COURS D'ARITHMÉTIQUE

par

Boyer Pascal

Table des matières

Introduction

L'arithmétique consiste, en résumé, à étudier les entiers relatifs, i.e. les éléments de $\mathbb{Z}$. Comme dans la saga *Star wars*, l'arithmétique a aussi un côté obscur et beaucoup plus puissant, à savoir la théorie des nombres, qui consiste à étudier l'arithmétique d'entiers plus généraux comme par exemple $\mathbb{Z}[i] = \{a + ib;\ a, b \in \mathbb{Z}\} \subset \mathbb{C}$ où $i^2 = -1$. Dans ce cours nous resterons de bons Jedi et ne nous laisserons pas tenter par le côté obscur, cependant il sera utile de raisonner pas à pas afin de séparer les résultats qui se généralisent, des autres. Toutefois le but de ce cours n'est pas de faire une présentation bourbakiste, ainsi nous n'hésiterons pas en amphi à traiter un exemple suffisamment générique en lieu et place d'une preuve rigoureuse. L'un des intérêts de l'arithmétique sont ses applications ludiques et concrètes, citons par exemple :

- la résolution d'équations diophantiennes simples, le développement décimal de $1/p$, des applications récentes des courbes elliptiques ;
- des problèmes typiquement liés à l'utilisation de l'ordinateur : critères de primalité, factorisation des entiers ;
- le jeu de Nim, de fléchettes, du solitaire, le partage de secret pour le déclenchement de l'arme atomique ;
- les problèmes de transmission, plus particulièrement, la cryptographie et les codes correcteurs.

Ce cours se tenant devant un auditoire d'informaticiens, nous proposerons de vérifier numériquement à l'aide de l'ordinateur quelques unes des conjectures qui résistent encore sur les nombres premiers : il s'agira par groupes de 5, de proposer un algorithme permettant de confirmer une conjecture et d'illustrer graphiquement les résultats. Les thèmes seront proposés en TD et le projet noté, sera à rendre début décembre.

J'espère que ces errements mathématiques passionneront ceux qui voudront bien nous accompagner et vous donneront l'envie d'en savoir plus.

Remarque : le texte est agrémenté de nombreux exercices dont la plupart sont difficiles et de niveau supérieur à ce que l'on attend de vous. On marquera avec des étoiles la difficulté des exercices.

1. Arithmétique de $\mathbb{Z}$

Selon la philosophie de ce cours nous ne nous étendrons pas sur la construction de l'ensemble des entiers relatifs $\mathbb{Z}$, rappelons simplement que

tout ensemble borné de $\mathbb{Z}$ admet un plus petit et un plus grand élément.

Remarque : cette propriété n'est pas aussi anodine qu'il y parait. Par exemple sur $\mathbb{R}$, elle n'est pas vraie mais peut être avantageuse remplacée par la suivante : *tout ensemble borné*

admet une borne supérieure et une borne inférieure. [1] En ce qui concerne $\mathbb{Q}$, l'ensemble des rationnels de valeur absolue inférieure à $\sqrt{2}$ est borné mais n'admet ni borne inférieure ni supérieure ; c'est d'ailleurs à partir de ce phénomène que l'on construit $\mathbb{R}$.

Une deuxième propriété tout aussi simple et utile, est l'implication suivante :

$$0 \leq n < 1 \Rightarrow n = 0.$$

Remarque : tout problème d'arithmétique peut se ramener à la résolution d'une équation diophantienne, i.e. savoir déterminer si une équation polynomiale à plusieurs inconnues possède une solution à coefficients dans $\mathbb{Z}$. Les questions difficiles et subtiles d'arithmétique, et donc notamment la résolution des équations diophantiennes, consistent le plus souvent à se ramener à l'implication précédente. Par exemple la quadrature du cercle qui consiste à montrer qu'on ne peut pas construire à la règle et au compas un carré de même aire qu'un cercle unité, repose sur le fait que *le nombre réel π est transcendant.* Comme nous ne voulons pas introduire des concepts trop évolués, nous allons montrer la proposition suivante beaucoup moins forte mais dont la preuve est très similaire.

Proposition 1.1. — *Le nombre réel π est irrationnel, i.e. $\pi \notin \mathbb{Q}$.*

Preuve : Soit D l'opérateur de dérivation sur les polynômes et on pose

$$\Delta = \sum_{k=0}^{+\infty} (-1)^k D^{2k}.$$

Remarquons tout d'abord que la somme est faussement infinie puisque pour tout polynôme P de degré inférieur ou égal à $2n$, on a $\Delta(P)(X) = P(X) - P"(X) + P^{(4)}(X) + \cdots + (-1)^n P^{(2n)}(X)$. On remarque alors que pour tout x réel et pour tout polynôme $P(X) \in \mathbb{R}[X]$, on a l'égalité suivante de fonctions réelles :

$$P(x)\sin x = \Big(\Delta(P')(x)\sin x - \Delta(P)(x)\cos x\Big)'$$

de sorte que par intégration, on obtient la *formule d'Hermite*

$$\int_0^\pi P(x)\sin x dx = \Delta(P)(0) + \Delta(P)(\pi).$$

Supposons $\pi = a/b$ avec $a, b \in \mathbb{N}$ et considérons $P(x) = \frac{1}{n!}x^n(a - bx)^n$. Comme $P(x)\sin x$ est continue positive non identiquement nulle sur $[0, \pi]$, le réel $I_n = \int_0^\pi P(x)\sin x dx$ est strictement positif. Par ailleurs comme $x(a - bx) \leq a^2/4b$ sur $[0, \pi]$, on en déduit que $I_n \leq \frac{1}{n!}\pi\left(\frac{a^2}{4b}\right)^n$ et tend donc vers 0 lorsque n tend vers $+\infty$. Il existe donc un entier N tel que pour tout $n \geq N$, $0 < I_n < 1$ de sorte que I_n ne peut pas être un entier. Or notons que pour tout $0 \leq k < n$, $P^{(k)}(0) = P^{(k)}(\pi) = 0$ (utiliser soit la notion de multiplicité d'une racine d'un polynôme, ou la formule de dérivation de Liebnitz) et pour tout $k \geq n$, $P^{(k)}(0)$ et $P^{(k)}(\pi)$ sont des entiers positifs de sorte que $I_n = \Delta(P)(0) + \Delta(P)(\pi)$ aussi ce qui contredit ce qui précède et donc $\pi \notin \mathbb{Q}$. □

1. Pensez à l'exemple de $[0, 1[$.

1.1. Divisibilité. — Rappelons qu'un entier m divise un entier n s'il existe un entier q tel que $n = qm$. L'ensemble des diviseurs d'un entier n contient toujours ± 1 et $\pm n$; on peut ainsi distinguer ceux dont cet ensemble est de cardinal minimal ce qui nous conduit à la notion suivante :

Définition 1.2. — Un entier $p > 1$ est dit premier [2] si ses seuls diviseurs sont $\pm 1, \pm p$.

Proposition 1.3. — *Tout entier $n \geq 2$ est divisible par un nombre premier ; il peut alors s'écrire comme un produit de nombres premiers.*

Preuve : On procède par récurrence sur n ; le cas $n = 2$ est vrai car 2 est premier, supposons donc la proposition vérifiée pour tout $k < n$ et montrons qu'elle l'est pour n. Si n est premier c'est clair et sinon il existe un diviseur a de n avec $1 < a < n$ qui, d'après l'hypothèse de récurrence, possède un diviseur premier qui divise n. Le deuxième point se montre exactement de la même manière. □

Nous noterons alors $\mathcal{P}$ l'ensemble des nombres premiers ; la question naturelle est alors de savoir si $\mathcal{P}$ est fini ou pas.

Théorème 1.4. — ***(Euclide)*** *L'ensemble $\mathcal{P}$ des nombres premiers est infini.*

Preuve : Raisonnons par l'absurde et supposons que $p_1, \cdots, p_r = n$ sont les seuls nombres premiers ; soit alors $N = n! + 1$, (ou bien $N = (\prod_{p \leq n} p) + 1$). Comme $N > n$ alors N n'est pas premier et possède donc un diviseur premier p qui est donc $\leq n$ de sorte que $p | n!$ et donc aussi $N - n! = 1$ d'où la contradiction. □

Remarque : nous verrons par la suite d'autres preuves de ce résultat. On peut par ailleurs se demander s'il l'ensemble des premiers de la forme $n! \pm 1$ est infini : à ce jour le résultat n'est pas connu. De la même façon on peut se demander si les nombres premiers de la forme $(\prod_{\mathcal{P} \ni q \leq p} q) \pm 1$ sont en nombre infini : à nouveau la réponse n'est pas connu.

Quand deux entiers n et $m \geq 0$ ne se divisent pas, on peut tout de même leur associer un couple de nombres (q, r) via la notion de *division euclidienne.*

Proposition 1.5. — *Pour tout $n, m \geq 0$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que*

$$n = qm + r \text{ et } 0 \leq r < |m|.$$

On dit que q est le quotient et r le reste de la division euclidienne de n par m.

Preuve : Commençons par l'unicité : $mq + r = mq' + r'$ avec $0 \leq r, r' < |m|$ de sorte que $|m|.|q - q'| = |r - r'| < |m|$ et donc $q = q'$ puis $r = r'$. En ce qui concerne l'existence, considérons l'ensemble $A = \{n - km : \ k \in \mathbb{Z}\} \cap \mathbb{N}$ qui est clairement non vide. Notons $r \geq 0$ son plus petit élément avec $n = mq + r$. Si on avait $r \geq |m|$ alors $0 \leq r - |m| = n - m(q \pm 1) \in A$ ce qui contredit la minimalité de r. □

1.6 — Numération en base b et application au jeu de Nim : tout entier naturel n s'écrit de manière unique sous la forme

$$n = \sum_{k=0}^{+\infty} a_k b^k$$

2. Pour ceux qui préfèrent une définition plus imagée, selon Paul Erdös, ≪ un nombre premier est un nombre qui ne se casse pas quand on le laisse tomber par terre ≫

où les a_k sont des entiers positifs $< b$ presque tous nuls. En effet on effectue la division euclidienne de $n = bq_0 + a_0$ par b, puis celle de $q_0 = bq_1 + a_1$ et ainsi de suite ce qui donne l'existence. Pour l'unicité, on reprend la preuve de l'unicité de la division euclidienne.

Le principe *du jeu de Nim* est le suivant : le plateau se présente sous la forme d'un certain nombre de piquets plantés dans un morceau de bois, lesquels ont un certain nombre d'anneaux. Chacun à leur tout, les deux joueurs retirent d'un piquet le nombre d'anneaux qu'ils désirent. Le jeu se termine lorsque tous les anneaux ont été retirés, le gagnant étant celui qui a pris le dernier anneau. Rappelons que le joueur possède une stratégie *gagnante* si quelles que soient les réactions de son adversaire, il sait quoi faire pour gagner la partie ; une position est dite *gagnante* pour le joueur I si jouant à partir de celle-ci, il possède une stratégie gagnante. La position $(0, \cdots, 0)$ est ainsi perdante puisqu'au tour précédent c'est son adversaire qui a pris le dernier anneau.
Remarque : si la position initiale d'une partie n'est pas gagnante pour le premier joueur, c'est que le deuxième a une suite de coups qui lui permettent de répondre aux coups du premier sans que celui-ci ne gagne ; c'est donc que cette position est gagnante pour le deuxième joueur. Moralité pour des joueurs sachant bien jouer, l'issue de la partie est déterminée par la position initiale, pas la peine de jouer donc ! Plus généralement citons le résultat suivant.

Théorème 1.7. — ***(Zemerlo)*** *Dans un jeu fini à deux joueurs, à information parfaite et ayant seulement deux issues possibles (victoire de I ou de II), l'un des deux joueurs a une stratégie gagnante.*

Remarque : la preuve est très simple, il s'agit à partir de l'arbre des positions possibles du jeu, de marquer les feuilles selon que la position est gagnante ou perdante pour le joueur I puis de remonter les niveaux dans l'arbre. La même démonstration s'applique à un ensemble T d'issues possibles du jeu et à son complémentaire.

Décrivons maintenant la stratégie gagnante du jeu de Nim ; on écrit en base 2 le nombre d'anneaux sur chaque piquet et l'on range ces écritures dans un tableau dont les lignes correspondent à ces nombres d'anneau et les colonnes correspondent aux puissances de 2 de ces écritures. Ainsi dans le cas de 4 piquets avec respectivement $33, 59, 13$ et 22 anneaux, on écrit le tableau suivant :

	2^6	2^5	2^4	2^3	2^2	2^1	2^0
33		1	0	0	0	0	1
59		1	1	1	0	1	1
13				1	1	0	1
22			1	0	1	1	0

Une position est alors perdante si dans chaque colonne du tableau, il y a un nombre pair de fois le chiffre 1. En effet partant d'une position dans laquelle chaque colonne contient un nombre pair de fois le chiffre 1, le deuxième joueur est toujours en mesure de ramener le jeu dans un état ayant la même propriété quel que soit le coup joué par le premier joueur. Le premier joueur doit retirer un certain nombre d'anneau et donc modifier une seule ligne du tableau dans laquelle un certain nombre de 1 vont être transformés en 0 et inversement, ce qui change la parité du nombre de 1 dans un certain nombre de colonnes. Pour rétablir la parité dans toutes les colonnes modifiées, le deuxième joueur choisit alors une ligne qui correspondent à un chiffre 1 dans la colonne modifiée la plus à gauche (c'est possible puisque ladite colonne contient forcément un nombre impair de fois le chiffre 1). Il lui faut alors retirer le nombre d'anneaux sur le piquet correspondant de façon à modifier exactement les chiffres

des colonnes affectées par le premier joueur. Comme la position finale $(0, \cdots, 0)$ correspond à un tableau dont toutes les colonnes ont un nombre pair de 1 c'est forcément le second joueur qui l'atteindra et qui gagnera la partie.
Remarque : dans notre exemple la position n'est pas perdante ; toutes les colonnes ont un nombre pair de 1 sauf la colonne de droite. La stratégie gagnante pour le premier joueur consiste à enlever un unique anneau dans l'un des trois premier piquets.
Compléments : considérons un jeu dans lequel les issue possibles appartiennent à un ensemble $\mathcal{I}$: pour $a, b \in \mathcal{I}$, la notation $a \leq_1 b$ (resp. $a \leq_2 b$) signifie que le joueur I (resp. II) préfère l'issue b à a. Un jeu à deux joueurs est dit *strictement compétitif* si les deux joueurs ont des buts diamétralement opposés, i.e. pour tout $a, b \in \mathcal{I}$

$$a <_1 B \Leftrightarrow b <_2 a.$$

L'exemple typique est celui du jeu d'échec. Une issue v du jeu est appelée *valeur du jeu* si le joueur I possède une stratégie qui lui garantit une issue dans l'ensemble $\{u \in \mathcal{I}, u \geq_1 v\}$ et si le joueur II possède une stratégie qui lui garantit une issue dans l'ensemble $\{u \in \mathcal{I},\ u \geq_2 v\}$. On peut alors montrer que tout jeu à deux joueurs strictement compétitif et à information complète possède une unique valeur.[3] Si on note S_1 et S_2 les stratégies qui garantissent respectivement aux joueurs I et II des issues au moins aussi bonnes que l'issue du jeu alors le couple (S_1, S_2) est un cas particulier d'*équilibre de Nash* au sens de la définition suivante.

Définition 1.8. — Une paire de stratégies (S_1, S_2) est *un équilibre de Nash* si :
- S_1 est une stratégie optimale pour le joueur I s'il sait que le joueur II va jouer selon S_2 ;
- S_2 est une stratégie optimale pour le joueur II s'il sait que le joueur I va jouer selon S_1.

Remarque : la notion d'équilibre de Nash est bien plus générale et a de nombreuses applications, en économie notamment.

1.9 — Le corollaire suivant nous fournit une manière élégante et plus savante d'utiliser le fait qu'un sous-ensemble minoré de $\mathbb{Z}$ admet un plus petit élément ; il suffit pour cela de considérer des sous-groupes et de prendre son générateur positif comme le justifie l'énoncé suivant.

Corollaire 1.10. — *Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$.*

Preuve : Soit H un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$ et notons $A = H \cap \mathbb{N}^*$ qui est donc non vide, car si $h \in H$ alors $-h \in H$. Notons n le plus petit élément de A ; soit $h \in H$; on considère la division euclidienne $h = qn + r$ de h par n avec donc $0 \leq r = h - qn < n$ qui appartient à $H \cap \mathbb{N}$ et est donc nul par minimalité de n. Ainsi donc $H \subset n\mathbb{Z}$ et l'inclusion réciproque est évidente. □

Lemme 1.11. — ***(d'Euclide)*** *Soit p premier divisant ab ; alors p divise a ou b.*

Preuve : Supposons que p ne divise pas a ; soit alors $A = \{n \in \mathbb{Z} :\ p|an\}$ qui est un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$ car $p, b \in A$. D'après le corollaire précédent $A = m\mathbb{Z}$ avec donc $m|p \in A$ et donc $A = p\mathbb{Z}$ de sorte, comme $b \in A$, $p|b$, d'où le résultat. □

Théorème 1.12. — ***(Factorialité de $\mathbb{Z}$)*** *Tout entier $n \geq 2$ s'écrit de manière unique sous la forme*

$$n = p_1^{n_1} \cdots p_r^{n_r},$$

3. L'unicité est évidente et pour l'existence il suffit de prendre l'élément maximal des issues que le joueur I peut forcer.

où les n_i sont des entiers naturels non nuls, et où les p_i sont des nombres premiers.

Preuve : L'existence découle de la proposition 1.3 en regroupant les facteurs. En ce qui concerne l'unicité supposons que l'on ait $n = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s}$ où les p_i, q_j sont premiers. D'après le lemme d'Euclide q_j est égal à l'un des p_i de sorte que $\{p_1, \cdots, p_r\} = \{q_1, \cdots, q_s\}$ et donc $r = s$. Supposons $n_1 < m_1$ alors en divisant n par $p_i^{n_i}$, on obtient que p_1 divise $p_2^{n_2} \cdots p_r^{n_r}$ ce qui contredit le lemme d'Euclide, d'où le résultat en raisonnant de même pour les autres indices. □

Définition 1.13. — Soit p un nombre premier ; pour $n \in \mathbb{Z}$, *la valuation p-adique* de n est le plus grand entier k tel que p^k divise n de sorte que

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}.$$

On dira que *n et m sont premiers entre eux* si pour tout $p \in \mathcal{P}$, $v_p(n).v_p(m) = 0$.

Remarque : la valuation p-adique permet de définir une norme ultramétrique sur $\mathbb{Q}$ par la formule $|a/b|_p = p^{v_p(b)-v_p(a)}$; comme on a construit $\mathbb{R}$ à partir de $\mathbb{Q}$ et de la valeur absolue, on peut alors construire la complétion $\mathbb{Q}_p$ de $\mathbb{Q}$ pour $|-|_p$.

Lemme 1.14. — ***(de Gauss)*** *Soient $a, b, c \in \mathbb{Z}$ tels que a divise bc avec a premier avec b ; alors a divise c.*

Preuve : Il s'agit donc de montrer que pour tout $p \in \mathcal{P}$, $v_p(a) \leq v_p(c)$. Si $v_p(a) = 0$ c'est clair ; supposons donc $v_p(a) \geq 1$ auquel cas $v_p(b) = 0$ et le résultat découle alors du fait que $v_p(a) \leq v_p(bc) = v_p(b) + v_p(c)$. □
Remarque : si a et b sont premiers entre eux et divisent c alors ab divise c ; en effet on a $c = au$ avec d'après le lemme de Gauss b qui divise u. On notera bien que l'hypothèse est nécessaire puisque $a = b = 2$ divise $c = 2$ mais que 4 ne divise pas 2.

1.2. Plus grand diviseur commun. —

Définition 1.15. — Pour $a, b \in \mathbb{Z}$, on note

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a), v_p(b)\}}, \qquad a \vee b = \prod_{p \in \mathcal{P}} p^{\max\{v_p(a), v_p(b)\}}.$$

Remarque : comme $\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} = v_p(a) + v_p(b)$, on en déduit que $(a \wedge b).(a \vee b) = ab$.

Proposition 1.16. — *L'entier $a \wedge b$ (resp. $a \vee b$) est le plus grand diviseur (resp. petit multiple) commun de a et b que l'on appelle encore le pgcd (resp. ppmc) de a et de b.*

Preuve : Comme pour tout $p \in \mathcal{P}$, $\min\{v_p(a), v_p(b)\} \leq v_p(a), v_p(b)$, on en déduit que $a \wedge b$ est un diviseur de a et de b. Par ailleurs si d divise a et b alors pour tout $p \in \mathcal{P}$, $v_p(d) \leq \min\{v_p(a), v_p(b)\}$ de sorte que d divise $a \wedge b$, d'où le résultat. Le cas du ppcm se montre de la même façon. □
Remarque : a et b sont premiers entre eux au sens de la définition 1.13 si et seulement si leur pgcd est égal à 1. Par ailleurs les entiers $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux.

On vérifie aisément que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$; en ce qui concerne $a \wedge b$, on a le résultat suivant qui donne une autre caractérisation du pgcd.

Proposition 1.17. — *Le sous-groupe de $\mathbb{Z}$ engendré par a et b est $(a \wedge b)\mathbb{Z}$.*

Preuve : Notons n l'entier naturel tel que $n\mathbb{Z}$ est le groupe engendré par a et b ; comme a et b appartiennent à $n\mathbb{Z}$, on en déduit que $n|a$ et $n|b$ et donc $n|a \wedge b$. En outre n s'écrit sous la forme $ua + vb$ de sorte que $a \wedge b|ua + vb = n$ d'où le résultat. □
Remarque : on déduit de la proposition précédente **le théorème de Bézout**, i.e. il existe des entiers relatifs u, v tels que $a \wedge b = ua + vb$.

