# Concepts mathématiques



# Concepts mathématiques

Arithmétique modulaire



En cryptographie on fait un usage intensif de l'arithmétique modulo n. Celle-ci permet de restreindre la taille de tous les résultats intermédiaires et de la valeur finale. C'est indispensable, par exemple, pour le calcul de logarithmes discret ou de racines carrées qui sont des opérations très coûteuses en ressources de calcul. Pour un module n qui peut être représenté par k bits, le résultat de toute addition, soustraction ou multiplication peut être représenté par au plus 2k bits. Idem pour les résultats intermédiaires.

## Divisibilité

- Soient a et n $\in \mathbb{N}$ quelconques

  $a = qn + r \qquad 0 \leq r < n \; ; \; q = \lfloor a/n \rfloor$

  Le reste r = le résidu

  - Exple :
    - a = 11, n = 7 → 11 = 1 * 7 + 4 → r = 4
    - a = -11, n = 7 → -11 = (-2) * 7 + 3 → r = 3
- Si a, n $\in \mathbb{N}$ et n > 0,
  - a mod n = le reste quand a est divisé par n.
  - $a = \lfloor a/n \rfloor * n + (a \bmod n)$
  - Exple : 11 mod 7 = 4



Etant donné n et a deux entiers quelconques, si on divise a par n, on obtient un quotient entier (q) et un reste entier (r) obéissant à la relation :

$a = qn + r \qquad 0 \leq r < n \; ; \; q = \lfloor a/n \rfloor$

Le reste r = le résidu

Exple :

Si a est un entier et n un entier positif, on défini
a mod n comme le reste quand a est divisé par n.

On peut donc écrire $a = \lfloor a/n \rfloor * n + (a \bmod n)$

Exple : 11 mod 7 = 4

## Diviseurs

- Soient a, b et m $\in \mathbb{N}$
  - b ($\neq 0$) divise a si a = mb
  - b est un diviseur de a.
  - Exple : les diviseurs de 24 sont 1,2,3,4,6,8,12,24
  - Propriétés :
    1. Si a|1 alors $a = \pm 1$
    2. Si a|b et b|a alors $a = \pm b$
    3. Tout b $\neq 0$ divise 0
    4. Si b|g et b|h alors b|(mg + nh) pour m et n arbitraires
    5. Si $a \equiv 0 \bmod n$ alors n|a

## Diviseurs

- Démonstration de la propriété 4 :
  - Si b|g et b|h alors b|(mg + nh) pour m et n arbitraires
    - Si b|g alors g est de la forme $g = b*g_1$
    - Si b|h alors h est de la forme $h = b*h_1$
    - Donc $mg + nh = mbg_1 + nbh_1 = b*(mg_1 + nh_1)$
  - Exple
    - b = 7, g = 14, h = 63, m = 3, n = 2
    - 7|14 et 7|63, on montre 7|(3*14 + 2*63)
    - On a (3*14 + 2*63) = 7(3*2 + 2*9)
    - Et il est clair que 7|(7(3*2 + 2*9))



**Critères de divisibilité :**

•n est divisible par 2 s'il se termine par 0,2,4,6,8.

•n est divisible par 3 si la somme de ses chiffres est divisible par 3.

•n est divisible par 4 si ses deux derniers chiffres forment un multiple de 4 (ex : 256628).

•n est divisible par 5 s'il se termine par 0 ou 5.

•n est divisible par 8 si ses 3 derniers chiffres forment un multiple de 8 (ex : 176072).

•n est divisible par 9 si la somme de ses chiffres est un multiple de 9 (ex : 37521=3+7+5+2+1=18=2×9).

•n est divisible par 11 si la différence (1erchiffre + 3èmechiffre + 5èmechiffre + ...) - (2èmechiffre + 4èmechiffre + 6èmechiffre + ...) est divisible par 11.

• Par exemple, 1485 est divisible par 11, car (1+8)-(4+5)=0 est divisible par 11.

