Cryptographie : outils mathématiques

A. Bonnecaze

Institut de Mathématiques de Marseille (I2M)

Polytech Marseille, INFO3

Organisation

1. 9 cours/TD + 9 TD/TP
2. Evaluation : Examens écrits et participation
3. Supports d'enseignement disponibles sur http://alexis.bonnecaze.perso.luminy.univ-amu.fr/Crypto3/Crypto3.html

Plan

Cryptographie

Des services informatiques sûrs

Confidentialité, Intégrité, Disponibilité
Authentification, Non Répudiation, Responsabilité

Les mécanismes cryptographiques contribuent à sécuriser les services informatiques. Il en existe beaucoup : chiffrement, signature, échange de clés, partage de secret, ...

Exemples d'applications :

Connexion au site d'une banque
Paiement sur Internet
Accès à une base de données
monnaie numérique
Surfer anonymement sur Internet
Empêcher la prise de ctrle à distance (avion, voiture, smartphone,...)

Outils théoriques

- Théorie de l'information (INFO4), probabilité (INFO3)
- Algèbre (INFO3)
- Arithmétique (ce cours)
- Théorie de la complexité (INFO3)
- Théorie des corps finis (ce cours)
- Algorithmique (INFO3)

Autres connaissances

Réseau, cloud, système d'exploitation, programmation, codage

Remarque

Il existe des mécanismes non cryptographiques : firewall, coffre fort, mécanismes de ctrle d'accès, ...

Objectif du cours

- Connaitre des outils mathématiques utilisés en crypto
- En particulier ceux basés sur l'arithmétique
- Étudier quelques primitives simples
- Savoir programmer une primitive crypto utilisant de grands nombres

Et donc être capable de suivre le cours de sécurité de INFO4.

Les algos cryptographiques s'insèrent dans des protocoles qui ont un ou plusieurs objectifs de sécurité

Exemples de protocoles : TLS, HTTPS, SSH, ...

Les bits, les octets, les entiers

- Les bits : On note $\mathbb{F}_2 = \{0, 1\}$. Chaque élément est appelé un bit.
  Les opérations classiques sont XOR (addition modulo 2), OR (borne sup) et AND (borne inf)
  Un mot est appelé en anglais un bit string
- Les octets : Un octet est une suite de 8 bits.
  On note $\mathbb{F}_{256}$ l'alphabet constitué des 256 octets.
  Les opérations : XOR (bit à bit), autres opérations plus complexes.
  Un mot est appelé en anglais un octet string
- Les entiers Les entiers utilisés en crypto sont en général des grands nombres. Ils sont traités grâce à des bibliothèques spécifiques (exemples : BigInteger en java, GMP en C)

Traductions

La plupart des primitives de chiffrement s'appliquent à des nombres entiers (chiffrements arithmétiques) ou à des blocs de bits (opérations booléennes).

Les données qu'on chiffre sont des fichiers qui en général ont des structures liées à des représentations sous forme d'octets (textes par exemple).

Il faut des procédures standards de traduction permettant de passer d'une représentation à une autre :

Fonctions ISO/IEC 18033-2

OS2BSP(u)	Octet String to Bit String Procedure
BS2OSP(b)	Bit String to Octet String Procedure
BS2IP(b)	Bit String to Integer Procedure
I2BSP(x,l)	Integer to Bit String Procedure
OS2IP(u)	Octet String to Integer Procedure
I2OSP(x,l)	Integer to Octet String Procedure

Encodage Base64

Transformer une suite d'octets en une suite de caractères imprimables en ASCII non étendu : On transforme 3 octets (24 bits) en 4 tranches de 6 bits

Valeur	Codage	Valeur	Codage	Valeur	Codage	Valeur	Codage
0 000000	A	17 010001	R	34 100010	i	51 110011	z
1 000001	B	18 010010	S	35 100011	j	52 110100	0
2 000010	C	19 010011	T	36 100100	k	53 110101	1
3 000011	D	20 010100	U	37 100101	l	54 110110	2
4 000100	E	21 010101	V	38 100110	m	55 110111	3
5 000101	F	22 010110	W	39 100111	n	56 111000	4
6 000110	G	23 010111	X	40 101000	o	57 111001	5
7 000111	H	24 011000	Y	41 101001	p	58 111010	6
8 001000	I	25 011001	Z	42 101010	q	59 111011	7
9 001001	J	26 011010	a	43 101011	r	60 111100	8
10 001010	K	27 011011	b	44 101100	s	61 111101	9
11 001011	L	28 011100	c	45 101101	t	62 111110	+
12 001100	M	29 011101	d	46 101110	u	63 111111	/
13 001101	N	30 011110	e	47 101111	v		
14 001110	O	31 011111	f	48 110000	w		
15 001111	P	32 100000	g	49 110001	x		
16 010000	Q	33 100001	h	50 110010	y		

Aritmétique

La cryptographie (asymétrique) utilise certaines propriétés des entiers modulaires :

- petit théorème de Fermat
- théorème d'Euler
- théorème des restes chinois
- ...

et s'appuie sur des problèmes

- calcul du logarithme discret
- factoriser un grand nombre
- ...

Les prochains slides sont une introduction à l'arithmétique

Division entière

Soit a et b entiers. On dit que a divise b, ou $a|b$ si $\exists d$ tq $b = ad$.

Théorème

On suppose que b est non nul. Alors, il existe un couple unique (q, r) de nombres entiers tels que :

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

La valeur $r \equiv a \mod b$ est appelée le reste de la division.

Théorème

Si $m|a$ et $m|b$, alors $m|(\alpha a + \beta b)$ pour tout entier α, β

Preuve : $a = rm$; $b = sm$. Ainsi, $\alpha a + \beta b = \alpha rm + \beta sm = m(\alpha r + \beta s)$

Division entière (suite)

Théorème

$a|a, \quad 1|a, \quad a|0$
$0|a \iff a = 0$

Théorème

Pour tout $a, b \in \mathbb{Z}, \quad a|b$ *et* $b|a \iff a = \pm b$

Preuve ?

Définition

c est un diviseur commun de a et b si $c|a$ et $c|b$

Exercice : diviseur commun de 66 et 759?

Tests de divisibilité

1. Un nombre est divisible par 2^k si ses k derniers chiffres sont divisibles par 2^k.
   31024 est divisible par 2^4
2. Un nombre est divisible par 5^k si ses k derniers chiffres sont divisibles par 5^k.
   2125 est divisible par 5^k, pour quel k?
3. Un nombre est divisible par (resp) 3 ou 9 si la somme de ses chiffres est divisible par (resp) 3 ou par 9.
   444 est-il divisible par 3? par 9?
   1638 est-il divisible par 9?

