Université d'Aix-Marseille
Institut Universitaire de Technologie
Département Télécommunications et Réseaux

Arithmétique pour le cryptage

Table des matières

1 Résolution d'équations diophantiennes

1.1 Calcul du plus grand commun diviseur de deux entiers

1.1.1 Un exemple

Pour calculer le plus grand commun diviseur de $a = 1179$ *et* $b = 126$, *effectuons les divisions euclidiennes suivantes :*

$$\begin{cases} 1179 &= 126 \times 9 &+ 45 \\ 126 &= 45 \times 2 &+ 36 \\ 45 &= 36 \times 1 &+ 9 \\ 36 &= 9 \times 4 &+ 0. \end{cases}$$

Le plus grand commun diviseur de a *et* b, *noté* $a \wedge b$, *est le dernier reste non nul de cette suite de divisions euclidiennes :*

$$1179 \wedge 126 = 9.$$

Démonstration.

- *9 divise bien* a *et* b *car, si l'on remonte la suite des divisions, on voit que 9 divise 36, donc comme 9 divise 9, 9 divise la somme* $45 = 36 \times 1 + 9$. *Ainsi, comme 9 divise 36 et 45, il divise la somme* $45 \times 2 + 36$ *soit* $\underbrace{126}_{b}$, *donc 9 divise la somme* $126 \times 9 + 45$, *soit finalement* $\underbrace{1179}_{a}$.
- *Tout diviseur* c *de* a *et de* b *divise forcément* 9. *En effet,* c *divisant* a *et* b *est diviseur de* $45 = a - 126 \times b$, *donc de* $36 = b - 45 \times 2$, *soit finalement de* $9 = 45 - 36$. ∎

Ce résultat se généralise facilement grâce à l'algorithme d'Euclide.

1.1.2 Algorithme d'Euclide

Proposition 1.1 *Soient* $a \geq b > 0$ *deux entiers. Alors le plus grand commun diviseur de* a *et* b *est le dernier reste non nul de la suite de divisions euclidiennes suivantes :*

$$\begin{cases} a &= bq_0 &+ r_1 \\ b &= r_1 q_1 &+ r_2 \\ r_1 &= r_2 q_2 &+ r_3 \\ \vdots &\vdots &\vdots \quad \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} &+ r_n \\ r_{n-1} &= r_n q_n &+ 0. \end{cases}$$

Remarque 1.1 *L'algorithme d'Euclide permet d'écrire* $\frac{a}{b}$ *sous forme de* $fraction\ continue$ *:*

$$\frac{a}{b} = q_0 + \frac{r_1}{b} \text{ avec } b = r_1 q_1 + r_2,$$

donc

$$\frac{a}{b} = q_0 + \underbrace{\frac{r_1}{r_1 q_1 + r_2}}_{\frac{1}{q_1 + \frac{r_2}{r_1}}} \text{ avec } r_1 = r_2 q_2 + r_3,$$

donc

$$\frac{a}{b} = q_0 + \underbrace{\frac{1}{q_1 + \frac{r_2}{r_2 q_2 + r_3}}}_{\frac{1}{q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}}}} \text{ avec } r_2 = r_3 q_3 + r_4,$$

soit finalement

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}}.$$

Ainsi pour l'exemple du §1.1.1 :

$$\frac{1179}{126} = 9 + \frac{1}{2 + \frac{1}{1 + \frac{1}{4}}}.$$

On vérifie bien que

$$9 + \frac{1}{2 + \frac{1}{\frac{5}{4}}} = 9 + \frac{1}{2 + \frac{4}{5}} = 9 + \frac{5}{14} = \frac{131}{14} = \frac{131}{14} \times \frac{9}{9} = \frac{1179}{126}.$$

1.2 Théorème de Bezout

1.2.1 Primalité

Deux entiers relatifs a *et* b *sont dits* $premiers\ entre\ eux$ *si* $a \wedge b = 1$.
Ainsi 14 *et* 131 *sont premiers entre eux puisque l'on a :*

$$\begin{cases} 131 &= 14 \times 9 &+ 5 \\ 14 &= 5 \times 2 &+ 4 \\ 5 &= 4 \times 1 &+ 1 \\ 4 &= 1 \times 4 &+ 0. \end{cases}$$

On remarque ensuite que l'avant dernière égalité se réécrit :

$$1 = 5 - \underbrace{4}_{14-5\times 2} \times 1,$$

soit

$$1 = \underbrace{5}_{131-14\times 9} \times 3 - 14,$$

ce qui donne finalement

$$1 = 3 \times \underbrace{131}_{a} - 28 \times \underbrace{14}_{b}.$$

En fait, il est possible de généraliser ce résultat comme suit :

Théorème 1.1 *(de Bezout). Quels que soient $a, b \in \mathbb{Z}^*$, on a l'équivalence*

$$a \wedge b = 1 \Longleftrightarrow \exists \alpha, \beta \in \mathbb{Z}\,,\ \alpha a + \beta b = 1.$$

Démonstration.

1. $\underline{\Leftarrow}$. *Supposons qu'il existe $\alpha, \beta \in \mathbb{Z}$ tel que $\alpha a + \beta b = 1$. Si c est un diviseur commun de a et b, il divise forcément $\alpha a + \beta b$, donc il divise 1. Par suite $a \wedge b = 1$.*
2. $\underline{\Rightarrow}$. *Réciproquement, supposons que $a \wedge b = 1$. D'après l'algorithme d'Euclide, on a :*

$$\begin{cases} a &= bq_0 &+ r_1 \\ b &= r_1 q_1 &+ r_2 \\ r_1 &= r_2 q_2 &+ r_3 \\ \vdots &\vdots &\vdots \\ r_{n-3} &= r_{n-2} q_{n-2} &+ r_{n-1} \\ r_{n-2} &= r_{n-1} q_{n-1} &+ \underbrace{r_n}_{1} \\ r_{n-1} &= r_n q_n &+ 0. \end{cases}$$

L'avant-dernière équation donne

$$1 = \underbrace{(-q_{n-1})}_{\alpha_{n-1}} r_{n-1} + \underbrace{1}_{\beta_{n-1}} \times r_{n-2},$$

donc, comme $r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}$,

$$1 = \underbrace{(\beta_{n-1} - \alpha_{n-1} q_{n-2})}_{\alpha_{n-2}} r_{n-2} + \underbrace{\alpha_{n-1}}_{\beta_{n-2}} r_{n-3}.$$

