Eléments mathématiques pour la cryptographie à clé publique

PAR PATRICK TELLER

(prière de me communiquer les coquilles èventuelles)

0. Excursion rapide dans Z

$\mathbb{Z}=$ les entiers relatifs

DEUX OPERATIONS $+$ et $\times$

Proposition 1. ***L'ensemble des entiers $\mathbb{Z}$ est muni de deux lois de composition interne $+$ et *, dont on rappellera les propriétés***

i) $\forall (x,y)\in \mathbb{Z}^2, x+y\in \mathbb{Z}$

ii) $\forall (x,y,z)\in \mathbb{Z}^3, x+(y+z)=(x+y)+z$

iii) $\forall x\in \mathbb{Z}, x+0=0+x=x$

iv) $\forall x\in \mathbb{Z}, \exists x'\in \mathbb{Z}, x+x'=x'+x=0$ *(en fait ce x' c'est - x)*

j) $\forall (x,y)\in \mathbb{Z}^2, x\,y=\mathrm{yx}\in \mathbb{Z}$

jj) $\forall (x,y,z)\in \mathbb{Z}^3, x(\mathrm{yz})=(\mathrm{xy})z$

jjj) $x\in \mathbb{Z}, x1=1x=x$

k) $\forall (x,y,z)\in \mathbb{Z}^3, x(y+z)=\mathrm{xy}+\mathrm{xz}$

la partie i) fait de (Z,+) un groupe commutatif

{les parties i,j,k font de (Z,+,.) un anneau commutatif}

Définition 2. ***GROUPE COMMUTATIF***

Un groupe est un ensemble G, avec une loi « de composition » notée Δ,

cette loi est

i) interne : si a et b sont dans G aΔb aussi

ii) associative: si a,b, c sont dans G $a\Delta(b\Delta c)= (a\Delta b)\Delta c$ « on regroupe comme on veut »

iii) commutative: si a et b sont dans G $a\Delta b = b\Delta a$ « on déplace comme on veut »

iv) il y a dans G un élément neutre, noté e: pour tout a de G $a\Delta e = e\Delta a = a$

v) tout élément de G est symétrisable: pour tout a de G il y a un élément (noté a') tel que $a\Delta a' = a'\Delta a = e$.

Exemple 3.

1) Z avec l'addition

2) $\mathbb{R}^*$ avec la multiplication

3) U(= l'ensemble des complexes de module 1) pour la multiplication est un groupe commutatif

MAIS

Avertissement 4. Contre-exemples

1) $\mathcal{M}_2(\mathbb{R})$ avec la multiplication matricielle

l'élément neutre est noté I=$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ mais les matrices O=$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, A=$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ ne peuvent pas avoir d'inverse

Exercice 1.

a) L'ensemble considéré est $\mathbb{N}$ et la loi, notée $\odot$, est définie comme suit: pour tout (a,b) de $\mathbb{N}^2$, $a \odot b = a^b$, est-ce un groupe commutatif ?

b) L'ensemble considéré est $\mathbb{Z}$ et la loi, notée Δ, est définie comme suit: pour tout (a,b) de $\mathbb{Z}^2$

$a\Delta b = ab + a + b$; est-ce un groupe commutatif ?

Proposition 5. *La division euclidienne*

$$\forall(a,b) \in \mathbb{N} \times \mathbb{N}^*, \exists!(q,r) \in \mathbb{N} \times \{0,...,b-1\}, a = bq + r$$

Exercice 2.

166=23*7+5 ou 166=23*5+51 ?

q = ? r= ?

quel est LE QUOTIENT ? quel est LE RESTE ?

527=23q+ r

q= ? r = ?

Définition 6. *Divisibilité*

Soient deux entiers naturels a et b on dit que b divise a lorsqu'il existe un entier c tel que a=bc.

Exemple 7.

45 divise 9 ou 9 divise 45 ?

Définition 8. *Entier premier*

On dit qu'un entier naturel est premier lorsqu'il est strictement supérieur à 1 et qu'il n'est divisible que par 1 et par lui-même.