Que ce soit pour calculer $a \wedge b$ où les coefficients u, v d'une relation de Bézout, il n'est pas nécessaire de calculer la factorisation en facteurs premiers de a et b, on dispose heureusement de l'*algorithme d'Euclide* : on pose $r_0 = a$ et $r_1 = b$. On construit alors par récurrence r_{i+1} comme le reste de la division euclidienne de r_{i-1} par r_i si ce dernier et non nul et sinon $r_{i+1} = 0$. Comme la suite est strictement décroissante et positive, il existe un indice $n \geq 1$ tel que $r_n > 0$ et $r_{n+1} = 0$. On pose par ailleurs

$$u_0 = 1, \quad u_1 = 0 \text{ et } v_0 = 0, \quad v_1 = 1,$$

$$u_{i+1} = u_{i-1} - u_i q_i \text{ et } v_{i+1} = v_{i-1} - v_i q_i$$

où pour tout $i = 1, \cdots, n-1$, q_i est le quotient de la division euclidienne de r_{i-1} par r_i.

Proposition 1.18. — *L'entier r_n est alors le pgcd de a et b avec $r_n = au_n + bv_n$.*

Preuve : Comme $r_{i-1} = q_i r_i + r_{i+1}$, alors $r_{i-1} \wedge r_i = r_i \wedge r_{i+1}$ et donc $a \wedge b = r_{n-1} \wedge r_n = r_n$ car $r_{n+1} = 0$. En ce qui concerne la relation de Bézout, il suffit de vérifier que pour tout $i = 1, \cdots, n$, on a $r_i = au_i + bv_i$. C'est clairement vrai pour $i = 0, 1$ et supposons que pour $1 \leq k < n$, la relation soit vraie pour tout $i \leq k$. On a alors

$$r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1}a + v_{k-1}b) - q_k(u_k a + v_k b) = au_{k+1} + bv_{k+1}$$

d'où le résultat. □
Remarque : Lamé a montré que si l'algorithme d'Euclide s'arrête au bout de n pas alors

$$a \geq (a \wedge b)F_{n+2}, \qquad b \geq (a \wedge b)F_{n+1}$$

où $F_0 = 0$, $F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$ est la suite de Fibonacci. Pour le montrer on raisonne par récurrence sur n, le cas $n = 1$ étant trivial ; le premier pas transforme (a, b) en $(b, c = a - qb)$ avec donc par hypothèse de récurrence $b \geq a \wedge bF_{n+1}$ et $c \geq a \wedge bF_n$ et donc $a \geq b + c \geq a \wedge b(F_n + F_{n+1}) = a \wedge bF_{n+2}$. On notera en particulier que le cas le pire est pour le couple (F_{n+1}, F_n).
1.19 — Résolution de l'équation $ax + by = c$: si c n'est pas divisible par $a \wedge b$ l'équation n'a pas de solution ; sinon en divisant cette équation par $a \wedge b$, on se ramène au cas où a et b sont premiers entre eux. Considérons alors une relation de Bézout $au_0 + bv_0 = 1$; si $au + bv = 1$ est une autre relation de Bézout, on a alors $a(u - u_0) = b(v_0 - v)$ de sorte que d'après le lemme de Gauss il existe q tel que $u = u_0 + qb$ et $v = v_0 - qa$. Les solutions (x, y) s'obtiennent alors de la même manière à partir d'une solution particulière $(x_0, y_0) = (cu_0, cv_0)$ et donc $(x, y) = (x_0 + qb, y_0 - qa)$. En ce qui concerne les solutions positives, on renvoie à l'exercice suivant.

1.3. Quelques résultats de la théorie des groupes. — Pour certaines des preuves des résultats de ce paragraphe, nous aurons besoin des notions de groupe (abélien), sous-groupe, groupe quotient ; précisément nous aurons besoin du théorème de Lagrange ainsi que le théorème de factorisation d'un morphisme de groupes. Comme le but de ce cours n'est pas de s'étendre sur la théorie des groupes nous rappelons très rapidement ces notions et résultats. Nous reprendrons ensuite au paragraphe suivant tout ceci dans le cadre de $\mathbb{Z}$.

- *Un groupe* (abélien) $(G,+)$ est un ensemble non vide G muni d'une loi interne $+ : G\times G \to G$, associative (commutative) admettant un élément neutre et tel que tout élément possède un opposé. *Un sous-groupe* H de G est un sous-ensemble non vide de G stable par la loi $+$ tel que pour tout $n \in H$, l'élément $-n \in H$.

Définition 1.20. — Un groupe est dit cyclique s'il est fini et engendré par un seul élément. L'ordre d'un élément d'un groupe G est par définition le cardinal du groupe qu'il engendre.

Remarque : bien que les groupes cycliques sont des exemples particulièrement simples, ils permettent de décrire et comprendre complètement les groupes abéliens finis : en effet on peut montrer que tout groupe abélien fini est un produit de groupes cycliques.

- Soit $f : G_1 \to G_2$ un morphisme de groupes ; *le noyau* $\operatorname{Ker} f$ de f est par définition le sous-ensemble de G_1 des éléments qui s'envoient sur l'élément neutre de G_2 ; c'est un sous-groupe de G_1 qui est réduit à l'élément neutre si et seulement si f est injectif.
- Étant donnés un sous-groupe H d'un groupe abélien G, on considère sur l'ensemble G la relation d'équivalence suivante :

$$g \sim g' \Leftrightarrow g - g' \in H;$$

l'ensemble des classes d'équivalence est alors noté G/H lequel est muni, via la loi de G, d'une structure de groupe tel que l'application $\pi : G \to G/H$ qui à g associe sa classe d'équivalence, est un morphisme de groupes.

Théorème 1.21. — ***(Lagrange)*** *Si G est un groupe fini et H un sous-groupe, alors le cardinal de H divise celui de G.*

Preuve : Les classes d'équivalence de G/H sont en bijection avec H et sont donc toutes de même cardinal de sorte que $|G| = |G/H|.|H|$, d'où le résultat. □

- Le morphisme $f : G_1 \to G_2$ induit alors un morphisme injectif $\bar{f} : G_1/\operatorname{Ker} f \to G_2$ tel que $f = \bar{f} \circ \pi$, où $\pi : G \to G/\operatorname{Ker} f$ désigne le morphisme canonique.

1.4. Congruences. — Nous allons reprendre dans le cas de $\mathbb{Z}$, toutes les notions du paragraphe précédent.

Définition 1.22. — Pour $n \in \mathbb{Z}$, on munit $\mathbb{Z}$ de la relation d'équivalence suivante :

$$x \sim_n y \Leftrightarrow n|x-y$$

et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence. On notera $\bar{x}$ la classe associée à $x \in \mathbb{Z}$, i.e. $\bar{x} = \{x + kn : \ k \in \mathbb{Z}\}$, de sorte que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$. Deux éléments x, y d'une même classe seront dits congrus modulo n et on le notera sous la forme $x \equiv y \mod n$.

Remarque : l'addition de $\mathbb{Z}$ muni l'ensemble $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe ; en effet soit $\bar{x}, \bar{y}$ deux classes d'équivalence, on définit alors $\bar{x} + \bar{y} = \overline{x_0 + y_0}$ où x_0 et y_0 sont des éléments quelconques de $\bar{x}$ et $\bar{y}$ respectivement. Le fait, trivial mais primordial, est que le résultat $\overline{x_0 + y_0}$ ne dépend pas du choix de x_0 et y_0. On notera

$$\psi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$$

la surjection dite canonique qui à un entier x associe sa classe d'équivalence $\bar{x}$.
Remarque : tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$; en effet soit $G =< g >$ et considérons le morphisme $f : \mathbb{Z} \to G$ qui à 1 associe g. Par définition le noyau de f est $n\mathbb{Z}$ de sorte que f induit un isomorphisme $\bar{f} : \mathbb{Z}/n\mathbb{Z} \simeq G$.

Proposition 1.23. — *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de cardinal d où d est un diviseur de n. Réciproquement pour tout $d|n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.*

Preuve : Le premier point est un cas particulier du théorème de Lagrange. Réciproquement soit H un sous-groupe de $G = \mathbb{Z}/n\mathbb{Z}$; considérons et $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow G/H$, où G/H est le groupe quotient de G par H. Le noyau de ϕ est un sous-groupe de $\mathbb{Z}$ donc de la forme $d\mathbb{Z}$, contenant $\operatorname{Ker}\psi = n\mathbb{Z}$, de sorte que d divise n. Ainsi H est cyclique, engendré par la classe de d ; son ordre est n/d. □

Corollaire 1.24. — *Le groupe engendré par un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est le groupe engendré par $\overline{k \wedge n}$; il est de cardinal $\frac{n}{n\wedge k}$.*

Preuve : Comme k est un multiple de $k \wedge n$, on a l'inclusion $(k) \subset (k \wedge n)$. Réciproquement on écrit une relation de Bezout $uk + vn = n \wedge k$ de sorte que modulo n, $n \wedge k$ appartient au groupe engendré par k et donc $(k \wedge n) \subset (k)$. On en déduit alors que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ qui est par définition le cardinal du groupe engendré par k, est $\frac{n}{n\wedge k}$. □
Remarque : un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur si et seulement si $k \wedge n = 1$; on notera $\psi(n)$ le cardinal de l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$, et donc aussi le cardinal des $1 \leq k \leq n$ premiers avec n.

Corollaire 1.25. — *L'ensemble des éléments d'ordre $d|n$ (resp. d'ordre divisant d) dans $\mathbb{Z}/n\mathbb{Z}$ est de cardinal $\psi(d)$ (resp. d). Par ailleurs on a $n = \sum_{d|n} \psi(d)$.*

Preuve : Remarquons tout d'abord que si d ne divise pas n, il n'y a aucun élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Si d divise n, tous les éléments d'ordre d appartiennent au groupe engendré par $(\frac{n}{d})$ qui est isomorphe, en tant que groupe cyclique d'ordre d, à $\mathbb{Z}/d\mathbb{Z}$. Ainsi les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre d de $\mathbb{Z}/d\mathbb{Z}$ qui sont en nombre $\psi(d)$.

Cherchons maintenant les éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z}$ qui sont donc d'ordre divisant $d \wedge n$ et qui appartiennent au groupe engendré par $\frac{n}{n\wedge d}$ isomorphe à $\mathbb{Z}/(n \wedge d)\mathbb{Z}$. Ainsi, comme précédemment, les éléments d'ordre divisant d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre divisant $n \wedge d$ de $\mathbb{Z}/(n \wedge d)\mathbb{Z}$, qui sont en nombre $n \wedge d$.

La dernière égalité découle du dénombrement des éléments de $\mathbb{Z}/n\mathbb{Z}$ selon leur ordre. □

Théorème 1.26. — ***(chinois)*** *Soient n et m des entiers premiers entre eux ; l'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui à un entier k associe sa classe modulo n et m, induit un isomorphisme*

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}.$$

Preuve : Considérons tout d'abord un élément k du noyau de sorte que n et m divise k et comme $n \wedge m = 1$, d'après le lemme de Gauss $nm|k$. Ainsi le noyau est contenu dans $nm\mathbb{Z}$, l'inclusion réciproque étant évidente de sorte que l'on a une injection de $\mathbb{Z}/nm\mathbb{Z} \hookrightarrow \mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}$ qui est un isomorphisme par égalité des cardinaux. □
Remarque : il peut être utile de savoir déterminer un antécédent d'un couple $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Pour cela on part d'une relation de Bézout $un + vm = 1$ et on pose $k = unb + vma$; on vérifie aisément que comme $un \equiv 1 \mod m$ et $vm \equiv 1 \mod n$, on a $k \equiv a \mod n$ et $k \equiv b \mod m$. Dans le cas où $n \wedge m = d$, le noyau est $n \vee m\mathbb{Z}$ et l'image

$$\{(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} : \ d|a - b\}.$$

1.27 — L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est aussi muni d'une structure d'anneau déduite de celle de $\mathbb{Z}$; on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$, i.e. l'ensemble des éléments inversibles muni de la multiplication.

Proposition 1.28. — *Un élément $k \in \mathbb{Z}/n\mathbb{Z}$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement s'il est un générateur additif de $\mathbb{Z}/n\mathbb{Z}$. En particulier $(\mathbb{Z}/n\mathbb{Z})^\times$ est de cardinal $\varphi(n)$.*

Preuve : Par définition k est inversible si et seulement s'il existe k' tel que $kk' \equiv 1 \mod n$, i.e. s'il existe $\lambda \in \mathbb{Z}$ tel que $kk' + \lambda n = 1$ ce qui est équivalent à $k \wedge n = 1$ et donc k est un générateur de $\mathbb{Z}/n\mathbb{Z}$. □
Remarque : comme $\mathbb{Z}/n\mathbb{Z}$ est monogène tout morphisme de source $\mathbb{Z}/n\mathbb{Z}$ est déterminé par l'image de $\bar{1}$ de sorte qu'en particulier le groupe $\mathrm{aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollaire 1.29. — *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n = p$ est premier auquel cas on le notera $\mathbb{F}_p$.*

Théorème 1.30. — ***(de Fermat)*** *Pour tout $n \in \mathbb{Z}$ et $k \wedge n = 1$, on a $k^{\varphi(n)} \equiv 1 \mod n$.*

Preuve : Nous avons vu que le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à $\varphi(n)$ et comme l'ordre d'un élément divise le cardinal du groupe, l'ordre de k divise $\varphi(n)$ et donc $k^{\varphi(n)} \equiv 1 \mod n$. □

Proposition 1.31. — *Pour $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, on a*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

Preuve : Le théorème chinois donne un isomorphisme

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times;$$

le résultat découle alors du fait que le cardinal des $1 \leq k \leq p^\alpha$ divisible par p est de cardinal $p^{\alpha-1}$ et donc $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. □

En ce qui concerne les $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, on a le résultat suivant que nous admettrons.

Proposition 1.32. — *Pour p premier impair et $\alpha \geq 1$, $(\mathbb{Z}/p^a\mathbb{Z})^\times$ est cyclique et pour $p = 2$, on a*

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}).$$

1.33 — Loi de réciprocité quadratique : on dit qu'un élément $a \in \mathbb{F}_p$ est un carré s'il existe $b \in \mathbb{F}_p$ tel que $a = b^2$.

Définition 1.34. — Pour $p \geq 3$ premier, le symbole de Legendre $(\frac{n}{p})$ est défini par :

$$(\frac{n}{p}) = \begin{cases} 0 \text{ si } p \text{ divise n} \\ +1 \text{ si } n \text{ est un carré dans } \mathbb{F}_p \\ -1 \text{ sinon} \end{cases}$$

Remarque : l'application $x \in \mathbb{F}_p^\times \mapsto x^2 \in \mathbb{F}_p^\times$ est un morphisme de groupe multiplicatif, dont le noyau est $\{-1, 1\}$ et donc de cardinal 2 ; ainsi son image qui est l'ensemble $\mathbb{F}_p^{\times 2}$ des carrés de $\mathbb{F}_p^\times$ est de cardinal $(p-1)/2$. Rappelons par ailleurs que d'après le petit théorème de Fermat, pour tout $x \in \mathbb{F}_p^\times$, on a $x^{p-1} = 1$ et donc $x^{(p-1)/2} = \pm 1$. Ainsi si $x \in \mathbb{F}_p^{\times 2}$, x est une solution de l'équation $X^{(p-1)/2} = 1$ laquelle dans $\mathbb{F}_p$ possède au plus $(p-1)/2$ solutions. Ainsi d'après

ce qui précède, $\mathbb{F}_p^{\times 2}$ est exactement égal à l'ensemble des racines de l'équation $X^{(p-1)/2} = 1$ dans $\mathbb{F}_p$ et que $(\frac{n}{p}) \equiv n^{(p-1)/2} \mod p$. On remarque en particulier que le symbole de Legendre est multiplicatif, i.e.

$$(\frac{nn'}{p}) = (\frac{n}{p})(\frac{n'}{p}).$$

Le calcul explicite des symboles de Legendre se fait au moyen du

Lemme 1.35. — ***(de Gauss)*** *Pour tout p premier impair on a $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.*

ainsi que de la loi de réciprocité quadratique :

Théorème 1.36. — *Pour tout p, q premiers impairs, on a*

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

Il y a plus de 200 preuves différentes de ce résultat ; historiquement la première est due à Gauss via l'utilisation des sommes de Gauss. Une preuve particulièrement élémentaire est d'identifier le symbole de Legendre avec la signature de la permutation de $\mathbb{Z}/q\mathbb{Z}$ associée à la multiplication par p.

Exercice 1.1. — ***** *Existe-t-il des couples $(a, b) \in \mathbb{N}^2$ tels que :*
- *$ab(a + b)$ n'est pas divisible par 7 ;*
- *$(a + b)^7 - a^7 - b^7$ est divisible par 7^7 ?*

Essayons de factoriser $P(x) = (x+1)^7 - x^7 - 1$ en regardant ses racines : on remarque qu'outre 0 et 1, le nombre complexe $j = e^{2i\pi/3}$ est aussi racine car $j + 1 = -j^2$ de sorte que $P(x)$ est divisible par $x(x + 1)(x^2 + x + 1)$ le quotient étant égal à $x^2 + x + 1$ et donc

$$(a + b)^7 - a^7 - b^7 = 7ab(a + b)(a^2 + ab + b^2)^2.$$

On est ainsi amené à résoudre $a^2 + ab + b^2 \equiv 0 \mod 7^3$ qui s'écrit encore

$$(a + \frac{b}{2})^2 \equiv -3(\frac{b}{2})^2 \mod 7^3$$

laquelle possède des solutions si et seulement si le symbole de Legendre $(\frac{-3}{7^3}) = 1$ ce que l'on vérifie aisément en utilisant la loi de réciprocité quadratique.

1.5. Exercices. —

Exercice 1.2. — ***** *Soit $n \geq 2$; montrez que si $k^2 + k + n$ est premier pour tout entier $0 \leq k \leq \sqrt{n/3}$ alors c'est encore vrai pour tout entier $0 \leq k \leq n - 2$.*
Remarque : on peut montrer que les seules valeurs n telles que la condition de l'énoncé est vérifiée sont $2, 3, 5, 16$ et 41 ; on peut montrer que cette condition est équivalent à demander que $\mathbb{Z}[\sqrt{1 - 4n}]$ est factoriel, résultat prouvé par Heegner en 1952 alors qu'il était professeur de lycée à Berlin. Par ailleurs le lecteur notera que si on numérote les entiers en spirale autour de n, les nombres $k^2 + k + n$ sont sur la diagonale $y = x$: spirales d'Ulam.

Exercice 1.3. — ****** *On considère l'ensemble suivant $\mathcal{E} \subset \mathbb{N}$ constitué des nombres dont l'écriture n en base 3 est de la forme $\sum_{i=0}^{10} a_i 3^i$ avec $a_i = 0, 1$. Montrez que trois éléments quelconques de $\mathcal{E}$ ne sont pas les termes consécutifs d'une progression arithmétique.*
Remarque : que pensez-vous de l'avenir de l'exercice suivant : existe-il 2008 entiers > 0 inférieurs ou égaux à 10^5 et tels que trois quelconques d'entre eux ne soient pas les termes consécutifs d'une progression arithmétique ?

Exercice 1.4. — *Dans l'émission Fort-Boyard, les candidats jouent au jeu suivant : sont disposés alignées n craies et les deux joueurs en retirent chacun à leur tour $1, 2$ ou 3, le gagnant étant celui qui retire la dernière craie. Trouvez une stratégie gagnante.*

Exercice 1.5. — *Trouvez les sous-groupes de $\mathbb{Z}$ contenant $48\mathbb{Z}$ et donnez leurs relations d'inclusion.*

Exercice 1.6. — ** *Un entier > 0 est dit alterné si deux chiffres quelconques de son écriture décimale sont de parité différentes.*

(i) Montrez que si $20|n$ alors n n'est pas alterné.

(ii) Soit n possédant un multiple alterné de premier chiffre impair ; montrez alors que pour tout $m \wedge 10$, l'entier mn possède un multiple alterné.

(iii) Montrez que pour tout k, 5^k possède un multiple alterné de k chiffres.

(iv) Pour tout k, 2^k possède un multiple alterné A_k de k chiffres avec k et $A_k/2^k$ de même parité.

(v) Montrez que tout entier n non divisible par 20, possède un multiple alterné.

Exercice 1.7. — * *Montrez la formule de Legendre*

$$v_p(n!) = \sum_{k\geq 1} \lfloor \frac{n}{p^k} \rfloor = a_1 + a_2 p + \cdots + a_k p^{k-1}) + (a_2 + \cdots + a_k p^{k-2}) + \cdots + (a_{k-1} + a_k p) + a_k$$

où $n = a_0 + a_1 p + \cdots + a_k p^k$ est l'écriture de n en base p.

Déduisez-en que la valuation 2-adique du coefficient binomial $\binom{b}{a+b}$ est égale à la somme $\sum_{k=0}^{+\infty} a_k b_k$ où $a = \sum_{k=0}^{+\infty} a_k 2^k$ et $b = \sum_{k=0}^{+\infty} b_k 2^k$ sont les écritures en base 2 de a et b ; en particulier notez que pour $0 < k < n$, $\binom{k}{n}$ est pair.

Exercice 1.8. — ***(* Un argument de descente infinie à la Fermat)*** *Soient $a, b > 0$ tels que $ab + 1|a^2 + b^2$; montrez que le quotient est un carré parfait.*

Exercice 1.9. — * *Soit n impair.*

(i) Montrez que $v_3(2^n + 1) = v_3(n) + 1$.

(ii) Montrez que si n est tel que n^2 divise $2^n + 1$ alors n est un puissance de 3 ; laquelle ?

