# ARITHMÉTIQUE MODULAIRE EN LANGAGE C SOUS LINUX

*DRAFT: 2013-14-15*

PHILIPPE LANGEVIN

Résumé. Dans ce cours, nous détaillons quelques points de l'algèbre et de la théorie des nombres en liaison avec la construction d'une clé pour le cryptosystème RSA : un système de chiffrement à clef publique fort célèbre. Une occasion d'implanter, en langage C, quelques algorithmes fondamentaux de l'arithmétique, et par là même, faire connaissance avec la bibliothèque multiprécision `gmp` et quelques fonctionnalités de la commande `openssl`.

## Table des matières



*Date*: 25 octobre 2017.

mlc.tex 2017−10−25 09:50:52.582633241 +0200
macros.tex 2015−11−06 12:45:17.302164363 +0100

Nous éviterons de parler du plus étrange des nombres premiers ! Sauf mention contraire, dans cette note, $p$ et $q$ désignent des nombres premiers impairs et $n$ un nombre composé impair.

Indeed, two is the oddest prime !

## 1. Fondation

L'arithmétique est une discipline fondamentale initiée par les mathématiciens grecs : Pythagore, Euclide, Diophante. En passant, le mot grec *mathêmas* signifie sciences et *arithmos* désigne un nombre. Les recherche en arithmétique ont pour objectif de comprendre les *propriétés cachées* des nombres entiers. La résolution d'une enigme diophantienne peut prendre un certain temps, voire un temps certain, rappelons par exemple que la résolution du grand théorème de Fermat s'appuie sur des travaux qui s'étalent sur plusieurs siècles. Le lecteur peut rechercher sur internet le documentaire réalisé par Simon Singh produit par la BBC dans la série horizons. Dans l'apologie d'un mathématicien 1940, Hardy déclare :

*... both Gauss and lesser mathematicians may be justified in rejoicing that there is one science (number theory) at any rate, and that their own, whose remoteness from ordinary human activities should keep it gentle and clean.*

Il encore souhaitable de penser comme le mathématicien Hardy mais un progrès considérable dans le domaine de la cryptographie rélalisé au milieu des années 70 va bouleverser le statut de la reine des mathématiques. En 1976, Diffie et Hellman décrivent un procédé pour transmettre une clé secrète. Il est fondé sur l'exponentiation modulaire qui, deux ans plus tard, permet à Rivest, Shamir et Adelman de proposer le premier système de chiffrement à clefs publiques, ces propositions s'appuient fortement sur la théorie des nombres.

## 2. cryptographie

On peut distinguer quatre genre de cryptographie : la cryptographie à clef secrète à flot ou par blocs, la cryptographie à clefs publiques dont il est fortement question dans ce cours, la cryptographie de propriétaire qui ne fonctionne jamais, et une

cryptographie physique qui devrait faire parler d'elle dans un futur plus ou moins proche.

Soient $X$ un espace de clairs, $K$ un ensemble de clés. Convenons d'appeler *algorithme cryptographique* la donnée de deux paramétrisations d'un ensemble de permutations des clairs par un ensemble de clés. La paramétrisation de chiffrement $E\colon X \times K \to X$, et celle de déchiffrement $D\colon X \times K \to X$, en pratique $E = D$, telles que pour toute clé $k \in K$, il existe une clé $k'$ vérifiant :

$$\forall k \in K, \quad \exists k' \quad , \forall x \in X, \qquad D(E(x,k),k') = x.$$

Le système est dit asymétrique quand $k' \neq k$ en général, et symétrique dans le cas $k' = k$. Un algorithme de chiffrement doit être efficace du point de vue calculatoire. Le système doit être prouvé robuste : la seule connaissance de quelques cryptogrammes $E(x_i, k)$ ne doit pas suffire pour retrouver un des clairs $x_i$, et encore moins la clée utilisée, sans un effort calculatoire passant par moins de $2^{80}$ étapes.

**Exercice 1.** *Une idée ?*

## 3. Outils pour permuter ?

Bijections are where it's at—Herb Wilf

D'aprés Pythagore, tout est nombre, et la cryptographie c'est l'art de permuter les nombres avec efficacité et robustesse. Il y a $n^n$ applications d'un ensemble à $n$ éléments dans lui-même, et $n!$ sont des permutations. Rappelons, la formule d'équivalence de Stirling qui relie de façon surprenante le nombre de bijections d'un ensemble à $n$ éléments à deux des nombres transcendants connus de tous, $\pi$ et $e$ :

$$n! \sim \sqrt{2\pi n} n^n e^{-n}$$

**Exercice 2.** *D'aprés certains physiciens, on peut estimer à $2^{256}$ le nombre de particules dans l'univers. Quel est le plus petit entier $n$ tel que $n! > 2^{256}$ ?*

Mézalor, comment décrire une permutation dans la jungle des applications ? L'algèbre s'est rapidement imposée comme un moyen approprié pour décrire des permutations sur un ensemble fini à partir de lois internes qui vérifient des règles analogues aux lois additions et multiplications sur les nombres, et qui nous sont familières : associativité, distributivité, etc...

## 4. Structure algébrique

Une structure algébrique est un ensemble muni de lois vérifiant des contraintes plus ou moins fortes. Une loi interne $\star$ sur un ensemble $E$ est une application de $E \times E$ dans $E$ qui envoie le couple $(x, y)$ sur $x \star y$. Sur un ensemble $E$ de cardinal $n$, il existe autant de lois internes que de tableaux $n \times n$ à valeurs dans $E$, et donc, il est possible de former $n^{n^2}$ lois internes mais trés peu d'entre elles possèdent un réel intérêt. On dit que la loi est associative quand on peut associer les termes dans n'importe quel ordre sans changer le résultat :

$$\forall x, y, z \in E \quad (x \star y) \star z = x \star (y \star z)$$

Un ensemble muni d'une loi interne sans condition est un magma. Une structure de semi-groupe $(E, \star)$ est magma dont la loi associative.

**Travaux-pratiques 1.** *Ecrire un programme pour compter le nombre de structure de semi-groupes à n éléments, pour n relativement petit : 1, 2, 3, 4. Puis utiliser l'encyclopédie Online Integer Sequence de Sloane pour retrouver de l'information sur le sujet.*

Un morphisme de la structure $(E, \star)$ vers la structure $(F, *)$ est une application $f\colon E \to F$ qui conserve les opérations

$$\forall x, y \in E \quad f(x \star y) = f(x) * f(y).$$

Dans ce contexte, il convient d'introduire la notion d'anti-morphisme. On dit que $f$ est un monomorphisme, un epimorphisme, un isomorphisme suivant que $f$ est une injection, une surjection ou une bijection. On dit que deux structures sont isomorphes quand il existe une isomorphisme de l'une sur l'autre, on doit alors s'intéresser aux classes s'isomorphies.

**Travaux-pratiques 2.** *Ecrire un programme pour compter le nombre de classes de semi-groupies à n éléments. Il y a 3192 semi-groupes à 4 éléments et 126 classes à anti-isomorphismes prés.*

L'ensemble des applications de $E$ dans $E$ muni de la composition des applications est un exemple de monoide. On remarque que l'application identique est un neutre, que les bijections sont précisément les éléments inversibles. L'ensemble des bijections de $E$ dans $E$ muni de la composition des applications forme une structure de groupe généralement noté $(S(E), \circ)$ et que ce groupe n'est pas commutatif dès que le cardinal de $E$ est supérieur à 2.

## 5. Ordre et Groupe

Un groupe $(G, *)$ est ensemble $G$ sur lequel opère une loi interne : associative, possèdant un neutre $1_G$, tout élément de $G$ est inversible. Le groupe est dit abélien quand la loi est commutative.

**Exercice 3.** *Dans un groupe $G$, il y a unicité du neutre et des inverses. Tout élément est simplifiable*

$$\forall x, y, z \in G, \quad x * y = x * z \Longrightarrow y = z.$$

*En particulier, pour tout $t \in G$, l'application $x \mapsto tx$ est une permutation de $G$.*

Précisons qu'un groupe peut-être présenté comme ci-dessus par une loi multiplicave, ou bien par une loi additive. Dans le second cas, le neutre est noté $0_G$ et les inverses sont des opposés. On définit l'ordre de $x$ comme étant le plus petit entier non nul $n$ tel que $x^n = 1_G$. On remarque sur le champ que si $x^m = 1_G$ pour un autre entier $m$ alors $n$ divise $m$.