Exemple 9. 173 mais pas 171

Il y a une infinité de nombres premiers

SVP : une liste de 15 nombres premiers

BREAKING NEWS !!!!!!!!!

$\mathbf{2^{74207281} - 1}$ **est le plus grand nombre premier connu à cette date (janvier 16)**

http://www.mersenne.org/primes/?press=M57885161

Les nombres premiers sont aux entiers ce que les atomes sont aux molécules (p teller 23-01-2016)

Théorème 10. *Théorème fondamental de l'arithmétique*

Tout entier naturel strictement supérieur à 1 s'écrit de manière unique comme un produit de puissances d'entiers premiers.

Exemple 11. **882000=$2^4 3^2 5^3 7^2$**

Remarque 12.

1. Pour vérifier qu'un entier a est premier il est nécessaire de tester sa divisibilité par tous les premiers inférieurs ou égaux à $\sqrt{a}$.

2. Ceci est donc difficile et long (complexité).

3. Il en est de même de la recherche de la factorisation de a.

Ce sont ces deux particularités qui ont conduit à la méthode RSA de cryptographie à clé publique.

Exercice 3.

Factoriser 13860 en produit de puissances de nombres premiers

Proposition 13. ***De la factorisation d'un entier en produit de puissances de nombres premiers on déduit la liste complète de leurs diviseurs.***

Exemple 14.

38896=2^3*3*11*13^2

les diviseurs de 38896 sont tous les nombres dont la décomposition « entre » dans celle de 38896

c'est à dire tous les produits $2^a*3^b*11^c*13^d$ **où** $\begin{cases} 0\leqslant a\leqslant 3\\ 0\leqslant b\leqslant 1\\ 0\leqslant c\leqslant 1\\ 0\leqslant d\leqslant 2\end{cases}$

Il y en aura 4*2*2*3= 48

les valeurs possibles de (a,b,c,d) sont

a	*b*	*c*	*d*		*a*	*b*	*c*	*d*		*a*	*b*	*c*	*d*		*a*	*b*	*c*	*d*
0	0	0	0		1	0	0	0		2	0	0	0		3	0	0	0
0	0	0	1		1	0	0	1		2	0	0	1		3	0	0	1
0	0	0	2		1	0	0	2		2	0	0	2		3	0	0	2
0	0	1	0		1	0	1	0		2	0	1	0		3	0	1	0
0	0	1	1		1	0	1	1		2	0	1	1		3	0	1	1
0	0	1	2	et	1	0	1	2	et	2	0	1	2	et	3	0	1	2
0	1	0	0		1	1	0	0		2	1	0	0		3	1	0	0
0	1	0	1		1	1	0	1		2	1	0	1		3	1	0	1
0	1	0	2		1	1	0	2		2	1	0	2		3	1	0	2
0	1	1	0		1	1	1	0		2	1	1	0		3	1	1	0
0	1	1	1		1	1	1	1		2	1	1	1		3	1	1	1
0	1	1	2		1	1	1	2		2	1	1	2		3	1	1	2

donc les diviseurs sont

a	*b*	*c*	*d*	*x*		*a*	*b*	*c*	*d*	*x*		*a*	*b*	*c*	*d*	*x*		*a*	*b*	*c*	*d*	*x*
0	0	0	0	1		1	0	0	0	2		2	0	0	0	4		3	0	0	0	8
0	0	0	1	13		1	0	0	1	$2*13$		2	0	0	1			3	0	0	1	
0	0	0	2	169		1	0	0	2	$2*169$		2	0	0	2			3	0	0	2	
0	0	1	0	11		1	0	1	0			2	0	1	0			3	0	1	0	
0	0	1	1	$11*13$		1	0	1	1			2	0	1	1			3	0	1	1	
0	0	1	2	$11*169$	et	1	0	1	2		et	2	0	1	2		et	3	0	1	2	
0	1	0	0	3		1	1	0	0			2	1	0	0			3	1	0	0	
0	1	0	1	$3*13$		1	1	0	1			2	1	0	1			3	1	0	1	
0	1	0	2	$3*169$		1	1	0	2			2	1	0	2			3	1	0	2	
0	1	1	0	$3*11$		1	1	1	0			2	1	1	0			3	1	1	0	
0	1	1	1	$3*11*13$		1	1	1	1			2	1	1	1			3	1	1	1	
0	1	1	2	$3*11*169$		1	1	1	2			2	1	1	2			3	1	1	2	