Exercice 1.10. — *** *Soit $\mathcal{E}$ un ensemble de 2008 entiers distincts strictement positifs dont tous les diviseurs premiers sont ≤ 23. Montrez que l'on peut trouver 4 éléments distincts de $\mathcal{E}$ dont le produit est la puissance quatrième d'un entier.*

Exercice 1.11. — *Soient a et b des entiers premiers entre eux tels que leur produit est une puissance k-ème d'un entier pour $k \geq 2$ entier. Montrez alors que a et b sont eux-mêmes des puissances k-ème d'entiers.*

Exercice 1.12. — *Donnez en fonction de n, le pgcd $(n^3 + n^2 + 1, n^2 + 2n - 1)$.*

Exercice 1.13. — *Donnez en fonction de n, le pgcd $(n^3 + n^2 - 6n + 2, 2n^2 + 5n - 3)$.*

Exercice 1.14. — * *Trouvez les solutions entières de l'équation diophantienne $y^2 - 4 = x^3$.*

Exercice 1.15. — * *Construisez pour tout $n \geq 4$, un ensemble $\{k, k+1, \cdots, k+n-1\}$ de n entiers consécutifs tel que le plus grand $k + n - 1$ divise le ppcm des $n - 1$ premiers.*

Exercice 1.16. — *Montrez la relation*

$$F_{n+m} = F_{n+1}F_m + F_nF_{m-1}$$

et déduisez-en que $F_n \wedge F_m = F_{n\wedge m}$.

Exercice 1.17. — ***** *Variations sur le théorème de Bezout :*

(a) En utilisant l'algorithme d'Euclide, trouver les relations de Bezout entre 650 *et* 66.

(b) On suppose que l'on ne dispose que de pieces de valeurs a *et* b *entières avec* $(a, b) = 1$.

(i) Quelles sommes peut-on payer si on nous rend la monnaie ?

(ii) Même question si on ne peut pas nous rendre la monnaie ? (Indication : montrer que si $m + n = ab - a - b$ *alors exactement une somme parmi* m *et* n *est payable).*

(c) Etudiez le cas de 3 *pièces de valeur* 15, 20 *et* 48 *en montrant que* 217 *est la plus grande somme que l'on ne peut pas payer.*

(d) Généralisez (c) en montrant que pour $a, b, c > 0$ *premiers entre eux deux à deux,* $2abc - ab - bc - ac$ *est le plus grand entier qui ne peut pas s'écrire sous la forme* $xbc + yca + zab$ *avec* $x, y, z \geq 0$.

(e) Montrez par récurrence sur n *que si* $a_1, \cdots, a_n$ *sont* n *entiers strictement positifs premiers entre eux deux à deux alors*

$$a_1 \cdots a_n \Big(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i} \Big)$$

est le plus grand entier qui ne peut pas s'écrire sous la forme $\sum_{i=1}^{n} x_i \prod_{j\neq i} a_j$ *avec* $x_i \geq 0$ *pour tout* $i = 1, \cdots, n$.

Exercice 1.18. — *Montrez que* 7 *divise* $3^{105} + 4^{105}$.

Exercice 1.19. — *Montrez l'équivalence* $3|a$ *et* $3|b \iff 3|a^2 + b^2$.

Exercice 1.20. — *Proposez à vos amis doués en calcul mental le jeu suivant : multiplier par* 13 *leur jour de naissance, multiplier par* 14 *leur mois de naissance, additionner ces deux résultats pour former un nombre* n *qu'il vous communique. Comment retrouver les données cachées ?*

Exercice 1.21. — *Un nouveau jeu pour des amis coopératifs : choisir un nombre* k *entre* 1 *et* 8, *puis communiquer le résultat* $n = 10A - 9k$ *où* A *est l'âge du candidat. Expliquez comment vous retrouvez* A.

Exercice 1.22. — *(i) Donnez le cardinal de l'ensemble des éléments d'ordre divisant* d *dans* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(ii) Pour $d = pq$ *avec* p *et* q *premiers divisant* n, *donnez le nombre d'éléments d'ordre* d *dans* $(\mathbb{Z}/n\mathbb{Z})^2$.

Exercice 1.23. — *En rappelant le cadre général, donnez les sous-groupes de* $\mathbb{Z}/24\mathbb{Z}$ *ainsi que leurs relations d'inclusion. On précisera aussi le sous-groupe engendré par* 18 *(resp.* 16*) ainsi que les sous-groupes contenant* (16) *et* (10) *puis ceux contenant* (16) *et inclus dans* (18).

Exercice 1.24. — *Donnez les morphismes de groupe* $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ *puis ceux de* $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$. *Trouvez une condition nécessaire et suffisante sur* m *et* n *pour que tout morphisme* $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ *soit nul.*

Exercice 1.25. — *Montrez l'équivalence* $6|a + b + c \iff 6|a^3 + b^3 + c^3$.

Exercice 1.26. — *Montrez que* 429 *est inversible dans* $\mathbb{Z}/700\mathbb{Z}$ *et donnez son inverse.*

Exercice 1.27. — *Soit* $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *l'application qui à* $k \in \mathbb{Z}$ *associe sa classe modulo* n *et* m*. Précisez le noyau et l'image de* π*. Donnez alors l'ensemble des* $k \in \mathbb{Z}$ *tels que*
(i) $k \equiv 2 \mod 5$ *et* $k \equiv 4 \mod 7$ *;*
(ii) $k \equiv 3 \mod 10$ *et* $k \equiv 2 \mod 6$ *;*
(iii) $k \equiv 4 \mod 10$ *et* $k \equiv 2 \mod 6$ *;*
Que peut-on dire de la congruence de k *modulo* 10 *sachant* $k \equiv 3 \mod 6$ *?*

Exercice 1.28. — *Résoudre dans* $\mathbb{Z}$ *les congruences suivantes :*
(i) $3x \equiv 4 \mod 7$ *;*
(ii) $9x \equiv 12 \mod 21$ *;*
(iii) $103x \equiv 612 \mod 676$.

Exercice 1.29. — *Donnez la congruence modulo* 17 *de* $(1035125)^{5642}$.

Exercice 1.30. — *Donnez la congruence modulo* 18 *de* 1823^{242} *puis celle de* 2222^{321} *modulo* 20.

Exercice 1.31. — *Montrez que* $n^7 \equiv n \mod 42$.

Exercice 1.32. — *Montrez que si* $p \neq 2$ *premier divise* $a^2 + b^2$, $a, b \in \mathbb{N}$ *non divisible par* p, *alors* $p \equiv 1 \mod 4$.

Exercice 1.33. — *Montrez que* $n^7 \equiv n \mod 42$.

Exercice 1.34. — *(*** théorème de Erdös-Ginzburg-Ziv) Soit* p *premier et* $\{x_1, \cdots, x_{2p-1}\} \subset \mathbb{N}$ *; pour* $I \subset [1, 2p-1]$, *on note* $S_I = \sum_{i \in I} x_i$ *et*

$$\Sigma = \sum_{I \subset [1,2p-1],\ |I|=p} S_I^{p-1}.$$

Montrez que $\Sigma \equiv 0 \mod p$ *et en déduire qu'il existe* I *tel que* $S_I \equiv 0 \mod p$. *En déduire que pour tout ensemble de* $2n-1$ *entiers, on peut en extraire* n *dont la somme est divisible par* n.

Exercice 1.35. — ** Soit* p *un nombre premier impair.*
(i) Montrez que $1+p+\cdots+p^{p-1}$ *admet un facteur premier* q *impair non congru à* 1 *modulo* p^2.
(ii) Montrez que pour tout entier n, q *ne divise pas* $n^p - p$.

Exercice 1.36. — ** Déterminez tous les entiers* $n > 0$ *qui sont premiers avec tous les nombres de la forme* $2^k + 3^k + 6^k - 1$.

Exercice 1.37. — *Étudiez les solutions entières de l'équation* $(x^2 - 9)(x^2 - 16) = y^2$.

Exercice 1.38. — *On considère l'équation* $y^2 = x^3 + 7$ *:*
(i) Montrez qu'il n'y a pas de solutions avec x *pair ;*
(ii) En écrivant l'équation sous la forme $y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$ *et en utilisant l'exercice 1 b, en déduire qu'il n'existe pas de solutions entières.*

Exercice 1.39. — *Trouvez les entiers* $n, m \in \mathbb{Z}$ *tels que les trois derniers chiffres de l'écriture décimale de* 2008^n *soient les mêmes et dans le même ordre que ceux de* 2008^m.

Exercice 1.40. — ** En raisonnant modulo 3 puis modulo 9, montrez que l'équation*

$$x^3 - 3xy^2 + y^3 = 2891$$

n'a pas de solutions entières.

Exercice 1.41. — ** Existe-t-il des couples $(a, b) \in \mathbb{N}^2$ tels que :*
- *$ab(a + b)$ n'est pas divisible par 7 ;*
- *$(a + b)^7 - a^7 - b^7$ est divisible par 7^7 ?*

2. Nombres premiers

2.1. Développement décimal. — Partons de quelques constatations amusantes :

$$\frac{1}{7} = 0,142\ 857\ 142\ 857\ 142\ 857\cdots$$

avec $7 \times 142857 = 999999$, $142 + 857 = 999$, $14 + 28 + 57 = 99$, $1 + 4 + 2 + 8 + 5 + 7 = 3 \times 9$ et encore

$$\frac{1}{7} = 0,142857\cdots, \quad \frac{2}{7} = 0,285714\cdots, \quad \frac{3}{7} = 0,428571\cdots$$
$$\frac{4}{7} = 0,571428\cdots, \quad \frac{5}{7} = 0,714285\cdots, \quad \frac{6}{7} = 0,857142\cdots$$

Sans calculs le 53-ème chiffre de $1/53$ est 0, le 52-ème étant 3 car $3 \times 3 = 9$. Essayons désormais d'ordonner toutes ces coïncidences.

Proposition 2.1. — *Le développement décimal de $\frac{1}{p}$ est périodique, après la virgule, de période l'ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^\times$.*

Preuve : L'écriture s'obtient en effectuant la division euclidienne par p, puis en multipliant le reste par 10 et en effectuant la division euclidienne par p... Ainsi en notant r_k les restes et q_k les quotients qui sont donc les chiffres du développement décimal de $\frac{1}{p}$, on a :

$$\begin{aligned} r_0 &= 1 \\ r_1 &= 10r_0 - q_1 p \\ &\vdots \\ r_k &= 10r_{k-1} - q_k p. \end{aligned}$$

On a donc $r_k \equiv 10^k \mod p$ et si on note k_0 l'indice à partir duquel le développement est périodique de période T, on a $q_{k_0+T} = q_k$ avec $r_{k_0+T} = r_k$ et donc $10^{k_0+T} \equiv 10^{k_0} \mod p$ soit $10^T \equiv 1 \mod p$. On en déduit que $r_0 = r_T$ et donc $q_1 = q_{T+1}$, i.e. le développement est périodique dès le premier chiffre après la virgule. Notons alors $d|T$ l'ordre de 10 modulo p ; comme précédemment on a $r_{k+d} = r_k$ pour tout $k > 0$ et donc $q_{k+d} = q_k$ et donc $T|d$ d'où le résultat. □

Exemples $\frac{1}{13} = 0,076923\cdots$ et 10 est d'ordre 6 dans $(\mathbb{Z}/13\mathbb{Z})^\times$.

Remarque : le même raisonnement s'applique pour les $\frac{k}{p}$ avec $1 \leq k \leq p - 1$.

Corollaire 2.2. — *Soit T la période du développement décimal de $\frac{1}{p} = 0, a_1 a_2 \cdots, a_T\ a_1 \cdots$ et notons $n = \sum_{i=1}^{d} a_i 10^{T-i}$. On a alors*

$$np = 10^T - 1.$$

Preuve : On a l'égalité

$$\frac{1}{p} = \sum_{i=1}^{+\infty} n10^{-iT} = \frac{10^{-T}n}{1-10^{-T}} = \frac{n}{10^T - 1}$$

et donc $np = 10^T - 1$. □

Remarque : pour retrouver l'entier n associé à $p = 7$, on peut partir de l'égalité $999999 = 7n$ soit classiquement par division $999999 = 7 \times 100000 + 299999...$ soit au contraire en partant de droite : $999999 = 7 \times 7 + 999950...$ C'est comme cela par exemple que l'on trouve aisément le $p-1$-ème chiffre du développement décimal de $1/p$.

Remarque : comme $10^{p-1} - 1$ s'écrit avec un nombre pair de 9, l'entier pn est divisible par 99 et donc pour $p \neq 3, 11$, n est divisible par 99 ainsi donc que la somme de ses paquets de 2 chiffres ($100 \equiv 1 \mod 99$). Si $3|p-1$ alors n est divisible par 999 ainsi donc que la somme de ses paquets de 3 chiffres ($1000 \equiv 1 \mod 999$). Dans le même genre d'idée, on a le résultat suivant.

Proposition 2.3. — *Soit $d = 2e$ un multiple de l'ordre T de 10 dans $(\mathbb{Z}/p\mathbb{Z})^\times$ tel que e n'est pas un multiple de T. Pour*

$$A = \sum_{i=1}^{e} a_i 10^{e-i}, \qquad B = \sum_{i=1}^{e} a_{e+i} 10^{e-i}.$$

on a alors $A + B = 10^e - 1$.

Preuve : On a $n = 10^e A + B$ avec $0 \leq A, B < 10^e - 1$ car $p > 1$. Ainsi on a

$$\frac{10^{2e}}{p} = 10^e A + B + \frac{1}{p} \Rightarrow \frac{10^e + 1}{p} \times (10^e - 1) = 10^e A + B$$

. Or comme $(10^e)^2 \equiv 1 \mod p$ et que $10^e \not\equiv 1 \mod p$, on en déduit que $10^e + 1 \equiv 0 \mod p$ de sorte que $A + B \equiv 0 \mod 10^e - 1$ et le résultat découle de l'encadrement $1 \leq A + B < 2(10^e - 1)$. □

Remarque : dans le cas où T est divisible par r, le raisonnement précédent donne que la somme des paquets de T/r chiffres de n est de la forme $k(10^r - 1)$ avec $1 \leq k < r$.

Exemples $\frac{1}{19} = 0,052631578947368421\cdots$ et on a

$$052+631+578+947+368+421 = 3\times 999 \quad 05+26+31+57+89+47+36+84+21 = 4\times 99.$$

Proposition 2.4. — *Soit p premier tel que la période de son développement décimal soit égale à $p-1$; le nombre dn s'obtient alors à partir de n par permutation circulaire.*

Par exemple : pour $p = 7$, on a

$$\begin{aligned} 2 \times 142857 &= 285714 \\ 3 \times 142857 &= 428571 \\ 4 \times 142857 &= 571428 \\ 5 \times 142857 &= 714285 \\ 6 \times 142857 &= 857142 \end{aligned}$$

Preuve : On reprend les notations de la proposition 2.1 : comme $T = p - 1$ on en déduit que $\{r_1, \cdots, r_{p-1}\} = \{1, \cdots, p-1\}$. En notant $1 \leq i_0 \leq p-1$ l'indice tel que $r_{i_0} = k$, on en déduit du calcul même du développement décimal que le i-ème chiffre b_i du développement décimal de k/p est égal à $i + i_0$, d'où le résultat. □

Remarque : une autre façon d'énoncer le résultat précédent est de dire que le n_k du développement décimal de k/p s'obtient par permutation circulaire de n en utilisant, avec les notations de la proposition 2.1 le premier reste $r_i = k$. Dans le cas général où la période est égale à T un diviseur quelconque de $p-1$, les restes des divisions euclidiennes des k/p pour k décrivant $\{1, \cdots, p-1\}$ se répartissent en $(p-1)/T$ sous-ensembles de sorte que les kn pour k décrivant $\{1, \ldots, p-1\}$, à permutations circulaires près, sont en nombre $(p-1)/T$.

Théorème 2.5. — *Soit $p > 11$ premier alors $a_{(p+1)/2} = 0$ si et seulement si $(\frac{10}{p}) = 1$ et sinon elle est égale à 9.*

Preuve : On écrit $A = \sum_{i=1}^{(p-1)/2} a_i 10^{(p-1)/2-i}$ et $B = \sum_{i=1}^{(p-1)/2} a_{(p-1)/2+i} 10^{(p-1)/2-i}$ de sorte que d'après 2.3 soit $A = B$ soit $A + B = 9 \cdots 9$. Dans le premier cas comme $a_1 = 0$, on en déduit que $a_{(p+1)/2} = 0$ et dans le deuxième on obtient 9. Il faut alors décider si $(p-1)/2$ est un multiple d'une période, i.e. si $10^{(p-1)/2} \equiv 1 \mod 2$ ce qui est équivalent à $(\frac{10}{p}) = 1$ d'où le résultat. □

Remarque : d'après la loi de réciprocité quadratique, le résultat ne dépend que de la congruence de p modulo 40. Dans le même ordre d'idée, on peut facilement déterminer le $(p-1)/2$-chiffres du développement décimal de $1/p$: en effet si $(p-1)/2$ est le multiple d'une période alors ce chiffre est le même que le $p-1$-ème que l'on détermine facilement comme expliqué ci-avant. Dans le cas où $(p-1)/2$ n'est pas une période comme avec les notations ci-dessus, $A + B = 9 \cdots 9$, on en déduit que le chiffre cherché est égal à 9 moins le $(p-1)$-ème chiffre.

Notons alors $\mathcal{P}(10)$ l'ensemble des premiers p tels que leur développement décimal est de période $p-1$: cet ensemble est-il infini et si oui quel est sa densité

$$d_{10}(x) = \frac{\sharp\{p \in \mathcal{P}(10),\ p \leq x\}}{\sharp\{p \in \mathcal{P},\ p \leq x\}}, \qquad \lim_{x \to +\infty} d_{10}(x).$$

On conjecture que cette limite est égale à

$$C_{Artin} = \prod_{p \in \mathcal{P}} \Big(1 - \frac{1}{p(p-1)}\Big) \simeq 0,3739558136 \cdots$$

Le choix de la base 10 ne semble pas intervenir dans le résultat, on conjecture que le résultat doit être vrai pour tout choix d'entier a en lieu et place de 10.

Remarque : essayez de faire des simulations numériques de ces densités.

2.2. Familles. — Nous avons vu que l'ensemble $\mathcal{P}$ des nombres premiers est infini mais il n'est pas si simple d'en exhiber, d'où ce paragraphe.

2.6 — Nombres de Fermat : comme -1 est racine du polynôme $X^{2n+1}+1$ celui-ci est divisible par $X+1$ (le quotient étant égal à $X^{2n} - X^{2n-1} + \cdots + 1$)). Soit alors $m = 2^n k$ avec k impair ; si $k > 1$, l'égalité

$$2^m + 1 = (2^{2^n})^k + 1 = (2^{2^n} + 1)((2^{2^n})^{k-1} - \cdots + 1)$$

montre que $2^{2^n} + 1$ est un diviseur propre de sorte que $2^m + 1$ n'est pas premier. Ainsi si l'on veut trouver des nombres premiers parmi la famille des $2^m + 1$, il faut prendre m de la forme 2^n. On pose alors pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$; F_n est le n-ème nombre de Fermat. On calcule $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ et l'on vérifie aisément qu'ils sont tous premiers.

Soit p premier divisant F_5, on a alors $2^{2^5} \equiv -1 \mod p$ de sorte que $\bar{2} \in \mathbb{Z}/p\mathbb{Z}$ est d'ordre 2^6 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. D'après le petit théorème de Fermat, on a $2^{p-1} = 1$ et donc 2^6 divise $p-1$, de

sorte qu'un diviseur premier de F_5 est forcément de la forme $64k+1$. Vérifions que le cas $k = 10$ est un bon candidat : déjà 641 est premier et on l'écrit sous la forme $641 = 1+5.2^7 = 5^4+2^4$. Dans le corps $\mathbb{Z}/641\mathbb{Z}$, on a $0 = 641 = 1+5.2^7$ soit $2^7 = -1/5$. Ainsi $F_5 = 2^32+1 = (2^7)^4.2^4+1$ car $32 = 7.4+4$. D'où dans $\mathbb{Z}/641\mathbb{Z}$, on a $F_5 = (-1/5)^4.2^4+1 = (2^4+5^4)/5^4 = 0$.
Remarque : à ce jour, malgré l'aide de l'ordinateur, on ne connaît pas d'entiers $n \geq 5$ tels que F_n est premier. Remarquons cependant que pour $n = m+r$ avec $r > 0$, F_n et F_m sont premiers entre eux ; en effet on a $2^{2^n} = (2^{2^m})^{2^r}$ et dans $\mathbb{Z}/F_m\mathbb{Z}$, on a alors $F_n \equiv (-1)^{2^r}+1 \mod F_m$. Ainsi le pgcd de F_m et de F_n divise 2 ; or 2 ne divise pas F_n d'où le résultat. L'ensemble $\mathcal{P}$ des nombres premiers positifs contient la réunion disjointe $\coprod_n \mathcal{F}_n$ où $\mathcal{F}_n$ est le sous-ensemble de $\mathcal{P}$ des diviseurs premiers divisant F_n ; $\mathcal{F}_n$ étant non vide pour tout n car $F_n > 1$, on en déduit alors une nouvelle preuve de l'infinité de $\mathcal{P}$.

2.7 — Nombres de Mersenne : de la factorisation $X^{pq}-1 = (X^p-1)(X^{p(q-1)}+\cdots+X^p+1)$, on en déduit que si 2^n-1 est premier alors n est un nombre premier. Ainsi pour p premier les nombres $M_p = 2^p-1$ sont dits de Mersenne $M_p = 2^p-1$; les premiers exemples sont $3 = 2^2-1$, $7 = 2^3-1$, $31 = 2^5-1$, $127 = 2^7-1$ qui sont premiers alors que $2047 = 2^{11}-1 = 23\times 89$ ne l'est pas. Comme précédemment si q est un diviseur de M_p alors l'ordre de la classe de 2 dans $\mathbb{Z}/q\mathbb{Z}$ est égale à p qui doit diviser $q-1$ et donc $q \equiv 1 \mod p$ (on a aussi $q \equiv 1 \mod 2p$). On en déduit aussi que 2 est un carré modulo q et donc $q \equiv \pm 1 \mod 8$.
Remarque : à ce jour on connaît 45 nombres de Mersenne qui sont premiers ; le dernier trouvé cet été possède plus de 10 millions de chiffres.