**Proposition 1.** *Dans un groupe abélien fini, l'ordre d'un élément divise le cardinal du groupe.*

*Démonstration.* En effet, notons $n$ l'ordre de $G$ :

$$\prod_{y \in G} y = \prod_{y \in G} (x * y) = x^n \prod_{y \in G} y.$$

Aprés simplification, $x^n = 1_G$. □

**Exercice 4.** *Déterminer les ordres des éléments du groupe $S(3)$.*

Une partie non vide $H \subset G$ stable par la loi de $G$ est un sous-groupe. La Propositioni 2 est en fait un cas particulier du théorème de Lagrange.

**Théorème 1** (Lagrange)**.** *Dans un groupe fini, le cardinal d'un sous-groupe divise le cardinal du groupe.*

*Démonstration.* Si $S$ est un sous groupe de $G$ alors les ensembles $t + S$ obtenus en faisant varier $t$ dans $G$ sont deux à deux égaux ou disjoints. □

**Exercice 5.** *La neutralité est préservée par morphisme. Généralisation aux sous-groupes.*

## 6. Anneau et corps

Une structure d'anneau $(A, +, \times)$ est la donnée d'un ensemble $A$ qui est muni de deux lois internes, une addition pour laquelle $(A, +)$ est un groupe et une multiplication vérifiant les axiomes :

(1) associativité

(2) existence d'un neutre $1_A$

(3) distributivité de la multiplication sur l'addition.

On pourra remarquer que :

**Exercice 6.** *Dans un anneau, les neutres sont uniques, le neutre additif est absorbant et que le groupe $(A, +)$ est nécessairement abélien !*

Quand la multiplication est commutative, l'anneau est dit commutatif. Quand tous les éléments non-nuls sont inversibles l'anneau est un corps. Un célèbre théorème de Wedderburn (1905) affirme qu'un corps avec un nombre fini d'élément est forcément commutatif, pour simplifier notre propos, nous admettrons ce résultat somme toute assez étonnant ! ! Le plus petit des anneaux contenant deux éléments distincts 0 et 1 est $\mathbb{F}_2$ le corps à deux éléments, il s'obtient en imposant la formidable relation :

$$1 + 1 = 0.$$

**Exercice 7.** *Un pre-semicorps est un ensemble fini $\mathfrak{S}$ de deux lois internes, une multiplication distributive à gauche et à droite sur une addition formant un groupe. La multiplication n'est pas nécessairement associative. On suppose que pour tout $t \in \mathfrak{S}$, la multiplication par $t$ est une bijection. Comme dans le cas d'un anneau, le groupe additif est abélien (commutatif). Prouvez le !*

## 7. Inversible et diviseur de zéro

Un élément $t$ est un *inversible* à droite quand il existe un élément non nul $t'$ tel que $tt' = 1$. Un élément $z$ est un *diviseur de zéro* à à droite quand il existe un élément non nul $r$ tel que $zr = 0$. Idem à gauche.

**Lemme 1.** *Dans un anneau fini, soit un élément est inversible soit c'est diviseur de zéro.*

*Démonstration.* Soit $y$ un élément de $A$. On considère la multiplication par $y$ : $x \mapsto xy$. Si cette application de $A$ dans lui-même est surjective alors $y$ est inversible sinon c'est un diviseur de zéro à gauche et donc à droite. □

On remarque que si $t$ est inversible à gauche alors il est inversible à droite, que les inverses à gauche et à droite sont identiques. Par ailleurs, si $x$ et $y$ sont inversibles d'inverse $x'$ et $y'$ alors $xy$ est inversible d'inverse $y'x'$. Les éléments inversibles de $A$ forment un groupe noté $A^\star$ : le groupe des inversibles de $A$.

**Exercice 8** (Ganesan)**.** *Soit $A$ un anneau avec $n \geq 2$ diviseurs de zéros. Montrer que $A$ est fini et d'ordre inférieur à $(n+1)^2$.*

## 8. Arithmétique modulaire

Nous notons $\mathbb{Z}/(n)$ l'anneau des résidus modulo $n$ i.e. l'ensemble des restes possibles 0,1,..., $n-1$ d'une division d'un entier par $n$, muni de deux lois internes

$$x \oplus y := [x+y]_n, \quad x \otimes y = \quad [x \times y]_n.$$

où $[t]_n$ est une autre notation pour désigner le reste de la division de $t$ par $n$. On montre que l'obtient un anneau en s'appuyant sur la notion de congruence. Deux entiers relatifs sont congruents modulo $n$ si $n$ divise la différence $y - x$.

$$y \equiv x \mod n \quad \Leftrightarrow \quad \exists k, y - x = kn.$$

La relation de congruence est une relation d'équivalence compatible avec les lois d'addition et de multiplication. Comme par ailleurs deux résidus congrus sont identiques il vient que $\mathbb{Z}/(n)$ est bien un anneau.

Comme dans tout anneau fini, un élément de $\mathbb{Z}/(n)$ est soit un diviseur de zéro, soit un élément inversible. Plus précisément, $x$ est inversible si et seulement si $x$ est premier avec $n$. Si $x$ est inversible modulo $n$ alors il existe $u$ tel que

$$xu \equiv 1 \pmod{n}$$

Par définition, il existe $v$ tel que $xu = 1 + nv$ i.e. une relation de Bâchet-Bézout. Réciproquement, si $x$ et $n$ sont premiers entre eux, l'algorithme d'Euclide étendu fournit une paire d'entiers $(u, v)$ tel que :

$$xu + nv = (x, n) = 1.$$

Ainsi, $x$ est inversible, son inverse modulo $n$ est le résidu congru à $u$.

**Proposition 2.** *L'anneau $\mathbb{Z}/(n)$ est un corps si et seulement si $n$ est premier.*

Nous verrons par la suite que ce fait d'apparence banale contient quelques propriétées cachées ! En général, pour $p$ premier, le corps à $p$ éléments est noté $\mathbb{F}_p$.

Du point de vue additif, les inversibles sont précisément les éléments d'ordre $n$. L'usage est de noter $\varphi(n)$ le nombre d'éléments inversibles modulo $n$.

$$n = \sum_{d|n} \varphi(d). \tag{1}$$

**Travaux-pratiques 3.** *Analyser le temps de calcul d'une multiplication modulaire implanter avec `gmp` en fonction de la taille du module. On pourra faire une comparaison avec un langage comme `python`, ou encore `bc`.*

**Exercice 9** (Wilson)**.** *Montrer que l'entier $n$ est premier si et seulement si*

$$(n-1)! = -1 \pmod{n}.$$

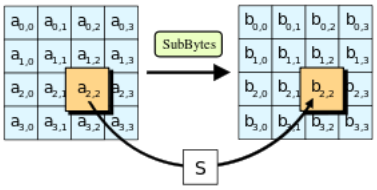



FIGURE 1. La brique de substitution de l'AES opére sur le corps à 256 éléments en envoyant un élément non nul sur son inverse multiplicatif.

## 9. ANALOGIE

Considérons $\mathbb{F}_2[X]$ l'ensemble des polynômes à coefficients dans le corps à deux éléments. Il s'agit d'un anneau infini muni d'une addition et d'une multiplication définies comme usuellement. Les anneaux $\mathbb{F}_2[X]$ et $\mathbb{Z}$ possèdent de profondes analogies arithmétiques. En effet, on commence par dire que le polynôme $B$ divise le polyôme $A$ s'il existe un troisième $Q$ tel que $A = BQ$. On utilise la notion de degré pour définir celle d'irréductibilité qui est l'analogue de la primalité. Un polynôme $A$ de degré positif est dit irréductible quand

$$A = BC \Longrightarrow \deg B \deg C = 0$$

Dans ce contexte, il existe une division euclidienne fondée sur le degré. Si $B$ désigne un polynôme non nul alors pour tout polynôme $A$, il existe une unique paire de polynômes $(Q, R)$, quotient et reste, tel que :

$$A = BQ + R, \qquad \text{avec} \quad R = 0, \quad \text{ou} \quad \deg R < \deg B. \tag{2}$$

**Proposition 3.** *Tout polynôme se décompose de manière essentiellement unique en un produit de polynômes irréductibles.*

On peut alors choisir un polynôme $M(T) \neq 0$ de degré $f$, l'ensemble des $2^f$ restes possibles d'une division par $M$ muni des lois internes

$$A \oplus A' := (A + A') \pmod M, \quad A \otimes A' := (A \times A') \pmod M,$$

est un anneau, noté $\mathbb{F}_2[T]/M(T)$.

