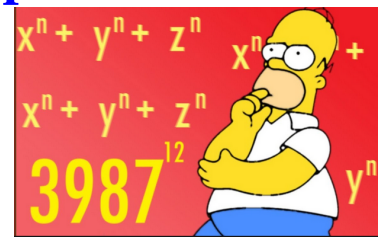
Rappels mathématiques



1 Les congruences

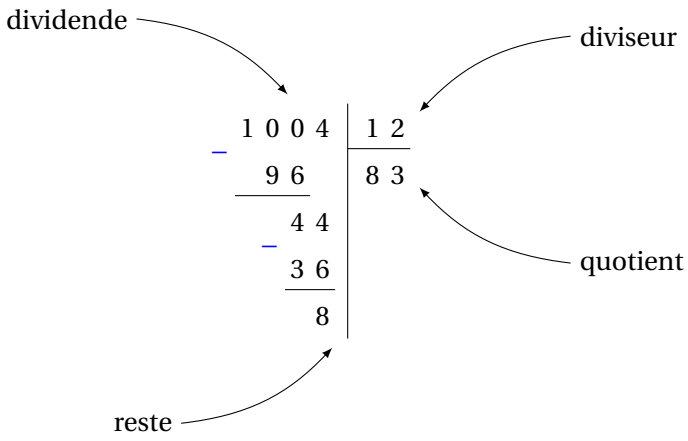
Définition 1 : *Division Euclidienne*

On considère deux entiers a, p. Si p n'est pas nul, on peut effectuer une division Euclidienne de a par p. Cela permet d'obtenir un quotient q et un reste $0 \leq r < p$ tels que

$$a = pq + r$$

Le reste r de la division de a par p est noté $a \pmod{p} = r$ ou $a\,[p] = r$.

Exemple :



Remarque 1 :

1. Si $a < p$ alors $a = a \pmod{p}$
2. Pour calculer $r = a \pmod{p}$ avec $a \in \mathbb{Z}$, on peut utiliser la formule suivante

$$r = a \pmod{p} = a - p \times E\left(\frac{a}{p}\right)$$

où $E(x)$ est la partie entière de x, c-à-d le plus grand entier inférieur ou égal à x. C-à-d l'unique entier relatif n (positif, négatif ou nul) tel que $n \leq x < n+1$

3. Si la division de a (positif) par p est $a = pq + r$, alors celle de $-a$ par p sera :

$$\begin{cases} -a = p(-q) & \text{Si} \quad r = 0 \\ -a = p(-q) - r = p(-q-1) + (p-r) & \text{Si} \quad r \neq 0 \quad \text{et donc} \quad p - r = -a \pmod{p} \end{cases}$$

Définition 2 : ***Congruences***

Soit $p \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo p si a et b ont le même reste de leur division euclidienne par p, autrement dit si p divise $a - b$. On note

$$a \equiv b \pmod{p} \quad \text{ou} \quad a \equiv b\ [p]$$

L'ensemble de tous les éléments de $\mathbb{Z}$ modulo p est noté $\mathbb{Z}/p\mathbb{Z}$.

Exemple : $25 = 4 \times 6 + 1$ et $37 = 6 \times 6 + 1$, donc $25 \equiv 1 \pmod{6}$ et $25 \equiv 37 \pmod{6}$.

Propriétés 1 :

1. Si $a \equiv b\ [p]$ alors $b \equiv a\ [p]$.
2. Si $a \equiv 0\ [p]$ alors p divise a.
3. Si $a \equiv r\ [p]$ et $0 \leq r < p$ alors $r = a\ [p]$.
4. $a \equiv b\ [p] \iff a - b$ est un multiple de p ou p divise $a - b$.
5. Si $a \equiv b\ [p]$ et si $b \equiv c\ [p]$ alors $a \equiv c\ [p]$.
6. Si $a \equiv b\ [p]$ et $a' \equiv b'\ [p]$ alors :
   - $a \pm a' \equiv b \pm b'\ [p]$.
   - $a \times a' \equiv b \times b'\ [p]$.
   - $a^n \equiv b^n\ [p]$.
7. Si $a \equiv b\ [p]$ alors $\forall c \in \mathbb{Z}$ on a $a \pm c \equiv b \pm c\ [p]$ et $ac \equiv bc\ [p]$.

Attention :

1. La relation de congruence n'est pas compatible avec la division, c-à-d

$$a \equiv b\ [p] \quad \text{et} \quad a' \equiv b'\ [p] \iff \frac{a}{a'} \equiv \frac{b}{b'}\ [p]$$

2. On ne peut pas simplifier les congruences, c-à-d

$$k \times a \equiv k \times b\ [p] \implies a \equiv b\ [p]$$

Par exemple : 45 et 63, multiples de 3 sont congrus à 0 modulo 3, donc $63 \equiv 45\ [3]$. En simplifiant par 9, on obtiendrait $7 \equiv 5\ [3]$. Or : $7-5=2$ qui n'est pas divisible par 3 et donc $7 \not\equiv 5\ [3]$

Remarque 2 :

Par unicité de la division Euclidienne de a par p, l'entier a ne peut être congru qu'à un seul entier compris entre 0 et p exclu. Cet entier étant le reste dans la division euclidienne de a par p et est considéré comme le représentant d'un ensemble de nombres qui lui sont congrus modulo p.

Par exemple : $25 = 4 \times 6 + 1$ et $37 = 6 \times 6 + 1$, donc $25 \equiv 1\ mod\ 6$ et $37 \equiv 1\ mod\ 6$; Ainsi, 1 est le représentant de 25 et 37.

Exercice : Déterminer le reste dans la division euclidienne de :

1. 54^{16} par 3
2. 21^{17} par 4

Réponse : L'idée ici est de trouver un représentant plus simple du nombre puis d'appliquer la puissance. Dans la plupart des cas, on pourra se contenter de prendre comme représentant le reste dans la division euclidienne.

1. On a $54 \equiv 0\ [3]$. Et comme la congruence est compatible avec la puissance, il vient $54^{16} \equiv 0\ [3]$. Donc le reste est 0.
2. On a $21 = 4 \times 5 + 1$. Donc $21 \equiv 1\ [4]$, d'où $21^{17} \equiv 1^{17}\ [4] \equiv 1\ [4]$. Le reste est donc 1.

Exercice : Trouver le reste de la division par 13 du nombre 100^{1000}.

Réponse : Il s'agit de calculer 100^{1000} modulo 13. Tout d'abord $100 \equiv 9$ [13] donc $100^{1000} \equiv 9^{1000}$ [13]. Or $9^2 \equiv 81 \equiv 3$ [13], $9^3 \equiv 9^2.9 \equiv 3.9 \equiv 1$ [13]. Dès que le reste est 1 le calcul devient facile. En effet, puisque $1000 = 3 \times 333 + 1$, il s'ensuit $100^{1000} \equiv 9^{1000} \equiv 9^{3.333+1} \equiv (9^3)^{333}.9 \equiv 1^{333}.9 \equiv 9$ [13]. Donc le reste est 9.

