Arithmétique modulaire pour la cryptographie

Pierre-Louis Cayrel

Université de Limoges, XLIM-DMI,
123, Av. Albert Thomas
87060 Limoges Cedex France
05.55.45.73.10
pierre-louis.cayrel@xlim.fr

Licence professionnelle Administrateur de Réseaux
et de Bases de Données
IUT Limoges

Sommaire

Les nombres premiers

Quelques pré-requis mathématiques

Arithmétique modulaire

Les nombres premiers suite et fin

Les nombres premiers

- Algo 2 : utilisable pour des nombres de 12 chiffres ou un peu plus

$\Rightarrow$ impossible de décomposer des nombres de 100 chiffres.

$\Rightarrow$ la multiplication est donc une fonction à sens unique (sous certaines conditions)

  - Si $n = pq$ (p et q grand), connaissant p et q il est facile de calculer n
  - **MAIS** connaissant n il est difficile de trouver p et q

Une infinité de nombres premiers

- **Théorème :**
  Le sous-ensemble constitué par les nombres premiers est infini.
- **Démonstration :** Supposons que cet ensemble soit fini :
  $E = \{p_1, ..., p_n\}.N = p_1 p_2 ... p_n + 1.N$ n'est divisible par aucun des p_i et n'est pas premier

$\Rightarrow$ contradiction

- Il y a une infinité de nombres premiers.

Quelques pré-requis mathématiques

Le pgcd

- **Définition :**
  Parmi l'ensemble des diviseurs communs à deux entiers a et b, le PGCD, est le plus grand commun diviseur.
- **Théorème :** a, b, c dans $\mathbb{N}$ et n dans $\mathbb{Z}$
  - $pgcd(ac, bc) = |c|.pgcd(a, b)$
  - $pgcd(a, b) = pgcd(a, b + na)$

Propriétés du pgcd

- **Propriétés :**
  - $pgcd(a; b) = pgcd(b; a)$
  - $pgcd(a; 1) = 1$
  - Soit $a_0 = a/pgcd(a; b)$ et $b_0 = b/pgcd(a; b)$.
    Alors $pgcd(a_0; b_0) = 1$.

Euclide

Quelques pré-requis mathématiques

Théorème d'Euclide

- Soit $a, b \in N / a \leq b$. Soit r le reste de la division euclidienne de a par b. Alors $pgcd(a, b) = pgcd(b, r)$.
- **Algorithme :**
  - Tq $b \neq 0 : (a, b) \rightarrow (b, a \mod b)$
  - si $b = 0$ renvoyer a
- **Exemple :** $pgcd(42, 30) = 6$

  $(42, 30) \rightarrow (30, 12)$
  $(30, 12) \rightarrow (12, 6)$
  $(12, 6) \rightarrow (6, 0)$

Calcul de pgcd

- Utilisation de l'algorithme d'Euclide pour déterminer $pgcd(a, b)$
  - $R_0 := |a|; R_1 := |b|; (b \neq 0)$
  - tant que $R_1 > 0$ faire
  - $R := ResteDivision(R_0; R_1); R_0 := R_1; R_1 := R;$
  - Le dernier reste non nul est le pgcd.
    Exemple : $a = 325, b = 145$
  - On a successivement
    $R_0 = a = 325; R_1 = b = 145$
    $R_0 = 2R_1 + 35 \Rightarrow R = 35; R_0 = 145; R_1 = R = 35;$
    $R_0 = 4R_1 + 5 \Rightarrow R = 5; R_0 = 35; R_1 = 5;$
    $R_0 = 7R_1 + 0; R_0 = 5; R_1 = 0.$
  - Donc $pgcd(325; 145) = 5.$

Nombres premiers entre eux

- **Définition :** lorsque $pgcd(a, b) = 1$, on dit que a et b sont premiers entre eux.
- Remarques :
  - cela signifie que leur seul diviseur commun est 1.
  - un nombre premier est premier avec n'importe quel autre nombre

Arithmétique modulaire

Congruence et modulo : arithmétique modulaire

- **Définition :** a est congru à b modulo n signifie :