Ainsi, de proche en proche, on construit pour tout indice k de 1 à $n-2$, des coefficients entiers α_{n-k} et β_{n-k} vérifiant

$$1 = \alpha_{n-k} r_{n-k} + \beta_{n-k} r_{n-k-1}.$$

En particulier, si $k = n-2$:

$$1 = \alpha_2 \underbrace{r_2}_{b - q_1 r_1} + \beta_2 r_1,$$

donc

$$1 = (\beta_2 - \alpha_2 q_1) \underbrace{r_1}_{a - b q_0} + \alpha_2 b,$$

d'où finalement :

$$1 = \underbrace{(\beta_2 - \alpha_2 q_1)}_{\alpha} a + \underbrace{[\alpha_2 - (\beta_2 - \alpha_2 q_1) q_0}_{\beta} b. \blacksquare$$

1.2.2 Lemme de Gauss

Le fait que 131 soit premier avec 14 était prévisible. Ceci résulte en fait des égalités $131 = \frac{1179}{9}$ et $14 = \frac{131}{9}$ tirées de l'exemple du §1.1.1 ainsi que de l'implication

$$c = a \wedge b \Longrightarrow \frac{a}{c} \wedge \frac{b}{c} = 1. \qquad (1)$$

En effet, si d est un diviseur commun à $\frac{a}{c}$ et $\frac{b}{c}$ alors cd divise simultanément a et b, donc d ne peut qu'être égal à 1 (puisque c est le plus grand commun diviseur de a et b). Par suite le plus grand commun diviseur de $\frac{a}{c}$ et $\frac{b}{c}$ est 1.

Corollaire 1.1 *Soient $a, b \in \mathbb{Z}^*$. Alors il existe α et β dans $\mathbb{Z}$ tels que*

$$\alpha a + \beta b = a \wedge b.$$

Démonstration.
Posons $c = a \wedge b$. On déduit immédiatemment du théorème 1.1 et de l'implication (1) l'existence de α et β dans $\mathbb{Z}$ tels que

$$\alpha \frac{a}{c} + \beta \frac{b}{c} = 1.$$

Il suffit ensuite de multiplier cette égalité par c. $\blacksquare$

Corollaire 1.2 *(Lemme de Gauss). Quels que soient $p, q, r \in \mathbb{Z}^*$, on a l'implication :*

$$\left.\begin{array}{l} p \wedge q = 1 \\ p \text{ divise } qr \end{array}\right\} \Longrightarrow p \text{ divise } r.$$

Démonstration.
Comme $p \wedge q = 1$, le théorème 1.1 garantit l'existence de α et β dans $\mathbb{Z}$ tels que $\alpha p + \beta q = 1$, donc en multipliant par r :

$$\alpha pr + \beta qr = r.$$

Or, p divise qr donc il existe $\gamma \in \mathbb{Z}$, tel que $qr = \gamma p$, d'où

$$\underbrace{\alpha pr + \beta\gamma p}_{(\alpha r + \beta\gamma)p} = r.$$

Donc p divise r. ∎

1.3 Equations diophantiennes linéaires

Il s'agit de trouver toutes les solutions $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ d'équations de la forme

$$a_1x_1 + a_2x_2 + \ldots a_nx_n = b, \qquad (2)$$

où les coefficients $a_1, a_2, \ldots, a_n$ et b appartiennent à $\mathbb{Z}$.

1.3.1 Résolution d'équations diophantiennes linéaires à 2 inconnues

On s'intéresse ici plus particulièrement aux équations diophantiennes du type

$$ax + by = c, \qquad (3)$$

les inconnues étant notées (x, y) plutôt que (x_1, x_2).

Proposition 1.2 *L'équation (3) admet une solution $(x, y) \in \mathbb{Z}^2$ si et seulement si $d = a \wedge b$ divise c. Dans ce cas, (x_0, y_0) désignant une solution particulière de (3), l'ensemble des solutions de cette équation est :*

$$\left\{(x, y) = (x_0 - k\frac{b}{d}, y_0 + k\frac{a}{d}),\ k \in \mathbb{Z}\right\}.$$

Démonstration.
Pour démontrer l'équivalence

$$(3) \text{ admet une solution} \Longleftrightarrow d \text{ divise } c,$$

posons $a' = \frac{a}{d}$ *et* $b' = \frac{b}{d}$*, et remarquons ensuite que si* (x, y) *est solution de (3) alors,*

$$d\underbrace{(a'x + b'y)}_{\in \mathbb{Z}} = c,$$

ce qui montre que d *divise* c*.*
Réciproquement, supposons que d *divise* c*. En vertu de l'implication (1),* $a' \wedge b' = 1$*, donc le théorème 1.1 garantit l'existence d'entiers* α *et* β *tels que*

$$\alpha a' + \beta b' = 1.$$

En multipliant par c*, on obtient ainsi :*

$$\underbrace{a'c\alpha}_{a \times \frac{c}{d}\alpha} + \underbrace{b'c\beta}_{b \times \frac{c}{d}\beta} = c,$$

ce qui prouve de $(x, y) = (\frac{c}{d}\alpha, \frac{c}{d}\beta)$ *est solution de (3).*
Enfin, lorsque (x_0, y_0) *est solution de (3), n'importe quelle solution* (x, y) *de (3) satisfait*

$$ax + by = ax_0 + by_0 = c,$$

soit

$$a'x + b'y = a'x_0 + b'y_0 = \frac{c}{d} \in \mathbb{Z}\,.$$

Ainsi, $a'(x - x_0) = -b'(y - y_0)$ *donc* b' *divise* $a'(x - x_0)$*. Comme* $a' \wedge b' = 1$*, le lemme de Gauss implique que* b' *divise* $x - x_0$*. Il existe donc* $k \in \mathbb{Z}$ *, tel que* $x - x_0 = kb'$*, soit* $x = x_0 + k\frac{b}{d}$*. Par suite,* $y = y_0 - \underbrace{\frac{a'}{b'}}_{\frac{a}{b}}(x - x_0) = y_0 - k\frac{a}{d}$*. Donc toute solution de (3) est nécessairement de la forme*

$$(x, y) = (x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}), k \in \mathbb{Z}\,.$$

Réciproquement, il est clair que tout couple (x, y) *de la forme précédente est bien solution de (3).* ∎

Exemple.
Trouver les solutions entières de $1179x + 126y = 72$*.*

Comme $1179 \wedge 126 = 9$ *divise* 72*, l'équation précédente possède des solutions entières.*

$$\left.\begin{array}{rcl} \frac{1179}{9} & = & 131 \\ \frac{126}{9} & = & 14 \end{array}\right\} \text{Th. de Bezout} \Longrightarrow 1 = 3 \times 131 - 28 \times 14,$$

donc, en multipliant par 9,

$$9 = 3 \times 1179 - 28 \times 126,$$

soit, en multipliant enfin par 8 :

$$72 = 24 \times 1179 - 224 \times 126.$$

Une solution particulière est donc $(x_0, y_0) = (24, -224)$.
Ensuite, il vient, en vertu de la proposition 1.2 :

$$\begin{array}{cc} & (x,y) \in \mathbb{Z}^2 \text{ satisfait } 1179x + 126y = 72 \\ \iff & 1179(x - x_0) = 126(y - y_0) \\ \iff & \left\{ \begin{array}{rcl} x & = & x_0 + 14k \\ y & = & y_0 - 131k, \end{array} \right. \end{array}$$

où $k \in \mathbb{Z}$.