**Exercice 10.** *Construire les tables des 4 anneaux modulaires pour les polynômes de degré 2. Déterminer les classes d'isomorphimes.*

**Proposition 4.** *Si $M$ est irréductible alors l'anneau des polynômes modulo $M$ est un corps à $2^f$ éléments, c'est le corps de Galois* $\mathrm{GF}(2, f)$ *(Galois Field).*

**Exercice 11.** *Vérifier que tout ce qui vient d'être dit s'applique aux corps $\mathbb{F}_p$, $p$ premier impair.*

Les auteurs du Rinjael (Advanced Encryption Standard) décrivent le système de chiffrement par blocs en utilisant un corps de Galois à 256 éléments.

**Exercice 12.** *Parcourir la spécification officielle fips-197, pour trouver le polynôme de degré 8 utilisé pour définir le corps à 256 éléments.*

## 10. Invariant et caractéristique

Un morphisme d'un anneau $(A, +, \times)$ dans un anneau $(B, \oplus, \otimes)$ est une application de $A$ dans $B$ qui envoie $1_A$ sur $1_B$ et qui transporte les lois :

$$\forall x, y \in A, \quad f(x \times y) = f(x) \otimes f(y) \quad f(x + y) = f(x) \oplus f(y)$$

**Exercice 13.** *Montrer qu'il existe une seule classe d'isomorphie d'anneau à trois éléments.*

Deux anneaux $A$ et $B$ sont isomorphes ($A \sim B$) s'il existe un isomorphisme de $A$ sur $B$. Un invariant est une foncion $\mathfrak{J}$ définie sur l'ensemble des anneaux tel que :

$$A \sim B \Longrightarrow \mathfrak{J}(A) = \mathfrak{J}(B)$$

L'ordre additif de l'unité est un invariant appelé caractéristique de l'anneau. Si la caractéristique de $A$ est égale à $m$ alors $m$ divise le cardinal de l'anneau et

$$\mathbb{Z}/(m) \ni k \mapsto k1_A = \underbrace{1_A + 1_A + \cdots + 1_A}_{k \text{ termes}} \in A$$

définit un monomorphisme de $\mathbb{Z}/(m)$ dans $A$. En particulier, le cardinal de $A$ est égal à la caractéristique de $A$ si et seulement si il est isomorphe à $\mathbb{Z}/(m)$.

Le nombre d'éléments inversibles, l'ordre du groupe multiplicatif, le nombre de diviseurs de zéro, la distribution des ordres sont des invariants.

## 11. Zoologie

On considère l'anneau des matrices carrées à coefficients dans le corps à 2 éléments.

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \times \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} = \begin{bmatrix} a\alpha + c\beta & a\gamma + c\delta \\ b\alpha + d\beta & b\gamma + d\delta \end{bmatrix}$$

(1) Quel est le cardinal de cet anneau ?
(2) L'anneau est-il commutatif ?
(3) Caractériser les matrices inversibles.
(4) Quels sont les diviseurs de zéros ?
(5) Quels sont les éléments inversibles ?
(6) Le groupe des inversibles est isomorphe à un groupe de permutation. Lequel ?
(7) Quelle est la nature de l'anneau engendré par la matrice $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ ?
(8) Quelle est la nature de l'anneau engendré par la matrice $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ ?

**Proposition 5.** *A isomorphisme prés, il y a quatre structures d'anneaux commutatifs à quatre éléments : le corps $\mathbb{F}_4$, l'anneau modulaire $\mathbb{Z}/(4)$, le produit $\mathbb{F}_2 \times \mathbb{F}_2$ et l'anneau $\mathbb{F}_2[T]/(T^2)$.*

On commence par montrer qu'un anneau à quatre éléments est forcément commutatif. En effet, les 4 éléments sont 0, 1, $x$ et $y$. On vérifie que $y = x + 1$ aprés quoi

$$xy = x(x + 1) = x^2 + x = (x + 1)x = yx$$

Il y a une seule classe d'anneau de caractéristique 4. Les classes d'anneaux de caractéristique 2 sont caractérisée par l'ordre maximal d'un élément inversible : 1 ($\mathbb{F}_2 \times \mathbb{F}_2$), 2 ($\mathbb{F}_2[T]/(T^2)$) ou 3 ($\mathbb{F}_4$).

## 12. Morphisme, cyclicité

Un morphisme $f$ d'une structure albégrique $(X, \circ)$ vers une structure $(Y, \star)$ est une application de $X$ vers $Y$ qui conserve les opérateurs :

$$\forall x, x' \in X, \quad f(x \circ x') = f(x) \star f(x').$$

On définit de ainsi des morphismes de groupes, et de façon similaire, des morphismes d'anneaux, de corps etc.... Un isomorphisme est un morphisme bijectif.

Vous pouvez vous convaincre rapidement que l'application qui suit un isomorphisme remarquable entre le groupe $\mathbb{Z}/4\mathbb{Z}$ et, $\mathbb{Z}/(5)^*$, le groupe des inversibles modulo 5.

$$f\colon 0 \mapsto 1, \quad 1 \mapsto 3, \quad 2 \mapsto 4, \quad 3 \mapsto 2.$$

On a par exemple,

$$f(2+3) = f(1) = 3 = 4 \times 2 = f(2) \times f(3).$$

Il nous faut avancer davantage dans notre exposé pour comprendre la finesse du petit exemple ci-dessus.

On constate que la suite : 1, $1+1$, $1+1+1$, ...etc décrit tous les résidus modulo $n$. On dit que le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique et que 1 est un générateur de ce groupe. Pour $n$ fixé, tous les groupes cycliques d'ordre $n$ sont isomorphes, et, $\varphi(n)$ est aussi le nombre de générateurs du groupe cyclique à $n$ éléments. En effet, $t$ est un générateur du groupe $\mathbb{Z}/n\mathbb{Z}$ si et seulement si la multiplication par $t$ est surjective.

## 13. Exponentiation modulaire

Soit $\gamma$ un élément inversible modulo $n$. L'exponentiation modulaire de base $\gamma$ transforme l'entier $x$

$$x \mapsto \gamma^x \mod n.$$

Quelques primitives cryptographiques célèbres reposent sur l'existence d'un algorithme efficace pour caculer les exponentielles modulaires.

Le temps de calcul d'un produit modulo $n$ est quadratique en $\log n$. L'algorithme d'exponentiation modulaire permet de caculer une $x^t$ modulo $n$ en $\mathrm{O}\big((\log n)^3\big)$.

L'exponentiation modulaire est un atout d'efficacité mais c'est aussi un point faible comme nous allons le montrer tout à l'heure !

```
expmod( x, t, n : nombre )
var r : nombre = 1
debut
tantque ( t > 0 )
   si impair( t ) alors
        r := prod( r, x , n)
   fsi
   x := prd(x, x, n )
   t := t div 2
ftq
retourner r
fin
```

**Exercice 14.** *Soit $n$ un entier de 512-bits. Une implantation de l'exponentiation modulaire calcule $x^t \pmod n$ en 1ms. Estimer le temps de calcul pour un module de taille deux fois plus grande.*

**Travaux-pratiques 4.** *Analyser le temps de calcul de l'exponentiation modulaire de gmp.*

```
if ! factor $1 | grep -qEc ":[[:space:]]+$1" ; then
   echo not prime
   exit
fi
bc << INPUT
p=$1
r=1;
x=2;
while ( x!=1 ) { x=(2*x) %p ; r=r+1; };
print r;
INPUT
echo
# usage> ./order.sh 83
# 82
```

FIGURE 2. Un script shell basé sur `bc` pour calculer l'ordre de 2 modulo un premier passé en argument sur la ligne de commande.

