L'ANNEAU $\mathbb{Z}/n\mathbb{Z}$

Plan

I : Structure quotient
- 1) Congruence
- 2) Opérations
- 3) Structure d'anneau
- 4) Morphismes de groupe de $\mathbb{Z}$

II : L'anneau $\mathbb{Z}/n\mathbb{Z}$
- 1) Idéal dans $\mathbb{Z}/n\mathbb{Z}$ et dans $\mathbb{K}[X]$
- 2) Inverse d'un élément
- 3) Fonction indicatrice d'Euler
- 4) Le petit théorème de Fermat
- 5) Anneau intègre et corps
- 6) Caractéristique d'un corps
- 7) Le théorème des restes chinois

Annexe I : Corps finis
Annexe II : Utilisation d'un corps fini dans le codage des transmissions
Annexe III : Utilisation d'un corps fini dans les disques compacts
Annexe IV : Cryptographie
- 1) Chiffrement de messages avec clef publique
- 2) Quelques problèmes de transmission confidentielle
- 3) Authentification de signatures
- 4) Sécurisation des communications par internet

Exercices
- 1) Enoncés
- 2) Solutions

I : Structure quotient

1- Congruence

Nous avons vu, dans le chapitre L1/ARITHMTQ qu'on définit une relation de congruence sur les entiers de la façon suivante (en notant | la relation de divisibilité).

$$x \equiv y \bmod n \Leftrightarrow n \mid (x - y) \Leftrightarrow \exists\, k \in \mathbb{Z},\ x = y + nk$$

Il s'agit d'une relation d'équivalence. Dans ce chapitre, nous nous intéressons plus particulièrement aux classes d'équivalence de cette relation, plutôt qu'aux entiers eux-mêmes. Une même classe d'équivalence regroupe tous les éléments équivalents entre eux. Ainsi, pour $n = 2$, la relation de congruence se traduit par la parité. Deux éléments sont équivalents modulo 2 si et seulement s'ils ont même parité. Il y a alors deux classes, celle des nombres pairs, et celle des nombres impairs.

Dans le cas général, il n'est pas difficile de vérifier que deux éléments sont congrus modulo n si et seulement si ils ont même reste dans la division euclidienne par n. Il y a alors n classes d'équivalence, la classe des nombres dont le reste vaut 0, respectivement 1, ..., $n - 1$. On appelle représentant d'une classe un élément de cette classe. Ce représentant peut être pris indifféremment, bien qu'on ait en général tendance à priviligier le choix des représentants entre 0 et $n - 1$. Si x est un entier, on note $\overline{x}$ sa classe. Ainsi, n étant fixé :

$$\overline{x} = \{x + nk, k \in \mathbb{Z}\}$$

L'ensemble des classes d'équivalence modulo n s'appelle l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n, et est noté $\mathbb{Z}/n\mathbb{Z}$. On a donc :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$$

Les congruences jouent un rôle important dans notre quotidien. Donnons quelques exemples :

❑ Le numéro INSEE est constitué de 15 chiffres. Le nombre A constitué des treize premiers identifie la personne alors que le nombre B constitué des deux derniers chiffres sert de contrôle. On peut détecter une erreur sur un chiffre, ou bien on peut détecter la permutation de deux chiffres consécutifs. B est défini par la formule B = 97 – (A mod 97). Considérons par exemple le nombre purement fictif A = 0230215012026. Alors B = 54.

Pour tester la validité du numéro 023021501202654, on calcule A + B, soit 230215012080 et on vérifie que c'est un multiple de 97. Si tel est le cas, le numéro est considéré comme valide. Dans le cas contraire, il y a une erreur.

Ce sera le cas si un chiffre est faux. En effet, si le n-ème chiffre se trouve décalé d'une quantité x par rapport à sa valeur réelle, A + B est égal modulo 97 à $x10^n$. Celui-ci n'étant pas divisible par 97, l'erreur est détectée.

Il en est de même si on a permuté deux chiffres consécutifs. En effet, dans ce cas, A + B est égal modulo 97 à un nombre de la forme $y \times 10^n + x \times 10^{n-1} - x \times 10^n - y \times 10^{n-1}$ soit $9 \times 10^{n-1} \times (y - x)$ qui n'est pas divisible par 97.

❑ Un procédé comparable est utilisé pour le relevé d'identité bancaire (RIB) : les deux derniers chiffres forment une clef choisie de façon que le nombre complet formé par la suite des différents codes (établissement, guichet, compte, clef) soit divisible par 97.

❑ Quant au code ISBN-10 des livres (*International Standard Book Number*), il est constitué de dix chiffres $a_1a_2a_3...a_{10}$, dont les neuf premiers identifient l'éditeur et le livre, et le dernier est une clef choisie de façon que $\sum_{i=1}^{10} ia_{11-i}$ soit divisible par 11. Là aussi, une erreur sur un chiffre est détectée. Si la clef doit se voir attribuer la valeur 10, elle sera notée X. Par exemple :

0-387-97993-X

(code ISBN d'un livre remarquable dont on ne peut que recommander la lecture ☺)

Le code ISBN-10 est obsolète et a été remplacé par le code ISBN-13 qui a une forme $a_1a_2...a_{13}$ telle que $\sum 3a_{2i} + \sum a_{2i+1}$ soit divisible par 10.

2- Opérations

Dans le cas de la parité, il est bien connu qu'on dispose des règles suivantes, concernant la relation entre addition, multiplication et parité :

pair + pair = pair
pair + impair = impair + pair = impair
impair + impair = pair
pair × pair = pair
pair × impair = impair × pair = pair
impair × impair = impair

ce qu'on peut encore écrire, en se plaçant dans $\mathbb{Z}/2\mathbb{Z}$:

$\overline{0} + \overline{0} = \overline{0}$

$\overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1}$

$\overline{1} + \overline{1} = \overline{0}$

$\overline{0} \times \overline{0} = \overline{0}$

$\overline{0} \times \overline{1} = \overline{1} \times \overline{0} = \overline{0}$

$\overline{1} \times \overline{1} = \overline{1}$

On a donc défini une addition et une multiplication dans $\mathbb{Z}/2\mathbb{Z}$, dont il n'est pas difficile de voir qu'elles munissent cet ensemble d'un structure d'anneau, $\overline{0}$ étant le neutre pour la somme et $\overline{1}$ le neutre pour le produit. Il s'agit même d'un corps, puisque le seul élément non nul est $\overline{1}$, égal à son propre inverse.

On souhaite de même définir dans $\mathbb{Z}/n\mathbb{Z}$ deux lois, l'une additive, l'autre multiplicative. On procède comme suit. Pour ajouter deux classes $\overline{x}$ et $\overline{y}$, on choisit deux représentants dans chacune de ses classes, on les ajoute et on prend la classe de cette somme. Par définition, on a donc :

$\overline{x} + \overline{y} = \overline{x + y}$

On procède de même pour le produit :

$\overline{x} \times \overline{y} = \overline{xy}$

Une vérification est cependant essentielle. Il convient de montrer que le résultat obtenu ne dépend que des classes initiales et pas de tel ou tel représentant choisi dans chaque classe pour effectuer le calcul. Par exemple, pour $n = 5$, on a $\overline{3} + \overline{11} = \overline{14} = \overline{4}$, mais comme $\overline{11} = \overline{1}$, il est heureux de constater que $\overline{3} + \overline{1}$ donne le même résultat $\overline{4}$. Effectuons cette vérification dans le cas général. Si on a $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors il existe h et k entiers tels que :

$x' = x + hn$
$y' = y + kn$

donc :

$x' + y' = x + y + (h + k)n \equiv x + y \bmod n$
$x'y' = xy + (hy + kx + hkn)n \equiv xy \bmod n$

de sorte qu'on a bien $\overline{x+y} = \overline{x'+y'}$ et $\overline{xy} = \overline{x'y'}$. On dit que les lois additive et multiplicative sont **compatibles** avec la relation de congruence. Le calcul se fait bien sur les classes et ne dépend pas des représentants choisis.

3- Structure d'anneau

Il est fastidieux, mais sans difficulté de vérifier que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif de neutre $\overline{0}$, et que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire d'unité $\overline{1}$. Par exemple, l'associativité de la somme se montre comme suit :

$$(\overline{x} + \overline{y}) + \overline{z} = \overline{x+y} + \overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x} + \overline{y+z} = \overline{x} + (\overline{y} + \overline{z})$$

Les définitions $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{xy}$ signifient que l'application $x \in \mathbb{Z} \to \overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneau, appelé **morphisme canonique**.

On prendra garde que les opérations dans $\mathbb{Z}/n\mathbb{Z}$ peuvent avoir un comportement inhabituel. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, le polynôme $X^2 - 1$ admet non pas deux racines, mais quatre, à savoir $\overline{1}$, $\overline{3}$, $\overline{5}$ et $\overline{7}$. Toujours dans cet anneau, $\overline{2} \neq \overline{0}$ et $\overline{4} \neq \overline{0}$ mais $\overline{2} \times \overline{4} = \overline{8} = \overline{0}$.

EXEMPLES :

❑ La structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$ est implicitement utilisée dans les tests de divisibilité. La preuve par 9, par exemple, consiste à dire qu'un nombre entier n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. On se place en fait dans $\mathbb{Z}/9\mathbb{Z}$, dans lequel, pour tout n, $10^n \equiv 1 \bmod 9$. Un entier est donc congru à la somme de ses chiffres modulo 9. De même, la preuve par 9 permet de tester une erreur de calcul dans la somme s ou le produit p de deux entiers a et b. La somme des chiffres de s doit être égale modulo 9 à la somme des chiffres de a et de b. La somme des chiffres de p doit être égale au produit de la somme des chiffres de a par la somme des chiffres de b. Ainsi, le produit $115 \times 238 = 27470$ est faux car 7×13 ou mieux encore 7×4 vaut 28 ou 1 modulo 9, alors que 27470 vaut 2 modulo 9. Ce test est directement lié à notre utilisation d'une base numérique décimale. Dans une base de numération quelconque b, on appliquera une preuve analogue par $b - 1$.

❑ Un autre test est la preuve par 11. Elle est analogue à la preuve par 9, sauf qu'au lieu de faire la somme des chiffres, on retranche le chiffre des dizaines au chiffre des unités, on ajoute celui des centaines, on retranche celui des milliers, etc. en alternance. On effectue juste un calcul dans $\mathbb{Z}/11\mathbb{Z}$ avec $10 \equiv -1 \bmod 11$ et donc $10^n \equiv (-1)^n \bmod 11$. Ainsi, $115 \times 238 = 27470$ est faux car $(5 - 1 + 1) \times (8 - 3 + 2) = 5 \times 7 = 35$ qui est congru à 2 modulo 11 alors que $0 - 7 + 4 - 7 + 2 = -8$ qui est congru à 3 modulo 11. Dans une base de numération quelconque b, on appliquera une preuve analogue par $b + 1$.

❑ On peut également définir un test de divisibilité par 7, 11 et 13 en raisonnant modulo 1001 qui est le produit de ces trois nombres. Modulo 1001, 1000 vaut –1 de sorte que :

$$2157779 \equiv 2 - 157 + 779 = 624$$

et $624 = 13 \times 48 \equiv 0 \bmod 13$ donc 2157779 est divisible par 13.

4- Morphismes de groupe de $\mathbb{Z}$

Les sous-groupes $\mathbb{Z}/n\mathbb{Z}$ interviennent naturellement dans le contexte suivant. Considérons un groupe G et un morphisme f de $(\mathbb{Z}, +)$ dans G. Il s'agit d'une application vérifiant $f(x + y) = f(x) + f(y)$ ou $f(x + y) = f(x)f(y)$ selon que la loi de G est notée additivement ou multiplicativement. On rappelle qu'alors, l'image du neutre 0 de $\mathbb{Z}$ est le neutre de G et l'image de $– x$ est le symétrique de $f(x)$. Comme $\mathbb{Z}$ est engendré par 1, il suffit, pour déterminer f de donner l'image de $a = f(1)$. On aura en effet, dans le cas d'une loi de G notée additivement :

$f(2) = f(1 + 1) = f(1) + f(1) = a + a$ noté $2a$

Plus généralement, pour tout entier x, on aura $f(x) = xa$ ou a^x selon que la loi de G est notée additivement ou multiplicativement, y compris si x est négatif. Le sous-groupe $f(\mathbb{Z})$ de G est engendré par a. Il est donc monogène. Il s'agit d'un sous-groupe commutatif de G, et nous noterons dorénavant sa loi additivement. On a donc :

$$f(\mathbb{Z}) = \{ax, x \in \mathbb{Z}\}$$

Intéressons-nous au fait de savoir si f est injective ou pas. Pour cela, on cherche son noyau, qui est un sous-groupe H de $\mathbb{Z}$ (cf. L2/GROUPES.PDF). Il y a deux cas :

❑ Ou bien ce sous-groupe est réduit à $\{0\}$, f est injective, et $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}$.

❑ Ou bien ce sous-groupe H possède un élément non nul. Montrons alors qu'il existe n tel que ce sous-groupe soit de la forme $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$. Prenons pour cela le plus petit élément n strictement positif de H. H étant un sous-groupe additif de $\mathbb{Z}$, $2n = n + n$ est dans H, de même que $3n = 2n + n$, et plus généralement kn, $k \in \mathbb{N}$ d'abord puis $k \in \mathbb{Z}$ ensuite par symétrisation. Ainsi $n\mathbb{Z}$ est inclus dans H.

Réciproquement, montrons que tout x de H est divisible par n. Effectuons la division euclidienne de x par n. Elle donne $x = qn + r$ avec $0 \leq r < n$. Donc $r = x – qn$ avec x dans H, qn dans $n\mathbb{Z} \subset$ H, donc r est dans H. n étant le plus petit élément de H strictement positif, et r étant un élément de H positif ou nul mais strictement inférieur à n, r est nécessairement nul. On a bien montré que x est multiple de n et donc que H est inclus dans $n\mathbb{Z}$.

Montrons alors que $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Considérons l'application associant à une classe module n la quantité xa où x est un représentant de la classe :

$$\psi : \overline{x} \in \mathbb{Z}/n\mathbb{Z} \rightarrow xa \in \text{G}$$

Il convient de vérifier que l'image dépend de la classe et pas de tel ou tel représentant dans cette classe. Autrement dit, si $\overline{x} = \overline{x'}$, il convient de montrer que $xa = x'a$. Or :

$\overline{x} = \overline{x'}$

$\Rightarrow$ $\exists\, k, x' = x + kn$

$\Rightarrow$ $x'a = xa + kna$ or $na = 0$ dans G

$\Rightarrow$ $x'a = xa$

Cette application est surjective puisque tout élément de $f(\mathbb{Z})$ est évidement de la forme xa. Il s'agit d'un morphisme car :

$$\begin{aligned}\psi(\overline{x} + \overline{x'}) &= \psi\,(\overline{x + x'}) \\ &= (x + x')a \\ &= xa + x'a \\ &= \psi(\overline{x}) + \psi\,(\overline{x'})\end{aligned}$$

Ce morphisme est injectif. Cherchons son noyau. Si $\psi(\overline{x}) = 0$, alors $xa = 0$, donc x est élément de H donc est un multiple de n donc $\overline{x} = \overline{0}$.

