

6 Congruences

$$a = nq + b \quad \text{alors} \quad a \equiv b [n]$$

6.1 Définition

Definition 6.1 Soit n un entier naturel. On dit que les entiers a et b sont congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n .

On note alors

$$a \equiv b [n].$$

$$2 = 0 \times 3 + 2 \quad \Rightarrow \quad 2 \equiv 2 [3]$$

$$5 = 1 \times 3 + \underline{2} \quad \Rightarrow \quad 5 \equiv 2 [3]$$

$$8 = 2 \times 3 + \underline{\underline{2}} \quad \Rightarrow \quad 8 \equiv 2 [3]$$

$$8 \equiv 5 [3] \equiv 2 [3]$$

Il est immédiat de voir que si

$$a = nq + r,$$

alors

$$a \equiv r[n].$$

C'est ce reste r qui représentera l'entier a modulo n .

Par exemple, puisque

$$101 = 7 \times 14 + 3,$$

$$101 \equiv 3 [7]$$

6.2 Propriétés

Les congruences rendent élémentaire le calcul du reste. Tout est dans la proposition suivante.

Proposition 6.2 Soient a, b, c et d trois nombres entiers naturels et n un entier naturel non nul. Si $a \equiv c[n]$, et $b \equiv d[n]$,

$$a + b \equiv c + d[n],$$

$$a - b \equiv c - d[n],$$

$$ab \equiv cd[n],$$

$$a^p \equiv c^p[n],$$

$$a = pn + c$$

$$b = qn + d$$

$$a + b = pn + qn + c + d$$

$$= (p+q)n + \underline{c+d}$$

$$a + b \equiv c + d[n].$$

pour tout entier naturel p .

$$40 \equiv 4 [36]$$

$$78 \equiv 6 [36]$$

$$40 - 78 \equiv 4 - 6 [36] \equiv -2 [36]$$

$$\equiv 36 - 2 [36]$$

$$\equiv 34 [36].$$

Par exemple, on rappelle que $101 \equiv 3[7]$ et que $66 \equiv 3[7]$. Ainsi :

$$167 = 101 + 66 \equiv 3 + 3[7] = 6[7]$$

$$66\ 66 = 66 \times 101 \equiv 3 \times 3[7] = 9[7] = 2[7]$$

$$287\ 496 = 66^3 \equiv 3^3[7] = 27[7] = 6[7] \quad .$$

On notera que si $a \equiv b[n]$ alors $a - b \equiv 0[n]$ et n divise $a - b$.

Evidences! $70 \equiv 0[7] \Leftrightarrow 7 \text{ divise } 70$.

$75 \equiv 5[7] \Leftrightarrow (75 - 5) \text{ divisible par } 7$.

6.3 Petit théorème de Fermat

Le théorème qui suit est fondamental dans la cryptologie moderne industrielle qui a besoin d'entiers naturels premiers à grands nombres de chiffres (codage RSA).

Theorem 6.3 *Si p est un nombre premier et si a est un entier non divisible par p , alors*

- $a^{p-1} \equiv 1[p]$,
- *ou, de manière équivalente, $a^p \equiv a[p]$.*

Petit thm de Fermat

p premier, a non divisible par p .

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

On a pour application directe

$$2^{97} - 2 = 158456325028528675187087900670$$

97 est premier, 97 ne divise pas 2.

$$2^{97} \equiv 2 [97] \Leftrightarrow 2^{97} - 2 \equiv 0 [97]$$

Donc ce nombre est divisible par 97.

3, 5 nombres premiers.

$$17 \equiv 2 [3]$$

premier avec 15.

$$17 \equiv 2 [5]$$

alors on a $17 \equiv 2 [3 \times 5]$

Corollary 6.4 Soit p et q des nombres premiers distincts. On pose $n = pq$. Pour tout a premier avec n on a

$$a^{(p-1)(q-1)} \equiv 1 [n].$$

Preuve: Montrons que, si $a \equiv b [p]$ et $a \equiv b [q]$ (par q de l'énoncé i.e. premiers)
alors $a \equiv b [pq]$

On a $a - b = kp$ et $a - b = mq \Rightarrow kp = mq$, donc
 p divise mq . Or p est premier avec q donc p divise m .
 $m = lp$ et $a - b = lpq \Rightarrow a \equiv b [pq]$