## Congruence

- Deux entiers a et b sont égaux (ou congrus) modulo n si n|a-b.
- Deux entiers a et b sont dits congruents modulo n si (a mod n) = (b mod n)
- s'écrit $a \equiv b \bmod n$
  - Exple : $73 \equiv 4 \bmod 23$ $21 \equiv -9 \bmod 10$
- Reste $\triangleq$ deux nombres congrus pour le module *n* sont résidus l'un de l'autre pour ce module



**RAPPELS SUR LA CONGRUENCE**

Définition: Soit $m \in \mathbb{Z} \setminus \{0\}$ On dit que " a est congru à *b* modulo *m*", et on écrit:

si $m \mid (a-b)$ ; dans le cas contraire, on dit que "a est non congru à *b* modulo *m*".

$$a \equiv b \mod(m)$$

## Propriétés de la congruence

1. $a \equiv b \bmod n$ ssi $n|a-b$
2. $a \equiv b \bmod n \Leftrightarrow ca \equiv cb \bmod (cn)$
3. $a \equiv b \bmod n \Leftrightarrow a^c \equiv b^c \bmod n$
4. $a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$
5. $a \equiv b \bmod n$ et $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$
6. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
7. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
8. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$



## Démonstrations

- P1 : $a \bmod n \equiv b \bmod n$
  - si $n|(a-b)$ alors $(a-b) = kn$ pour un k.
  - On peut écrire $a = b + kn$.
  - Ainsi $(a \bmod n)$ = (le reste quand $b + kn$ est divisé par n)
    = (le reste de b divisé par n) = $(b \bmod n)$
- P6 : $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  - Définissons $r_a = (a \bmod n)$ et $r_b = (b \bmod n)$
  - On peut écrire $a = r_a + jn$ et $b = r_b + kn$ (j et k des entiers)
  - Alors $(a + b) \bmod n = (r_a + jn + r_b + kn) \bmod n$
    $= (r_a + r_b + (k + j)n) \bmod n = (r_a + r_b) \bmod n$
    $= [(a \bmod n) + (b \bmod n)] \bmod n$

## Exemples :

- P1 :
  - $23 \equiv 8 \pmod 5$ car $23 - 8 = 15 = 5 * 3$
  - $-11 \equiv 5 \pmod 8$ car $-11 - 5 = -16 = 8*(-2)$
- Si 11 mod 8 = 3 15 mod 8 = 7
- P6 :
  - [(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2
  - (11 + 15) mod 8 = 26 mod 8 = 2
- P7
  - [(11 mod 8) – (15 mod 8)] mod 8 = -4 mod 8 = 4
  - (11 – 15) mod 8 = -4 mod 8 = 4



## Exemples :

- P8
  - [(11 mod 8) * (15 mod 8)] mod 8 = 21 mod 8 = 5
  - (11 * 15) mod 8 = 165 mod 8 = 5
- Décomposition par facteurs plus simples
- Exple :
  - Pour trouver $11^7$ mod 13, on peut procéder comme suit
    - $11^2 = 121 \equiv 4 \pmod{13}$
    - $11^4 = 4^2 \equiv 3 \pmod{13}$
    - $11^7 = 11 * 11^4 * 11^3 \equiv (11*4*3)\ 132 \equiv 2 \pmod{13}$

## $\mathbb{Z}_n$

- Soit $\mathbb{Z}_n$ l'ensemble des entiers $\mathbb{Z}_n = \{0,1,\ldots,(n-1)\}$

  $\mathbb{Z}_n$ représente l'ensemble des résidus ou les classes de résidu modulo n (chaque entier dans $\mathbb{Z}_n$ est une classe de résidu). On peut écrire ces classes [0], [1],…,[n 1] où [r] = {a : a est entier, a ≡ r mod n}

  - Exple : classes de résidu modulo 4
    - [0] = {…, -8, -4,0,4,8,…}
    - [1] = {…,-7,-3,1,5,9,…}
    - [2] = {…,-6,-2,2,6,10,…}
    - [3] = {…,-5,-1,3,7,11,…}



De tous les nombres entiers dans une classe de résidu, le plus petit nombre entier non négatif est celui habituellement utilisé pour représenter la classe de résidu.