On peut donc énoncer :
PROPOSITION
Soit f un morphisme de $\mathbb{Z}$ *dans un groupe* G.

Ou bien f est injective et alors f($\mathbb{Z}$) *est isomorphe à* $\mathbb{Z}$.

Ou bien f n'est pas injective, et il existe n tel que f($\mathbb{Z}$) *est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$. *Un tel groupe est dit* **cyclique**.

Un groupe cyclique est donc un groupe monogène fini. $\mathbb{Z}/n\mathbb{Z}$ est le modèle de base de tous les groupes cycliques d'ordre n.

EXEMPLES :
❑ U_n, groupe des racines n-èmes de l'unité dans $\mathbb{C}$ est un groupe multiplicatif cyclique, isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Un isomorphisme est donné par $\overline{x} \in \mathbb{Z}/n\mathbb{Z} \rightarrow \exp(\frac{2ix\pi}{n})$.

❑ Soit α un irrationnel. Considérons l'application $x \in \mathbb{Z} \rightarrow r(x) \in SO_2(\mathbb{R})$, où $r(x)$ est la rotation plane d'angle $x\alpha\pi$. Il est aisé de montrer qu'il s'agit d'un morphisme. Le noyau est formé des x tels que $x\alpha\pi = 2k\pi$, $k \in \mathbb{Z}$. α étant est irrationnel, la seule solution est $x = k = 0$ et l'image du morphisme est isomorphe à $\mathbb{Z}$.

II : L'anneau $\mathbb{Z}/n\mathbb{Z}$

1- Idéal dans $\mathbb{Z}/n\mathbb{Z}$ et dans $\mathbb{K}[X]$

Nous avons montré dans le paragraphe précédent que les sous-groupes H de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$. Ces sous-groupes vérifient en outre la propriété suivante relative au produit :

$$\forall\, a \in H, \forall\, b \in \mathbb{Z}, ab \in H$$

On dit que H est un **idéal**. La notion d'idéal intervient dans les morphismes d'anneaux. Si A et B sont deux anneaux, un **morphisme** ψ de A dans B est une application vérifiant, pour tout a et b de A :

$\psi(a + b) = \psi(a) + \psi(b)$
$\psi(ab) = \psi(a)\psi(b)$

Si les anneaux possèdent un neutre pour le produit, on impose généralement la condition supplémentaire $\psi(1) = 1$. Pour savoir si ψ est injective, on s'intèresse à son noyau, à savoir :

$\mathrm{Ker}(\psi) = \{a \in A, \psi(a) = 0\}$

Il s'agit d'un idéal de A. En effet, ψ étant a fortiori un morphisme de groupe, on sait déjà que $\mathrm{Ker}(\psi)$ est un sous-groupe de A (voir le chapitre L2/GROUPES.PDF). En outre :

$a \in \mathrm{Ker}(\psi)$, $b \in A$
$\Rightarrow$ $\psi(a) = 0$
$\Rightarrow$ $\psi(a)\psi(b) = 0$
$\Rightarrow$ $\psi(ab) = 0$
$\Rightarrow$ $ab \in \mathrm{Ker}(\psi)$

et de même $ba \in \mathrm{Ker}(\psi)$ (dans le cas où l'anneau n'est pas commutatif).

Nous avons donc montré qu'un idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$.

On montre de même qu'un idéal de l'anneau des polynômes $\mathbb{K}[X]$ est de la forme $\{PQ, Q \in \mathbb{K}[X]\}$, en considérant non plus le plus petit entier strictement positif de l'idéal, mais un polynôme non nul de degré minimal élément de l'idéal. Plus précisment, soit H un idéal de $\mathbb{K}[X]$, c'est-à-dire un sous-groupe de $(\mathbb{K}[X], +)$ vérifiant de plus la propriété :

$$\forall P \in H, \forall Q \in \mathbb{K}[X], PQ \in \mathbb{K}[X]$$

Si $H = \{0\}$, H est de la forme $\{PQ, Q \in \mathbb{K}[X]\}$ avec $P = 0$.

Si $H \neq \{0\}$, soit P polynôme non nul élément de H et de degré minimal. Montrons que H est égal à l'ensemble $\{PQ, Q \in \mathbb{K}[X]\}$. L'inclusion $\{PQ, Q \in \mathbb{K}[X]\} \subset H$ est triviale du fait de la propriété supplémentaire donnée ci-dessus qui fait de H un idéal. Réciproquement, soit S élément de H. effectuons la division euclidienne de S par P : $\exists (Q, R), S = PQ + R$ avec $\deg(R) < \deg(P)$. On a donc $R = S - PQ$ élément de H (car $PQ \in H$ puisque H est un idéal, $S \in H$, donc $S - PQ \in H$ car H est un sous-groupe pour l'addition). Mais $\deg(R) < \deg(P)$ et P est de degré minimal parmi les éléments non nul de H. La seule possibilité est donc que $R = 0$. Donc $S = PQ$ et l'on a bien :

$$H \subset \{PQ, Q \in \mathbb{K}[X]\}$$

Finalement, $H = \{PQ, Q \in \mathbb{K}[X]\}$. P est élément de H et divise tout autre élément de H. Il est défini à une constante multiplicative près.

EXEMPLE :

❑ Soit E un espace vectoriel de dimension finie et u un endomorphisme de E. L'ensemble H des polynômes annulateurs P de u (i.e. tels que $P(u) = 0$, voir le chapitre L2/DIAGONAL.PDF) forme un idéal de $\mathbb{K}[X]$. En effet, la différence de deux polynômes annulateurs est annulateur, et le produit d'un polynôme annulateur P par n'importe quel polynôme Q est annulateur :

$$(PQ)(u) = (QP)(u) = Q(u) \circ P(u) = 0$$

Par conséquent, il existe un polynôme P tel que $H = \{PQ, Q \in \mathbb{K}[X]\}$. P est un polynôme annulateur de u, de degré minimal. On l'appelle **polynôme minimal** de u.

Un idéal engendré par un unique élément (comme l'est $n\mathbb{Z}$ engendré par n) est dit **principal**, et un anneau dont tous les idéaux sont principaux est dit **anneau principal**. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont donc des anneaux principaux.

Dans un anneau principal A, l'**identité de Bézout** est vérifiée. Soit en effet deux éléments a et b de A. Considérons $I = \{ax + by, x \in A, y \in A\}$. Il n'est pas difficile de vérifier que I est un idéal. I est en effet stable par addition et passage au symétrique, donc c'est un sous-groupe de A, et le produit de tout élément de I par un élément quelconque de A une combinaison linéaire de a et b à coefficients dans A, donc est un élément de I. Mais A étant principal, I est engendré par un élément d de A : $I = \{dz, z \in A\}$. En particulier, pour $x = 1$ et $y = 0$, $ax + by = a \in I$, donc $\exists z, x = dz$ donc d divise x dans A. De même, d divise y. Donc d est un diviseur commun de a et b. Montrons que c'est le plus grand, au sens de la divisibilité. Soit q un diviseur commun de a et b. q divise alors tout élément de la forme $ax + by$ donc divise tout élément de I donc q divise d qui est élément de I (pour $z = 1$). d étant lui-même élément de I, il est de la forme $d = ax + by$.

La même démonstration s'applique pour n éléments a_1, ..., a_n de A en considérant l'idéal $I = \{\sum_{k=1}^{n} a_k x_k, x_k \in A\}$. Le générateur de I est le PGCD d_n de a_1, ..., a_n. d_n étant élément de I, il est combinaison linéaire des a_k à coefficients entiers.
Malheureusement, cette preuve est non constructive et ne surpasse pas l'algorithme d'Euclide dans $\mathbb{Z}$ ou $\mathbb{K}[X]$ pour déterminer explicitement un PGCD. Mais elle explique la raison pour laquelle la notion de PGCD et d'identité de Bézout est définie dans ces deux anneaux.

2- Inverse d'un élément

Dans ce paragraphe, on s'intéresse aux éléments de $\mathbb{Z}/n\mathbb{Z}$, admettant un inverse, c'est-à-dire un symétrique pour le produit.

PROPOSITION

$\bar{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x est premier avec n.

Démonstration :

❑ $\bar{x}$ inversible

$\Leftrightarrow$ $\exists\, y, \bar{x}\,\bar{y} = \bar{1}$
$\Leftrightarrow$ $\exists\, y, xy \equiv 1 \mod n$
$\Leftrightarrow$ $\exists\, y, \exists\, k, xy = 1 + kn$
$\Leftrightarrow$ $\exists\, y, \exists\, k, xy - kn = 1$
$\Leftrightarrow$ $x \wedge n = 1$ d'après l'identité de Bézout.

EXEMPLE :

❑ Dans $\mathbb{Z}/15\mathbb{Z}$, $\overline{12}$ n'est pas inversible alors que $\bar{8}$ et $\overline{11}$ le sont.
On a en effet $15 \wedge 12 = 3 \neq 1$. On a d'ailleurs, modulo 15 :

$$\bar{5} \times \overline{12} = \overline{60} = \bar{0}$$

Ainsi, on constate que, bien que $\bar{5}$ et $\overline{12}$ ne soient pas nuls, leur produit l'est. On dit que $\bar{5}$ et $\overline{12}$ sont des **diviseurs** de $\bar{0}$.

Par contre, $\bar{8} \times \bar{2} = \overline{16} = \bar{1}$, et $\overline{11} \times \overline{11} = \overline{121} = \bar{1}$, donc $\overline{11}$ est son propre inverse. On remarque à ce propos que l'équation $X^2 = 1$ admet plus de deux solutions dans $\mathbb{Z}/15\mathbb{Z}$, à savoir, au moins $\bar{1}$, $-\bar{1} = \overline{14}$ et $\overline{11}$. Ainsi, le fait qu'un polynôme de degré m admette au plus m racines n'est pas valide dans un anneau quelconque.

L'intêret d'être inversible est primordial quand on veut résoudre des équations du type $ax = b$. Si a est inversible, il suffit de multiplier par l'inverse de a pour trouver x.

EXEMPLES :

❑ Résoudre dans $\mathbb{Z}/15\mathbb{Z}$ l'équation $\bar{8}x = \bar{3}$.

$\overline{8}$ étant inversible d'inverse $\overline{2}$, il suffit de multiplier par $\overline{2}$ pour obtenir $x = \overline{6}$.

❑ Résoudre dans $\mathbb{Z}/15\mathbb{Z}$ l'équation $\overline{12}x = \overline{4}$.

On ne peut procéder de même ici. Il convient de revenir aux congruences :

$\overline{12}x = \overline{4}$

$\Leftrightarrow$ $\exists\, k,\ 12x = 4 + 15k$

Comme $12x - 15k$ est divisible par 3 et que 4 ne l'est pas, il n'y a pas de solution.

❑ Résoudre dans $\mathbb{Z}/15\,\mathbb{Z}$ l'équation $\overline{12}x = \overline{9}$.

On a maintenant :

$\overline{12}x = \overline{9}$

$\Leftrightarrow$ $\exists\, k,\ 12x = 9 + 15k$

$\Leftrightarrow$ $\exists\, k,\ 4x = 3 + 5k$

$\Leftrightarrow$ $\overline{4}x = \overline{3}$ dans $\mathbb{Z}/5\mathbb{Z}$

$\Leftrightarrow$ $-x = \overline{3}$ dans $\mathbb{Z}/5\mathbb{Z}$

$\Leftrightarrow$ $x = -\overline{3} = \overline{2}$ dans $\mathbb{Z}/5\mathbb{Z}$

$\Leftrightarrow$ $x \in \{\overline{2}, \overline{7}, \overline{12}\}$ dans $\mathbb{Z}/15\mathbb{Z}$

❑ Résoudre dans $\mathbb{Z}/15\,\mathbb{Z}$ l'équation $\overline{3}x = \overline{9}$.

On prendra garde que la solution n'est pas seulement $x = \overline{3}$, mais aussi $x = \overline{8}$ ou $x = \overline{13}$.

3- Fonction indicatrice d'Euler

Soit n entier strictement positif. On note $\varphi(n)$ le nombre d'éléments entre 1 et $n - 1$ premiers avec n. Il s'agit également du nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Cette fonction possède les propriétés suivantes.

PROPOSITION

(i) *Si p est premier, alors* $\varphi(p) = p - 1$

(ii) *Si p est premier, alors* $\varphi(p^k) = p^k - p^{k-1}$

(iii) *Si n et m sont premiers entre eux, alors* $\varphi(n)\varphi(m) = \varphi(nm)$.

(iv) *Si n se décompose en facteurs premiers sous la forme* $n = \prod_i p_i^{k_i}$, *alors* :

$$\varphi(n) = \prod_i (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_i (1 - \frac{1}{p_i})$$

Démonstration :

❑ a) résulte du fait que tous les entiers 1, 2, ..., $p - 1$ sont premiers avec p.

❑ b) résulte du fait que les entiers premiers avec p sont ceux qui ne possèdent pas p comme diviseurs. Aux p^k entiers 1, 2, ..., p^k, il convient donc de retirer $2p$, $3p$, ..., $(p^{k-1})p$, qui sont au nombre de p^{k-1}.

❑ c) : Ce point est le plus difficile. Commençons par montrer que, si a varie de 0 à $n-1$ et b de 0 à $m-1$, alors $am + bn$ mod mn prend mn valeurs différentes. En effet, si $am + bn \equiv a'm + b'n$ mod mn, alors il existe k tel que $am + bn = a'm + b'n + kmn$ ou encore :

$$(a - a')m = n(b' - b + km)$$

Donc n divise $(a - a')m$, et comme n est premier avec m, n divise $a - a'$ (théorème de Gauss, voir L1/ARITHMQ.PDF). Comme a et a' sont compris entre 0 et $n - 1$, la seule solution est $a = a'$. On a de même $b = b'$. Il en résulte que les valeurs prises par $am + bn$ mod mn sont toutes différentes. Comme a prend n valeurs et b en prend m, $am + bn$ mod mn en prend mn. Si on choisit le représentant de $am + bn$ mod mn entre 0 et $mn - 1$, il en résulte que tout entier entre 0 et $mn - 1$ est de la forme $am + bn$ mod mn. Et puisque tout entier possède un représentant entre 0 et $mn - 1$, tout entier est également de la forme $am + bn$ mod mn.

Montrons maintenant que, si a est premier avec n et b premier avec m, alors $am + bn$ mod mn est premier avec mn. En effet, si p est un diviseur premier de $am + bn$ et de mn, et donc par exemple de m, alors p divise $bn = (am + bn) - am$, mais p est premier avec n car m l'est, donc p divise b. Mais p divise alors b et m contrairement à l'hypothèse selon laquelle ces deux nombres sont premiers entre eux.

Réciproquement, tout élément premier avec mn peut se mettre sous la forme $am + bn$ mod mn, comme on l'a vu dans la première partie de la démonstration, mais de plus a est premier avec n et b avec m, car si par exemple a et n possède un diviseur commun p, alors p est aussi diviseur commun de $am + bn$ mod mn et de mn.