  $\exists k \in \mathbb{Z} / a = k.n + b$

  $\equiv$ a et b ont le même reste dans la division par n

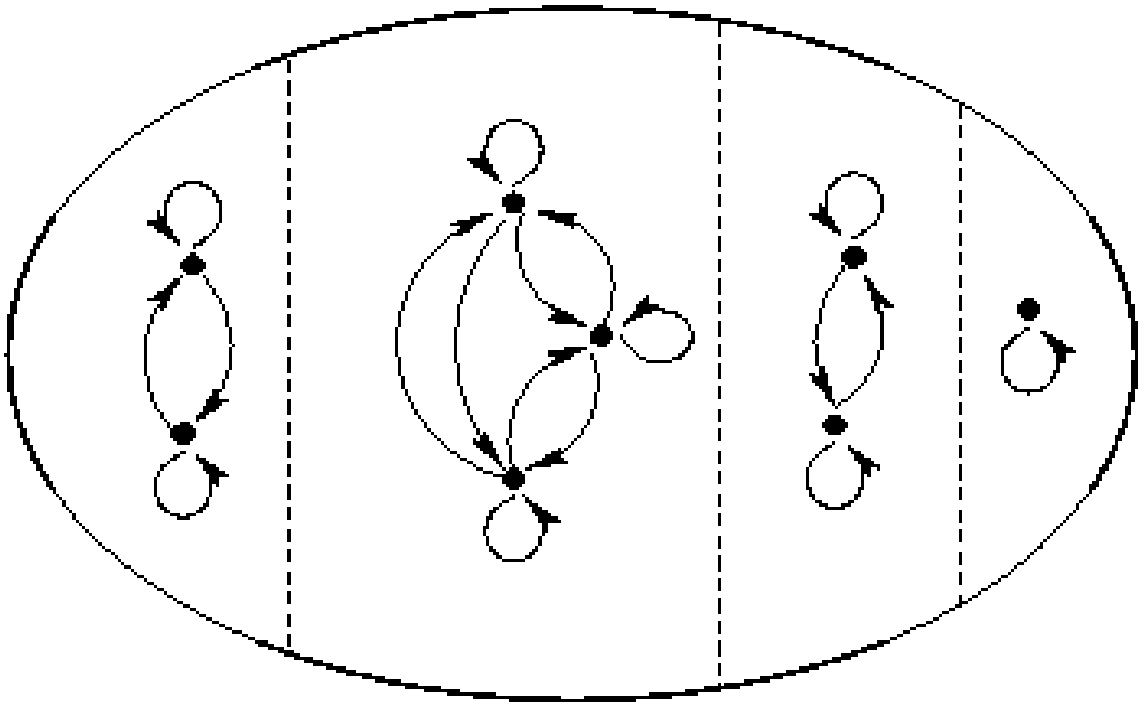
  Ne diffère que par un multiple de n.

  $a - b$ est un multiple de n.
- **Écriture :** $a = b \mod n$ ou $a = b[n]$

Classes d'équivalence

- **Définition :** On appelle classe modulo n d'un élément x de $\mathbb{N}$, l'ensemble des y qui sont congrus à x modulo n.
- **Remarques :**
  - $x = y \mod n$ ssi ils ont le même reste dans la division par n
  - les n restes possibles permettent de définir les n classes d'équivalence modulo n.
  - Ces n classes se notent $\mathbb{Z}/n\mathbb{Z}$
  - $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble quotient de $\mathbb{Z}$ par la congruence $\mod n$

Classe d'équivalence



Classes d'équivalence : addition

- L'addition sur $\mathbb{Z}/n\mathbb{Z}$ conserve ses propriétés classiques :
  - Commutativité : $x + y = y + x \mod n$
  - Associativité : $(x + y) + z = x + (y + z) \mod n$
  - Élément neutre : $0 + x = x + 0 = x \mod n$
  - Existence d'un opposé : $x - x = 0 \mod n$