Trouver le plus petit nombre entier non négatif pour lequel k est congruent modulo n s'appelle **la réduction de k modulo n.**

## Propriétés de l'arithmétique de $\mathbb{Z}_n$

| Property | Expression |
|---|---|
| Commutative laws | $(w + x) \bmod n = (x + w) \bmod n$<br>$(w \times x) \bmod n = (x \times w) \bmod n$ |
| Associative laws | $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$<br>$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$ |
| Distributive laws | $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$<br>$[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$ |
| Identities | $(0 + w) \bmod n = w \bmod n$<br>$(1 \times w) \bmod n = w \bmod n$ |
| Additive inverse ($-w$) | For each $w \in Z_n$, there exists a $z$ such that $w + z \equiv 0 \bmod n$ |

## PGCD

- PGCD – plus grand commun diviseur
  - L'entier c est le plus grand commun diviseur de a et b si
    - c est un diviseur de a et de b
    - tout diviseur de a et b est un diviseur de c
  - gcd(a,b) = max [k : k|a et k|b]
  - gcd(a,b) = gcd(|a|,|b|)  et  gcd(a, 0) = |a|



## Nombres premiers

- Théorème fondamental de l'arithmétique :
  - *Tout nombre naturel n>1 peut s'écrire comme un produit de nombres premiers, et cette représentation est unique, à part l'ordre dans lequel les facteurs premiers sont disposés.*
- Deux entiers sont relativement premiers si leur unique facteur commun positif est 1
- Notation : soient a et c relativement premiers :
  - (a,c) = 1 ou pgcd(a, c) = 1



Démonstration:

•Si *n* est premier, alors la preuve est terminée.

•Supposons que *n* n'est pas premier et considérons l'ensemble: D={d tel que d|n et 1 < d < n}

•Alors, $D \in \mathbb{N}$ et , puisque *n* est composé, on a que $D \neq \varnothing$

•D'après le principe du bon ordre (tout ensemble non vide contient un plus petit élément) , *D* possède un plus petit élément $p_1$ qui est premier, sans quoi le choix minimal de $p_1$ serait contredit.

•On peut donc écrire $n=p_1n_1$

•Si $n_1$ est premier, alors la preuve est terminée

•Si $n_1$ est composé, alors on répète le même argument que précédemment et on en déduit l'existence d'un nombre premier $p_2$ et d'un entier $n_2 < n_1$ tels que $n=p_2p_1n_2$

En poursuivant ainsi on arrive forcément à la conclusion que $n_k$ sera premier

## Propriétés de $\mathbb{Z}_n$

- Propriété de l'addition
  - $(a + b) \equiv (a + c) \bmod n \Rightarrow b \equiv c \bmod n$
  - Démonstration : additionner l'inverse additif de a
  - Exple : $(5 + 23) \equiv (5 + 7) \bmod 8 \rightarrow 23 \equiv 7 \bmod 8$
- Propriété de la multiplication
  - Si (a,n) = 1 : $(a*b) \equiv (a*c) \bmod n \Rightarrow b \equiv c \bmod n$
  - Démonstration : multiplier par l'inverse modulaire de a
  - La condition doit absolument être vérifiée
  - Exple : $(6,8) \neq 1 \rightarrow 6 * 3 \equiv 2 \bmod 8$ et $6 * 7 \equiv \bmod 8$ or $3 \neq 7 \bmod 8$



La raison de ce résultat étrange est que pour un modulo général n, un multiplieur a qui est appliqué aux entiers de 0 à (n-1) ne produira pas un ensemble complet de résidus si a et n ont des facteurs communs

## Explication :

- Exemple(1)
  - Avec a = 6 et n = 8

| $\mathbb{Z}_8$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Multiplié par 6 | 0 | 6 | 12 | 18 | 24 | 30 | 36 | 42 |
| résidus | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |

  - Pas d'ensemble complet de résidus
  - Plusieurs résidus identiques (plusieurs nombres donnent le même résidu)

  $\Rightarrow$ Pas d'inverse unique



Comme on n'obtient pas un ensemble complet de résidus quand on multiplie par 6, plus de un entier de $\mathbb{Z}_8$ donne le même résidu. Ainsi, 6*0 mod8 = 6*4 mod8, 6*1 mod8 = 6*5 mod8, etc. Comme il s'agit d'une relation n-à-1, il n'y a pas d'inverse unique dans les opérations de multiplication

## Particularité de $\mathbb{Z}_n$

- Exemple(2)
  - Avec a = 5 et n = 8

| $\mathbb{Z}_8$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Multiplié par 5 | 0 | 5 | 10 | 15 | 20 | 25 | 30 | 35 |
| résidus | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |

  - La ligne des résidus contient tous les entiers de $\mathbb{Z}_8$ dans le désordre.
  - En général un entier a un inverse multiplicatif dans $\mathbb{Z}_n$ si cet entier est relativement premier à n