• D'après le petit théorème de Fermat,

$$\begin{cases} a^{p-1} \equiv 1 [p] & \text{et donc} & a^{(p-1)(q-1)} \equiv 1^{q-1} [p] \equiv 1 [p] \\ a^{q-1} \equiv 1 [q] & \text{et donc} & a^{(p-1)(q-1)} \equiv 1^{p-1} [q] \equiv 1 [q] \end{cases}$$

$$\text{Donc} \quad a^{(p-1)(q-1)} \equiv 1 [pq] \equiv 1 [n].$$

6.4 Groupe cyclique

On s'aperçoit que, pour n fixé, les congruences reviennent à considérer un nombre comme son reste dans la division par n . Par conséquent, les nombres

$$p, \quad p + n, \quad p - n, \quad p + 2n, \quad p - 2n, \quad p + 3n, \quad \dots$$

ont tous le même reste $p < n$ dans la division par n . Ils ont donc la même congruence modulo n , qui est p . Cette *classe d'équivalence* \bar{p} représente donc tous ces nombres.

L'ensemble des classes d'équivalences

$$\bar{0}, \bar{1}, \dots, \overline{n-2}, \overline{n-1},$$

forment l'ensemble $\mathbb{Z}/n\mathbb{Z}$. On définit une somme et un produit entre classes d'équivalences grâce à la propriété 6.2. Avec la stabilité pour ces deux lois, la structure de $\mathbb{Z}/n\mathbb{Z}$ s'appelle groupe. Le groupe est dit cyclique car en ajoutant 1 à \bar{a} , et en itérant l'implémentation, on finira par revenir sur \bar{a} au bout d'un certain nombre de fois.

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

$$5 \equiv 0[5] \text{ donc } \bar{5} = \bar{0}$$

$$\overline{2+3} = \bar{5} = \bar{0}$$

$$\hookrightarrow \begin{array}{l} 2 \equiv 2[5] \\ 3 \equiv 3[5] \end{array}$$

$$\nearrow 2+3 \equiv 0[5]$$

Definition 6.5

- On peut définir l'inverse \bar{b} d'un élément \bar{a} comme la classe d'équivalence telle que

$$\bar{a}\bar{b} \equiv 1[n].$$

- Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, s'il existe $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ telle que $\bar{a}\bar{b} = \bar{0}$, on dit que \bar{a} est un diviseur de zéro.

Dans $\mathbb{Z}/15\mathbb{Z}$: On cherche l'inverse de 7 modulo 15.
Autrement dit, l'inverse de $\bar{7}$.
 $\text{PGCD}(7, 15) = 1$. Il existe u et v tels que

$$7u + 15v = 1.$$

S'il n'y a pas de solution évidente à l'équation, on remonte l'algorithme d'Euclide. Ici, il y a une solution évidente :

$$7 \times (-2) + 15 \times 1 = 1.$$

$$7 \times (-2) = -1 \times 15 + 1 \Leftrightarrow 7 \times (-2) \equiv 1 \pmod{15}$$

$$\text{On, dans } \mathbb{Z}/15\mathbb{Z}; \quad \overline{-2} = \overline{15-2} = \overline{13}.$$

$$\text{Donc } 7 \times 13 \equiv 1 \pmod{15}$$

Donc 13 est l'inverse
de 7 modulo 15.

Theorem 6.6

- Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, \bar{a} est inversible si et seulement si $\text{PGCD}(a, n) = 1$.
- Si n est premier, seule $\bar{0}$ n'est pas inversible.
- Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, \bar{a} est un diviseur de zéro si a et n ne sont pas premiers entre eux.

6.5 Théorème chinois des restes

Le théorème chinois des restes, dont le nom renseigne sur l'endroit de première parution, nous montre comment décomposer un ensemble $\mathbb{Z}/n\mathbb{Z}$ sur deux (ou plusieurs) espaces plus simples grâce à la décomposition en facteurs premiers.

Theorem 6.7 Soit $n = n_1 n_2$ avec les nombres n_1 et n_2 premiers entre eux. On note u_1 et u_2 tels que

$$u_1 n_1 + u_2 n_2 = 1,$$

dont l'existence est assurée par le théorème de Bachet–Bezout 5.8. Pour $x \in \mathbb{Z}$,

$$\begin{cases} x \equiv r_1 \pmod{n_1} \\ x \equiv r_2 \pmod{n_2} \end{cases} \iff x \equiv r_2(u_1 n_1) + r_1(u_2 n_2) \pmod{n}.$$

En pratique, cela signifie que l'on peut décomposer $\mathbb{Z}/12\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$. On a

car $12 = 4 \times 3$ et 4 et 3 sont premiers entre eux.