2 PGCD

Définition 3 :
Soit $a, b \in \mathbb{Z}$, le $\mathbf{pgcd}(a,b)$ est le plus grand diviseur commun de a et b.

Définition 4 : *Nombres premiers entre eux*
Soient $a, b \in \mathbb{N}^*$. a et b sont premiers entre eux si et seulement si $\mathbf{pgcd}(a,b) = 1$. On dit aussi que a est premier avec b.

Propriétés 2 :

1. $\mathbf{pgcd}(a,b) \leq a$ et $\mathbf{pgcd}(a,b) \leq b$.
2. Si b divise a alors $\mathbf{pgcd}(a,b) = b$.
3. $\mathbf{pgcd}(a,1) = 1$ et $\mathbf{pgcd}(a,0) = a$.
4. $\mathbf{pgcd}(k\,a, k\,b) = k\ \mathbf{pgcd}(a,b)$
5. Soient q et r le quotient et le reste de la division Euclidienne de a par b, c-à-d $a = bq + r$ alors
   - si $r = 0 \Longrightarrow \mathbf{pgcd}(a,b) = b$.
   - si $r \neq 0 \Longrightarrow \mathbf{pgcd}(a,b) = \mathbf{pgcd}(b,r)$.
6. (**Théorème de Gauss**) : Soient a, b et c trois entiers. Si $\mathbf{pgcd}(a,b) = 1$ et si a divise bc alors a divise c.

Exercice : Soit 3 entiers relatifs non nuls a, b et c. Montrer que si b et a sont premiers entre eux et divisent c, alors le produit ba divise c .

Réponse : b divise c donc il existe un entier relatif k tel que $c = kb$ et a divise c donc il existe un entier relatif k' tel que $c = k'a$. D'où $kb = k'a$. Ainsi, a divise kb, or b et a sont premiers entre eux, donc d'après le théorème de Gauss, a divise k. Alors il existe un entier relatif q tel que $k = aq$. Il s'ensuit alors $c = kb = baq$, d'où ba divise c.

Exercice : Montrer que si $\mathbf{pgcd}(p,q) = 1$ et si $x \equiv a$ [p] et $x \equiv a$ [q] alors $x \equiv a$ [pq].

Réponse : Si $x \equiv a\ [p]$ alors $x-a$ est divisible par p. De même $x \equiv a\ [q]$ entraîne $x-a$ divisible par q. Or p et q sont premiers entre eux donc d'après l'exercices précédent $x-a$ est divisible par pq. Ainsi $x \equiv a\ [pq]$.

2.1 Recherche du PGCD par l'algorithme d'Euclide

L'algorithme d'Euclide permet de calculer le **pgcd** de deux entiers naturels non nuls a et b avec $a \geq b$. On procède de la manière suivante :

- On effectue la division euclidienne de a par b. On note r le reste (on n'utilise pas le quotient).
- On remplace ensuite a par b et b par r.
- Tant que le reste est différent de 0, on réitère le procédé.

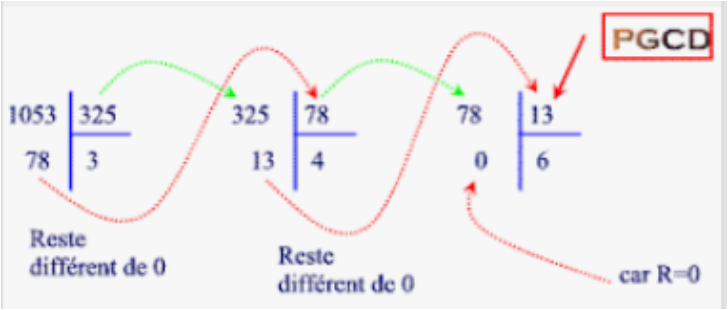
Après un certain nombre d'itérations, on obtiendra un reste égal à 0. Le **pgcd** de a et b est alors le reste précédent, c'est à dire **le dernier reste non nul**.

Formellement, l'algorithme d'Euclide construit une suite finie d'entiers r_k par récurrence double :

$$r_{k-1} = r_k \times q_k + r_{k+1}, \qquad r_0 = a,\ r_1 = b$$

r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k. La suite r_k est une suite strictement décroissante d'entiers positifs à partir du rang 1 : elle est donc finie et s'arrête au premier m tel que $r_m = 0$.

Exemple : On souhaite calculer le $\mathbf{pgcd(1053,325)}$. Voici en image les étapes de calcul



et voici les détails de calcul

$$\underset{r_0}{1053} = \underset{r_1}{325} \times \underset{q_1}{3} + \underset{r_2}{78}$$

$$\underset{r_1}{325} = \underset{r_2}{78} \times \underset{q_2}{4} + \underset{r_3}{13}$$

$$\underset{r_2}{78} = \underset{r_3}{13} \times \underset{q_3}{6} + \underset{r_4}{0}$$

Le $\mathbf{pgcd(1053,325)} = r_3 = 13$ et $m = 4$.

Exercice : On souhaite calculer le $\mathbf{pgcd(255,141)}$.

$$\underset{r_0}{255} = \underset{r_1}{141} \times \underset{q_1}{1} + \underset{r_2}{114}$$

$$\underset{r_1}{141} = \underset{r_2}{114} \times \underset{q_2}{1} + \underset{r_3}{27}$$

$$\underset{r_2}{114} = \underset{r_3}{27} \times \underset{q_3}{4} + \underset{r_4}{6}$$

$$\underset{r_3}{27} = \underset{r_4}{6} \times \underset{q_4}{4} + \underset{r_5}{3}$$

$$\underset{r_4}{6} = \underset{r_5}{3} \times \underset{q_5}{2} + 0$$

Le $\mathbf{pgcd(255,141)} = r_5 = 3$ et $m = 6$.

Théorème 1 : ***Théorème de Bézout***

Si $\mathbf{pgcd}(a,b) = d$ alors il existe $u, v \in \mathbb{Z}^*$ tels que :

$$au + bv = d$$

Etienne Bézout (1730 -1783)

Mathématicien français, célèbre pour le théorème de Bachet-Bézout lié aux équations diophantiennes en arithmétique et pour son théorème sur le nombre de points d'intersection de deux courbes algébriques, résultat crucial en géométrie algébrique.

Comment calculer les coefficients de Bézout ?

Algorithme d'Euclide généralisé

L'algorithme d'Euclide généralisé est un algorithme qui permet de calculer $d = \mathbf{pgcd}(a,b)$, ainsi que deux entiers u et v tels que $au + bv = d$, c'est-à-dire une relation de Bézout, de façon simultanée. On suppose $a \geq b > 0$.