# Concepts mathématiques

Algorithmes d'Euclide

## Algorithme d'Euclide : introduction

- Objectif : permet de déterminer le PGCD de deux nombres entiers positifs sans avoir besoin de faire leur décomposition en facteurs premiers
- Principe :
  - Si a et b $\in \mathbb{N}$ et a $\geq$ b, si $\forall$ b>0 a $\equiv$ r mod b, alors pgcd(a,b) = pgcd(b,r).
  - Base : soient a et b $\in \mathbb{N}$, a $\geq$ 0 et b > 0

    gcd(a,b) = gcd(b,a mod b)
  - Exple : gcd(55,22) = gcd(22, 55 mod 22) = gcd(22,11) = 11



## Algorithme d'Euclide : algorithme

- a > b > 0
- `Euclid(a, b)`

```
1. A ← a;  B ← b
2. IF B = 0 RETURN A = gcd(a, b)
3. R = A mod B
4. A ← B
5. B ← R
6. GOTO 2
```

## Algorithme d'Euclide : exemple

- Exple : gcd(1970,1066)
  - 1970 = 1*1066 + 904 gcd(1066,904)
  - 1066 = 1*904 + 162 gcd(904,162)
  - 904 = 5*162 + 94 gcd(162,94)
  - 162 = 1*94 + 68 gcd(94,68)
  - 94 = 1*68 + 26 gcd(68,26)
  - 68 = 2*26 + 16 gcd(26,16)
  - 26 = 1*16 + 10 gcd(16,10)
  - 10 = 1*6 + 4 gcd(6,4)
  - 6 = 1*4 + 2 gcd(4,2)
  - 4 = 2*2 + 0 gcd(2,0)



# Concepts mathématiques

Champs finis (GF)

## Champs finis d'ordre p

- GF(p) $\triangleq$ l'ensemble $\mathbb{Z}_p$ des entiers {0,1,…,p-1} avec l'arithmétique des opérations modulo p.
- $\forall w \in \mathbb{Z}_p$, $w \neq 0$, $\exists$ un $z \in \mathbb{Z}_p$ tel que $w*z \equiv 1 \bmod p$
- L'ensemble GF(p) est consistant avec l'existence d'un inverse multiplicatif,

  SI $(a*b) \equiv (a*c) \bmod p$ ALORS $b \equiv c \bmod p$
- Remarque : GF(2) :
  - Dans ce cas particulier, l'addition est équivalente à un XOR et la multiplication est équivalente à l'opération logique AND.



**Démonstration**

On sait que n'importe quel entier dans $Z_n$ a un inverse multiplicatif si et seulement si ce nombre entier est relativement premier à n.

Si n est premier alors tous les nombres entiers non nuls dans $Z_n$ sont relativement premiers à n, et donc il existe un inverse multiplicatif pour tous les nombres entiers non nuls dans $Z_n$.**

Il est possible d'étendre l'algorithme d'Euclide de sorte que, en plus de trouver gcd(m, b), si le gcd donne 1, l'algorithme retourne l'inverse multiplicatif de b

## Arithmétique dans GF(7)

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

(a) Addition modulo 7

| w | −w | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 6 | 1 |
| 2 | 5 | 4 |
| 3 | 4 | 5 |
| 4 | 3 | 2 |
| 5 | 2 | 3 |
| 6 | 1 | 6 |

(c) Additive and multiplicative inverses modulo 7

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

(b) Multiplication modulo 7

# Algorithme d'Euclide étendu

- EXTENDED EUCLID(m,b)

1. (A1, A2, A3) ← (1,0,m); (B1,B2,B3) ← (0,1,b)
2. IF B3 = 0 RETURN A3 = gcd(m,b);  no inverse
3. IF B3 = 1 RETURN B3 = gcd(m,b); B2 = $b^{-1}$ mod m
4. Q = ⌊ A3/B3 ⌋
5. (T1,T2,T3) ← (A1-QB1, A2-QB2, A3-QB3)
6. (A1,A2,A3) ← (B1,B2,B3)
7. (B1,B2,B3) ← (T1,T2,T3)
8. GOTO 2



# Euclide étendu : exemple

- Exemple d'exécution de l'algorithme :
  - gcd(550,1759) = 1
  - Inverse multiplicatif de 550 = 355 : (550*355) ≡ 1 mod 1759