Algorithmes de division

L'algorithme le plus simple consiste à soustraire autant de fois b de a qu'il est possible, jusqu'à obtenir un reste $< b$.

```
division:=proc(a,b)
local r, q, u;

r := a;
q := 0;
while (r >= b)
  do
    r := r − b;
    q := q + 1;
 od;
u := [q, r];
return(u);
end;
```

Algorithmes

Dans la pratique a est souvent très grand devant b

Par exemple
a de 1024 bits (donc de l'ordre de 2^{1024})
b de 128 bits.
Quel est le nombre de soustractions à faire?

L'algorithme de Division binaire est plus efficace. Il est basé sur l'écriture binaire des nombres.

Division binaire

```
local r,q,aux,n,u;
  r := a; q := 0; n := 0; aux := b;
  while (aux <= a)
     aux := 2 * aux;
     n := n + 1;
  while (n > 0)
     aux := aux/2;
     n := n - 1;
     if (r < aux)
       then
         q := 2 * q;
       else
         q := 2 * q + 1;
         r := r - aux;
  u := [q, r];
  return(u);
end;
```

Comparaison des deux algorithmes

- Le premier algorithme (Euclide pour la division) est inutilisable car le nombre de tours de boucles contenant des opérations simples est $O(a)$
- Le deuxième algorithme aboutit même pour de grands nombres, son nombre de tours de boucles contenant des opérations simples est $O(\ln(a))$.

PGCD

Soit a, b des entiers dont au moins un est non nul

- $$pgcd(a,b) = max(d : d|a \text{ et } d|b)$$
- $$ppcm(a,b) = min(d > 0 : a|d \text{ et } b|d)$$
- a et b sont premiers entre eux si $pgcd(a,b) = 1$

Algorithme d'Euclide

Calcul du PGCD

$R0 := |a|$;
$R1 := |b|$; $(b \neq 0)$
Tantque $R1 > 0$ Faire
$R := Reste\_Division(R0, R1)$;
$R0 := R1$;
$R1 := R$;

En sortie $R1 = 0$, et $R0 = pgcd(a, b)$.
Les conditions :

$$\begin{cases} \text{L'ensemble des diviseurs communs de } R0 \text{ et } R1 \text{ est} \\ \quad \text{l'ensemble des diviseurs communs de } a \text{ et } b. \\ \\ R_1 \geq 0 \end{cases}$$

constituent un invariant de boucle.

Algorithme d'Euclide

Calcul du PGCD

$R0 := |a|$;
$R1 := |b|$; $(b \neq 0)$
Tantque $R1 > 0$ Faire
$R := Reste\_Division(R0, R1)$;
$R0 := R1$;
$R1 := R$;

En sortie $R1 = 0$, et $R0 = pgcd(a, b)$.
L'algorithme se termine car $R1$ décroît strictement à chaque tour de boucle. A la fin $R1 = 0$, donc l'ensemble des diviseurs de $R0$ et de $R1$ est l'ensemble des diviseurs de $R0$, et par conséquent $R0 = \text{pgcd}(a, b)$.

Exemple : $pgcd(53, 39)$

$$
\begin{array}{lrcl}
pgcd & (R_0 & , & R_1) \\
pgcd & (53 & , & 39) \\
pgcd & (39 & , & 14) \\
pgcd & (14 & , & 11) \\
pgcd & (11 & , & 3) \\
pgcd & (3 & , & 2) \\
pgcd & (2 & , & 1) \\
pgcd & (1 & , & 0)
\end{array}
$$

$$pgcd(53, 39) = 1$$

Propriétés

Théorème

Soit a, b deux entiers non tous nuls et d le plus petit entier positif de $S = \{ax + by : x, y \in \mathbb{Z}\}$. Alors $pgcd(a, b) = d$

preuve : $|a| \in S$ donc S contient un entier positif.
Par définition, il existe x, y tq $d = ax + by$. $d \leq |a|$, donc il existe q, r tq

$$a = qd + r, \quad 0 \leq r < d$$

donc,

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy) \in S.$$

$r < d$ implique que $r = 0$, et ainsi $d|a$. De même, on a $d|b$.
donc $d \leq pgcd(a, b)$.
D'autre part $pgcd(a, b)|a$ et $pgcd(a, b)|b$, et ainsi $pgcd(a, b)$ divise toute combinaison linéaire de a, b, donc tout élément de S , donc d, et ainsi $pgcd(a, b) \leq d$. Donc $d = pgcd(a, b)$.

Propriétés (suite)

Corollaire: Bézout

a et b sont premiers entre eux $\iff \exists x,\ y \in \mathbb{Z}$ tel que $xa + yb = 1$.

Preuve :

($\Leftarrow$) Soit $d = pgcd(a, b)$, et $xa + yb = 1$. $d|a$ et $d|b$ et ainsi, $d|1$, donc $d = 1$.

($\Rightarrow$) $pgcd(a, b) = 1$. d'après le théo précédent, 1 est le plus petit entier positif dans $S = \{ax + by : x, y \in \mathbb{Z}\}$, cad. $\exists x, y$ tel que $ax + by = 1$.

Propriétés (suite)

Théorème fondamental de l'arithmétique

Si $c|ab$ et $pgcd(b, c) = 1$ alors $c|a$.

Preuve : On sait que $c|ab$. On a, $c|ac$.
Donc,
$c|pgcd(ab, ac) = a.pgcd(b, c) = a.1 = a$.

Entiers et nombres premiers

Définition

Un entier $p \geq 2$ est appelé un nombre premier s'il est divisible seulement par 1 et lui-même.

Théorème d'unique factorisation

Tout entier positif peut être représenté comme un produit de nombres premiers d'une manière unique (à permutation des nombres premiers près)

Preuve du théorème

Tout entier peut être représenté comme un produit de premiers car si un élément n'est pas premier, il peut être factorisé en nombres premiers plus petits.
Unicité : Supposons qu'un entier puisse être représenté de deux manières.

$$p_1 p_2 p_3 \dots p_s = q_1 q_2 q_3 \dots q_r$$

où tous les facteurs sont premiers, et $p_i \neq q_j$
Alors

$$p_1 | q_1 q_2 q_3 \dots q_r$$

Mais $pgcd(p_1, q_1) = 1$ et donc

$$p_1 | q_2 q_3 \dots q_r$$

en continuant, on obtient $p_1 | q_r$. Contradiction.

Conséquence de la factorisation unique

Il existe une infinité de nombres premiers

Supposons qu'il existe un nombre fini de nombres premiers :

$$p_1, \ldots, p_n$$

Le nombre

$$q = p_1 \ldots p_n + 1$$

n'est divisible par aucun des p_i, le reste étant toujours égal à 1. N'étant pas dans la liste, q n'est pas premier, et il est donc divisible par un nombre premier, ce qui est absurde.

