Petit théorème de Fermat et codage RSA

Jean-Paul Quelen

1er juin 2015

1. Théorème

Soit p un nombre premier et a un entier naturel premier avec p alors $a^{p-1}-1$ est divisible par p. En d'autres termes $a^{p-1} \equiv 1\ [p]$.

Démonstration
p ne divise aucun nombre de la suite a, $2a$, $3a$, ..., $(p-1)a$. En effet, d'après le théorème de Gauss, si p divisait un de ces produits $k\ a$, p diviserait k puisque a et p sont premiers entre eux. Ceci est impossible puisque $1 < k < p$.
De plus les restes des divisions de a, $2a$, $3a$, ..., $(p-1)a$ par p sont tous différents. Si on trouvait des restes identiques pour $k\ a$ et $k'\ a$, $(k > k')$ alors le reste de $(k-k')a$ par p serait nul, ce qui est impossible d'après ce qui précède. Donc à l'ordre près des facteurs les restes de a, $2a$, $3a$, ..., $(p-1)a$ par p sont 1, 2, 3, ..., $p-1$.
Par conséquent la division du produit $a\ 2a\ 3a\ \ldots\ (p-1)a$ par p a pour reste le produit $1\ 2\ 3\ \ldots\ (p-1)$ et donc $a\ 2a\ 3a\ \ldots\ (p-1)a$ qui s'écrit encore
$a^{p-1}\ 2\ 3\ \ldots\ (p-1)$ est congru à $2\ 3\ \ldots\ (p-1)$ modulo p. Il existe donc un entier relatif k tel que $(a^{p-1}-1)\,(2\ 3\ \ldots\ (p-1)) = k\ p$. Comme p est premier avec $2\ 3\ \ldots\ (p-1)$, d'après le théorème de Gauss, p divise $a^{p-1}-1$. a^{p-1} est donc congru à 1 modulo p.
Ce théorème est encore appelé petit théorème de Fermat.

2. Corollaire

Soit p un nombre premier et a un entier quelconque alors $a^p \equiv a\ [p]$.

Démonstration
D'après ce qui précède, si a et p sont premiers entre eux, $a^{p-1}-1$ est congru à 0 modulo p. Sinon, p étant premier, a est congru à 0 modulo p. On a donc soit $a^{p-1} \equiv 1\ [p]$ soit $a^p \equiv a \equiv 0\ [p]$ et par conséquent dans les deux cas $a^p \equiv a\ [p]$.

3. Autre méthode

Par récurrence :
La propriété $a^p \equiv a\ [p]$ est vraie pour $a = 0$.
Si $a^p \equiv a\ [p]$ alors il existe un entier k tel que $a^p = k\ p + a$. Dans ces conditions :

$$(a+1)^p = a^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} a^i = k\ p + a + 1 + \sum_{i=1}^{p-1} \binom{p}{i} a^i.$$

Or $\binom{p}{i} = \dfrac{p(p-1)\dots(p-i+1)}{1\times 2\times \dots \times i}$. Comme p est premier et i strictement inférieur à p, aucun nombre parmi 2, 3, …, i ne divise p. Par suite $\dfrac{(p-1)\dots(p-i+1)}{1\times 2\times \dots \times i}$ est entier et :

$$(a+1)^p = a+1+p\left(k+\sum_{i=1}^{p-1}\frac{(p-1)\dots(p-i+1)}{1\times 2\times \dots \times i}a^i\right).$$

D'où : $(a+1)^p \equiv (a+1)\ [p]$. CQFD
$a^p - a = a(a^{p-1}-1)$. Par suite si a n'est pas divisible par p, p étant premier, $a^{p-1}-1$ est divisible par p.

4. Le cryptage RSA

Le cryptage RSA (du nom des inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman) est intéressant car la clé de cryptage est publique et il n'a donc pas de risques liés à l'envoi de la clé et au procédé de codage des données. Bob comme tout le monde peut crypter et envoyer un message. Par contre, seul la destinataire, Alice, qui connaît la clé privée correspondante pourra reconstituer le message initial.

Alice, la destinataire rend publique deux nombres n et c où n est le produit de deux grands nombres premiers p et q qu'elle est seule à connaître, où c est un entier premier avec le produit $(p-1)(q-1)$ compris entre 2 et $(p-1)(q-1)$.

Pour coder le message « BONJOUR », par exemple, on commence par remplacer les lettres par leurs positions dans l'ordre alphabétique ce qui donne 02 15 14 10 15 21 18.
Si on utilise $n = 10573 = 97\times 109$ on peut regrouper les chiffres par 4 sans risquer de dépasser n. Ce qui donne 0215 1410 1521 0018. Pour chaque nombre a de la série, on détermine alors b, reste de la division de a^c par n. On obtient alors dans ce cas avec $c = 5$ la série : 9131 7391 0690 7574. C'est cette série de nombres qu'envoie Bob à Alice.

Alice qui connaît les deux facteurs premiers de n (ici $p = 97$ et $q = 109$) détermine alors facilement le nombre entier d vérifiant $1 < d < (p-1)(q-1)$ et tel que $c\ d \equiv 1\ [(p-1)(q-1)]$. Ici $d = 6221$.
Alice peut alors retrouver la série initiale de nombres car pour chaque entier b de cette série on démontre que b^d est congru à a modulo n.