On calcule une suite $r_0; r_1; \ldots r_k; \ldots$ de restes obtenus par divisions euclidiennes successives à partir de $r_0 = a$, $r_1 = b$. En effet, l'algorithme d'Euclide montre qu'il existe un rang n tel que $r_n \neq 0$ et

$r_{n+1} = 0$:

$$\begin{cases} r_0 = r_1 q_1 + r_2 \\ r_1 = r_2 q_2 + r_3 \\ \vdots \\ r_{n-2} = r_{n-1} \times q_{n-1} + r_n \\ r_{n-1} = r_n \times q_n + 0 \end{cases}$$

Ainsi, pour calculer u et v, on utilise deux autres suites d'entiers u_k et v_k définies de la façon suivante : on pose $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$ et pour $k \geq 1$

$$u_k = u_{k-2} - q_{k-1} u_{k-1}$$
$$v_k = v_{k-2} - q_{k-1} v_{k-1}$$

On a alors :

$$\boxed{d = \text{pgcd}(a,b) = r_n \quad \text{et} \quad au_n + bv_n = d}$$

Attention :

- n est le rang du dernier reste non nul.
- Puisque $a > b$ alors le coefficient u_n est toujours relatif au nombre le plus grand a et v_n est toujours relatif au nombre le plus petit b.

Exemple : Prenons l'exemple précédent. On souhaite calculer le $d = \text{pgcd}(255, 141)$ et les coefficients de Bézout u et v tels que :

$$255 \times u + 141 \times v = d$$

Comme précédemment, l'algorithme d' Euclide donne :

$$\underset{r_0}{255} = \underset{r_1}{141} \times \underset{q_1}{1} + \underset{r_2}{114}$$
$$\underset{r_1}{141} = \underset{r_2}{114} \times \underset{q_2}{1} + \underset{r_3}{27}$$
$$\underset{r_2}{114} = \underset{r_3}{27} \times \underset{q_3}{4} + \underset{r_4}{6}$$
$$\underset{r_3}{27} = \underset{r_4}{6} \times \underset{q_4}{4} + \underset{r_5}{3}$$
$$\underset{r_4}{6} = \underset{r_5}{3} \times \underset{q_5}{2} + 0$$

Ainsi, $\mathbf{pgcd(255,141) = r_5 = 3}$ et $\mathbf{n = 5}$. Il s'ensuit que $\mathbf{u = u_5}$ et $\mathbf{v = v_5}$. Il faut donc calculer $\mathbf{u_5}$ et $\mathbf{v_5}$. En effet, on a $\mathbf{u_0 = 1}$, $\mathbf{v_0 = 0}$, $\mathbf{u_1 = 0}$, $\mathbf{v_1 = 1}$ et

$$u_k = u_{k-2} - q_{k-1}u_{k-1}$$
$$v_k = v_{k-2} - q_{k-1}v_{k-1}$$

Ainsi

$$u_2 = u_0 - q_1u_1 = 1 - 1 \times 0 = 1 \qquad u_3 = u_1 - q_2u_2 = 0 - 1 \times 1 = -1$$
$$v_2 = v_0 - q_1v_1 = 0 - 1 \times 1 = -1 \qquad v_3 = v_1 - q_2v_2 = 1 - 1 \times (-1) = 2$$

$$u_4 = u_2 - q_3u_3 = 1 - 4 \times (-1) = 5 \qquad u_5 = u_3 - q_4u_4 = -1 - 4 \times 5 = -21$$
$$v_4 = v_2 - q_3v_3 = -1 - 4 \times 2 = -9 \qquad v_5 = v_3 - q_4v_4 = 2 - 4 \times (-9) = 38$$

Donc, $\mathbf{255 \times (-21) + 141 \times 38 = pgcd(255,141) = 3}$.

2.2 Inverses multiplicatifs modulo p

Définition 5 :
On dit que c est l'inverse de a modulo p si et seulement si

$$ac \equiv 1\ [p]$$

Remarque 3 :
D'après la Définition 5, si c est l'inverse de a modulo p alors a est l'inverse de c modulo p.

Théorème 2 :
Un entier a est inversible modulo p si et seulement si $\mathbf{pgcd}(a,p) = 1$.

Comment calculer l'inverse de a modulo p ?

Supposons que l'inverse a modulo p existe avec $a > p$, d'après le Théorème 2, forcement $\mathbf{pgcd}(a,p) = 1$. En appliquant l'algorithme d'Euclide généralisé on obtient un couple (u,v) tels que $au + pv = 1$. On a alors

$$1 = au + pv \implies au + pv\ [p] = 1\ [p] \implies au\ [p] + pv\ [p] = 1\ [p]$$

Or $pv\ [p] = 0$ car p divise pv. Il s'ensuit $au\ [p] = 1\ [p]$. D'où

$$au \equiv 1\ [p]$$

Ceci veut dire que $u \mod p$ est l'inverse de a modulo p.

Conclusion : Pour calculer l'inverse c de a modulo p, il faut calculer le coefficient de Bézout u relatif à a (car $a > p$) et faire $c = u \mod p$.

Remarque 4 :
Pour calculer l'inverse c' de p modulo a, il faut calculer le coefficient v relatif à p (car $p < a$) et faire $c' = v \mod a$.

Exemple : Inverse de 23 modulo 26 : On applique l'algorithme d'Euclide étendu pour trouver le $\text{pgcd}(23,26)$.

$$\underset{r_0}{26} = \underset{r_1}{23} \times \underset{q_1}{1} + \underset{r_2}{3}$$

$$\underset{r_1}{23} = \underset{r_2}{3} \times \underset{q_2}{7} + \underset{r_3}{2}$$

$$\underset{r_2}{3} = \underset{r_3}{2} \times \underset{q_3}{1} + \underset{r_4}{1}$$

$$\underset{r_3}{2} = \underset{r_4}{1} \times \underset{q_4}{2} + \underset{r_5}{0}$$

Ainsi, $\text{pgcd}(26,23) = r_4 = 1$ et $n = 4$. Donc, 23 est inversible modulo 26 et on a $u = u_4$ et $v = v_4$. Puisque $23 < 26$ d'après la remarque 4, l'inverse de 23 modulo 26 est donc $v_4 \mod 26$. Il faut donc calculer v_4. En effet,

$$v_2 = v_0 - q_1 v_1 = 0 - 1 \times 1 = -1$$

$$v_3 = v_1 - q_2 v_2 = 1 - 7 \times (-1) = 8$$

$$v_4 = v_2 - q_3 v_3 = -1 - 1 \times 8 = -9$$

Ainsi, l'inverse de 23 modulo 26 est $-9 \mod 26 = -9 - 26 \times E\left(\frac{-9}{26}\right) = -9 - 26 \times (-1) = 17$.