Ainsi, les $\varphi(mn)$ nombres premiers avec mn sont de la forme $am + bn$ mod mn avec a parcourant les $\varphi(n)$ valeurs premières avec n, et b parcourant les $\varphi(m)$ valeurs premières avec m. On a donc bien $\varphi(mn) = \varphi(m)\,\varphi(n)$. Une telle application φ est dite **multiplicative**.

d) En appliquant c) puis b), on a :

$$\varphi(n) = \varphi\left(\prod_i p_i^{k_i}\right) = \prod_i \varphi\left(p_i^{k_i}\right) = \prod_i \left(p_i^{k_i} - p_i^{k_i-1}\right)$$

EXEMPLE :

❑ Calculer $\varphi(15)$. On a :

$$\varphi(15) = \varphi(3 \times 5) = \varphi(3)\,\varphi(5) = 2 \times 4 = 8.$$

Si on reprend la démonstration du c) avec $m = 3$, $n = 5$, les entiers a compris entre 1 et $n - 1$ et premiers avec n sont 1, 2, 3, 4. Les entiers b compris entre 1 et $m - 1$ et premiers avec m sont 1 et 2. Les valeurs de $am + bn$ sont :

$1 \times 3 + 1 \times 5 = 8$
$1 \times 3 + 2 \times 5 = 13$
$2 \times 3 + 1 \times 5 = 11$
$2 \times 3 + 2 \times 5 = 16 \equiv 1 \bmod 15$
$3 \times 3 + 1 \times 5 = 14$
$3 \times 3 + 2 \times 5 = 19 \equiv 4 \bmod 15$
$4 \times 3 + 1 \times 5 = 17 \equiv 2 \bmod 15$
$4 \times 3 + 2 \times 5 = 22 \equiv 7 \bmod 15$

et on obtient bien tous les nombres compris entre 1 et $mn - 1$ et premiers avec 15.

4- Le petit théorème de Fermat

On généralise le petit théorème de Fermat vu dans L1/ARITHMTQ.PDF.

THEOREME

(i) *Si p est premier et si a n'est pas divisible par p, alors* $a^{p-1} \equiv 1 \bmod p$.

(ii) *Si n et a sont deux entiers premiers entre eux, alors* $a^{\varphi(n)} \equiv 1 \bmod n$, *où* φ *est la fonction indicatrice d'Euler.*

Démonstration :

❑ (i) n'est qu'un cas particulier de la seconde, lorsque $n = p$ est premier. On en trouvera une démonstration plus élémentaire dans L1/ARITHMTQ.PDF.

❑ (ii) : Il suffit de remarquer que, dans $\mathbb{Z}/n\mathbb{Z}$, l'ensemble des $\overline{x}$ avec x premier avec n forme un groupe multiplicatif d'ordre $\varphi(n)$. Dans ce groupe, l'ordre de $\overline{a}$ divise, d'après le théorème de Lagrange (voir L2/GROUPES.PDF), l'ordre du groupe. On a donc $\overline{a}^{\varphi(n)} = \overline{1}$ et donc $a^{\varphi(n)} \equiv 1 \bmod n$.

EXEMPLE :

❑ Prenons $n = 15 = 3 \times 5$, et $a = 8$. $\varphi(n) = 2 \times 4 = 8$, donc on a $8^8 \equiv 1 \bmod 15$, ce qu'on pourra vérifier directement.

5- Anneau intègre et corps

DEFINITION

On dit qu'un anneau A *est* **intègre** *s'il ne possède pas de diviseur de* 0.

Autrement dit, l'implication suivante est vérifiée, a et b étant des éléments quelconques de A :

$ab = 0 \Rightarrow a = 0$ ou $b = 0$

PROPOSITION

Il y a équivalence entre :

(i) *n est premier.*

(ii) $\mathbb{Z}/n\mathbb{Z}$ *est intègre.*

(iii) $\mathbb{Z}/n\mathbb{Z}$ *est un corps.*

On a vu par exemple que $\mathbb{Z}/15\mathbb{Z}$ n'est pas intègre, car $\overline{3} \times \overline{5} = \overline{0}$.

Démonstration :

❑ (i) $\Rightarrow$ (iii) : Si $\overline{a} \neq \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$, a n'est pas divisible par n, donc, n étant premier, a et n sont premiers entre eux. On a vu plus haut que, dans ce cas, $\overline{a}$ est inversible.

❑ (iii) $\Rightarrow$ (ii) : Tout corps est intègre, car si $\overline{a}\,\overline{b} = \overline{0}$, et si $\overline{a} \neq \overline{0}$, alors $\overline{a}$ admet un inverse, et en multipliant l'égalité par cet inverse, on obtient $\overline{b} = \overline{0}$.

❑ (ii) $\Rightarrow$ (i) : Par l'absurde, si n composé, alors $n = ab$ avec $1 < a < n$ et $1 < b < n$. Donc $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, mais pourtant $\overline{ab} = \overline{0}$.

On dispose donc, à côté des corps de nombres traditionnels $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, des corps de nombres $\mathbb{Z}/p\mathbb{Z}$ pour tout p premier. Ces corps ont la propriété d'être finis. La plupart des propriétés valides sur $\mathbb{R}$ ou $\mathbb{C}$ sont valides dans de tels corps, à quelques exception près. Par exemple, il n'y a plus d'identification possible entre polynôme formel et fonction polynomiale. La fonction $x \in \mathbb{Z}/2\mathbb{Z} \to x + x^2$ est identiquement nulle, alors que le polynôme formel $X + X^2$ est non nul de degré 2. Par contre, l'algorithme de division euclidienne des polynômes reste valide, ainsi que le fait qu'un polynôme de degré n admet au plus n racines.

6- Caractéristique d'un corps

Considérons un corps $\mathbb{K}$ et l'application $\psi : n \in \mathbb{Z} \to n1 \in \mathbb{K}$ où 1 désigne ici le neutre du produit de $\mathbb{K}$. $n1$ est la somme de 1 par lui-même n fois. ψ est un morphisme d'anneau. Il y a deux cas.

❑ Ou bien il est injectif, et dans ce cas, il se prolonge en un morphisme de $\mathbb{Q}$ dans $\mathbb{K}$ en posant $\psi(\frac{1}{n}) = (n1)^{-1}$ pour n non nul. Dans ce cas, $\mathbb{K}$ possède un sous-corps isomorphe à $\mathbb{Q}$. On dit que $\mathbb{K}$ est un corps de **caractéristique nulle**.

❑ Ou bien il n'est pas injectif et possède un noyau, idéal de $\mathbb{Z}$ et donc de la forme $n\mathbb{Z}$. Dans ce cas, de même que nous l'avons fait pour les morphismes de groupe de $\mathbb{Z}$ dans $\mathbb{Z}$, on montre que :

$$\overline{\psi} : \overline{x} \in \mathbb{Z}/n\mathbb{Z} \to x1 \in \mathbb{K}$$

est un morphisme de corps injectif. Autrement dit, $\mathbb{K}$ possède un sous-corps isomorphe à $\mathbb{Z}/n\mathbb{Z}$. n est nécessairement premier puisqu'un corps est intègre. Cet entier n est appelé **caractéristique** du corps $\mathbb{K}$. Elle est non nulle.

7- Le théorème des restes chinois

THEOREME

Soient n_1, n_2, ..., n_p des entiers premiers entre eux deux à deux, et x_1, ..., x_p des entiers quelconques. Alors il existe un entier x tel que, pour tout i, $x \equiv x_i \bmod n_i$. x est unique modulo $n_1n_2...n_p$.

Le même énoncé s'applique aux polynômes, en remplaçant ci-dessus le mot *entier* par le mot *polynôme*.

Démonstration :

❑ Considérons l'application :

$$\Phi : \mathbb{Z}/n_1n_2...n_p\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_p\mathbb{Z}$$
$$x \bmod n_1...n_p \to (x \bmod n_1, ..., x \bmod n_p).$$

Il est facile de montrer que c'est un morphisme de groupe additif (et même d'anneau). Montrons qu'elle est injective en cherchant son noyau :

$x \in \mathrm{Ker}(\Phi)$

$\Leftrightarrow$ $(x \bmod n_1, ..., x \bmod n_p) = (0, ..., 0)$

$\Leftrightarrow$ $n_1 \mid x, n_2 \mid x, ..., n_p \mid x$

$\Rightarrow$ $n_1n_2...n_p \mid x$ puisque les n_i sont premiers entre eux deux à deux

$\Rightarrow$ $x = 0 \bmod n_1n_2...n_p$.

Les deux ensembles $\mathbb{Z}/n_1n_2...n_p\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_p\mathbb{Z}$ ayant même cardinal et Φ étant injective, Φ est bijective. Donc, si on se donne $(x_1, ..., x_p) \in \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_p\mathbb{Z}$, il existe un unique x défini modulo $n_1n_2...n_p$ tel que, pour tout i, $x \equiv x_i \bmod n_i$.

Cette démonstration non constructive peut être complétée en donnant un moyen explicite de déterminer x. les nombres $n_2n_3...n_p$, $n_1n_3...n_p$, $n_1n_2n_4...n_p$, ..., $n_1...n_{i-1}n_{i+1}...n_p$, $n_1n_2...n_{p-1}$ sont premiers entre eux dans leur ensemble puisqu'un hypothétique diviseur commun premier p doit diviser l'un des n_i mais alors il ne peut diviser $n_1...n_{i-1}n_{i+1}...n_p$. D'après l'identité de Bézout appliqué à cette famille, il existe des entiers a_1, ..., a_n tels que l'on ait : $\sum_{i=1}^{p} a_i\, n_1...n_{i-1}n_{i+1}...n_p = 1$. Pour tout i, on a alors :

$$a_i\, n_1...n_{i-1}n_{i+1}...n_p \equiv 1 \bmod n_i$$

Ainsi, a_i est l'inverse de $n_1...n_{i-1}n_{i+1}...n_p$ dans $\mathbb{Z}/n_i\mathbb{Z}$.

Il suffit alors de prendre $x = \sum_{i=1}^{p} x_i\, a_i\, n_1...n_{i-1}n_{i+1}...n_p$.

EXEMPLE :

❑ Résoudre $\begin{cases} x \equiv 3 \bmod 15 \\ x \equiv 18 \bmod 35. \\ x \equiv 60 \bmod 77 \end{cases}$

Le système équivaut à $\begin{cases} x \equiv 3 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 18 \bmod 5 \\ x \equiv 18 \bmod 7 \\ x \equiv 60 \bmod 7 \\ x \equiv 60 \bmod 11 \end{cases}$ (la réciproque utilise le fait que $3 \wedge 5 = 1$, $5 \wedge 7 = 1$ et $7 \wedge 11 = 1$), ou plus simplement à $\begin{cases} x \equiv 0 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 7 \\ x \equiv 5 \bmod 11 \end{cases}$. On prend ici $n_1 = 3$, $n_2 = 5$, $n_3 = 7$ et $n_4 = 11$. Les $n_1...n_{i-1}n_{i+1}...n_p$ valent respectivement 385, 231, 165 et 105. Une identité de Bézout vérifiée par ces nombres peut être obtenue de la façon suivante. On cherche d'abord l'identité de Bézout entre 385 et 231 de PGCD 77 :

$$-385 + 2 \times 231 = 77$$

puis on cherche une identité de Bézout entre 77 et 165 de PGCD 11 :

$$-2 \times 77 + 165 = 11$$

Enfin, on cherche une identité de Bézout entre 11 et 105, premiers entre eux :

$$-19 \times 11 + 2 \times 105 = 1$$

Donc finalement :

$$\begin{aligned} 1 &= -19 \times 11 + 2 \times 105 = -19(-2 \times 77 + 165) + 2 \times 105 \\ &= 38 \times 77 - 19 \times 165 + 2 \times 105 \\ &= 38 \times (-385 + 2 \times 231) - 19 \times 165 + 2 \times 105 \\ &= -38 \times 385 + 76 \times 231 - 19 \times 165 + 2 \times 105 \end{aligned}$$

donc $a_1 = -38$, $a_2 = 76$, $a_3 = -19$, $a_4 = 2$. La solution du système est :

$$x = 3 \times 76 \times 231 - 4 \times 19 \times 165 + 5 \times 2 \times 105 = 41178 \equiv 753 \bmod 1155.$$

❑ On peut aussi résoudre le système initial précédent équation par équation :

$$x \equiv 3 \bmod 15 \Leftrightarrow \exists\, k,\ x = 3 + 15k$$

puis $3 + 15k \equiv 18 \bmod 35 \Leftrightarrow 15k \equiv 15 \bmod 35 \Leftrightarrow 3k \equiv 3 \bmod 7 \Leftrightarrow k \equiv 1 \bmod 7$ (3 est inversible dans $\mathbb{Z}/7\mathbb{Z}$), donc $\exists\, m$, $k = 1 + 7m$ donc $x = 18 + 105m$

puis $18 + 105m \equiv 60 \bmod 77 \Leftrightarrow 105m \equiv 42 \bmod 77 \Leftrightarrow 15m \equiv 6 \bmod 11 \Leftrightarrow 4m \equiv 6 \bmod 11$
$\Leftrightarrow 3 \times 4m \equiv 3 \times 6 \bmod 11 \Leftrightarrow m \equiv 18 \bmod 11 \equiv 7 \bmod 11$ donc $\exists\, n,\ m = 7 + 11n$
donc $x = 18 + 7 \times 105 + 1155n = 753 + 1155n$

Annexe I : Corps finis

Nous avons vu que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier. Nous donnons ici d'autres exemples de corps finis.

De même qu'on construit $\mathbb{C}$ à partir de $\mathbb{R}$ en introduisant un symbole i racine de $X^2 + 1$, on construit des corps finis à partir de $\mathbb{Z}/p\mathbb{Z}$ en introduisant un symbole α racine d'un polynôme irréductible sur $\mathbb{Z}/p\mathbb{Z}$. Nous prendrons, dans la suite de ce paragraphe, le cas $p = 2$, bien adapté au calcul binaire sur ordinateur. On détermine ci-dessous des polynômes irréductibles sur $\mathbb{Z}/2\mathbb{Z}$, en partant des deux polynômes élémentaires X et 1 + X, puis en classant les polynômes de degré supérieur suivant qu'on les obtient comme produit de polynômes de degré plus faible (ils sont réductibles) ou pas (ils sont irréductibles). On obtient ainsi :

degré	polynômes réductibles	polynômes irréductibles
1		X, $X+1$
2	X^2, $X^2+X = X(X+1)$, $X^2+1 = (X+1)^2$	X^2+X+1
3	$XP(X)$ (4 polynômes) $X^3+1 = (X+1)(X^2+X+1)$ $X^3+X^2+X+1 = (X+1)^3$	X^3+X^2+1 X^3+X+1
4	$XP(X)$ (8 polynômes) $X^4+1 = (X+1)^4$ $X^4+X^3+X+1 = (X+1)^2(X^2+X+1)$ $X^4+X^2+X+1 = (X+1)(X^3+X^2+1)$ $X^4+X^3+X^2+1 = (X+1)(X^3+X+1)$ $X^4+X^2+1 = (X^2+X+1)^2$	$X^4+X^3+X^2+X+1$ X^4+X^3+1 X^4+X+1
5	$XP(X)$ (16 polynômes) $(X+1)P(X)$ (8 autres polynômes) $X^5+X+1 = (X^2+X+1)(X^3+X^2+1)$ $X^5+X^4+1 = (X^2+X+1)(X^3+X+1)$	$X^5+X^4+X^3+X^2+1$ $X^5+X^4+X^3+X+1$ $X^5+X^4+X^2+X+1$ $X^5+X^3+X^2+X+1$ X^5+X^3+1 X^5+X^2+1

etc.

