Eléments mathématiques pour la cryptographie à clé publique

deuxième séance

Définition 1. *Groupe cyclique*

Un groupe (G,), de cardinal n, est dit cyclique lorsqu'il existe (au moins) un élément d'ordre n.*

Exemple 2. (Z/nZ,$\oplus$) est cyclique: voir ordre de $\bar{1}$

Remarque 3.

Attention: tout groupe n'est pas forcément cyclique.

D'abord parce qu'il y a des groupes infinis comme $(\mathbb{Z}, +)$

Ensuite parce qu'il y a des groupes finis qui ne sont quand même pas cycliques, comme le prouve l'exemple suivant:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Ordre de e 1

ordre de a 2

ordre de b 2

ordre de c 2

Remarque 4. (fondamentale)

Soit un groupe (G,*), de cardinal n, cyclique, et a un élément d'ordre n, alors

$\{a, a*a, a*a*a, ..., a*....*a\,(n-1\,\text{fois}), a*....*a(n\,\text{fois}) = e\} = G;$

tous les éléments de G peuvent être « produits » à partir de a.

on dit que « a engendre G »

Théorème 5.

1. Pour tout n le groupe (Z/nZ,$\oplus$) est cyclique

2. Les générateurs de $(Z/nZ,\oplus)$ sont les $\bar{a}$ tels que $a \wedge n = 1$

Exercice 1. Soit le groupe $(\mathbb{Z}/15Z, \oplus)$.

a. Déterminer ses générateurs.

b. Vérifier pour chacun qu'il « fabrique » effectivement tout le groupe en écrivant la liste $[a, a \oplus a, a \oplus a \oplus a, ...,$ $a \oplus .... \oplus a\ (n-1 \text{ fois}), a \oplus .... \oplus a (n \text{ fois}) = e]$.

c. Déterminer la liste des éléments que l'on peut « fabriquer » avec $\bar{6}$.

Théorème 6. *Procédure maxima*

generateurs(modulo):=block([k,L],k:1,L:[],while(k<modulo)do((if gcd(k,modulo)=1 then (L:endcons(k,L)))k:k+1,return(L))dollar

Théorème 7.

Soit un groupe de cardinal commutatif (G,) de cardinal n, tout élément a un ordre qui divise n.*

Exercice 2. Soit le groupe $(\mathbb{Z}/12Z, \oplus)$ déterminer les ordres de chacun de ses éléments.

Exercice 3. Même question avec Maxima et $(\mathbb{Z}/165Z, \oplus)$

2.2 (Z/nZ,⊕, ⊙)

On peut aussi définir une multiplication modulo n

Exemple 8.

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Théorème 9. *$(Z/nZ,\oplus,\odot)$ est un anneau commutatif*

(en gros les propriétés de calcul commmode de $(\mathrm{Z},+,\times)$ sont aussi vraies dans $(\mathrm{Z/nZ},\oplus,\odot)$.

Théorème 10. *TRES IMPORTANT pour simplifier les calculs*

Soit $(Z/nZ,\oplus,\odot)$ si $a \equiv b$ modulo (n) et $x \equiv y$ modulo (n) alors $ax \equiv$by modulo (n)

***Exemple* 11.** *n=124*

pour *calculer* $\bar{18} \odot \bar{35} \odot \bar{46}$

au lieu de calculer d'abord $18 \times 35 \times 46 = 28980$ *puis 28980 modulo (124)= 88*

on calculera d'abord $18 \times 35 = 630$

puis 630 modulo (124)=10

puis $10 \times 46 = 460$

et 460 modulo (124)= 88

Exercice 4. Calculer $\overline{13}^{12}$ dans (Z/51Z,$\oplus, \odot$)

Théorème 12. *procédure maxima*

*multimod(a,b,modulo):=block([c],c:mod(a*b,modulo),return(c))$*

LES INVERSIBLES

Définition 13. *Les inversibles de l'anneau (Z/nZ,*$\oplus, \odot$*) sont les éléments* $\bar{a}$ *pour lesquels il existe* $\bar{b}$ *vérifiant* $\bar{a}\bar{b} = \bar{1}$.