  $\Rightarrow$ On dit que $\mathbb{Z}/n\mathbb{Z}$, est un groupe pour $+$

Addition $\mathbb{Z}/4\mathbb{Z}$

+	0·	1·	2·	3·
0·	0·	1·	2·	3·
1·	1·	2·	3·	0·
2·	2·	3·	0·	1·
3·	3·	0·	1·	2·

Classes d'équivalence : multiplication

- La multiplication conserve :
  - La commutativité
  - L'associativité
  - L'élément neutre 1
  - L'élément absorbant 0
  - La distributivité par rapport à l'addition
  - PAS L'EXISTENCE D'UN INVERSE

$\Rightarrow$ On dit que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif

Multiplication $\mathbb{Z}/4\mathbb{Z}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Multiplication $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$

Exercice :
Faire les tables de multiplication modulo 6 et modulo 7

Multiplication $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$

modulo 7

x	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

modulo 6

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Les diviseurs de zéro

- Pour que x possède une classe inverse, il faut et il suffit que $pgcd(x, n) = 1$. Cet inverse est unique et on le note x^{-1}.
- Si $pgcd(x, n) \neq 1$ alors il existe y tel que $x \times y = 0$. On dit que x est un **diviseur de zéro**.
- Si n est premier alors tout élément sauf 0 possède un inverse.

Etienne Bezout

Quelques pré-requis mathématiques (2)

Théorème de Bezout

- Soient $a, b \in \mathbb{Z}$ et $d = pgcd(a, b)$. Alors $\exists (u, v) \in \mathbb{Z}^2$ tels que $au + bv = d$

  Les entiers u et v sont appelés coefficients de Bezout.
- **Calcul pratique : Algorithme d'Euclide Etendu**
  - $(E_0) : 1 \times a + 0 \times b = a$
  - $(E_1) : 0 \times a + 1 \times b = b$
  - $(E_{i+1}) = (E_{i-1}) - q_i(E_i)u_i \times a + v_i \times b = r_i$

Application sur le calcul d'inverse modulaire

Exercice :
Calcul de $17^{-1} \mod 50$

Application sur le calcul d'inverse modulaire

- Calcul des coefficients de Bezout pour $a = 50$ et $b = 17$

$$E_0 : 1 \times 50 + 0 \times 17 = 50$$

$$E_1 : 0 \times 50 + 1 \times 17 = 17; q_1 = \frac{50}{17} = 2; r_1 = 50 \mod 17 = 16$$

$$E_2 : E_0 - 2 \times E_1; 1 \times 50 + (-2) \times 17 = 16; q_2 = \frac{17}{16} = 1; r_2 = 17 \mod 16 = 1$$

$$E_3 : E_1 - 1 \times E_2; (-1) \times 50 + 3 \times 17 = 1; q_3 = \frac{16}{1} = 16; r_3 = 16 \mod 1 = 0$$

- Bilan : $(-1) \times 50 + 3 \times 17 = 1 \Rightarrow 17^{-1} = 3 \mod 50$

Théorèmes (1/2) :

- **Théorème :**
  si $a = b \mod n$ et $u = v \mod n$ alors $a + u = b + v \mod n$ et $a \times u = b \times v \mod n$
- **Théorème :**
  Un entier a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi a et n sont premiers entre eux

Théorèmes (2/2) :

- **Théorème :**
  si p est premier alors tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible

  Notation : $\mathbb{Z}/p\mathbb{Z}^*$ désigne l'ensemble des éléments inversible de $\mathbb{Z}/p\mathbb{Z}$

  Remarque : si p est premier $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z}$ privé de 0.
- **Théorème :**
  un entier p est premier ssi $\mathbb{Z}/p\mathbb{Z}$ ne contient pas de diviseurs de 0

Résolution des équations sur les congruences

Supposons que l'on cherche à résoudre :

$$3x = 5 \mod 7$$

Cela est facile car le **modulo est premier** : On sait que $3^{-1} = 5 \mod 7$, on a donc $x = 5 \times 5 = 4 \mod 7$.

Quand le **modulo n'est pas premier** nous avons le théorème suivant :

- **Théorème :**
  Si a, b et m sont des entiers, et si $pgcd(a, m) = d$ alors :
  - Si d ne divise pas b, alors $ax = b \mod m$ n'a pas de solution
  - Sinon l'équation précédente a exactement d solutions.

