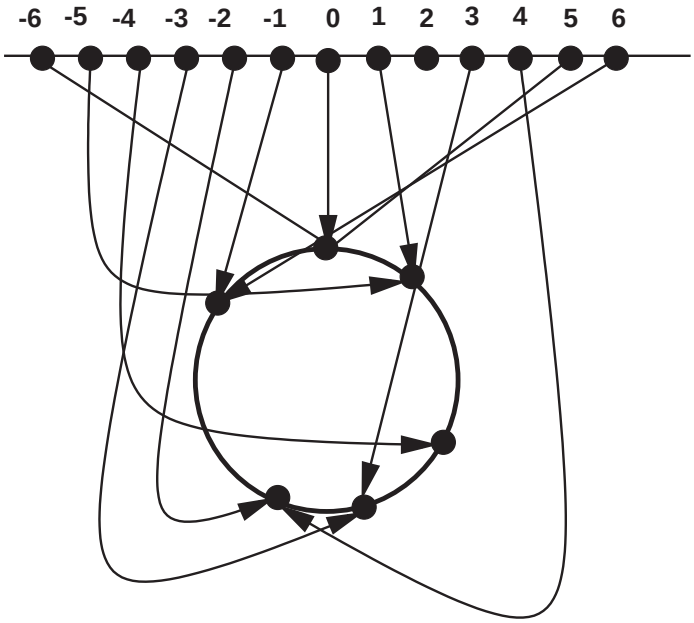
Université de Clermont1
IUT d'Informatique
1ière année -
Denis RICHARD

ARITHMÉTIQUE MODULAIRE et CRYPTOGRAPHIE

ARITHMÉTIQUE MODULAIRE et CRYPTOGRAPHIE

1 Les anneaux $\mathbb{Z}/_{n\mathbb{Z}}$ et la fonction d'EULER

1.1 Enroulement de $\mathbb{Z}$ sur un cercle.



La relation : *être sur un même sommet* se dit de plusieurs façons :
xC_ny ; $x \equiv y(\mod n)$; $\exists k \in \mathbb{Z}(x - y = kn)$

Remarque : Ces relations ne sont intéressantes que pour $n \geq 2$. En effet, pour $n = 0$, la relation C_o est l'égalité, et pour $n = 1$, tous les entiers de $\mathbb{Z}$ sont C_1-équivalents.

Définition 1.1 $x + n\mathbb{Z} = \{x + nz / z \in \mathbb{Z}\}$.

Notation : $x + n\mathbb{Z} = \bar{x} \subset \mathbb{Z}$ mais $\bar{x} \notin \mathbb{Z}$

Théorème 1.1 (fondamental)

i) *Il est vrai que* x ≡ y(mod n) *si et seulement si* x *et* y *ont même reste dans la division par* n. (rappel)

ii) *La relation* C_n *est pour tout* n *une* ***relation d'équivalence***. (réflexive, transitive, symétrique)

iii) *Il y a* n *classes d'équivalence* modulo n *(donc disjointes et recouvrant* $\mathbb{Z}$*) qui sont (par exemple)* $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ *(leur ensemble est noté* $\mathbb{Z}/_{n\mathbb{Z}}$*)*

Exemple *:*

$$\begin{aligned} \mathbb{Z}/_{5\mathbb{Z}} &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} \\ &= \{\overline{-1}, \bar{0}, \bar{1}, \bar{2}, \bar{3}\} \\ &= \{\overline{-2}, \overline{-1}, \bar{0}, \bar{2}\} = \cdots \end{aligned}$$

iv) *L'application* s_n *:* x → x̄ *de* $\mathbb{Z}$ *dans* $\mathbb{Z}/_{n\mathbb{Z}}$ *est surjective.* (surjection canonique)

L'ensemble $\mathbb{Z}$ structuré par les opérations (applications de $\mathbb{Z}\times\mathbb{Z}$ dans $\mathbb{Z}$) d'addition (et $(\mathbb{Z},+)$ est un **GROUPE** et de multiplication (et $(\mathbb{Z},+,\times)$ est un **ANNEAU**.

On voudrait bien structurer $\mathbb{Z}/_{n\mathbb{Z}}$ *comme* l'est $\mathbb{Z}$.

