Chiffrement RSA

On commence par récapituler toute l'arithmétique des entiers, connue depuis la L1, et sans faire appel à la théorie des groupes. On détaille ensuite un exemple pratique de chiffrement RSA, et on explique les mathématiques se trouvant derrière à l'aide de la première partie.

I - Arithmétique dans $\mathbb{Z}$

1. Divisibilité dans $\mathbb{Z}$

Définition 1. Soient a et b deux entiers relatifs. On dit que b **divise** a (ou que a est un **multiple** de b) s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. On note ceci par $b \mid a$.

Exemple 2.
— $6 = 2 \times 3$ donc 2 et 3 sont des diviseurs de 6. Les diviseurs dans $\mathbb{N}$ de 6 sont : 1, 2, 3 et 6.
— $-52 = (-4) \times 13$ donc -4, 4, -13 et 13 sont des diviseurs de -52. Les diviseurs dans $\mathbb{Z}$ de -52 sont : -52, -26, -13, -4, -2, -1, 1, 2, 4, 13, 26 et 52.

Proposition 3.
(i) Tout entier relatif b divise 0 (car $0 = 0 \times b$).
(ii) 1 divise tout entier relatif a (car $a = a \times 1$).
(iii) Si $c \mid a$ et $c \mid b$ alors $c \mid (au + bv)$ pour tout $u, v \in \mathbb{Z}$.

Démonstration. Montrons le dernier point : il existe k, k' tels que $a = kc$ et $b = k'c$. Donc $ua + vb = ukc + vk'c = (uk + vk')c$. D'où $c \mid (au + bv)$. □

Définition 4. Un nombre entier $p \geq 2$ est dit **premier** si ses seuls diviseurs positifs sont 1 et lui-même.

Exemple 5. 2, 3, 5, 7, 11 et 13 sont des nombres premiers et il en existe une infinité.

2. Division euclidienne

Théorème 6 (Division euclidienne dans $\mathbb{Z}$)**.** Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. On appelle **division euclidienne** de a par b, l'opération qui à (a, b), associe le couple d'entiers (q, r) tel que $a = bq + r$ où $0 \leq r < b$. Un tel couple existe forcément et est unique.

Démonstration. Si $a < b$, alors il suffit de prendre $q = 0$ et $r = a$. Nous supposerons donc dans la suite $a \geq b$.

— Existence : On note S l'ensemble des entiers naturels s qui s'écrivent $s = a - tb$ où $t \in \mathbb{N}$. Cet ensemble est non vide (car il contient a) et comme c'est un sous-ensemble de $\mathbb{N}$, il admet un plus petit élément $r = a - qb$. On a forcément $r < b$ (sinon $a - (q+1)b$ serait dans S et serait plus petit que r). Donc $0 \leq a - qb < b$ et ce couple (q, r) vérifie les conditions données par le théorème.

— Unicité : On suppose qu'il existe un deuxième couple (q', r') vérifiant les conditions du théorème. On a $a = bq + r = bq' + r'$, donc $b(q - q') = r - r'$. Comme $0 \leq r < b$ alors $-b < -r \leq 0$. De plus $0 \leq r' < b$, donc en additionnant les inégalités on a $-b < r' - r < b$. Comme $b \mid r - r'$ on a $r - r' = 0$ (i.e. $r = r'$) et donc $q = q'$. D'où $(q', r') = (q, r)$.

□

Définition 7. En reprenant les notations du théorème, a s'appelle le **dividende**, b le **diviseur**, q le **quotient** et r le **reste** de la division euclidienne.

Remarque 8. Il est possible d'étendre le principe de la division euclidienne aux entiers relatifs. La condition pour le reste r devient alors $0 \leq r < |b|$.

Exemple 9. On souhaite effectuer la division euclidienne de 314 par 7. Détaillons étape par étape :

— On cherche combien de fois 7 est contenu dans 31 (cela ne sert à rien de commencer par 3 car $3 < 7$). On a $4 \times 7 = 28$ et $5 \times 7 = 35$ donc, on écrit 4 sous le diviseur et le reste $31 - 28 = 3$. Puis, on abaisse le chiffre des unités qui est 4.