1.3.2 Résolution d'équations diophantiennes linéaires à $n \geq 3$ inconnues

On revient au cas général en cherchant les solutions entières de (2).
Le plus grand commun diviseur de $a_1, a_2, \ldots, a_n$ *sera noté* $a_1 \wedge a_2 \wedge \ldots \wedge a_n$. *Cet entier est en fait défini par récurrence sur* n *grâce à l'égalité*

$$a_1 \wedge a_2 \wedge \ldots \wedge a_n = (a_1 \wedge a_2 \wedge \ldots \wedge a_{n-1}) \wedge a_n,$$

qui ramène le calcul pratique de $a_1 \wedge a_2 \wedge \ldots \wedge a_n$ *à* $n - 1$ *applications de l'algorithme d'Euclide.*

Proposition 1.3 *L'équation (2) admet une solution* $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ *si et seulement si l'entier* $d = a_1 \wedge a_2 \wedge \ldots \wedge a_n$ *divise* b.

Démonstration.
<u>La condition est nécessaire.</u> En effet, si $(x_1, x_2, \ldots, x_n)$ *est une solution entière de (2) alors, en posant* $a'_i = \frac{a_i}{d}$ *pour tout* i *de 1 à* n, *on a :*

$$d \underbrace{(a'_1 x_1 + a'_2 x_2 + \ldots + a'_n x_n)}_{\in \mathbb{Z}} = b,$$

ce qui montre que d *divise* b.
<u>La condition est suffisante.</u> On procède par récurrence sur n. *Le résultat étant acquis pour* $n = 2$, *supposons que l'équation* $a'_1 x_1 + a'_2 x_2 + \ldots + a'_{n-1} x_{n-1} = y$, $y \in \mathbb{Z}$, *possède une solution entière* $(x_1, x_2, \ldots, x_{n-1})$ *dès lors que* $d' = a_1 \wedge a_2 \wedge \ldots \wedge a_{n-1}$ *divise* y *(hypothèse dite "de récurrence", notée* (HR) *dans la suite). Alors,*

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = \underbrace{a_1 x_1 + a_2 x_2 + \ldots + a_{n-1} x_{n-1}}_{d'\left(a'_1 x_1 + a'_2 x_2 + \ldots + a'_{n-1} x_{n-1}\right)} + a_n x_n = d'y + a_n x_n = b,$$

en posant $y = a'_1x_1 + a'_2x_2 + \ldots + a'_{n-1}x_{n-1}$. *Par suite :*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \Longleftrightarrow \left\{ \begin{array}{lrcl} (a) & d'y + a_nx_n & = & b \\ (b) & a'_1x_1 + a'_2x_2 + \ldots + a'_{n-1}x_{n-1} & = & y. \end{array} \right.$$

Comme $d = d' \wedge a_n$ *divise* b, (a) *possède une solution entière* (y, x_n). *Ensuite,* $a'_1 \wedge a'_2 \wedge \ldots \wedge a'_{n-1} = \frac{a_1}{d'} \wedge \frac{a'_2}{d'} \wedge \ldots \wedge \frac{a'_{n-1}}{d'} = 1$ *divise* y *donc* (HR) *montre que* (b) *a bien une solution entière.* ■

Exemple.
Résoudre dans $\mathbb{Z}$ *l'équation* $1024x_1 + 1536x_2 + 243x_3 = 1$.

On a $1024 \wedge 1536 = 512$ *et* $1024x_1 + 1536x_2 = 512\underbrace{(2x_1 + 3x_2)}_{y}$, *donc*

$$1024x_1 + 1536x_2 + 243x_3 = 1 \Longleftrightarrow \left\{ \begin{array}{lrcrcl} (a) & 512y & + & 243x_3 & = & 1, \\ (b) & 2x_1 & + & 3x_2 & = & y. \end{array} \right.$$

Résolution de (a). *Comme* $512 \wedge 243 = 1$, *l'équation* (a) *possède des solutions entières :*

$$(y, x_3) = (-28 + 243k, 59 - 512k),\ k \in \mathbb{Z}\,.$$

Résolution de (b). *L'équation* $2x_1 + 3x_2 = 1$ *admet* $(x_1, x_2) = (-1, 1)$ *comme solution particulière, donc* (b) *admet* $(x_1, x_2) = (-y, y)$ *comme solution particulière, ce qui fait que la solution générale de* (b) *est*

$$(x_1, x_2) = (-y + 3k', y - 2k'),\ k \in \mathbb{Z}\,.$$

La solution générale de l'équation initiale est donc :

$$(x_1, x_2, x_3) = (28 - 243k + 3k', -28 + 243k + 2k', 59 - 512k),\ (k, k') \in \mathbb{Z}^2.$$

Exemple.
Résoudre dans $\mathbb{Z}$ *l'équation* $\underbrace{13x_1 + 39x_2}_{13y_1} + \underbrace{6x_3 + 24x_4}_{6y_2} = 1$.