7	...	X^7+X^3+1 par exemple

On définit alors :

- $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ avec α racine de $X^2 + X + 1$, donc $\alpha^2 + \alpha + 1 = 0$, ou bien $\alpha^2 = \alpha + 1$ (puisque les calculs se font modulo 2). On a alors :

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\} = \{0, 1, \alpha, 1 + \alpha\}$

On constate que les éléments de $\mathbb{F}_4$ peuvent s'exprimer aussi bien comme polynôme de α de degré strictement inférieur à celui du polynôme irréductible, mais aussi comme puissance de α (en dehors de l'élément nul). Cette propriété est générale. On peut montrer que, pour tous les degrés, il existe un polynôme irréductible et une racine α de ce polynôme tel que les éléments du corps peuvent s'exprimer soit comme polynôme en α, soit comme puissance de α (sauf le 0). On peut montrer par ailleurs que, à isomorphisme près, un corps fini est déterminé par son nombre d'éléments.

❑ $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ avec $\alpha^3 = \alpha + 1$, en prenant α racine du polynôme irréductible $X^3 + X + 1$. Les éléments de $\mathbb{F}_8$ sont :

0
1
α
α^2
$\alpha^3 = \alpha + 1$
$\alpha^4 = \alpha^2 + \alpha$
$\alpha^5 = \alpha^2 + \alpha + 1$
$\alpha^6 = \alpha^2 + 1$

On a $\alpha^7 = 1$.
Les racines de $X^3 + X + 1$ sont α, α^2, α^4.
Les racines de $X^3 + X^2 + 1$ sont α^3, α^5, α^6.

❑ $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ avec $\alpha^4 = \alpha + 1$. Les éléments de $\mathbb{F}_{16}$ sont :

0
1
α
α^2
α^3
$\alpha^4 = \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$
$\alpha^6 = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha^3 + \alpha + 1$
$\alpha^8 = \alpha^2 + 1$
$\alpha^9 = \alpha^3 + \alpha$
$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^{14} = \alpha^3 + 1$

On a $\alpha^{15} = 1$.
Les racines de $X^4 + X^3 + X^2 + X + 1$ sont α^3, α^6, α^9 et α^{12}.
Les racines de $X^4 + X^3 + 1$ sont α^7, α^{11}, α^{13} et α^{14}.
Les racines de $X^4 + X + 1$ sont α, α^2, α^4 et α^8

etc.

❑ $\mathbb{F}_{128} = \mathbb{F}_2[\alpha]$ avec $\alpha^7 = \alpha^3 + 1$. Les éléments de $\mathbb{F}_{128}$ sont de la forme $a_0\alpha^6 + a_1\alpha^5 + ... + a_5\alpha + a_6$, les a_i étant éléments de $\mathbb{F}_2$, et sont aussi (en dehors de 0) les puissances de α, depuis $1 = \alpha^0$ jusqu'à α^{126}. On a $\alpha^{127} = 1$.

Annexe II : Utilisation d'un corps fini dans le codage des transmissions

Le Minitel était un objet de la fin du XXème qui a précédé l'introduction d'internet en France. Malgré sa désuétude, son mode de communication est représentatif de procédés toujours utilisés

actuellement dans tous les moyens de transmission numérique moderne (téléphone portable, téléviseur, internet ...). Les messages envoyés par Minitel étaient codés de façon à pouvoir détecter une erreur et la corriger. Pour cela, on utilise $\mathbb{F}_{128}$, corps fini possédant 128 éléments. $\mathbb{F}_{128}$ a été défini dans l'annexe précédente comme étant égal à $\mathbb{F}_2[\alpha]$, avec $\alpha^7 = \alpha^3 + 1$.

Pour envoyer un message de 15 octets (soit $15 \times 8 = 120$ chiffres binaires ou bits) de la forme $M = b_0 b_1 ... b_{119}$, où les b_i sont des éléments de $\mathbb{F}_2$, on considère l'élément de $\mathbb{F}_{128}$ égal à :

$$T = b_0 \alpha^{126} + ... + b_{119} \alpha^7 = \sum_{k=0}^{119} b_k \alpha^{126-k}$$

Il existe des éléments b_{120}, b_{121}, ..., b_{126} de $\mathbb{F}_2$ tels que cet élément puisse s'exprimer sous la forme $b_{120} \alpha^6 + ... + b_{125} \alpha + b_{126}$. On envoie alors le message $b_0 b_1 ... b_{119} b_{120} ... b_{126}$, soit 127 bits. (Si on ajoute également un bit de parité prévu pour que le nombre total de bits égaux à 1 soit pair, on obtient exactement 16 octets. Nous n'en tenons pas compte ici). Le message envoyé correspond donc dans $\mathbb{F}_{128}$ au nombre :

$$S = b_0 \alpha^{126} + ... + b_{119} \alpha^7 + b_{120} \alpha^6 + ... + b_{125} \alpha + b_{126} = T + T = (1 + 1)T = 0$$

(qui est nul puisque $1 + 1 = 0$ dans $\mathbb{F}_2$). Le message reçu est :

$$S' = b'_0 \alpha^{126} + ... + b'_{119} \alpha^7 + b'_{120} \alpha^6 + ... + b'_{125} \alpha + b'_{126}$$

où certains b_i sont susceptibles d'avoir été changés en b'_i à la suite d'une erreur de transmission. Les 120 premiers bits $b'_0 ... b'_{119}$ forme un message M' que l'on souhaite être égal au message initial M.

A l'arrivée, on calcule S' dans $\mathbb{F}_{128}$. Si $S' = 0$, on considère qu'il n'y a pas eu d'erreur de transmission et que M' = M. Sinon, on suppose que les erreurs de transmission sont suffisamment rares pour qu'une seule erreur se soit produite, par exemple au bit k. On a donc :

$b'_i = b_i$ pour $i \neq k$

$b'_k = b_k + 1 \bmod 2$

De sorte que $S' = S + \alpha^{126-k} = \alpha^{126-k}$ puisque $S = 0$. Or connaissant la valeur de S' (il y a 127 valeurs possibles non nulles dans $\mathbb{F}_{128}$), il suffit de déterminer parmi les 127 puissances possibles distinctes de α celle qui est égale à la valeur de S'. Une et une seule puissance de α convient. L'indice k correspondant permet de corriger l'erreur de transmission.

La démarche suivie par le Minitel avec $\mathbb{F}_{128}$ peut s'appliquer avec n'importe quel corps du même type. Si le corps possède 2^n éléments, on envoie des messages M constitués de $2^n - n - 1$ bits. Ceux-ci sont complétés par n bits. Le choix de 2^{128} est astucieux, car il permet de coder 15 octets par un octet supplémentaire.

Voici des exemples plus élémentaires et abordables manuellement :

❑ Dans $\mathbb{F}_4$, avec $\alpha^2 = \alpha + 1$.

On souhaite transmettre le message $M = a_0$. Or $a_0 \alpha^2 = a_0(\alpha + 1)$. D'où :

$S = a_0\alpha^2 + a_0\alpha + a_0 = 0$

On envoie donc le message $a_0 a_0 a_0$. αinsi :

0 est codé 000

1 est codé 111

S'il y a une erreur, elle est facile à corriger. Ce code est peu performant, il multiplie la longueur des messages par 3.

❑ Dans $\mathbb{F}_8$ avec $\alpha^3 = \alpha + 1$

On souhaite transmettre le message M = $a_0a_1a_2a_3$. Il correspond au polynôme :

$$a_0\alpha^6 + a_1\alpha^5 + a_2\alpha^4 + a_3\alpha^3 = \alpha^2(a_0 + a_1 + a_2) + \alpha(a_1 + a_2 + a_3) + (a_0 + a_1 + a_3)$$

On envoie donc le message : $a_0a_1a_2a_3[a_0 + a_1 + a_2][a_1 + a_2 + a_3][a_0 + a_1 + a_3]$

Par exemple, on veut envoyer 0110. On envoie en fait 0110001.

On reçoit 0111001 = $\alpha^5 + \alpha^4 + \alpha^3 + 1 = \alpha^3$ $\Rightarrow$ erreur sur a_3

On reçoit 0110101 = $\alpha^5 + \alpha^4 + \alpha^2 + 1 = \alpha^2$ $\Rightarrow$ erreur sur a_4

On reçoit 0100011 = $\alpha^5 + \alpha + 1 = \alpha^2$ $\Rightarrow$ erreur sur a_4 (Il y a en fait deux erreurs)

On reçoit 0010001 = $\alpha^4 + 1 = \alpha^2 + \alpha + 1 = \alpha^5$ $\Rightarrow$ erreur sur a_1.

Dans le cas de $\mathbb{F}_8$ qui n'est pas très gros, on peut comprendre à la main pourquoi la recherche d'une erreur sera possible. Notons :

$$A = a_0,\ B = a_1,\ C = a_2,\ D = a_3,\ E = a_0 + a_1 + a_2,\ F = a_1 + a_2 + a_3,\ G = a_0 + a_1 + a_3$$

Le message est constitué de ABCD, le code correcteur de EFG. On voit que celui-ci a été construit de façon que :

(i) A + B + C + E = 0

(ii) B + C + D + F = 0

(iii) A + B + D + G = 0

Si ces trois égalités sont en défaut, cela signifie qu'une erreur porte sur B

Si les égalités (i) et (ii) sont en défaut, l'erreur porte sur C

Si les égalités (i) et (iii) sont en défaut, l'erreur porte sur A

Si les égalités (ii) et (iii) sont en défaut, l'erreur porte sur D

Si l'égalité (i) seule est en défaut, l'erreur porte sur E

Si l'égalité (ii) seule est en défaut, l'erreur porte sur F

Si l'égalité (iii) seule est en défaut, l'erreur porte sur G

Plus généralement, l'utilisation de k bits de corrections conduit à la mise au point de k telles égalités. Si les k égalités sont vérifiées, le message est considéré comme correct. Si un sous-ensemble de p lignes est en défaut, pour $1 \le p \le k$, cela permettra de corriger un bit du message, chaque bit correspondant à l'un des sous-ensembles. Le nombre total de bits du message pouvant être utilisés est donc :

$$\sum_{p=1}^{k} \binom{k}{p} = 2^k - 1$$

Sur ces $2^k - 1$ bits, k serviront de bits correcteurs, les $2^k - k - 1$ autres servant à transmettre le message. On peut ajouter 1 bit de parité à la fin afin d'obtenir un mot de longueur 2^k. Cela permet de détecter la présence de deux erreurs (mais sans qu'on puisse les corriger). Ci-dessous, on indique, pour diverses valeurs de k, le nombre de bits signifiants du message ($2^k - k - 1$), le nombre de bits correcteurs (k), le nombre de bits d'un mot ($2^k - 1$). Le minitel utilisait $k = 7$. Bien entendu, comme k est négligeable devant 2^k quand il augmente indéfiniment, plus k est grand, plus le rapport $\frac{\text{Nombre de bits correcteurs}}{\text{Longueur du message}}$ est faible. On peut alors être tenté de prendre k arbitrairement grand, mais on n'oubliera pas que la méthode précédente suppose qu'il y a au plus une erreur par mot, et que plus le mot est grand, plus il y a de chances d'avoir plus d'une erreur de transmission. La valeur de k sera donc choisie en fonction de la qualité du canal de transmission.

Nombre de bits correcteurs k	Nombre de bits signifiants $2^k - k - 1$	Longueur du mot $2^k - 1$
2	1	3
3	4	7
4	11	15
5	26	31
6	57	63
7	120	127

Ci-dessous, une méthode encore plus performante : la correction d'erreurs dans les disques compacts.

Annexe III : Utilisation d'un corps fini dans les disques compacts

Un octet étant une suite de huit chiffres binaires 0 ou 1, il y a 256 octets différents qu'on peut représenter par les nombres 0 à 255 ou par les éléments de $\mathbb{F}_{256}$, corps fini à 256 éléments. La construction de tels corps finis est expliquée dans l'annexe I. En ce qui concerne $\mathbb{F}_{256}$, on a $\mathbb{F}_{256} = \mathbb{F}_2[\alpha]$ où α est un symbole vérifiant :

$$\alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1 = 0$$

Les éléments de $\mathbb{F}_{256}$ sont de la forme $a_0 + a_1\alpha + ... + a_7\alpha^7$, avec a_i valant 0 ou 1. Il y a bien $2^8 = 256$ éléments possibles. On peut également vérifier qu'on obtient tous les éléments de $\mathbb{F}_{256}$ sous la forme α^k, $0 \le k \le 254$, auxquels on adjoint le 0. On a $\alpha^{255} = 1$. On a par exemple :

$$\alpha^{20} = \alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$$

Considérons un mot M constitué de r octets, où r est inférieur ou égal à 251. En adjoignant 4 octets formant un code C, on obtient un mot MC de $r + 4$ octets. C est défini de façon que si, lors de la transmission ou de la lecture de MC, on commet deux erreurs, on est capable de les localiser et de les rectifier. Si quatre octets de MC sont illisibles, on sait également les reconstituer. Comment s'y prend-on ? Supposons que M soit de la forme $[a_0, a_1, ..., a_{r-1}]$, avec a_i élément de $\mathbb{F}_{256}$ (chaque a_i est un octet). On considère M comme un polynôme $a_0 + a_1X + ... + a_{r-1}X^{r-1}$. On multiplie ce polynôme par $(X + \alpha)(X + \alpha^2)(X + \alpha^3)(X + \alpha^4)$ ce qui donne un polynôme de degré $r + 3$ possédant $r + 4$ coefficients. Ces coefficients forment les composantes de MC. MC peut donc être vu ou bien comme une suite particulière de $r + 4$ octets (ou éléments de $\mathbb{F}_{256}$), ou bien comme un polynôme MC(X) de degré $r + 3$ à coefficients dans $\mathbb{F}_{256}$ possédant les racines α, α^2, α^3 et α^4.

