Cryptologie
Les outils arithmétiques

L'Arithmétique, et plus généralement la théorie des groupes, est l'outil mathématique par excellence pour faire de la Cryptologie. Nous présentons ici les connaissances minimales requises pour suivre le cours de Cryptologie de S4 et ce de façon purement arithmétique. Tous ces résultats seront repris dans le cadre du cours de S4Groupe avec le formalisme de la théorie des groupes.
Il est indispensable d'être familier avec les résultats de la première partie. Les résultats de la seconde partie ne sont nécessaires que pour comprendre les preuves des protocoles RSA et Diffie-Hellman.

1 Résultats fondamentaux

1.1 Divisibilité et congruence

Commençons par rappeler des définitions bien connues :

- **Divisibilité**
  Soient a et b deux entiers relatifs (c'est à dire $\in \mathbb{Z}$). On dit que b divise a (ou que a est un multiple de b) s'il existe $n \in \mathbb{N}$ tel que $a = nb$.

- **Division euclidienne**
  Théorème 1 *Pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{N}^*$ il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :*
  $$a = qb + r, \text{ avec } 0 \leq r < b.$$
  q s'appelle le quotient de la division euclidienne de a par b, r s'appelle le reste de la division euclidienne de a par b.

- **Congruence**
  Soit $n \in \mathbb{N}^*$ et soient a et b deux entiers relatifs. On dit que a est congru à b modulo n, noté $a \equiv b\,[n]$, s'il existe $k \in \mathbb{Z}$ tel que $(a - b) = kn$.

La relation de congruence vérifie les propriétés suivantes :

Proposition 1 *Soit $n \in \mathbb{N}^*$, et soit a, b, c et d des entiers relatifs.*

1. *La congruence modulo n est une relation réflexive, symétrique et transitive : c'est une relation d'équivalence (cf S1Logique).*

2. *Si* $a \equiv b\,[n]$ *et si* $c \equiv d\,[n]$ *alors* $a+c \equiv b+d\,[n]$. *On a le même résultat avec la soustraction.*

3. *Si* $a \equiv b\,[n]$ *et si* $c \equiv d\,[n]$ *alors* $ac \equiv bd\,[n]$.

4. *Soit* $m \in \mathbb{N}^*$. *Si* $a \equiv b\,[n]$ *alors* $a^m \equiv b^m\,[n]$.

Démonstration

Le premier point ayant été très détaillé en S1Logique, nous ne reviendrons pas dessus. Supposons que $a \equiv b\,[n]$ *et que* $c \equiv d\,[n]$. *D'après la définition de la congruence, il existe donc deux entiers relatifs,* k_1 *et* k_2, *tels que* $a - b = k_1 n$ *et* $c - d = k_2 n$. *Alors,*

$$(a + c) - (b + d) = (a - b) + (c - d) = k_1 n + k_2 n = (k_1 + k_2)n.$$

On en déduit donc bien que $a + c \equiv b + d\,[n]$, *ce qui démontre 2).*

De la même façon,

$$ac - bd = ac - bc + bc - bd = (a - b)c + (c - d)b = k_1 cn + k_2 bn = (k_1 c + k_2 b)n.$$

On en déduit donc bien que $ac \equiv bd\,[n]$, *ce qui démontre 3).*

Le point 4) se montre directement par récurrence en utilisant le point 3).□

1.2 Classes d'équivalence

Remarquons que deux entiers relatifs a et b sont congrus modulo n si et seulement si ils ont le même reste par la division euclidienne par n (preuve en exercice). On peut regrouper entre eux les entiers relatifs qui sont congrus modulo n ; ces regroupements sont les **classes d'équivalence modulo n**, et il y a autant de classes que de restes possibles par la division euclidienne par n, c'est à dire n. Chaque classe se note $\overline{r}$, où r est le reste correspondant.
Il y a par exemple 4 classes d'équivalence modulo 4 :