Exercice : Calculer l'inverse de 17 modulo 59

Réponse : On applique l'algorithme d'Euclide étendu pour trouver le **pgcd(17,59)**.

$$\underset{r_0}{59} = \underset{r_1}{17} \times \underset{q_1}{3} + \underset{r_2}{8}$$

$$\underset{r_1}{17} = \underset{r_2}{8} \times \underset{q_2}{2} + \underset{r_3}{1}$$

$$\underset{r_2}{8} = \underset{r_3}{1} \times \underset{q_3}{8} + \underset{r_4}{0}$$

Ainsi, $\mathbf{pgcd(17,59)} = r_3 = \mathbf{1}$ et $n = \mathbf{3}$. Donc, **17** est inversible modulo **59** et puisque $\mathbf{17 < 59}$ d'après la remarque 4, l'inverse de **17** modulo **59** est donc $v_3 \mod \mathbf{59}$. Il faut donc calculer v_3. En effet,

$$v_2 = v_0 - q_1 v_1 = \mathbf{0 - 3 \times 1 = -3}$$

$$v_3 = v_1 - q_2 v_2 = \mathbf{1 - 2 \times (-3) = 7}$$

Ainsi, l'inverse de **17** modulo **59** est $\mathbf{7 \mod 59 = 7}$.

3 Nombres premiers

Définition 6 :
Soit $a \in \mathbb{N}^*$, a est premier si $a \geq 2$ et n'est divisible que par **1** et par lui-même.

Propriétés 3 :

1. Il existe une infinité de nombres premiers.
2. Soit $a \in \mathbb{N}^*$ alors :
   - a possède au moins un diviseur premier.
   - a peut s'écrire sous la forme

     $$a = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_s^{k_s}$$

     où les entiers p_i sont premiers et vérifient $p_1 < p_2 < \cdots < p_s$. Les entiers k_i sont strictement positifs
   - si a n'est pas premier alors au moins un des diviseurs premier de a est inférieur à $\sqrt{a}$.
3. (**Lemme d'Euclide**) Soient b et c deux entiers. Si un nombre premier p divise le produit bc, alors p divise b ou c.

Remarque 5 :

D'après la propriété 2, pour montrer qu'un nombre entier est premier, il suffit de vérifier qu'il n'est divisible par aucun nombre premier inférieur ou égal à sa racine carrée.

Théorème 3 : ***Petit théorème de Fermat***

Soit p un nombre premier:

- **Enoncé 1 :** Si a est un entier non divisible par p, alors :

  $$a^{p-1} \equiv 1 \ [p]$$

- **Enoncé 2 :** Si a est un entier quelconque, alors :

  $$a^p \equiv a \ [p]$$

Exercice : Soit p un nombre premier. Démontrer que, pour tout entier naturel n, $3^{n+p} - 3^{n+1}$ est divisible par p.

Réponse : Puisque p est un nombre premier, le petit théorème de Fermat implique $3^p \equiv 3\ [p]$. Donc pour tout entier naturel n on a

$$3^n \times 3^p \equiv 3^n \times 3\ [p] \iff 3^{n+p} \equiv 3^{n+1}\ [p] \iff 3^{n+p} - 3^{n+1} \equiv 0\ [p]$$

Par conséquent $3^{n+p} - 3^{n+1}$ est divisible par p.

3.1 Indicateur d'Euler

On considère l'ensemble suivant : $E_n = \{0, 1, \cdots, n-1\}$.

Théorème 4 :

1. Soit $a \in E_n$, alors a est inversible si et seulement si $\text{pgcd}(a, n) = 1$ (Théorème 2).
2. Si n est premier alors chaque élément de E_n est inversible sauf 0.

Définition 7 : *Indicateur d'Euler*

On note $\phi(n)$ le nombre d'éléments inversibles de E_n. On l'appelle l'indicateur d'Euler.

Propriétés 4 : *Soient $n, m \in \mathbb{N}$.*

1. Si n est premier alors $\phi(n) = n - 1$
2. Si $\text{pgcd}(n, m) = 1$ alors $\phi(m \times n) = \phi(m) \times \phi(n)$
3. Si n et m sont premiers alors $\phi(n \times m) = (n-1)(m-1)$
4. Si $a \in E_n$ est inversible alors $a^{\phi(n)} \equiv 1\ [n]$ (Théorème d'Euler).

Exercice : calculer $16^{216} \mod 247$.

Réponse : On a $247 = 13 \times 19$ et $\text{pgcd}(19, 13) = 1$. Il vient $\phi(247) = \phi(19) \times \phi(13) = 12 \times 18 = 216$ car 19 et 13 sont premiers. D'autre part, on a $\text{pgcd}(16, 247) = 1$ et $16 \in E_{247}$, donc 16 est inversible modulo 247. Le théorème d'Euler indique donc $16^{\phi(247)} \equiv 1\ [247]$ soit $16^{216} \equiv 1\ [247]$.

3.2 Test de primalité

Un test de primalité est un algorithme permettant de savoir si un nombre entier est premier.

Méthode naïve

Le test le plus simple est le suivant : pour tester n, on vérifie s'il est divisible par l'un des entiers compris entre 2 et $n-1$. Si la réponse est négative, alors n est premier, sinon il est composé.
Plusieurs changements permettent d'améliorer les performances de cet algorithme :

- il suffit de tester tous les nombres de 2 à $\sqrt{n}$ seulement, puisque si $n = pq$ alors $p \leq q$ et donc $p^2 \leq pq = n$, c'est-à-dire $p \leq \sqrt{n}$.
- on peut encore diviser par deux le travail en ne testant que les nombres impairs, une fois que la divisibilité par deux a échoué,

Complexité: Ce test de primalité exécute $\sqrt{n}/2$ divisions, soit en base 2 : $2^{\frac{\log_2(n)-1}{4}}$. Pour des entiers représentables sur 32 chiffres binaires, la complexité ne dépasse donc pas 215 divisions, qui peuvent être effectuées en quelques millisecondes sur une machine moderne.
Si l'on dispose de fonctions pour effectuer des opérations exactes sur des entiers de longueur quelconque, il est hors de question d'appliquer cet algorithme à des nombres ayant beaucoup plus de chiffres; si n s'écrit avec 50 chiffres décimaux, le temps d'exécution dépasse l'âge de l'univers.

Test de Fermat

Rappel :

$$\text{Si } A \Longrightarrow B \quad \text{alors} \quad non\ B \Longrightarrow non\ A$$

Le petit théorème de Fermat énonce que, si p est premier, et si a n'est pas un multiple de p alors :

$$p \text{ est premier} \Longrightarrow a^{p-1} \equiv 1\ [p]$$

Pour tester si p est premier, on peut donc choisir $a < n$ (a est appelé base du test), par exemple $a = 2$, et calculer $a^{p-1}\ [p]$; si le résultat est différent de 1, p est certainement composite; par contre, on ne peut rien conclure de façon sûre si le résultat vaut 1, car la réciproque du petit théorème de Fermat est fausse : il y a seulement une assez forte probabilité pour que p soit premier. En recommençant le test pour d'autres valeurs de la base a on améliore en général fortement la probabilité d'obtenir une réponse correcte, lorsque p semble premier.