L'intérêt pour Alice est bien sûr d'avoir un nombre n produit de deux nombres premiers très grands de façon à ce que les calculateurs même les plus rapides ne puissent pas trouver en un temps suffisamment court les deux facteurs premiers nécessaires pour calculer d.
Notons d'autre part que c et d jouent le même rôle et sont interchangeables. Ainsi Alice peut décider de coder elle-même un message en utilisant sa clé privée $d = 6221$. Bob décryptera alors aisément ce message avec la clé publique c. Le message envoyé à Bob constitue en fait une signature du message d'Alice. En effet si Bob réussit

à décrypter sans problème le message à l'aide de la clé c, c'est que ce message a été codé avec la clé privée d connue d'Alice seule et cela suffit pour en garantir l'authenticité.

5. Propriétés justifiant la méthode RSA

Propriété 1

Soit p et q deux nombres premiers. Si c, tel que $1 < c < (p-1)(q-1)$, est premier avec le produit $(p-1)(q-1)$ alors il existe d unique tel que $1 < d < (p-1)(q-1)$ et vérifiant $c\ d \equiv 1\ [(p-1)(q-1)]$.

Démonstration

Si c et $(p-1)(q-1)$ sont premiers entre eux, il existe d'après le théorème de Bezout deux entiers relatifs u_0 et v_0 tels que $u_0\ c + v_0(p-1)(q-1) = 1$. Par suite (u, v) est solution de $u\ c + v(p-1)(q-1) = 1$ si et seulement si il existe un entier relatif k tel que $u = u_0 - k(p-1)(q-1)$ et $v = v_0 + k\ c$.

Soit donc k tel que u soit le plus petit des entiers positifs. Dans ces conditions $u\ c = 1 - v(p-1)(q-1)$ est congru à 1 modulo $(p-1)(q-1)$ et le nombre d recherché est par conséquent égal à u.

Il est unique car s'il en existait un autre, d', alors on aurait $c(d-d') \equiv 0\ [(p-1)(q-1)]$. Comme c est premier avec $(p-1)(q-1)$ alors, d'après le théorème de Gauss, $d - d' \equiv 0\ [(p-1)(q-1)]$. Mais comme on a $1 < d < (p-1)(q-1)$ et $1 < d' < (p-1)(q-1)$ et bien on ne peut avoir que $d = d'$.

Propriété 2

Dans les conditions précédentes, si p et q sont différents et si $b \equiv a^c\ [p\ q]$ alors $b^d \equiv a\ [p\ q]$.

Démonstration

Si $b \equiv a^c\ [p\ q]$ alors $b^d \equiv a^{c\ d}\ [p\ q]$. $c\ d \equiv 1\ [(p-1)(q-1)]$. Il existe donc un entier $k \geqslant 0$ tel que $c\ d = 1 + k(p-1)(q-1)$. On obtient donc $a^{c\ d} = a\left((a^{p-1})^{q-1}\right)^k$. Si a est divisible par p alors de façon évidente $a^{c\ d} \equiv a \equiv 0\ [p]$, sinon, d'après le petit théorème de Fermat, $a^{p-1} \equiv 1\ [p]$ d'où $a^{c\ d} \equiv a\ [p]$. De même $a^{c\ d} \equiv a\ [q]$.

Il existe donc deux entiers k et k' tels que $a^{c\ d} = a + k\ p$ et $a^{c\ d} = a + k'\ q$.

Ainsi $k\ p = k'\ q$, entier qui se trouve donc être multiple de $p\ q$ puisque p et q sont des nombres premiers différents. On obtient donc dans ces conditions : $a^{c\ d} \equiv a\ [p\ q]$.

Rappel : $a \equiv b\ [c]$ signifie que $b - a$ est un multiple de c.

6. Algorithmes utilisés

a) Recherche le premier entier c tel que c et $(p-1)(q-1)$ soient premiers entre eux.

$c \longleftarrow 1$ // c ne peut être qu'impair :
$j \longleftarrow c+2$ // on essaie donc tous les nombres impairs de 3 à $(p-1)(q-1)$
$b \longleftarrow$vrai // et on s'arrête au premier c trouvé, mais on pourrait aussi continuer...
tant que b et $j < (p-1)(q-1)$ faire
    $i1 \longleftarrow (p-1)(q-1)$ //on applique l'algorithme d'Euclide à $(p-1)(q-1)$ et j
    $j1 \longleftarrow j$
    faire
        $k \longleftarrow i1 \ \% \ j1$ // reste de la division de $i1$ par $j1$
        $i1 \longleftarrow j1$
        $j1 \longleftarrow k$
    jusqu'à $k \leqslant 1$
    si $k = 0$
        $j \longleftarrow j+2$ // $k = 0$: ça ne va pas
    sinon
        $b \longleftarrow$ faux //ça convient car 1 est le PGCD de c et de $(p-1)(q-1)$.
si b
    afficher "pas de c"
sinon
    $c \longleftarrow j$
afficher "le résultat est c"

b) Recherche d tel que $c\ d \equiv 1\ [(p-1)(q-1)]$.

// recherche le premier $i = 1 + k(p-1)(q-1)$ divisible par c.
$i \longleftarrow 1$
faire
    $i \longleftarrow i + (p-1)(q-1)$
jusqu'à $i\ \%\ c = 0$ // on boucle tant que c n'est pas un diviseur de i.
$d \longleftarrow i/c$
afficher d

c) Calcul du reste de la division de a^c (ou a^d par n).

// comme c peut être grand on alterne multiplication et reste de la division
$b \longleftarrow 1$
faire de $i = 0$ à c
    $b \longleftarrow b \times a$
    $b \longleftarrow b\ \%\ n$
afficher b