- les entiers relatifs dont le reste par la division euclidienne par quatre vaut 0 :

$$\overline{0} = \{..., -8, -4, 0, 4, 8, ...\},$$

- les entiers relatifs dont le reste par la division euclidienne par quatre vaut 1 :

$$\overline{1} = \{..., -7, -3, 1, 5, 9, ...\},$$

- les entiers relatifs dont le reste par la division euclidienne par quatre vaut 2 :

$$\overline{2} = \{..., -6, -2, 2, 6, 10, ...\},$$

- et enfin les entiers relatifs dont le reste par la division euclidienne par quatre vaut 3 :

$$\overline{3} = \{..., -5, -1, 3, 7, 11, ...\}.$$

On note de plus $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n. Ainsi $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, et plus généralement $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-2}, \overline{n-1}\}$.

On peut désormais traduire les points 2) et 3) de la proposition 1 dans le langage des classes d'équivalence : quand on additionne un entier relatif d'un certaine classe avec un entier relatif d'une autre classe, on arrive toujours dans la même classe d'équivalence, idem pour la soustraction et la multiplication.
Par exemple dans $\mathbb{Z}/4\mathbb{Z}$, quand on additionne n'importe quel entier relatif de la classe $\overline{1}$ avec n'importe quel entier de la classe $\overline{2}$, le résultat est **toujours** dans la classe $\overline{3}$.

Ceci permet de définir dans $\mathbb{Z}/n\mathbb{Z}$ une addition notée $\oplus_n$, une soustraction notée $\ominus_n$ et une multiplication notée $\otimes_n$: l'**addition modulo n**, la **soustraction modulo n** et la **multiplication modulo n**. Ainsi si $\overline{p}$ et $\overline{m}$ sont deux classes modulo n, $\overline{p} \oplus_n \overline{m}$ est la classe dans laquelle se trouve le résultat de l'addition de n'importe quel entier relatif de la classe $\overline{p}$ avec n'importe quel entier relatif de la classe $\overline{m}$, idem pour la soustraction et la multiplication.

Exemples dans $\mathbb{Z}/4\mathbb{Z}$:

- $\overline{1} \oplus_4 \overline{3} =$?
  Prenons un entier relatif de $\overline{1}$ et additionnons-le avec un entier relatif de $\overline{3}$, on cherche la classe du résultat. Puisque cela ne dépend pas de notre choix, autant prendre les plus simples : 1 et 3. On a alors :
  $$1 + 3 = 4 \equiv 0\,[4]\,.$$
  Le résultat est donc toujours dans la classe de 0 soit $\overline{1} \oplus_4 \overline{3} = \overline{0}$

- $\overline{1} \ominus_4 \overline{3} =$?
  On procède exactement de la même façon :
  $$1 - 3 = -2 \equiv 2\,[4]\,.$$
  On en déduit que $\overline{1} \ominus_4 \overline{3} = \overline{2}$.

- $\overline{3} \otimes_4 \overline{3} =$?
  On procède exactement de la même façon :
  $$3 \times 3 = 9 \equiv 1\,[4]\,.$$
  On en déduit que $\overline{3} \otimes_4 \overline{3} = \overline{1}$.

On peut faire de même pour toutes les combinaisons de classes, on retrouve alors les résultats contenus dans les tableaux suivants (le tableau se lit de la façon suivante : classe en colonne *opération* classe en ligne) :

$\oplus_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\ominus_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$

$\otimes_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

1.3 Deux exemples fondamentaux

Il y a deux ensembles de classe à connaître absolument pour comprendre le cours de cryptologie : $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/26\mathbb{Z}$. Nous les détaillons ci-dessous.

1.3.1 Étude de $\mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z}$ est l'ensemble des classes d'équivalence modulo 2. Il y en a donc deux : $\overline{0}$ l'ensemble des nombres congrus à 0 modulo 2 (c'est à dire les pairs), $\overline{1}$ l'ensemble des nombres congrus à 1 modulo 2 (c'est à dire les impairs). Les résultats classiques sur la parité (pair+pair=pair, pair×impair=impair etc...) permettent de retrouver facilement les tables des opérations modulo 2 :

$\oplus_2$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\ominus_2$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\otimes_2$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

On remarque que dans ce cas, addition et soustraction sont en fait identiques : ces deux opérations ont exactement les mêmes tables.