— On recommence : combien de fois 7 est-il contenu dans 34 ? Comme $4 \times 7 = 28$ et $5 \times 7 = 35$, 7 est contenu 4 fois dans 34 et il reste $34 - 28 = 6$.

— Comme $6 < 7$, la division euclidienne est terminée : on a $314 = 7 \times 44 + 6$.

Donnons, pour finir, une propriété qui nous sera utile dans la sous-section suivante.

Proposition 10. Soit $n \in \mathbb{N}^*$. Deux entiers relatifs a et b ont le même reste dans la division euclidienne par n si et seulement si $a - b$ est un multiple de n.

Démonstration. Supposons que a et b ont le même reste dans la division euclidienne par n i.e. $a = qn + r$ et $b = q'n + r$. Alors par différence, $a - b = (q - q')n$ donc $a - b$ est un multiple de n.

Réciproquement, si $a - b$ est un multiple de n alors il existe k tel que $a - b = kn$. En effectuant la division euclidienne de a par n, on a $a = qn + r$, d'où $nq + r - b = kn$. Ainsi, $b = (q - k)n + r$ avec $0 \leq r < q - k$, ce que l'on voulait. □

Voici également un énoncé qui sera utilisé par la suite. C'est un corollaire du théorème de théorème de Bézout.

Proposition 11 (Corollaire du théorème de Bézout)**.** Soient a et b deux entiers naturels non nuls premiers entre eux. Alors, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Démonstration. On note par S l'ensemble des entiers naturels strictement positifs s qui s'écrivent $s = na + mb$ où $n, m \in \mathbb{Z}$. Cet ensemble est non-vide (car il contient a) et comme c'est un sous-ensemble de $\mathbb{N}$, il admet un plus petit élément $d = au + bv > 0$.

— On a $1 \mid d$ (car $1 \mid a$ et $1 \mid b$) donc $1 \leq d$.

— Faisons la division euclidienne de a par d : on a $a = dq + r \iff r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq)$ donc $r = 0$ (car sinon on aurait $r \in S$ mais $r < d$ et d est le plus petit élément de S). Donc d divise a et par le même raisonnement, d divise b. Donc d divise leur plus grand diviseur commun positif qui est 1. Donc $d \leq 1$.

D'où finalement $d = 1$. □

Remarque 12. Il est possible de trouver de tels entiers u et v en effectuant la division euclidienne de a par b, puis de b par le reste de la division précédente, etc…et en remontant. Il s'agit de la remontée de **l'algorithme d'Euclide**.

Corollaire 13. Soient a et b deux entiers naturels non nuls premiers entre eux. Soit $c \in \mathbb{Z}$ tel que $a \mid c$ et $b \mid c$. Alors $ab \mid c$.

Démonstration. On écrit $c = ka$ et $c = k'b$. De plus, par le Proposition 11, il existe u et v tels que $au + bv = 1$. En multipliant l'égalité par c, on obtient $c = auc + bvc = au(k'b) + bv(ka) = ab(k'u + kv)$. D'où le résultat. □

Lemme 14 (Euclide)**.** Soit p un nombre premier et a et b deux entiers. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Démonstration. Soit p un nombre premier tel que $p \mid ab$. Supposons que p ne divise pas a. Alors comme p est premier, ses seuls diviseurs sont 1 et p. Comme a n'est pas divisible par p, le plus grand diviseur commun positif à a et p est 1. Donc par le Proposition 11 il existe $u, v \in \mathbb{Z}$ tels que $au + pv = 1$. En multipliant par b on obtient $\underbrace{abu}_{\text{Multiple de } p} + \underbrace{pbv}_{\text{Multiple de } p} = b$. Ainsi $p \mid b$. □

3. Congruences dans $\mathbb{Z}$

Dans toute cette sous-section, on fixe un entier naturel $n \geq 2$.

Définition 15. On dit que deux entiers relatifs a et b sont **congrus** modulo n si a et b ont le même reste dans la division euclidienne par n. On note alors $a \equiv b \mod n$.

Remarque 16. On remarque que a est un multiple de n si et seulement si $a \equiv 0 \mod n$.