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 1759 | 0 | 1 | 550 |
| 3 | 0 | 1 | 550 | 1 | –3 | 109 |
| 5 | 1 | –3 | 109 | –5 | 16 | 5 |
| 21 | –5 | 16 | 5 | 106 | –339 | 4 |
| 1 | 106 | –339 | 4 | –111 | 355 | 1 |



SI B3 = 0 \rightarrow pas d'inverse

SI B3 = 1 \rightarrow pgcd = 1 et inverse modulaire = B2

## Résolution d'équations de la forme $a*x \equiv b \bmod n$

**The equation**

$$a \cdot x \equiv b \bmod n$$

**has**

**1. one solution** iff $\gcd(a, n) = 1$

$x = a^{-1} \cdot b \pmod n$

**2. no solutions** iff $d = \gcd(a, n) \neq 1$, and $d \nmid b$

**3. *d* solutions** iff $d = \gcd(a, n) \neq 1$, and $d \mid b$

The solutions are

$x_0,\ x_0 + n/d,\ x_0 + 2 \cdot n/d,\ x_0 + 3 \cdot n/d,\ \ldots,\ x_0 + (d\text{-}1) \cdot n/d,$

where $x_0 = (a/d)^{-1} \cdot (b/d) \pmod{n/d}$



## Autres concepts utiles

## Petit théorème de Fermat

- **Théorème :** Soit p un nombre premier, (a,p)=1. Alors :

$$a^{p-1}=1 \bmod p$$

- Intérêt : déduire un test de non-primalité :
  - Si $n \in \mathbb{N}$ est donné, soit a tel que (a,n)=1
  - On calcule $a^{n-1}$. Si $a^{n-1} \neq 1 \bmod n$ : n n'est pas premier.
- Ce test est très rapide, car on calcule $a^{n-1}$ en effectuant au plus 2 log n opérations.
  - Exple : calculer $3^{12}$,
    on remarque que $12=23+22$, d'où $3^{12}=((32)^2)^2(32)^2$.



**Théorème :** Soit p un nombre premier, et a un entier premier avec p. Alors $a^{p-1}$ a pour reste 1 dans la division par p :

$$a^{p-1}=1 \bmod p$$

## Petit théorème de Fermat

- Cependant, ce théorème est une condition nécessaire mais pas suffisante de primalité :
  - Si p est un nombre premier, $\nexists$ a < p avec (a,p)=1 tel que $a^{p-1}$ 1ait un résidu non nul modulo p
  - Mais pas de résidu ne signifie pas que p est premier !



Le petit théorème de Fermat est cependant également valable pour quelques nombres *N* qui ne sont pas premiers. Mais les nombres qui vérifient ça sans être premiers sont "rares", et du coup ça vaut la peine de déclencher un algorithme plus "sophistiqué" pour savoir si *N* est réellement premier ou non (disons que dans ce cas, *N* est un bon candidat à la primalité et est alors appelé "nombre pseudo-premier"). Pour tester si le nombre *N* non-premier est "suffisamment premier", on essaie avec un algorithme de tester le petit théorème de Fermat pour un nombre maximal de $a \in \mathbb{N}$ avec a < N .

## Fonction totient d'Euler

- Soit la fonction d'Euler définie par :
- $\phi(m) = \#\{n \leq m \mid (n,m)=1\}$
- $\phi(n) =$
  - L'indicateur d'Euler
  - Le cardinal des entiers inversibles de n
  - Si n est premier : $\phi(n) =$ ก 1
  - Donne le nombre d'entiers positifs plus petits ou égaux à n relativement premiers à n .



Il faut lire: la fonction \phi du nombre *m* a pour résultat un nombre *n* inférieur ou égal à *m* et tel que le plus grand commun diviseur de *n* et *m* soit 1.