Exercices pour les TD

Exercice 1: Test de primalité de Lucas-Lehmer

Partie A

Pour tout entier naturel $k \geqslant 2$, on pose $M_k = 2^k - 1$. On dit que M_k est le k-ième nombre de **Mersenne**.

1. **a.** Reproduire et compléter le tableau suivant, qui donne quelques valeurs de M_k :

k	2	3	4	5	6	7	8	9	10
M_k	3								

On calcule M_k pour quelques valeurs de k:

k	2	3	4	5	6	7	8	9	10
M_k	3	7	15	31	63	127	255	511	1023

b. D'après le tableau précédent, si k est un nombre premier, peut-on conjecturer que le nombre M_k est premier ?

Pour $k=2$ premier, $M_2=3$ est premier. Pour $k=3$ premier, $M_3=7$ est premier. Pour $k=5$ premier, $M_5=31$ est premier. Pour $k=7$ premier, $M_7=127$ est premier.
D'après ce tableau, on peut conjecturer que si k est premier, alors M_k est premier.

2. Soient p et q deux entiers naturels non nuls. On admet que

$$1+2^p+\left(2^p\right)^2+\left(2^p\right)^3+\cdots+\left(2^p\right)^{q-1}=\frac{(2^p)^q-1}{2^p-1}$$

a. Montrer que $2^{pq}-1$ est divisible par 2^p-1.

Le nombre $1+2^p++(2^p)^2+(2^p)^3+\cdots(2^p)^{q-1}$ est entier et, d'après la question précédente, $\left(1+2^p++(2^p)^2+(2^p)^3+\cdots(2^p)^{q-1}\right)\times(2^p-1)=2^{pq}-1$ donc $2^{pq}-1$ est divisible par 2^p-1.

b. En déduire que si un entier k supérieur ou égal à 2 n'est pas premier, alors M_k ne l'est pas non plus.

Soit k un nombre non premier; alors il existe deux entiers strictement plus grands que 1 tels que $k=pq$.
$M_k=2^k-1=2^{pq}-1$ est divisible par 2^p-1 qui est strictement plus grand que 1: donc M_k n'est pas premier.

3. **a.** Prouver que le nombre de Mersenne M_{11} n'est pas premier.

$M_{11}=2^{11}-1=2047=23\times89$ donc M_{11} n'est pas premier.

b. Que peut-on en déduire concernant la conjecture de la question 1. b. ?

La conjecture de la question **1.b.** est donc fausse: 11 et premier et M_{11} ne l'est pas.

Partie B

Le test de **Lucas-Lehmer** permet de déterminer si un nombre de Mersenne donné est premier. Ce test utilise la suite numérique (u_n) définie par $u_0=4$ et pour tout entier naturel n

$$u_{n+1}=u_n^2-2.$$

Si n est un entier naturel supérieur ou égal à 2, le test permet d'affirmer que :

Le nombre M_n est premier si et seulement si $u_{n-2} \equiv 0 \pmod{M_n}$

Cette propriété est admise dans la suite.

1. Utiliser le test de Lucas-Lehmer pour vérifier que le nombre de Mersenne M_5 est premier.

D'après le test de Lucas-Lehmer, M_5 est premier si et seulement si $u_3 \equiv 0 \pmod{M_5}$.

$M_5 = 31$; $u_0 = 4$; $u_1 = u_0^2 - 2 = 14$; $u_2 = u_1^2 - 2 = 194$; $u_3 = u_2^2 - 2 = 37634 = 31 \times 1214$.

Donc u_3 est divisible par M_5 donc le test de Lucas-Lehmer est vérifié pour $k = 5$.

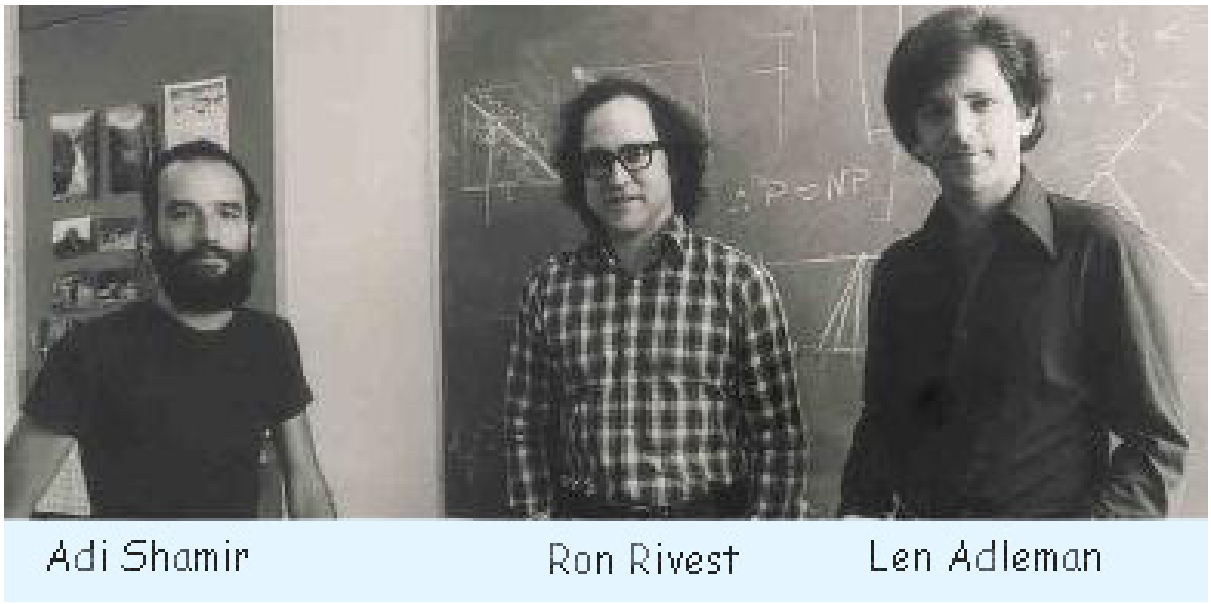
2. Soit n un entier naturel supérieur ou égal à 3. L'algorithme suivant permet de vérifier si le nombre de Mersenne M_n est premier, en utilisant le test de Lucas-Lehmer:

Variables :	u, M, n et i sont des entiers naturels
Initialisation :	u prend la valeur 4
Traitement :	Demander un entier $n \geqslant 3$
	M prend la valeur .....
	Pour i allant de 1 à ... faire
	u prend la valeur ...
	Fin Pour
	Si M divise u alors afficher M .....
	sinon afficher M .....

Recopier et compléter cet algorithme de façon à ce qu'il remplisse la condition voulue.