Afin de simplifier les notations, nous écrirons désormais $1+0$ à la place de $\overline{1} \oplus_2 \overline{0}$, 1×1 à la place de $\overline{1} \otimes_2 \overline{1}$ etc... Par extension on écrira simplement "+" , ou "-" ou "×" pour désigner les opérations modulo 2 **effectuées bit à bit sur des nombres binaires**. Par exemple, $101 + 001 = (1+0).(0+0).(1+1) = 100$. **Dans tout le cours de cryptologie, ce sont ces opérations que nous effectuerons quand nous ferons des calculs avec des nombres binaires.**
ATTENTION : les opérations modulo 2 sont très différentes et de l'addition binaire classique, et de l'addition booléenne vue en logique. Par exemple $1+1$ vaut 10 pour l'addition binaire classique, 1 pour l'addition booléenne et enfin 0 pour l'addition modulo 2.

1.3.2 Étude de $\mathbb{Z}/26\mathbb{Z}$

$\mathbb{Z}/26\mathbb{Z}$ est l'ensemble des classes d'équivalence modulo 26. Il y en a donc 26 : $\overline{0}$ l'ensemble des nombres congrus à 0 modulo 26, $\overline{1}$ l'ensemble des nombres congrus à 1 modulo 26,..., $\overline{25}$ l'ensemble des nombres congrus à 25 modulo 26. Les tables des opérations modulo 26 sont cette fois très grandes, nous ne les donnerons donc pas.
Comme dans le cas de $\mathbb{Z}/2\mathbb{Z}$, on simplifie les notations on écrivant simplement "+", "-" et "× " pour les opérations modulo 26. On simplifie également la notations des classes mais en utilisant cette fois l'alphabet :

$$a := \overline{0}, b := \overline{1}, c := \overline{2}, ..., y := \overline{24}, z := \overline{25}.$$

Avec ces notations, on a les exemples de calcul suivants : $\mathbf{c} + \mathbf{z} = \mathbf{b}$ (car $2 + 25 = 27 = 1 \times 26 + 1$ soit $\overline{2} + \overline{25} = \overline{1}$), $\mathbf{d} - \mathbf{b} = \mathbf{c}$ (car $3 - 1 = 2$ soit $\overline{3} - \overline{1} = \overline{2}$), ou encore $\mathbf{g} \times \mathbf{u} = \mathbf{q}$ (car $6 \times 20 = 120 = 4 \times 26 + 16$ soit $\overline{6} \times \overline{20} = \overline{16}$).
Comme précédemment, on étendra ces opérations aux chaînes de caractères en les réalisant **caractère par caractère**. Ainsi $cc + zb = (c+z).(c+b) = bd$. **Dans tout le cours de cryptologie, ce sont ces opérations que nous effectuerons quand nous ferons des calculs avec des chaînes de caractères.**

2 Quelques résultats fondamentaux

Nous présentons ici les résultats permettant de prouver la validité des protocole RSA et Diffie-Hellman, avec en point d'orgue le petit théorème de Fermat et son corollaire.
Rappelons tout d'abord le théorème de Gauss (cf S1Logique) :

Théorème 2 *Si a divise bc et si a et b sont premiers entre eux alors a divise c.*

Ce théorème nous permet de prouver les deux corollaires suivants qui seront très pratiques par la suite.