Propriété remarquable : compter le nombre d'entiers positifs plus petits que *m* et "relativement premiers" (attention, nous reviendrons sur cette terminologie) à *m*, c'est-à-dire:

$$\phi(m) = \sum_{\substack{k=1 \\ (k,m)=1}}^{m} 1$$

## Fonction totient d'Euler

- Exple : n = 11 $\rightarrow$ $\phi(n) = 10$
- Soient p et q deux nombres premiers et n = pq

  $\phi(n) = \phi(pq) = \phi(p)*\phi(q) = (p-1)(q-1)$
- Exple : p=11, q=13 $\rightarrow$ n=143 et $\phi(n) = 10*12 = 120$



**Démonstration $\phi(n) = \phi(p)\phi(q)$**

Soit l'ensemble des résidus de n ($\mathbb{Z}_n$) : {0,1,…,(pq-1)}

Les résidus qui ne sont pas premiers à n sont les ensembles {p, 2p, …, (q-1)p}, {q,2q,…,(p-1)q} et 0

De la sorte :

$\phi(n)$

$= pq – [(q-1)+(p-1)+1]$

$= pq – (p+q) + 1$

$= (p-1)*(q-1)$

$= \phi(p) * \phi(q)$

## Théorème d'Euler (généralisation Fermat)

- Théorème : soit (a,m)=1 alors $a^{\phi(m)} = 1 \bmod (m)$
- Démonstration
  - Lemme 1 : un système de résidus modulo m est un ensemble d'entiers $r_i$ tel que
    - $(r_i,m)=1$
    - $r_i$ n'est pas congru $r_j$ modulo m pour $i \neq j$
    - Pour chaque x tel que (x,m)=1, x est congru à un certain $r_i$ mod m
  - Exple :
    - {1,5} est un système réduit de résidus modulo 6. {1,2,3,4,5,6,7} est un srr modulo 7
    - 1 n'est pas congru 5 modulo 6 ($6 \nmid (5-1)$)



Système réduit de résidus = l'ensemble des résidus premiers par rapport à n (c'est un sous-ensemble de tous les résidus modulo n)

Calcul d'un inverse modulaire: si (a,x) mod n = b et (a,n)=1

Par Euler : x = (b.a^{\phi(n)-1} mod n

Par Euclide : x = b(a^{-1}mod n))mod n

En général Euclide est plus rapide

## Théorème d'Euler

- Lemme 2 : soit $\{r_1,r_2,..,r_{\phi(m)}\}$ un système réduit de résidus modulo *m.* $\{ar_1,ar_2,..,ar_{\phi(m)}\}$ est aussi un système réduit de résidus modulo *m.*
- Corollaire *:* si $(r_i,m)=1$ et (a,m)=1, alors $(ar_i,m)=1$ est aussi satisfait
- Démonstration :
  - Posons d=1
  - $(r_i, m)=1$ (lemme1) et (a,m)=1 (hypothèse du théorème)
  - Puisque $(r_i,m)=d \rightarrow d|r_i$ et $d_m$. idem pour (a,m)=d
  - Si d|a ou $d|r_i$, on a $d|ar_i$ et d|m. Ce qui nous permet d'écrire :

$$(ar_i,m) = (r_ia,m) = 1$$



Remarque: Vous pouvez observer que le nombre de résidus correspondent, pour un modulo *m* premier donné, au résultat défini par la fonction $\phi$ d'Euler. On parle alors de "conjecture", c'est-à-dire une supposition fondée sur des probabilités

## Théorème d'Euler

- Donc, il y a bijection entre les deux ensembles de résidus.
- On peut écrire : $\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} r_i \mod(m)$
- Et par les règles élémentaires d'algèbre :

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \mod(m)$$

- Puisque $\left(m, \prod_{i=1}^{\phi(m)} r_i\right) = 1$ (vous pouvez vérifier!),
- on est bien obligé de conclure que: $a^{\phi(m)} \equiv 1 \mod m$



Revenons à notre théorème d'Euler. Nous venons de démontrer qu'il y a bijection entre les deux ensembles de résidus. C'est-à-dire que pour chaque résidu $r_i$ du système réduit modulo *m*, on aura un résidu $ar_i$ du système réduit modulo *m* selon la propriété fondamentale de la congruence qui rappelons-le dit que:

"On peut multiplier les deux membres d'une congruence par un même nombre entier et il restera congru modulo *m* et modulo *m* multiplié par ce nombre entier.«

Exemple : prenons $35 \equiv 5 \mod 6$, effectivement 6|(35-5=30) car le reste de la division de 30 par 6 est bien nul. Si on prend par exemple $2*35 \equiv 2*5 \mod (2*6)$ alors également 12|(70-10=60) et le reste est nul également

Petit rappel sur la bijection: On dit que l'on a une bijection, si à chaque élément d'un ensemble de départ correspond au moins un élément dans l'ensemble d'arrivée (s'il y avait pour chaque homme sur Terre un femme – à proportions égales donc – il y aurait bijection entre l'ensemble des Hommes et des Femmes).