On signale que la congruence est une **relation d'équivalence**.

Proposition 17. Pour tout $a, b, c \in \mathbb{Z}$:

(i) $a \equiv a \mod n$ (**réflexivité**)

(ii) Si $a \equiv b \mod n$, alors $b \equiv a \mod n$ (**symétrie**)

(iii) Si $a \equiv b \mod n$, et si $b \equiv c \mod n$, alors $a \equiv c \mod n$ (**transitivité**)

De plus, le congruence est compatible avec les opérations usuelles sur les entiers relatifs.

Théorème 18. Soient a, b, c et $d \in \mathbb{Z}$ tels que $a \equiv b \mod n$ et $c \equiv d \mod n$. Alors on a la compatibilité avec :

(i) L'**addition** : $a + c \equiv b + d \mod n$.

(ii) La **multiplication** : $ac \equiv bd \mod n$.

(iii) Les **puissances** : pour tout $k \in \mathbb{N}$, $a^k \equiv b^k \mod n$.

Démonstration. (i) Comme $a \equiv b \mod n$, et $c \equiv d \mod n$, alors $(a-b)$ et $(c-d)$ sont des multiples de n. Donc il existe deux entiers relatifs k et k' tels que $a - b = kn$ et $c - d = k'n$. En additionnant ces deux égalités on trouve que $(a+c) - (b+d) = (k+k')n$. Donc par la Remarque 16, $a + c \equiv b + d \mod n$.

(ii) Comme précédemment, on a $a - b = kn$ et $c - d = k'n$. En multipliant les deux égalités on trouve que $ac = (b+kn)(d+k'n) = bd + (k'b + kd + kk'n)n$. Donc par la Remarque 16, $ac \equiv bd \mod n$.

(iii) On utilise la compatibilité avec la multiplication : $a \equiv b \mod n$ et $a \equiv b \mod n$ donc $a^2 \equiv b^2 \mod n$. De même, on a $a^3 \equiv b^3 \mod n$. Il suffit de répéter l'opération k fois et on a $a^k \equiv b^k \mod n$.

□

Exemple 19. Comme $7 \equiv 3 \mod 4$, et $5 \equiv 1 \mod 4$, on a $35 = 5 \times 7 \equiv 1 \times 5 \mod 4$.

Nous utiliserons le résultat suivant dans la sous-section suivante.

Théorème 20 (Petit théorème de Fermat)**.** Soit p un nombre premier et a un entier quelconque. Alors $a^p \equiv a \mod p$.

Démonstration. Soit p un nombre premier et soit a tel que p ne divise pas a. Notons :

— $N = a \times 2a \times 3a \times \cdots \times (p-1)a$.

— r_k le reste de la division euclidienne de ka par p pour tout $k \in \mathbb{N}$ tel que $1 \leq k \leq p-1$.

— $(p-1)! = 1 \times 2 \times \ldots \times p-1$.

Montrons que $N = (p-1)!a^{p-1}$. Il suffit en fait de réordonner les facteurs de N :

$$N = a \times 2a \times \cdots \times (p-1)a = 1 \times 2 \times 3 \times \cdots \times (p-1) \times a \times a \times \cdots \times a = (p-1)!a^{p-1} \qquad (*)$$

De plus, r_k est le reste de la division euclidienne de ka par p donc $ka \equiv r_k \mod p$. Par $(*)$, $N = a \times 2a \times \cdots \times (p-1)a \equiv r_1 r_2 \ldots r_{p-1} \mod p$. $0 \leq k \leq p-1 < p$, donc k ne peut pas être divisible

par p. Ainsi, par le Lemme 14, ka n'est pas divisible par p et donc $r_k \neq 0$.

Soit i tel que $1 \leq i \leq p-1$ et $r_i = r_k$. Montrons que $(i-k)a$ est divisible par p. Comme r_i et r_k sont respectivement le reste de la division euclidienne de ia et ka par p, on a $r_i - r_k = 0 \equiv (i-k)a \mod p$ donc $(i-k)a$ est divisible par p. Comme p ne divise pas a, par le Lemme 14, on a $i-j$ divise p. Et comme $-p < i-j < p$, on en déduit que $i = j$.