Idéaux de $\mathbb{Z}$

Définition

Un **idéal** de $\mathbb{Z}$ est un ensemble non vide d'entiers qui est clos par addition et par multiplication par un entier arbitraire

Définition

Un ensemble $I \subseteq \mathbb{Z}$ non vide est un idéal si et seulement si pour tout $a, b \in I$ et pour tout $z \in \mathbb{Z}$, $a + b \in I$ et $az \in I$.

Remarques :

1. Si $a \in I$ alors $-a \in I$
2. $0 \in I$ car $a + (-a) \in I$
3. Si $1 \in I$ alors $I = \mathbb{Z}$.

Idéaux (suite)

Définition

$a\mathbb{Z} := \{az : z \in \mathbb{Z}\}$ est l'ensemble des multiples de a. $a\mathbb{Z}$ est un idéal généré par a. Tous les idéaux de la forme $a\mathbb{Z}$ sont appelés **idéaux principaux**

Exemple : $a = 3,\ \ aZ = \{\ldots, -9, -6, -3, 0, 3, 6, \ldots\}$

Théorème

Pour tout idéal $I \subset \mathbb{Z}$, il existe un unique entier positif d tel que $I = d\mathbb{Z}$

- $a_1 = 3, a_2 = 5,\ \ a_1\mathbb{Z} + a_2\mathbb{Z} = ?$
- $a_1 = 4, a_2 = 6,\ \ a_1\mathbb{Z} + a_2\mathbb{Z} = ?$

Théorème

Pour tout $a, b \in \mathbb{Z}$, il existe un unique PGCD d de a et b et de plus $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Exercices

1. Faire tourner l'algorithme de division binaire pour calculer $123/23$, puis $256/2$.
2. Calculer $PGCD(79, 23)$ avec l'algorithme d'Euclide
3. Calculer $3\mathbb{Z} + 5\mathbb{Z}$, $6\mathbb{Z} + 9\mathbb{Z}$
4. Que vaut $a\mathbb{Z} + b\mathbb{Z}$ si a et b sont premiers entre eux?
5. Soit $a, b, c \in \mathbb{Z}$ tel que $c|ab$ et $PGCD(a, c) = 1$, montrer que $c|b$.
6. Si $PGCD(a_1, \ldots, a_k) = 1$, les entiers a_i sont-ils premiers deux à deux?
7. Soit p un premier, $a, b \in \mathbb{Z}$. Montrer que $p|ab$ implique que $p|a$ ou $p|b$.
8. Soit $a_1, \ldots, a_k$ des entiers et p un premier. Montrer que si $p| \prod a_i$, alors $p|a_i$ pour un $i \in 1, \ldots, k$.

TP

1. Programmer l'algorithme de division simple et l'algorithme de division binaire.
2. Réécrire les deux algorithmes en utilisant la librairie GMP. Comparer les deux algorithmes en les testant avec des nombre grands.
3. Programmer l'algorithme d'Euclide pour le calcul du PGCD de deux nombres
4. Programmer une fonction qui retourne le PGCD de n nombres

Modulo

Si $n|(a-b)$ alors

$$(a \mod n) = (b \mod n)$$

On écrit

$$a \equiv b \mod n$$

et on dit que *a* est congru à *b* modulo *n*
Les entiers peuvent être divisés en *n* classes d'équivalences en fonction de leur résidu modulo *n*

$$[a]_n = \{a + kn,\ k \in \mathbb{Z}\}$$

$$\mathbb{Z}_n = \{[a]_n\ : 0 \leq a \leq n-1\}$$

ou simplement

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

Propriétés de la congruence

$\forall\, a, a_1, b, b_1, c \in \mathbb{Z}$:

- $a \equiv b \pmod{n} \iff a$ et b ont le même reste dans la division par n.
- $a \equiv a \pmod{n}$ (réflexivité).
- $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ (symétrie).
- $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (transitivité).
- $a \equiv a_1 \pmod{n}$ et $b \equiv b_1 \pmod{n} \Rightarrow \begin{cases} a + b \equiv a_1 + b_1 \pmod{n}, \\ ab \equiv a_1 b_1 \pmod{n}. \end{cases}$

Exemple : Résoudre $3x + 4 \equiv 6 \mod 7$.
On peut écrire $3x \equiv 2 \mod 7$ puis multiplier l'équation par 5 pour obtenir $x \equiv 3 \mod 7$.

Remarque : $a \equiv b \mod n$ si et seulement si il existe c tel que $a = b + cn$.

Inverses

Définition : Soit a un entier. Il est inversible si il existe b tel que

$$ab \equiv 1 \mod n$$

Dans ce cas b est l'inverse de a modulo n. On écrit $b \equiv a^{-1} \mod n$.

Théorème

Si $pgcd(a, n) = 1$, il existe b tel que $ab \equiv 1 \mod n$

Preuve D'après Bézout, il existe $x, y \in \mathbb{Z}$ tel que $xa + yn = 1$.
Donc, $xa \equiv 1 \mod n$.

Conclusion : a admet un inverse modulo n SSi $pgcd(a, n) = 1$.
L'inverse peut être calculé avec l'algo d'Euclide étendu

Algorithme d'Euclide Etendu

Calculer l'inverse de 39 modulo 53

$$\begin{aligned}
53 &= 1.39 + 14 &\Rightarrow\quad & 14 = 53 - 39\\
39 &= 2.14 + 11 &\Rightarrow\quad & 11 = 39 - 2.14 = -2.53 + 3.39\\
14 &= 1.11 + 3 &\Rightarrow\quad & 3 = 14 - 1.11 = 3.53 - 4.39\\
11 &= 3.3 + 2 &\Rightarrow\quad & 2 = 11 - 3.3 = -11.53 + 15.39\\
3 &= 1.2 + 1 &\Rightarrow\quad & 1 = 3 - 1.2 = 14.53 - 19.39\\
2 &= 2.1 + 0
\end{aligned}$$

On obtient $14.53 - 19.39 = 1$

Remarque :

On obtient que :

$$39.(-19) \equiv 1 \mod 53$$

donc $39.34 \equiv 1 \mod 53$

Exercices

- Calculer l'inverse de 2 modulo 7
- Calculer $17^{-1} \mod 21$
- Calculer $17^{-1} \mod 34$
- Calculer $25/4 \mod 17$
- Calculer $37/3 \mod 31$
- Calculer $37/3 \mod 30$

Résoudre les congruences linéaires

Théorème

Soit $a, n, z, z' \in \mathbb{Z}$, $n > 0$. Si $PGCD(a, n) = 1$ alors

$$az \equiv az' \mod n \Leftrightarrow z \equiv z' \mod n$$

et si $PGCD(a, n) = d$ alors

$$az \equiv az' \mod n \Leftrightarrow z \equiv z' \mod n/d$$

Preuve ?