Théorème 14.

1. Les inversibles de l'anneau (Z/nZ,$\oplus, \odot$*) forment un groupe (multiplicatif), noté* $(R_n, \odot)$

2. Les inversibles de l'anneau (Z/nZ,$\oplus, \odot$*) sont les éléments* $\bar{a}$ *tels que* $a \wedge n = 1$.

Exercice 5.

Déterminer dans (Z/15Z,$\oplus, \odot$) les éléments $\bar{a}$ tels que $a \wedge 15 = 1$ et vérifier qu'ils sont inversibles en trouvant leurs inverses.

Exercice 6.

Déterminer les éléments inversibles de (Z/24Z,$\oplus, \odot$)

Théorème 15. *Calcul de l'inverse dans (Z/nZ,*$\oplus, \odot$*)*

Soit n un entier naturel non nul et $a \wedge n = 1$

1. $\bar{a}$ *est inversible dans l'anneau (Z/nZ,*$\oplus, \odot$*)*

2. L'inverse de $\bar{a}$ *est* $\bar{u}$ *tel que au+nv=1*

Exercice 7. On considère (Z/128Z,$\oplus, \odot$)

1. Déterminer si $\bar{5}$ y est inversible
2. Si oui déterminer son inverse
3. Mêmes questions pour $\overline{66}$

Théorème 16. *procédure maxima*

invmodulo(a,modulo):=block([r,u,v,r1,u1,v1,r2,u2,v2],r1:a,u1:1,v1:0,r2:modulo,u2:0,v2:1,

while(r2>0)do(([r,u,v]:[r2,u2,v2],[r2,u2,v2]:[r1,u1,v1]-
quotient(r1,r2)[r2,u2,v2],[r1,u1,v1]:[r,u,v]),return(second([r1,u1,v1])))$*

Question 17. *Combien d'inversibles dans (Z/nZ,$\oplus, \odot$) ?*

Définition 18. *La fonction φ d'Euler*

Pour tout n on désigne par $\varphi(n)$ le cardinal de $\{a \in \{0,1,...,n-1\}, a \wedge n = 1\}$.

Théorème 19. *Calcul de $\varphi(n)$*

1. Si p est premier $\varphi(p^k) = p^k(1-1/p)$

2. Si $a \wedge b = 1$, $\varphi(\mathrm{ab}) = \varphi(a)\varphi(b)$

3. Si n a pour factorisation en produit de puissances de premiers $n = \prod_{i=1}^{r} p_i^{k_i}$, alors $\varphi(n) = n\prod_{i=1}^{r}(1-1/p_i)$.

Exercice 8. Déterminer $\varphi(24)$ et les $\varphi(24)$ éléments inversibles de l'anneau $(\mathrm{Z}/24\mathrm{Z}, \oplus, \odot)$

Théorème 20.

Avec Maxima la fonction φ s'appelle « totient »

LE GROUPE DES INVERSIBLES

2.3 $(R_n, \odot)$

Définition 21.

Soit un entier n, on désigne par R_n l'ensemble des éléments inversibles de l'anneau (Z/nZ,$\oplus, \odot$)

Théorème 22. *Soit un entier n>1*

1. $(R_n, \odot)$ est un groupe de cardinal $\varphi(n)$

2. $\forall \bar{a} \in R_n, \bar{a}^{\varphi(n)} = \bar{1}$ (théorème d'Euler)

3. Si p est premier, $\forall \bar{a} \in R_p$, $\bar{a}^{p-1} = \bar{1}$; c'est à dire Si p est premier, $\forall a$, $a \wedge p = 1 \Longrightarrow a^{p-1} \equiv 1[p]$(th de Fermat).

C'EST TOUT SIMPLEMENT le THEOREME 29 du chapitre 1

Exercice 9. Soit n=40

a. Déterminer la liste des éléments de R_{40}.

b. Déterminer les ordres de chacun de ces éléments.

c. Le groupe $(R_{40}, \odot)$ est-il cyclique ?