2.8 — Quelques formules : notons tout d'abord qu'il ne peut pas exister de polynômes de $\mathbb{Z}[X]$ non constant ne prenant sur $\mathbb{N}$ que des valeurs premières : en effet soit $P(X) = a_nX^n+\cdots+a_0$ de sorte qu'en particulier $a_0 \in \mathcal{P}$. Comme $P(n)$ tends vers l'infini quand n tends vers l'infini, il existe une valeur n_0 à partir de laquelle $P(n) > a_0$. Ainsi pour k assez grand, on a $P(ka_0) > a_0$ alors que $P(ka_0)$ est divisible par a_0.
Remarque : pour des polynômes du second degré donnant pour les premières valeurs de n des nombres premiers, citons les résultats suivant :

- spirales d'Ulam : il s'agit des premiers p pour lesquels n^2+n+p est premier pour $n = 0, \cdots, n-2$: on remarquera en effet que p divise $(p-1)^2+(p-1)+p$, cf. aussi l'exercice 1.2. Heegner a montré que les seuls p qui conviennent sont $2, 3, 5, 16$ et 41. On conjecture que pour tout A, il existe B tel que n^2+n+B soit premier pour tout $n = 0, \cdots, A$. Pour $A = 41$, B est nécessairement plus grand que 10^{18} et n'est pas connu.
- R. Ruby : $103n^2-3945n+32381$ est premier pour $n = 0, 1, \cdots, 42$;
- G. Fung : $47n^2-1701n+10181$ est premier pour $n = 0, 1, \cdots, 42$;
- R. Ruby : $36n^2-810n+2753$ est premier pour $n = 0, 1, \cdots, 44$.

En utilisant le théorème de Wilson, on montre facilement que la fonction

$$f(n) = 2+2(n!) \mod n+1$$

produit tous les nombres premiers exclusivement mais plusieurs fois. En 1947 W. Mills établit l'existence d'une constante A telle que pour tout $n > 1$,

$$\lfloor A^{3n} \rfloor \in \mathcal{P}, \qquad A \simeq 1,306377883863...$$

cependant le calcul de cette constante nécessite la connaissance de $\mathcal{P}$ ce qui convenons le n'est pas très honnête. L'escroquerie est du même genre que la suivante : posons

$$L = 0,2,003000050000007000000011...$$

le n-ème nombre premier étant placé en position n^2. On vérifie alors aisément que

$$\lfloor L \times 10^{n^2} \rfloor - \lfloor L \times 10^{(n-1)^2} \rfloor 10^{2n-1}$$

est égal au n-ème nombre premier p_n.

On s'interdit désormais d'utiliser des nombres pouvant cacher une infinité d'informations. Le premier exemple du à Roland Yéléhada repose sur la formule suivante

$$t(n) = 2 + n \lfloor \frac{1}{1 + \sum_{p=2}^{m+1} \lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor \rfloor} \rfloor$$

laquelle tous les nombre premiers. Le principe est très élémentaire : si $n+2$ est un multiple de p alors $(n+2)/p$ est un entier q et donc $(n+1)/p = q - 1/p$ et donc $\lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor$ est égal à 1 alors qu'il est nul si p n'est pas un diviseur. Autrement dit la somme compte le nombre de diviseurs de $n+2$ compris entre 2 et $n+1$; ainsi si $n+2$ est premier on obtient $t(n) = n+2$ qui est premier alors que si $n+2$ n'est pas premier on a $t(n) = 2$. Ainsi la formule ne donne que des nombres premiers mais très lentement, 2 apparaissant très souvent. En utilisant la formule de Wilson, Minac simplifie la formule précédente :

$$t(n) = 2 + n \lfloor \frac{(n+1)! + 1}{n+2} - \rfloor \frac{(n+1)!}{n+2} \rfloor \rfloor$$

laquelle contient moins de symbole et plus de somme, mais requiert de lourds calculs de factoriels.

En 1995 Minac et Willans ont imaginé une formule, avec plus de 52 symboles, donnant tous les nombres premiers dans l'ordre et sans répétition :

$$\pi(m) = \sum_{j=2}^{m} \frac{\sin^2\left(\frac{\pi}{j}(j-1)!^2\right)}{\sin^2(\frac{\pi}{j})} = \sum_{j=2}^{m} \lfloor \frac{(j-1)! + 1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor$$

alors le n-ème nombre premier p_n est donné par

$$p_n = 1 + \sum_{m=1}^{2^n} \lfloor \lfloor \frac{n}{1 + \pi(m)} \rfloor^{1/n} \rfloor.$$

En 2000, Ruiz a donné la formule suivante :

$$p_n = 1 + \sum_{k=1}^{2(\lfloor n \ln n \rfloor + 1)} \left(1 - \lfloor \frac{\psi(k)}{n} \rfloor\right)$$

où $\psi(k) = k - 1 + \sum_{j=2}^{k} \lfloor \frac{2}{j} \left(1 + \sum_{s=1}^{\lfloor \sqrt{j} \rfloor} \left(\lfloor \frac{j-1}{s} \rfloor - \lfloor \frac{j}{s} \rfloor\right)\right) \rfloor$.

Remarque : signalons aussi la suite de Perrin définie par

$$u_0 = 3,\ u_1 = 0,\ u_2 = 2 \qquad u_{n+1} = u_{n-1} + u_{n-2}.$$

Lucas a montré que pour p premier p divise u_p et on conjecture que la réciproque est vraie.

2.3. Test de primalité. — La technique enseignée au lycée est le crible d'Eratosthène qui bien qu'efficace pour des nombres inférieurs à 10^{11} s'avère ensuite trop lente.

2.9 — Critères de primalité particuliers : c'est à dire adaptés à certaines familles d'entiers :

- *Critère de Pépin* : $p = F_n$ est premier si et seulement si $3^{(p-1)/2} \equiv -1 \mod p$.
- *Critère de Lucas-Lehmer* : pour $q \geq 3$, M_q est premier si et seulement si $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$.

– *Test de primalité de Lucas-Lehmer* : soit $(L_i)_{i\geq 0}$ la suite de Lucas-Lehmer définie par $L_0 = 4$ et $L_{i+1} = L_i^2 - 2 \mod M_q$, alors M_q est premier si et seulement si $L_{q-2} \equiv 0 \mod M_q$.

2.10 — Fermat-Euler and co : un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \mod n$. Par exemple $n = 105 = 3.5.7$ est pseudo-premier de base 13 : en effet on a $13^{104} = (13^2)^{52} \equiv 1 \mod 3$, $13^{104} = (13^4)^{26} \equiv 1 \mod 5$ et $13^{104} = (13^6)^{17} \times 13^2 \equiv 1 \mod 7$, de sorte que d'après le lemme chinois on a $13^{104} \equiv 1 \mod 105$. En revanche on a $2^{104} = (2^6)^{17} \times 2^2 \equiv 4 \mod 7$ de sorte que 105 n'est pas pseudo-premier de base 2. Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p.

Ce test serait « bon » dans le sens où calculer a^{N-1} requiert, en utilisant l'exponentiation rapide, $O(\log N)$ multiplications ; cependant il est « mauvais » à cause des nombres de Carmichael qui vérifient le test sans être premier : le plus petit de ces nombres est $561 = 3.11.17$ et on sait que l'ensemble de ces nombres est infini. Une amélioration de ce test est donné par le test de *Solovay-Strassen* qui consiste à vérifier les congruences $a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \mod N$ dont la véracité est assurée par la proposition suivante.

Proposition 2.11. — *Soit* $H = \{a \in (\mathbb{Z}/N\mathbb{Z})^\times : a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \mod N\}$ *; alors* $H = (\mathbb{Z}/N\mathbb{Z})^\times$ *si et seulement si* N *est premier.*

Preuve : On a déjà vu que si N est premier alors $H = (\mathbb{Z}/N\mathbb{Z})^\times$. Réciproquement si p^2 divise N, il existe alors un élément $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ d'ordre $p(p-1)$ et comme p ne divise pas $N-1$, $a^{N-1} \not\equiv 1 \mod N$. Si $N = pp_2 \cdots p_r$ sans facteurs carrés ; par le lemme chinois soit $a \equiv 1 \mod p_2 \cdots p_r$ et a non carré modulo p de sorte que $(\frac{a}{N}) = -1$ mais $a^{(N-1)/2} \equiv 1 \mod p_2 \cdots p_r$ et donc $a^{(N-1)/2} \not\equiv 1 \mod N$. □

Applications :

– *Test probabiliste* : si N est composé alors comme $[(\mathbb{Z}/N\mathbb{Z})^\times : H] \geq 2$, en prenant a aléatoirement on a au moins une chance sur deux d'avoir $a \notin H$ de sorte que si N passe successsivement k tests, on peut dire qu'il est premier avec une probabilité $\geq 1 - 2^{-k}$.

– *Test déterministe sous GRH* : l'hypothèse de Riemann généralisée implique que si N est composé, il existe $a \leq 2(\log N)^2$ qui ne passera pas le test de Solovay-Strassen

– *Test probabiliste de Rabin-Miller* : un entier $n = 1+2^k q$ impair, q impair, est dit fortement pseudo-premier de base b si l'une des conditions suivantes est vérifiée :

$$b^q \equiv 1 \mod n \qquad \exists 0 \leq j < k,\ b^{2^j q} \equiv -1 \mod n$$

Si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leq b < n$: en effet $b^{2^k q} \equiv 1 \mod n$ et soit donc $0 \leq i \leq k$ le plus petit entier tel que $b^{2^i q} \equiv 1 \mod n$. Si $i = 0$, on a $b^q \equiv 1 \mod n$ et si $i > 0$ alors $b^{2^{i-1} q} \equiv -1 \mod n$ car dans un corps $x^2 = 1$ entraine $x = \pm 1$.

Remarque : si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b : en effet il existe $0 \leq i \leq k$ tel que $b^{2^i q} \equiv 1 \mod n$; or $2^i q$ divise $n-1$ de sorte que $b^{n-1} \equiv 1 \mod n$.

Exemple : $n = 561$ est pseudo-premier de base 13 mais il n'est pas fortement pseudo-premier de base 2 : en effet $n-1 = 2^4 35$ et $2^{352^3} \equiv 1 \mod 561$ mais $2^{352^2} \equiv 67 \mod 561$.

Théorème 2.12. — *(Rabin) Pour* n *impair soit*

$$B_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ /\ n \text{ est fortement pseudo-premier de base } x\}.$$

Alors si n est non premier alors $\frac{|B_n|}{\phi(n)} \leq 1/4$ sauf pour $n = 9$.

Remarque : autrement dit si $|B_n| \geq \phi(n)/4$ alors n est premier. Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier. Par exemple pour $n = 561$, on obtient $|B_{561}| = 10$ de sorte qu'outre ± 1, il ne reste plus que 8 entiers qui font croire que 561 est premier et le rapport $\frac{|B_{561}|}{\varphi(561)} = 1/32$ est relativement faible. Ce critère est particulièrement adapté à la méthode RSA.

En juillet 2002, Agrawal-Kayal-Saxena ont donné un test de primalité en temps polynomial. Cependant pour les applications pratiques telles que RSA, le test probabiliste de Rabin-Miller est suffisant.

2.4. Factorisation. — La factorisation naive via le crible d'Erathostene est rapidement inefficace car trop longue à mettre en oeuvre : sa complexité est $O(\sqrt{N})$. Nous allons dans ce paragraphe présenter quelques autres algorithmes plus rapides, même si on le rappelle, jusqu'à présent, le problème de la factorisation n'a pas trouvé d'algorithme en temps polynomial. En pratique en 2006 on sait factoriser en quelques heures un nombre entiers de 100 chiffres, en quelques mois avec plusieurs ordinateurs un nombre de 150 chiffres et l'on ne sait toujours pas factoriser en 100 ans, un nombre RSA de 300 chiffres. Dans la suite pour évaluer la complexité des algorithmes considérés, on introduit la notation suivante

$$L(b, N) = \exp\Big(C(\log N)^b(\log\log N)^{1-b}\Big)$$

où C est une constante ; le cas $b = 0$ correspond aux algorithmes polynomiaux, le cas $b = 1$ aux algorithmes exponentiels et le cas $0 < b < 1$ aux algorithmes sous-exponentiels.

2.13 — L'algorithme de Fermat : bien que l'algorithme que nous allons présenter n'est pas implémenté de nos jours, sauf si le nombre n à factoriser possède deux facteurs relativement proche de $\sqrt{n}$, son principe est au coeur de la plupart des algorithmes modernes. L'idée est la suivante : si n peut s'écrire comme la différence de deux carrés, $n = x^2 - y^2$ alors $n = (x - y)(x + y)$ est une factorisation non triviale de n.
Remarque : tout nombre n impair non premier peut s'écrire sous la forme $x^2 - y^2$: en effet si $n = ab$ alors on peut prendre $x = (a + b)/2$ et $y = (a - b)/2$.

L'algorithme est alors le suivant : on prend $x = \lceil\sqrt{n}\rceil$ et en partant de $y = 0$ et en incrémentant de 1 à chaque fois que $x^2 - y^2 > n$, on teste si $n = x^2 - y^2$. Si un des tests est positif, c'est gagné sinon on incrémente x de 1 et on recommence. Il est possible d'améliorer cet algorithme en implémentant un test probabiliste pour savoir si $x^2 - n$ est un carré, malgré tout cet algorithme est encore trop lent.

2.14 — L'amélioration de Kraitchik : le principe est que n n'est pas premier si et seulement si l'équation $x^2 \equiv 1 \mod n$ a au moins 4 solutions. Ainsi si on disposait d'un bon algorithme $\mathcal{A}$ « racine carrée », on factoriserait N comme suit : on prend a au hasard, puis on calcule a^2 dont on prend la racine carrée par l'algorithme $\mathcal{A}$: il y a alors au moins une chance sur deux pour que le résultat b soit différent de a de sorte que $n \wedge (a \pm b)$ fournit un diviseur non trivial de n. Evidemment on ne dispose pas de tel algorithme et il est raisonnable de penser qu'il n'en existe pas.

L'idée est alors de considérer des paires « aléatoires » d'entiers (x, y) telles que $x^2 \equiv y^2 \mod n$ de sorte que n divise $(x - y)(x + y)$ de sorte que « moralement » il y a une chance sur

2 pour que les facteurs premiers de n se répartissent sur les deux facteurs $(x-y)$ et $(x+y)$. Ainsi le pgcd $(x-y)\wedge(x+y)$ a de bonnes chances de donner un diviseur non trivial de n.

Peu après, en 1931, D. H. Lehmer et R. E. Powers ont montré comment construire de telles paires systématiquement en utilisant les fractions continues. L'idée est la suivante : si t est petit avec $x^2 \equiv t \mod n$, alors $x = t + kd^2n$ et donc $(x/d)^2 - kn = t/d^2$ est petit, autrement dit x/d est une bonne approximation de $\sqrt{kn}$. Or on sait que les fractions continues sont de bonnes approximations rationnelles : ainsi on calcule via les fractions continues de bonnes approximations P/Q de $\sqrt{kn}$ pour divers k et on essaie de factoriser $t = P^2 - Q^2kn$ via la base de petits nombres premiers que l'on considère.

Remarque : avec l'arrivée d'ordinateurs puissants, des algorithmes particulièrement performants ont alors été utilisés dès les années 70. Récemment avec l'arrivée de la mémoire à bon marché, des algorithmes plus rapides sont utilisés comme celui du crible quadratique que nous présentons plus loin.

2.15 — L'algorithme de Dixon : on choisit a proche de $\sqrt{N}$ au hasard et on réduit a^2 modulo N en prenant le représentation dans $[-N/2, N/2]$ et on regarde si on peut le factoriser avec des petits facteurs premiers. Une fois que l'on a obtenu quelques a_i, b_j on essaie de construire une égalité du type

$$a^2 = \prod_i a_i^2 \equiv \prod_j b_j = b^2 \mod N$$

En remarquant que si N n'est pas premier, il y a dans $(\mathbb{Z}/N\mathbb{Z})^\times$ au moins 4 racines carrés de 1, on en déduit qu'il y a au moins une chance sur deux pour que $\pm b$ soit distinct de a. On a alors une chance sur deux en étudiant $(a-b\wedge N)$ et $(a+b\wedge N)$ d'obtenir une factorisation non triviale de N. Cet algorithme a en fait une complexité $L(1/2, N) = \exp(C(\log N)^{1/2}(\log\log N)^{1/2})$ ce qui est déjà remarquable même si insuffisant pour factoriser de très grands nombres.

Dans la pratique par petits diviseurs de a on entend plus petit que 10^4. On répète le processus de sorte à trouver un nombre de telles factorisation plus grand que le nombre de premier plus petit que 10^4, i.e. ici 1229. On représente alors une telle factorisation $p_1^{r_1}\cdots p_{1229}^{r_{1229}}$ par le vecteur $v(a) = (r_1, \cdots, r_{1229})$. Si toutes les coordonnées de $v(a)$ sont paires alors $a^2 - n$ est un carré ce qui donne une factorisation de n. Dans le cas contraire comme on a plus de vecteurs que de coordonnées, on en déduit qu'il existe une somme de $v(a)$ dont toutes les coordonnées sont paires : pour obtenir cette somme, on pose $w(a) = (s_1, \cdots, s_{1229})$ avec $s_i = 0$ si r_i est paire et $s_i = 1$ sinon. L'algorithme de Gauss sur les vecteurs $w(a)$ de $(\mathbb{Z}/2\mathbb{Z})^{1229}$, très rapide dans cette situation, fournit alors la somme à considérer.

2.16 — L'amélioration de Pomerance (1981) : le crible quadratique. Au lieu de prendre les a au hasard dans l'algorithme de Dixon, on prend $k = \lfloor\sqrt{n}\rfloor$ et on considère pour $a = k+1, k+2, \cdots \leq \sqrt{2n}$, les entiers $Q(a) = a^2 - N$. Supposons que l'on ait déjà testé que les premiers p inférieurs à 10^4 ne divisent pas n de sorte que si p divise $a^2 - n$ alors $\left(\frac{n}{p}\right) = 1$. Ainsi il ne faut tester la divisibilité de $a^2 - n$ que la moitié des premiers $p \leq 10^4$, ceux pour lesquels n est un résidu quadratique modulo p : cet ensemble de premiers est appelé *la base de facteurs*. Pour un tel premier on a $n \equiv (\pm t)^2$ et donc $a \equiv \pm t \mod p$: réciproquement si $a \equiv \pm t$ alors p divise $a^2 - n$.

Le procédé est alors le suivant : on prend dans l'ordre croissant les premiers de la base de facteur, étant donné un tel p soit $a_+(p) \geq \sqrt{n}$ le plus petit entier congru à t modulo p. On sait alors que p divise $Q(a_+(p)) = a_+(p)^2 - n$, ainsi que tous les $Q(a_+(p) + pk)$. On considère alors une table $b(a)$ indexée par les k en l'initialisant à $\ln Q(a)$; pour un tel p on soustrait

alors à chacun des entrées indexées par $a_+(p)+kp$ la valeur $\ln p$. On recommence ce procédé pour les $a_-(p) \equiv -t \mod p$ puis on passe au p suivant. Les calculs sur les ln sont arrondi à la partie entière et quand les $b(a)$ sont proches de zéro alors a^2-n se factorise avec des petits premiers.
Remarque : dans le procédé ci-dessus, il faut aussi tenir compte du fait que p peut diviser a^2-n plus d'une fois, de sorte que l'on est amené à résoudre des congruences $x^2 \equiv n \mod p^r$ avec $1 \leq r \leq 2\ln L/\ln p$ où L est le plus grand premier dans la base de facteurs. Dans la pratique, on peut ignorer ces puissances.
Remarque : plus la majoration demandée sur les petits premiers sera grande plus la probabilité que a^2-n soit factorisable dans la base de facteurs associée sera grande, par contre la résolution du système linéaire associé par la méthode de Gauss sera plus longue.
Remarque : le but étant de trouver des a tels que a^2-n ait des petits facteurs, on peut s'intéresser au cas de 2. Les entiers à factoriser sont bien évidemment impairs ; si $n \equiv 3,7 \mod 8$ alors $a^2-n \equiv 2 \mod 4$ pour tout $a \equiv 1 \mod 2$, si $n \equiv 5 \mod 8$ alors $a^2-n \equiv 4 \mod 8$ et si $n \equiv 1 \mod 8$ alors $a^2-n \equiv 0 \mod 8$. Afin de se retrouver dans la situation favorable où $n \equiv 1 \mod 8$, on multiplie n par $3,5,7$ de façon à s'y ramener : l'algorithme précédent est tout aussi rapide à trouver de grands facteurs pour n que pour $3n$.
Remarque : pour p premier dans la base de facteurs, i.e. p petit et n est un résidu quadratique modulo p, il faut savoir résoudre l'équation $x^2 \equiv n \mod p$.

2.17 — Algorithme ρ de Pollard : cet algorithme construit en 1975 est le plus efficace pour trouver des petits facteurs par exemple d'ordre 10^7. En pratique, on commence par l'utiliser systématiquement pour tester s'il y a des diviseurs d'ordre 10^5 et dans la négative, on passe à des algorithmes plus efficaces comme le crible quadratique.