❑ Supposons que deux erreurs au plus se produisent dans la transmission de MC, cela signifie qu'on reçoit ou qu'on lit non le polynôme MC(X), mais $R(X) = MC(X) + kX^i + lX^j$, où $0 \le i \le j \le r + 3$ et k ou l non nul. Si on note $b_1 = R(\alpha)$, $b_2 = R(\alpha^2)$, $b_3 = R(\alpha^3)$ et $b_4 = R(\alpha^4)$ la valeur en α, α^2, α^3 et α^4 du polynôme reçu, on obtient le système suivant :

$$(I)\begin{cases} k\alpha^i + l\alpha^j = b_1 \\ k\alpha^{2i} + l\alpha^{2j} = b_2 \\ k\alpha^{3i} + l\alpha^{3j} = b_3 \\ k\alpha^{4i} + l\alpha^{4j} = b_4 \end{cases}$$

où b_1, b_2, b_3 et b_4 sont connus, mais k, l, i et j sont inconnus. On va voir qu'on est capable de les déterminer. On vérifiera que (on rappelle qu'on calcule modulo 2) :

$$\text{(II)} \begin{cases} (\alpha^i + \alpha^j)b_2 + \alpha^{i+j}b_1 = b_3 \\ (\alpha^i + \alpha^j)b_3 + \alpha^{i+j}b_2 = b_4 \end{cases}$$

Voyons le système (II) comme celui de deux équations aux deux inconnues $S = \alpha^i + \alpha^j$ et $P = \alpha^{i+j}$ et de coefficients $\begin{pmatrix} b_2 & b_1 \\ b_3 & b_2 \end{pmatrix}$.

Si le déterminant $\begin{vmatrix} b_2 & b_1 \\ b_3 & b_2 \end{vmatrix}$ est non nul, on déduit du système (II) les valeurs de $S = \alpha^i + \alpha^j$ et $P = \alpha^i\alpha^j$. α^i et α^j sont racines de $X^2 + SX + P$. On en tire α^i et α^j en résolvant cette équation du second degré, puis on en déduit i et j. Il est facile ensuite d'avoir k et l. On est donc capable de détecter deux erreurs et de les corriger.

Si le déterminant $\begin{vmatrix} b_2 & b_1 \\ b_3 & b_2 \end{vmatrix}$ est nul, on a (on rappelle que 2 = 0 dans $\mathbb{F}_{256}$) :

$$0 = \begin{vmatrix} b_2 & b_1 \\ b_3 & b_2 \end{vmatrix} = {b_2}^2 + b_1b_3 = kl\alpha^i\alpha^j(\alpha^{2i} + \alpha^{2j}) \qquad \text{(en utilisant les valeurs des } b_i \text{ dans (I))}$$

Donc $k = 0$ ou $l = 0$ ou $\alpha^{2i} = \alpha^{2j}$. Dans ce dernier cas, on aurait $\alpha^{2i-2j} = 1$ ou $2i - 2j$ multiple de 255 (car seul $\alpha^{255} = 1$) donc $i - j$ multiple de 255 et donc $i = j$ (car $|i - j| \leq r + 3 < 255$). Dans tous les cas, cela signifie qu'il n'y a qu'une seule erreur de commise. On peut supposer que l'erreur porte sur l'octet i uniquement avec $k \neq 0$, et que $l = 0$. On utilise alors seulement les deux premières équations du système (I) : $\begin{cases} k\alpha^i = b_1 \\ k\alpha^{2i} = b_2 \end{cases}$ pour en déduire que $k = \dfrac{{b_1}^2}{b_2}$ et que $\alpha^i = \dfrac{b_2}{b_1}$ d'où on tire i. L'erreur est ainsi déterminée et peut être corrigée.

❑ Supposons maintenant que quatre octets quelconques de MC soient illisibles. Ils sont localisés en i_1, i_2, i_3 et i_4. Attribuons à ces octets provisoirement la valeur 0. Notons R le message MC ainsi modifié. Il s'agit alors de déterminer k_1, k_2, k_3 et k_4 tels que :

$$\begin{cases} k_1\alpha^{i_1} + k_2\alpha^{i_2} + k_3\alpha^{i_3} + k_4\alpha^{i_4} = R(\alpha) \\ k_1\alpha^{2i_1} + k_2\alpha^{2i_2} + k_3\alpha^{2i_3} + k_4\alpha^{2i_4} = R(\alpha^2) \\ k_1\alpha^{3i_1} + k_2\alpha^{3i_2} + k_3\alpha^{3i_3} + k_4\alpha^{3i_4} = R(\alpha^3) \\ k_1\alpha^{4i_1} + k_2\alpha^{4i_2} + k_3\alpha^{4i_3} + k_4\alpha^{4i_4} = R(\alpha^4) \end{cases}$$

A la différence du cas précédent, les valeurs i_1, ..., i_4 sont connues. Il suffit alors de résoudre le système pour déterminer k_1, ..., k_4. On est donc capable de remédier à quatre effacements.

Voyons maintenant comment cet outil est utilisé pour corriger les incidents de lecture de disques compacts. Les informations continues dans ces disques sont codées par paquets de 24 octets. On leur adjoint 4 octets comme précédemment pour pouvoir corriger deux erreurs ou quatre effacements. On obtient ainsi des mots de 28 octets, le $i^{\text{ème}}$ mot étant noté MC[i]. Le $k^{\text{ème}}$ octet de ce mot ($1 \leq k \leq 28$) sera noté MC[i,k]. Mais les octets de chaque mot ne sont pas enregistrés à la suite. Ils sont entrelacés avec les octets de plusieurs autres mots de la façon suivante. Pour un indice i donné, on enregistre à la suite les octets suivants :

MC[i,1] MC[i – 4,2] MC[i – 8,3] ... MC[i – 108,28]

Appelons ligne d'indice i cette suite de 28 octets. Chacune de ces lignes est elle-même renforcée par 4 octets permettant là aussi de corriger deux erreurs ou quatre effacements, donnant en fait des lignes de 32 octets.

Supposons que seize lignes successives soient complètement effacées (ce qui représente $16 \times 32 = 512$ octets successifs effacés). Les mots MC[i] ne faisant intervenir les lignes que tous les

quatre rangs, la reconstitution de MC[*i*] ne laissera que quatre octets effacés. On est capable alors de reconstituer chaque mot MC. Ainsi, on est capable de réparer l'effacement de 512 octets successifs. La densité d'information sur un CD étant de l'ordre de 2 ko par cm de piste, on peut donc se permettre des rayures transversales de 2 mm de large.

Annexe IV : Cryptographie

1- Chiffrement de messages avec clef publique

Vous souhaitez recevoir d'un correspondant un message confidentiel. Un seul moyen, chiffrer le message. Dans les communications numériques, il est fait abondamment usage des chiffrements dits à clef publique (ou à clef révélée). De quoi s'agit-il ?

Une personne B veut recevoir un message confidentiel M d'une personne A. La personne B rend public (dans un annuaire spécialisé, par exemple) un procédé de chiffrement C_B. Ce procédé est donc connu de tous. La personne B est la seule à posséder le procédé de déchiffrement D_B. La personne A, expéditrice du message M, envoie le message $C_B(M)$. La personne B, destinataire du message n'a plus qu'à appliquer son procédé de déchiffrement : $D_B(C_B(M)) = M$. Autrement dit, $D_B \circ C_B = Id$.

Procédé général de chiffrement à clef publique C_B

Personne A
Message M à transmettre à B

↓

$C_B(M)$ chiffré

↓

Personne B
Procédé de déchiffrement privé D_B
$D_B(C_B(M)) = M$ déchiffré

Le point fondamental est le suivant : comment est-il possible que le procédé de déchiffrement D_B reste secret, et uniquement connu de la personne B, alors que le procédé de chiffrement C_B est public ? Cela est possible car la connaissance d'une fonction *f* bijective ne suffit pas toujours pour calculer simplement sa réciproque. Une telle fonction est appelée **fonction trappe**. On en connaît plusieurs. Il n'est pas exclu que des fonctions trappes aujourd'hui cessent de le devenir demain, la difficulté de calculer f^{-1} étant essentiellement due à notre ignorance. Mais il n'est pas exclu non plus que l'on puisse prouver qu'une fonction est par nature une fonction trappe, le calcul de f^{-1} étant alors intrinsèquement difficile. Une fonction trappe actuelle est le calcul du logarithme discret. Etant donné trois nombres *a*, *b* et *p*, on sait facilement calculer a^b mod *p* (le temps de calcul est de l'ordre de ln(*b*), cf L1/ALGO1.PDF). Mais connaissant *a*, a^b et *p*, on ne connaît pas de méthode rapide de calculer *b*. Lorsque les nombres en question possèdent plusieurs dizaines de chiffres, la méthode consistant à essayer toutes les valeurs possibles de *b* prend trop de temps (il est de l'ordre de *b*). Il existe cependant des algorithmes efficaces si $p - 1$ possède de petits facteurs premiers. Le choix de *p* pour définir une bonne fonction trappe est donc crucial.

EXEMPLES :

❑ Le premier exemple est le système de **ElGamal**. La personne B souhaitant recevoir des messages choisit un nombre premier *q* et choisit secrètement un nombre *a*. Tous les calculs sont effectués

modulo q. Il publie g élément de $[\![1, q-1]\!]$, q et $g^a \bmod q$. Pour envoyer un message M élément de $[\![1, q-1]\!]$ à B, on choisit un entier k au hasard et on envoie le couple $(g^k, Mg^{ak}) \bmod q$. Connaissant a, B peut calculer facilement $g^{ak} = (g^k)^a \bmod q$ à partir de la première composante du couple reçu, et donc déduire la valeur de M à partir de la deuxième composante. Par contre, on ne connait pas actuellement de moyen efficace de calculer a connaissant g et g^a modulo q.

Procédé de chiffrement ElGamal, $C_B = (g, q, g^a \bmod q)$ *est publié par* B

Personne A
Message M à transmettre à B
choix d'un nombre k au hasard

↓

$(g^k, Mg^{ak}) \bmod q = (x, y)$

↓

Personne B
Nombre a privé
$y/x^a \bmod q$ = M déchiffré

En ce qui concerne le calcul de puissance modulo un entier, il est maladroit de calculer la puissance d'abord avant de faire la réduction modulo l'entier, car le calcul de puissance peut conduire à des nombres entiers très grands. Les deux opérations doivent se faire conjointement.

❑ Voici un autre exemple classique de cryptographie, le système **RSA** (Rivest-Shamir-Adleman). La personne B choisit en secret deux nombres premiers p et q, ainsi qu'un nombre d, premier avec $(p-1)(q-1)$. Il rend public $n = pq$, et m positif ou nul tel que md soit de la forme $1 + k(p-1)(q-1)$ (ce qui est possible grâce à l'identité de Bézout).

Procédé de chiffrement C_B : Découper le message en groupe de lettres et remplacer chaque lettre par un nombre (par exemple, son rang dans l'alphabet), de façon que le message à transmettre soit une suite de nombres M inférieurs à n. Transmettre les nombres $M' = M^m \bmod n$.
Procédé de déchiffrement D_B : Calculer $M'^d \bmod n$.
Montrons que le résultat est M.
Si M est divisible par p et q, alors $M \equiv 0 \bmod n$, donc M' puis M'^d aussi, donc $M'^d \equiv M \bmod n$.
Si M est divisible par p et est premier avec q, alors on a :

$M'^d \equiv M^{md} \bmod p = 0 \equiv M \bmod p$

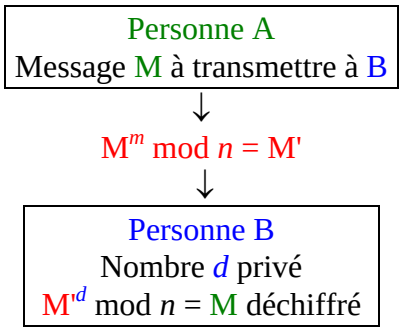
et $M'^d \equiv M^{md} \bmod q = M^{1+k(p-1)(q-1)} \equiv M \bmod q$

car, d'après le théorème de Fermat, on a $M^{q-1} \equiv 1 \bmod q$. On en conclut que p et q divisent $M'^d - M$, et comme p et q sont premiers entre eux, il en est de même de leur produit n. Donc $M'^d \equiv M \bmod n$.
Si M est premier avec p et q, alors il est premier avec n. Donc le théorème de Fermat affirme dans ce cas que $M^{\varphi(n)} \equiv 1 \bmod n$, où φ est la fonction indicatrice d'Euler, avec :

$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q)$ car $p \wedge q = 1$
$= (p-1)(q-1)$ car p et q sont premiers

donc $M^{(p-1)(q-1)} \equiv 1 \bmod n$
donc $M'^d \equiv M^{md} = M^{1+k(p-1)(q-1)} \equiv M \bmod n$

Procédé de chiffrement RSA, $C_B = (n, m)$ *est publié par* B



Prenons un exemple avec des petits nombres :

$p = 5$
$q = 11$
$n = 55$
$(p - 1)(q - 1) = 40$
$d = 23$
$m = 7$
$md = 161 = 1 + 4(p - 1)(q - 1)$

$n = 55$ et $m = 7$ sont rendus publics. On veut envoyer le message M = 17.
On expédie $M' \equiv M^7 \bmod 55 = 8$
On décode $M'^{23} \bmod 55$. On retrouve bien M = 17.

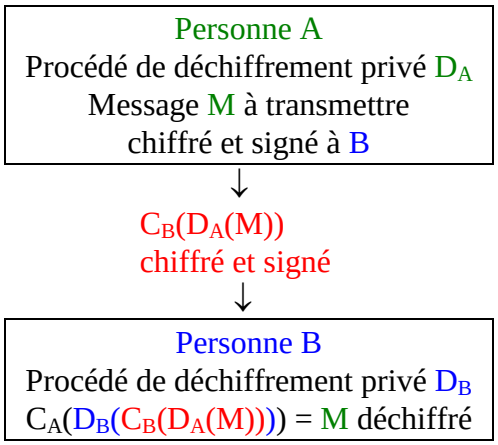
Voyons pourquoi il est si difficile en général de déchiffrer D_B. On travaille avec des nombres p et q d'une cinquantaine de chiffres. On sait déterminer sur ordinateur en quelques minutes si un nombre est premier ou pas. Le choix de p et q ne pose donc pas de problèmes. On sait également déterminer en quelques minutes le PGCD de deux nombres. Il en découle un choix facile de d. Les coefficients du théorème de Bézout se calcule aussi rapidement, d'où la découverte rapide de m.

Par contre, le produit n étant donné, on ne connaît pas d'algorithme rapide de factorisation de n. Si n compte une centaine de chiffres, on estime que le temps nécessaire à la découverte de p et q est actuellement de l'ordre de plusieurs milliard d'années. La connaissance de C_B, et donc de n ne suffit pas, et de loin, pour déterminer p et q, et donc D_B.

Cette méthode permet également d'identifier de façon certaine l'auteur d'un message si chacun a sa propre procédure de chiffrement et de déchiffrement RSA. Il suffit que l'expéditeur A envoie le message $C_B(D_A(M))$, qu'il est seul à pouvoir envoyer, puisqu'il est le seul à connaître son propre procédé de déchiffrement D_A. Le destinataire B applique alors sur le message reçu $C_A \circ D_B$. En effet, il est facile de voir que, dans le cas du chiffrement RSA, les procédés de chiffrement C_A et de déchiffrement D_A commutent, et que l'on a donc :

$$C_A \circ D_B \circ C_B \circ D_A(M) = C_A \circ D_A(M) = D_A \circ C_A(M) = M$$

Procédé général de chiffrement RSA *avec authentification de la signature,* C_A *et* C_B *sont publics*

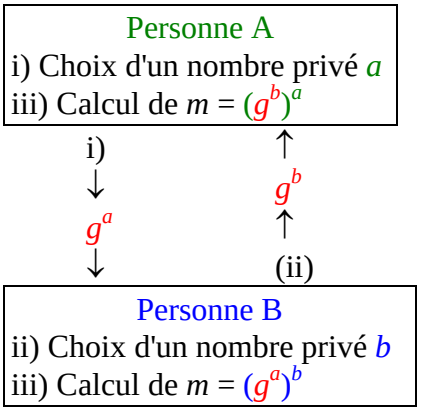


Ces méthodes de chiffrement sont tellement efficaces que les gouvernements ont promulgués des lois visant à limiter la taille des nombres p et q.