On part de l'équivalence suivante

$$13x_1 + 39x_2 + 6x_3 + 24x_4 = 1 \Longleftrightarrow \left\{ \begin{array}{lrcrcl} (a) & 13y_1 & + & 6y_2 & = & 1 \\ (b) & x_1 & + & 3x_2 & = & y_1 \\ (c) & x_3 & + & 4x_4 & = & y_2. \end{array} \right.$$

Résolution de (a). *Comme* $13 \wedge 6 = 1$, *l'équation* (a) *possède des solutions entières :*

$$(y_1, y_2) = (1 + 6k, -2 - 13k),\ k \in \mathbb{Z}\,.$$

Résolution de (b). L'équation $x_1 + 3x_2 = 1$ admet $(x_1, x_2) = (4, -1)$ comme solution particulière, donc (b) admet $(x_1, x_2) = (4y_1, -y_1)$ comme solution particulière, ce qui fait que la solution générale de (b) est :

$$(x_1, x_2) = (4y_1 + 3k', -y_1 - k'),\ k \in \mathbb{Z}\,.$$

Résolution de (c). L'équation $x_3 + 4x_4 = 1$ admet $(x_3, x_4) = (5, -1)$ comme solution particulière, donc (c) admet $(x_3, x_4) = (5y_2, -y_2)$ comme solution particulière, et la solution générale de (c) est donc :

$$(x_3, x_4) = (5y_2 + 4k'', -y_2 - k''),\ k'' \in \mathbb{Z}\,.$$

Finalement, la solution générale de l'équation initiale est :

$$(x_1, x_2, x_3, x_4) = (4 + 24k + 3k', -1 - 6k - k', -10 - 65k + 4k'', 2 + 13k - k''),\ (k, k', k'') \in \mathbb{Z}^3.$$

2 Groupes quotients de $\mathbb{Z}$

2.1 Définitions

Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. D'après l'égalité de division euclidienne, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}_{n-1}$ tel que

$$a = nq + r.$$

On note usuellement $r = a \bmod n$, de sorte que :

$$\forall a, b \in \mathbb{Z}\,,\ a \bmod n = b \bmod n \iff n \text{ divise } b - a.$$

Exemple.
Nous sommes jeudi. Quel jour de la semaine serons-nous dans 1000 jours ? Quel jour de la semaine étions-nous il y a 500 jours ?

Comme $1000 = 7 \times 142 + 6$, dans 1000 jours nous serons jeudi + $\underbrace{1000 \bmod 7}_{6}$ jours = mercredi.

De même, $-500 = 7 \times (-72) + 4$, donc, il y a 500 jours de cela, nous étions un jeudi $-\underbrace{500 \bmod 7}_{4}$ jours = lundi.

2.2 Congruence

Soit $n \in \mathbb{N}^*$ (bien qu'ici, seul le cas $n \geq 2$ ait de l'intérêt).

2.2.1 Relation de congruence

Pour tous a *et* b *dans* $\mathbb{Z}$ *, on dit que* a *est congru à* b *modulo* n *si* $a \bmod n = b \bmod n$*. On note alors* $a \equiv_n b$ *ou bien* $a \equiv b \bmod n$*, voire tout simplement* $a \equiv b$ *lorsqu'il n'y a pas d'ambiguité.*
On définit ainsi une relation entre entiers relatifs, appelée $\textit{relation de congruence modulo } n$*, qui est une* $\textit{relation d'équivalence}$*, parce qu'elle vérifie les 3 propriétés suivantes :*

- *réflexivité :* $\forall a \in \mathbb{Z},\ a \equiv a \bmod n$*,*
- *symétrie :* $\forall a, b \in \mathbb{Z},\ a \equiv b \bmod n \Longrightarrow b \equiv a \bmod n$*,*
- *transitivité :* $\forall a, b, c \in \mathbb{Z},\ \left.\begin{array}{c} a \equiv b \bmod n \\ b \equiv c \bmod n \end{array}\right\} \Longrightarrow a \equiv c \bmod n.$

On peut donc définir les $\textit{classes d'équivalence}$ *de cette relation, qui sera notée* $\equiv_n$ *ou plus simplement* $\equiv$ *lorsqu'il n'y a pas d'ambiguité :*

$$\forall r \in \mathbb{Z},\ [r]_n = \{x \in \mathbb{Z},\ x \equiv r \bmod n\} = \{r + kn,\ k \in \mathbb{Z}\}.$$

$[r]_n$ *est appelée* $\textit{classe d'équivalence de } r \textit{ modulo } n.$

2.2.2 L'ensemble des classes d'équivalence modulo n

Il existe n *classes d'équivalence modulo* n *distinctes :*

$$\begin{array}{ccccc} [0]_n & = & \{kn,\ k \in \mathbb{Z}\} & = & n\mathbb{Z} \\ [1]_n & = & \{1 + kn,\ k \in \mathbb{Z}\} & = & 1 + n\mathbb{Z} \\ [2]_n & = & \{2 + kn,\ k \in \mathbb{Z}\} & = & 2 + n\mathbb{Z} \\ \vdots & & \vdots & & \vdots \\ [n-1]_n & = & \{(n-1) + kn,\ k \in \mathbb{Z}\} & = & (n-1) + n\mathbb{Z}. \end{array}$$

En effet, l'ensemble des classes d'équivalence modulo n *(c'est donc un ensemble d'ensembles) est* $\textit{cyclique}$*, puisque*

$$a \equiv b \bmod n \Longleftrightarrow [a]_n = [b]_n,$$

ce qui implique que pour tout $r \in \mathbb{N}_n$*, on a :*

$$[\pm n + r]_n = [r]_n.$$

Autrement dit :

$$\begin{array}{ccccccccccccc} \ldots & = & [-2n]_n & = & [-n]_n & = & [0]_n & = & [n]_n & = & [2n]_n & = & \ldots \\ \ldots & = & [-2n+1]_n & = & [-n+1]_n & = & [1]_n & = & [n+1]_n & = & [2n+1]_n & = & \ldots \\ \ldots & = & [-2n+2]_n & = & [-n+2]_n & = & [2]_n & = & [n+2]_n & = & [2n+2]_n & = & \ldots \end{array}$$

De plus, deux classes modulo n *distinctes sont disjointes :*

$$\forall a, b \in \mathbb{N}_n,\ a \neq b \Longrightarrow [a]_n \cap [b]_n = \emptyset.$$

On peut remarquer que $\mathbb{Z}$ est la réunion de toutes les classes modulo n :

$$\mathbb{Z} = [0]_n \cup [1]_n \cup \ldots \cup [n-1]_n = \bigcup_{i=0}^{n-1} [i]_n.$$

On note $\mathbb{Z}/n\mathbb{Z}$ ou plus simplement $\mathbb{Z}_n$ l'ensemble des classes modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

On remarque que $\mathbb{Z}_n$ est en bijection avec $\mathbb{N}_n$.