On choisit a_0 entre 1 et N et on considère la suite $a_{i+1} = f(a_i)$ avec $f(a) = a^2+1 \mod N$. On suppose que la suite des a_i modulo p est suffisamment aléatoire, ce qui est assez bien vérifié par l'expérience et la pratique. Ainsi la probabilité pour que r nombres pris au hasard modulo p soient tous distincts est

$$P_r = (1-\frac{1}{p})(1-\frac{2}{p})\cdots(1-\frac{r-1}{p}) \leq \exp(-\frac{r(r-1)}{2p})$$

Prenons r de l'ordre de $\sqrt{p}$ et disons $r > 2\sqrt{p}$ de sorte que $P_r \leq \exp(-r(r-1)/(2p)) \leq \exp(-2+1/\sqrt{p}) < 1/2$. On a ainsi une bonne chance qu'il existe $1 < i < j < r$ tels que $a_i \equiv a_j \mod p$ ce qui implique $a_{i+m} \equiv a_{j+m} \mod p$ pour tout $m \geq 0$. Ainsi pour $m = j-2i$ et $k = j-i$ on aura $a_k \equiv a_{2k} \mod p$. En résumé on a au moins une chance sur deux qu'il existe k d'ordre $O(\sqrt{p})$ tel que $(a_{2k}-a_k) \wedge n$ soit distinct de 1, ce qui fournit un algorithme qui avec une bonne probabilité donne une factorisation de N en temps $O(\sqrt[4]{N})$.

2.18 — Algorithme $p-1$ de Pollard : supposons que n possède un facteur premier p tel que les facteurs premiers de $p-1$ soient petits, i.e. plus petit que 10^4. Supposons en fait que $p-1$ divise 10000!. Comme l'exponentiation modulo n est très rapide, on calcule $m = 2^{10000!} \mod n$. Comme $p-1$ divise 10000!, $m \equiv 1 \mod p$ et donc p divise $m-1$ et comme par ailleurs il y a de bonnes chances que n ne divise pas 10000!, $g = (m-1) \wedge n$ devrait être un facteur non trivial de n. Dans la pratique on teste $(2^{k!}-1) \wedge n$, s'il est égal à 1 on passe à $k+1$ et s'il est égal à n alors on peut essayer de remplacer 2 par une autre valeur c, ou alors essayer un autre algorithme.

2.19 — Méthode de factorisation de Lenstra : soit Y un entier ; on dit qu'un nombre est *Y-friable* (resp. *Y-puissance friable*) si tous ses diviseurs premiers sont inférieurs à Y (resp.

si toute puissance d'un premier le divisant est inférieure à Y). Soit N le nombre à factoriser et p un diviseur de N ; si $p-1$ est Y-puissance friable pour Y de taille raisonnable, alors $p-1$ divise $m(Y) = ppcm(2, 3, \cdots, Y)$. Si donc $a \wedge N = 1$, alors $a^{m(Y)} \equiv 1 \mod p$ et donc

$$(a^{m(Y)} - 1) \wedge N \neq 1.$$

La méthode sera donc efficace si N possède un facteur premier Y-puissance friable pour Y pas trop grand : le problème est que les grands nombres premiers tels que $p-1$ soit Y-friable sont assez rares. L'idée clef de l'algorithme de Lenstra est que l'on est en train de raisonner dans $(\mathbb{Z}/p\mathbb{Z})^\times$ qui est cyclique de cardinal $p-1$ (cf. ci dessus l'algorithme $p-1$ de Pollard). Ainsi plus généralement soient n un entier à factoriser et G un groupe tel que :

- l'ensemble sous-jacent à G est un sous-ensemble de $(\mathbb{Z}/n\mathbb{Z})^r$ pour un certain entier r ;
- la loi de G est définie en termes d'opérations arithmétiques modulo n.

Pour $d|n$, on note $G|d$ le groupe obtenu à partir de G en réduisant les coordonnées modulo d.

Proposition 2.20. — *Soient n et G comme ci-dessus.*
(1) Test de primalité : s'il existe un $x \in G$ et un entier m satisfaisant les conditions suivantes, alors n est premier :

- *m est plus grand que l'ordre de $G|q$ pour tout éventuel diviseur q de n inférieur à $\sqrt{n}$;*
- *$x^m = e$ l'élément identité de G ;*
- *pour tout premier p divisant m, une coordonnée de $x^{m/p} - e$ est première à n.*

(2) Factorisation : soit p premier divisant n, si l'ordre de $G|p$ divise $k!$ et si n ne divise pas la i-ème coordonnées de $x^{k!} - e$ alors le pgcd de celle-ci avec n fournit un diviseur non trivial de n.

Preuve : (1) Si n n'est pas premier soit alors q un diviseur plus petit que $\sqrt{n}$. Soit alors x et m vérifiant les deux dernières propriétés de l'énoncé. On en déduit alors que l'image de x dans $G|q$ est égale à m ce qui contredit la première hypothèse.

(2) Le résultat découle du fait que p divise toutes les coordonnées de $x^{k!} - e$. □

Remarque : l'algorithme $p-1$ de Pollard correspond à l'application de cette proposition pour le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi pour trouver un diviseur q de n, il faut que $q-1$ divise $k!$ pour un entier $k \ll$ petit $\gg$. Pour appliquer pleinement la proposition précédente, il faut disposer de nombreux exemples de groupes G comme ci-dessus. Les courbes elliptiques $E(a,b) : \{[x,y,z] \in \mathbb{P}^2(\mathbb{C}) : zy^2 = x^3 + axz^2 + bz^3\}$ que l'on regarde modulo n fournissent de tels exemples. Citons sans démonstration les résultats suivants.

Théorème 2.21. —

- *(Hasse) L'ordre de $E(a,b)|p$ appartient à l'intervalle $I(p) =]p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}[$.*
- *(Waterhouse) Étant donné un premier $p \geq 3$ et $n \in I(p)$, il existe a et b tels que le cardinal de $E(a,b)|p = n$.*
- *(conjecture de Sato-Tate prouvée en 2006 par M. Harris et R. Taylor) On écrit*

$$-\frac{1}{2\sqrt{p}}(|E(a,b)|p - p - 1) = \cos(\theta_{a,b}),$$

alors la mesure de probabilité de θ est $\frac{2}{\pi}\sin\theta^2 d\theta$.

Ainsi pour factoriser n, il suffit de trouver un entier un entier dans un intervalle $I(p)$ qui divise $k!$ ce qui est bien plus souple que la méthode $p-1$ de Pollard. Cependant il n'est pas simple de calculer l'ordre de $E(a,b)|p$, ni étant donné $n \in I(p)$ de trouver a et b tels

que $E(a,b)|p$ soit de cardinal n. Le procédé consiste alors, d'après Sato-Tate, à prendre des courbes elliptiques « au hasard ».
Remarque : on peut montrer que la complexité de cet algorithme est $\exp\sqrt{2\log p\log\log p}$ où p est le plus petit facteur premier divisant N. Par ailleurs cet algorithme est peu gourmand en mémoire puisque l'on doit stocker un nombre de données polynomial en $\log N$.
Remarque : il existe un autre algorithme moins élémentaire appelé *le crible algébrique* dont la complexité est de l'ordre de $L(1/3)$ qui est donc plus efficace que celui de Lenstra pour les N ne possédant pas de facteurs premiers de taille moyenne, ce qui est typiquement le cas pour RSA. Enfin en 1997, Shor a montré que le problème de la factorisation pouvait être résolu en temps polynomial à l'aide d'un ordinateur quantique dont un premier exemplaire vient juste d'être construit.

2.5. Répartition des nombres premiers. — Commençons par une citation du grand Euler : « Les mathématiciens ont tâché jusqu'ici en vain de découvrir quelque ordre dans la progression des nombres premiers, et l'on a lieu de croire que c'est un mystère auquel l'esprit humain ne saura jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers que quelques-uns se sont donné la peine de continuer au-delà de cent mille et l'on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle. »Ne nous décourageons pas pour autant et essayons de voir ce que l'on peut actuellement dire sur le sujet.

2.22 — Théorème de Dirichlet : nous avons déjà vu que l'ensemble $\mathcal{P}$ des nombres premiers était infini. Dirichlet améliore ce résultat, en affirmant que pour tout $a \wedge b = 1$, il existe une infinité de nombres premiers $p \equiv a \mod b$. Le cas $a = 1$ est relativement simple à prouver et ne nécessite pas l'utilisation d'argument d'analyse contrairement au cas général, pour l'instant. En utilisant la loi de réciprocité quadratique, on peut montrer quelques cas simples.

Proposition 2.23. — *Il existe une infinité de nombres premiers p tels que*
(a) $p \equiv 3 \mod 4$ *;* *(b)* $p \equiv 1 \mod 4$ *;*
(c) $p \equiv 1 \mod 2^m$ *;* *(d)* $p \equiv 5 \mod 6$ *;*
(e) $p \equiv 5 \mod 8$ *;* *(f)* $p \equiv 1 \mod 6$ *;*
(g) $p \equiv -1 \mod 12$ *;* *(h)* $p \equiv -1 \mod 10$.

Preuve : Le schéma de démonstration sera toujours le même : on raisonne par l'absurde en supposant la finitude de l'ensemble considéré et on construit un entier N qui permet d'aboutir à une contradiction. On note n le plus grand élément de l'ensemble supposé fini. Toute la difficulté revient donc à construire N en fonction de n et de l'ensemble considéré :

(a) $N = n! - 1$; si p divise N alors $p > n$ et donc $p \equiv 1 \mod 4$ de sorte que $N \equiv 1 \mod 4$ ce qui n'est pas.

(b) $N = (n!)^2 + 1$; si p premier divise N alors -1 est un carré modulo p soit $p \equiv 1 \mod 4$ et donc par hypothèse $p \leq n$ soit p divise $n!$ et donc $p|N - (n!)^2 = 1$ d'où la contradiction .

(c) si p divise $a^{2^{m-1}} + b^{2^{m-1}}$ avec p premier avec a, alors $\frac{a}{b}$ est d'ordre divisant 2^m et d'ordre distinct de 2^{m-1} ; il est donc d'ordre 2^m. Or l'ordre de tout élément divise le cardinal du groupe soit $p \equiv 1 \mod 2^m$. Soit alors $N = (n!)^{2^{m-1}} + 1$; tout diviseur p premier de N est congru à $1 \mod 2^n$ et supérieur à n d'où la contradiction.

(d) $p \equiv 5 \mod 6$ est équivalent à $p \equiv 1 \mod 2$ et $p \equiv 2 \mod 3$ soit $p > 2$ et $p \equiv 2 \mod 3$. Soit $N = n! - 1$; pour p premier divisant N, on a $p > n$ et donc $p \equiv 1 \mod 3$ de sorte que $N \equiv 1 \mod 3$ ce qui n'est pas.

(e) $N = 3^2 5^2 7^2 11^2 \cdots n^2 + 2^2$; N est visiblement impair. Soit alors p premier divisant N, p ne divise pas 4, de sorte que $p \equiv 1 \mod 4$, soit $p \equiv 1, 5 \mod 8$. À nouveau $p \equiv 5 \mod 8$ est exclu car sinon p diviserait $4 = N - 3^2 \cdots n^2$. On en déduit donc $N \equiv 1 \mod 8$. Or si p est premier impair on a $p \equiv 1, 3, 5, 7 \mod 8$ et on vérifie aisément que p^2 est alors congru à 1 modulo 8 et donc $N \equiv 5 \mod 8$, d'où la contradiction.

(f) $p \equiv 1 \mod 6$ est équivalent à $p > 2$ et $p \equiv 1 \mod 3$. Or si p divise $a^2 + 3b^2$ et p premier avec b, alors -3 est un carré modulo p et donc $(\frac{-3}{p}) = 1 = (-1)^{(p-1)(3-1)/4}(\frac{p}{3})(\frac{-1}{p}) = (\frac{p}{3})$ et donc -3 est un carré modulo p si et seulement si $p \equiv 1 \mod 3$. Soit alors $N = 3(n!)^2 + 1$; tout diviseur premier de N est alors congru à 1 modulo 3 et supérieur à n d'où la contradiction.

(g) si p divise $a^2 - 3b^2$ et p premier avec b alors 3 est un carré modulo p. Or on a $(\frac{3}{p}) = (\frac{p}{3})(-1)^{(p-1)/2}$ et donc 3 est un carré modulo p dans les deux situations suivantes :

- $(\frac{p}{3}) = (-1)^{(p-1)/2} = 1$ soit $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$ soit $p \equiv 1 \mod 12$;
- $(\frac{p}{3}) = (-1)^{(p-1)/2} = -1$ soit $p \equiv -1 \mod 3$ et $p \equiv -1 \mod 4$ soit $p \equiv -1 \mod 12$;

Soit alors $N = 3(n!)^2 - 1$; tout diviseur premier p de N est alors congru à ± 1 modulo 12 et supérieur à n de sorte que par hypothèse, $p \equiv 1 \mod 12$. On en déduit alors que $N \equiv 1 \mod 12$ ce qui n'est pas car $N \equiv -1 \mod 12$.

(h) pour p premier $p \equiv -1 \mod 10$ si et seulement si $p \equiv -1 \mod 5$. Or si p divise $a^2 - 5b^2$ avec p premier avec b alors $(\frac{5}{p}) = 1 = (\frac{p}{5})$ et donc $p \equiv \pm 1 \mod 5$. Soit alors $N = 5(n!)^2 - 1$; tout diviseur premier p de N est strictement supérieur à n et congru à $\pm 1 \mod 5$. Par hypothèse il est donc congru à 1 modulo 5 et donc N aussi ce qui n'est pas. □

Remarque : en 2005 Benjamin Green et Terence Tao généralise encore le théorème de Dirichlet en prouvant que pour tout entier k, il existe une infinité de suites de k nombres premiers en progression arithmétique, i.e. il existe a et b tels que

$$a,\ a+b,\ a+2b,\ \cdots, a+(k-1)b \in \mathcal{P}$$

Par exemple pour $k = 10$ le plus petit a est 199 avec $b = 210$ ce qui donne

$$199,\ 409,\ 619,\ 1039,\ 1249,\ 1459,\ 1669,\ 1879,\ 2089.$$

Étant donné k on peut noter a_k et b_k les plus petits entiers tels que $a_k + ib_k$ soient premiers pour tout $i = 0, \cdots, k-1$; Green et Tao donne une majoration de la taille de $a_k + (k-1)b_k$ en fonction de k.

2.24 — Théorème des nombres premiers : nous avons vu que $\mathcal{P}$ était infini, on ne peut donc pas le dénombrer mais on peut par contre essayer de compter ses éléments dans des compacts, typiquement $[0, x]$ et s'il n'est pas possible d'obtenir une formule, essayer de trouver un équivalent, voire un développement limité de ce nombre quand $x \to +\infty$.

Théorème 2.25. — *Pour $x > 0$, soit $\pi(x)$ le cardinal de l'ensemble des nombres premiers inférieurs ou égaux à x ; on a alors l'équivalent suivant quand x tends vers $+\infty$:*

$$\pi(x) \sim \frac{x}{\ln x}.$$

Remarque : la démonstration classique utilise des résultats d'analyse complexe ; il existe toutefois une preuve purement algébrique, élémentaire et donc très difficile, due indépendamment à Erdös et Selberg. Un résultat du à Tchebychef qui est relativement simple à prouver est l'encadrement suivant

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x},$$

avec $c_1 = \ln\left(\frac{\sqrt{2}\sqrt[3]{3}\sqrt[5]{5}}{\sqrt[30]{30}}\right) \simeq 0,921$ et $C_2 = 6c_1/5 \simeq 1,106$. Ce dernier résultat suffit à prouver :
- *le postulat de Bertrand* à savoir que $\pi(2n) - \pi(n) > 0$;
- les résultats d'Ishikawa : $p_n + p_{n+1} > p_{n+2}$ et $p_n p_m > p_{n+m}$.

Une autre façon d'interpréter le théorème des nombres premiers est :
- p_n est de l'ordre de $n \ln n$; plus précisément Felgner en 1990 a montré que

$$0,91n \ln n < p_n < 1,7n \ln n;$$

- autour de n l'écart moyen entre deux nombres premiers est de l'ordre de $\ln n$.

2.26 — La fonction trou : la fin du paragraphe précédent suggèrent d'étudier la fonction trou sur $\mathcal{P}$ définie comme suit :

$$p_{n+1} = p_n + g(p_n) + 1.$$

- Notons déjà que $\limsup g = +\infty$; en effet l'intervalle $[n^2, n^2 + n]$ ne contient aucun nombre premier, on construit ainsi des « trous » dans $\mathcal{P}$ aussi large que l'on veut.
- En ce qui concerne la limite inf, on conjecture qu'elle est égale à 1, i.e. il existe une infinité de premiers jumeaux, soit $p, p + 2 \in \mathcal{P}$.
  Remarque : en 1919, Brun a montré que la somme des inverses des nombres premiers jumeaux était convergente. Notons $\pi_2(x)$ le nombre de premiers $p \leq x$ tels que $p+2 \in \mathcal{P}$, Hardy et Littlewood conjecturent que

$$\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{(\ln t)^2}, \quad C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \simeq 0,66.$$

- Le théorème des nombres premiers nous dit que pour tout $\epsilon > 0$, il existe n_0 tel que pour tout $n \geq n_0$, on a $g(p_n) \leq \epsilon p_n$. En 1937 Ingham a amélioré cette majoration en montrant que pour tout $\epsilon > 0$, il existe une constante K telle que $g(p) \leq K p^{5/8+\epsilon}$ et depuis le 5/8 a été régulièrement amélioré.
- Le théorème des nombres premiers dit que la valeur moyenne de $g(p)/\ln p$ est égale à 1 et Ricci a montré que l'ensemble des valeurs d'adhérences de $\{g(p)/\ln p : \ p \in \mathcal{P}\}$ avait une mesure de Lebesgue non nulle bien qu'à l'instant seul $+\infty$ ait été exhibé, prouvé en 1931 par Westzynthius. Maier a montré que la plus petite de ces valeurs d'adhérence était $\leq 0,249$: bien évidemment on pense qu'elle est en fait égale à 0 comme le suggère la conjecture des nombres premiers jumeaux.
- Sous l'hypothèse de Riemann, Cramer a montré l'existence d'une constante K telle que $g(p) < K\sqrt{p} \ln p$. On conjecture en fait qu'il existe une constante K telle que

$$g(p) \leq K(\ln p)^2.$$

2.27 — Quelques autres conjectures : une étude assez simple des anneaux euclidiens $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$ et $\mathbb{Z}[i\sqrt{3}]$ permet de montrer que :

$$\begin{array}{rcl} p = x^2 + y^2 & \Leftrightarrow & p \equiv 1 \mod 4 \\ p = x^2 + 2y^2 & \Leftrightarrow & p \equiv 1, 3 \mod 8 \\ p = x^2 + 3y^2 & \Leftrightarrow & p = 3 \text{ ou } p \equiv 1 \mod 3 \end{array}$$

Plus généralement on peut montrer le résultat suivant.

Théorème 2.28. — *Soit $n > 0$ un entier sans facteur carré tel que $n \not\equiv 3 \mod 4$. Il existe alors un polynôme irréductible unitaire $f_n(X) \in \mathbb{Z}[X]$ de degré $h(-4n)$ tel que si p premier*

impair ne divisant pas n ni le discriminant de $f_n(X)$ alors

$$p = x^2 + ny^2 \Leftrightarrow \begin{cases} (\frac{-n}{p}) = 1 \text{ et } f_n(x) \equiv 0 \mod p \\ \text{a une solution entière} \end{cases}$$

Exemples pour $n = 14$ on obtient

$$p = x^2 + 14y^2 \Leftrightarrow \begin{cases} (\frac{-14}{p}) = 1 \text{ et } (x^2+1)^2 \equiv 8 \mod p \\ \text{a une solution entière.} \end{cases}$$

En ce qui concerne le cas d'une seule variable, on conjecture que si a, b, c sont premiers entre eux avec $a > 0$, $a + b \equiv c \equiv 1 \mod 2$ et $b^2 - 4ac$ qui n'est pas un carré parfait, alors il existe une infinité de premiers de la forme $an^2 + bn + c$: le cas classique est $n^2 + 1$ que l'on ne sait toujours pas prouver.

Relativement à la fonction π, Hardy et Littlewood conjecturent [4] que pour tout $x, y \geq 2$:

$$\pi(x + y) \leq \pi(x) + \pi(y)$$

ce qui implique en particulier la conjecture des nombres premiers jumeaux. Enfin on conjecture que $\pi(n^2) < \pi((n+1)^2)$.

Plus généralement, soient $f_1, \cdots, f_k$ des polynômes de degré 1, irréductibles et vérifiant la propriété que pour tout nombre premier p il y ait au moins un entier n parmi $0, \cdots, p-1$ tel que p ne divise pas le produit des $f_i(n)$. On note $\omega(p)$ le complémentaire à p du nombre de tels entiers. Un tel ensemble de polynômes est dit admissible ; on cherche à connaître la proportion d'entiers en lesquels les polynômes prennent simultanément des valeurs premières. *Remarque :* se limiter à des ensembles de polynômes admissibles permet d'éviter des cas triviaux comme $f_1(t) = t$, et $f_2(t) = t + 1$.

Il est alors conjecturé que le nombre d'entiers $n \leq x$ tels que les valeurs $f_1(n), \cdots, f_k(n)$ sont simultanément premières, est pour x assez grand, de l'ordre de :

$$\Big(\prod_{p \in \mathcal{P}} \frac{1 - \frac{\omega(p)}{p}}{(1 - \frac{1}{p})^k}\Big) \frac{x}{\ln|f_1(x)| \cdots \ln|f_k(x)|}.$$

Le théorème des nombres premiers correspond au cas $k = 1$ et $f_1 = t$, le théorème de Dirichlet à $k = 1$ et $f_1 = at + b$, et pour $k = 2$, $f_1(t) = t$ et $f_2(t) = t + 2$, on obtient une version quantitative (et donc plus générale) de la conjecture des nombres premiers jumeaux.

La conjecture de Goldbach affirme que tout entier $n > 2$ est la somme de deux nombres premiers. Schnizel a montré que la conjecture de Goldbach était équivalente au fait que tout entier $n > 17$ était la somme de trois premiers distincts. Ramaré a montré que tout entier n est la somme d'au plus 6 nombres premiers et en 1966 Chen a montré que tout entier suffisament grand est la somme d'un nombre premier et d'un entier possédant au plus deux facteurs premiers.

