Théorème d'Euler et Code RSA

I. Groupe des éléments inversibles de Z/nZ et générateurs du groupe $(Z/nZ,+)$

En général, $G=\left\{\bar{x}\in Z/nZ \ / \ \bar{x}\neq\bar{0}\right\}$ muni de la multiplication n'est pas un groupe.
Pour $n\in\mathbf{N}^*$, notons $U_n=\left\{\bar{x}\in Z/nZ \ / \ \bar{x} \ est \ inversible \ dans \ Z/nZ\right\}$
C'est-à-dire $U_n=\left\{\bar{x}\in Z/nZ \ / \ \exists\bar{u}\in Z/nZ \ , \bar{x}\bar{u}=\bar{u}\bar{x}=\bar{1}\right\}$

Nous savons que $U_n=\left\{\bar{x}\in Z/nZ \ / \ pgcd(x,n)=1\right\}$

Théorème
$(U_n,\times)$ est un groupe abélien.

Preuve

- $\forall\bar{x},\bar{y}\in U_n$ on a : $\bar{x}\times\bar{y}\in U_n$ (à vérifier)
- La loi $\times$ est associative dans U_n car elle est associative dans Z/nZ
- $\bar{1}$ est l'élément neutre de $(U_n,\times)$
- Tout élément de U_n admet un inverse dans $(U_n,\times)$ (à vérifier)
- $\forall\bar{x},\bar{y}\in U_n$, $\bar{x}\times\bar{y}=\bar{y}\times\bar{x}$

Proposition
Les éléments de U_n sont les générateurs du groupe $(Z/nZ,+)$
c'est-à-dire $\boxed{\bar{a}\in U_n\Leftrightarrow\bar{a} \text{ est un générateur du groupe } (Z/nZ,+)}$

Preuve
Soit $\bar{x}\in U_n$. On a : $pgcd(x,n)=1$
donc l'ordre de $\bar{x}$ dans le groupe $(Z/nZ,+)$ est donné par $ord(\bar{x})=\dfrac{n}{x\wedge n}=\dfrac{n}{1}=n$ par suite $\bar{x}$ est un générateur du groupe $(Z/nZ,+)$.
Réciproquement si $\bar{a}$ est un générateur du groupe $(Z/nZ,+)$ alors $Z/nZ=\left\{k\bar{a} \ / \ k\in\mathbf{Z}\right\}$
et comme $\bar{1}\in Z/nZ$ d'où il existe $k\in\mathbf{Z}$ tel que $\bar{1}=k\bar{a}=\bar{k}\bar{a}=\bar{a}\bar{k}$ donc $\bar{a}\in U_n$

Exemples
1) $U_4=\left\{\bar{1},\bar{3}\right\}$ donc les générateurs de $(Z/4Z,+)$ sont $\bar{1}$ et $\bar{3}$ d'où $Z/4Z=\left\langle\bar{1}\right\rangle=\left\langle\bar{3}\right\rangle$
2) Si p est un entier premier alors $U_p=\left\{\bar{x}\in Z/pZ \ / \ \bar{x}\neq\bar{0}\right\}$ et $ord(U_p)=p-1$

Exercice
1) Donnez l'ensemble des générateurs du groupe $(Z/16Z,+)$
2) Montrez que $\forall\bar{x}\in U_{16}$, $\left(\bar{x}\right)^8=\bar{1}$

3) Déterminez l'ordre de $\bar{3}$ et son inverse dans $(U_{16},\times)$

Solution :
1) Les générateurs du groupe $(Z/16Z,+)$ sont les éléments de l'ensemble
$U_{16}=\left\{\bar{x}\in Z/16Z\ /\ x\wedge 16=1\right\}=\left\{\bar{1},\bar{3},\bar{5},\bar{7},\bar{9},\overline{11},\overline{13},\overline{15}\right\}$
2) D'après la question précédente, le groupe $(U_{16},\times)$ est d'ordre 8 d'où $\forall\bar{x}\in U_{16}$, $\left(\bar{x}\right)^8=\bar{1}$