Résolution des équations sur les congruences (2)

Cherchons à résoudre par exemple :

$$6x = 9 \mod 15 \Rightarrow 3(2x-3) = 0 \mod 15$$

On sait que 3 est un diviseur de zéro, donc :

$$3\times 0 = 0 \mod 15, \quad 3\times 5 = 0 \mod 15, \quad 3\times 10 = 0 \mod 15$$

Donc les solutions sont :

- $2x-3 = 0 \mod 15$ d'où $x = 9 \mod 15$,
- $2x-3 = 5 \mod 15$ d'où $x = 4 \mod 15$,
- $2x-3 = 10 \mod 15$ d'où $x = 14 \mod 15$.

Fonction indicatrice d'Euler

- Elle est notée f ou ϕ
- **Définition :** $\phi(n)$ est égale au nombre d'entiers entre 0 et $n-1$ premiers avec n.
- $\phi(n)$ correspond aussi au nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
- Par convention, $\phi(0) = 0$ et $\phi(1) = 1$

Théorèmes (1/3) :

- **Théorème :**
  Un entier p est premier ssi $\phi(p) = p - 1$
- **Théorème :**
  Si n et m sont entiers strictement positifs et premiers entre eux alors $\phi(n \times m) = \phi(n) \times \phi(m)$
- **Théorème :**
  Si p est premier et $n = p^k$ alors $\phi(n) = p^k(1 - 1/p) = p^k - p^{k-1}$

Théorèmes (2/3) :

- **Théorème :**
  Si n se décompose en produit de facteurs premiers $p_1 \times p_2 \times ... \times p_r$ alors
  $$\phi(n) = n \times (1 - \frac{1}{p_1}) \times (1 - \frac{1}{p_2}) \times ... \times (1 - \frac{1}{p_r})$$
- **Théorème :**
  tout $n > 0$ peut s'écrire $\phi(n) = \sum_{d|n} \phi(d)$
- **Théorème :**
  Si n et a sont deux entiers strictement positifs et premiers entre eux alors $a^{\phi(n)} = 1 \mod n$

Pierre de Fermat

Théorèmes (3/3) :

- **Petit théorème de Fermat :** Si p est premier et ne divise pas a (p et a premiers entre eux) alors $a^{p-1} = 1 \mod p$
- **Généralisation :** Si n et a sont deux entiers strictement positifs et premiers entre eux, alors

$$\exists k > 0 / a^k = 1 \mod n$$

et le plus petit k vérifiant cette propriété divise $\phi(n)$.

Élément générateur

- **Théorème :**
  Soit p un nombre premier. Alors, le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique. C'est-à dire que ce groupe peut être engendré par un élément générateur (dit aussi élément primitif) : il existe un élément α tel que
  $$\mathbb{Z}/p\mathbb{Z}^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{p-2}\}.$$
- **Théorème :**
  Le nombre de générateurs de $\mathbb{Z}/p\mathbb{Z}^*$ est égal à $\phi(p-1)$ où ϕ est la fonction indicatrice d'Euler.

Exponentielle et logarithme modulaire

- **Définition :** La fonction exponentielle de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est définie par $x \longrightarrow a^x \mod n$.
- **Définition :** Calculer le logarithme en base a, c'est, étant donné $A = a^x \mod n$, déterminer x dans $\mathbb{Z}/n\mathbb{Z}$
- Ce calcul n'est possible que si $x \longrightarrow a^x \mod n$ est une bijection

Calcul de la puissance modulaire

- $10^{7} = 130 \mod 257$
- $10^{15} = 130 \times 130 \times 10 = 151 \mod 257$
- $10^{31} = 151 \times 151 \times 10 = 51 \mod 257$
- $10^{62} = 51 \times 51 = 31 \mod 257$
- $10^{124} = 31 \times 3 = 190 \mod 257$
- $10^{249} = 190 \times 190 \times 10 = 172 \mod 257$
- $10^{499} = 172 \times 172 \times 10 = 33 \mod 257$
- $10^{999} = 33 \times 33 \times 10 = 96 \mod 257$