2.3 Structure arithmétique de $\mathbb{Z}_n$

L'objectif de ce § est de définir une addition $+_n$ et une multiplication $._n$ sur $\mathbb{Z}_n$. On parle alors parfois $d'addition\ et\ de\ multiplication\ modulo\ n$.
Dans $\mathbb{Z}_8$ par exemple, on aimerait avoir :

$$\begin{cases} [2]_8 +_8 [5]_8 = [2+5]_8 = [7]_8 \\ [2]_8 ._8 [5]_8 = [2.5]_8 = [10]_8 = [2]_8 \end{cases}$$

2.4 Addition et multiplication modulo n

Lemme 2.1 *Pour tout $n \in \mathbb{N}^*$ et tous a, a', b, b' dans $\mathbb{N}_n$, on a :*

$$[a]_n = [a']_n \text{ et } [b]_n = [b']_n \Longrightarrow [a \pm b]_n = [a' \pm b']_n \text{ et } [a.b]_n = [a'.b']_n.$$

Démonstration.

Grâce au lemme 2.1, on peut définir l'addition et la multiplication modulo n comme suit :

$$\forall a, b \in \mathbb{N}_n, \begin{cases} [a]_n +_n [b]_n &= [a+b]_n \\ [a]_n ._n [b]_n &= [a.b]_n. \end{cases}$$

Il résulte alors de cette définition que $+_n$ et $._n$ héritent des propriétés de l'addition et de la multiplication entières. En particulier :

- *$+_n$ et $._n$ sont commutatives : $[a]_n +_n [b]_n = [b]_n +_n [a]_n$ et $[a]_{n\cdot n}[b]_n = [b]_{n\cdot n}[a]_n$;*
- *$[0]_n$ est élement neutre de $+_n$: $[0]_n +_n [a]_n = [a]_n$;*
- *$[1]_n$ est élement neutre de $._n$: $[1]_{n\cdot n}[a]_n = [a]_n$;*
- *$._n$ est distributive par rapport à $+_n$: $[a]_{n\cdot n}([b]_n +_n [c]_n) = [a]_{n\cdot n}[b]_n +_n [a]_{n\cdot n}[c]_n$.*

Exemple.

Tables de $+_5$ et $._5$.

On sait que dans $\mathbb{Z}$, l'unique solution de l'équation $a + x = 0$ est l'opposé de a, noté $-a$. De même, dans $\mathbb{Z}_n$, l'unique solution $[x]_n$ de

$$[a]_n +_n [x]_n = [0]_n,$$

est notée $-[a]_n$. Ainsi, l'exemple 2.4 montre que

$$-[2]_5 = [3]_5 \text{ et } -[3]_5 = [2]_5.$$

En toute généralité on a donc :

$$-[a]_n = [n - a]_n = [-a]_n.$$

2.5 Inversibilité dans $\mathbb{Z}_n$

Il s'agit de trouver tous les éléments $[a]_n$ de $\mathbb{Z}_n$ pour lesquels il existe $[x]_n \in \mathbb{Z}_n$ tel que

$$[a]_n.[x]_n = [1]_n.$$

Dans ce cas, on dira que $[a]_n$ est $inversible\ dans\ \mathbb{Z}_n$ et $[x]_n$ s'appelle $l'inverse\ de\ [a]_n$ et se note $[a]_n^{-1}$. L'ensemble des éléments inversibles dans $\mathbb{Z}_n$ est noté $\mathbb{Z}_n^*$.

Proposition 2.1

$$[a]_n \in \mathbb{Z}_n^* \Longleftrightarrow a \wedge n = 1.$$

Démonstration.

On rappelle qu'un entier naturel $n \geq 2$ *est dit* $premier$ *s'il n'est divisible que par* 1 *et par lui-même. En convenant de noter* P *l'ensemble des nombres premiers, on a donc :*

$$\begin{aligned} P \;=\; \{&2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107,\\ &109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199,211,223,227,\\ &229,233,239,241,251,257,263,269,271,277,281,283,293,307,311,313,317,331,337,347,349,\\ &353,359,367,373,379,383,389,397,401,409,419,421,431,433,439,443,449,457,461,463,467,\\ &479,487,491,499,503,509,521,523,541,547,557,563,569,571,577,587,593,599,601,607,613,\\ &617,619,631,641,643,647,653,659,661,673,677,683,691,701,709,719,727,733,739,743,751,\\ &757,761,769,773,787,797,809,811,821,823,827,829,839,853,857,859,863,877,881,883,887,\\ &907,911,919,929,937,941,947,953,967,971,977,983,991,997,\ldots\}\,. \end{aligned}$$

En particulier, il résulte de la proposition 2.1 que lorsque n *est premier, tous les éléments non nuls de* $\mathbb{Z}_n$ *sont inversibles : on dit alors que* $\mathbb{Z}_n$ *est un corps.*
Ensuite, on remarque que pour calculer $[a]_n^{-1}$*, il suffit en fait de résoudre l'équation diophantienne*

$$ax - ny = 1,$$

d'inconnues x *et* y*, puisque* $[a]_n^{-1} = [x]_n$*.*

Exemple.
Cas où $a = 393$ *et* $n = 1000$*.*

On trouve que $1 = (-101) \times 1000 + 257 \times 393$*, donc que* $[393]_{1000}^{-1} = [257]_{1000}$*.*
En fait, $\mathbb{Z}_n^*$ *est* $stable\ pour\ .n$*, car :*

$$[a]_n \in \mathbb{Z}_n^* \text{ et } [b]_n \in \mathbb{Z}_n^* \Longrightarrow [a]_n \cdot_n [b]_n \in \mathbb{Z}_n^*.$$

En effet, c'est une conséquence de l'égalité :

$$[ab]_n^{-1} = [a]_n^{-1}.{}_n[b]_n^{-1}.$$

3 Le théorème d'Euler

3.1 La fonction indicatrice d'Euler

3.1.1 Définition

Pour tout $n \geq 1$, *posons*

$$P_n = \{x \in \mathbb{N}_n^*,\ n \wedge x = 1\} \text{ et } \varphi(n) = \mathrm{card}(P_n).$$

La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ *ainsi définie est la* $fonction\ indicatrice\ d'Euler.$
On évidemment :

$$\begin{cases} \varphi(1) &= 1 \\ \varphi(n) &= n-1 \quad \textit{si } n \textit{ est premier.} \end{cases}$$

Exemple.
Un rapide dénombrement montre que $\varphi(6) = 2$ *et* $\varphi(15) = 8$.

3.1.2 Calcul de $\varphi(n)$, $n \in \mathbb{N}^*$

Lemme 3.1 *Si* p *est premier alors* $\varphi(p^k) = p^{k-1}(p-1)$ *pour tout* $k \geq 1$.