Corollaire 1 *Soient p et q deux nombres premiers entre eux. Si p divise a et si q divise a, alors pq divise a.*

Démonstration
Si p divise a, il existe alors $k \in \mathbb{N}^*$ tel que $a = kp$. Or q divise $a = kp$, et p et q sont premiers entre eux donc q divise k d'après le théorème de Gauss. Il existe donc $k' \in \mathbb{N}^*$ tel que $k = k'q$. On a donc $a = k'pq$ et donc a est bien divisible par pq. □

L'hypothèse d'avoir p et q premiers entre eux est absolument nécessaire dans le corollaire précédent. On peut en effet facilement donner un contre-exemple dans le cas contraire : 4 divise 12 et 6 divise 12, et pourtant $4 \times 6 = 24$ ne divise pas 12.

Corollaire 2 *Soit p est un nombre premier, alors p est premier avec $(p-1)!$.*

Démonstration
Puisque p est un nombre premier, il suffit de montrer que p ne divise pas $(p-1)!$, ce que nous allons prouver par l'absurde.
Supposons que p divise $(p-1)! = (p-1) \times (p-2)!$. Puisque p et $(p-1)$ sont premiers entre eux (p est premier et $p-1 < p$) on déduit du théorème de Gauss que p divise $(p-2)! = (p-2) \times (p-3)!$. Pour les mêmes raisons on en déduit que p divise $(p-3)! = (p-3) \times (p-4)!$ etc... Finalement on en déduit que p divise 1, ce qui est bien entendu faux.□

Nous avons à présent à notre disposition tous les outils nécessaires à la démonstration du petit théorème de Fermat et de son corolaire.

Théorème 3 *Soit p un nombre premier. Pour tout $a \in \mathbb{N}$, $a^p \equiv a\,[p]$.*
Si de plus p ne divise pas a alors $a^{p-1} \equiv 1\,[p]$.

Démonstration
Remarquons que le premier point est un cas particulier très simple du second. En effet si p divise a, alors a et a^p sont tout les deux congrus à 0 modulo p, ils sont donc congrus modulo p. Et si p ne divise pas a, on retrouve que a et a^p sont congrus modulo p en multipliant l'égalité modulaire du deuxième point par a. Reste à montrer le deuxième point.

Considérons les $(p-1)$ nombres a, $2a$, $3a$, ... , $(p-1)a$. Aucun de ces nombres n'est divisible par p, et aucun de ces nombres n'est dans la même classe d'équivalence modulo p ; nous démontrerons ceci en fin de preuve.
Rappelons que les différentes classes d'équivalence modulo p sont $\overline{0}$, $\overline{1}$, $\overline{2}$,...,$\overline{p-2}$, $\overline{p-1}$. Puisque aucun des nombres a, $2a$, $3a$, ... , $(p-1)a$ n'est divisible par p, aucun d'entre eux n'est dans la classe $\overline{0}$. Et puisqu'ils sont tous dans des classes différentes, il y en a exactement 1 dans la classe $\overline{1}$ et donc congru à 1 modulo p, exactement 1 dans la classe $\overline{2}$ et donc congru à 2 modulo p, ... , exactement 1 dans la classe $\overline{p-1}$ et donc congru à $p-1$ modulo p. D'après les règles de calcul sur la congruence (proposition 1), on en déduit que :

$$a \times 2a \times ... \times (p-1)a \equiv 1 \times 2 \times ... \times (p-1)\,[p], \text{ soit que}$$

$$(p-1)!a^{p-1} \equiv (p-1)!\,[p], \text{ soit que}$$

$$(p-1)!(a^{p-1}-1) \equiv 0\,[p].$$

Du dernier point on déduit donc que p divise $(p-1)!(a^{p-1}-1)$. Or p est premier avec $(p-1)!$ d'après le corollaire 2, donc p divise $(a^{p-1}-1)$ d'après le théorème de Gauss. On en déduit que $(a^{p-1}-1) \equiv 0\,[p]$, soit que $a^{p-1} \equiv 1\,[p]$ ce qui est bien la conclusion du petit théorème de Fermat.