La conjecture de Polignac affirme que tout entier naturel pair peut s'écrire comme différence de deux nombres premiers consécutifs et cela d'une infinité de manières.

Soit la suite, dite *d'Euclide-Mullin*, de premier terme $u_1 = 2$ et telle que le terme u_n soit le plus petit nombre premier diviseur du produit des termes u_i, pour $i < n$, augmenté de 1. Daniel Shanks conjecture que l'on obtient ainsi tous les nombres premiers.

4. La croyance des experts est que cette conjecture devrait pouvoir être infirmée.

2.29 — La fonction zêta de Riemann est définie pour $\mathrm{Re}\,(s) > 1$ par la série $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Cette fonction et ses généralisations (fonctions zêta de Dedekind, de Hasse-Weil, et plus généralement les fonctions L de Dirichlet, des formes modulaires, représentations automorphes...) jouent un rôle central en arithmétique. En particulier leurs valeurs aux entiers contiennent une multitude de renseignements concernant l'arithmétique des objets auxquels elles sont en fait attachées.

En guise d'introduction signalons la preuve d'Euler du fait qu'il existe une infinité de nombres premiers : celle-ci repose sur ce que désormais on appelle produit eulérien. Soit $f : \mathbb{N} \longrightarrow \mathbb{C}$ une fonction fortement multiplicative, i.e. $f(nm)f(n)f(m)$ pour tout n, m ; en particulier comme $f(n)f(1) = f(n)$, en prenant n tel que $f(n) \neq 0$, on obtient $f(1) = 1$. On suppose en outre que la série $\sum_n |f(n)|n^{-s}$ est absolument convergente de sorte que la série $\sum_k f(p^k)p^{-ks}$ est égale à $(1 - f(p)p^{-s})^{-1}$ et pour tout entier N

$$u_N(s) = \prod_{p \leq N} (\sum_k f(p^k)p^{-ks})$$

est un produit fini de séries absolument convergentes que l'on peut développer en utilisant la multiplicativité de f, soit $u_N(s) = \sum_n f(n)n^{-s}$ où la somme porte sur les n dont les facteurs premiers sont inférieurs à N.
Remarque : si on suppose seulement que f est multiplicative, i.e. $f(mn) = f(m)f(n)$ pour tout $n \wedge m = 1$, on obtient alors l'égalité

$$\sum_n f(n)n^{-s} = \prod_p (1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots)$$

Considérons alors le cas où $f(n) = 1$ pour tout $n \geq 1$ de sorte que si la série $\sum_{p \in \mathcal{P}} \frac{1}{p}$ converge alors la série des $\log(1 - 1/p)$ converge aussi et donc le produit $\prod(1 - 1/p)^{-1}$ converge. On en déduit alors que la série $\sum_n 1/n$ converge, ce qui est faux. Au final on obtient outre l'existence d'une infinité de nombres premiers, le fait que la série $\sum_{p \in \mathcal{P}} p^{-1}$ diverge, ce qui est plus fort.

Citons quelques résultats connus ou conjecturés sur la fonction ζ :

- **Prolongement analytique** : ζ a un prolongement méromorphe à $\mathbb{C}$ tout entier, holomorphe en dehors d'un pôle simple en $s = 1$ de résidu 1 ;
- pour $n \in \mathbb{N}$, on a $\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1} \in \mathbb{Q}$, où B_n est le n-ème nombre de Bernouilli, i.e. $\sum_{n=1}^{\infty} \frac{B_n t^n}{n!} = \frac{t}{e^t - 1}$

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad \cdots, \quad B_{12} = -\frac{691}{2730}$$

- $\pi^{-2k}\zeta(2k) = \frac{2^{2k-1}(-1)^k}{(2k)!} B_{2k} \in \mathbb{Q}$.
- Kummer : si $p \geq 3$ premier ne divise pas $\zeta(-1), \zeta(-3), \cdots, \zeta(2 - p)$ alors p ne divise pas le nombre de classes d'idéaux du corps $\mathbb{Q}(e^{2i\pi/p})$;
- Mazur et Wiles : ont donné une formule faisant intervenir le groupe des classes d'idéaux des $\mathbb{Q}(e^{2i\pi/p^n})$, pour calculer la puissance de p qui divise exactement le numérateur de $\zeta(-2k - 1)$;
- Rivoal : il existe une infinité de $\zeta(2k + 1)$ qui sont irrationnels ;
- **Hypothèse de Riemann** : hormis les zéros triviaux en les $-2n$, tous les autres sont sur la droite critique $\mathrm{Re}\,(s) = 1/2$: ce que l'on sait :
  - les zéros non triviaux sont dans la bande critique $0 < \mathrm{Re}\,(s) < 1$ et même dans une certaine zone...

– il y a une infinité de zéros sur la droite critique ;
– au moins 1/3 des zéros sont sur la droite critique.

Elle a des applications très importantes sur la répartition des nombres premiers :

$$\pi(x) = \mathrm{Li}(x) + \mathcal{O}(\sqrt{x}\log x)$$

où $\mathrm{Li}(x) := \int_2^x \frac{dt}{\ln t}$: le théorème des nombres premiers donne $\pi(x) \sim \mathrm{Li}(x)$.

2.6. Exercices. —

Exercice 2.1. — *En utilisant le théorème des nombres premiers $\pi(x) \sim \frac{x}{\ln x}$, donnez des équivalents quand N et x tendent vers l'infini de :*

$$p_N, \quad \sum_{n=1}^{N} p_n, \quad \sum_{p\leq x} p, \quad \sum_{p\leq x} \ln p, \quad \sum_{p\leq x} p^{-1}, \quad \sum_{p\leq x} \frac{\ln p}{p}$$

où p_n désigne le n-ième nombre premier. On désigne par d_n le ppcm des entiers $1, 2, 3, \cdots, n$: vérifiez que $\ln d_n \sim n$ pour $n \to \infty$.

3. Corps finis

Rappelons qu'un corps est un triplet $(K, +, \times)$ tel que $(K, +)$ est un groupe commutatif et où $(K - \{0\}$ est un groupe tel que $\times$ est distributif par rapport à $+$, i.e.

$$\forall (a, b, c) \in K^3 : \ a \times (b + c) = a \times b + a \times c \text{ et } (b + c) \times a = b \times a + c \times a.$$

Remarque : parfois le mot corps est réservé à la situation où $\times$ est commutative ; dans le cas contraire on parle d'algèbre à division. Cependant dans la situation où K est fini, la sémantique est évacuée par le fameux théorème de Wedderburn qui affirme que tout algèbre à division finie est commutative. *Nous admettrons* ce résultat bien que sa démonstration n'invoque pas de connaissances particulières. Avant de nous lancer dans la construction explicite de corps fini, commençons par étudier quelques propriétés élémentaires.

Proposition 3.1. — *Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.*

Preuve : Soit donc G un sous-groupe fini du groupe multiplicatif d'un corps K (commutatif), et soit n le cardinal de G. Si $g \in G$, son ordre est un diviseur de n car le sous-groupe engendré par g est de cardinal son ordre, et le cardinal d'un sous-groupe divise le cardinal du groupe (cf. cours). Ainsi pour d divisant n, on note A_d (resp. H_d) l'ensemble des éléments de G d'ordre d (reps. divisant d) : en particulier on a $H_d = \{g \in G \ / \ g^d = 1\}$. Le corps K étant commutatif, on a $|H_d| \leq d$, car le polynôme $X^d - 1$ y a au plus d racines. En outre si $A_d \neq$, alors $|H_d| = d$ car tout élément de A_d engendre un sous-groupe d'ordre d dans lequel tout élément g est tel que $g^d = 1$. Or $A_d \subset H_d$ soit $|A_d| \leq \varphi(d)$, l'inégalité $|A_d| \geq \varphi(d)$ étant évidente. En résumé soit A_d est vide soit son cardinal est égal à $\varphi(d)$. En reprenant le comptage de la question précédente, $G = \coprod_{d|n} A_d$, on obtient

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

où $\epsilon(d)$ est nul si A_d est vide, et égal à 1 sinon. En comparant cette égalité avec celle de (v), on en déduit que $\epsilon(d) = 1$ pour tout $d|n$, soit A_d non vide et en particulier A_n, d'où le résultat. □

On a déjà vu que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier ; nous allons ici donner une construction des corps finis.

Proposition 3.2. — *Soit K un corps, l'application $\phi : n \in \mathbb{Z} \mapsto n.1_K \in K$ a pour noyau $p\mathbb{Z}$ avec p nul ou premier.*

Preuve : Si ϕ est injective alors $n = 0$ sinon le noyau est de la forme $n\mathbb{Z}$. Soit alors $n = ab$ de sorte que $(a.1_K).(b.1_K) = 0_K$ et comme K est intègre, on a $a.1_K = 0_K$ ou $b.1_K = 0_K$ soit $n|a$ ou $n|b$. En résumé toute factorisation de $n = ab$ est telle que $a = \pm n$ et $b = \pm 1$ ou $a = \pm 1$ et $b = \pm n$ ce qui prouve que n est un nombre premier. □

Définition 3.3. — L'entier p nul ou premier de la proposition précédente est appelé la caractéristique de K.

Remarque : si K est fini sa caractéristique est nécessairement non nulle.

Définition 3.4. — Une extension K de L est un corps L contenant K que l'on peut considérer comme un K-espace vectoriel dont on note la dimension $[L : K]$.

Remarque : si K est fini de caractéristique p, c'est alors une extension de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ de dimension finie n de sorte que son cardinal est égal à $|K| = p^n$. Il résulte alors de ce qui précède qu'étant donné un corps fini K de cardinal $q = p^n$, on a $x^{q^n-1} = 1$ pour tout $x \in K^\times$ et donc $x^{q^n} = x$ pour tout $x \in K$. Ainsi l'ensemble K est de la forme $\{0_K, 1_K, \alpha, \alpha^2, \cdots, \alpha^{p^n-2}\}$: la multiplication de deux éléments est explicite par contre à priori on n'a pas de formule pour l'addition, de toute façon celle-ci dépendrait du choix de α.

3.1. Arithmétique sur $K[X]$. — Ici K désigne un corps quelconque ; l'anneau $K[X]$ possède exactement les mêmes propriétés arithmétiques que $\mathbb{Z}$ et même plus. Les questions difficiles sur $\mathbb{Z}$ ont aussi un intérêt en remplaçant $\mathbb{Z}$ par $K[X]$; en utilisant la dérivation le plus souvent on parvient à avancer et les résultats sont une source d'inspiration pour les questions sur $\mathbb{Z}$.

Théorème 3.5. — *Soient A et B des polynômes de $K[X]$ avec $B \neq 0$. Il existe alors un unique couple $(Q, R) \in K[X]$ tel que*

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

Remarque : Q s'appelle le quotient et R le reste de *la division euclidienne* de A par B.

Preuve : Elle est basée sur le fait élémentaire suivant : soient $U, V \in K[X]$ avec $k = \deg(U) \geq \deg(V) = q$ si a_k (resp. b_q) désigne le coefficient dominant de U (resp. de V) alors pour $Q = \frac{a_k}{b_q} X^{k-q}$ on a $\deg(U - VQ) < \deg(U)$.

Existence : soit $\mathcal{A} = \{A - BQ : \ Q \in K[X]\}$ et notons r le plus petit des degrés de ses éléments. Si on avait $r \geq \deg(B) \geq 0$ alors en appliquant ce qui précède, on construit un monôme Q' tel que $A - B(Q + Q') \in \mathcal{A}$ et de degré $< r$ d'où la contradiction.

Unicité : soient Q_1, Q_2 tels que $\deg(A - Q_i B) < \deg(B)$ pour $i = 1, 2$. On en déduit que

$$\deg(B) > \deg\Big((a - BQ_1) - (A - BQ_2)\Big) = \deg(B(Q_2 - Q_1))$$

et donc $Q_1 = Q_2$. □

Muni de cette division euclidienne, on peut reprendre les énoncés du premier chapitre et on obtient que :

- les idéaux de $K[X]$ sont principaux, i.e. engendrés par un unique polynôme ;
- notion de pgcd, ppcm ;
- relation de Bezout que l'on peut calculer via l'algorithme d'Euclide ;
- les lemmes d'Euclide et de Gauss sont vérifiés ;
- les éléments premiers sont les polynômes irréductibles et tout polynôme se décompose de manière unique aux inversibles près, comme un produit de polynômes premiers ;
- le quotient $K[X]/(P)$ est par définition l'ensemble des classes d'équivalence pour la relation d'équivalence
$$Q \sim Q' \Leftrightarrow P|(Q - Q').$$
Remarque : Les lois $+, \times$ et la multiplication par un scalaire de K, munissent alors ce quotient d'une structure d'algèbre : comme dans le cas de $\mathbb{Z}$, on remarque les calculs dans le quotient sont indépendants du choix des représentants dans $K[X]$.

  Toute classe d'équivalence possède un unique représentant dont le degré est strictement inférieur à celui de P : il se calcule comme le reste de la division euclidienne par P.

Proposition 3.6. — *Soit P un polynôme non constant ; la classe $\bar{A}$ d'un polynôme $A \in K[X]$ est inversible dans $K[X]/(P)$ si et seulement si A est premier avec P.*

Preuve : Si $\bar{A}$ est inversible alors il existe $\bar{B}$ tel que $\bar{A}.\bar{B} = \bar{1}$, autrement dit il existe Q tel que $AB + PQ = 1$ et donc $A \wedge P = 1$. Réciproquement si $A \wedge P = 1$, on considère une relation de Bezout $AB + PQ = 1$ de sorte que $\bar{B}$ est l'inverse de $\bar{A}$ dans $K[X]/(P)$. □

Corollaire 3.7. — *L'algèbre $L = K[X]/(P)$ est un corps si et seulement si P est un polynôme premier de $K[X]$; dans ce cas on a $[L : K] = \deg P$ et P possède une racine dans L.*

Preuve : Il reste à vérifier que $[L : K] = \deg P =: n$ ce qui découle directement du fait que la famille $(1, \bar{X}, \bar{X}^2, \cdots, \bar{X}^{\deg P - 1})$ est une base. Vérifions tout d'abord la liberté : si $\sum_{i=0}^{n-1} a_i \bar{X}^i = \bar{0}$ alors $P| \sum_{i=0}^{n-1} a_i X^i$ ce qui impose $a_i = 0$ pour tout $i = 0, \cdots, n-1$. Vérifions enfin que la famille est génératrice : soit $\bar{A} \in L$ et soit $A \in \bar{A}$. On effectue la division euclidienne de A par P soit $A = PQ + R$ avec $\deg R < n$ avec $\bar{A} = \bar{R} = \sum_{i=0}^{n-1} a_i \bar{X}^i$.

Notons ensuite $\alpha := \bar{X}$; on a alors $P(\alpha) = \overline{P(X)} = \bar{0}$ et donc α est une racine de P dans L. □

Une recette : le corollaire précédent nous fournit alors un moyen simple pour construire un corps fini de cardinal p^n : il suffit de prendre un polynôme $P(X) \in \mathbb{F}_p[X]$ irréductible de degré n et de considérer $K = \mathbb{F}_p[X]/(P(X))$. Le seul problème est alors de savoir s'il pour tout p premier et $n \geq 1$, il existe un polynôme de $\mathbb{F}_p[X]$ de degré n qui soit irréductible sur $\mathbb{F}_p$: ce sera l'objet essentiel du paragraphe précédent. Notons par ailleurs « la réciproque » de ce fait donnée par la proposition suivante.

Proposition 3.8. — *Soit K un corps fini de cardinal p^n, il existe alors un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n tel que K soit isomorphe au corps $\mathbb{F}_p[X]/(P(X))$.*

Preuve : Soit α un générateur du groupe multiplicatif $K^\times$ dont l'existence est assurée par la proposition 3.1 et soit $f : \mathbb{F}_p[X] \twoheadrightarrow K$ définie par $f(Q) = Q(\alpha)$: elle est surjective puisque tout élément non nul de K est de la forme α^k. Le noyau $\mathrm{Ker}\, f$ est un idéal forcément principal,

non nul engendré par un polynôme que l'on peut prendre unitaire et que l'on note μ_α de sorte que par passage au quotient f induit un isomorphisme $\mathbb{F}_p[X]/(\mu_\alpha(X)) \simeq K$. L'égalité des dimensions donne alors $\deg \mu_\alpha = n$. □
Remarque : le résultat précédent est un cas particulier du théorème de l'élément primitif ; le polynôme μ_α s'appelle le polynôme minimal de α sur $\mathbb{F}_p$.

3.9 — La notion d'irréductibilité d'un polynôme dépend du corps dans lequel on le considère ; ainsi par exemple X^2+1 est irréductible dans $\mathbb{R}[X]$ et réductible dans $\mathbb{C}[X]$. En général montrer qu'un polynôme est irréductible n'est pas chose aisée, signalons toutefois les deux critères suivant.

Théorème 3.10. — *Soit $K \subset L$ une extension telle que $[L:K] = n$ et soit $\alpha \in L$. L'ensemble $I_{K,\alpha} = \{P \in K[X] :\ P(\alpha) = 0\}$ est un idéal engendré par le polynôme unitaire $\mu_{K,\alpha}$ appelé polynôme minimal de α sur K qui est irréductible sur K de degré $\leq n$.*

Preuve : Soit $A, B \in I_{K,\alpha}$ et $Q \in K[X]$ alors $A-B$ et QA appartiennent à $I_{K,\alpha}$ car $(A-B)(\alpha) = 0$ et $(QA)(\alpha) = 0$. Par ailleurs comme $1, \alpha, \cdots, \alpha^n$ est une famille de cardinal $> n$, elle est liée de sorte qu'il existe un polynôme de degré n appartenant à $I_{K,\alpha}$. Ainsi $\mu_{K,\alpha}$ est un polynôme non nul de degré $\leq n$; vérifions qu'il est irréductible. Soit $\mu_{K,\alpha} = AB$ alors $A(\alpha)B(\alpha) = 0$ et comme K est intègre, on a $A(\alpha) = 0$ ou $B(\alpha) = 0$ et donc $\mu_{K,\alpha}$ divise A ou B d'où le résultat. □

Théorème 3.11. — *Soit $P \in K[X]$ alors P est irréductible dans $K[X]$ si et seulement si pour tout $K \subset L$ tel que $[L:K] \leq \frac{\deg P}{2}$, P n'a pas de racine dans L.*

Preuve : Supposons P irréductible et soit $K \subset L$ tel que $[L:K] < (\deg P)/2$ tel que P possède une racine $x \in L$. Soit $I_K(x) := \{Q \in K[X] :\ Q(x) = 0\}$; il s'agit clairement d'un idéal dont nous notons $\mu_{K,x}$ le générateur unitaire. L'application qui à $Q \in K[X] \mapsto Q(x) \in K[x] \subset L$ induit alors un isomorphisme $K[x] \simeq K[X]/(\mu_{K,x})$ de sorte que $\deg \mu_{K,x} < \deg P$ et donc $\mu_{K,x}$ est un diviseur strict de P ce qui n'est pas.

Réciproquement, raisonnons par contraposition : si P est réductible il possède alors un facteur irréductible Q de degré $\leq (\deg P)/2$. Notons $L = K[X]/(Q)$ de sorte que P possède une racine dans L, à savoir la classe de X. □
Remarque : pour $\deg P \leq 3$, on retrouve le fait élémentaire suivant : P est irréductible si et seulement s'il n'a pas de racines dans K.

3.2. Construction. — Le corollaire 3.7 donne un procédé pour construire des corps finis ; prendre $K = \mathbb{F}_p$ et construire un polynôme $P(X) \in \mathbb{F}_p[X]$ irréductible. Considérons les premiers exemples suivant :

(i) $\mathbb{F}_2[X]/(X^2+X+1)$ est un corps à 4 éléments ;
(ii) $\mathbb{F}_2[X]/(X^3+X+1)$ est un corps à 8 éléments ;
(iii) $\mathbb{F}_2[X]/(X^4+X+1)$ est un corps à 16 éléments ; le sous-corps engendré par X^2+X est de cardinal 4 ;
(iv) $\mathbb{F}_3[X]/(X^2+X-1)$ est un corps à 9 éléments.

Preuve : (i) On vérifie rapidement que X^2+X+1 n'a pas de racines dans $\mathbb{F}_2$, étant de degré 2 il y est alors irréductible de sorte que $\mathbb{F}_2[X]/(X^2+X+1)$ est un corps, une extension de degré 2 de $\mathbb{F}_2$ et donc isomorphe à $\mathbb{F}_4$ qui par convention est **le** corps de cardinal 4 contenu dans une clôture algébrique $\bar{\mathbb{F}}_2$ de $\mathbb{F}_2$ fixée une fois pour toute. Comme $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$, tout élément autre que $0, 1$ est un générateur de $\mathbb{F}_4^\times$, soit X et $X+1$.

Remarque : on notera par ailleurs que X^2+X+1 est le seul polynôme irréductible de degré 2 ce qui permet dès à présent en utilisant la proposition 3.8, de conclure à l'unicité, à isomorphisme près, d'un corps de cardinal 4.

(ii) De même, on vérifie que X^3+X+1 n'a pas de racines dans $\mathbb{F}_2$; étant de degré 3 il est alors irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^3+X+1)$ est un corps de cardinal 8 et donc isomorphe à $\mathbb{F}_8$. Comme $\mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$ tout élément autre que $0,1$ est un générateur du groupe des inversibles, par exemple X.

(iii) Encore une fois X^4+X+1 n'a pas de racines sur $\mathbb{F}_2$ mais cela ne suffit pas pour conclure à son irréductibilité, en effet il pourrait être le produit de deux polynômes irréductibles de degré 2. Or d'après (i), X^2+X+1 est l'unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$ et comme X^4+X+1 n'a pas de racines multiples, son polynôme dérivée étant égal à 1, il ne peut pas être égal à $(X^2+X+1)^2$: évidemment plus simplement on peut calculer $(X^2+X+1)^2 = X^4+X^2+1$.