3) On a : $ord(\bar{3})\,|\,8$ (cf. 2) donc $ord(\bar{3})\in\{1,2,4,8\}$.
Or $\left(\bar{3}\right)^1\neq\bar{1}$, $\left(\bar{3}\right)^2\neq\bar{1}$ et $\left(\bar{3}\right)^4=\overline{81}=\bar{1}$ dans $Z/16Z$, donc $ord(\bar{3})=4$ par suite l'inverse de $\bar{3}$ dans $(U_{16},\times)$ est $\left(\bar{3}\right)^{-1}=\left(\bar{3}\right)^3=\overline{11}$ car $\left(\bar{3}\right)^4=\left(\bar{3}\right)\times\left(\bar{3}\right)^3=\bar{1}$

II. Petit théorème de Fermat

Théorème (Petit théorème de Fermat)

Si p est un entier premier, alors on a : $\forall n\in\mathbf{Z}$, $n^p\equiv n\,[p]$

Preuve
Rappelons d'abord les deux résultats suivants:

- Si p est un entier premier alors $\forall n\in\mathbf{Z}$ on a : $p\wedge n=1$ ou $p\,|\,n$
- Si p est un entier premier alors $U_p=\left\{\bar{x}\in Z/pZ\ /\ \bar{x}\neq\bar{0}\right\}$ et $ord(U_p)=p-1$

Soient p est un entier premier et $n\in\mathbf{Z}$:
1er cas : si $p\wedge n=1$ alors $\bar{n}\in U_p=\left\{\bar{x}\in Z/pZ\ /\ x\wedge p=1\right\}=\left\{\bar{x}\in Z/pZ\ /\ \bar{x}\neq\bar{0}\right\}$ car p est un entier premier et $ord(U_p)=p-1$ d'où $\left(\bar{n}\right)^{p-1}=\bar{1}$ dans Z/pZ
Donc $n^{p-1}\equiv 1\,[p]$ d'où $n^p\equiv n\,[p]$

2ième cas : si $p\,|\,n$ alors $\bar{n}=\bar{0}$ dans Z/pZ , donc $n\equiv 0\,[p]$ d'où $n^p\equiv 0\equiv n\,[p]$
Conclusion : si p est un entier premier alors pour tout $n\in\mathbf{Z}$, $n^p\equiv n\,[p]$

Exemples :
1) $\forall n\in\mathbf{Z}$, $n^{19}\equiv n\,[19]$ car 19 est premier
2) $2^7\equiv 2\,[7]$ car 7 est premier ,
D'où $2^6\equiv 1\,[7]$ car $2\wedge 7=1$. Par suite, l'inverse de $\bar{2}$ dans $(U_7,\times)$ est $\left(\bar{2}\right)^{-1}=\left(\bar{2}\right)^5=\bar{4}$

III. Indicatrice d'Euler et théorème d'Euler
Définition (indicatrice d'Euler)
Soit $n\in\mathbf{N}^*$. On appelle l'indicatrice d'Euler de n et on note $\varphi(n)$, le nombre
$\varphi(n)$ = le nombre d'entiers $k, 1\leq k\leq n$ tel que $n\wedge k=1$.

Exemples : On a $\varphi(1)=1,\varphi(2)=1,\ \varphi(3)=2$ et $\varphi(8)=4$
Proposition
Pour $n\in\mathbf{N}^*$, $\varphi(n)$ = le nombre des éléments inversibles de Z/nZ .

Soit $\boxed{\varphi(n) = ord(U_n)}$

Remarque : $\boxed{\varphi(n)}$ **permet de calculer l'ordre du groupe** $(U_n,\times)$

Théorème d'Euler

Pour tout $n \in \mathbf{N}^*$, et pour tout $a \in \mathbf{Z}$ tel que $a \wedge n = 1$, on a : $a^{\varphi(n)} \equiv 1 \left[n\right]$

Preuve. On a : $ord(U_n) = \varphi(n)$

De plus si $a \in \mathbf{Z}$ tel que $a \wedge n = 1$, alors $\bar{a} \in U_n$

D'où $\left(\bar{a}\right)^{\varphi(n)} = \bar{1}$ dans Z/nZ c'est-à-dire $a^{\varphi(n)} \equiv 1 \left[n\right]$

Proposition (calcul de l'indicatrice d'Euler)

1) Si p est premier, alors $\varphi(p) = p - 1$

2) Si p est premier et $n \in \mathbf{N}^*$, alors $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$

3) Si p et q sont deux entiers premiers distincts, alors $\varphi(p \times q) = (p-1)(q-1)$

Preuve

1) Si p est premier, on a $U_p = \left\{\bar{x} \in Z/pZ \,/\, \bar{x} \neq \bar{0}\right\}$ d'où $\varphi(p) = ord(U_p) = p - 1$

2) Soient p est un entier premier et $n \in \mathbf{N}^*$.