Démonstration.
On commence par remarquer que :

$$\begin{aligned} \varphi(p^k) &= \mathrm{card}\left(\mathbb{Z}_{p^k}^*\right) \\ &= \mathrm{card}\left(\mathbb{Z}_{p^k}\right) - \textit{nb éléments non inversibles de } \mathbb{Z}_{p^k}. \end{aligned}$$

Or, $m \in \mathbb{Z}_{p^k}$ *n'est pas inversible si et seulement si* $q = m \wedge p^k \neq 1$. *Comme les seuls diviseurs* (> 1) *de* p^k *sont les* p^j, $1 \leq j \leq k$, *nécessairement* p *divise* m. *En résumé, si* m *n'est pas inversible dans* $\mathbb{Z}_{p^k}$ *alors* m *est multiple de* p.
Comme, réciproquement, tout multiple de p *n'est pas inversible dans* $\mathbb{Z}_{p^k}$, *on a montré que l'ensemble des éléments non inversibles de* $\mathbb{Z}_{p^k}$ *est celui des multiples de* p. *Et comme il y a un multiple de* p *tous les* p *éléments de* $\mathbb{Z}_{p^k}$, *on dénombre au total :*

$$\frac{p^k}{p} = p^{k-1} \textit{ multiples de } p \textit{ dans } \mathbb{Z}_{p^k}.$$

Par suite, $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. ∎

Lemme 3.2 *Si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m) \times \varphi(n)$.*

Démonstration.
Il s'agit de montrer que $\mathrm{card}\,(\mathbb{Z}^*_{mn}) = \mathrm{card}\,(\mathbb{Z}^*_m) \times \mathrm{card}\,(\mathbb{Z}^*_n)$*, c'est-à-dire qu'il existe une bijection de* $\mathbb{Z}^*_{mn}$ *sur* $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$*. Pour cela, posons*

$$\begin{array}{rccc} f: & \mathbb{Z}_{mn} & \to & \mathbb{Z}_m \times \mathbb{Z}_n \\ & x \bmod nm & \mapsto & (x \bmod m, x \bmod n). \end{array}$$

On va d'abord montrer que f est une bijection de $\mathbb{Z}_{mn}$ sur $\mathbb{Z}_m \times \mathbb{Z}_n$ et ensuite que f envoie $\mathbb{Z}^*_{mn}$ sur $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$, c'est-à-dire que $f\,(\mathbb{Z}^*_{mn}) = \mathbb{Z}^*_m \times \mathbb{Z}^*_n$.
a) Montrons que f est une bijection de $\mathbb{Z}_{mn}$ sur $\mathbb{Z}_m \times \mathbb{Z}_n$.
D'abord, f est $injective$ car

$$\forall x, y \in \mathbb{Z}_{mn},\ f(x) = f(y) \Longrightarrow x = y.$$

En effet, on a l'implication

$$f(x) = f(y) \Longrightarrow \left\{ \begin{array}{rcl} x \bmod m & = & y \bmod m \\ y \bmod n & = & y \bmod n \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} x - y \text{ est multiple de } m \\ x - y \text{ est multiple de } n, \end{array} \right.$$

donc il existe $k, k' \in \mathbb{Z}$ tels que :

$$x - y = km = k'n.$$

Par suite, m divise nk' donc, comme $m \wedge n = 1$, n divise k'. Il existe donc $q \in \mathbb{Z}$ tel que $k' = qn$. Ainsi, $y - x = k'm = qnm$ est multiple de nm donc $x = y \bmod nm$.
Ensuite, f est une $surjection$ de $\mathbb{Z}_{mn}$ sur $\mathbb{Z}_m \times \mathbb{Z}_n$ car tout $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ possède un antécédent $x \in \mathbb{Z}_{mn}$ par f puisque :

$$(a, b) = f(x) \Longleftrightarrow \left\{ \begin{array}{rcl} x \bmod m & = & a \\ x \bmod n & = & b \end{array} \right. \Longleftrightarrow x = any_1 + bmy_2 \text{ où } \left\{ \begin{array}{rcl} y_1 & = & n^{-1} \bmod m \\ y_2 & = & m^{-1} \bmod n. \end{array} \right.$$

b) Montrons enfin que f envoie $\mathbb{Z}^*_{mn}$ sur $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$
Voyons d'abord que $f\,(\mathbb{Z}^*_{mn}) \subset \mathbb{Z}^*_m \times \mathbb{Z}^*_n$. Pour cela, prenons x dans $\mathbb{Z}^*_{mn}$, de sorte que $x \wedge nm = 1$, ce qui implique forcément $x \wedge m = 1$ et $x \wedge n = 1$, d'où $x \bmod m \in \mathbb{Z}^*_m$ et $x \bmod n \in \mathbb{Z}^*_n$. Ainsi on a finalement $f(x) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n$.
Pour l'inclusion réciproque, considérons $(a, b) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n$ et cherchons $x \in \mathbb{Z}^*_{mn}$ tel que $f(x) = (a, b)$. Si un tel x existe, c'est, d'après ce qui précède, forcément

$$x = any_1 + bmy_2 \text{ où } \left\{ \begin{array}{rcl} y_1 & = & n^{-1} \bmod m \\ y_2 & = & m^{-1} \bmod n. \end{array} \right.$$

Montrons que x appartient effectivement à $\mathbb{Z}^*_{mn}$. Cela revient à prouver l'existence de $y \in \mathbb{Z}_{mn}$ pour lequel on a $xy = 1 \bmod mn$. Or, comme f est une bijection de $\mathbb{Z}_{mn}$ sur $\mathbb{Z}_m \times \mathbb{Z}_n$, on sait que

$$xy = 1 \bmod mn \Longleftrightarrow f(xy) = f(1) = \underbrace{(1 \bmod m, 1 \bmod n)}_{(1,1)} \Longleftrightarrow \left\{ \begin{array}{rcl} xy \bmod m & = & 1 \\ xy \bmod n & = & 1 \end{array} \right.$$

Or, $xy \bmod m = (any_1 + bmy_2)y \bmod m = any_1 y \bmod m$ *et* $xy \bmod n = (any_1 + bmy_2)y \bmod n = bmy_2 y \bmod n$, *donc*

$$x \in \mathbb{Z}^*_{mn} \Longleftrightarrow \exists y \in \mathbb{Z}_{mn} \text{ solution de} \begin{cases} any_1 y \bmod m &= 1 \\ bmy_2 y \bmod n &= 1. \end{cases}$$

Il suffit donc de prendre $y = a'ny_1 + b'my_2$ *avec* $a' = a^{-1} \bmod m$ *et* $b' = b^{-1} \bmod n$. ■

Proposition 3.1 *Pour tout* $n \in \mathbb{N}^*$ *dont la décomposition en produit de facteurs premiers s'écrit*

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},\ p_i \in P,\ k_i \geq 1,\ 1 \leq i \leq r,$$

on a :