## 14. Petit théorème de Fermat

**Théorème 2** (Fermat)**.** *Si $p$ est premier alors*

$$\forall x \in \mathbb{F}_p, \quad x^p = x, \quad x^{p-1} = \begin{cases} 1, & x \neq 0; \\ 0, & x = 0. \end{cases}$$

Les démonstrations de ce théorème font légion : combinatoire, Fermat, Lagrange...

**Exercice 15.** *Pour $p$ premier, vérifier que le nombre de parties à $k$ éléments dans un ensemble à $p$ éléments satisfait à $C_p^k = 1$ si et seulement si $k = 0$ ou $k = p$. En déduire le petit théorème de Fermat.*

Si $x$ est un résidu non nul l'application $k \mapsto kx$ est une permutation des inversibles et donc

$$(p-1)! = 1.2.\ldots.(p-1) = \prod_{k\neq 0} k = \prod_{k\neq 0} (kx) = x^{p-1}.(p-1)!$$

Il ne reste plus qu'à simplifier par $(p-1)!$ alias $-1$ pour terminer la preuve de Fermat.

## 15. Groupe multiplicatif

On note $K$ un corps fini de cardinal $q$. L'ensemble des éléments non nuls forme un groupe, noté $K^\star$, c'est le groupe multiplicatif de $K$.

Pour tout élément de $K$, il existe un entier positif $r$ tel que $x^r = 1$. Le plus petit d'entre-eux est appelé l'ordre de $x$.

**Lemme 2.** *Si $f$ est l'ordre de $x$, et si $x^t = 1$ alors $f$ divise $t$.*

*Démonstration.* Utiliser la division de $n$ par $f$. □

**Théorème 3** (Lagrange)**.** *Dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe.*

*Démonstration.* Faisons la démonstration dans le cas d'un groupe commutatif fini d'ordre $n$. Considérons un élément $x$ du groupe et $y_1, y_2, \ldots, y_n$ une énumération des éléments de $G$. L'application $y \mapsto yx$ est une permutation de $G$ et donc :

$$\prod_{i=1}^{n} y_i = \prod_{i=1}^{n} (y_i x) = (\prod_{i=1}^{n} y_i) \times x^n.$$

Il suffit alors de simplifier par le produit des $y_i$. □

**Exercice 16.** *Faire une démonstration dans le cas d'un groupe non commutatif.*

On peut montrer par induction que, dans un corps commutatif, un polynôme de degré $n$ possède au plus $n$ racine. Pour tout diviseur $d$ de $q-1$, le nombre d'éléments d'ordre $d$ dans $K^\star$ est majoré par $d$. Convenons de noter $\kappa(d)$ le nombre d'éléments d'ordre exactement égal à $d$ :

$$q - 1 = \sum_{d|q-1} \kappa(d), \quad \kappa(d) \leq \varphi(d).$$

**Théorème 4.** *Dans un corps fini d'ordre $q$, il existe un élément d'ordre $q-1$.*

*Démonstration.* Il suffit de rapprocher l'égalité précédente avec [1]. □

Les éléments d'ordre $q-1$ sont des *racines primitives* du corps. Il en existe $\varphi(q-1)$, si $\gamma$ est l'une d'entre-elles, les autres sont $\gamma^t$ avec $(t, q-1) = 1$. Par exemple, dans un corps à 11 éléments, il existe $\varphi(10) = 4$ racines primitives.

**Exercice 17.** *Un nompre premier de Sophie Germain est un nombre premier $s$ tel que $p := 2s + 1$ soit un nompre premier. On dit alors que $p$ est un premier sûr. Montrer que qu'un élément $x$ est d'ordre multiplicatif $p-1$ si et seulement si $x \not\equiv \pm 1$ et $x^s \neq 1 \pmod p$, et dans ce cas, que vaut $x^s$ ? Quelle est la probabilité qu'un résidu $x \in \mathbb{F}_p{}^\star$ soit d'ordre $p-1$ ?*

## 16. Logarithme discret

On suppose que $p$ est un premier impair. Le groupe des inversibles modulo $p$ est cyclique d'ordre $p-1$. Etant donné un générateur $\gamma$, résoudre le problème discret de base $\gamma$ pour un résidu $y$ c'est déterminer un entier $x$ tel que

$$\gamma^x = y \mod p.$$

Il n'existe d'algorithme efficace pour résoudre le problème du logarithme discret. L'algorithme de Fig. (3) dit : "pas de bébés, pas de géants" calcule le logarithme discret en $O(\sqrt{p})$ étapes. Pour chaque étape, il s'agit de rechercher un élément dans un ensemble de cardinalité $O(\sqrt{p})$ ce qui peut se faire à temps constant sur une machine possédant suffisament de mémoire.

**Travaux-pratiques 5.** *Il s'agit de coder une expérimentation numérique autour du logarithme discret en langage C avec gmp, la bibliothèque de calcul mulpiprécision de* ***gnu*** *.*

1. *Ecrire une commande pour déterminer le plus petit premier $p$ de $k$ bits qui soit sûr.*
2. *Modifier la commande pour déterminer le plus petit générateur, disons $\gamma_p$, du groupe mulptiplicatif $\mathbb{F}_p{}^\star$.*

```
BSGS( entier p , residu g, residu y)
m := sqrt( p )
b := 1
i := 0
L := vide
// baby steps
tantque (i < m )
   stocker (i, b ) dans L
   b := b * g mod p
   i := i + 1
ftq
j := 0
X := y
b := inverse( b )
// giant steps
tantque X n'est pas dans L
     X := X * b modulo p
     j := j + 1
ftq
i := index( X , L )
retourner i + j*m
```

FIGURE 3. L'algorithme *pas de bébés, pas de géants* calcule le logarithme discret en $O(\sqrt{p})$ étapes.

TABLE 1. Solution de l'exercice pour $k \leq 15$.

| $k$ | $p$ | $\gamma$ | $\log(1+\gamma)$ |
|---|---|---|---|
| 3 | 5 | 2 | 3 |
| 4 | 11 | 2 | 8 |
| 5 | 23 | 5 | 18 |
| 6 | 47 | 5 | 38 |
| 7 | 83 | 2 | 72 |
| 8 | 167 | 5 | 134 |
| 9 | 263 | 5 | 240 |
| 10 | 563 | 2 | 530 |
| 11 | 1187 | 2 | 646 |
| 12 | 2063 | 5 | 150 |
| 13 | 4127 | 5 | 1840 |
| 14 | 8423 | 5 | 4222 |
| 15 | 16487 | 5 | 14250 |

(3) *Implanter un algorithme naif pour déterminer le logarithme discret du résidu* $\gamma_p + 1$.

(4) *Préciser le temps de calcul.*

(5) *Estimer les limites.*

(6) *Implanter l'algorithme "pas de bébés, pas de géants" pour calculer le logarithme discret pour des modules de tailles raisonnable, disons 64-bits.*

(7) *Préciser le temps de calcul.*

```c
#include <stdio.h>
#include <stdlib.h>
#include <gmp.h>

int main( int argc, char* argv[] )
{
int k = atoi( argv[1] );
mpz_t p;
mpz_init(p);
mpz_ui_pow_ui( p, 2, k-1 );
mpz_nextprime( p , p );
gmp_printf ("k=%3d p=%Zd\n", k, p);
return 0;
}
```

FIGURE 4. Calcul du plus petit premier de $k$ bits en `gmp`, source à compiler avec la bibliothèque `lgmp`, comme dans ce makefile

*(8) Estimer les limites.*

## 17. Diffie-Hellman

Le protocole Diffie-Helleman s'appuie sur la difficulté du problème du logarithme discret. Une fois fixé un entier $\gamma$ d'ordre $p-1$ modulo $p$, Alice et Bob peuvent s'échanger une quantité secrète :

(1) Alice choisit un entier $a$. Calcule $A := \gamma^a$ et envoie $A$ à Bob.
(2) Bob choisit un entier $b$. Calcule $B := \gamma^b$ et envoie $B$ à Alice.
(3) Alice calcule $B^a$
(4) Bob calcule $A^b$.

