d_o,m_o) = 1$, alors $a^{\varphi(m_o)+1} \equiv a \pmod m$.

En effet, vient du théorème avec $s = 1$ et $m_1 = m_o$.

Cette relation a une forme semblable au théorème de Fermat :

$$a^{\varphi(p)+1} \equiv a \pmod p .$$

C - UN ALGORITHME POUR RESOUDRE LES CONGRUENCES.

On va construire un algorithme et montrer le schéma logique permettant de calculer s et m_s du théorème.

Données à entrer : deux nombres entiers a et m, $m \neq 0$.

Résultats en sortie : s et m_s ainsi que $a^{\varphi(m_s)+s} \equiv a^s \pmod m$.

Méthode :
(1) A := a
M := m
i := 0
(2) Calculer $d = (A,M)$ et $M' = M/d$.
(3) Si $d = 1$ prendre $S = i$ et $m_s = M'$; stop.
Si $d \neq 1$ prendre $A := d$, $M := M'$,
$i := i+1$, et aller en (2).

Rem : la correction d'algorithme résulte du lemme 3 et du théoréme.
Voir organigramme page suivante.
Dans cet organigramme, SUBROUTINE CMMDC calcule $D = (A,M)$ et choisit $D > 0$.

Application : Dans la résolution des exercices on utilise le théorème et l'algorithme pour calculer s et m_s.

Exemple : $6^{25604} \equiv ? \pmod{105765}$

L'on ne peut pas appliquer Fermat ou Euler car $(6,105765) = 3 \neq 1$.

On applique donc l'algorithme pour calculer s et m_s et puis le théorème antérieur :

$d_o = (6,105765) = 3$ $\quad m_o = 105765/3 = 35255$

$i = 0$; $3 \neq 1$ donc $i = 0 + 1 = 1$, $d_1 = (3,35255) = 1$,

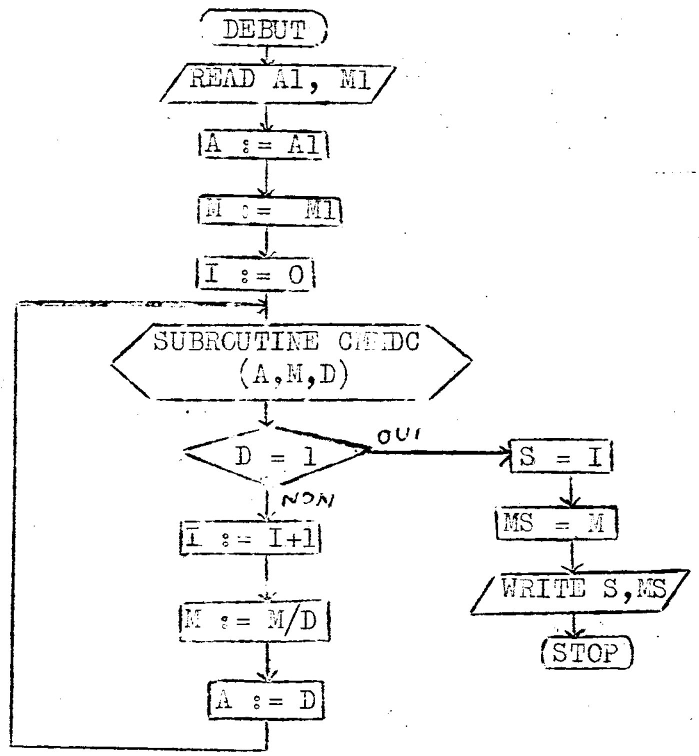
$m_1 = 35255/1 = 35255$.

Donc $6^{\varphi(35255)+1} \equiv 6^{1} \pmod{105765}$ donc

$$6^{25604} \equiv 6^{4} \pmod{105765}.$$

***

Organigramme :



***

BIBLIOGRAPHIE :

[1] Popovici, Constantin P. - "Teoria numerelor",Curs,Bucarest, Editura didactică si pedagogică, 1973.

[2] Popovici, Constantin P. - "Logica si teoria numerelor",Editura didactică si pedagogică, Bucarest, 1970.

[3] Creangă I, Cazacu C, Mihut P, Opait Gh, Reischer Corina - "Introducere în teoria numerelor",Editura didactică si pedagogică, Bucarest, 1965.

[4] Rusu E. - "Arithmetica si teoria numerelor",Editura didactică si pedagogică, Ediția a 2-a, Bucarest, 1963.