$$10 \equiv 10 \pmod{12} \leadsto \begin{cases} 10 \equiv 1 \pmod{3} \\ 10 \equiv 2 \pmod{4} \end{cases}$$

Réciproquement, $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \end{cases} \leadsto x \equiv ? \pmod{12} ?$

On a

$$4 \times 1 - 1 \times 3 = 1$$

$$(au + bv = 1)$$

$$x \equiv 1[3]$$

$$x \equiv 2[4]$$

$$x \equiv 1 \times 1 \times 4 + 2 \times (-1) \times 3 [12] = -2 [12] = 12 - 2 [12] = 10 [12] \quad \text{☺}$$

évident

$\mathbb{Z}/12\mathbb{Z}$	0	1	2	3	4	5	6	7	8	9	10	11
$\mathbb{Z}/3\mathbb{Z}$	0	1	2	0	1	2	0	1	2	0	1	2
$\mathbb{Z}/4\mathbb{Z}$	0	1	2	3	0	1	2	3	0	1	2	3

théorème
Chinois

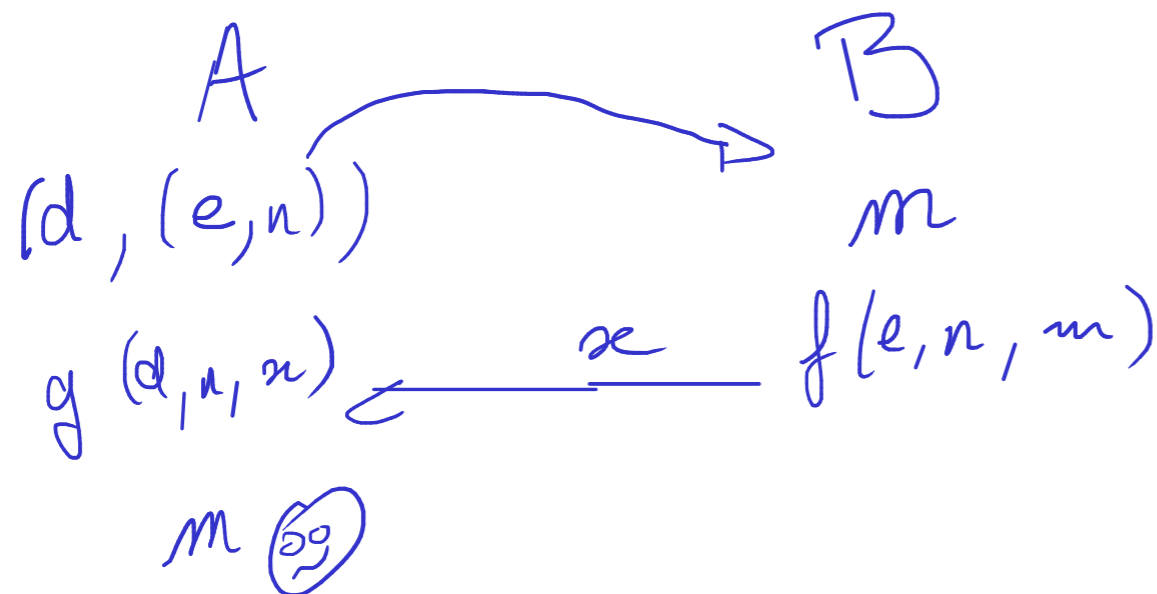
6.6 Codage RSA

Il s'agit d'un codage très populaire, utilisé à une échelle industrielle, sur lequel ont travaillé Rivest, Shamir et Adleman, MIT (USA). R et S sont informaticiens, A est un matheux.

L'idée de RSA est d'utiliser la difficulté de décomposer un nombre en produit de (grand) facteurs premiers. Bref, la méthode est publique, une des clés est publique, les données cryptées sont publiques, mais sans la clé privée, personne ne peut rien faire (attention à l'ordinateur quantique).

6.6.1 Scénario

Alice souhaite que Bob lui envoie un message m . Elle envoie à Bob la clef publique pour chiffrer le message. Ainsi, Alice pourra le déchiffrer grâce à sa clef privée. Le principe de chiffrement est connu tous, les clefs publiques sont connues de tous. On notera e (comme encoding) la clef publique, et d (comme decoding) la clef privée.



Choisissons $n = pq$ où p et q sont des grands nombres premiers distincts. Il est à noter que, connaissant n , il est très difficile de trouver p et q .

Bob va envoyer x tel que

$$x \equiv m^e[n].$$

Alice déchiffrera

$$m \equiv x^d[n].$$

Il reste à choisir d, e , à rendre public (à Bob) la clef (n, e) .