Variables:	u, M, n et i sont des entiers naturels
Initialisation:	u prend la valeur **4**
Traitement:	Demander un entier $n \geqslant 3$
	M prend la valeur $2^n - 1$
	Pour i allant de 1 à $n-2$ faire
	u prend la valeur $u^2 - 2$
	Fin Pour
	Si M divise u alors afficher " M est premier "
	sinon afficher " M n'est pas premier "

Chiffrement RSA



Introduction :

Le système de chiffrement RSA a été inventé en 1978 par Ron Rivest, Adi Shamir et Len Adleman à la suite de la découverte de la cryptographie à clé publique par Diffie et Hellman. C'est le premier chiffrement (cryptage) dit asymétrique (clé publique, clé privée). Son invention est due au hasard : au départ, Rivest, Shamir et Adleman voulaient prouver que tout système à clé publique possédait une faille.

Le système RSA est un système utilisé dans plusieurs applications comme les télécommunications, les transactions sécurisée sur Internet, la finance et les cartes a puce.

la sécurité du système RSA repose en grande partie sur la difficulté de factoriser les grand nombres entiers.

Principe : ***Alice et Bob sont choisis pour expliciter le principe***

Choix des clefs : 

Si Bob désire que l'on puisse communiquer avec lui de façon secrète, il procède de la manière suivante :

1. Bob engendre deux grands nombres premiers p et q (test de primalité).
2. Il calcule $n = p \times q$, donc $\phi(n) = (p-1)(q-1)$ où ϕ est l'indicateur d'Euler.
3. Il choisit un nombre aléatoire e avec $1 < e < \phi(n)$ tel que $\text{pgcd}(e, \phi(n)) = 1$.
4. Il calcule l'inverse de e modulo $\phi(n)$, noté d, c'est-à-dire : $d \times e \equiv 1 \mod \phi(n)$ (Algorithme d'Euclide généralisé).
5. Bob publie (n, e) (clef publique) et garde d qui forme la clef secrète.

Chiffrement : 

Alice veut envoyer un message converti en nombre M à Bob. Elle procède de la manière suivante:

1. Elle découpe M en partie M_i de même longueur telle que $M_i < n$.
2. Elle chiffre chaque partie M_i avec la clef publique (e, n) de Bob, c'est-à-dire :

$$M_i^e \mod (n) = C_i$$

3. Elle rassemble les parties C_i pour former la chaine cryptée $C = (C_1, C_2, \cdots)$.
4. Elle envoie C à Bob.

Déchiffrement : 

Bob reçoit C et redécoupe le message crypté C en formant des blocs C_i. Il décrypte ensuite chaque C_i en utilisant sa clef secrète d par:

$$C_i^d \mod (n) = M_i$$

Il rassemble enfin les parties M_i pour retrouver le message M.

Démonstration :

Rappel : Si $\mathbf{pgcd}(p,q) = 1$ et si $x \equiv a\ [p]$ et $x \equiv a\ [q]$ alors $x \equiv a\ [pq]$.

Il faut montrer que

$$C^d \equiv (M^e)^d \equiv M^{ed} \mod n \equiv M \mod n = M$$

En effet, comme p et q sont deux grands nombres premiers, et puisque M n'est pas un multiple de p et q (car $M < p$ et $M < q$) alors d'après le petit théorème de Fermat :

$$M^{p-1} \equiv 1 \mod p\,, \qquad M^{q-1} \equiv 1 \mod q$$

Or

$$ed \equiv 1 \mod \underbrace{(p-1)(q-1)}_{\phi(n)}$$

ce qui signifie qu'il existe un entier k tel que

$$ed = k(p-1)(q-1) + 1$$

Ainsi, si M n'est pas multiple de p d'après le petit théorème de Fermat

$$M^{ed} \mod p = M^{1+k(p-1)(q-1)} \mod p = M \times \left(M^{p-1}\right)^{k(q-1)} \mod p = M \mod p$$

De même, si M n'est pas multiple de q

$$M^{ed} = M \mod q$$

Finalement, d'après le rappel et $n = pq$

$$M^{ed} \equiv M \mod \underbrace{pq}_{n} = M$$

car $M < n = pq$.

Sécurité de RSA

La sécurité de l'algorithme RSA repose sur la difficulté à factoriser n. Pour déchiffrer le message, il est nécessaire de trouver d connaissant e, ce qui nécessite de calculer $\phi(n)$, et donc de connaître p et q, les deux facteurs premiers de n.
Or, la factorisation d'un entier (de très grande taille) en facteurs premiers est un problème difficile, c'est-à-dire qu'il n'existe pas d'algorithme rapide (de complexité polynomiale) pour résoudre cette question.

Exemple

Données de Bob: $p = 53$, $q = 97$ et donc $n = 5141 = 53 \times 97$ et $\phi(n) = (53-1)(97-1) = 4992$. $e = 7$ premier avec $\phi(n)$. Ainsi $d = 4279$.

Alice veut donc envoyer un message "JEVOUSAIME" à Bob. Elle cherche dans l'annuaire la clef de chiffrement que Bob a publié et trouve $n = 5141$ et $e = 7$. Elle transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet. Ainsi, "JEVOUSAIME" devient :

$$M = 10\,05\,22\,15\,21\,19\,01\,09\,13\,05$$

Puis elle découpe son message numérique en blocs de même longueur représentant chacun un nombre plus petit que n. Par exemple pour des blocs de longueur 3 son message devient

$$M = \underbrace{010}_{M_1}\ \underbrace{052}_{M_2}\ \underbrace{215}_{M_3}\ \underbrace{211}_{M_4}\ \underbrace{901}_{M_5}\ \underbrace{091}_{M_6}\ \underbrace{305}_{M_7}$$

Chaque bloc M_i est chiffré par la formule $C_i = M_i^e \mod (n)$, par exemple

$$010^7 \mod (5141) = 0755 = C_1$$

$$052^7 \mod (5141) = 1324 = C_2$$

Après avoir chiffré chaque bloc, le message chiffré s'écrit :

$$C = \underbrace{0755}_{C_1}\ \underbrace{1324}_{C_2}\ \underbrace{2823}_{C_3}\ \underbrace{3550}_{C_4}\ \underbrace{3763}_{C_5}\ \underbrace{2237}_{C_6}\ \underbrace{2052}_{C_7}$$

Déchiffrement: Quand Bob reçoit le message chiffré $C = 0755\ 1324\ 2823\ 3550\ 3763\ 2237\ 2052$, il déchiffre avec sa clef secrète chacun des blocs C_i du message chiffré par la formule $M_i = C_i^d \mod (n)$. Par exemple :

$$0755^{4279} \mod (5141) = 10 = M_1$$

$$1324^{4279} \mod (5141) = 52 = M_2$$

Il trouve enfin le message clair:

$$M = 010\,052\,215\,211\,901\,091\,305$$

En regroupant les chiffres deux par deux et en remplaçant les nombres ainsi obtenus par les lettres correspondantes, il sait que Alice l'aime secrètement **" M=JE VOUS AIME "**.