Exemples :

a) $5.2 \equiv 5.(-4) \mod 6$.
On peut simplifier par 5 des deux cotés car $PGCD(5, 6) = 1$. On obtient $2 \equiv -4 \mod 6$.
b) $3.5 \equiv 3.3 \mod 6$.
On ne peut pas simplifier par 3 car $PGCD(3, 6) \neq 1$, mais on peut écrire $5 \equiv 3 \mod 2$.

Congruences linéaires

Théorème

Soit $a, b, n \in \mathbb{Z}$, $n > 0$ et $PGCD(a, n) = d$.
Si $d|b$, alors
$az \equiv b \mod n$ admet une solution z et tout z' est aussi solution
si et seulement si $z \equiv z' \mod n/d$.
Si $d \nmid b$, la congruence n'admet pas de solution.

Exercices : Résoudre les équations suivantes
$2z \equiv 3 \mod 15$,
$3z \equiv 4 \mod 15$,
$3z \equiv 12 \mod 15$.
$4x \equiv 6 \mod 10$,
$15x \equiv 2 \mod 18$

Résolution de systèmes

Si le modulo est premier, pas de problème, on est dans un corps

Exemple

$$\begin{cases} 5x + 6y & \equiv & 8 & \mod 13 \\ 7x + 3y & \equiv & 5 & \mod 13 \end{cases}$$

On trouve

$$\begin{cases} x \equiv & 6 & \mod 13 \\ y \equiv & 5 & \mod 13 \end{cases}$$

Dans cet exemple, on travaille dans le corps $\mathbb{F}_{13}$

Restes Chinois

Comment travailler avec plusieurs modules?

Théorème

Si m et n sont premiers entre eux alors la condition :

$$\begin{cases} a \equiv b & (m) \\ a \equiv b & (n) \end{cases}$$

est équivalente à :

$$a \equiv b \quad (mn).$$

Preuve Si $a \equiv b \quad (mn)$ les deux relations $a \equiv b \quad (m)$ et $a \equiv b \quad (n)$ ont bien lieu.
Réciproquement si ces deux relations ont lieu alors il existe k_1 et k_2 tels que :

$$a - b = k_1 m = k_2 n.$$

On voit alors que m divise $k_2 n$ et comme il est premier avec n il divise k_2. Si bien que :

$$a - b = k_3 mn.$$

Restes Chinois : un exemple numérique

Résoudre

$$\begin{cases} x \equiv 2 & \mod 3 \\ x \equiv 3 & \mod 5 \end{cases}$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$x \mod 3$	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
$x \mod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

Le couple $(2, 3)$ correspond à $z = 8$

Comment résoudre le problème sans calculer le tableau?

- voir la suite du cours
- (pour les paresseux) On peut utiliser le logiciel magma : $CRT([2, 3], [3, 5])$;

Restes Chinois

Soient m et n premiers entre eux. On cherche toutes les solutions entières de :

$$\begin{cases} x \equiv a & (m) \\ x \equiv b & (n) \end{cases}$$

On considère u et v tels que $um + vn = 1$.

Théorème des restes chinois

On obtient une solution en prenant :

$$x = bum + avn.$$

Toutes les solutions sont alors de la forme :

$$x + kmn.$$

Preuve du théorème

Par un calcul direct on vérifie que $x = bum + avn$ est bien une solution. On vérifie alors que pour tout entier k, $x + kmn$ est aussi une solution.
Si maintenant x et y sont deux solutions, par différence on obtient :

$$\begin{cases} x \equiv y & (m) \\ x \equiv y & (n) \end{cases},$$

ce qui nous permet de conclure :

$$y = x + kmn$$

grâce au théorème précédent
Remarque Il y a donc une solution unique y vérifiant $0 \leq y < mn$; ce qui peut s'exprimer encore en disant qu'il y a une unique solution dans $\mathbb{Z}/mn\mathbb{Z}$.

Généralisation

Théorème

Si les entiers $n_1, n_2, \ldots, n_k$ sont deux à deux premiers entre eux, alors le système :

$$\begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \\ \quad \vdots \\ x \equiv a_k \mod n_k \end{cases}$$

a une solution unique modulo $n = n_1 n_2 \ldots n_k$.

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i \mod n,$$

avec $N_i = n/n_i$ et $M_i = N_i^{-1} \mod n_i$

Exercices

1. Calculer x tel que $\begin{cases} x = 12 \mod 21 \\ x = 4 \mod 5 \\ x = 6 \mod 22 \end{cases}$
2. Calculer x tel que $\begin{cases} x = 12 \mod 19 \\ x = 6 \mod 23 \end{cases}$

TP

1. Programmer une fonction qui calcule l'inverse d'un entier modulo un autre entier (si l'inverse existe)
2. Programmer une fonction CRT qui prend en input $n_1, n_2, \ldots, n_k$ et $a_1, a_2, \ldots, a_k$ et retourne la solution du système

$$\begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \\ \quad \vdots \\ x \equiv a_k \mod n_k \end{cases}$$

Groupes

Un groupe $(G, \oplus)$ est un ensemble G muni d'une opération binaire $\oplus$ tq

- Cloture : $a \oplus b \in G$ pour tout $a, b \in G$
- Identité : il existe un élément $e \in G$ tq $e \oplus a = a \oplus e = a$ pour tout $a \in G$
- Associativité : $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ pour tout $a, b, c \in G$
- Inverses : pour tout élément $a \in G$ il existe un unique élément $b \in G$ vérifiant $a \oplus b = b \oplus a = e$

Un groupe commutatif est appelé abélien

Définition

L'ordre du groupe, $|G|$, est le nombre d'éléments dans G.

Lemme : $(\mathbb{Z}_n, +_n)$ est un groupe fini abélien additif modulo n.

Propriétés

Soit $a^k = \underbrace{a \oplus a \oplus \cdots \oplus a}_{k}$ (notation multiplicative)

- $a^0 = e$
- e est unique
- tout élément $a \in G$ admet un et un seul inverse noté a^{-1}
- $a^{-k} = \oplus_{i=1}^{k} a^{-1}$
- $a^m \oplus a^n = a^{m+n}$
- $(a^m)^n = a^{mn}$

Ordre

L'ordre d'un élément a d'un groupe G est le plus petit $t > 0$ tel que $a^t = e$.
Notation $Ord(a, G)$ ou $Ord(a)$

Exemples

- L'ordre de 2 dans $(\mathbb{Z}_3 \setminus \{0\}, .3)$ est 2
- Quel est l'ordre de 2 dans $(\mathbb{Z}_3, +3)$?
- Quels sont les ordres des éléments de $(\mathbb{Z}_7 \setminus \{0\}, .7)$?