2- Quelques problèmes de transmission confidentielle

❑ Deux personnes A et B, éloignées l'une de l'autre, veulent convenir d'un nombre commun, qui pourra par exemple leur servir ultérieurement de clef pour s'envoyer des messages codés. Ils peuvent se téléphoner ou s'écrire, mais rien ne garantit la confidentialité de leurs échanges. Comment faire ? Là aussi, on utilise des fonctions trappes au moyen du protocole de **Diffie et Hellman**. Diffie et Hellman ont en effet présumé qu'il était infaisable, avec les connaissances actuelles, de calculer un nombre de la forme g^{ab} mod q, connaissant g, g^a mod q et g^b mod q, lorsque g, a et b sont grands. Ceci est une variante du problème du logarithme discret.
Il suffit donc à A et à B de se communiquer (éventuellement publiquement) les nombres g et q.
i) A choisit secrètement un nombre a et envoie à B le nombre g^a.
ii) De même, B choisit secrètement un nombre b et envoie à A le nombre g^b.
iii) A et B peuvent alors tous deux calculer facilement $g^{ab} = (g^b)^a = (g^a)^b$, mais personne d'autre ne le peut.

Protocole de Diffie-Hellmann *pour convenir d'un nombre commun.*
g et q sont communs à A *et à* B.

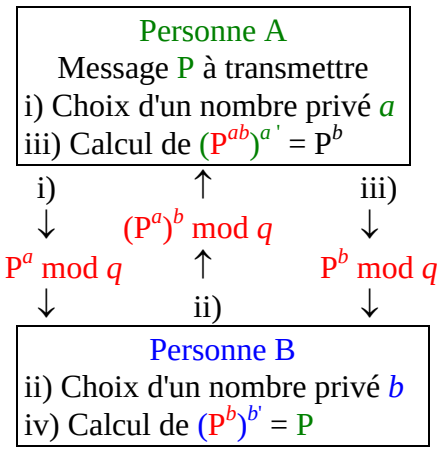


❑ Dans un pays fictif, les postiers sont particulièrement malhonnêtes et pillent les colis qui leur sont confiés. Les usagers disposent de colis rigides susceptibles d'être munis de cadenas. Seuls ces

derniers colis arrivent intacts à leur destinataire. Comment l'usager A peut-il transmettre à l'usager B un objet précieux, sans déplacement de l'un ou de l'autre ? Il va de soi que, si A place un cadenas sur son colis, B ne dispose pas de la clef du cadenas !

Voici la réponse. A place son cadenas sur le colis et l'envoie à B. B pose lui aussi son cadenas sur le colis et le renvoie à A. A enlève son cadenas et renvoie le colis à B. Il suffit alors à B de retirer son cadenas. Ce procédé est utilisé en cryptographie dans le système de **Massey-Omura**. Le colis est un message à transmettre, le cadenas représente un procédé de chiffrement confidentiel propre à chaque personne. A et B conviennent de travailler modulo q, q étant un nombre premier (éventuellement public). A veut envoyer confidentiellement un message à B, représenté par un nombre P compris entre 1 et $q - 1$.
i) A choisit un nombre a premier avec $q - 1$ et envoie $P^a \bmod q$. L'identité de Bézout entre a et $q - 1$ lui permet de trouver a' tel que $aa' \equiv 1 \bmod q - 1$.
ii) B choisit de même un nombre b et son inverse b' modulo q, et renvoie $(P^a)^b = P^{ab} \bmod q$.
iii) A calcule alors $(P^{ab})^{a'} \equiv P^b \bmod q$ en vertu du théorème de Fermat ($P^{q-1} \equiv 1 \bmod q$) et le renvoie à B.
iv) B calcule alors $(P^b)^{b'} \equiv P \bmod q$.

Système de Massey-Omura, *q est commun à* A *et à* B

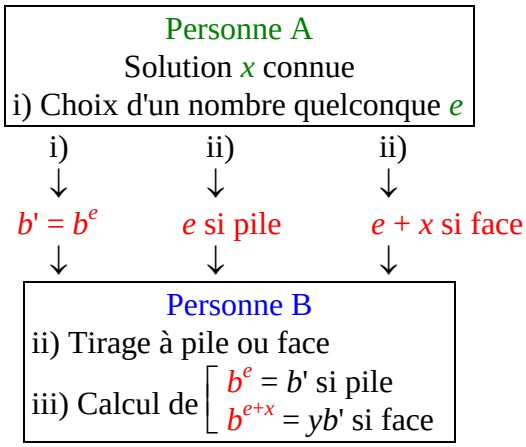


❑ A veut convaincre B qu'il a réussi à résoudre une équation du type logarithme discret, autrement dit, étant donné y, il prétend avoir découvert x tel que $b^x = y$. Cependant, A ne veut pas dévoiler à B la valeur de x. Voilà comment procéder.
i) A choisit un nombre e quelconque et envoie à B le nombre $b' = b^e$.
ii) B tire alors à pile ou face

- Si la pièce tombe sur pile, il demande à A la valeur de e et iii) vérifie que b' est bien égal à b^e.
- Si la pièce tombe sur face, il demande à A la valeur de $e + x$, et iii) B vérifie que $yb' = b^{x+e}$.

Recommencer au i) jusqu'à ce que B soit convaincu que A connaît bien la valeur de x. Si A ignore cette valeur, il ne peut répondre qu'à un seul des deux tirages. Par ailleurs, B ne peut déterminer ce que vaut x, puisqu'il ignore la valeur de e dans le cas d'un tirage sur face.

Preuve de la résolution d'un problème sans donner sa solution. b et y sont publics.



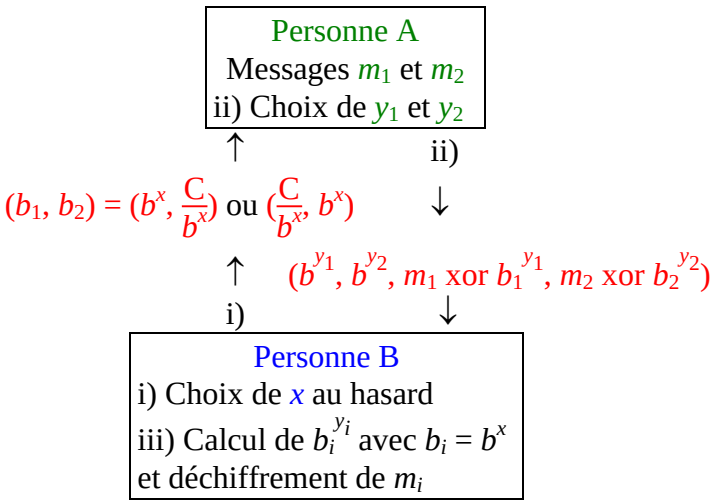
❑ Indiquons enfin un problème curieux. A peut envoyer à B deux messages codés. B peut en décoder alors un et un seul, mais A ne peut savoir lequel. On utilise là aussi la supposition de Diffie-Hellmann. On travaille modulo un nombre premier q et on suppose donné un nombre C dont ni A ni B ne connaisse le logarithme en base b. Voici comment procéder, b et C étant publics :

i) B choisit un nombre x au hasard et envoie à A l'un des deux couples $(b_1, b_2) = (b^x, \frac{C}{b^x})$ ou $(b_1, b_2) = (\frac{C}{b^x}, b^x)$. A ignore lequel de ces deux couples il reçoit.

ii) A choisit deux entiers y_1 et y_2. Si les deux messages sont m_1 et m_2 codés en binaires, A envoie les nombres b^{y_1}, b^{y_2}, m_1 xor $b_1^{y_1}$, m_2 xor $b_2^{y_2}$, les deux premiers étant donnés modulo q, les deux derniers codés en binaires. L'opérateur xor est le *ou exclusif* qui agit sur les chiffres binaires correspondant des deux nombres de la façon suivante : 0 xor 1 = 1 xor 0 = 1, 0 xor 0 = 1 xor 1 = 0.

iii) B sait si $b^x = b_1$ ou b_2, puisque c'est lui qui a créé le couple (b_1, b_2). Soit donc i tel que $b^x = b_i$. B peut calculer $b_i^{y_i} = (b^{y_i})^x$ sans connaître y_i, car il connaît x ainsi que b^{y_i}, communiqué par A. Connaissant $b_i^{y_i}$ et m_i xor $b_i^{y_i}$, il peut déchiffrer le message m_i. Mais il ne peut pas décoder l'autre message, car il aurait besoin de calculer l'autre puissance $(\frac{C}{b^x})^{y_j}$, mais il ignore la valeur de y_j. Par ailleurs, A ne connaît pas la valeur de l'indice i tel que $b^x = b_i$ et il ne peut savoir quel message a été décodé.

Déchiffrement d'un message sur deux, b et C sont publics



3- Authentification de signatures

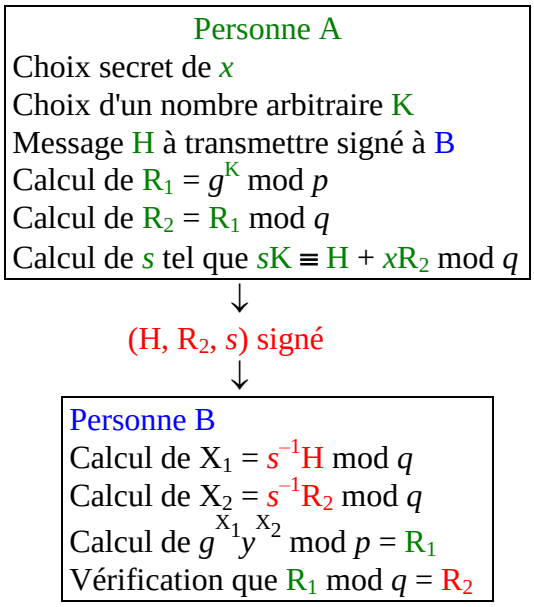
Nous avons vu un moyen de signer ses messages dans le cadre du chiffrement RSA. En voici un autre, le système d'authentification de signature **DSS** (Digital Signature Standard).

A veut envoyer à B un message, accompagné d'une procédure de certification de sa signature. A procède comme suit :
i) A choisit un nombre premier q de plusieurs dizaine de chiffres. Il suffit de disposer d'un générateur de nombres aléatoires et d'un test de nombres premiers (*isprime* et *nextprime* en MAPLE).
ii) A choisit un nombre premier p de plusieurs dizaines de chiffres tel que $p \equiv 1 \bmod q$. (On teste la primalité de nombres de la forme $1 + rq$, en faisant varier r).
iii) A choisit un nombre g pour lequel q est la plus petite puissance vérifiant $g^q \equiv 1 \bmod p$. (Si a est un entier qui n'est pas divisible par p, on a $a^{p-1} \equiv 1 \bmod p$ d'après le théorème de Fermat. Comme il existe k tel que $p - 1 = kq$, il suffit de prendre $g = a^k$ si $a^k \neq 1 \bmod p$, sinon choisir un autre a).
iv) A choisit un entier x aléatoire entre 1 et $q - 1$, et calcule $y = g^x \bmod p$. x est gardé secret, mais g, y, p et q sont publiés par A.

Pour signer un message H, nombre entier entre 0 et $q - 1$, A calcule ce qui suit :
v) A choisit un entier K entre 1 et $q - 1$, et calcule $R_1 = g^K \bmod p$, puis $R_2 = R_1 \bmod q$.
vi) A calcule enfin s tel que $sK \equiv H + xR_2 \bmod q$ (s existe car K est inversible dans $\mathbb{Z}/q\mathbb{Z}$).
La signature est donnée par (R_2, s).

Pour vérifier la signature (R_2, s) du message H qu'il a reçu, B opère ainsi. Il connaît g, y, p, q, H, R_2 et s mais ni x ni K.
a) Il calcule $X_1 = s^{-1}H \bmod q$.
b) Il calcule $X_2 = s^{-1}R_2 \bmod q$.
c) Il calcule $g^{X_1}y^{X_2} \bmod p$, qui n'est autre que $g^{(H+xR_2)/s \bmod q} = g^{K \bmod q} = g^K \bmod p = R_1$ compte tenu du fait que $g^q \equiv 1 \bmod p$.
d) Il calcule $R_1 \bmod q$ et il doit retrouver R_2.

Authentification de signature, (g, y, p, q) sont publiés par A



Cette procédure est basée sur la difficulté de calculer x connaissant $y = g^x \bmod p$ ou de calculer K connaissant $R_1 = g^K \bmod p$. K est un élément confidentiel que choisit A pour chaque message M qu'il envoie. Seule la personne connaissant x et K est supposée capable de créer la paire (R_2, s).

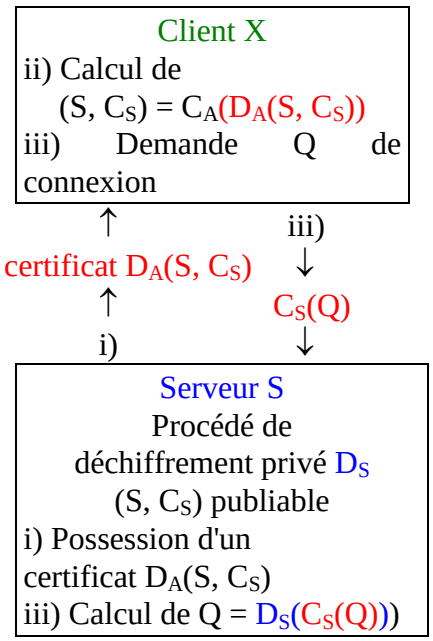
4- Sécurisation des communications par internet

Lorsqu'un utilisateur (le client) souhaite se connecter à un site internet (serveur S), il entre le nom de domaine du serveur dans la barre d'adresse de son navigateur internet. Il existe plusieurs moyens pour des pirates d'orienter le client vers un faux serveur usurpant l'identité du serveur S. En voici trois par ordre décroissant de difficulté :
1) Pour se connecter au serveur S, le navigateur du client se connecte à un serveur dit DNS (*Domain name system*) qui possède une correspondance entre les noms de domaine sous forme de chaîne de caractères et l'adresse numérique IP (*Internet protocol*) localisant le serveur S. Si le serveur DNS a été piraté, la correspondance peut être falsifiée et le client dirigé vers un faux site usurpant l'identité du vrai site S. Ce type de falsification est très rare et ne peut être mise en oeuvre que par des pirates très expérimentés.
2) Une autre fraude possible consiste à tromper les moteurs de recherche en forçant le classement d'un faux site en lieu et place du vrai site recherché par le client. Si le client essaie de se connecter au serveur S à partir du résultat donné par un moteur de recherche, il sera orienté vers le faux site. Ce type de falsification peut arriver occasionnellement, mais peut être détectable si on est attentif au nom du domaine falsifié vers lequel on est dirigé. Pour les sites d'organismes sensibles tels les sites

bancaires, il est déconseillé d'utiliser un moteur de recherche. Il vaut mieux utiliser directement l'adresse figurant sur un document officiel de l'organisme.
3) La fraude la plus fréquente et très facile à mettre en oeuvre consiste à envoyer au client un courriel d'hameçonnage imitant un courriel officiel du serveur S et contenant un lien à cliquer dirigeant vers le faux site. Il est recommandé de ne jamais cliquer sur un lien contenu dans un courriel, mais de se connecter directement au site officiel du serveur par l'intermédiaire de son navigateur.