Mise en oeuvre pratique de RSA

Même si le protocole RSA est assez simple, sa mise en œuvre pose toutefois quelques problèmes pour Alice et Bob. En effet, les deux protagonistes se trouvent confrontés au problème d'élever de façon efficace un **gros** nombre à une **grosse** puissance, modulo n comme dans l'exemple précédent $1324^{4279} \mod (5141)$.

Idée: Prenons un exemple simple, sans se préoccuper pour le moment de **mod**. Pour calculer a^{128}, il est maladroit d'effectuer les **127** produits successifs qui définissent la puissance. Pour avoir le résultat, il vaut mieux procéder ainsi: calcul de $a^2 = \alpha_1$, puis de $a^4 = (\alpha_1)^2 = \alpha_2$, $a^8 = (\alpha_2)^2 = \alpha_3$, $a^{16} = (\alpha_3)^2 = \alpha_4$, $a^{32} = (\alpha_4)^2 = \alpha_5$, $a^{64} = (\alpha_5)^2 = \alpha_6$ et enfin $a^{128} = (\alpha_6)^2 = \alpha_7$, ce qui ne demandera que **7** élévations au carré successives.

Question: Que se passe-t-il si l'exposant n'est pas une puissance de 2 ?

Réponse: La méthode peut toujours être mise en œuvre car écrire un nombre sous la forme d'une somme de puissances de **2** revient à décomposer ce nombre dans la base **2**.

Principe

Examinons par exemple ce que l'on obtiendrait pour calculer $5^{1063} \mod (2159)$. Procédons par étapes.

Étape 1 : On décompose **1063** en base **2**, en procédant à des divisions successives par **2**.

1063	2
1	531 | 2
1	265 | 2
1	132 | 2
0	66 | 2
0	33 | 2
1	16 | 2
0	8 | 2
0	4 | 2
0	2 | 2
0	1 | 2
1	0

Ainsi, le nombre en base **2** s'écrit en partant des derniers restes obtenus soit

$$\mathbf{1063} = \underset{\downarrow 10}{1}\,\underset{}{0}\,\underset{}{0}\,\underset{}{0}\,\underset{}{0}\,\underset{\downarrow 5}{1}\,\underset{\downarrow 4}{0}\,\underset{\downarrow 3}{0}\,\underset{\downarrow 2}{1}\,\underset{\downarrow 1}{1}\,\underset{\downarrow 0}{1}$$

d'où l'on déduit la décomposition de **1063** en somme de puissances de **2** : (il faut compter le nombre de bits en allant de la droite vers la gauche et en commençant par **0**)

$$\mathbf{1063 = 2^0 + 2^1 + 2^2 + 2^5 + 2^{10} = 1 + 2 + 4 + 32 + 1024}$$

Étape 2 : Par suite, d'après les propriétés des puissances, on peut écrire :

$$\mathbf{5^{1063} = 5^{1+2+4+32+1024} = 5 \times 5^2 \times 5^4 \times 5^{32} \times 5^{1024}}$$

Étape 3 : On procède ensuite à des élévations au carré successives à partir de **5** :

$$\boxed{\mathbf{5}};\boxed{\mathbf{5^2}};\boxed{\mathbf{5^4}};\mathbf{5^8};\mathbf{5^{16}};\boxed{\mathbf{5^{32}}};\mathbf{5^{64}};\mathbf{5^{128}};\mathbf{5^{256}};\mathbf{5^{512}};\boxed{\mathbf{5^{1024}}}$$

Il suffit maintenant de faire le produit de ces entiers, éventuellement modulo **2159**, pour avoir le résultat cherché.

$$\begin{aligned}
\mathbf{5} &\equiv \mathbf{5} \mod (2159)\\
\mathbf{5^2} &\equiv \mathbf{5 \times 5} \mod (2159) \equiv \mathbf{25}\\
\mathbf{5^4} &\equiv \mathbf{5^2 \times 5^2} \mod (2159) \equiv \mathbf{25 \times 25} \mod (2159) \equiv \mathbf{625}\\
\mathbf{5^8} &\equiv \mathbf{5^4 \times 5^4} \mod (2159) \equiv \mathbf{625 \times 625} \mod (2159) \equiv \mathbf{2005}\\
\mathbf{5^{16}} &\equiv \mathbf{5^8 \times 5^8} \mod (2159) \equiv \mathbf{2005 \times 2005} \mod (2159) \equiv \mathbf{2126}\\
\mathbf{5^{32}} &\equiv \mathbf{5^{16} \times 5^{16}} \mod (2159) \equiv \mathbf{2126 \times 2126} \mod (2159) \equiv \mathbf{1089}\\
\mathbf{5^{64}} &\equiv \mathbf{5^{32} \times 5^{32}} \mod (2159) \equiv \mathbf{1089 \times 1089} \mod (2159) \equiv \mathbf{630}\\
\mathbf{5^{128}} &\equiv \mathbf{5^{64} \times 5^{64}} \mod (2159) \equiv \mathbf{630 \times 630} \mod (2159) \equiv \mathbf{1803}\\
\mathbf{5^{256}} &\equiv \mathbf{5^{128} \times 5^{128}} \mod (2159) \equiv \mathbf{1803 \times 1803} \mod (2159) \equiv \mathbf{1514}\\
\mathbf{5^{512}} &\equiv \mathbf{5^{256} \times 5^{256}} \mod (2159) \equiv \mathbf{1514 \times 1514} \mod (2159) \equiv \mathbf{1497}\\
\mathbf{5^{1024}} &\equiv \mathbf{5^{512} \times 5^{512}} \mod (2159) \equiv \mathbf{1497 \times 1497} \mod (2159) \equiv \mathbf{2126}
\end{aligned}$$

Il ne reste qu'à rassembler

$$\begin{aligned} 5^{1063} \mod (2159) &= 5^{1+2+4+32+1024} \mod (2159) \\ &= 5 \times 5^2 \times 5^4 \times 5^{32} \times 5^{1024} \mod (2159) \\ &= 5 \times 25 \times 625 \times 1089 \times 2126 \mod (2159) \\ &= 588 \end{aligned}$$

Le tableau suivant résume les calculs.

Remarque: Dans le tableau, on s'intéresse uniquement à ceux qui sont entourés, qui permettent d'obtenir

$$5^{1063} \mod (2159) = 5 \times 5^2 \times 5^4 \times 5^{32} \times 5^{1024} \mod (2159)$$

Remarquons qu'ils correspondent en fait à des bits égaux à **1**. C'est la raison pour laquelle on ne cumule dans la colonne **4** que le calcul modulo **2159** de ces valeurs.