Exercice 10. Soit n=17

a. Déterminer la liste des éléments de R_{17}.

b. Déterminer les ordres de chacun de ces éléments.

c. Le groupe $(R_{17}, \odot)$ est-il cyclique ?

Théorème 23. *Procédure maxima*

R(modulo):=block([k,L],k:1,L:[],while(k<modulo)do((if gcd(k,modulo)=1 then (L:endcons(k,L)))k:k+1,return(L))dollar

SI n est un nombre premier tout est plus simple

Théorème 24.

Soit un entier premier p

1. $\forall \bar{a} \in R_p, \bar{a}^{\,p-1} = \bar{1}$ *; c'est à dire Si p est premier,* $\forall a, a \wedge p = 1 \Longrightarrow a^{p-1} \equiv 1[p]$(th de Fermat).

Mieux encore

2. Le groupe $(R_p, \odot)$ *est cyclique.*

Exercice 11. A la recherche d'un générateur

Déterminer (en testant autant d'éléments qu'il le faudra) un générateur du groupe cyclique $(R_{19}, \odot)$.

ATTENTION ici le groupe $(R_p, \odot)$ est multiplicatif

Problème 1. On considère l'anneau (Z/165Z,$\oplus, \odot$)

1. Déterminer si $\bar{3}$ est inversible
2. Montrer que $\bar{4}$ est inversible
3. Déterminer son inverse
4. Déterminer le nombre d'éléments inversibles

Problème 2. à préparer pour le TD

Recherche avec Maxima d'un générateur du groupe $(R_{263}, \odot)$

1. La fonction primep qui s'utilise commme suit: « primep(263); » permetrra de véridier si 263 est premier
2. Déterminer le nombre d'éléments de R_{263}.
3. Déterminer les ordres possibles des éléments de $(R_{263}, \odot)$
4. On pourra utiliser les procédures suivantes pour trouver un générateur de $(R_{263}, \odot)$

ord(a,n):=block([aa,k],aa:a,k:1,while(aa>1)do(aa:mod(aa*a,n),k:k+1),return(k))dollar

cherchegene(n):=block([b,u,v],b:1,u:totient(n),v:ord(b,n),while(v<u)do(b:b+1,v:ord(b,n)),return(b))dollar

5. Déterminer laliste des générateurs du groupe $(R_{263}, \odot)$

Travaux dirigés

Exercice 12.

On considère l'ensemble Z/46Z

1. Pour la loi d'addition modulo 46 (Z/46Z,$\oplus$) est un groupe. Déterminer

a. Le symétrique de $\overline{24}$

b. Si $\overline{21}$ est un générateur

c. La (ou les) solutions de l'équation $x + \overline{37} = \overline{19}$

2. Pour les deux lois, addition modulo 46 et multiplication modulo 46, (Z/46Z,$\oplus, \odot$) est un anneau

o. Calculer $\overline{31} \otimes \overline{52}$; $\overline{23} \otimes \overline{18}$

a. Déterminer le nombre de ses éléments inversibles

b. Déterminer l'inverse de $\overline{13}$

c. Déterminer l'inverse de $\overline{45}$

3. Résoudre l'équation $\overline{13} \otimes x = \overline{18}$

4. Résoudre l'équation $\overline{13} \otimes x \oplus \overline{21} = \overline{18}$

Exercice 13. On considère l'anneau $(Z/43Z, \oplus, \otimes)$

1. Déterminer le nombre d'éléments inversibles

2. Déterminer l'inverse de $\overline{13}$

3. Déterminer la valeur de $\overline{13}^{42}$

4. Déterminer la valeur de $\overline{45}^{43}$

5. Expliquer pourquoi $\overline{45}^{6000} = \overline{45}^{36}$

6. Soit x$\in R_{43}$ expliquer pourquoi x^{5*17}=x

Exercice 14. On considère le groupe $(R_{33}, \odot)$

1. Déterminer le nombre de ses éléments.

2. Déterminer l'ordre de chacun de ses éléments.

3. Ce groupe est-il cyclique ?

4. Soit x$\in R_{33}$, que vaut x^{10} ?

5. Trouver le plus petit entier strictement positif d tel que $\forall x \in R_{33}, x^d = \bar{1}$.

6. On désigne par f l'application x$\in R_{33} \longmapsto x^3$.

a. Trouver un entier u tel que $3u \equiv 1[10]$

b. Expliquer pourquoi $\forall x \in R_{33}, x^{3u} = x$.