Il convient donc de sécuriser les accès aux sites internet en les authentifiant. Les sites sécurisés possèdent un nom de domaine en https (et non http pour les sites non sécurisés). Lorsque le client se connecte à un tel site, alors :
i) le client reçoit du serveur un certificat contenant son nom complet de domaine et sa clef publique de chiffrement C_S, le certificat lui-même étant signé et chiffré par une autorité de confiance A au moyen de sa clef privée D_A.
ii) Les clefs publiques de déchiffrement C_A des autorités de confiance sont contenues dans tout navigateur internet utilisé par le client. Le navigateur du client peut alors déchiffrer le certificat, vérifier l'authenticité de sa signature, et vérifier que le nom du domaine auquel il est connecté est bien celui contenu dans le certificat. Le navigateur du client dispose alors de la clef publique C_S de chiffrement du serveur S.
iii) Il peut alors envoyer sous forme chiffrée avec la clef C_S une demande Q de communication avec le serveur. Cette demande consiste en un échange d'une clef de chiffrement propre à la connexion en cours. Si un pirate a usurpé ou détourné le nom de domaine, et copié un certificat du site officiel, il ne sera pas en mesure de déchiffrer la demande de communication reçue et d'y répondre, car il ne connaît pas le procédé de déchiffrement D_S. La communication ne pourra donc pas se faire.

Connexion à un site sécurisé https utilisant la signature et le chiffrement d'une autorité de confiance A



Exercices

1- Enoncés

Exo.1) Montrer que $2^{147} - 1$ est divisible par 343.

Exo.2) Montrer que : x impair et $k \geq 3 \Rightarrow x^{2^{k-2}} \equiv 1 \bmod 2^k$

Exo.3) Quels sont les deux derniers chiffres décimaux de 3^{2020} ?

Exo.4) Trouver les entiers n tels que $\begin{cases} 3n \equiv 1 \bmod 4 \\ 2n \equiv 4 \bmod 5 \end{cases}$

Exo.5) Résoudre les systèmes :

a) $\begin{cases} x \equiv 11 \bmod 13 \\ x \equiv 13 \bmod 7 \\ x \equiv 7 \bmod 11 \end{cases}$ b) $\begin{cases} 7x \equiv 11 \bmod 13 \\ 11x \equiv 13 \bmod 7 \\ 13x \equiv 7 \bmod 11 \end{cases}$

Exo.6) Résoudre dans $\mathbb{Z}/7\mathbb{Z}$ le système $\begin{cases} 2x + 4y = 1 \\ 5x + 3y = a \end{cases}$ en fonction du paramètre a.

Exo.7) Tout entier possède-t-il un multiple de la forme $2^l(2^k - 1)$, $k > 0$?

Exo.8) Le problème de Frobenius. On considère deux pièces de monnaie, de valeurs a et b unités, où a et b sont deux entiers strictement positifs, premiers entre eux. Quelle est la plus grande somme qu'on ne puisse pas payer avec ces pièces ? Par exemple, pour $a = 2$ et $b = 5$, on ne peut pas payer 3 unités, mais toute valeur strictement supérieure à 3 peut être payée.

Exo.9) a) Pour $n \geq 2$, montrer que $1 + \frac{1}{2} + ... + \frac{1}{n}$ n'est pas un entier.

b) Pour tout $n \geq 2$, posons $1 + \frac{1}{2} + ... + \frac{1}{n} = \frac{a_n}{b_n}$ avec a_n et b_n entiers premiers entre eux. Montrer que, si p est un nombre premier strictement supérieur à 2, alors a_{p-1} est divisible par p.

Exo.10) Soit $P = \sum_{k \geq 0} a_k X^k$ et $Q = \sum_{k \geq 0} b_k X^k$ deux polynômes à coefficients entiers. On dit que $P \equiv Q \bmod n$ si et seulement si : $\forall\ k,\ a_k \equiv b_k \bmod n$. Il est facile de vérifier que la relation de congruence est compatible avec l'addition et le produit des polynômes. Soit p un nombre premier :

a) Montrer que $(1 + X)^p \equiv 1 + X^p \bmod p$

b) En considérant $(1 + X)^{ap+b}$, en déduire que $\binom{ap + b}{cp + d} \equiv \binom{a}{c}\binom{b}{d} \bmod p$ pour tout entiers a, b, c, d tels que $0 \leq d \leq b < p$, $0 \leq c \leq a$.

Exo.11) Soit p un nombre premier et n un nombre strictement positif. On note $\deg_p(n)$ l'exposant de p dans la décomposition en facteurs premier de n. On remarquera que, pour tout entier n et m, $\deg_p(mn) = \deg_p(m) + \deg_p(n)$. Pour tout entier d strictement positif, on note n div d le quotient entier de la division euclidienne de n par d. Enfin, soit s la somme des chiffres de n dans sa décomposition en base de numération p : si les a_k sont les chiffres de n, éléments de $[\![1, p - 1]\!]$, on a $n = \sum_{k \geq 0} a_k p^k$ et $s = \sum_{k \geq 0} a_k$ (voir *bases de numération* dans /L1/ARITHMTQ.PDF).

a) Un **théorème de Legendre** (1808). Montrer que $\deg_p(n!) = \sum_{k \geq 1} (n \text{ div } p^k) = \frac{n - s}{p - 1}$. Pour la première égalité, on peut dénombrer de deux façons l'ensemble $\{(k, m) \mid 1 \leq k \leq n,\ 1 \leq m \leq n$ et p^k divise $m\}$.

b) Par combien de zéros de termine 1000! ?

c) Quelle puissance de 2 divise $(2^n - 1)$! ?

d) **Le théorème de Kummer** (1852). Soient m et n deux entiers strictement positifs. Montrer que $\deg_p(\binom{n + m}{m})$ est égal au nombre de retenues nécessaires pour ajouter m et n en base de numération p. Le vérifier sur $\binom{12}{5}$ pour les nombres premiers p variant de 2 à 11.

e) Soit $e > 0$ et $1 \leq j \leq p^e - 1$. Montrer que $\deg_p(\binom{p^e}{j}) = e - \deg_p(j)$.

f) Soit e et x des entiers strictement positifs, et $n = \deg_p(x - 1)$. Montrer que, si $n > 0$, p^{e+n} divise $x^{p^e} - 1$, et si $n = 0$, $x^{p^e} - 1$ n'est pas divisible par p.

2- Solutions

Sol.1) $2^{10} = 1024$ alors que $343 \times 3 = 1029$ donc :

$2^{10} \equiv -5 \bmod 343$

$2^{11} \equiv -10 \bmod 343$

$2^{22} \equiv 100 \bmod 343$

$2^{33} \equiv -1000 \bmod 343 \equiv 29 \bmod 343$

$2^{132} \equiv 29^4 \equiv 15 \bmod 343$

$2^{147} \equiv 2^{15} \times 15 \equiv 2^5 \times -5 \times 15 \equiv 32 \times -75 \equiv 1 \bmod 343$

On peut remarquer que $343 = 7^3$ et que 2 est premier avec 343. Le théorème de Fermat donne alors $2^{\varphi(343)} \equiv 1 \bmod 343$, avec φ la fonction indicatrice d'Euler. $\varphi(343) = \varphi(7^3) = 7^3 - 7^2 = 294$, donc $2^{294} \equiv 1 \bmod 343$, ce qui est bien cohérent avec $2^{147} \equiv 1 \bmod 343$ puisque 294 est le double de 147, mais est moins précis.

Sol.2) Par récurrence sur k. x est impair donc de la forme $2n + 1$. Pour $k = 3$, on a :

$x^{2^{k-2}} = x^2 = 4n(n+1) + 1$ avec $n(n+1)$ pair

$\equiv 1 \bmod 8$

Supposons la relation vraie au rang $k - 1$. On a donc :

$x^{2^{k-3}} \equiv 1 \bmod 2^{k-1}$

donc $\exists\, m,\ x^{2^{k-3}} = 1 + 2^{k-1}m$

donc $x^{2^{k-2}} = (1 + 2^{k-1}m)^2 = 1 + 2^k(m + 2^{k-2}m^2) \equiv 1 \bmod 2^k$

Le théorème de Fermat n'est pas suffisant. Il donne seulement (avec φ la fonction d'Euler) :

$\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$

et x impair est premier avec 2^k, donc $x^{2^{k-1}} \equiv 1 \bmod 2^k$.

Sol.3) Appliquons le théorème de Fermat. On a $100 = 2^2 \times 5^2$ avec :

$\varphi(100) = (2^2 - 2)(5^2 - 5) = 2 \times 20 = 40$

donc, 3 étant premier avec 100, $3^{40} \equiv 1 \bmod 100$.

En élevant à la puissance 50, on a $3^{2000} \equiv 1 \bmod 100$, donc $3^{2020} \equiv 3^{20} \bmod 100$.

On a $3^5 = 243 \equiv 43 \bmod 100$, donc $3^{20} \equiv 43^4 = 3418801 \equiv 1 \bmod 100$. Ainsi, $3^{2020} \equiv 1 \bmod 100$.

Sol.4) $3x \equiv 1 \bmod 4 \Leftrightarrow -x \equiv 1 \bmod 4 \Leftrightarrow x \equiv 3 \bmod 4 \Leftrightarrow \exists\, k \in \mathbb{Z},\ x = 3 + 4k$. On reporte dans la deuxième équation.

$2x = 6 + 8k \equiv 4 \bmod 5 \Leftrightarrow 8k \equiv -2 \bmod 5 \Leftrightarrow 3k \equiv 3 \bmod 5 \Leftrightarrow k \equiv 1 \bmod 5$ car 3 est inversible modulo 5 (d'inverse 2), donc $\exists\, m,\ k = 1 + 5m$. Les solutions sont donc :

$x = 7 + 20m$

On peut aussi utiliser la méthode exposée dans le théorème des restes chinois, avec ici $n_1 = 4$ et $n_2 = 5$, soit $n_2 - n_1 = 1 = a_1n_2 + a_2n_1$ avec $a_1 = 1$ et $a_2 = -1$. La première équation s'écrit $x \equiv x_1 \bmod 4$ avec $x_1 = 3$. La deuxième s'écrit $x \equiv x_2 \bmod 5$ avec $x_2 = 2$. Les solutions sont :

$x \equiv x_1a_1n_2 + x_2a_2n_1 \bmod n_1n_2 \equiv 15 - 8 = 7 \bmod 20$

Sol.5) On applique le théorème des restes chinois avec $n_1 = 13$, $n_2 = 7$ et $n_3 = 11$. Une identité de Bézout entre $n_2n_3 = 77$ et $n_1n_3 = 143$ est $2n_2n_3 - n_1n_3 = n_3$, avec pour PGCD n_3. Puis une identité de Bézout entre n_3 et n_1n_2 donne $-33n_3 + 4n_1n_2 = 1$. Donc :

$-66n_2n_3 + 33n_1n_3 + 4n_1n_2 = 1$

a) Les solutions sont :

$x \equiv -11 \times 66n_2n_3 + 13 \times 33n_1n_3 + 7 \times 4n_1n_2 \bmod n_1n_2n_3 \equiv 986 \bmod 1001$

b) On se débarrasse d'abord des coefficients 7, 11, 13 de x dans les membres de gauche en le multipliant les équations par leur inverse respectifs 2, 2, –5 modulo respectivement 13, 7, 11. On obtient les équations :

$x \equiv 22 \equiv 9 \bmod 13$

$x \equiv 26 \equiv 5 \bmod 7$

$x \equiv -35 \equiv -2 \bmod 11$

puis, comme dans le a) :

$$x \equiv -9 \times 66n_2n_3 + 5 \times 33n_1n_3 - 2 \times 4n_1n_2 \bmod n_1n_2n_3 \equiv 152 \bmod 1001$$

Sol.6) Les deux équations sont liées car le déterminant du système vaut $\begin{vmatrix} 2 & 4 \\ 5 & 3 \end{vmatrix} = -14 \equiv 0 \bmod 7$.
On passe de $2x + 4y$ à $5x + 3y$ en multipliant par 6. Par conséquent, si $a \not\equiv 6 \bmod 7$, il n'y a pas de solution. Dans le cas contraire, les solutions sont celles de la seule première équation :

$2x + 4y = 1$
$\Leftrightarrow$ $8x + 16y = 4$ en multipliant par l'élément inversible 4
$\Leftrightarrow$ $x + 2y = 4$ car on calcule modulo 7
$\Leftrightarrow$ $x = 4 - 2y$

ce qui donne les solutions $(x, y) \in \{(4, 0), (2, 1), (0, 2), (5, 3), (3, 4), (1, 5), (6, 6)\}$

Sol.7) Il suffit de le montrer pour les entiers p impairs. On doit alors montrer qu'il existe k tel que $2^k \equiv 1 \bmod p$. Or, lorsque n varie, les restes de la division euclidienne de 2^n par p ne peuvent être tous distincts (il n'y a qu'un nombre fini de restes pour une infinité de valeurs de n), donc il existe $n \geq m$ tels que $2^n \equiv 2^m \bmod p$, donc p divise $2^n - 2^m = 2^m(2^{n-m} - 1)$, et comme p est impair, $p \wedge 2^m = 1$, donc p divise $2^{n-m} - 1$. On prend $k = n - m$.
Le théorème de Fermat indique aussi que, puisque $2 \wedge p = 1$, $2^{\varphi(p)} \equiv 1 \bmod p$. On prend donc $k = \varphi(p)$. Mais ce n'est peut-être pas le plus petit possible.
EXEMPLE :
Soit $p = 21 = 3 \times 7$, $\varphi(p) = 2 \times 6 = 12$, donc $2^{12} \equiv 1 \bmod 21$, mais on pourra vérifier que $2^6 \equiv 1 \bmod 7$.