L'associativité du produit modulaire montre que les quantités calculées par Alice et Bob sont identiques. Les deux protagonistes se sont inchangés une quantité $K$ secrète. Alice et Bob doivent s'appuyer sur un tiers pour signer les éléments échangés afin de ne pas se faire attaquer par un homme du milieu.

**Exercice 18.** *Décrire un scénario d'attaque "man in the midle".*

## 18. Rivest-Shamir-Adleman

Le cryptosystème RSA est un système de chiffrement à clef publique proposé [7] par Rivest, Shamir et Adleman à la fin des années 70 qui s'appuie sur certaines propriétés cachées des nombres.

(1) Bob définit la taille des messages, disons $2t$ bits.
(2) Il construit au hasard deux nombres premiers $p$ et $q$ de $t$ bits.
(3) Calcule les produits $n := pq$ et $\phi := (p-1)(q-1)$.
(4) Choisit un entier $e$ premier avec $\phi$.
(5) Détermine $d$ l'inverse de $e$ modulo $\phi$.

(6) Enfin, Bob publie la clé $(e, N)$.

Alice utilise un algorithme d'exponentiation modulaire pour calculer le chiffré $y$ d'un clair $x$, il s'agit de

$$y := E(x) := x^e \pmod{n}$$

Bob effectue une tâche similaire pour déchiffrer $y$, il calcule :

$$x := D(y) = y^d \mod n$$

La faisabilité du système s'appuie d'une part, sur la relative abondance des nombres premiers, d'autre part sur l'existence de tests de primalité probabiliste. La correction du schéma repose sur un résultat d'arithmétique : le théorème d'Euler. La robustesse du système est attribuée à l'apparente complexité du problème de factorisation des entiers. Enfin, l'exponentiation rapide permet une mise en oeuvre même sur des machines modesres.

**Travaux-pratiques 6.** *D'aprés le manuel, la commande* `ssh` *permet d'identifier un utilisateur avec une clé* RSA *pour établir une connexion cryptée. Quels sont les noms des algorithmes à clé symétrique disponibles ? Aprés avoir construit une paire de clés* RSA *avec* `ssh-keygen`*, vérifié le fonctionnement de* `ssh-copy-id` *et* `ssh`*, vous utiliserez* `openssl` *pour trouver les paramètres* RSA *: module, premiers etc... de la clé privée* `id-rsa`*. Utilisez la commande* `bc` *pour vérifier les relations entre tous ces éléments. Refaire les mêmes calculs avec* `gmp`*. Utilisez l'option* `rsautl` *de* `openssl` *pour crypter un petit fichier.*

## 19. Correction de rsa

Soit $n = pq$ un entier RSA. Les éléments non inversibles sont les résidus qui sont des multiples de $p$ ou de $q$. Il y en a $p$+$q$-1, le groupe des inversibles est d'ordre

$$\phi = pq - p - q + 1 = (p-1)(q-1)$$

et donc, pour tout résidu inversible $z$, le théorème d'Euler affirme que

$$z^\phi = 1. \tag{3}$$

Par Bâchet, il existe $v$ tel que

$$ed = 1 + \phi v$$

Ainsi, pour tout inversible $z$

$$\begin{aligned} D(E(z)) &= D(z^e) \\ &= z^{ed} \\ &= z^{1+v\phi} \\ &= z \end{aligned}$$

Le résultat tient aussi pour un élément non inversible, c'est une conséquence du théorème Chinois. Insistons que le fait que nous aurions pu imaginer le contraire tant la probabilité d'un clair non inversible est négligeable !

**Exercice 19.** *Soit $p$ et $q$ deux nombres premier. Montrer le nombre d'éléments inversibles modulo $pq$ est bien égal à $(p-1)(q-1)$.*

## 20. Théorème d'Euler

L'ensemble des inversibles modulo $n$ forme un groupe multiplicatif, généralement noté $\mathbb{Z}/(n)^*$ son ordre est traditionnelement noté $\varphi(n)$. En particulier, si $p$ est premier alors

$$\varphi(p) = p - 1, \quad \varphi(p^r) = (p-1)p^{r-1}.$$

**Exercice 20.**

$$\varphi(p^r) = p^{r-1}(p-1)$$

*Expliquer !*

La fonction Euler est multiplicative : si $m$ et $n$ sont premiers entre eux alors

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{4}$$

**Théorème 5** (Euler)**.** *Si $x$ est un résidu inversible modulo $n$ alors*

$$x^{\varphi(n)} = 1.$$

Il s'agit d'une manifestation du célèbre théorème de Lagrange de la théorie des groupes.

*Démonstration.* Notons $y_1, y_2, \ldots$ une énumération des inversibles. Notons $w$ le produit de ces $\phi$ éléments.

$$\begin{aligned} w &= (xy_1)(xy_2)\cdots(xy_\phi) \\ &= x^\phi w \end{aligned}$$

Il suffit alors de simplifier par $w$. □

## 21. Répartition des premiers

La toute première raison d'effectivité concerne la bonne densité des nombres premiers. Il est facile de prouver la non finitude de l'ensemble des nombres premiers.

Traditionnemlement, si on note $\pi(x)$ le nombre de premier inférieurs à $x$, Legendre, puis Gauss, ont conjecturé la formule asymptotique :

$$\pi(x) \sim \frac{x}{\log x}$$

Cette conjecture a été prouvée De La Vallée Poussin et Hadamard à la fin du XIX-ième siècle, c'est le théorème des nombres premiers. Le petit livre de Jean Itard [2], contient une preuve fausse mais fortement instructive d'Euler.

**Travaux-pratiques 7.** *Implanter l'algorithme du crible d'Eratostène. Vérifier que $\pi(x) \sim \frac{x}{\log x}$ en reconstruisant la figure Fig. (5), en utilisant* `gnuplot`*.*

En 1912, Landau a présenté quatre problèmes difficiles, 100 ans aprés, ils sont toujours ouverts, Landau avait raison !

(1) La conjecture de Goldbach : tout entier pair strictement supérieur à 2 peut s'écrire comme la somme de deux nombres premiers.
(2) La conjecture des nombres premiers jumeaux : il existe une infinité de nombres premiers $p$ tels que $p + 2$ est premier.
(3) La conjecture de Legendre : il existe toujours au moins un nombre premier entre deux carrés parfaits consécutifs.
(4) Il existe une infinité de nombres premiers de la forme $n^2 + 1$.


FIGURE 5. Le calcul de $\pi(x)$ est facile à réaliser avec le crible d'Eratostène, il permet de se convaincre que $\pi(x)\log x \sim x$.

## 22. ATTAQUE PAR CANAL CACHÉ

L'observation de la consommation en courant d'une phase de chiffrement est le premier exemple d'attaque par canal caché, décrit par Paul Kocher dans les années 90. On suppose que le chiffrement RSA est réalisé par un processeur qui sollicite un co-processeur arithmétique pour effectuer les calculs modulaires. Les opérations du co-processeur demandent plus de puissance, et le produit modulaire de deux entiers différents demande plus d'efforts qu'un carré modulaire Fig. (6).Au final, l'analyse de la courbe révèle l'exposant secret $s$ à acuse du traitement asymétrique des bits de l'exposant : un bit égal à 1 provoque une multiplication et un carré, un bit nul génère un carré. Une simulation de cette attaque utilisant `ltrace` est proposée dans [3].