Théorème 1.2 *En posant* $\bar{\mathrm{x}}\oplus\bar{\mathrm{y}}=\overline{\mathrm{x}+\mathrm{y}}$ *et* $\bar{\mathrm{x}}\otimes\bar{\mathrm{y}}=\overline{\mathrm{xy}}$*, on fait de* $(\mathbb{Z}/_{\mathrm{n}\mathbb{Z}},\oplus,\otimes)$ *un* ***anneau commutatif unitaire****.*

Pour prouver le théorème 2, on peut utiliser le lemme suivant :

Lemme 1.1 *Soit* $(\mathrm{A},+,\times)$ *un anneau commutatif et* A' *un ensemble muni de deux opérations* $\oplus,\otimes$.

Soit $\mathrm{f}:\mathrm{A}\to\mathrm{A}'$ *une application telle que :*

$$\left.\begin{array}{rcl}\mathrm{f(x+y)} & = & f(x)\oplus f(y)\\ \mathrm{f(xy)} & = & f(x)\otimes f(y)\end{array}\right\}\text{(homomorphisme d'anneau)}$$

Alors $(\mathrm{f(A)},+,\times)$ *est un anneau commutatif unitaire.*

Exemple : $(Z/_{5\mathbb{Z}},\oplus,\otimes)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Remarque : Tous les éléments de $(\mathbb{Z}/_{5\mathbb{Z}})^*$ sont multiplicativement inversibles :

$$\bar{1}\otimes\bar{1}=\bar{1}\ ;\bar{2}\otimes\bar{3}=1\ ;\bar{3}\otimes\bar{2}=\bar{1}\ ;\bar{4}\otimes\bar{4}=\bar{1}.$$

Cet anneau est un **CORPS**, puisqu'un corps est un anneau unitaire dont tous les éléments non nuls sont multiplicativement inversibles.

Remarques :

☞ Dans $\mathbb{Z}/_{6\mathbb{Z}}$, on aura $\bar{3}\neq\bar{0}$, $\bar{2}\neq\bar{0}$ mais $\bar{3}\otimes\bar{2}=\bar{0}$ de sorte que ($\mathbb{Z}/_{n\mathbb{Z}}$ peut contenir des **DIVISEURS** de **zéro**).

☞ Les règles et résultats connus dans les corps $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ ne fonctionnent en général pas dans $\mathbb{Z}/_{n\mathbb{Z}}$. Ainsi

$\bar{4}x=\bar{0}$ possède 4 solutions dans $\mathbb{Z}/_{16\mathbb{Z}}$ et

$\bar{4}x=\bar{6}$ n'en a pas dans le même anneau.

☞ Le système $\left.\begin{array}{rcrcl}\bar{2}x & + & \bar{3}y & = & \bar{5}\\ \bar{9}x & + & \bar{2}y & = & \bar{2}\end{array}\right\}$ n'a pas de solution dans $\mathbb{Z}/_{23\mathbb{Z}}$.

☞ Les anneaux $\mathbb{Z}/_{n\mathbb{Z}}$ qui sont des corps (finis et utiles en théorie des codes) sont caractérisés par le :

Théorème 1.3 $\mathbb{Z}/_{\mathrm{n}\mathbb{Z}}$ *est un* ***corps*** *si et si seulement si* n *est* ***premier****.*

Exercices :

1) Résoudre dans $\mathbb{Z}/_{13\mathbb{Z}}$ l'équation $x^2 + x - \bar{2} = \bar{0}$.

2) Résoudre, dans $\mathbb{Z}/_{24\mathbb{Z}}$, les deux équations :
$$(\bar{2})^x - (\bar{5})^y = \bar{1} \text{ et } (\bar{2})^x - (\bar{5})^y = \bar{1}.$$

Soit $(G, ^*)$ un groupe dont e est l'élément neutre muni d'une opération externe ainsi définie :

$$\left\{ \begin{array}{l} \mathbb{Z} \times G \to G \text{ en posant } \left\{ \begin{array}{lcl} 0.g & = & e \\ 1.g & = & g \end{array} \right. \\ (z, g) \to z.g \end{array} \right.$$

si $n \in \mathbb{N}$ alors $(n+1).g = ng^*g$.
Si $z \in \mathbb{Z}$ alors $z.g$ = l'opposé de G de $(-z).g$.