c. Expliquer pourquoi l'application réciproque de f est x$\in R_{33} \longmapsto x^u$.

---------- FIN

3. Cryptographie à clé publique, RSA

l'objectif est de réaliser le schéma suivant

- Texte clair M $\xrightarrow[\mathcal{E}_K]{\text{chiffrement}}$ Texte crypté $M'=\mathcal{E}_K(M)$ $\xrightarrow[\mathcal{D}_{K'}]{\text{déchiffrement}}$ $\mathcal{D}_{K'}(M')=\mathcal{D}_{K'}\circ\mathcal{E}_K(M)=M$

Il existe des systèmes de cryptage à « clé secrète » (ou systèmes symétriques) dans lesquels l'algorithme de chiffrement et l'algorithme de déchiffrement sont facilement dérivées l'un de l'autre; par suite celui qui connait l'un connait l'autre, ce qui impose d'une part de conserver le secret, d'autre part de commmuniquer (avec prudence) entre l'émetteur et le destinataire, qui ont besoin de partager le secret de la méthode.

Depuis quelques dizaines d'années existent des systèmes de cryptage à « clé publique », dans lesquels il n'est besoin d'aucune communication privée entre l'émetteur et le destinataire, parce qu'il n ' y a plus de symétrie, la connaissance de l'algorithme de chiffrement ne permet en aucun cas de connaître l'algorithme de déchiffrement.

C'est le cas de l'algorithme RSA (bien connu mais ce n'est pas le seul). 1978

3.1 l'idée c'est Euler + Bezout...

Soit un entier n>1 et $\varphi(n)$ le cardinal du groupe $(R_n,\odot)$ alors $\forall\bar{a}\in R_n,\bar{a}^{\,\varphi(n)}=\bar{1}$; si on considère un entier e, premier avec $\varphi(n)$ alors on sait trouver deux entiers relatifs (u,d) tels que $u\varphi(n)+\text{de}=1$

alors $\bar{a}^{\,u\varphi(n)+\text{de}}=\bar{a}^{\,1}=\bar{a}$, mais par ailleurs $\bar{a}^{\,u\varphi(n)+\text{de}}=\bar{a}^{\,u\varphi(n)}\bar{a}^{\,\text{de}}=\bar{1}\,\bar{a}^{\,\text{de}}=\bar{a}^{\,\text{de}}$;

en conclusion, $\bar{a}^{\,\text{de}}=\bar{a}$.

Supposons que le message à coder soit: $\bar{a}$

l'émetteur le chiffre comme suit: $\bar{a}\longrightarrow\bar{b}=\bar{a}^{\,e}$; c'est à dire il envoie $\bar{b}$

le destinataire reçoit $\bar{b}$ et, pour déchiffrer, il opère comme suit: $\bar{b}\longrightarrow\bar{b}^{\,d}$ et il obtient qui vaut $(\bar{a}^{\,e})^d=\bar{a}^{\,\text{de}}=\bar{a}$.

donc

on chiffre en élevant à la puissance e, on déchiffre en élevant à la puissance d.

3.2 Mais qui sait quoi ?

1. L'émetteur sait qu'on calcule modulo n et qu'il élève à la puissance e.

Il n'a pas besoin de connaître $\varphi(n)$, ni d.

2. Le destinataire a besoin de savoir qu'on calcule modulo n et de connaître d et, bien sûr, d doit être secret, sinon toute personne qui met la main sur le message crypté (qui vaut b) pourrait le déchiffrer.