**Exercice 21.** *Donner la valeur de l'exposant secret utilisé dans la phase de chiffrement de Fig. (6).*

## 23. THÉORÈME CHINOIS

Soient $m$ et $n$ deux entiers. Avec les anneaux $\mathbb{Z}/(m)$ et $\mathbb{Z}/(n)$ on forme un anneau produit $\mathbb{Z}/(m)\times\mathbb{Z}/(n)$ en opérant termes à termes :

$$(x,y)\oplus(x',y') = (x+x', y+y')$$
$$(x,y)\otimes(x',y') = (x\times x', y\times y')$$

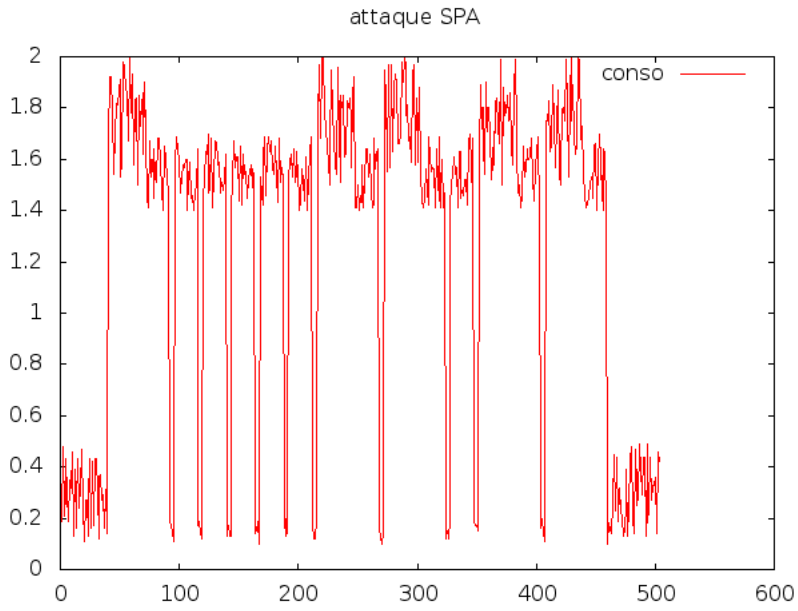



FIGURE 6. L'analyse de la consomation de courant révèle les bits de l'exposant secret.

L'application naturelle :

$$z \mapsto \Psi(z) := (z \pmod m, z \pmod n)$$

est un morphisme de l'anneau $\mathbb{Z}/(mn)$ dans l'anneau produit $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$.

$$\Psi(z+z') = \Psi(z) \oplus \Psi(z'), \quad \Psi(z \times z') = \Psi(z) \otimes \Psi(z').$$

**Théorème 6.** *Si $m$ et $n$ sont premiers entre eux alors $\Psi$ est un isomorphisme d'anneau.*

*Démonstration.* Comme les anneaux ont le même nombre d'éléments, il suffit de montrer que nous sommes en présence d'une injection. Le noyau est formé des résidus multiples de $m$ et $n$. □

On retrouve des traces du théorème dans un traité de Qin Jiushao publié en 1247, où le mathématicien chinois rapporte un problème qui aurait été posé par le maître Sun Zi entre le III-ième siècle et le V-ième siècle :

*Soit des objets dont on ignore le nombre. En les comptant 3 par 3 il en reste 2 ; en les comptant 5 par 5, il en reste 3 et en les comptant 7 par 7, il en reste 2. Combien y a-t-il d'objets ?*

Le théorème de Bâchet-Bézout permet de construire les antécédants de $(1,0)$ et $(0,1)$. En effet, une relation $mu + nv = 1$ montre que :

$$mu \mapsto (0,1), \quad nv \mapsto (1,0).$$

En particulier, l'antécédant de $(x,y)$ est $muy + nvx$.

Revenons sur les fonctions de chiffrement/déchiffrement pour le module $pq$, dans le cas d'un clair non nécessairement premier avec le module.

$$\begin{aligned} D(E((x,y))) &= D((x^k, y^k)) \\ &= (x^{ks}, y^{ks}) \\ &= (x^{1+v\phi}, y^{1+v\phi}) \\ &= (x,y) \end{aligned}$$

En effet, que $x$ soit inversible ou pas, le petit théorème de Fermat montre que $x^{1+v\phi} = x$, et c'est idem pour $y$.

On remarque que le théorème Chinois se généralise sans peine. Si

$$n = p_1^{r_1} p_2^{r_2} \cdots p_f^{r_f},$$

où les $p_i$ sont des nombres premiers alors

$$\mathbb{Z}/(n) \sim \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_f^{r_f})$$

**Exercice 22.** *Quels sont les antécédants de* $(1,0,0)$, $(0,1,0)$ *et* $(0,0,1)$ *par l'isomorphisme naturel*

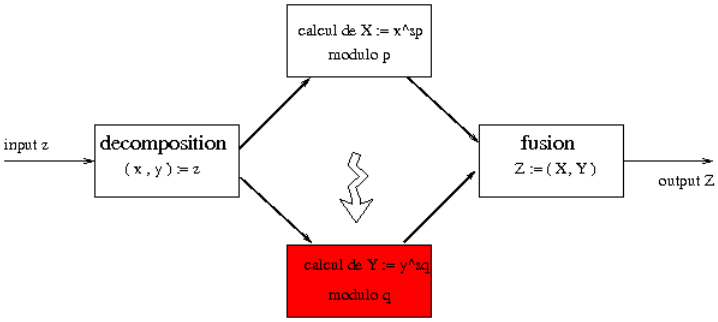
$$\mathbb{Z}/(30) \longrightarrow \mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(5)?$$

**Exercice 23.** *Soient des objets en nombre inconnu. Si on les compte par trois, il en reste deux ; par cinq, il en reste trois, et par sept, il en reste deux. Combien y a-t-il d'objets ?*

## 24. Attaque par faute

On suppose qu'une boîte noire fait du chiffrement RSA en utilisant le CRT pour calculer sur des nombres de petite taille. Le déchiffrement de $z \in \mathbb{Z}/(n)$ est calculé comme suit :

(1) décomposition de $z \mapsto (x,y) \in \mathbb{Z}/(p) \times \mathbb{Z}/(q)$
(2) calcul de $X := x^{sp} \pmod p$, où $sp = s \pmod{p-1}$
(3) calcul de $Y := y^{sq} \pmod q$, où $sq = s \pmod{q-1}$
(4) fusion du résultat $Z$ par inversion $(X,Y)$




L'attaque consiste à déchiffrer $z$, plusieurs fois en essayant de provoquer des fautes lors du calcul sur une composante. Dans le cas d'une puce electronique, le bombardement par des rayons X est un moyen d'injection de faute. Si la boîte envoie deux valeurs différentes $z'$ et $z''$, l'attaque est un succès, un des facteurs du module $n$ est tout simplement :

$$\text{PGCD}(z'' - z', n)$$

En effet, si le calcul correct vérifie $\Psi(z') = (x', y')$, une erreur de sur la première composante donne un une autre valeur vérifiant $\Psi(z'') = (x'', y'')$ avec $x'' \neq x'$ et $y'' = y'$. Ainsi, $\Psi(z'') - \Psi(z')$ est de la forme $(\neq 0, 0)$, et donc $z'' - z'$ est un multiple de $q$ mais pas de $p$.

Une simulation de cette attaque utilisant `ptrace` est proposée dans [3].

**Travaux-pratiques 8.** *Implanter le chiffrement RSA pour des modules de $2t$ bits en langage `C` sans utiliser de bibliothèque de calcul. Il s'agit d'utiliser le CRT pour faire les calculs modulo des premiers de $t$ bits. Le paramètre $t$ dépend de l'architecture. Utiliser `gdb` pour simuler une attaque par injection de faute.*

## 25. Racine carrée de l'unité

**Proposition 6.** *Soit $p$ un nombre premier impair, $r$ un entier positif et $n = p^r$. L'équation $x^2 = 1$ possède exactement deux solutions modulo $n$.*

*Démonstration.* Soit $x$ une solution. Comme $p$ est premier alors $x \equiv \pm 1 \pmod{p}$. Notons $s$ le plus grand entier tel que $x = \pm 1 + kp^s$, avec $(p, k) = 1$. De la relation,

$$x^2 = (\pm 1 + kp^s)^2 = 1 + 2kp^s + p^{2s} \equiv 1 \pmod{p^r}$$

on tire que $r \leq s$ i.e. $x = \pm 1 \pmod{p^r}$. □

**Exercice 24.** *Vérifier que l'énoncé précédent reste correcte pour $p = 2$ et $r \leq 2$ mais est erroné pour $r = 3$ et $r > 3$.*