Sol.8) La valeur demandée est $ab - a - b$.
Supposons $a < b$. On peut payer les $ak + bm$, $k \geq 0$, $m \geq 0$. Remarquons que les valeurs $bm \bmod a$, $0 \leq m \leq a - 1$, sont toutes différentes. En effet, si $bm \equiv bn \bmod a$, avec $0 \leq m, n \leq a - 1$ alors a divise $b(n - m)$, et comme $a \wedge b = 1$, a divise $n - m$ (théorème de Gauss). Comme $|n - m| < a$, on a $n = m$. Il en résulte que l'application $m \in [\![1, a - 1]\!] \rightarrow bm \bmod a$ est bijective. En particulier, toutes les valeurs de 0 à $a - 1$ sont de la forme $bm \bmod a$.
On ne peut payer $b(a - 1) - a = ab - a - b$, car s'il existe k et m positifs ou nuls tels que $b(a - 1) - a = ak + bm$, alors $b(a - 1) \equiv bm \bmod a$ donc $m \equiv a - 1 \bmod a$ (car b étant premier avec a, b est inversible modulo a) donc $\exists\, n$, $m = a - 1 + na$. $n \geq 0$ car $m \geq 0$. On a alors :

$$b(a - 1) - a = ak + bm = ak + b(a - 1) + bna$$

donc $-a = ak + bna$
ce qui est absurde car $-a < 0$ et $ak + bna \geq 0$.
On peut payer toute somme strictement supérieure à $ab - a - b$. Soit $ab - a - b + r$ une telle somme, avec $r > 0$. Comme les $bm \bmod a$ prennent toutes les valeurs de 0 à $a - 1$, il existe un unique m entre 0 et $a - 1$ tel que $ab - a - b + r \equiv bm \bmod a$. Donc, il existe k tel que $ab - a - b + r = ak + bm$. Il reste à montrer que $k \geq 0$. On a :

$$ak = ab - a - b + r - bm = b(a - 1 - m) - a + r \geq -a + r > -a$$

donc $k > -1$ donc $k \geq 0$.
EXEMPLE : Pour $a = 6$ et $b = 35$, $ab - a - b = 169$. Quand m varie de 0 à 5, les $bm \bmod a$ valent respectivement 0, 5, 4, 3, 2, 1.
Prenons la somme $170 \equiv 2 \bmod a$. On prend donc $m = 4$, $bm = 140$, $ak = 30$, donc $k = 5$.
Prenons la somme $215 \equiv 5 \bmod a$. On prend $m = 1$, $bm = 35$, $ak = 180$, donc $k = 30$.

Sol.9) a) On montre par récurrence sur $n \geq 2$ que $1 + \frac{1}{2} + ... + \frac{1}{n} = \frac{a_n}{b_n}$ avec a_n impair et b_n pair. On a $1 + \frac{1}{2} = \frac{3}{2}$. Supposons la relation vraie au rang $n - 1$.

Si n est impair, alors $1 + \frac{1}{2} + ... + \frac{1}{n} = \frac{a_{n-1}}{b_{n-1}} + \frac{1}{n} = \frac{na_{n-1} + b_{n-1}}{nb_{n-1}}$ qui est de la forme voulue car nb_{n-1} est pair et $na_{n-1} + b_{n-1}$ est impair.
Si n est pair, écrivons-le $2^k m$, avec $k \geq 1$ et m impair, et de même $b_{n-1} = 2^r s$, $r \geq 1$, s impair. On a alors :

$$1 + \frac{1}{2} + ... + \frac{1}{n} = \frac{a_{n-1}}{b_{n-1}} + \frac{1}{2^k m} = \frac{a_{n-1}}{2^r \mathrm{s}} + \frac{1}{2^k m}$$
$$= \begin{cases} \frac{m a_{n-1} + 2^{r-k}\mathrm{s}}{2^r ms} \text{ si } k < r \\ \frac{2^{k-r} m a_{n-1} + s}{2^k ms} \text{ si } k > r \end{cases}$$

Dans les deux cas précédents, le numérateur est impair et le dénominateur est pair.
Le cas $k = r$ ne se présente pas. En effet, le facteur 2^k apparaît pour la première fois comme facteur du dénominateur quand on ajoute $\frac{1}{n} = \frac{1}{2^k}$. Dans ce cas, b_{n-1} est le PPCM de tous les entiers entre 1 et $2^k - 1$, et la puissance r de 2 dans ce PPCM est strictement inférieure à k, puisqu'elle l'est pour tous les entiers entre 1 et $2^k - 1$. A partir de $n = 2^k$, la plus grande puissance de 2 divisant le dénominateur est 2^k et ceci jusqu'au prochain entier n ayant 2^k en facteur, à savoir $n = 2^k \times 2 = 2^{k+1}$. Pour ce n, le PPCM des dénominateurs passera à une puissance de 2 égale à $k + 1$, et il n'y aura donc jamais de cas où l'on aura $b_{n-1} = 2^k s$ et $n = 2^k m$ avec s et m impairs.
Ainsi, les premiers exposants des puissances de 2 dans la factorisation de n variant de 2 à 20 sont :

1, 0, 2, 0, 1, 0, 3, 0, 1, 0, 2, 0, 1, 0, 4, 0, 1, 0, 2, ...

alors que, pour b_{n-1}, on a :

0, 1, 1, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3, 4, 4, 4, 4, ...

b) $\frac{a_{p-1}}{b_{p-1}} = 1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{\mathrm{N}}{(p-1)!}$ pour un certain entier N. Si d est le PGCD de N et $(p - 1)!$, alors $\mathrm{N} = da_{p-1}$ et $(p - 1)! = db_{p-1}$. Pour k variant de 1 à $p - 1$, notons k^* l'entier tel que $k \times k^* \equiv 1 \bmod p$. On a $(p - 1)! \times k^* \equiv \frac{(p-1)!}{k} \bmod p$, donc :

$$(p-1)! \times \sum_{k=1}^{p-1} k^* \equiv \sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv \mathrm{N} \bmod p$$

L'application $k \to k^*$ étant bijective dans $\mathbf{Z}/p\mathbf{Z} \setminus \{0\}$, on a $\sum_{k=1}^{p-1} k^* \equiv \sum_{k=1}^{p-1} k = \frac{p(p-1)}{2} \equiv 0 \bmod p$.

Donc $p \mid \mathrm{N} = da_{p-1}$. Comme p est premier avec $(p - 1)! = db_{p-1}$, p est premier avec d, donc $p \mid a_{p-1}$.

Sol.10) a) Développer le membre de gauche avec le binôme de Newton et remarquer que, pour $1 \leq j \leq p - 1$, $\binom{p}{j}$ est divisible par p (c'est aussi un cas particulier du e) de l'exercice suivant).
b) $(1 + \mathrm{X})^{ap+b} \equiv (1 + \mathrm{X}^p)^a (1 + \mathrm{X})^b \bmod p$

donc les coefficients de degré $cp + d$ des deux membres sont congrus modulo p. Celui de gauche vaut $\begin{pmatrix} ap+b \\ cp+d \end{pmatrix}$. Celui de droite vaut $\begin{pmatrix} a \\ c \end{pmatrix}\begin{pmatrix} b \\ d \end{pmatrix}$.

Sol.11) a) Pour k fixé, on dénombre les $m \in [\![1, n]\!]$ tels que p^k divise m et il y en a n div p^k. Le cardinal de l'ensemble $\{(k, m) \mid 1 \le k \le n, 1 \le m \le n$ et p^k divise $m\}$ est donc $\sum_{k\ge1} (n \text{ div } p^k)$.

Pour m fixé, on dénombre les k tels que p^k divise m et il y en a $\deg_p(m)$. Le cardinal du même ensemble vaut donc $\sum_{m=1}^{n} \deg_p(m) = \deg_p(1 \times 2 \times ... \times n) = \deg_p(n!)$.

On a donc déjà obtenu l'égalité $\deg_p(n!) = \sum_{k\ge1} (n \text{ div } p^k)$.

Puis, si $n = a_q p^q + a_{q-1}p^{q-1} + ... + a_1 p + a_0$, alors $s = \sum_{j\ge0} a_j$, et, pour tout k :

$$n \text{ div } p^k = a_q p^{q-k} + a_{q-1}p^{q-k-1} + ... + a_k$$

donc :

$$\sum_{k\ge1} (n \text{ div } p^k) = \sum_{k\ge1} \sum_{j\ge k} a_j p^{j-k} = \sum_{j\ge1} \sum_{1\le k\le j} a_j p^{j-k} = \sum_{j\ge1} a_j \frac{p^j - 1}{p-1} = \frac{1}{p-1} (\sum_{j\ge1} a_j p^j - \sum_{j\ge1} a_j)$$

$$= \frac{1}{p-1} (\sum_{j\ge0} a_j p^j - \sum_{j\ge0} a_j) = \frac{n-s}{p-1}$$

b) Il suffit de chercher $\deg_5(1000!)$ puisque la puissance de 2 sera supérieure à celle de 5. Pour $p = 5$, on a $1000 = 625 + 125 \times 3 = 13000_p$ donc $\deg_5(1000!) = \frac{1000-4}{4} = \frac{996}{4} = 249$. Il y a 249 zéros.

c) le développement binaire de $2^n - 1$ est constitué de n chiffres 1, donc la plus grande puissance de $p = 2$ qui divise $(2^n - 1)!$ est $2^n - 1 - n$.

d) Si la somme des chiffres de la décomposition de m en base p est s, celle de n est t et celle de $n + m$ est u, alors :

$$\deg_p(\begin{pmatrix} n+m \\ m \end{pmatrix}) = \deg_p((n+m)!) - \deg_p(m!) - \deg_p(n!) = \frac{n+m-u}{p-1} - \frac{m-s}{p-1} - \frac{n-t}{p-1}$$

$$= \frac{s+t-u}{p-1}$$

Notons (a_k) les chiffres de m, (b_k) ceux de n, (c_k) ceux de $m + n$. Dans l'algorithme d'addition, les retenues (r_k) sont définies de la façon suivante :

$r_0 = 0$

$\forall\ k \ge 0$, $c_k = (a_k + b_k + r_k) \bmod p$, $r_{k+1} = (a_k + b_k + r_k) \text{ div } p$

donc $a_k + b_k + r_k = p r_{k+1} + c_k$

donc $a_k + b_k - c_k = p r_{k+1} - r_k$

donc $s + t - u = \sum_{k\ge0} a_k + b_k - c_k = \sum_{k\ge0} (p r_{k+1} - r_k) = p \sum_{k\ge0} r_{k+1} - \sum_{k\ge0} r_k = (p-1) \sum_{k\ge0} r_k$

car, comme $r_0 = 0$, $\sum_{k\geq 0} r_{k+1} = \sum_{k\geq 1} r_k = \sum_{k\geq 0} r_k$.

On a donc bien $\frac{s+t-u}{p-1} = \sum_{k\geq 0} r_k$ somme des retenues.

EXEMPLE : $\binom{12}{5} = 792 = 2^3 \times 3^2 \times 11$.

- Pour $p = 2$, on a $5 = 101_p$ et $7 = 111_p$ et la somme de 5 et 7 en base 2 nécessite trois retenues. On a aussi $12 = 1100_p$ donc $s = 2$, $t = 3$, $u = 2$ et $\frac{s+t-u}{p-1} = 3$.
- Pour $p = 3$, $5 = 12_p$ et $7 = 21_p$ et il faut deux retenues. On a aussi $12 = 110_p$ donc $s = t = 3$, $u = 2$ et $\frac{s+t-u}{p-1} = 2$.
- Pour $p = 5$, $5 = 10_p$ et $7 = 12_p$ et il n'y a aucune retenue. On a aussi $12 = 22_p$ donc $s = 1$, $t = 3$, $u = 4$ donc $\frac{s+t-u}{p-1} = 0$.
- Pour $p = 7$, $5 = 5_p$, $7 = 10_p$ et il n'y a aucune retenue. On a aussi $12 = 15_p$ donc $s = 5$, $t = 1$, $u = 6$ donc $\frac{s+t-u}{p-1} = 0$.
- Pour $p = 11$, $5 = 5_p$, $7 = 7_p$, et il y a une retenue. On a aussi $12 = 11_p$ donc $s = 5$, $t = 7$, $u = 2$ et $\frac{s+t-u}{p-1} = 1$.

e) Comme $\deg_p(n!) = \frac{n-r}{p-1}$ où r est la somme des chiffres de n dans sa décomposition en base p, on a $\deg_p((p^e)!) = \frac{p^e-1}{p-1}$. Pour j entre 1 à $p^e - 1$, on a :

$\deg_p(j!) = \frac{j-s}{p-1}$ où s est la somme des chiffres de j dans sa décomposition en base p. Si $j = a_k p^k + ... + a_{e-1}p^{e-1}$ avec $k = \deg_p(j)$, $0 < a_k < p$ et $0 \leq a_m < p$ pour m variant de $k+1$ à $e-1$, $s = a_k + ... + a_{e-1}$.

$\deg_p((p^e - j)!) = \frac{p^e - j - t}{p-1}$ où t est la somme des chiffres de $p^e - j$ dans sa décomposition en base p.Avec les notations précédentes :

$p^e - j = (p - a_k)p^k + (p - 1 - a_{k+1})p^{k+1} + ... + (p - a_{e-1} - 1)p^{e-1}$

avec $0 \leq p - a_k < p$, et $0 \leq p - 1 - a_m < p$ pour m variant de $k+1$ à $e-1$.

Donc $t = p - a_k + p - 1 - a_{k+1} + ... + p - a_{e-1} - 1$

$= 1 - s + (p-1)(e-k)$

Donc $\deg_p(\binom{p^e}{j}) = \frac{p^e-1}{p-1} - \frac{j-s}{p-1} - \frac{p^e-j-t}{p-1} = e - k = e - \deg_p(j)$.

Cette expression finale est aussi valable pour $j = p^e$, puisqu'alors $k = e$ et $\binom{p^e}{j} = 1 = p^0 = p^{e-k}$.

f) Par définition de n, $\exists\, k$, $x = 1 + mp^n$ et $m \wedge p = 1$. Donc :

$$x^{p^e} = (1 + mp^n)^{p^e} = 1 + \sum_{j=1}^{p^e} \binom{p^e}{j} m^j p^{nj}$$

D'après le e), $\deg_p(\binom{p^e}{j} m^j p^{nj}) = e - \deg_p(j) + nj$.

Si n est nul, $\deg_p(\binom{p^e}{j} m^j) = e - \deg_p(j)$. Comme $0 \le \deg_p(j) < e$ quand j varie de 1 à $p^e - 1$, $e - \deg_p(j) > 0$, donc p divise $\binom{p^e}{j} m^j$. On a donc :

$$x^{p^e} \equiv 1 + m^{p^e} \bmod p$$

et $x^{p^e} - 1$ n'est pas divisible par p car $m \wedge p = 1$.

Si n est non nul et $1 \le j \le p^e$, en posant $k = \deg_p(j)$, on a $j \ge p^k$ donc :

$$e - \deg_p(j) + nj \ge e - k + np^k \ge e - k + n2^k \ge e + n \quad \text{car } n(2^k - 1) \ge 2^k - 1 \ge k$$

Donc tous les termes $\binom{p^e}{j} m^j p^{nj}$ sont divisibles par p^{e+n}.

EXEMPLE :

❑ $e = 1$, $p = 2$, $x = 3$, $x - 1 = 2$ donc $n = 1$.

On a $x^2 - 1 = 8 = 2^3$ divisible par $p^{e+n} = 2^2$.

◆