Bref, comme il y a bijection, on peut écrire:

$$\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} r_i \mod(m)$$

Exemple: L'ensemble {1,5} est un système réduit de résidus modulo 6 comme nous l'avons déjà vu. On a donc $(r_2,m) = (5,6) = 1$ . Si l'on prend un a tel que (a,m)=1 , par exemple a=7 car effectivement (7,6)=1 . Alors $7*5 \equiv 5 \mod 6$ car 6|(35-5 = 30) . Effectivement 6 divise bien 30 avec un reste nul.

## Théorème du reste chinois

- **Théorème :** Prenons $m_1$, ..., $m_n$ des entiers supérieurs à 2 deux à deux premiers entre eux, et $a_1$,...,$a_n$ des entiers. Le système d'équations :

$$x=a_1 \mod m_1$$

...

$$x=a_n \mod m_n$$

admet une unique solution modulo $M=m_1 \times ... \times m_n$ donnée par la formule :

$$x=a_1M_1y_1+...+a_nM_ny_n \mod M$$

où $M_i=M/m_i$, et $y_i=M_i^{-1} \mod m_i$ pour i compris entre 1 et n.



Si on connaît la décomposition en facteurs premier de n, on peut utiliser le CRT pour résoudre un système d'équation particulier.

## Exemple

- Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces.
- Mais les pirates se querellent, et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces.
- Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier.
- Quelle est la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates?



## Exemple

- Si x est ce nombre, x est le plus petit entier positif tel que :

  $x = 3 \bmod 17.$

  $x = 4 \bmod 11.$

  $x = 5 \bmod 6.$

- On applique le théorème chinois :
  - On a $M = 17 \times 11 \times 6 = 1122$, $M_1 = 66$, $M_2 = 102$, $M_3 = 187$.
  - L'inversion de chaque $M_i$ donne $y_1 = 8$, $y_2 = 4$, $y_3 = 1$.
  - On obtient donc :

    $x = 3 \times 66 \times 8 + 4 \times 102 \times 4 + 5 \times 187 \times 1 \bmod 1122 = 785 \bmod 1122.$

- 785 pièces d'or, voila qui reste particulièrement motivant!

## Résidus quadratiques

- Si p est premier et a < p alors a est un résidu quadratique modulo p si $x^2 \equiv a \pmod p$ pour un certain x
- Attention, une valeur quelconque de a ne satisfait pas spécialement cette propriété
- Il existe (p-1)/2 résidus quadratiques modulo p
- Si n = pq (p et q premiers), il y a exactement (p-1)(q-1)/4 résidus quadratiques modulo n



Exple : si p=7 les résidus quadratiques sont 1,2,4

$1^2 = 1 \equiv 1 \bmod 7$

$2^2 = 4 \equiv 4 \bmod 7$

$3^2 = 9 \equiv 2 \bmod 7$

$4^2 = 16 \equiv 2 \bmod 7$

$5^2 = 25 \equiv 4 \bmod 7$

$6^2 = 36 \equiv 1 \bmod 7$

Chaque résidu quadratique apparaît 2 fois dans la liste. Mais 3,6 et 5 ne satisfont pas cette équation

## Symbole de Legendre

- **Définition :**. Si p est premier impair, on définit le symbole de Legendre :

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si x carré dans } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{sinon.} \end{cases}$$

- **Autre définition** : L(a,p) pour a $\in \mathbb{N}$ et p un nombre premier >2 :
  - L(a,p) = 0 si p|a
  - L(a,p) = 1 si a est un résidu quadratique modulo p
  - L(a,p) =- 1 sinon



L'équation $y^2=x$, x fixé, n'est pas toujours résoluble dans **Z**_n. on a besoin de savoir si cette équation a des solutions ou non!

## Symbole de Legendre

- Pour calculer, le symbole de Legendre, on dispose des 4 propriétés suivantes :
  - $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
  - $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
  - $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
  - $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. si p et q sont deux premiers impairs distincts
- La dernière proposition s'appelle loi de réciprocité quadratique.



La dernière proposition s'appelle loi de réciprocité quadratique. Elle fut longtemps un problème ouvert avant que Gauss ne la démontre, et en donne d'ailleurs plusieurs preuves différentes.