**Corollaire 1.** *Soit $n$ un entier impair. On note $f$ le nombre de facteurs premiers divisant $n$. L'équation*

$$x^2 \equiv 1 \pmod{n}$$

*possède exactement $2^f$ solutions.*

*Démonstration.* Il suffit d'appliquer le théorème des restes chinois. En notant, $p_1$, $p_2$, …, $p_f$ les premiers divisant $n$, l'isomorphisme naturel :

$$x \mapsto (x_1, x_2, \ldots, x_f)$$

envoie une solution sur des composantes $x_i$ solutions de $X^2 = 1 \pmod{p_i^{r_i}}$. □

**Exercice 25.** *Quelles sont les racines de l'unité modulo 143 ?*

## 26. Théorème de Lagrange

Soit $G$ un groupe multiplicatif. Le cardinal de $G$ s'appelle l'ordre de $G$. Une partie $S$ de $G$ contenant 1 est un sous-groupe de $G$ quand

$$\forall x, y \in S, \quad xy \in S \qquad \wedge \qquad \forall x \in S, \quad x^{-1} \in S.$$

Les produits itérés d'un élément $x$ forment un sous-groupe de $G$, on le note $\langle x \rangle$, son ordre, qui est noté $\text{ord}\,(x)$, est appelé l'ordre de $x$. Le groupe $G$ est dit cyclique quand il existe un élément $x$ vérifiant

$$G = \text{ord}\,(x).$$

**Exercice 26.** *L'ordre de $x$ est égal au plus petit entier non nul tel $r$ tel que $x^r$.*

**Lemme 3.** *Soit $x$ un élément d'un groupe $G$. Pour tout entier $n$ tel que $x^n = 1$, l'ordre de $x$ divise $n$.*

*Démonstration.* Faire la division euclienne de $n$ par l'ordre de $x$. □

**Exercice 27.** *Soit $x$ d'ordre $n$, montrer que*

$$\operatorname{ord}(x^t) = \frac{n}{(n,t)}$$

**Théorème 7** (Lagrange)**.** *L'ordre d'un groupe est divisible par l'ordre d'un sous-groupe arbitraire, et donc par celui de l'ordre d'un élément arbitraire.*

*Démonstration.* On considère les ensembles

$$t + S := \{t + s \mid s \in S\}, \quad t \in G.$$

Deux de ces ensembles sont égaux ou disjoints, ils ont tous la même cardinalité. □

**Exercice 28.** *Soit $n$ un entier positif. On note $S_n$ le groupe des permutations de $n$ lettres. Ecrire un algorithme efficace pour calculer l'ordre d'un élément de $S_n$.*

## 27. CYCLE DES UNITÉS

**Lemme 4.** *Soit $k$ un entier. Si $p$ est premier impair alors*

$$(1+p)^{p^k} \equiv 1 + p^k p \pmod{p^k p^2}. \quad (*)$$

*Démonstration.* Une induction sur $k$ ? Pourquoi pas ! Tout d'abord, (*) est vérifiée pour $k = 0$ car $(1+p)^{p^0} = 1 + p$. Si (*) est vraie pour un certain $k$ alors

$$\begin{aligned}(1+p)^{p^{k+1}} &= (1 + p^k p + X p^k p^2)^p \\ &\equiv 1 + p^k p^2 \pmod{p^k p^3}\end{aligned}$$

□

Le lemme précédent montre que $(1+p)$ est d'ordre $p^{p-1}$ dans $\mathbb{Z}/(p^r)^*$.

**Exercice 29.** *Montrer l'affirmation précédente. Comment ? En calculant $(1+p)^{p^{r-1}}$, et ...*

Un groupe $G$ d'ordre $n$ est dit cyclique quand il est engendré par un élément. Un tel groupe est possède $\varphi(n)$ générateurs car il est isomorphe au groupe $\mathbb{Z}/(n)$, et tous les inveribles modulo $n$ sont des générateurs de $\mathbb{Z}/(n)$. En particulier,

$$\sum_{d|n} \varphi(d) = n \tag{5}$$

Partant de cette formule, on montre qu'un groupe abélien dans lequel il existe au plus $d$ éléments d'ordre divisant $d$ est nécessairement cyclique.

**Théorème 8.** *Le groupe multiplicatif de $\mathbb{F}_p$ est cyclique.*

*Démonstration.* En effet , dans un corps commutatif, l'équation $x^d = 1$ possède au plus $d$ solutions ! □

## 28. structure multiplicative

**Théorème 9** (Gauss)**.** *Le groupe multiplicatif de* $\mathbb{Z}/(p^r)$ *est cyclique.*

*Démonstration.* On sait que son ordre est $\varphi(p^r) = (p-1)p^{r-1}$, il contient un élément $x$ d'ordre $(p-1)$. Le lemme (4) montre que $(1+p)$ est d'ordre $p^{r-1}$, au final $(1+p)x$ engendre les inversibles.

□

**Exercice 30.** *Déterminer un élément d'ordre* 4 *modulo* 125*, puis un élément d'ordre* 100*.*

## 29. Nombre de Carmichael

Un entier composé $n$ est dit nombre de Carmichael lorsque :

$$\forall x \in \mathbb{Z}/(n)^*, \quad x^{\varphi(n)} = 1.$$

Ces nombres mettent en défaut le test de Fermat. Notons qu'un tel nombre est nécessairement impair, ils sont rares mais en nombre infini.

**Théorème 10** (Korselt,1899)**.** *Un entier* $n$ *est de Carmichael si et seulement si* $n$ *est sans facteur premier double et pour tout diviseur premier* $p$ *de* $n$*,* $p-1$ *divise* $n-1$*.*

*Démonstration.* Supposons que $p^r$ divise $n$. Le groupe $\mathbb{Z}/(p^r)^*$ contient un élément d'ordre $p^{p-1}(p-1)$. Le théorème des restes chinois montre qu'il en est de même pour $\mathbb{Z}/(n)^*$. L'ordre de cet élément divise $n-1$ et donc $(p-1)$ divise $n-1$ mais aussi $r = 1$. Réciproquement, pour $x$ inversible modulo $n$, et pour chaque diviseur $p$ de $n$, on a $x^{n-1} \equiv x^{p-1} \equiv 1 \pmod{p}$. Comme il existe un élément d'ordre $p-1$ modulo $p$, cette dernière congruence montre que $p-1$ divise $n-1$. □

Les nombres de Carmichael possèdent au moins trois facteurs premiers. Les premiers nombres de Carmichael sont : 561, 1105, 1729, 2465, 2821, 6601, 8911 etc...

**Exercice 31.** *Soit* $n$ *un nombre de Carmichael. Montrer que* $n$ *possède trois facteur premiers.*

## 30. Fermat, Solovay-Strassen

Un test de primalité probabiliste s'appuie sur un algorithme $T(x,n)$ qui prend en entrée un résidu $x$ modulo $n$ et renvoie VRAI ou FAUX.

$$\exists x \neq 0, \neg T(x,n) \Longrightarrow n \text{ composé}$$
$$\forall x \neq 0, T(x,n) \Longrightarrow n \text{ premier}$$

Pour un entier composé $n$ (impair), les résidus tels que $\neg T(x,n)$ sont des témoins de non-primalité, les autres sont des menteurs. Nous notons $\mu(T,n)$ le nombre de menteurs pour l'entier $n$ du point de vue du test $T$, la probabilité d'erreur aprés un test vaut :

$$\theta(T,n) = \frac{\mu(T,n)}{n}$$

et le paramètre :

$$\Theta(T) = \sup_{n \text{ composé}} \theta(T,n)$$

mesure l'efficacité du test. Quand $\Theta(T) < 1$, il est possible de se convaincre du caractère premier d'un nombre, cela d'autant plus rapidement que $\Theta(T)$ est petit.

Rappelons que, d'aprés Emile Borel, un individu néglige les évènements de probabilité moindre que $10^{-6}$, les terriens ceux de probabilité $10^{-15}$, enfin les évènements de probabilité moindre que $10^{-45}$ ne sont pas observables !