(iv) À nouveau X^2+X-1 n'a pas de racines dans $\mathbb{F}_3$, il y est donc irréductible et $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+X-1)$. En outre $\mathbb{F}_9^\times \simeq \mathbb{Z}/8\mathbb{Z}$ de sorte qu'il y a $\varphi(8)=4$ générateurs et donc 4 non générateurs. On a $X^4 = (X-1)^2 = X^2-2X+1 = -3X+2 = -1$ et X est un générateur de $\mathbb{F}_9^\times$. □

Lemme 3.12. — *Soit K un corps de caractéristique p et $P(X) \in K[X]$ alors $P(X) \in \mathbb{F}_p[X]$ si et seulement si $P(X^p) = P(X)^p$.*

Preuve : Soit $P(X) = \sum_{i=0}^n a_i X^i$ avec $a_i \in K$; si $P(X) \in \mathbb{F}_p[X]$ alors $\left(\sum_{i=0}^n a_i X^i\right)^p = \sum_{i=0}^n a_i^p X^{pi} = \sum_{i=0} a_i (X^p)^i = P(X^p)$. La réciproque se montre de la même façon en remarquant que l'ensemble des $x \in K$ tels que $X^p = X$ est égal à $\mathbb{F}_p \subset K$: en effet tout élément de $\mathbb{F}_p$ est une racine du polynôme $X^p - X$ lequel a au plus p solutions dans K d'où le résultat. □

Proposition 3.13. — *Soit P un polynôme irréductible unitaire de $\mathbb{F}_p[X]$ de degré r. Si L est une extension de $\mathbb{F}_p$ possédant une racine α de P alors $P(X) = \prod_{i=0}^{r-1}(X-\alpha^{p^i})$.*

Preuve : Notons p^n le cardinal de L ; d'après la proposition 3.1, on a $\alpha^{p^n} = \alpha$. Par ailleurs l'ensemble des m tels que $\alpha^{q^m} = \alpha$ est un sous-groupe de $\mathbb{Z}$; notons s son générateur positif. Comme $P(X) \in \mathbb{F}_p[X]$, d'après le lemme précédent on a $P(X^p) = P(X)^p$ de sorte que les α^{p^i} pour $i = 0, \cdots, s-1$ sont des racines de P dans L. Notons

$$Q(X) = \prod_{i=0}^{s-1}(X-\alpha^{p^i})$$

qui est à coefficients dans $\mathbb{F}_p[X]$ car $Q(X^p) = Q(X)^p$ et divise P ; on en déduit donc que $P = Q$ car P est irréductible et donc $s = r$ d'où le résultat. □

Proposition 3.14. — *Soit p un nombre premier et n un entier ≥ 1 ; on a alors l'égalité*

$$X^{p^n} - X = \prod P$$

où P décrit l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré divisant n.

Preuve : Si on suppose que P divise $X^{p^n}-X$ alors $r = \deg P$ divise n ; si réciproquement on suppose que r divise n alors les racines α^{q^i} pour $i = 1, \cdots, r$ sont aussi racines de $X^{p^n}-X$ et donc P divise $X^{p^n}-X$. Le résultat découle alors de l'observation évidente que $X^{p^n}-X$

n'a pas de racines multiples puisqu'il est premier avec son polynôme dérivé qui est égal au polynôme constant égal à -1. □

Corollaire 3.15. — *Pour tout $n \geq 1$, il existe au moins un polynôme irréductible unitaire de $\mathbb{F}_p[X]$ de degré n.*

Preuve : Notons $I_n(p)$ le cardinal de l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p$; d'après la proposition précédente on a

$$p^n = \sum_{d|n} I_d(p) d.$$

On va alors montrer par récurrence sur n que $I_n(p) > 0$. Le résultat est clair pour $n = 1$, supposons donc le résultat acquis jusqu'au rang $n-1$ et traitons le cas de n. On réécrit l'égalité précédente sous la forme

$$p^d = dI_d(p) + \sum_{d'|d,\ d'<d} I_{d'}(p) d' \qquad \forall d < n$$

avec d'après l'hypothèse de récurrence $p^d > dI_d(p)$. Ainsi la formule ci-dessus pour $d = n$ donne les inégalités

$$p^n < nI_n(p) + \sum_{d|n,\ d\neq n} p^d \leq nI_n(p) + \sum_{k=0}^{n-1} p^k = nI_n(p) + \frac{p^n - 1}{p-1} < nI_n(p) + p^n$$

et donc $I_n(p) > 0$ d'où le résultat. □

Corollaire 3.16. — *Pour tout $n \geq 1$ et pour tout nombre premier p, il existe un corps de cardinal p^n.*

Preuve : Il suffit de considérer $K = \mathbb{F}_p[X]/(P(X))$ pour P un polynôme irréductible sur $\mathbb{F}_p$ et de degré n dont l'existence est assurée par le corollaire précédent. □

3.3. Résultats généraux. —

Proposition 3.17. — *Deux corps finis de même cardinal sont isomorphes.*

Preuve : Soit K un corps fini ; son cardinal est de la forme p^n avec p premier. D'après la proposition 3.1 il existe $\alpha \in K^\times$ d'ordre $p^n - 1$. On considère alors le morphisme $\mathbb{F}_p[X] \to K$ qui à X associe α ; il est surjectif et son noyau est un idéal de la forme $(P(X))$ pour un polynôme $P(X) \in \mathbb{F}_p[X]$ nécessairement irréductible. Quitte à le diviser par son coefficient dominant, on peut le prendre unitaire de sorte d'après la proposition 3.14 il divise $X^{p^n} - X = \prod_{a\in K}(X - a)$.

Si L st un corps de cardinal p^n comme tout $a \in L$ vérifie $a^{p^n} = a$, les racines de $X^{p^n} - X$ dans L sont exactement tous ses éléments de sorte que le polynôme $P(X)$ est totalement décomposé dans L. Étant donné une racine a quelconque de P dans L, le morphisme de $\mathbb{F}_p[X] \to L$ qui à X associe a se factorise pas $\mathbb{F}_p[X]/(P(X))$ et induit un isomorphisme de K sur L. □

Remarque : pour tout q de la forme p^r, soit $\mathbb{F}_q$ « le » corps de cardinal q ; les résultats du paragraphe précédent s'adaptent en remplaçant $\mathbb{F}_p$ par $\mathbb{F}_q$ et donc p par q.

Proposition 3.18. — *Soit K un corps de cardinal p^n ; si $L \subset K$ est un sous-corps de K son cardinal est alors de la forme p^d pour $d|n$. Réciproquement pour tout diviseur d de n, il existe un sous-corps de K de cardinal p^d.*

Preuve : Dans le sens direct, en considérant K comme un L-espace vectoriel on obtient que son cardinal est égal à $p^n = (p^d)^e$ et donc d divise n. Réciproquement si d divise $n = kd$, on a $p^n - 1 = (p^d - 1)N$ avec $N = (p^d)^{k-1} + \cdots + 1$ et donc

$$X^{p^n} - X = X(X^{p^{dk}-1} - 1) = X(X^{p^d-1} - 1)(X^{(p^d-1)(N-1)} + \cdots + 1)$$

et donc comme K est l'ensemble des racines de $X^{p^n} - X$ dans K, l'ensemble des racines dans K du polynôme $X^{p^d} - X$ forme un corps de cardinal p^d. □

3.19 — Construction de $\bar{\mathbb{F}}_p$: considérons par récurrence un corps $\mathbb{F}_{p^{n!}}$ de cardinal $p^{n!}$ comme une extension de degré n de $\mathbb{F}_{p^{(n-1)!}}$ qui existe d'après ce qui précède (unique à isomorphisme près). Notons alors $\bar{\mathbb{F}}_p$ la réunion croissante $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$; c'est un corps. En effet pour $x, y \in k$, il existe n tels que $x, y \in \mathbb{F}_{p^{n!}}$ et $x + y, xy$ sont définis dans $\mathbb{F}_{p^{n!}}$. Il est en outre immédiat que $\bar{\mathbb{F}}_p$ est algébrique sur $\mathbb{F}_p$ car tout $x \in k$ est un élément d'un $\mathbb{F}_{p^{n!}}$ pour n assez grand. Il reste alors à voir que $\bar{\mathbb{F}}_p$ est algébriquement clos ; soit donc $P(X) \in k(X)$ irréductible et soit $\mathbb{F}_{p^m}$ une extension contenant les coefficients de P et soit L un corps de rupture de P dans $\bar{\mathbb{F}}_p$ sur $\mathbb{F}_{p^m}$; L est alors une extension finie de $\mathbb{F}_{p^m}$ et est donc égale à un certain $\mathbb{F}_{p^r}$ et donc inclus dans $\mathbb{F}_{p^{r!}} \subset k$. Ainsi tout polynôme irréductible sur k est de degré 1 soit k algébriquement clos.

Remarque : étant donné une construction de $\bar{\mathbb{F}}_p$ comme ci-dessus, pour tout $n \geq 1$ on notera $\mathbb{F}_{p^n}$ **le** corps de cardinal p^n contenu dans $\bar{\mathbb{F}}_p$: il est égal à l'ensemble des racines dans $\bar{\mathbb{F}}_p$ du polynôme $X^{p^n} - X$.

Corollaire 3.20. — *Les sous-corps de $\mathbb{F}_{p^n}$ sont exactement les $\mathbb{F}_{p^r}$ où r divise n ; en particulier le plus petit sous-corps de $\bar{\mathbb{F}}_p$ contenant $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^m}$ est $\mathbb{F}_{p^{n\vee m}}$ alors que $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{n\wedge m}}$.*

Preuve : Le premier point découle directement de la proposition 3.18. En particulier si $\mathbb{F}_{p^r}$ contient $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^m}$ alors $n|r$ et $m|r$ de sorte que $n \vee m|r$ et $\mathbb{F}_{p^{n\vee m}} \subset \mathbb{F}_{p^r}$; on conclut alors en remarquant que $\mathbb{F}_{p^{n\vee m}}$ contient $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^m}$.

De la même façon $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m}$ est un corps $\mathbb{F}_{p^d}$ tel que $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^m}$ en sont des extensions. On en déduit donc que d divise n et m et donc d divise $n \wedge m$ et donc $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^{n\wedge m}}$. Réciproquement comme $n \wedge m$ divise n et m, on en déduit que $\mathbb{F}_{p^{n\wedge m}} \subset \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m}$ d'où le résultat. □

3.4. Exercices. —

Exercice 3.1. — ***Partage de secret*** *: Soit p un nombre premier "grand" ; tous les entiers considérés dans la suite seront supposés inférieur à p. Soit s_0 un entier. On choisit alors $n-1$ entiers $s_1, \cdots, s_{n-1}$ "au hasard" (inférieur à p donc) et soit P le polynôme $\sum_{i=0}^{n-1} s_i X^i$.*

(1) On introduit les n formes linéaires : $f_i : Q \in \mathbb{Q}_{n-1}[X] \mapsto Q(i) \in \mathbb{Q}$. En considérant les polynômes de Lagrange

$$L_i(X) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{X - j}{i - j}$$

montrer que la famille $(f_i)_{0 \leq i \leq n-1}$ est libre. Montrer alors que la connaissance des $P(i)$ pour $1 \leq i \leq n$, permet de retrouver s_0.

(2) On fixe $1 \leq i_0 \leq n$; décrivez

$$\cap_{\substack{1\leq i\leq n\\ i\neq i_0}} \operatorname{Ker} f_i$$

On suppose connu les $P(i)$ pour $1 \leq i \neq i_0 \leq n$. Sachant que $P(X)$ est de la forme $\sum_{i=0}^{n-1} s_i X^i$, que sait-on sur s_0 ?

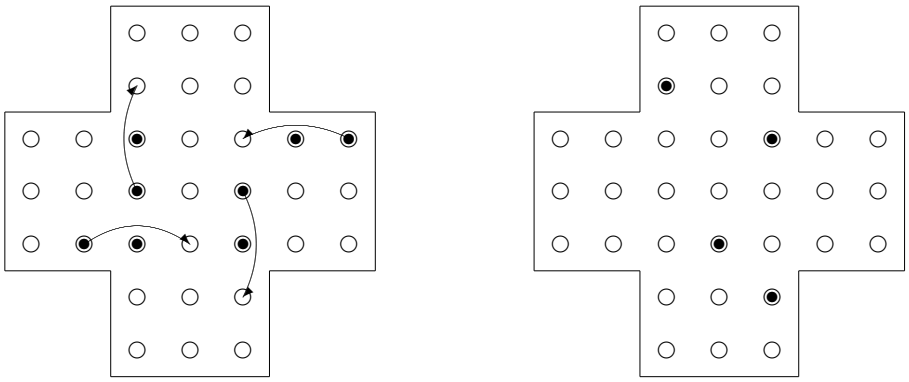
(3) On suppose désormais connue la congruence modulo p des $P(i)$ pour $i \neq i_0$, i.e. le reste de la division euclidienne de $P(i)$ par p. Montrer alors que l'on ne sait rien sur s_0.

Indication (on l'admettra) : l'ensemble des restes de la division euclidienne par p de $\lambda \frac{n!}{i_0}$ lorsque λ décrit $\mathbb{Z}$, est égal à $\{0, 1, \cdots, p-1\}$.

(4) Le code pour déclencher une frappe nucléaire est un nombre inférieur à p que seul le président connaît. Au cas où celui-ci serait dans l'impossibilité d'agir, il est prévu que son état major constitué de n membres puissent déclencher la frappe sans que toutefois $n-1$ parmi eux y parviennent. Proposer une solution mathématique à ce problème en vous inspirant des questions précédentes.

(5) Généraliser la question précédente au cas où l'on voudrait que k d'entre eux le puissent sans que $k-1$ n'y parviennent.

Exercice 3.2. — *Le jeu du solitaire se joue sur un plateau disposant de 33 réceptacles (cercle vide) dans lesquels il peut y avoir des billes notés avec un cercle plein. À chaque étape on peut faire passer une bille au dessus d'une autre sur un axe vertical ou horizontal, pourvu que le réceptacle suivant soit vide, comme dans la figure suivante*



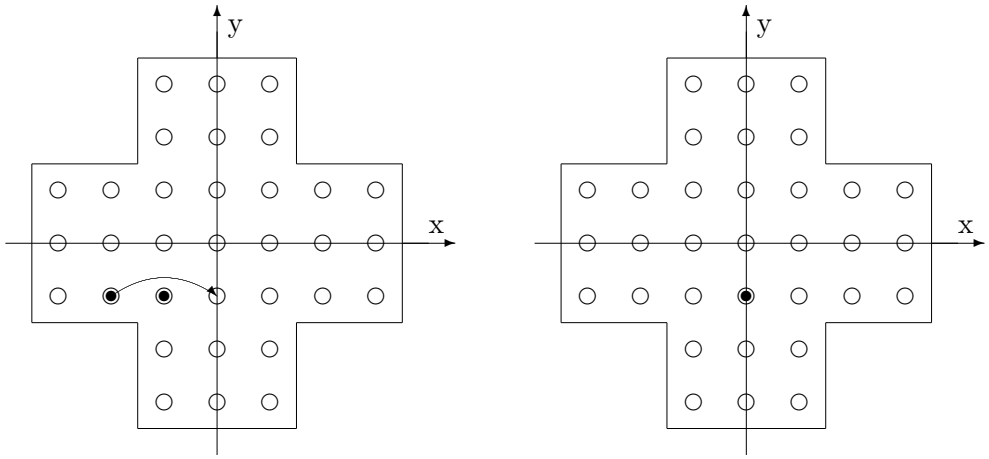
Soit alors O placé au centre du plateau et un repère (O, x, y) comme dans la figure suivante et pour une configuration $\mathcal{C}$ quelconque de billes sur le plateau on introduit

$$\alpha_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x+y} \in \mathbb{F}_4 \quad \beta_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x-y} \in \mathbb{F}_4$$

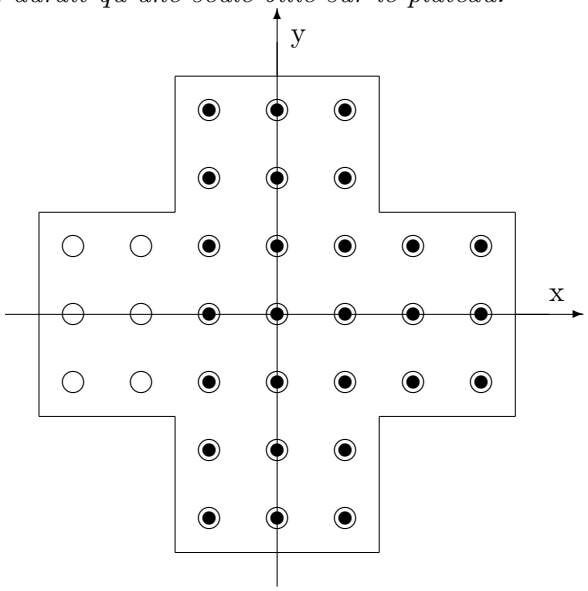
où j est un générateur de $\mathbb{F}_4^\times$.

(1) Montrer que (α, β) est un invariant du jeu.

(2) Habituellement le jeu consiste à partir d'une configuration où l'on place des billes dans tous les réceptacles sauf un seul disons (x_0, y_0) et à arriver à la configuration où tous les réceptacles sont vides sauf celui (x_0, y_0). Montrer qu'effectivement les deux configurations précédentes, possèdent les mêmes invariants (α, β).



(3) Partant de la configuration suivante, montrer qu'il est impossible d'arriver à une configuration où il n'y aurait qu'une seule bille sur le plateau.



4. Un peu de cryptographie

La cryptographie consiste à communiquer avec une autre personne sans que des oreilles indiscrètes puisse comprendre le sens du message : on pense bien sûr aux communications sur le champ de bataille, aux télécommunications, aux transferts de données bancaires sur internet...

4.1. La méthode de cryptographie RSA. — Il s'agit d'un système dit à clef publique, i.e. tout le monde connaît le procédé de cryptage mais seul une personne (le receveur) connaît

la clef qui permet de déchiffrer. Concrètement on choisit deux nombres premiers p et q distincts impairs très grands (plus quelques autres contraintes) et on pose $n = pq$; on fixe aussi $0 \leq c < n$ un entier premier avec $\varphi(n)$. Sont publiques les entiers n et c ainsi que le procédé suivant. Si A veut envoyer un message à R, il le coupe d'abord en bouts et les transforme en des nombre m_i plus petit que n ; ensuite il envoie les m_i^c modulo n.

Le problème pour R ou pour B indiscret est de retrouver m connaissant n et c et sachant que $n = pq$ avec p, q premiers connus seulement de R. Pour R la méthode est assez simple, il lui suffit de connaître l'inverse e de c dans $(\mathbb{Z}/n\mathbb{Z})^\times$; en effet on a alors $(m^c)^e \equiv m \mod n$. Pour calculer e, R utilise le théorème chinois et calcule donc les inverses e_p et e_q de c dans respectivement $(\mathbb{Z}/p\mathbb{Z})^\times$ et $(\mathbb{Z}/q\mathbb{Z})^\times$ qui est d'après le petit théorème de Fermat égal à c^{p-2} et c^{q-2}. On construit alors facilement e en utilisant la version constructive du théorème chinois. Pour B, la situation est plus critique ; pour l'instant sa stratégie est de casser n, i.e. de trouver p ce qui est très long pourvu que R ait choisi p et q très grand convenablement. A ce propos signalons les précautions élémentaires à prendre :

- p et q doivent être pris tous deux grands, sinon l'algorithme ρ de Pollard pourrait très facilement trouver le petit facteur ;
- il faut que $|p - q|$ soit grand sinon pour $q = p + \delta$ avec δ beaucoup plus petit que p, on aurait pour $N = pq, \sqrt{N} = p\sqrt{1+\delta} \sim p + \delta/2$ et on pourra trouver p par un algorithme naïf en $O(\delta)$ étapes ;
- il faut que $p - 1$ et $q - 1$ ne soit pas trop friable au sens précédent, sinon l'algorithme $p - 1$ de Pollard permettrait de le trouver rapidement ;
- il faut que l'exposant secret e ne soit pas trop petit ; trivialement si $e = O(\log N)$ alors en faisant $O(\log N)$ essais on trouvera e. En fait on peut montrer qu'il faut éviter $e << N^{1/4}$.

Il existe sûrement d'autres contraintes connues ou pas sur les choix de p, q, e. Signalons tout de même que la construction de grands nombres premiers ne posent pas de problèmes pratiques : pour cela on part d'un entier impair k grand, on test en temps polynomial s'il est premier et sinon on teste $k + 2$ et ainsi de suite. Le théorème des nombres premiers nous dit qu'en moyenne on devrait tomber sur un nombre premier au bout de $\ln k$ étapes. Si la conjecture sur la fonction trou, comme quoi $g(p_n) \leq K(\ln p_n)^2$ est vrai, on est assuré de trouver ainsi un nombre premier en temps polynomial.

4.2. Logarithme discret. — Étant donné un corps K et un générateur α de $K^\times$, le problème du logarithme discret est pour $x \in K$, de trouver n tel que $x = \alpha^n$. Certains algorithmes de cryptographie sont basés sur la croyance que pour les corps finis tels que $q - 1$ est difficilement factorisable, ce problème est difficile à résoudre. Signalons tout de même l'algorithme suivant dans le cas où $q - 1$ est friable.