Par définition, $\varphi(p^n)$ = le nombre d'entiers $k, 1 \leq k \leq p^n$ tel que $p^n \wedge k = 1$.

Soit $k \in \mathbf{N}, 1 \leq k \leq p^n$ tel que $p^n \wedge k = 1$ c-à-d $p \wedge k = 1$ car $a \wedge b = 1 \Leftrightarrow a^n \wedge b = 1$ pour $n \in \mathbf{N}^*$

De plus pour $k \in \mathbf{N}, 1 \leq k \leq p^n$, on a $p \wedge k = 1$ ou $p \,|\, k$ car p est premier,

et $p, p \times 2, p \times 3, \ldots p \times p^{n-1}$ sont les p^{n-1} entiers multiples de p compris entre 1 et p^n,

d'où $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$

3) Soient p et q deux entiers premiers tels que $p \neq q$

On a : $\varphi(p \times q)$ = le nombre d'entiers $k, 1 \leq k \leq pq$ tel que $(pq) \wedge k = 1$.

Soit $k \in \mathbf{N}, 1 \leq k \leq pq$ tel que $(pq) \wedge k = 1$.

On a : $p \wedge k = 1$ et $q \wedge k = 1$ car $(a \times b) \wedge c = 1 \Leftrightarrow a \wedge c = 1 \; et \; b \wedge c = 1$

Or $p, p \times 2, p \times 3, \ldots p \times (q-1)$ sont les $(q-1)$ entiers multiples de p compris **strictement** entre 1 et pq, les autres sont premiers avec p sauf évidement pq.

Idem $q, q \times 2, q \times 3, \ldots, q \times (p-1)$ sont les $(p-1)$ entiers multiples de q compris **strictement** entre 1 et pq, les autres sont premiers avec q sauf évidement pq.

De plus pq est le seul multiple commun de p et q compris entre 1 et pq,

d'où $\varphi(p \times q) = pq - (q-1) - (p-1) - 1 = (p-1)(q-1)$

IV. Application au code RSA

Théorème

Soient $n = p \times q$ où p et q sont deux entiers premiers et distincts, et d et e deux entiers tels que : $de \equiv 1 \left[(p-1)(q-1)\right]$. Alors ,

pour tout entier m, on a : si $c \equiv m^e \left[n\right]$, alors $c^d \equiv m^{ed} \equiv m \left[n\right]$

Preuve : $de \equiv 1 \left[(p-1)(q-1)\right] \Leftrightarrow de \equiv 1 \left[\varphi(n)\right] \Leftrightarrow \exists k \in \mathbf{Z}, \; de = 1 + k\varphi(n)$

- **1er cas** : $m \wedge n = 1$

On a : $c^d \equiv m^{e\,d}\,[n] \Leftrightarrow c^d \equiv m^{1+k\varphi(n)}\,[n] \Leftrightarrow c^d \equiv m \times (m)^{k\varphi(n)}\,[n] \Leftrightarrow c^d \equiv m \times \left(m^{\varphi(n)}\right)^k\,[n]$

D'après le théorème d'Euler, $m^{\varphi(n)} \equiv 1\,[n]$ puisque $m \wedge n = 1$

Par suite , donc $c^d \equiv m \times 1^k\,[n]$. Soit $c^d \equiv m[n]$

- **2ème cas** : $m \wedge n \neq 1$

Puisque p et q sont des entiers premiers, on a :

$$m \wedge n \neq 1 \Leftrightarrow m \wedge p \neq 1 \text{ ou } m \wedge q \neq 1$$
$$\Leftrightarrow p \mid m \text{ ou } q \mid m$$

On distingue alors 3 cas :($p \mid m$ et $m \wedge q = 1$) ou ($q \mid m$ et $m \wedge p = 1$) ou ($p \mid m$ et $q \mid m$)

1) $p \mid m$ et $m \wedge q = 1$:

On a : $c^d \equiv m^{1+k\varphi(n)}\,[q] \Leftrightarrow c^d \equiv m \times (m)^{k(p-1)(q-1)}\,[q] \Leftrightarrow c^d \equiv m \times \left(m^{(q-1)}\right)^{k(p-1)}\,[q] \Leftrightarrow c^d \equiv m[q]$

car d'après le théorème d'Euler, $m^{\varphi(q)} \equiv m^{(q-1)} \equiv 1\,[q]$ puisque $m \wedge q = 1$ et q est premier