Pour tout k, on a $1 \leq r_k \leq p-1$. De plus, par ce qui précède, on a $p-1$ r_k qui sont tous différents les uns des autres. Donc $\{r_1, r_2, \dots, r_{p-1}\} = \{1, 2, \dots, p-1\}$ Ainsi, $r_1 r_2 \dots r_{p-1} = (p-1)!$.

Enfin, on a $N = (p-1)!a^{p-1} = a \times 2a \times \cdots \times (p-1)a \equiv r_1 r_2 \dots r_{p-1} \mod p$ et $r_1 r_2 \dots r_{p-1} \equiv (p-1)! \mod p$, donc, on a $N \equiv (p-1)! \mod p$. De par la définition des congruences modulo p, on a $N-(p-1)!$ divisible par p et $N-(p-1)! = (p-1)!(a^{p-1}-1)$. Comme p divise $(p-1)!(a^{p-1}-1)$ mais que pour tout $k \in \mathbb{N}$ tel que $1 \leq k \leq p-1$, p ne divise pas k, alors, en appliquant le Lemme 14 à chaque facteur de $(p-1)!$, il en résulte que p divise $a^{p-1}-1$.

Pour conclure, comme $a^{p-1}-1 \equiv 0 \mod p$ alors $a^{p-1} \equiv 1 \mod p$ et donc $a^p \equiv a \mod p$. Nous venons de montrer que pour tout a non divisible par p, on a $a^p \equiv a \mod p$. Soit maintenant b un entier divisible par p. Alors $b \equiv 0 \mod p$ et donc $b^p \equiv 0^p \equiv 0 \mod p$. D'où $b^p \equiv b \mod p$. □

Exemple 21. Cherchons le reste de la division euclidienne de 2019^5 par 5.

Posons $a = 2019$ et $p = 5$. En faisant la division euclidienne de a par p, on a $a = 403p + 4$ donc $a \equiv 4 \mod p$. Donc $a^p \equiv a \equiv 4 \mod p$.

II - RSA par un exemple

1. Calcul de le clé publique et de la clé privée

Alice souhaite envoyer un code à Bob et uniquement à lui à travers un groupe de messagerie. Pour éviter de communiquer son code à tous les autres membres du groupe de messagerie, ils cherchent donc un moyen pour que seul Bob soit capable de le lire et de le déchiffrer : ils vont employer la méthode de chiffrement **RSA**.

Ce chiffrement se base sur le choix de deux nombres premiers p et q distincts. On pose alors $n = pq$ et $N = (p-1)(q-1)$, puis on choisit $e < N$ premier avec N.

Définition 22. Le couple (n, e) est la **clé publique** de ce chiffrement et est utilisée pour chiffrer des nombres, des caractères, des mots, ...

Pour déchiffrer un nombre, on détermine deux entiers u et v vérifiant $ue + vN = 1$ (ils existent par le Proposition 11). On pose d comme le reste de la division euclidienne de u par N.

Définition 23. Le triplet (p, q, d) est la **clé privée** du chiffrement.

Dans notre exemple, c'est Bob qui va générer la clé publique et la clé privée. Ainsi, il choisit $p = 5$, $q = 7$ (donc $n = 35$ et $N = 24$) et $e = 5$. Comme $5e - N = 1$, alors $d = u = 5$.

Il communique sa clé publique (qui est $(35,5)$) dans la conversation et garde bien précieusement sa clé privée (qui est $(5,7,5)$).

2. Chiffrement du code

Le code d'Alice est 2743, elle le décompose en chacun de ses chiffres : $a_0 = 2$, $a_1 = 7$, $a_3 = 4$ et $a_4 = 3$. Pour tout k, elle calcule ensuite b_k qui est le reste de la division euclidienne de a_k^e par n. Ainsi, elle obtient :

a_k	2	7	4	3
b_k	32	7	9	33

Par conséquent, elle écrit dans la conversation :

32 7 9 33

À titre d'exemple, pour calculer b_1, il s'agit de calculer le reste de la division euclidienne de $a_1^5 = 7^5$ par $n = 35$. On peut, par exemple, procéder comme ceci :