Sous-groupes

Si $(G, \oplus)$ est un groupe, $G' \subseteq G$, et $(G', \oplus)$ est aussi un groupe, alors $(G', \oplus)$ est appelé un sous-groupe de G.

Théorème

Si $(G, \oplus)$ est un groupe fini et G' un sous ensemble de G tel que $a \oplus b \in G'$ pour tout $a, b \in G'$, alors $(G', \oplus)$ est un sous-groupe de $(G, \oplus)$

Exemples

- $(\{0, 2, 4, 6\}, +_8)$ est un sous-groupe de $(Z_8, +_8)$
- $(\mathbb{Z}_3, +_3)$ est-il un sous-groupe de $(\mathbb{Z}_6, +_6)$?
- $(\{0, 2, 4\}, .6)$ est-il un sous-groupe de $(\mathbb{Z}_6, .6)$?

Lagrange

Si $(G, \oplus)$ est un groupe fini et $(G', \oplus)$ est un sous-groupe de $(G, \oplus)$, alors $|G'|$ divise l'ordre de $|G|$

Générateurs

Soit $g \in G$, on note $\langle g \rangle = \{g^k, 1 \leq k \leq Ord(g)\}$

Théorème

$\langle g \rangle$ admet $Ord(g)$ éléments distincts

Preuve (par contradiction) suppose qu'il existe $1 \leq i < j \leq Ord(g)$, tel que $g^i = g^j$. Ainsi, $e = g^{j-i}$ or $Ord(g) > j - i > 0$.

Lemme

$\langle g \rangle$ est un sous-groupe de G

$\langle g \rangle$ est appelé un **groupe cyclique**, il est engendré par g.
g est appelé un générateur de $\langle g \rangle$.

Exemples

- $\{0, 2, 4, 6\} \subset \mathbb{Z}_8$ peut être généré par 2 ou 6
- 3 est-il un générateur de $\mathbb{Z}_4$?

Propriétés des sous-groupes

- L'ordre d'un élément divise l'ordre du groupe
- Tout groupe d'ordre premier est cyclique
- Soit G un groupe fini et $a \in G$, alors $a^{|G|} = e$

Théorème

Soit $a \in G$ tel que $a^s = e$, alors $Ord(a)|s$

Preuve On a $s = q.Ord(a) + r$, où $0 \leq r < Ord(a)$.
Ainsi,

$$e = a^s = a^{q.Ord(a)+r} = (a^{Ord(a)})^q \oplus a^r = a^r.$$

Puisque $Ord(a)$ est minimal, on a $r = 0$.

Le groupe multiplicatif $\mathbb{Z}_n^*$

Définition

L'ensemble des entiers inversibles modulo n est noté $\mathbb{Z}_n^*$

$$\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n \quad : \quad pgcd(i, n) = 1\}$$

Exemples

- Si p premier, $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$
- Quel est l'ordre de $\mathbb{Z}_p^*$?
- Quels sont les éléments de $\mathbb{Z}_{15}^*$?
- Peut-on comparer $|\mathbb{Z}_{15}^*|$ avec $|\mathbb{Z}_3^*|$ et $|\mathbb{Z}_5^*|$?
- Existe-t-il un entier n tq $\mathbb{Z}_n^* = \mathbb{Z}_n$?

Exercices

1. Déterminer Z_{15}^* ainsi que l'ordre de chacun de ses éléments. Z_{15}^* admet-il un générateur?
2. Déterminer Z_{18}^* ainsi que tous ses générateurs. Combien admet-il de générateur? Calculer l'ordre de 7. Quels sont les ordres possibles des éléments de Z_{18}^*?
3. Montrer que Z_{11}^* est un groupe cyclique.
4. $(Z_{15}^*, ., 1)$ est-il un groupe cyclique? pourquoi?
5. $(Z_{18}^*, ., 1)$ est-il un groupe cyclique? pourquoi?
6. $(Z_3 \times Z_3, +, (0,0))$ est-il cyclique?
7. $(Z_3, +, 0)$ est-il un sous groupe de $(Z_9, +, 0)$?
8. $(3Z_{15}, +, 0)$ est-il un sous groupe de $(Z_{15}, +, 0)$?
9. $(2Z_{15}, +, 0)$ est-il un sous groupe de $(Z_{15}, +, 0)$?

Cosets et quotients

Soit G un groupe et H un sous-groupe de G. $a, b \in G$
On écrit $a \equiv b \mod H$ si $a - b \in H$. C'est à dire :

$$a \equiv b \mod H \iff a = b + h, \text{ pour un } h \in H$$

"$\equiv$" est une relation d'équivalence qui partitionne G.
La classe contenant a est

$$a + H = \{a + h : h \in H\}$$

C'est le coset de H dans G contenant a.
En représentation multiplicative, on a

$$a \equiv b \mod H \text{ si } a/b \in H$$

$$aH = \{ah : h \in H\}$$

Cosets et quotients

Exercices :

1. $G = Z_4$ et $H = 2G$. Quel est le coset contenant 1?
2. Soit $a, a', b, b' \in G$. Si $a \equiv b \mod H$ et $a' \equiv b' \mod H$, montrer que $a + a' \equiv b + b' \mod H$

Définition

Soit $a, b \in G$.

$$(a + H) + (b + H) := (a + b) + H$$

Cette opération définit un groupe abélien, où H agit comme l'identité et l'inverse du coset $a + H$ et $(-a) + H$.
Ce groupe s'appelle le groupe quotient de G modulo H, noté G/H.

Homomorphisme de groupes

Soit deux groupes $(G, \perp, e_G)$ et $(G', \top, e_{G'})$.

Définition

Une application $f : G \to G'$ est un homomorphisme de groupe si :

1. $f(e_G) = e_{G'}$
2. Si $x, y \in G$, $f(x \perp y) = f(x) \top f(y)$

De plus

- $G = G'$ f est un endomorphisme
- Si f est bijective, f est un isomorphisme ($G \simeq G'$)
- si f est un isomorphisme et un endomorphisme, alors f est un automorphisme

Exercices

1. Déterminer le coset de $H = 3Z_{15}$ dans $G = Z_{15}$ contenant 5. Déterminer G/H.
2. Soit f un morphisme. Montrer que $f(x^{-1}) = f(x)^{-1}$
3. $(Z_8, +, 0)$ est-il isomorphe à $(Z_{30}^*, ., 1)$
4. Quel est l'ordre du groupe additif Z_n? Quel est celui du groupe multiplicatif Z_p^* (p premier)?
5. Le groupe $(Z_3, +, 0)$ est-il un sous groupe de $(Z_{15}, +, 0)$?
6. Quels sont les générateurs du groupe cyclique additif Z?
7. Sachant que tous les éléments de Z_{15}^* ont un ordre multiplicatif qui divise 4, est-il possible de savoir si Z_{15}^* est cyclique?