Par ailleurs, $c^d \equiv m^{1+k\varphi(n)}\,[p] \Leftrightarrow c^d \equiv 0\,[p]$ car $m \equiv 0\,[p]$ puisque $p \mid m$ donc $c^d \equiv m\,[p]$

On a donc : $c^d \equiv m[q]$ et $c^d \equiv m\,[p]$

D'après le théorème des restes chinois, $c^d \equiv m\,[p\,q]$ puisque p et q sont premiers entre eux

2) $q \mid m$ et $m \wedge p = 1$:

Même démonstration que dans le cas précédent en remplaçant p par q

3) $p \mid m$ et $q \mid m$:

On a $c^d \equiv 0 \equiv m\,[p]$ et $c^d \equiv 0 \equiv m\,[q]$.

D'après le théorème des restes chinois, $c^d \equiv 0 \equiv m\,[p\,q]$ puisque $p \wedge q = 1$

Principe du code RSA :

- Alice souhaite recevoir de Bob un message m .
  Elle fait le choix de deux grands nombres premiers p et q , calcule $n = p \times q$ et choisit un entier e tel que $e \wedge (p-1)(q-1) = 1$ puis elle publie (n, e) .
  Les nombres premiers p et q restent secrets et ne sont connus que par Alice.

- Bob souhaite transmettre son message m à Alice en utilisant le code RSA modulo n et de clé public e .
  Bob calcule $c \equiv m^e\,[n]$ et envoie le message chiffré c à Alice

- A la réception de c , Alice calcule c^d (modulo n) où $d \in \mathbf{N}^*$ tel que $d\,e \equiv 1\,[(p-1)(q-1)]$
  Ainsi, elle obtient le message m puisque $m \equiv c^d\,[n]$

Exemples

1) Dans un chiffrement utilisant le code RSA modulo n et de clé public e , Alice publie $(n = 26,\ e = 11)$ et reçoit de Bob le message m^{11} Comment pourra-t-elle le déchiffrer ?

Solution : On a $n = 2 \times 13$ donc $\varphi(n) = 1 \times 12 = 12$. Pour déchiffrer le message, cherchons $d \in \mathbf{N}^*$ tel que $d \times 11 \equiv 1\,[12]$, soit $-d \equiv 1\,[12] \Leftrightarrow d \equiv -1 \equiv 11\,[12]$

Par suite on a : $m \equiv \left(m^{11}\right)^{11} [26]$

2) Un professeur envoie à un élève sa note de contrôle par mail.
Le professeur a chiffré la note de l'élève en utilisant le code RSA modulo n et de clé public e, et a publié $(n = 391 = 17 \times 23,\ e = 13)$. L'élève reçoit de son professeur le message 379.
Pouvez-vous aider l'élève à connaître sa note ?

Solution : On a $n = 17 \times 23$ donc $\varphi(n) = 16 \times 22 = 352$.
L'élève reçoit $379 \equiv m^{13} [391]$. Pour connaître la note de l'élève, cherchons $d \in \mathbf{N}^*$ tel que $d \times 13 \equiv 1 [352]$.
On a : $13d \equiv -351 [352] \Leftrightarrow d \equiv -27 [352]$ car $13 \wedge 352 = 1$
Donc $d \equiv 325 [352]$. Par suite, $m \equiv \left(m^{13}\right)^{325} [391]$, soit $m \equiv 379^{325} [391]$
de plus $379 \equiv -12 [391]$, d 'où $m \equiv (-12)^{325} \equiv -12^{325} [391]$
On a : $12^4 \equiv 13 [391]$, $12^{16} \equiv 13^4 \equiv 18 [391]$ et $12^{176} \equiv 18^{11} \equiv 1 [391]$
d'où $12^{325} \equiv 12^{176} \times 12^{149} \equiv 12^{149} \equiv 12^{16 \times 9 + 5} \equiv 12^{16 \times 9} \times 12^4 \times 12 \equiv 18^9 \times 13 \times 12 [391]$
Par suite $m \equiv -377 \equiv 14 [391]$.
Conclusion : la note de l'élève est 14/20.