Il reste à démontrer les deux affirmations "Aucun de ces nombres n'est divisible par p" et "aucun de ces nombres n'est dans la même classe d'équivalence modulo p".
Si l'un d'entre eux, mettons ka, est divisible par p, alors k est divisible par p d'après le théorème de Gauss ce qui est impossible vu que $0 < k < p$.
De la même façon, si deux d'entre eux, mettons ka et $k'a$ avec $k > k'$, sont dans la même classe d'équivalence modulo p, alors ils ont le même reste par la division euclidienne par p. On en déduis donc que leur différence $(k-k')a$ est divisible par p. Ce qui implique, d'après le théorème de Gauss, que p divise $k-k'$ ce qui est impossible puisque $0 < k-k' < p$. □

Nous pouvons à présent énoncer un corollaire du petit Théorème de Fermat, qui sera le point clé du protocole RSA ainsi que le dernier résultat de ce polycopié.

Corollaire 3 *Soient p et q deux nombres premiers distincts et soit a un nombre premier avec nq. Alors $a^{(p-1)(q-1)} \equiv 1\,[pq]$.*

Démonstration
Puisque a est premier avec pq, alors a est premier avec p et q. D'après le petit théorème de Fermat, on a donc :

$$a^{p-1} \equiv 1\,[p] \text{ et } a^{q-1} \equiv 1\,[q], \text{ soit}$$

$$(a^{p-1})^{q-1} \equiv 1^{q-1}\,[p] \text{ et } (a^{q-1})^{p-1} \equiv 1^{p-1}\,[q], \text{ soit}$$

$$a^{(p-1)(q-1)} \equiv 1\,[p] \text{ et } a^{(p-1)(q-1)} \equiv 1\,[q], \text{ soit}$$

$$a^{(p-1)(q-1)} - 1 \equiv 0\,[p] \text{ et } a^{(p-1)(q-1)} - 1 \equiv 0\,[q].$$

Ce dernier résultat nous indique que $a^{(p-1)(q-1)}-1$ est divisible par p et q, soit que $a^{(p-1)(q-1)}-1$ est divisible par pq d'après le corollaire 1. On a donc que $a^{(p-1)(q-1)} - 1 \equiv 0\,[pq]$, soit que $a^{(p-1)(q-1)} \equiv 1\,[pq]$. □

EXERCICES

Exercice 1

Montrer que deux entiers relatifs a et b sont congrus modulo n si et seulement si ils ont le même reste par la division euclidienne par n.

Exercice 2

1. *Calculer* 3^k *modulo* 5 *pour* $i = 1$, 2, 3 *et* 4.
2. *Faire la division euclidienne de* 2011 *par* 4 *puis calculer* 3^{2011} *modulo* 5.
3. *Calculer* 3^{2011} *modulo* 4.

Exercice 3

Soit C une chaîne de caractères, $C(i)$ désignant le i-ème caractère de C. On partitionne C en blocs de longueur 5. *Donner en fonction de i la position du caractère $C(i)$ dans son bloc. (on attend une réponse de la forme "si $i \equiv$ .... alors $C(i)$ est à la ... position de son bloc".*

Exercice 4

1. *Trouver deux nombres a et b, non divisibles par* 58, *tels que* $ab \equiv 0\,[58]$.
2. *Faire la table de multiplication de* $\mathbb{Z}/6\mathbb{Z}$.
3. *Quels sont les éléments* $\overline{r}$ *de* $\mathbb{Z}/6\mathbb{Z}$ *pour lesquels il existe un autre élément* $\overline{i} \neq \overline{0}$ *vérifiant* $\overline{r} \otimes_6 \overline{i} = \overline{0}$ *?*
4. *Pourriez-vous donner une telle liste dans* $\mathbb{Z}/n\mathbb{Z}$ *pour n quelconque ?*

Exercice 5

1. *Effectuer les calculs suivants dans* $\mathbb{Z}/2\mathbb{Z}$ *:*
   - *10110101+11001100*
   - *11111-10101*
2. *Effectuer les calculs suivants dans* $\mathbb{Z}/26\mathbb{Z}$ *:*
   - *abc+drk*
   - *jud-poi*