Corps

Définition

Un corps $(F, \oplus, \otimes)$ est un ensemble muni de deux opérations binaires $\oplus$ et $\otimes$, et deux éléments 0 et 1, ayant les propriétés suivantes :

- $(F, \oplus)$ est un groupe abélien (0 est l'identité)
- $(F \backslash \{0\}, \otimes)$ est un groupe abélien (1 est l'identité)
- Distributivité : $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Exemples

- $(\mathbb{Q}, +, .)$, $(\mathbb{Z}_p, +, .)$, p premier, sont des corps
- Les structures suivantes sont-elles des corps : $(\mathbb{Z}_6, +, .)$, $(\{1, 2, 3, 4\}, +_5, .5)$?

Fonction d'Euler

Définition

La fonction d'Euler $\phi(n)$ représente le nombre d'éléments dans $\mathbb{Z}_n^*$

$$\phi(n) = |\mathbb{Z}_n^*| = |\{i \in \mathbb{Z}_n \ : \ pgcd(i, n) = 1\}|$$

$\phi(n)$ est le nombre d'éléments de $\{0, \ldots, n-1\}$ qui sont premiers avec n
$\phi(1) = 1$ car $\mathbb{Z}_1^* = \{0\}$

Exemples

- Que vaut $\phi(23)$?
- Que vaut $\phi(64)$?

Fonction d'Euler

Théorème

Soit $n = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ l'unique factorisation de n. Alors

$$\phi(n) = \prod(p_i^{e_i - 1}(p_i - 1)) = n \prod(1 - \frac{1}{p_i})$$

Si la factorisation de n n'est pas connue, on ne sait pas déterminer $\phi(n)$

- $\phi(p) = p - 1$
- $\phi(p^e) = (p-1)p^{e-1} = p^e - p^{e-1}$
- $\phi(pq) = (p-1)(q-1)$
- Si $pgcd(a, b) = 1$ alors $\phi(ab) = \phi(a)\phi(b)$

Fonction d'Euler

- Soit $n = pq$ le produit de deux premiers
- Connaissant n et $\phi(n)$, peut-on retrouver p et q?

Exercices

- Soit $n = pq = 247$ et $\phi(n) = 216$. Déterminer p et q.
- Que vaut $\phi(55)$?
- Que vaut $\phi(65)$?

Théorème d'Euler

Pour tout a et n, si $pgcd(a, n) = 1$ alors

$$a^{\phi(n)} \equiv 1 \mod n$$

Preuve On sait que $a \in \mathbb{Z}_n^*$. Donc on sait que $a^{|\mathbb{Z}_n^*|} = a^{\phi(n)} = 1$

Petit théorème de Fermat

Soit p un nombre premier, pour tout entier a, on a

$$a^p \equiv a \mod p$$

Exercices

- Calculer $8^{11} \mod 11$, $7^{11} \mod 11$, $5^8 \mod 7$, $14^{16} \mod 17$, $67^{258} \mod 68$, $3^{45} \mod 5$, $7^{31} \mod 11$, $4^{25} \mod 35$, $7^8 \mod 30$.
- Montrer que Z_5 peut s'écrire sous la forme $Z_5 = \{0\} \cup \{g^0, g^1, g^2, g^3\}$.
- Chiffrement RSA (avec des petits nombres) : Bob désire chiffrer un message pour Alice.
  - Alice choisit p et q premiers et calcule $n = pq$. (elle choisit 3.11)
  - Alice choisit alors un entier $d < n = 33$ (elle choisit $d = 7$). d est la clé privée d'Alice.
  - Alice calcule sa clé publique e telle que $ed = 1 \mod (\phi(n))$. Quelle est la valeur de e?
  - Bob chiffre en calculant $C = m^e \mod n$ et Alice déchiffre en calculant $D = C^d \mod n$. Pourquoi D est-il égal à m?
  - Bob souhaite chiffrer le message BONJOUR. Il utilise le codage suivant A=01, B=02, C=03, ..., J=10,... et chiffre chaque lettre du message avec la clé publique. Quel est le résultat?

Générateurs de $\mathbb{Z}_n^*$

- Si $\mathbb{Z}_n^*$ admet un générateur, alors $\mathbb{Z}_n^*$ est cyclique
- $\mathbb{Z}_n^*$ admet un générateur SSI $n = 2, 4, p^k$, où $2p^k$ (p premier)
- Si α est un générateur de $\mathbb{Z}_n^*$, alors

$$\mathbb{Z}_n^* = \{\alpha^i \mod n : 0 \leq i \leq \phi(n) - 1\}$$

- Si α est un générateur de $\mathbb{Z}_n^*$, alors $b = \alpha^i \mod n$ est aussi générateur SSI $PGCD(i, \phi(n)) = 1$
- Si $\mathbb{Z}_n^*$ est cyclique, alors le nombre de générateurs de $\mathbb{Z}_n^*$ est $\phi(\phi(n))$

Calcul de l'inverse modulaire

Soit un entier a. Supposons que $\phi(n)$ soit connu. Alors

$$a^{\phi(n)} \equiv a.a^{\phi(n)-1} \equiv 1 \mod n$$

Donc

$$a^{-1} \mod n \equiv a^{\phi(n)-1}$$

Exemple Soit $n = 15$ $a = 11$, $\phi(15) = 8$,

$$a^{-1} \mod n \equiv 11^7 \mod 15 \equiv 11$$

En général cette méthode n'est pas plus rapide que l'algorithme d'Euclide étendu.

Application : Attaque sur RSA

- Stephane doit envoyer le même message M à Alice, Claire et Corinne
- les clés publiques sont respectivement $(n_1 = 26, e = 7),\ (n_2 = 35, e = 7),\ (n_3 = 33, e = 7)$, où n_i sont les modules RSA.
- Stephane envoie les valeurs $C_1 = 24,\ C_2 = 23,\ C_3 = 29$.
- Comment Estelle va-t-elle procéder pour retrouver M après avoir intercepté les trois valeurs et les clés publiques?

RQ

Soit $a \in \mathbb{Z}_n^*$; a est un résidu quadratique modulo n s'il existe $x \in \mathbb{Z}_n^*$ tel que $x^2 = a$ ($x^2 \equiv a \mod n$). Si un tel x n'existe pas, a est un non-résidu quadratique modulo n.
L'ensemble de tous les RQ modulo n est noté Q_n et celui des non-RQ, $\overline{Q}_n$.
Par définition $0 \notin \mathbb{Z}_n^*$, et donc $0 \notin Q_n$ et $0 \notin \overline{Q}_n$.