3. Donc le destinataire doit être le seul à connaître d, tandis que le même e peut être utilisé et connu par tout le monde.

4. Comment faire ?

En fait le chef d'orchestre c'est le destinataire; il dit en public

« toute personne qui veut m'écrire, on se placera modulo n, et vous élèverez le message $\bar{a}$ à la puissance e ».

5. Comment faire pour que, même si tout le monde connaît n et e, il leur soit difficile de trouver tous seuls d ?

Il faut que la connaissance de n ne permette pas facilement de trouver $\varphi(n)$; or, dès qu'est connue la factorisation de n en produit de puissances de premiers, on est en en mesure de trouver $\varphi(n)$.

Donc la clé c'est n. Comment rendre difficile de trouver sa factorisation ?

6. Pour que la recherche des diviseurs de soit difficile il faut qu'ils soient grands; on prendra n=pq, deux facteurs premiers tous les deux grands, plus ou moins proches.

3.3 Cryptage et authentification

Soient donc Alice et Bob.

Supposons que Alice a publié son n, noté n_A et l'entier e_A qu'elle a choisi premier avec $\varphi(n_A)$ qu'elle seule connaît; Alice a déterminé d_A mais ne le rend surtout pas public.

De même Bob a publié son n, noté n_B et l'entier e_B qu'il a choisi premier avec $\varphi(n_B)$; Bob a déterminé d_B, mais ne le rend surtout pas public.

3.3.A

Si Bob veut envoyer le message x à Alice, où $x \wedge n_A = 1$, il envoie $\bar{x'} = \bar{x}^{\,e_A}$ et Alice calcule $\bar{x'}^{d_A}$ ce qui lui donne $\bar{x}$.

3.3.B

Si Alice veut envoyer le message y à Bob, où $y \wedge n_B = 1$, elle envoie $\bar{y'} = \bar{y}^{\,e_B}$ et Bob calcule $\bar{y'}^{d_B}$ ce qui lui donne $\bar{y}$.

3.3.AA Et si Bob veut prouver à Alice qu'il est bien Bob

Soit la signature bob de Bob, Bob envoie à Alice le message $\bar{z'} = \overline{\text{bob}}^{\,d_B e_A}$, elle l'élève à la puissance $d_A e_B$; si Bob est Bob alors le message qu'elle a déchiffré est la signature de Bob, sinon elle n'obtient pas la signature de Bob.

3.3. BB De même si Alice veut prouver à Bob qu'elle est bien Alice

Soit la signature ali d'Alice, Alice envoie à Bob le message $\overline{w'} = \overline{\text{ali}}^{\,d_A e_B}$, il l'élève à la puissance $d_B e_A$; si Alice est Alice alors le message qu'il a déchiffré est la signature d'Alice, sinon il n'obtient pas la signature d'Alice.

Exercice 15. Exponentiation rapide

a. Soit n=323

Vérifer que le calcul de 201^{99} pose un problème technique

Proposer une méthode de calcul de 201^{99} mod(323)

b. Ecrire 99 en base 2

Montrer qu'au moyen de calculs succesifs de carrés on peut trouver rapidement 201^{64} mod(323)

Exploiter l'écriture de 99 en base 2 pour trouver une méthode de calcul rapide et réaliste de 201^{99} mod(323)

Exercice 16.

i. Factoriser 323 en produit de facteurs premiers

ii. Déterminer la valeur de $\varphi(323)$

iii. Déterminer (u,v) dans Z tels que 288u+227v=1

iv. Calculer a=2^{227} mod (323)

Si nécessaire appliquer l'algorithme d'exponentiation rapide

v. Vérifer que $a^v = 2 \bmod (323)$

Exercice 17. Simuler le cryptage et le décryptage d'un message numérique

n=323

e=49

i. Déterminer la clé d de décryptage

ii. Crypter le message « 11 »

iii. Décrypter le message et vérifier que vous retrouvez « 11 »