Le théorème des restes chinois

- Soit $m_1, m_2, \ldots, m_r$ une suite d'entiers positifs premiers entre eux deux à deux. Alors le système de congruences :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

a une solution unique $x \mod M = m_1 \times m_2 \times \ldots \times m_r$:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r$$

avec

$$M_i = M/m_i \quad y_i M_i = 1 \mod m_i$$

Le théorème des restes chinois : un exemple

Cherchons à résoudre le système de congruences suivant :

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

On pose $M = 3 \times 5 \times 7 = 105$

$$\begin{array}{lll} M_1 = 105/3 = 35 & y_1 \times 35 \equiv 1 \pmod 3 & y_1 = 2 \\ M_2 = 105/5 = 21 & y_2 \times 21 \equiv 1 \pmod 5 & y_2 = 1 \\ M_3 = 105/7 = 15 & y_3 \times 15 \equiv 1 \pmod 7 & y_3 = 1 \end{array}$$

$$x \equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \equiv 157 \equiv 52 \pmod{105}$$

Le théorème des restes chinois : un exemple (2)

Quand les modulos ne sont pas premiers entre eux

$$\begin{cases} x \equiv 1 \pmod 6 \\ x \equiv 4 \pmod{15} \end{cases} \iff \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5 \end{cases}$$

$$x \equiv 1 \pmod 6 \iff \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \end{cases}$$

$$x \equiv 4 \pmod{15} \iff \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5 \end{cases}$$

Racines primitives

- **Définition :** soit n un entier et $\phi(n)$ l'indicateur d'Euler. On appelle racine primitive de n un nombre a avec $1 < a < n$ tel que :
  - a est premier avec n
  - $a^d \neq 1, \forall d / 0 < d < \phi(n)$
- En particulier, si n est un nombre premier et $1 < a < n$, a est une racine primitive de n si

$$a^d \neq 1, \forall d / 0 < d < n - 1$$

Ordre et racines primitives :

- **Définition :**
  Soit p un nombre premier. On appelle ordre d'un nombre a de $\mathbb{Z}/p\mathbb{Z}$, la plus petite valeur $k/a^k = 1 \mod p$.
- Une racine primitive est donc un élément a d'ordre maximal $p-1$, i.e. $a^{p-1} = 1 \mod p$.

Exponentiation rapide modulaire : calcul de $a^e \mod n$

- Basé sur la remarque suivante :
  - si e est pair, $a^e = (a^{e/2})^2$
  - si e est impair $a^e = (a^{e/2})^2 \times a$
- Algorithme d'exponentiation rapide modulaire
  1. Décomposer e en binaire : $e = \sum_{i=0}^{k} e_i 2^i$
  2. Calcul de $\{a^{2^i} \mod n\}_{0 \leq i \leq k}$
     - Utiliser la relation : $a^{2^{i+1}} = (a^{2^i})^2 \mod n$
  3. En déduire $a^e = \Pi_{i=0}^{k} (a^{2^i})^{e_i}$

Exponentiation rapide modulaire

Exercice :
Calcul de $51447^{21} \mod 17$ (E)

Exponentiation rapide modulaire

$51447 = 3026 \times 17 + 5$ donc $(E) \equiv 5^{21} \mod 17$

1. Décomposition de 21 en binaire : $21 = 2^4 + 2^2 + 2^0$
2. Calcul de $\{5^{2^i} \mod 17\}_{0 \leq i \leq 4}$
   - $i = 0 : 5^{2^0} = 5 \mod 17$
   - $i = 1 : 5^{2^1} = 5^2 = 25 = 8 \mod 17$
   - $i = 2 : 5^{2^2} = 8^2 = 64 = 13 = -4 \mod 17$
   - $i = 3 : 5^{2^3} = (-4)^2 = 16 = -1 \mod 17$
   - $i = 4 : 5^{2^4} = (-1)^2 = 1 \mod 17$
3. On en déduit : $5^{21} = 5^{2^4} \times 5^{2^2} \times 5^{2^0} = 1 \times (-4) \times 5 = -20 = 14 \mod 17$