## Symbole de Legendre

- **Exemple :** x2=219 admet-elle une solution modulo 383? On calcule le symbole de Legendre :

$$\begin{aligned}\left(\frac{219}{383}\right) &= \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)\\ &= -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right)\\ &= -\left(\frac{-1}{3}\right)\left(\frac{18}{73}\right)\\ &= \left(\frac{2}{73}\right) = 1\end{aligned}$$

oui

## Symbole de Legendre

- Calcul direct :
  - $L(a,p) = a^{(p-1)/2} \bmod p$
- Calcul récursif :
  - Si a = 1 : L(a,p) = 1
  - Si a est pair : $L(a,p) = L(a/2,p) * (-1)^{(p^2-1)/8}$
  - Si a est impair : $L(a,p) = L(p \bmod a, a) * (-1)^{(a-1)((p-1)/4)}$
- Remarque : si p est premier : c'est un moyen efficace de calculer un résidu quadratique



## Symbole de Jacobi (J(a,n))

- Généralisation du symbole de Legendre
- Définition :
  - J(a,n) n'est défini que pour n impair
  - J(0,n) = 0
  - Si n est premier alors
    - J(a,n) = 0 si n|a
    - J(a,n) = 1 si a est un résidu quadratique modulo n
    - J(a,n) = -1 si a n'est pas un résidu quadratique modulo n
  - Si n est un nombre composé alors $J(a,n)=J(a,p_1)*\ldots*J(a,p_n)$ où $p_1,\ldots,p_n$ est la décomposition en facteurs premier de n



Le symbole de Jacobi ne permet plus de tester si x est un résidu quadratique modulo n. En revanche, on peut toujours le calculer en utilisant la loi de réciprocité quadratique, valable pour tous entiers impairs premiers entre eux. L'intérêt du symbole de Jacobi consiste essentiellement en le test de primalité

## Symbole de Jacobi - calcul

1. J(1,n) = 1
2. J(a*b, n) = J(a, n)*J(b,n)
3. J(2,n) = 1 si $(n^2-1)/8$ est paire, -1 sinon
4. J(a,n) = J((a mod n),n)
5. $J(a, p_1*p_2) = J(a,p_1)*J(a,p_2)$
6. Si (a,b)=1 et a et b sont impairs
   a) J(a,b) = +J(b,a) si (a 1)(b 1)/4 est pair
   b) J(a,b) =- J(b,a) si (a 1)(b 1)/4 est impair



Si n est premier : il suffit de calculer a^{(n-1)/2} mod n et J(a,b)=L(a,b)

## Test de primalité Solovay-Strassen

- Etapes :
  - Choisir un nombre a < p et p est premier
  - Si (a,p) ≠ 1 → p échoue, il est composé
  - Calculer $j = a^{(p-1)/2} \bmod p$
  - Calculer J(a,p)
  - Si j ≠ J(a,p) → p n'est certainement pas premier
  - Si j = J(a,p) → la probabilité que p soit non premier est de maximum 50%
- a = témoin : répéter le test pour plusieurs témoins



Aussi le miller rabin

•D'après un théorème d'Euler, si n est premier, il satisfait au test de Solovay-Strassen pour tout entier a.

•S'il n'est pas premier, on prouve qu'il existe au moins un entier premier avec n sur deux pour lequel n ne satisfait pas le test.

•Si on effectue k tests successifs, avec des entiers a différents chaque fois choisis au hasard, la probabilité pour que n soit premier s'il satisfait à chacun des tests est de l'ordre de 1-1/2k.

•C'est en utilisant ce type de test qu'on fabrique les entiers premiers nécessaires dans les algorithmes de cryptographie comme le RSA.

## Questions

- Expliquer les résultats suivants :
  - Congruence et propriétés
  - Classe de résidus
  - Inverse modulaire
  - Algorithmes d'Euclide
  - Petit théorème de Fermat
  - Indicateur d'Euler, théorème d'Euler
  - Théorème du reste chinois
  - Symboles de Legendre, Jacobi
  - Tests de primalité



## Références

- http://mathworld.wolfram.com/topics/NumberTheory.html
- http://www.bibmath.net/dico/index.php3?action=rub&quoi=600
- [stinson] → ch1, ch4
- [stallings] → ch4, ch8
- [schneier] → ch11