Définition 1.2 - *Un groupe* $(\mathrm{G}, +)$ *additif est dit* ***cyclique*** *si et seulement si*
$$\exists \mathrm{a} \in \mathrm{G} \forall \mathrm{x} \in \mathrm{G} \exists \mathrm{z} \in \mathbb{Z} (\mathrm{x} = \mathrm{z.a}).$$

- *Un groupe* $(\mathrm{H}, \times)$ *multiplicatif est dit* ***cyclique*** *si et seulement si*
$$\exists \mathrm{a} \in \mathrm{H} \forall \mathrm{x} \in \mathrm{H} \exists \mathrm{z} \in \mathbb{Z} (\mathrm{x} = \mathrm{a}^{\mathrm{z}}).$$

Exemple :

$((\mathbb{Z}/_{27\mathbb{Z}})^*, \times)$ est **cyclique**

$((\mathbb{Z}/_{27\mathbb{Z}})^*, \times)$ est isomorphe à $(\mathbb{Z}/_{18\mathbb{Z}}, +)$

x	1	2	4	5	7	8	10	11	13
$\varphi(x)$	2^{18}	2^1	2^2	2^5	2^{16}	2^3	2^6	2^{13}	2^8

x	14	16	17	19	20	22	23	25	26
$\varphi(x)$	2^{17}	2^4	2^{15}	2^{12}	2^7	2^{14}	2^{11}	2^{10}	2^9

Ce n'est pas un hasard :

Théorème 1.4
1)Tout groupe cyclique de cardinal $\mathrm{n} \geq 1$ *est isomorphe à* $(\mathbb{Z}/_{\mathrm{n}\mathbb{Z}}, +)$.
2) Tout groupe cyclique infini est isomorphe à $\mathbb{Z}$.

Théorème 1.5 *Si* a *et* b *premiers entre eux, alors* $\mathbb{Z}/_{\mathrm{a}\mathbb{Z}} \times \mathbb{Z}/_{\mathrm{b}\mathbb{Z}} = \mathbb{Z}/_{\mathrm{ab}\mathbb{Z}}$.

Très classiques et indispensables en théorie des nombres sont :

Théorème 1.6 (EULER)
Soit $\mathrm{a} \in (\mathbb{Z}/_{\mathrm{n}\mathbb{Z}})^*$ *(c'est-à-dire* a *inversible).*
Soit $\varphi(\mathrm{n})$ *le nombre d'éléments de* $(\mathbb{Z}/_{\mathrm{n}\mathbb{Z}})^*$.
Alors $\mathrm{a}^{\varphi(\mathrm{n})} = \bar{1}$.

qui a pour corollaire :

Théorème 1.7 (FERMAT)
Si p *premier et* $\mathrm{a} \in \mathbb{Z}$, *alors* $\mathrm{a}^{\mathrm{p}} \equiv \mathrm{a}(\mod \mathrm{p})$.

et enfin

Théorème 1.8 (WILSON)
Un entier $\mathrm{p} > 1$ *est premier si et seulement si* $\overline{(\mathrm{p}-1)!} = \bar{1}$ *dans* $\mathbb{Z}/_{\mathrm{p}\mathbb{Z}}$.

2 Indicateur d'EULER

Si G est un groupe fini d'ordre n, on désignera par $\varphi_G(d)$, pour d diviseur de n, le nombre d'éléments de G qui sont d'ordre d.

On a donc $\varphi_G(1) = 1$

$$n = \sum_{d|n} \varphi_G(d).$$

Par définition, l'**Indicateur d'EULER** est la fonction φ définie par $\varphi(n) = \varphi_{\mathbb{Z}/_{n\mathbb{Z}}}(n)$, pour tout entier n non nul.

Proposition 2.1 $\varphi(\mathrm{n})$ *est égal*
1) au nombre de générateur de $\langle \mathbb{Z}/_{\mathrm{n}\mathbb{Z}}, + \rangle$,
2) au nombre d'entier inférieurs à n *et premiers avec* n,
3) au nombre d'éléments inversibles de $\mathbb{Z}/_{\mathrm{n}\mathbb{Z}}$.