Proposition

Soit $p > 2$ un nombre premier et a un générateur de $\mathbb{Z}_p^*$. Alors $b \in \mathbb{F}_p$ est un RQ modulo p s'il existe un entier pair i tel que : $b \equiv a^i \mod p$. Il s'ensuit que :

$$|Q_p| = |\overline{Q}_p| = \frac{p-1}{2}.$$

La moitié des éléments sont des résidus et l'autre moitié des non-résidus.

RQ

Exercice : Un générateur de $\mathbb{Z}_p^*$ peut-il être un RQ modulo p?

Critère d'Euler : x est un résidu quadratique modulo p, premier, ssi :

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Exemple. 6 est un générateur de $\mathbb{Z}_{13}^*$. Les puissances de 6 sont :

i	0	1	2	3	4	5	6	7	8	9	10	11
6^i	1	6	10	8	9	2	12	7	3	5	4	11

Ainsi $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ et $\overline{Q}_{13} = \{2, 5, 6, 7, 8, 11\}$.

RQ

Proposition

Soit $n = pq$, p et q étant premiers distincts. Alors $a \in \mathbb{Z}_n$ est un RQ modulo n ssi la classe de a modulo p appartient à Q_p et celle de a modulo q à Q_q.

Dans la situation précédente on a :

$$\begin{aligned} |Q_n| &= |Q_p|.|Q_q| \\ &= \frac{(p-1)(q-1)}{4} \\ |\overline{Q}_n| &= 3\,\frac{(p-1)(q-1)}{4}\,. \end{aligned}$$

Exemple. $Q_{21} = \{1, 4, 16\}$, $\overline{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$.

Symboles de Legendre et Jacobi

Le symbole de Legendre permet de savoir si $a \in \mathbb{Z}$ est un RQ modulo p

Définition.

Soit $p > 2$ un premier et $a \in \mathbb{Z}$. Le symbole de Legendre $(\frac{a}{p})$ est ainsi défini :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p|a\,, \\ 1 \text{ si } a \in Q_p\,, \\ -1 \text{ si } a \in \overline{Q}_p\,. \end{cases}$$

a est un RQ modulo p si et seulement si le symbole de Legendre est égal à 1.

Propriétés du symbole de Legendre

- $(\frac{a}{p}) \equiv a^{(p-1)/2} \pmod{p}$. En particulier, $(\frac{1}{p}) = 1$ et $(\frac{-1}{p}) = (-1)^{(p-1)/2}$. Ainsi, $-1 \in Q_p$ si $p \equiv 1 \pmod 4$ et $-1 \in \overline{Q}_p$ si $p \equiv 3 \pmod 4$.
- $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. Donc, si $a \in \mathbb{Z}_n$, $a \neq 0$, alors $(\frac{a^2}{p}) = 1$.
- $a \equiv b \pmod p \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$.
- $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$. Donc, $(\frac{2}{p}) = 1$ si $p \equiv \pm 1 \pmod 8$ et $(\frac{2}{p}) = -1$ si $p \equiv \pm 3 \pmod 8$.
- Loi de réciprocité quadratique : si $q \neq p$ est premier impair, alors :

$$(\frac{p}{q}) = (-1)^{\frac{(p-1)(q-1)}{4}} (\frac{q}{p}).$$

Exercice : Que vaut $(\frac{33}{47})$?

Symbole de Jacobi (généralisation à entiers impairs)

Soit $n \geq 3$ un entier impair dont la factorisation en puissances de premiers est :

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} .$$

Alors le symbole de Jacobi est ainsi défini :

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$$

Si n est premier on retrouve le symbole de Legendre.

Attention

Contrairement au symbole de Legendre, le symbole de Jacobi ne dit pas si un nombre est RQ modulo n (non premier).
Il est vrai que si a est un RQ, alors $(\frac{a}{n}) = 1$, mais la réciproque est fausse.

TP

1. Programmer une fonction qui détermine les éléments de $\mathbb{Z}_n^*$ et teste si $\mathbb{Z}_n^*$ est cyclique
2. Programmer une fonction qui prend en input un entier n et retourne les générateurs de $\mathbb{Z}_n^*$, s'ils existent.
3. Programmer une fonction qui retourne les éléments d'ordre k dans $\mathbb{Z}_n^*$
4. Programmer une fonction qui retourne les éléments d'ordre k dans $\mathbb{Z}_n$
5. Programmer une fonction EulerPhi qui prend en input un entier x et calcule $\phi(x)$
6. Comparer le résultat de $a^y \mod n$ avec celui de $a^{y \mod \phi(n)} \mod n$
7. Programmer une fonction EncryptRSA qui prend en input un module, une clé publique et un message et retourne le chiffré du message. Le message étant un entier inférieur au module.
8. Programmer une fonction DecryptRSA qui prend en input un module, une clé privée et un chiffré et retourne le message clair.
9. Option : programmer une fonction qui teste si un entier est un carré modulo un entier premier

Autres algorithmes utiles

- Exponentiation modulaire
- Test de primalité
- Construction de nombres premiers
- Calcul du logarithme discret

Exponentiation modulaire : Algo square and multiply

Il s'agit de calculer dans un groupe a^n (ou na en notation additive).

Hörner

entrées : un tableau N de $K+1$ bits représentant n en binaire

sortie : le nombre $n = \sum_{i=0}^{K} N[i]2^i$

$n \leftarrow 0$;
$i \leftarrow K$;
Tantque $i \geq 0$ faire
  $n \leftarrow 2 * n$;
  si $N[i] == 1$
    alors $n \leftarrow n + 1$;
  $i \leftarrow i - 1$;
retourner n;

Square and multiply

entrées : un tableau N de $K+1$ bits représentant n en binaire

sortie : le nombre $P = a^n$

$P \leftarrow 1$;
$i \leftarrow K$;
tq $i \geq 0$ faire
  $P \leftarrow P^2$;
  si $N[i] == 1$
    alors $P \leftarrow P * a$;
  $i \leftarrow i - 1$;
retourner P;

Square and multiply : aspect récursif

fonction *puissance*(a, n)

si n vaut 0
  alors retourner 1
  sinon si n est pair
    alors retourner $(puissance(a, n/2))^2$
    sinon retourner $a * (puissance(a, (n-1)/2))^2$

Comparaison entre Hörner et square and multiply :
leurs nombres d'itérations sont identiques.
le nombre de boucles $=$ taille de n
A chaque boucle on fait une élévation au carré plus éventuellement une multiplication par a.
Si on note $t = \lfloor \ln(n) + 1 \rfloor$ la taille de n,
L'algorithme utilise $O(t)$ opérations simples.