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \dots p_r^{k_r-1}(p_1 - 1)(p_2 - 1)\dots(p_r - 1).$$

Démonstration.
Pour tout $(i,j) \in \mathbb{N}_r$, $i \neq j \Longrightarrow p_i \wedge p_j = 1 \Longrightarrow p_i^{k_i} \wedge p_j^{k_j} = 1$, *donc* $\varphi(p_i^{k_i} p_j^{k_j}) = \varphi(p_i^{k_i})\varphi(p_j^{k_j})$ *d'après le lemme 3.2, soit finalement :*

$$\varphi(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r}).$$

Ensuite, comme $p_i \in P$ *pour tout* i *de 1 à* r, $\varphi(p_i^{k_i}) = p_i^{k_i-1}(p_i - 1)$ *d'après le lemme 3.1, donc :*

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \dots p_r^{k_r-1}(p_1 - 1)(p_2 - 1)\dots(p_r - 1). \blacksquare$$

Exemple.
A partir de la décomposition $1980 = 2^2 \times 3^2 \times 5 \times 11$, *on obtient :*

$$\varphi(1980) = 2^{2-1} \times 3^{2-1} \times 5^{1-1} \times 11^{1-1} \times (2-1) \times (3-1) \times (5-1) \times (11-1) = 480.$$

3.2 Le théorème d'Euler : énoncé et applications

3.2.1 Enoncé du théorème d'Euler

Théorème 3.1 *Pour tout* $a \in \mathbb{N}^*$, *on a l'implication*

$$a \wedge n = 1 \Longrightarrow a^{\varphi(n)} \equiv 1 \bmod n.$$

Démonstration.
Comme $a \wedge n = 1$, a est inversible modulo n et l'application

$$\begin{array}{rccc} \mu_a : & \mathbb{Z}_n^* & \to & \mathbb{Z}_n^* \\ & r & \mapsto & ar, \end{array}$$

est bijective. En effet :

- *$\mu_a(m) = \mu_a(p) \Longrightarrow am \equiv ap \mod n \Longrightarrow \underbrace{a^{-1}a}_{\equiv 1 \mod n} m \mod n = \underbrace{a^{-1}a}_{\equiv 1 \mod n} p \mod n \Longrightarrow \underbrace{m \mod n}_{m} = \underbrace{p \mod n}_{p}$, donc μ_a est injective ;*
- *quel que soit $m \in \mathbb{Z}_n^*$, $a^{-1}m$ appartient à $\mathbb{Z}_n^*$ et $m = \mu_a(a^{-1}m)$ donc μ_a est surjective.*

Notons $r_1, r_2, \ldots, r_{\varphi(n)}$ les éléments de $\mathbb{Z}_n^*$: $\mathbb{Z}_n^* = \left\{r_1, r_2, \ldots, r_{\varphi(n)}\right\}$.
Comme μ_a est une bijection de $\mathbb{Z}_n^*$ sur lui-même, on a forcément :

$$\underbrace{\mu_a(r_1)}_{ar_1}\underbrace{\mu_a(r_2)}_{ar_2}\ldots\underbrace{\mu_a(r_{\varphi(n)})}_{ar_{\varphi(n)}} = r_1 r_2 \ldots r_{\varphi(n)},$$

soit

$$a^{\varphi(n)}\underbrace{r_1 r_2 \ldots r_{\varphi(n)}}_{b} = r_1 r_2 \ldots r_{\varphi(n)}.$$

Ainsi, puisque b est inversible dans $\mathbb{Z}_n$:

$$a^{\varphi(n)}\underbrace{bb^{-1}}_{1 \mod n} \equiv bb^{-1} \mod n,$$

ce qui démontre le résultat. ■

Exemple.
Etude du cas où $n = 8$ et $a = 3$.
On a en fait $\varphi(n) = \varphi(2^3) = 4$ et $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. Ainsi,

$$a^{\varphi(n)} = 3^4 = 9^2 = 81 = 8 \times 10 + 1 \equiv 1 \mod 8,$$

et $\mu_a(1) = 3$, $\mu_a(3) = 1$, $\mu_a(5) = 7$, $\mu_a(7) = 5$, de sorte que :

$$\mu_a(1)\mu_a(3)\mu_a(5)\mu_a(7) = 3 \times 1 \times 7 \times 5 = 1 \times 3 \times 5 \times 7.$$

3.2.2 Applications du théorème d'Euler

Première application : *calcul de $18^{19^{20^{21}}} \mod 25$.*
On sait que $25 = 5^2$ donc $\varphi(25) = 5 \times 4 = 20$. Ensuite, comme $18 \wedge 25 = 1$ le théorème d'Euler 3.1 entraîne :

$$18^{N_1} \equiv 18^{r_1} \mod 25 \text{ si } N_1 \equiv r_1 \mod \varphi(25).$$

C'est pourquoi, il est utile de calculer $19^{20^{21}} \bmod 20$. *De même,* $19 \wedge 20 = 1$, *donc :*

$$19^{N_2} \equiv 19^{r_2} \bmod 20 \text{ si } N_2 \equiv r_2 \bmod \varphi(20).$$

Ensuite, $\varphi(20) = \varphi(5 \times 2^2) = 4 \times 2 = 8$, *donc il faut calculer* $20^{21} \bmod 8$. *Or, on a*

$$20^{21} = (2^2 \times 5)^{21} = 2^{42} \times 5^{21} = \underbrace{2^3}_{8} \times 2^{39} \times 5^{21} \equiv 0 \bmod 8,$$

donc $19^{20^{21}} \equiv \underbrace{19^0}_{1} \bmod 20$, *soit finalement :*

$$18^{19^{20^{21}}} \equiv \underbrace{18^1}_{18} \bmod 25 \Longrightarrow 18^{19^{20^{21}}} \bmod 25 = 18.$$

Deuxième application : *calcul de* $11^{773} \bmod 17$.
On utilise la méthode d'exponentiation rapide, basée sur l'égalité suivante :

$$a^{2^{n+1}} \bmod n = a^{2^n \times 2} \bmod n = a^{2^n + 2^n} \bmod n = a^{2^n} \times a^{2^n} \bmod n.$$