V. Théorème du reste chinois et attaque RSA

Théorème 1.
Soient p et q deux entiers premiers entre eux (c'est-à-dire $p \wedge q = 1$) et $a \in \mathbf{Z}$, on a :
$$\begin{cases} x \equiv a [p] \\ x \equiv a [q] \end{cases} \Leftrightarrow x \equiv a [p\,q]$$

Preuve. Utiliser la propriété : si $p \wedge q = 1$, p divise a et q divise a alors $p\,q$ divise a

Théorème 2.
Soient p et q deux entiers tel que $p \wedge q = 1$ et $(a,b) \in \mathbf{Z}^2$, on a :
$$\begin{cases} x \equiv a [p] \\ x \equiv b [q] \end{cases} \Leftrightarrow x \equiv c [p\,q] \text{ où } c \text{ existe et vérifie } c \equiv a [p] \text{ et } c \equiv b [q]$$

Preuve. $p \wedge q = 1 \Leftrightarrow \exists (u,v) \in \mathbf{Z}^2,\ p\,u + q\,v = 1$, on pose $c = b\,p\,u + a\,q\,v$.
Avec ce choix, on a : $c \equiv a [p]$ et $c \equiv b [q]$ d'où
$$\begin{cases} x \equiv a [p] \\ x \equiv b [q] \end{cases} \Leftrightarrow \begin{cases} x \equiv c [p] \\ x \equiv c [q] \end{cases} \Leftrightarrow x \equiv c [p\,q] \text{ (d'après le théorème1)}$$

Exemple
Résoudre dans $\mathbf{Z}$, le système suivant : $\begin{cases} x \equiv 4 [13] \\ x \equiv 6 [11] \end{cases}$

1er méthode
$$\begin{cases} x \equiv 4 [13] \\ x \equiv 6 [11] \end{cases} \Leftrightarrow \begin{cases} x \equiv 17 [13] \\ x \equiv 17 [11] \end{cases} \Leftrightarrow x \equiv 17 [143] \text{ car } 11 \wedge 13 = 1$$

2ème méthode
D'après l'algorithme d'Euclide, on a : $6 \times 11 - 5 \times 13 = 1$
On pose alors $c = 4 \times 6 \times 11 - 6 \times 5 \times 13 = -126$ d'où

$$\begin{cases} x \equiv 4 [13] \\ x \equiv 6 [11] \end{cases} \Leftrightarrow \begin{cases} x \equiv -126 [13] \\ x \equiv -126 [11] \end{cases} \Leftrightarrow x \equiv -126 [143] \text{ car } 11 \wedge 13 = 1$$

Exercice 1

Résoudre dans $\mathbf{Z}$, les systèmes suivants :

(1) $\begin{cases} 2x \equiv 7 [23] \\ x \equiv -1 [11] \end{cases}$; (2) $\begin{cases} 5x \equiv 4 [8] \\ 16x \equiv 6 [7] \end{cases}$; (3) $\begin{cases} 5x \equiv 4 [6] \\ 16x \equiv 6 [7] \end{cases}$

Exercice 2

Résoudre dans $\mathbf{Z}$, l'équation $x^2 \equiv 1 [55]$

Exercice 3.

Résoudre dans $\mathbf{Z}$, le système suivant : $\begin{cases} 5x \equiv 19 [2] \\ 3x \equiv 8 [11] \end{cases}$

Exercice 4.

Trouvez le temps t de la conjonction de deux astres A et B de périodes de révolution respectivement $6h$ et $11h$, connaissant deux instants de passage $t_1 = 5h$ et $t_2 = 4h$ (respectivement) de ces deux astres en un même azimuth.

Exercice 5. (Problème du cuisinier chinois)

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés et le partage laisserait 5 pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Attaque RSA

Supposons qu'un même message m soit chiffré selon RSA, avec une clef publique commune e, et deux modulos distincts (n_1 et n_2) (publics eux aussi).

Autrement dit les deux messages chiffrés c_1 et c_2 sont diffusés, où

$c_1 \equiv m^e [n_1]$ et $c_2 \equiv m^e [n_2]$

Si $n_1 \wedge n_2 = 1$, alors d'après le théorème Chinois appliqué au système

$\begin{cases} m^e \equiv c_1 [n_1] \\ m^e \equiv c_2 [n_2] \end{cases}$ on a $m^e \equiv c \ [n_1 n_2]$

Dans le cas où $m^e < n_1 n_2$ (ce qui peut arriver si e est suffisamment petit), on peut espérer déchiffrer le message m en calculant $\sqrt[e]{c} = m$.