Test de primalité

En cryptographie à clé publique, on a besoin de grands nombres premiers.
Déterminer si un nombre est premier est appelé le problème "Prime" noté $\mathcal{P}$.
On sait depuis 2002 que ce problème est polynomial
Mais en pratique,

- on utilise un test probabiliste de non-primalité
- et si besoin est, on lance un algorithme déterministe pour confirmer que le candidat premier trouvé par l'algorithme probabiliste est réellement premier

Test de non-primalité de Miller-Rabin

D'après le petit théorème de Fermat,

$$p \text{ premier} \Longrightarrow a^{p-1} \equiv 1 \mod p$$

Mais la réciproque est fausse : $561 = 3.11.17$ passe le test de Fermat (nombre de Carmichael)
Le test de Miller-Rabin améliore la méthode

- s'il répond qu'un nombre n'est pas premier alors il est sûr que ce nombre ne l'est pas
- Il peut aussi répondre qu'un nombre est probablement premier

Les témoins de Miller

Théorème

Soit n un entier impair > 1. Posons $n-1 = 2^s t$ avec t impair. S'il existe a $(1 < a < n)$ tel que :

$$a^t \not\equiv 1 \mod n$$

et :

$$a^{2^i t} \not\equiv -1 \mod n \quad \forall i = 0, \cdots, s-1,$$

alors n n'est pas premier.

Preuve Supposons n premier. Pour $i = 0, \cdots, s$ posons $a_i = a^{2^i t} \mod n$. D'après le petit théorème de Fermat $a_s = 1$. Dans ces conditions ou bien tous les a_i valent 1 et dans ce cas a_0 vaut 1, ou bien il existe un i tel que $0 \leq i < s$, $a_i \neq 1$ et $a_{i+1} = 1$. Dans ce cas, puisque $a_{i+1} \equiv a_i^2 \mod n$ et que $\mathbb{Z}/n\mathbb{Z}$ est un corps on en déduit que $a_i \equiv -1 \mod n$.

Les témoins de Miller

- Si a vérifie les conditions du théorème
- il apporte une preuve de la non-primalité de n
- a s'appelle un témoin de Miller relatif à n.

Idée : utiliser le théorème pour détecter si un nombre est premier ou tout au moins s'il a de bonnes chances de l'être.

Le théorème de Rabin permet de majorer pour un entier n composé, le nombre d'éléments strictement compris entre 1 et n qui ne sont pas des témoins de Miller.

Théorème (Théorème de Rabin)

Soit n un entier impair composé > 9. Posons $n-1 = 2^s t$ avec t impair. Les entiers $1 < a < n$ qui satisfont à la condition :

$$a^t \equiv 1 \mod n,$$

ou bien à l'une des conditions :

$$a^{2^i t} \equiv -1 \mod n \quad (0 \leq i \leq s-1),$$

sont en nombre au plus :

$$\frac{\Phi(n)}{4}.$$

Test de Miller-Rabin

On choisit a au hasard ($a < n$) et on calcule :

$$a^t \mod n.$$

Si on trouve 1 alors a n'est pas un témoin de Miller pour n, sinon on calcule les nombres :

$$a^{2^i t} \mod n,$$

et si pour un certain i on trouve -1 alors a n'est pas un témoin de Miller pour n.
Faisons ce test avec k valeurs aléatoires de a; si aucune des valeurs a, tirées au hasard, n'est témoin de Miller, le nombre n est vraisemblablement premier.
Plus précisément, si n est composé, la probabilité d'être déclaré premier est $< \frac{1}{4^k}$. On peut prendre par exemple $k = 50$.

Construire un nombre premier de taille donnée

- On choisit aléatoirement un nombre impair
- On teste ce nombre
- S'il n'est pas premier, on lui ajoute 2

Construire p et q premiers tels que $p = kq + 1$

- On fixe un nombre premier q
- On choisit aléatoirement un entier pair k
- On teste si $p = kq + 1$ est premier
- Si p n'est pas premier, on incrémente k de 2 et on reteste la primalité de $p = kq + 1$

L'algorithme aboutit en pratique.
Cette méthode est utilisée dans le système RSA

Les nombres de Sophie Germain

- au lieu de fixer q, on fixe k (par exemple 2)
- Si q et $2q+1$ sont premiers, q est un nombre de Sophie Germain.
- On construit un q premier et on teste si $2q+1$ est premier, sinon on passe au nombre premier q suivant.

DLP

Soit G un groupe cyclique d'ordre n (noté multiplicativement)
Soit α un générateur du groupe G. On a

$$G = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

Ainsi tout élément x de G s'écrit d'une unique façon sous la forme :

$$x = \alpha^k$$

avec $0 \leq k \leq n-1$. L'exposant k est appelé le logarithme discret de x.

Le problème du logarithme discret (DLP) est de trouver k connaissant x.

Pour certains groupes, le DLP est difficile (par exemple $\mathbb{Z}/p\mathbb{Z}^*$, $|p| > 1024 bits$)

Cas de $\mathbb{Z}/p\mathbb{Z}^*$

- Si on représente les éléments comme des entiers de $\{1, \cdots, p-1\}$, il existe des algorithmes sous-exponentiels pour résoudre DLP
- Pour un groupe générique, le problème est exponentiel
- L'algorithme "pas de géant, pas de bébé" est un algo exponentiel qui permet de résoudre DLP dans tout groupe fini
- Conséquence : dans le premier cas, la taille du groupe doit être plus grande que dans le second
- 1024 bits contre 160 bits pour un groupe générique
- Sous-groupe d'ordre premier q de $\mathbb{Z}/p\mathbb{Z}^*$ se comporte comme un groupe générique (environ 1024 bits pour p, 160 bits pour q)
- Groupe des points d'une courbe elliptique : aucun algo sous-exponentiel, donc exposants et clés plus petits

DLP : Pas de bébé, pas de géant

$x = \alpha^k$

- On fixe $w < n \quad (n = Ord(\alpha))$
- On pose $k = k_0 + w\,k_1$, $0 \leq k_0 < w$, $0 < k_1 < n/w$
- On veut résoudre $\alpha^{k_0} = x\,\alpha^{-wk_1}$
- On calcule et stocke tous les α^{k_0} (pas de bébés)
- On calcule $x\,\alpha^{-wk_1}$ (pas de géant) que l'on compare à α^{k_0}
- Si les valeurs sont différentes, on incrémente k_1

Le coût de cet algorithme est $O(w)$ opérations pour la première phase, et $O(n/w)$ pour la seconde. En choisissant w de l'ordre de $(n)^{1/2}$, on obtient une complexité de $O((n)^{1/2})$.

Exercice : Déterminer k tel que $\alpha^k = 57 \mod 113$. Prendre $\alpha = 3$ et $w = 10$.