Proposition 2.2 (calcul de φ)
1) $\varphi(\mathrm{n}) > 0$.
2) Si p *est un entier premier et* $\mathrm{s} \geq 1$ *:*

$$\varphi(\mathrm{p}) = \mathrm{p} - 1 \quad et \quad \varphi(\mathrm{p^s}) = \mathrm{p^s} - \mathrm{p^{s-1}} = \mathrm{p^{s-1}}(\mathrm{p} - 1).$$

3) Si m *et* n *sont premiers entre eux :*

$$\varphi(\mathrm{mn}) = \varphi(\mathrm{m}).\varphi(\mathrm{n}).$$

4) Si $\mathrm{n} > 0$, *on a*

$$\mathrm{n} = \sum_{\mathrm{d|n}} \varphi(\mathrm{d}).$$

Théorème 2.1 (2ème théorème d'EULER)
Si k *est un entier et si* n *et un entier* ***sans facteur carré****, alors* $\mathrm{m^{k\varphi(n)+1}} \equiv \mathcal{M}$*, pour tout entier* m.

3 Cryptographie

3.1 Le sac-à-dos

Problème :
On se donne des **paquets** de contenance $C_1, C_2, \ldots, C_n$ et un sac-à-dos de contenance C.

On veut **REMPLIR** le sac au maximum, c'est-à-dire qu'on cherche des *variables booléennes* x_i, pour décider si un paquet c_i est -ou non- mis dans le sac.

Soit $(x_1, x_2, \ldots, x_n)$ tel que $\sum x_i c_i = C$ avec $x_i \in \{0, 1\}$.

1358	
679	$0 \times 1358 + 1 \times 679 + 1 \times 340 + 1 \times 169 + 0 \times 83 +$
340	$1 \times 41 + 1 \times 20 + 1 \times 11 + 0 \times 5 +$
169	$0 \times 3 = 1260$ 1260
83	*Message transmis* $\boldsymbol{M = 0011101110}$
41	
20	Sac-à-dos *facile* : $c_j > \sum_{i=1}^{j-1} ci$
11	
5	
3	

3.2 Méthode de cryptage dite du sac-à-dos

☞ Le chef (de réseau)

CHOISIT $(C_1, \ldots, C_n)$ formant un sac-à-dos facile :

$$\forall j \leq n \Big(C_j > \sum_{i=1}^{j-1} Ci) \Big).$$

CHOISIT $N > C_1 + C_2 + \cdots + C_n$
D tel que pgcd $(N, D) = 1$
D' tel que $DD' \equiv 1$ (mod N).

CALCULE pour tout $i \in [1, n]$
$a_i \equiv c_i D'$ (mod N).

PUBLIE $a_1, a_2, \ldots, a_n$ et N.

GARDE SECRET $C_1, C_2, \ldots, C_n$ et D et D'.

☞ Celui qui veut envoyer un message (au chef),

CODEÊ M sur n bits $M = (x_1, x_2, \ldots, x_n)$,

CALCULE $C \equiv a_1x_1 + a_2x_2 + \cdots + a_nx_n$ (mod N).

ENVOIE publiquement le **CRYPTOGRAMME** C.

☞ Le chef **CALCULE**

$$DC \equiv \sum_{i=1}^{n} Da_ix_i \equiv \sum_{i=1}^{n} DD'c_ix_i \equiv \sum_{i=1}^{n} c_ix_i < N.$$

RESOUD le problème du sac-à-dos (facile) et trouve M.

ALICE envoie	LLAIC 1
Texte en clair	**DES CRÉDITS (HELP)**
Message M codé $\{0,1\}^*$	00111 01110 10110
Bloc de n bits $x = (x_1, x_2, \ldots, x_n)$ $y = (y_1, y_2, \ldots, y_n)$	(10 bits) $x = (0,0,1,1,1,0,111,0)$ $y = \ldots$
CLÉ (PUBLIQUE) Cryptogramme $(a_1, a_2, \ldots, a_n) C_1 = \Sigma a_ix_i$ $C_2 = \Sigma a_iy_i$	CLÉ PUBLIQUE (2292, 1089, 211, 1625, 1283, 599, 759, 315, 2597, 2463)
TRANSMISSION (PUBLIQUE)	$C_1 = 0 \times 2292 + 0 \times 1089 + 211 + 1 \times 1625$ $+1 \times 1283 + 0 \times 599 + 1 \times 759 + 1 \times 315$ $+1 \times 2597 + 0 \times 2463 = 6790$