— $7^2 = 49 \equiv 14 \mod 35$

— $7^3 = 7^2 \times 7 \equiv 28 \equiv -7 \mod 35$

— $7^5 = 7^3 \times 7^2 \equiv -98 \equiv 7 \mod 35$

3. Déchiffrement du code

Bob a donc reçu, une suite de quatre nombres (b_k) avec $b_0 = 32$, $b_1 = 7$, $b_2 = 9$ et $b_3 = 33$. Pour déchiffrer la suite (b_k) en une suite (a_k), il s'agit alors pour tout k, de calculer le reste de la division euclidienne de b_k^d par n. Ce reste est a_k. Ainsi, dans le cadre de notre exemple, cela nous donne :

b_k	32	7	9	33
a_k	2	7	4	3

Le code déchiffré est donc :

2 7 4 3

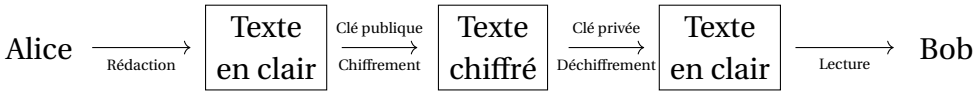
Ce qui correspond bien au code qu'Alice a voulu transmettre. De plus, seul Bob connaît le nombre d qui permet de déchiffrer le code. Leur objectif est donc atteint.

L'algorithme RSA est dit "asymétrique" car pour chiffrer un message, il suffit de connaître la clé publique (n,e). Cependant, pour déchiffrer un message, il faut connaître n et d. Or, d se calcule à partir de e et n en trouvant les nombres premiers p et q qui divisent n. Donc finalement, pour

déchiffrer un message, il faut connaître la clé privée (p, q, d).

Dans cet exemple, les nombres p et q ont été choisis petits de manière à simplifier les calculs, mais si on souhaitait mettre en place cet algorithme de chiffrement dans un cadre plus sécuritaire, il faudrait ainsi choisir des nombres p et q beaucoup plus grands.

Le chiffrement demande donc de pouvoir vérifier que de très grands nombres sont des nombres premiers, pour pouvoir trouver p et q, mais aussi que le produit de ces deux très grands nombres, ne soit pas factorisable pratiquement. En effet les algorithmes efficaces connus qui permettent de vérifier qu'un nombre n'est pas premier ne fournissent pas de factorisation.



III - Explication mathématique

Soient p et $q \geq 2$ des nombres premiers distincts.

Notation 24. On note $n = pq$ et $N = \varphi(n) = (p-1)(q-1)$.

Proposition 25. Soit e un entier premier avec N soit 1. Alors il existe $d < N$ tel que $de \equiv 1 \mod N$.

Démonstration. En effet, par le Proposition 11, il existe u et $v \in \mathbb{Z}$ tels que $ue + vN = 1$. Donc, on a $ue = 1 - vN$ et ainsi $ue \equiv 1 - vN \equiv 1 \mod N$. Il suffit alors de poser d le reste de la division euclidienne de u par N. □

Montrons enfin que ce chiffrement est valide.

Proposition 26. Soit M un entier naturel strictement inférieur à n que nous souhaitons (dé-)chiffrer. On pose C le reste de la division euclidienne de M^e par n. Alors, $M \equiv C^d \mod n$.

Démonstration. On a $C^d \equiv (M^e)^d \equiv M^{ed} \mod n$ et $ed \equiv 1 \mod N$ donc il existe k tel que $ed = Nk + 1$. Comme p et q sont deux nombres premiers, alors par le Théorème 20, on a $M^{p-1} \equiv 1 \mod p$ et $M^{q-1} \equiv 1 \mod q$. Donc $M^{ed} = M^{Nk+1} = M(M^{p-1})^{k(q-1)} \equiv M \mod p$. En faisant le même raisonnement, on a $M^{ed} \equiv M \mod q$. Ainsi, $M^{ed} - M$ est un multiple de p et de q (deux premiers distincts), donc aussi de n par le Corollaire 13. On conclue que $M \equiv M^{ed} \equiv C^d \mod n$. □