Définition 15. *PGCD*

Parmi les diviseurs communs à deux entiers (a,b) il y en a un qui est le plus grand, on l'appelle pgcd (a,b) ou a∧b et

les diviseurs communs de a et de b sont les diviseurs de pgcd(a,b)=a∧b.

Exemple 16. 1256∧165=1; on dit qu'ils sont premiers entre eux

1353∧165=33

Définition 17. *Entiers premiers entre eux*

Soient deux entiers naturels a et b , on dit qu'ils sont premiers entre eux lorsque leur pgcd est égal à 1.

Remarque 18.

Attention les deux phrases suivantes n'ont pas le même sens

1) 25 et 7 sont premiers

2) 25 et 7 sont premiers entre eux

Attention à la paresse des mots !!!!

ATTENTION

la méthode du lycée pour trouver le pgcd: factoriser et chercher les facteurs communs, est inefficace

Théorème 19. *Recherche du pgcd : l'algorithme d'Euclide*

Divisions euclidiennes successives jusqu'au dernier reste non nul

Exemple 20. 645 et 18

645=18*35 +15

18=15*1+3

15=3*5+0

$645 \wedge 18 = 3$

Exercice 4.

322∧148= ?

Théorème 21. *Bezout*

Soient (a,b) deux entiers et d=pgcd(a,b), alors il existe deux entiers relatifs (u,v) tels que au+bv=d.

ATTENTION ce couple n'est pas unique, il y en a une infinité

Soient (u',v') tels que $au_0+bv_0=d$ alors l'ensemble des (u,v) tels que au+bv=d est l'ensemble $\left\{\left(u'+\frac{bt}{d}, v'-\frac{at}{d}\right), t\in\mathbb{Z}\right\}$.

ATTENTION

1) la réciproque du théorème de Bezout n'est vraie que lorsque d=1.

2) elle est juste mais inefficace

Comme nous allons avoir besoin de trouver effectivement des couples de Bezout voici l'algorithme d'Euclide étendu, seul capable de nous donner des couples de Bezout (l'idée de « remonter » la suite de divisions euclidiennes n'est pas réaliste dès qu'il y a une longue suite).

r	u	v
$r_0 = a$	$u_0 = 1$	$v_0 = 0$
$r_1 = b$	$u_1 = 0$	$v_1 = 1$
...	...	...
r_{k-1}	u_{k-1}	v_{k-1}
r_k	u_k	v_k
$r_{k+1} = r_{k-1} - (r_{k-1}\colon r_k)r_k$	$u_{k+1} = u_{k-1} - (r_{k-1}\colon r_k)u_k$	$v_{k+1} = v_{k-1} - (r_{k-1}\colon r_k)v_k$
...	...	...
$r_n = a \wedge b$	u	v
0	on s'en fiche	de $m$ême

On remarquera que la première colonne c'est en fait l'algorithme d'Euclide classique et qu'à chaque ligne r=au+bv.

Si on veut que u ou v soit dans un intervalle donné on utilise la connaissance de ce premier couple

(u',v′) et le théorème précédent.

Exemple 22.

Je reprends les notations du cours

a=30, b=7

	u	v	r	
ligne 0	1	0	30	à chaque ligne : $a \times u + b \times v = r$
ligne1	0	1	7	

puis on trouve le quotient de la ligne0 de r par la ligne1 de r

ici 30=4×7+ 2; donc q=4

j'ajoute une colonne pour les quotients

	u	v	r	q
ligne 0	1	0	30	
ligne1	0	1	7	
ligne2	$1 - 4 \times 0 = 1$	$0 - 4 \times 1 = -4$	$30 - 4 \times 7 = 2$	4

;

ligne2 vaut « ligne0 - q×ligne1 »

c'est à dire

	u	v	r	q
ligne 0	1	0	30	
ligne1	0	1	7	
ligne2	1	-4	2	4

.