30.1. **Test de Fermat.** Il s'appuie directement sur le petit théorème de Fermat :

```
Fermat( x, n )
y := expmod( x, n-1, n )
retourner y = 1
```

On constate que le test de Fermat est vraiment efficace sur les nombres primaires. En effet, si $n = p^r$ avec $p$ impair alors le groupe $\mathbb{Z}/(n)^*$ est cyclique d'ordre $\phi(n)$. Un calcul direct montre que $\text{PGCD}(n-1, \varphi(n)) = p-1$, le nombre menteurs de Fermat est majoré par $p-1$ et

$$\theta(F, p^r) \leq \frac{1}{p^{r-1}} \ll \frac{1}{3}.$$

On constate que le test de Fermat se comporte assez bien sur les nombres composés ayant au moin un témoin de composition. Pour un tel nombre $n$, il existe un élément $x$ tel que $x^n \neq 1$. Cet élément permet de faire d'associé un témoin $xy$ à chaque menteur de Fermat, au final

$$\theta(F, n) < \frac{1}{2}.$$

Malheureusement, d'aprés les arithméticiens, il existe une infinité de nombre entiers $n$ sans témoin de Fermat. Il s'agit des nombres de Carmichael, pour lesquels :

$$\theta(F, n) = \frac{\varphi(n)}{n} \to 1 = \Theta(F).$$

30.2. **Test de Solovay-Strassen.**

$$S(x, n) := x^{\frac{n-1}{2}} = \pm 1$$

ce teste est plus efficace que le test de Fermat, c'est le test de Solovay-Strassen "faible". Malheureusement, on peut encore prouver que $\Theta(S) = 1$ ! La version originale de ce test détecte tous les nombres composés, mais elle utilise le symbole de Jacobi qui est hors programme.

On peut comprendre intuitivement, les raisons qui font que le test de Solovay-Strassen faible est meilleur que le test de Fermat. Si $x$ est un Fermat-menteur pour l'entier $n$, $x^{n-1} = 1$ mezalor $x^{\frac{n-1}{2}}$ est une racine carrée de l'unité, et la probabilité que cette dernière soit égale à 1 est potentielement $2^{1-f}$, où $f$ désigne le nombre de diviseurs premiers de $n$.

**Exercice 32.** *Utiliser un programme pour déterminer les nombres composés impair $n \leq 1024$ qui possèdent plus de 0.25 menteurs.*

## 31. Test de Rabin-Miller

```
Miller-Rabin( n : nombre )
var
    k := 0
    m := n-1
    z := n-1
debut
tantque ( pair( m ) )
   m:= m / 2
   k:= k + 1
ftq
x := aleas( n )
y := expmod(x, m , n)
```

```
tantque ( k >= 0 )
   y := prd( y, y, n)
   si ( y = 1 )
      retourner
         minus( z )
   fsi
   z := y
   k := k-1
ftq
retourner faux
fin
```

**Théorème 11.** *Pour un nombre de Carmichael $n$, on a : $\theta(MR, n) < \frac{1}{4}$.*

*Démonstration.* Pour $n-1 = 2^k m$, $m$ impair, convenons de parler des témoins, et menteurs de niveau $0 \leq l \leq k$. Un menteur $x$ de niveau 0 est caractérisé par $x^m = 1$, inversement, un témoin de niveau 0 par $x^m \neq \pm 1$. Si $p$ est un premier divisant $n$ alors $(p-1)$ ne divise pas $m$ et donc il existe des éléments vérifiant $x^m \neq 1 \mod p$. Au final, pour le niveau 0, la proportion de menteurs est inférieur à 1/4. Si $x = (x_1, x_2, \ldots, x_r)$ est un menteur au niveau $l$, alors pour chaque $j$, $(\ldots, x_{j-1}, 1, x_{j+1}, \ldots)$ est un témoin de niveau $l$, à nouveau, la proportion des menteurs de niveau $l$ est moindre que 1/4. □

**Remarque 1.** *Le théorème est valide pour tous les nombres composés, au final :*

$$\Theta(MR) < \frac{1}{4}.$$

**Exercice 33.** *Pour un impair $n$, montrer que :*

$$\theta(R, n) \leq \theta(S, n) \leq \theta(F, n)$$

.

## 32. Premiers industriels

Le résultat de la section précédente montre qu'il n'y a pas de grand risque à considérer premier un nombre passant le test de Rabin 25 fois consécutives, évènement de probabilité moindre que $2^{-50}$. Pour se faire une idée, c'est un événement moins probable que de gagner deux fois de suite le gros lot du loto !

**Exercice 34.** *Vérifier ce qui vient d'être dit à propos du loto et du test de Rabin.*

**Travaux-pratiques 9.** *Programmer l'expérience numérique de la figure Fig. (7).*

**Travaux-pratiques 10.** *Implanter votre propre algorithme de Rabin-Miller en utilisant les fonctions arithmétiques de base de la bibiothèque gmp pour construire des nombres premiers industriels.*

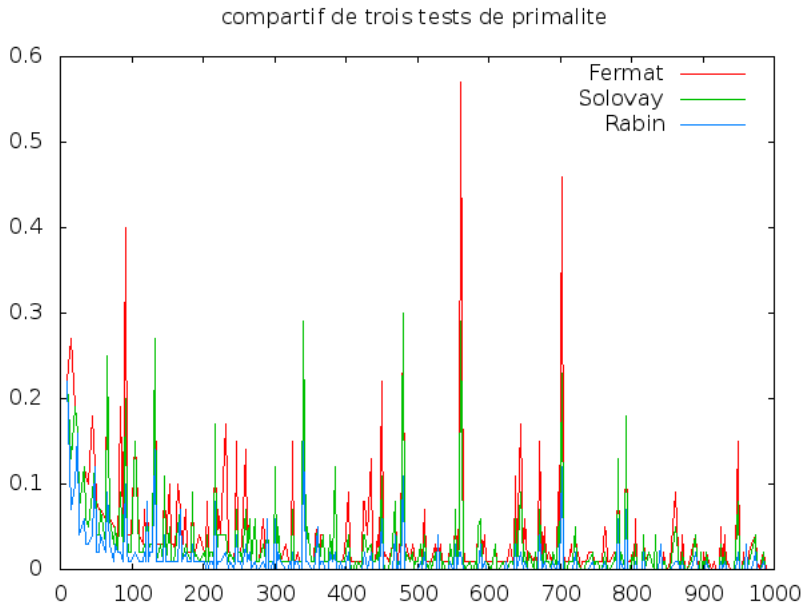



FIGURE 7. comparaison des tests de Fermat, Solovay-Strassen et Rabin-Miller. On constate que la proportion de menteurs pour le teste de Rabin est inférieur à 0.25.

## RÉFÉRENCES

[1] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6) :644–654, 1976.

[2] Jean Itard. *Les nombres premiers*. "Que sais-je ?", No. 571. Presses Universitaires de France, Paris, 1969.

[3] Philippe Langevin. Le bidouillage en informatique. http://langevin.univ-tln.fr/cours/DARKCODE/darkoding.pdf.

[4] Philippe Langevin. Une brève histoire des nombres. http://langevin.univ-tln.fr/notes/rsa/rsa.pdf.

[5] Peter L. Montgomery. Modular multiplication without trial division. *Math. Comp.*, 44(170) :519–521, 1985.

[6] Michael Rabin. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 12 :128–138, 1980.

[7] R.L. Rivest, A. Shamir, and L. Adleman. A probalistic algorithm for testing primality. *Journal of Number Theory*, 21 :120–126, 1978.

```c
#include <stdio.h>
#include <gmp.h>
#include <time.h>
#include <unistd.h>
int main (void) {
    mpz_t rand_Num;
    unsigned long int i, seed;
    gmp_randstate_t r_state;

    seed = time(NULL) + getpid();

    gmp_randinit_default (r_state );
    gmp_randseed_ui(r_state, seed);

    mpz_init(rand_Num);

    for(i = 0; i < 10; ++i) {
        mpz_urandomb(rand_Num,r_state,14);
        gmp_printf("%Zd\n", rand_Num);
    }

    gmp_randclear(r_state);
    mpz_clear(rand_Num);
    return 0;
}
```

FIGURE 8. Un exemple de tirage aléatoire avec gmp