1063 en base 2	élévat au carré successives	carrés mod n=2159	Résultat modulo n=2159
1	5	**5**	**5**
1	5^2	**25**	$5 \times 25 \mod (n) = 125$
1	5^4	**625**	$125 \times 625 \mod (n) = 401$
0	5^8	**2005**	Rien faire
0	5^{16}	**2126**	Rien faire
1	5^{32}	**1089**	$401 \times 1089 \mod (n) = 571$
0	5^{64}	**630**	Rien faire
0	5^{128}	**1803**	Rien faire
0	5^{256}	**1514**	Rien faire
0	5^{512}	**1497**	Rien faire
1	5^{1024}	**2126**	$571 \times 2126 \mod (n) = 588$

Voici le pseudo code de cette méthode.

Pseudo-code: Exponentiation modulaire rapide

Algorithme 1 Calcul de $y = x^p \mod (n)$

Entrées: $n \geq 2, x > 0, p \geq 2$
Sortie: $y = x^p \mod (n)$

Début
$p = (d_{k-1}; d_{k-2}; \cdots; d_1; d_0)$ % Écriture de p en base 2
$R_1 \leftarrow 1$
$R_2 \leftarrow x$

Traitement
Pour $i = 0; \cdots; k-1$ **Faire**
  Si $d_i == 1$ **Alors**
    $R_1 \leftarrow R_1 \times R_2 \mod (n)$ % Calcul de la colonne 4 du tableau si le bit est 1
  Fin Si
  $R_2 \leftarrow R_2^2 \mod (n)$ % carré modulo n de la colonne 3 du tableau
Fin Pour

Exemple

On désire calculer $41^{37} \mod (527)$. On a $p = 37 =$, $x = 41$ et $n = 527$

Début:

$$37 = 100101$$

$$R_1 = 1$$

$$R_2 = 41$$

Traitement: (On lit les bits de droite à gauche)

- Le premier bit est 1, donc
  - R_1 prend la valeur $R_1 \times R_2 \mod (527) = 1 \times 41 \mod (527) = 41$
  - R_2 devient $R_2^2 \mod (527) = 41^2 \mod (527) = 100$
- Le $2^{\text{ème}}$ bit est 0, donc
  - $R_1 = 41$ reste inchangé
  - R_2 devient $R_2^2 \mod (527) = 100^2 \mod (527) = 514$
- Le $3^{\text{ème}}$ bit est 1, donc
  - R_1 prend la valeur $R_1 \times R_2 \mod (527) = 41 \times 514 \mod (527) = 521$
  - R_2 devient $R_2^2 \mod (527) = 514^2 \mod (527) = 169$

- Le $\mathbf{4}^{\text{ème}}$ bit est **0**, donc
  - $\boldsymbol{R_1 = 521}$ reste inchangé
  - $\boldsymbol{R_2}$ devient $\boldsymbol{R_2^2 \mod (527) = 169^2 \mod (527) = 103}$
- Le $\mathbf{5}^{\text{ème}}$ bit est **0**, donc
  - $\boldsymbol{R_1 = 521}$ reste inchangé
  - $\boldsymbol{R_2}$ devient $\boldsymbol{R_2^2 \mod (527) = 103^2 \mod (527) = 69}$
- Le dernier bit est **1**, donc
  - $\boldsymbol{R_1}$ prend la valeur $\boldsymbol{R_1 \times R_2 \mod (527) = 521 \times 69 \mod (527) = 113}$
- **Fin**

Conclusion: $\mathbf{41^{37} \mod (527) = 113}$

Signature RSA

4 Introduction

Tout comme la signature manuscrite que l'on appose sur un document, la signature électronique (ou numérique) permet de valider la conformité d'un document. Elle ne doit pas être confondue avec la signature numérisée faite par exemple avec un stylet sur une tablette même si cette dernière est aussi reconnue légalement depuis 2010. Un système de signature numérique requiert la mise en place de sécurités informatiques faisant appel à la cryptographie.
la signature électronique permet à quelqu'un de prouver qu'il est celui qu'il prétend être ou qu'il a le droit d'accéder à un service. C'est la fonction réalisée par exemple lors d'une connexion à un ordinateur à l'aide d'un mot de passe où lorsque l'on tape le code secret de sa carte bancaire.

5 Principe

Tout d'abord, remarquons qu'une signature manuscrite est physiquement liée au document signé mais qu'une signature numérique ne peut pas l'être de la même manière. Par conséquent, il faut trouver un moyen d'associer la signature numérique au message. Pour cela, le principe est de construire une signature qui dépendra du signataire mais aussi du contenu du message de sorte qu'une signature valide ne puisse pas être utilisée avec un autre message que le message signé initialement. D'une manière générale, une signature électronique devra être :

- authentique : elle convainc le destinataire que le signataire a délibérément signé un document;
- infalsifiable;
- non réutilisable : elle est attachée à un document donné et ne pourra pas être utilisée sur un document différent;
- inaltérable : toute modification du document doit être détectable;
- non reniable : le signataire ne peut répudier le document signé.

Principe :

Données: Alice (n_A, e_A, d_A). Bob (n_B, e_B, d_B).

Alice souhaite envoyer un message M à Bob d'une manière secrète mais elle veut aussi que Bob soit sûr que le message vient bien d'elle. Pour ceci, elle effectue les opérations suivantes :

1. Elle génère d'abord la signature du message par sa clef secrète comme:

$$S = M^{d_A} \ mod(n_A)$$

on aura remarqué qu'elle est la seule à pouvoir générer cette signature étant la seule à posséder d_A.

2. Elle chiffre ensuite S et M par la clef publique de Bob comme :

$$C_s = S^{e_B} \ mod(n_B)$$

$$C = M^{e_B} \ mod(n_B)$$

3. Le document signé est alors le couple (C, C_s) et est envoyé à Bob.

Lorsque Bob reçoit le document signé (C, C_s), il déchiffre d'abord C_s par sa clef secrète d_B pour trouver la signature S du message:

$$S = C_s^{d_B} \ mod(n_B)$$

Ensuite, il vérifie l'authenticité de la signature par récupération du message M par la clef publique d'Alice (n_A, e_A) et sa clef secrète d_B comme :

$$C^{d_B} \ mod(n_B) = M = S^{e_A} \ mod(n_A)$$

Si, au contraire, $C^{d_B} \ mod(n_B) \neq S^{e_A} \ mod(n_A)$, alors la signature n'est pas valide.

Remarque importante : Si la confidentialité n'est pas sollicitée, Alice envoie simplement le couple (M, S) c-à-d, elle envoie le message M et sa signature S.

Exemple : Un professeur envoie ses notes au secrétariat de l'école par mail. La clef publique du professeur est $(e_p, n_p) = (3, 55)$, celle du secrétariat $(e_s, n_s) = (3, 33)$.

1. Déterminer la clef privée du professeur et du secrétariat de l'école.
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 15 ?
3. Pour assurer l'authenticité de ses messages, le professeur signe chaque note. Le secrétariat reçoit ainsi le message $(C = 24, C_s = 29)$. Quelle est la note correspondante ?