	Cryptogramme	TRANSMISSION	
CLÉS SECRÈTES	Transformé		
de BOB	$C_1' \equiv DC_1(N)$	Clés secrètes	C_1' est
	$C_2' \equiv \ldots$	$N = 2731$	6790×1605
D, N, (D')		$D = 1605$	(mod 2731)
		$D' = 764$	$= 1260$
↓	Résolution		
	Sac-à-dos (facile)	↓	
$(C_1, C_2, \ldots, C_n)$	$C_1' \equiv \Sigma x_ic_i(N)$	$(C_1, C_2, \ldots, C_n)$	$C_1 = C \times 1358$
$C_i = Da_i$	$C_2' \equiv$	=(3,5,11,20	$+1 \times 679 + 1 \times 340$
		41,83,169	$+1 \times 169 + 0 \times 83$
	M codé $\{0,1\}$	340,679,1358)	$+1 \times 41 + 1 \times 20$
Texte en clair	(sac-à-dos facile)	$+1 \times 11 + 0 \times 5$	
	reçu par BOB		$+0 \times 3 = 1260$

$\boldsymbol{x = (0,0,1,1,0,1,1,1,0)}$.

AVANTAGES	INCONVÉNIENTS
Facilités utilisation clé publique	**Disymétrie émetteur-récepteur**

3.3 La fameuse méthode (R.S.A.)

[Rivest Shamir Adleman]

- Nombres publics et nombres secrets

1) **CHOISIR** deux nombres premiers p et q de cinquante chiffres environ.

2) **CALCULER** $n = pq$ et $\varphi(n) = (p-1)(q-1)$.

3) **CALCULER** e tel que $ed \equiv 1 \pmod{\varphi(n)}$.

n et e sont **publics**.
p, q, $\varphi(n)$ et d sont **secrets**.

- Émission et réception des messages

ALICE veut envoyer le message M à BOB.

BOB a publié n et e.

ALICE VÉRIFIE $M < n$,
CALCULE le cryptogramme $C \equiv M^e \pmod{n}$
ENVOIE C.

BOB CALCULE : $C^d \equiv (M^e)^d = M^{k\varphi(n)+1} \equiv M \pmod{n}$
[car si r *est sans facteur carré* et $r \equiv 1 \pmod{\varphi(n)}$ alors $a^r \equiv a \pmod{n}$ pour tout $a \in \mathbb{Z}$.]

Avantages :
1) Clés publiques
2) Le calcul de d à partir de e équivaut à la factorisation de l'entier n : très difficile si n grand. On verra que c'est un problème NP complet.

Exemple d'application de la méthode RSA :

Soit à coder un message à écrire ci-dessous

				□					□					□	□
					□				□						□
					□				□					□	□

NUMÉRISÉ à partir de

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
1	3	4	6	5	8	10	11	9	12	15	14	16	17	18	19	20	21	21

t	u	v	w	x	y	z
7	13	1	23	24	25	26

et ponctuation ad libitum.

Considérons par exemple $n = 55$, $e = 3$ (publiés), correspondant à :
$p = 5$, $q = 11$, $\varphi(n) = 40$ et $d = 27$ car $3 \times 27 = 81 \equiv 1 \ (\mod 40)$.
Soit $C = (1, 14, 1, 15, 49, 14, 52, 13)$ le cryptogramme envoyé par ALICE.

C	1	14	1	15	49	14	52	13
$C^d M$	1	9	1	5	14	9	13	7

Connaissant M la numérisation de l'aphabet donnée ci-dessus fournit le message en clair.

Le calcul de a^b modulo n peut être programmé de façon rapide en écrivant b en base 2, et en utilisant la suite des restes modulo n des entiers

$$a,\ a^2,\ a^{(2^2)} = \left(a^2\right)^2, a^{(2)^3} = \left(a^{(2^2)}\right)^2, \text{ etc.}$$

Exemple : Calculer y^{1503} avec 18 multiplications seulement.