Ainsi, comme $773 = 2^0 + 2^2 + 2^8 + 2^9$ *et que :*
- $11^2 \equiv (-6)^2 \bmod 17 \equiv 2 \bmod 17$,
- $11^{2^2} \equiv 2^2 \bmod 17 \equiv 4 \bmod 17$,
- $11^{2^3} \equiv 4^2 \bmod 17 \equiv (-1) \bmod 17$,
- $11^{2^4} \equiv (-1)^2 \bmod 17 \equiv 1 \bmod 17$,

on a nécessairement :

$$11^{2^k} \equiv 1 \bmod 17 \text{ si } k \geq 4.$$

Par suite,

$$\begin{aligned} 11^{773} \bmod 17 &= 11^{2^0+2^2+2^8+2^9} \bmod 17 \\ &= 11.11^{2^2}.11^{2^8}.11^{2^9} \bmod 17 \\ &= 11.4.1.1 \bmod 17 \\ &= 44 \bmod 17 = 10. \end{aligned}$$

4 Système de cryptage RSA

4.1 Principe de fonctionnement

Soient $n \geq 1$ *(grand !),* $M < n$ *un message numérisé (sous forme d'entier naturel) vérifiant*

$$M \wedge n = 1,$$

et un système de clés $(e, d) \in \mathbb{N}^2$ *liées par la relation*

$$ed \equiv 1 \bmod \varphi(n),$$

ce qui garantit l'existence de $k \in \mathbb{Z}$ *tel que* $ed = 1 + k\varphi(n)$.
Considérons ensuite le message crypté (c'est un entier) : $C = M^e \bmod n$.
Pour retrouver M *à partir de* C, d *et* n, *il suffit de calculer* $C^d \bmod n = M$.
En effet, on a :

$$\begin{aligned} C^d &= M^{ed} \bmod n \\ &= M^{1+k\varphi(n)} \bmod n \\ &= M \times \underbrace{\left(M^{\varphi(n)}\right)^k \bmod n}_{1} \\ &= M. \end{aligned}$$

4.2 Description du système de cryptage RSA

4.2.1 Les clés de chaque utilisateur

Chaque utilisateur A *de ce système possède :*
- *une clé publique* (e_a, n_a),
- *une clé privée* d_a, *secrète.*

Les quantités e_a, n_a *et* d_a *sont liées par la relation* $e_a d_a \equiv 1 \bmod \varphi(n_a)$.
Dans la pratique, on choisit (la raison sera donnée un peu après) $n = p_a q_a$ *où* p_a *et* q_a *sont deux entiers premiers grands.*

4.2.2 Encryptage

Un message numérisé M *supposé* $< n_a$ *à envoyer à* A *est crypté sous la forme*

$$C = E_A(M) = M^{e_a} \bmod n_a.$$

Le message crypté C *est ensuite expédié à* A.

4.2.3 Décryptage

A *reçoit ensuite* C *qu'il doit décrypter (pour lire le message* M*), selon la méthode exposée au* §*4.1 :*

$$M = C^{d_a} \bmod n_a.$$

4.2.4 Garantie du secret

Si le message crypté C *est intercepté par toute autre personne que* A, *ne disposant pas de* d_a, *il lui est nécessaire de trouver* d_a *pour reconstituer* M. *En effet, seuls* e_a *et* n_a *et la relation* $e_a d_a \equiv 1 \bmod \varphi(n_a)$ *sont connus car il s'agit de données publiques. Par suite, il lui faut calculer*

$$d_a = e_a^{-1} \bmod \varphi(n_a).$$

Le calcul de d_a est donc facile dès lors que $\varphi(n_a)$ est connu.
Or, $n_a = p_a q_a$ donc $\varphi(n_a) = (p_a - 1)(q_a - 1)$. Il "suffit" donc de trouver les deux mombres premiers p_a et q_a satisfisant $n_a = p_a q_a$. Ce problème (d'apparence simple) est en fait très complexe, et le meilleur algorithme actuellement connu pour résoudre ce problème nécessite environ $\mathrm{e}^{\sqrt{\ln n_a \times \ln(\ln n_a)}}$ opérations élémentaires, ce qui représente plus d'un million d'années de calcul (à raison de 10^{11} opérations élémentaires par jour) si n_a a plus de 512 positions binaires. C'est pourquoi, la stratégie consiste à choisir p_a et q_a assez grands de façon que n_a ait au moins 512 positions binaires. Il devient ainsi quasiment impossible de retrouver d_a à partir e_a et n_a.

4.2.5 Garantie de récupération du message par le destinataire

Pour que $D_A(M)$ soit égal à M, il est nécessaire (et suffisant) que $M \wedge n_a = 1$. Comme $n_a = p_a q_a$ où p_a et q_a sont premiers, le nombre de messages $M < n_a$ qui ne sont pas premiers avec n_a est

$$n_a - \varphi(n_a) = n_a - (p_a - 1)(q_a - 1) = p_a + q_a - 1.$$

Un message $M < n_a$ choisi au hasard a donc

$$\frac{p_a + q_a - 1}{n_a} = \frac{1}{p_a} + \frac{1}{q_a} - \frac{1}{p_a q_a}$$

chances de ne pas être premier avec n_a. C'est pourquoi, on choisit p_a et q_a grands et du même ordre de grandeur.

4.3 Le système RSA en version signée

On va améliorer le système précédent en y ajoutant une garantie de provenance pour le destinataire. Soient A et B deux utilisateurs du système. Les clés publiques et privées de A sont respectivement (e_a, n_a) et d_a, celles de B sont notées (e_b, n_b) et d_b. Elles sont toujours liées par les relations suivantes :

$$e_a d_a \equiv 1 \bmod \varphi(n_a) \text{ et } e_b d_b \equiv 1 \bmod \varphi(n_b).$$

Supposons que A veuille envoyer un message numérisé M à B et lui garantir qu'il en est bien l'expéditeur.

4.3.1 Cas où $n_a < n_b$

La méthode comporte 4 étapes :

- *A commence par signer son message M en traitant le message M comme s'il s'agissait d'un cryptogramme reçu :*
$$C_1 = D_A(M) = M^{d_a} \bmod n_a.$$
- *A crypte ensuite C_1 à destination de B*
$$C = E_B(C_1) = C_1^{e_b} \bmod n_b,$$
puis expédie C à A.

– *A la réception de* C, B *décrypte* C :

$$D_B(C) = C^{d_b} \bmod n_b = C_1.$$

– *Puis* B *vérifie la signature de* A :

$$E_A(C_1) = C_1^{e_a} \bmod n_a = M.$$

Le protocole a "respecté les restes" car C_1 *peut être traité comme un reste modulo* n_b *puisque* $n_a < n_b$.

4.3.2 Cas où $n_b < n_a$

Dans ce cas, les opérations effectuées sont :
– *pour* A : $C = D_A[E_B(M)]$,
– *pour* B : $M = D_B[E_A(C)]$.