Lemma 6.8 Soit $n = pq$ où p et q sont des nombres premiers distincts. On pose $\varphi(n) = (p-1)(q-1)$. On se donne e premier avec $\varphi(n)$. Soit d un inverse de e modulo $\varphi(n)$. Alors, pour tout entier m ,

$$x \equiv m^e[n] \quad \Rightarrow \quad m \equiv x^d[n].$$

Note. On peut utiliser l'algorithme d'Euclide généralisé pour trouver d et e .

(e, n) chiffrable.

Bob envoie $x \equiv m^e[n]$

$n = pq$, p, q premiers distincts.

$\varphi(n) = (p-1)(q-1)$

e premier avec $\varphi(n)$

d inverse de e modulo $\varphi(n)$

alors $x \equiv m^e[n] \Rightarrow m \equiv x^d[n]$

Preuve: On veut montrer que

$$m \equiv \underbrace{m^{ed}}_{\equiv 1[n]} [n]$$

$ed \equiv 1[\phi(n)]$ d est l'inverse de e mod. $\phi(n)$.

$$ed = k\phi(n) + 1.$$

$$\begin{aligned} m^{ed} &= m^{1+k\phi(n)} \\ &\equiv m \times (m^{\phi(n)})^k [n] \end{aligned}$$

m n'est pas premier avec $n = pq$.

alors m n'est pas premier avec p ou q .
(p et q N premiers), m est multiple de p ou q .

Supposons que p divise m .

$$m \equiv 0 [p]$$

$$m^{ed} - m = ap$$

$$\text{alors } m^{ed} - m = bq.$$

Cf preuve lemme 6.4

Si m est premier avec n ,
d'après le corollaire 6.4,

$$m^{\phi(n)} = m^{(p-1)(q-1)} \equiv 1 [n]$$

$$\text{Donc } m^{ed} = m \times (m^{\phi(n)})^k \equiv m [n]$$

$$m^{ed} = m^{1+k\phi(n)} = m (m^{\phi(n)})^k \equiv m [q] \quad \left/ \begin{array}{l} \text{car} \\ m \text{ premier avec } q \end{array} \right. \left(m^{q-1} \equiv 1 [q] \right)$$

$$\text{LLD } m^{ed} - m \equiv 0 [pq] \Rightarrow m^{ed} \equiv m [n].$$

CQFD

Note. En pratique, c'est une **portion** de message à transmettre qui est d'abord transformée en un nombre x . Plusieurs lettres doivent être groupées pour éviter l'analyse fréquentielle.

Alice souhaite que Bob lui envoie des données cryptées.

Elle fournit (n, e) la clé publique pour crypter

Elle garde (\hat{n}, d) sa clé privée pour de'crypter.

6.6.3 Exemple

deux nombres premiers.

(i) Alice prépare ses clés pour elle et pour Bob.

- Elle choisit $p = 11$ et $q = 23$, d'où $n = 253$. On calcule aussi $\varphi(n) = (p - 1)(q - 1) = 10 \times 22 = 220$.

\uparrow
 pq

- Elle choisit e pour faire la clé publique (n, e) .

e doit être premier avec $\varphi(n)$. On prend $e = 3$, premier avec 220.

Alice fournit la clé publique $(253, 3)$.

- Elle calcule l'inverse d de e modulo $\varphi(n) = 220$:

$$ed \equiv 1[220] \iff 3d \equiv 1[220] \iff 3d - 220k = 1.$$

Utilisons l'algorithme d'Euclide généralisé.

$$220 = 3 \times 73 + 1 \iff 220 - 3 \times 73 = 1.$$

Notons que -73 n'est pas top, et que sa classe d'équivalence est $-73 \equiv 220 - 73[220] \equiv 147[220]$. On gardera $d = 147$.

$$\text{On a } 147 \times 3 = 441 = 2 \times 220 + 1.$$

$$147 \times 3 \equiv 1[220].$$

147 est l'inverse de 3 modulo 220 $\swarrow \varphi(n)$

Clé privée n : (253, 147)

- envoie la clef publique $(253,3)$ et garde sa clé $(253,147)$.

$$x = m^e [n]$$

(ii) Bob crypte son message $m = 123$ par exemple. Il crypte

$$x \equiv 123^3 [253] \equiv 52[253].$$

Bob envoie $x = 52$.

Reçu : $x = 52$

$$m = x^d [n]$$

(iii) Alice déchiffre

$$m \equiv 52^{147} [253] \equiv 123 [253],$$

merci Python ! Alice a déchiffré le bon nombre !