On recommence

quotient de la ligne1 de r par la ligne2 de r

ici 7=3×2+ 1; donc q=3

	u	v	r	q
ligne 0	1	0	30	
ligne1	0	1	7	
ligne2	1	-4	2	4
ligne3				3

et on complète ligne3 vaut « ligne1 - q×ligne2 »

	u	v	r	q
ligne 0	1	0	30	
ligne1	0	1	7	
ligne2	1	-4	2	4
ligne3	$0-3\times 1=-3$	$1-3\times(-4)=13$	$7-3\times 2=1$	3

c'est à dire

	u	v	r	q
ligne 0	1	0	30	
ligne1	0	1	7	
ligne2	1	-4	2	4
ligne3	$0-3$	13	1	3

puis quotient la ligne2 de r par la ligne3 de r

ici 2=$2\times 1+0$; donc q=2 et le reste est nul

	u	v	r	q
ligne 0	1	0	30	
ligne1	0	1	7	
ligne2	1	-4	2	4
ligne3	-3	13	1	3
ligne4			0	2

on sait qu'alors le pgcd est le dernier reste non nul, c'est à dire « 1 » et la bonne ligne pour Bezout est la ligne 3

$-3\times 30+13\times 7=1$

Théorème 23. *Procédure Maxima*

Bezout(a,b):=block([r1,u1,v1,r2,u2,v2,r,u,v],r1:a,u1:1,v1:0,r2:b,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($[r1,u1,v1]$)) dollar

Exercice 5.

a. Déterminer deux entiers relatifs u e t v tels que 1143*u+631*v=1

b. Ce couple est-il unique ?

c. Existe-il une solution où u et v sont positifs ?

d. Déterminer une (la) solution où u est positif et minimal.

e. Déterminer deux entiers positifs (p,q) tels que 1143*p-631*q=1

f. Combien y a t il de solutions positives ?

1. Z/nZ

Définition 24. *Congruences*

Soit un entier n on dira que deux entiers a et b sont congrus modulo n lorsque n divise la différence a-b.

On écrira $a \equiv b[n]$ ***ou, s'il n'y a pas d'ambiguité,*** $\bar{a} = \bar{b}$***.***

On désigne par $\mathbb{Z}/n\mathbb{Z}$ **l'ensemble** $\{\bar{0}, \bar{1}, ..., \overline{n-1}\}$ **des classes modulo n et on définit pour cet ensemble une loi de composition interne , notée** $\oplus$**, de la manière suivante:** $\bar{a} \oplus \bar{b} = \overline{a+b}$ **.**

Exemple 25.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	etc
etc	...	...	...	...	...	...

on remarquera que cette loi est bien commutative, (l'associativité aussi, mais c'est un peu plus long à vérifier, $\bar{0}$ **est élément neutre et que chaque classe possède un symétrique:**

$\bar{0} \oplus \bar{0} = \bar{0}$; $\bar{1} \oplus \bar{5} = \bar{0}$; $\bar{2} \oplus \bar{4} = \bar{0}$; $\bar{3} \oplus \bar{3} = \bar{0}$

Théorème 26. *procédure maxima*

addit(a,b,modulo):=block([c],c:mod(a+b,modulo),return(c))dollar

Exercice 6. Ecrire la table de l'addition $\oplus$ **pour l'ensemble** $\mathbb{Z}/9\mathbb{Z}$

2.1 (Z/nZ,⊕)

Théorème 27. *le groupe (Z/nZ,⊕)*

i) $\forall(\bar{x}, \bar{y}) \in \mathbb{Z}/n\mathbb{Z}^2, \bar{x} \oplus \bar{y} \in \mathbb{Z}/n\mathbb{Z}$

ii) $\forall(\bar{x}, \bar{y}, \bar{z}) \in \mathbb{Z}/n\mathbb{Z}^3, \bar{x} \oplus (\bar{y} \oplus \bar{z}) = (\bar{x} \oplus \bar{y}) \oplus \bar{z}$

iii) $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}, \bar{x} \oplus \bar{0} = \bar{0} \oplus \bar{x} = \bar{x}$

iv) $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}, \exists \bar{x'} \in \mathbb{Z}/n\mathbb{Z}, \bar{x} \oplus \bar{x'} = \bar{x'} \oplus \bar{x} = \bar{0}$

(Comme on vient de le voir pour le cas particulier de $\mathbb{Z}/6\mathbb{Z}$***) l'ensemble Z/nZ, muni de l'addition*** $\oplus$***, est un groupe commutatif.***

le neutre est $\bar{0}$***, le symétrique de*** $\bar{a}$ ***est*** $\overline{n-a}$ ***.***

Définition 28. *Ordre d'un élément dans un groupe*

Soit un groupe (G,) d'élément neutre e et a∈G, on appelle ordre de a* ***le plus petit entier strictement positif k*** *(s'il existe) tel que a*a*...*a (k fois) =e*

Exemple 29. **Dans (Z/12Z,⊕)**

ATTENTION: ICI la loi est ⊕ donc on cherche le plus petit entier strictement positif k (s'il existe) tel que a⊕a⊕...⊕a (k fois) =$\bar{0}$.

l'ordre de $\bar{1}$ c'est 12

l'ordre de $\bar{2}$ c'est 6

l'ordre de $\bar{3}$ c'est 4

l'ordre de $\bar{5}$ c'est 12

Théorème 30. *procédure maxima*

ordre(a,modulo):=block([aa,k],aa:a,k:1,while(aa>0)do(aa:addit(aa,a,modulo)k:k+1),return(k))dollar

Théorème 31. *Théorème d'Euler*

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

Problème 1. **à résoudre à la main ou avec une calculatrice**

1. Déterminer le pgcd de 1741 et 1995

2. Déterminer la factorisation en produit de puisssances de nombres premiers de 7892

Problème 2. **(avec Maxima) à préparer pour le TD**

Les calculs se feront dans (Z/nZ,⊕) où n=10!+1

1. Déterminer si n est premier

2. Calculer $\overline{55!}\oplus\overline{99!}$

3. En vous aidant du théorème 31 déterminer le maximum des ordres des éléments de ce groupe; déterminer les éléments d'ordre maximal dans ce groupe

4. Déterminer les éléments non nuls d'ordre minimal

Expliquer

Exercice 7.

1. Déterminer le pgcd de 7007 et de 2057

2. Déterminer deux entiers u et v tels que 7007u+2057v=7007∧2057

3. Déterminer le plus petit entier positif v tel que 7007u+2057v=7007∧2057

Exercice 8.

1.2.3.Mêmes questions avec 8784 et 1404

4. Déterminer deux entiers u et v tels que 8784u++1404v=36

5. Déterminer deux entiers u et v tels que 8784u+1404v=180

Conclusion sur ces deux questions ?

Exercice 9.

Calcul dans (Z/512Z,⊕)

1. Calculer $\overline{239}\oplus\overline{425}$

2. Déterminer l'ordre de $\overline{64}$

3. Déterminer l'ordre de $\overline{511}$

4. Déterminer un élément d'ordre 2; un élément d'ordre 4, un élément d'ordre 512, un autre , encore un autre.

5. On considère l'élément $\bar{3}$ déterminer son ordre; soit l'élément $\overline{505}$ trouver, à l'aide de la procédure de Bezout, un entier naturel b tel que $\overline{505}$=b$\bar{3}$.

6. Montrer que pour tout élément $\bar{x}$ de (Z/512Z,$\oplus$) il existe un entier naturel b tel que $\bar{x}$=b$\bar{3}$

7. Déterminer l'ordre de $\overline{66}$?

8. Est ce que pour tout élément $\bar{x}$ de (Z/512Z,$\oplus$) il existe un entier naturel b tel que $\bar{x}$=b$\overline{66}$?

Exercice 10. En vous aidant des factorisations en produit de puissances de premiers des nombres 8784 et 1404

déterminer tous leurs multiples communs.