4.1 — Algorithme de Silver, Pohlig et Hellman : on suppose connue la factorisation de $q - 1$ en facteurs premiers

$$q - 1 = \prod_{p | q-1} p^{r_p};$$

l'algorithme sera d'autant plus efficace que les premiers divisant $q - 1$ sont petits. D'après le lemme chinois, il suffit de connaître n modulo p^{r_p} ; écrivons

$$n \equiv n_0 + n_1 p + \cdots + n_{r_p - 1} p^{r_p - 1} \mod p^{r_p} \qquad 0 \leq n_i < p,$$

et cherchons à déterminer les n_i. Comme $x^{\frac{q-1}{p}}$ appartient au groupe μ_p des racines p-èmes de l'unité dans K lequel est engendré par $\zeta_p = g^{\frac{q-1}{p}}$, on a $x^{\frac{q-1}{p}} = \zeta_p^{n_0}$ ce qui détermine n_0. Les

entiers $n_0, \cdots, n_{i-1}$ étant déterminés, soit

$$x_i = \frac{x}{g^{n_0+\cdots+n_{i-1}p^{i-1}}},$$

on a $x^{\frac{q-1}{p^{i+1}}} = \zeta^{n_i}$, ce qui détermine n_i.

4.2 — Algorithme de chiffrement à clé publique de El Gamal : Alice souhaite permettre à quiconque de lui transmettre des messages confidentiels ; elle choisit (K, g) comme précédemment et le rend publique.

- Alice choisit aléatoirement $1 < a < q-1$ qui sera sa clé secrète et calcule g^a qui sera sa clé publique.
- Pour envoyer un message $m \in K$, Bob choisit aléatoirement $1 < x < q-1$ et transmet à Alice (g^x, mg^{ax}).
- Afin de décrypter le message reçu, Alice connaissant $a$et g^x détermine l'inverse dans K de g^{ax}, i.e. g^{-ax} et le multiplie à mg^{ax} pour obtenir m.

4.3 — Protocole de Diffie-Hellman : Alice et Bob souhaitent se construire une clé secrète commune afin de communiquer sur un canal non sûr en utilisant cette clé pour chiffrer leur correspondance. Le principe qui date de 1976 est le suivant : soit (K, g) un corps fini de cardinal $q = p^n$ et g un générateur de $K^\times$, cette donnée est publique.

- Alice choisit secrètement et aléatoirement un entier $1 < a < q-1$ et elle transmet à Bob publiquement g^a ;
- Bob fait de même avec g^b ;
- Alice et Bob calculent g^{ab} qui constitue leur clé secrète.

4.4 — L'attaque de l'Homme du milieu : le protocole précédent est vulnérable à l'attaque de l'homme du milieu qui implique un attaquant capable de lire et de modifier tous les messages échangés entre Alice et Bob. L'attaquant intercepte la clé g^a envoyée par Alice et envoie à Bob une autre clé $g^{a'}$. De même, il remplace la clé g^b envoyée par Bob par une clé $g^{b'}$. L'attaquant peut ainsi communiquer avec Alice en utilisant la clé partagée $g^{ab'}$ et communiquer avec Bob en utilisant la clé partagée $g^{a'b}$. Alice et Bob croient ainsi avoir échangé une clé secrète alors qu'en réalité ils ont chacun échangé une clé secrète avec l'attaquant, l'homme du milieu.

4.5 — Algorithme de signature à clé publique de El Gamal : la parade classique à l'attaque de l'Homme du milieu consiste à signer les échanges de clés. Il s'agit alors pour l'expéditeur de signer son message afin que son destinataire puisse l'authentifier. Comme précédemment on choisit $(\mathbb{F}_p, g)$:

- Alice choisit $1 < a < p-1$ et publie g^a : a est la clé secrète et g^a la clé publique.
- Elle choisit ensuite $1 < e < p-1$ premier avec $p-1$ et calcule son inverse d modulo $p-1$.
- Alice calcule les entiers r, s définis par les conditions

$$g^e \equiv r \mod p, \quad 1 \leq r < p \text{ et } s \equiv d(m - ar) \mod p-1, \quad 1 \leq s < p.$$

  On a ainsi la congruence $\tilde{m} \equiv es + ar \mod p-1$.
- Alice envoie alors le message signé $(m, (r, s))$.

Bob peut alors authentifier Alice en calculant $(g^a)^r r^s \in \mathbb{F}_p^\times$ puis en vérifiant l'égalité attendue

$$g^{\tilde{m}} = r^s (g^a)^r \in \mathbb{F}_p^\times.$$

4.3. La méthode du sac à dos. — Le problème asymétrique utilisé par Merkle et Hellman est le suivant : étant donnés n entiers positifs $a_1 1, a_2, \cdots, a_n$ ainsi qu'un entier c, existe-t-il

un choix judicieux parmi les a_i tel que leur somme vaille exactement c, i.e. existe-t-il des $\epsilon_i \in \{0,1\}$ tels que $\sum_{i=1}^n \epsilon_i a_i = c$.

On parle de « problème de sac à dos »car on peut imaginer en pratique la recherche d'un empilage optimal d'objets de hauteur ai afin de remplir exactement un sac à dos de hauteur c.

Exemples considérons le problème suivant : $a_1 = 366$, $a_2 = 385$, $a_3 = 392$, $a_4 = 401$, $a_5 = 422$, $a_6 = 437$ et la valeur cible est $c = 1214$. Quels-sont les a_i (s'il en existe) qui, additionnés, valent c ? Une recherche rapide montre qu'une solution est $a_2 + a_3 + a_6 = 385 + 392 + 437 = 1214 = c$ soit $(e_1, e_2, e_3, e_4, e_5, e_6) = (0, 1, 1, 0, 0, 1)$.

Remarque : une version, dite décisionnelle, de ce problème consiste juste à demander s'il existe de tels e_i, sans chercher à les calculer. Ce problème est considéré comme très difficile (en théorie de la complexité on parle de problème NP-complet) et l'on ne connaît pas d'algorithme polynomial en n permettant de le résoudre dans tous les cas ; il est de plus très improbable qu'un tel algorithme existe. Un algorithme, exponentiel en n, fort simple au demeurant, permet cependant de résoudre ce problème : il suffit d'essayer toutes les possibilités pour les e_i, soit 2^n combinaisons. Une telle approche est désignée sous le terme de « recherche exhaustive »en cryptographie. L'inconvénient est que, si n est suffisamment grand (de l'ordre de 50 en pratique), le temps de calcul devient totalement impraticable.

Le cryptosystème de Merkle et Hellman utilise le problème de sac à dos précédemment décrit de la manière suivante : un entier positif n suffisamment grand est fixé pour tout le système, puis on chosit une suite $(b_1, b_2, \cdots, b_n)$ d'entiers positifs vérifiant la propriété suivante

$$\forall 2 \leq i \leq n, \quad b_i > \sum_{j=1}^{i-1} b_j.$$

On choisit ensuite un entier M, appelé module, supérieur à $\sum_{i=1}^n b_i$ puis $1 \leq W \leq M-1$ premier avec M. On calcule $a'_i = W \times b_i \mod M$ ainsi que la permutation π de $\{1, 2, \cdots, n\}$ telle que $a'_{\pi(1)}, a'_{\pi(2)}, \cdots, a'_{\pi(n)}$ soit une suite croissante notée $(a_1, a_2, \cdots, a_n)$ qui constituera la clé publique, la clé privée étant composée de M, W, $(b_1, b_2, \cdots, b_n)$ ainsi que de la permutation π.

Le message à chiffrer est écrit en binaire sous la forme $m_1 m_2 \cdots m_n$, avec $m_i \in \{0,1\}$ (si le message est trop long, il est coupé en blocs de n bits au plus). On calcule alors $c = \sum_{i=1}^n m_i a_i$ que l'on transmet. Pour déchiffrer le message, on calcule $d = W^{-1} c \mod M$ puis les $\epsilon_1, \cdots, \epsilon_n$ tels que $d = \sum_{i=1}^n \epsilon_i a b_i$ qui est un problème de sac à dos très simple via un algorithme glouton. Les m_i sont alors donnés par $\epsilon_{\pi(i)}$.

Remarque : bien que l'on pense que le problème du sac à dos général soit NP-complet, il s'avère que tous les systèmes cryptographiques construits sur la méthode précédentes ont été cassés, essentiellement via le fameux algorithme LLL.

4.4. Exercices. —

Exercice 4.1. — *Soit $K = \mathbb{F}_3[X]/(X^3 + 2X + 1)$; montrez que K est un corps de cardinal 27 et que X est un générateur du groupe multiplicatif. Trouvez i tel que $X^2 + X = X^i$.*

Exercice 4.2. — *Expliquez comment Alice et Bob arrivent à communiquer pour réussir le tour de magie suivant. Un quidam retire 5 cartes quelconques d'un jeu de 52 cartes. Alice en choisit une parmi les 5 puis repose les 4 autres cartes devant Bob qui devine alors la carte gardée par Alice.*

5. Codes correcteurs

La problématique des codes correcteurs est la suivante : A veut transmettre une information à B via un canal bruité (les ondes dans l'air ambiant, un flux d'électrons dans un cable...) de sorte que B le reçoit avec éventuellement des erreurs que l'on supposera pas trop nombreuses (sinon il faut changer de mode de transmission). Il s'agit alors pour B de détecter ces erreurs et si possible, les corriger. L'idée est alors pour A de rajouter de la redondance à son message ; citons l'exemple un peu bête suivant.
Exemples on prend pour alphabet $\mathbb{F}_2$. Supposons que A veuille transmettre l'un des 4 messages suivant : $00, 01, 10, 11$; il peut alors décider de l'envoyer en double de sorte que si B reçoit le message 0001 il sait qu'il y a eu une erreur de transmission. Cependant même en supposant qu'il n'y a qu'une seule erreur il ne sait pas si le message était 00 ou 01 ; il peut alors demander à A de lui renvoyer le message. Une solution moins coûteuse et aussi efficace est donnée par *le bit de parité* : on rajoute au message la parité de la somme des données soit $000, 011, 101, 110$. Bien sûr si A répète trois fois le message, on voit que B pourra détecter et corriger une erreur mais on sent bien qu'on peut faire plus brilliant.

5.1. Mise en place. — On fixe un alphabet fini F de cardinal q (rapidement F sera un corps fini) de sorte que tous les messages à transmettre constituent un sous-ensemble de F^k. La phase d'encodage consiste ensuite à choisir $n > k$ puis à associer injectivement à chaque information $I \in F^k$ un message $M \in F^n$; le sous-ensemble obtenu de F^n s'appelle *le code C de longueur n*. Le rapport k/n qui mesure la redondance s'appelle *le taux d'information* du code. On dit que le message $(m_1, \cdots, m_n)$ est affecté de r erreurs si r de ses coordonnées ne sont pas correctes.

Définition 5.1. — Soient $(x_1, \cdots, x_n)$ et $(y_1, \cdots, y_n)$ deux éléments de F^n ; la distance de Hamming entre x et y notée $d_H(x, y)$ est le nombre d'indices $1 \leq i \leq n$ tels que $x_i \neq y_i$.

Remarque : $d_h : F^n \times F^n \to \mathbb{N}$ mérite bien le nom de distance comme le lecteur le vérifiera facilement.

Lors de la phase de décodage, on supposera toujours que le nombre d'erreurs possibles sur un mot est limité de sorte que si le message reçu R appartient au code alors le nombre d'erreurs est nul et sinon le message initial M est un mot du code C qui minimise la distance de Hamming. On peut alors formaliser le processus de décodage comme une application $D : F^n \to F^n$ dont l'image appartient à C et qui est l'identité sur C. Pour que tout cela fonctionne correctement, il y a un certain nombre de contraintes que nous allons essayer d'exposer.

Définition 5.2. — Soit C un code sur F, on appelle distance minimum de C l'entier

$$d = \min\{d_H(x, y) : \ x \neq y \in C\}.$$

S'il existe un mot $m' \in C$ tel que $d_H(m', R) < r$, alors clairement $m' \neq m$ et donc il ne faut pas décoder par m' même s'il s'agit du mot de C le plus proche de R ; en résumé il faut supposer que le nombre d'erreur r est tel que $r \leq \lfloor d/2 \rfloor$: en effet si on avait $d_H(m', R) < s$ alors d'après l'inégalité triangulaire on aurait $d_H(m, m') < 2r \leq d$ ce qui contredit la définition de la distance minimum d de C. Pour d pair et $r = d/2$, il n'est pas non plus exclu qu'il y ait deux mots distincts de C à distance r de R ce qui ne permet pas de décoder correctement.

Définition 5.3. — La capacité de correction de C, notée souvent t, est l'entier

$$t = \lfloor \frac{d-1}{2} \rfloor.$$

On dit alors que C est un code t-correcteur.

Remarque : ainsi pour tout $m \neq m'$ dans C, les boules fermées $B(m,t)$ et $B(m,t')$ sont disjointes et pour tout $x \in F^n$, la boule $B(x,t)$ contient au plus un mot de C. Signalons la situation idéale, mais rare, suivante où tout mot de F^n peut se décoder.

Définition 5.4. — Un code C est dit parfait si F^n est la réunion disjointe des boules fermées $B(m,t)$ où m décrit C.

Remarque : en utilisant que le cardinal de toute boule fermée de rayon r est de cardinal $\sum_{i=0}^{r} \binom{i}{n}(q-1)^i$, le code C est parfait si et seulement si on a

$$|C|.\sum_{i=0}^{t} \binom{i}{n}(q-1)^i = q^n.$$

Un code est bon si $|C|$ et d sont grands ; évidemment ces exigences sont contradictoires.

5.2. Codes linéaires. — On prend pour F le corps $\mathbb{F}_q$; le code C est dit linéaire si C est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k. *Le poids* $\omega(x)$ d'un élément $x \in \mathbb{F}_q^n$ est le nombre de ses composantes non nulles, soit aussi $d_H(x,0)$. Ainsi on a $d = \min_{0 \neq x \in C} \omega(x)$.

Proposition 5.5. — ***(Borne du singleton)*** *On a l'égalité*

$$d \leq n - k + 1.$$

Preuve : Notons E le sous-espace vectoriel de $\mathbb{F}_q^n$ formé des éléments dont les $k-1$ dernières composantes sont nulles de sorte qu'en notant $(e_i)_{1 \leq i \leq n}$ la base canonique, E est engendré par $e_1, \cdots, e_{n-k+1}$. Comme $\dim E + \dim C > n$, $E \cap C$ n'est pas réduit à 0 et il existe donc x tel que $\omega(x) \leq n - k + 1$ d'où le résultat. □
Remarque : la distance relative d/n de C et son taux d'information k/n ne peuvent pas être simultanément proche de 1 vu que leur somme est plus petite que $1 + 1/n$. On dit que C est *un code MDS*, en anglais Maximum Distance Separable, si on a $d = n - k + 1$.

Définition 5.6. — Une matrice génératrice G d'un code C est une matrice dont les lignes forment une base. Une matrice vérificatrice H d'un code C est une matrice telle que $x \in C \Leftrightarrow Hx = 0$.

Proposition 5.7. — *La matrice H est vérificatrice si et seulement si elle est de rang $n-k$ et $G^t H = 0$.*

Preuve : Le résultat découle directement du fait qu'une matrice est vérificatrice pour $C = \{(u_1, \cdots, u_k)G : \ (u_1, \cdots, u_k) \in \mathbb{F}_q^k\}$ si et seulement si ses lignes forment une base des formes linéaires de $C^\perp$ s'annulant sur C. □

Remarque : rappelons comment on calcule une base des formes linéaires s'annulant sur C. On considère la matrice $\tilde{G}$ construite à partir de G en rajoutant une dernière ligne $(x_1 \cdots x_n)$. En opérant sur les colonnes de $\tilde{G}$, on se ramène alors à une matrice étagée de la forme

$$\begin{pmatrix} * & 0 & \cdots & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & * & \cdots & * & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & & & \ddots & 0 & & & \vdots \\ \vdots & & & & & * & 0 & \cdots & 0 \\ f_1 & f_2 & \cdots & \cdots & \cdots & f_k & f_{k+1} & \cdots & f_n \end{pmatrix}$$

et $f_{k+1}, \cdots, f_n$ forment une base de $C^{\perp}$. Une autre façon de procéder est d'utiliser les codes systématiques.

Définition 5.8. — Un code C est dit systématique s'il existe une matrice B ayant k lignes et $n-k$ colonnes telles que $(I_k|B)$ soit une matrice génératrice de C ; une matrice de cette forme est dite normalisée.

Remarque : si elle existe, la matrice normalisée est nécessairement unique. L'avantage de celle-ci est que le message se lit directement sur les k-premières composantes. En opérant sur les lignes, C de matrice génératrice G est systématique si et seulement si la matrice extraite des k premières colonnes et lignes, est inversible. En s'autorisant aussi à permuter les coordonnées, on se ramène toujours à un code systématique. Le lemme suivant fournit alors un algorithme pour construire H à partir de G.

Lemme 5.9. — *Si $G = (I_k|B)$ est la matrice génératrice normalisée de C alors $H = (-{}^tB|I_{n-k})$ est une matrice de contrôle.*

Correction des erreurs : supposons que le code est 1-correcteur et notons m' le message reçu différant du message envoyé x en au plus une coordonnée alors l'erreur à corrigée est $\epsilon = x' - x$ avec ϵ égal au vecteur e_i de la base canonique tel que $He_i = Hx'$. Plus généralement pour décoder un message, on commence par calculer tous les Hx pour les x tels que $\omega(x) \leq t$ de sorte que lorsque l'on reçoit un message m', la correction à apporter est ϵ tel que $\omega(\epsilon) \leq t$ et $H(\epsilon) = H(m')$.

Proposition 5.10. — *Soit H une matrice de contrôle de C ; la distance d de C est égal au nombre minimum de colonnes de H qui en tant que vecteurs de $\mathbb{F}_q^{n-k}$, sont linéairement dépendantes.*

Preuve : Le résultat découle des observations évidentes suivantes : s'il existe dans c un mot $(x_1, \cdots, x_n)$ de poids r alors de la relation $Hx = 0$, on en déduit qu'il existe r colonnes de H linéairement dépendantes ; la réciproque est identique. □

5.11 — **Code de Hamming de longueur 7 :** prenons l'ensemble des mots de sept chiffres binaires, $q = 2$, $n = 7$ et $\mathcal{C}$ le code ayant pour base

$$e_0 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix},$$

Pour transmettre un message $m = (m_0, m_1, m_2, m_3)$, on transmet $x = m_0e_0 + m_1e_1 + m_2e_2 + m_3e_3$. Les paramètres de ce code sont $(7, 4, 3)$. Une matrice vérificatrice est

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Remarque : la matrice H a été obtenue en opérant sur les lignes comme annoncés précédemment ; le lecteur pourra aussi vérifier qu'elle est de rang 3 et que $G^tH = 0$. En outre toutes les colonnes de H sont distinctes de sorte qu'on obtient toutes les vecteurs non nuls de $\mathbb{F}_3$. On en déduit alors que deux colonnes sont obligatoirement libres et qu'étant données deux colonnes quelconques de H, leur somme est une colonne de H. De la proposition précédente on en déduit que $d = 3$. Ainsi le code de Hamming de longueur 7 est 1-correcteur parfait mais il n'est pas MDS. Etant donné un message reçu x' on dira que le message initial était $x = x' + e_i$ où i est l'indice de la colonne de H égale à Hx'. En ce qui concerne l'information de départ

$$y = A^{-1} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \text{ où } A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

5.3. Codes linéaires cycliques. — L'exemple précédent suggère de rajouter une structure d'algèbre à un code linéaire C ; on obtient ce que l'on appelle un code linéaire cyclique ; précisément $C \subset \mathbb{F}_q^n$ est dit cyclique s'il est stable par l'automorphisme de décalage cyclique $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ défini par

$$T(a_1, \cdots, a_n) = (a_n, a_1, \cdots, a_{n-1})$$

.

Proposition 5.12. — *Considérons l'isomorphisme naturel d'espace vectoriel $\psi : \mathbb{F}_q^n \simeq \mathbb{F}_q[X]/Q(X)$ où $Q(X) = X^n - 1$ défini par*

$$\psi(x_1, \cdots, x_n) = x_1X^{n-1} + \cdots + x_{n-1}X + x_n.$$

Le code linéaire $C \subset \mathbb{F}_q^n$ est cyclique si et seulement si son image par ψ est un idéal de sorte que les codes cycliques de longueur n sont en bijection avec les polynômes unitaires divisant $X^n - 1$.

Preuve : L'automorphisme T de $\mathbb{F}_q^n$ dans l'identification donnée par ψ, correspond à la multiplication par X de sorte que C est cyclique si et seulement si $\psi(C)$ est un sous-espace vectoriel de $\mathbb{F}_q[X]$ stable par la multiplication par X et donc par tout élément de $\mathbb{F}_q[X]$; c'est

donc un idéal de $\mathbb{F}_q[X]/(Q(X))$. La fin de la proposition découle du fait que les idéaux du quotient $\mathbb{F}_q[X]/(X^n-1)$ sont en bijection avec les diviseurs de X^n-1. □

Remarque : le diviseur unitaire g de X^n-1 associé au code linéaire cyclique C s'appelle *le polynôme générateur* de C ; la dimension de C est $k = n - \deg g$. Le procédé de codage systématique est donné par la division euclidienne par g : le vecteur $(x_1, \cdots, x_k) \in \mathbb{F}_q^k$ est codé par le polynôme $c = c_I - c_R$ où $C_i = c_1 X^{n-1} + \cdots + x_k X^{n-k}$ et c_R de degré $< n-k$ est le reste de la division euclidienne de c_I par g, i.e. c_I porte l'information et c_R la redondance.

Corollaire 5.13. — *On suppose $n \wedge p = 1$. Les codes linéaires cycliques de longueur n sur $\mathbb{F}_q$ sont en bijection avec les parties $I \subset \mathbb{Z}/n\mathbb{Z}$ stables par la multiplication par q.*

Preuve : D'après la proposition 3.13, les racines d'un polynôme irréductible P sur $\mathbb{F}_q$ sont de la forme $\{\alpha, \alpha^q, \cdots, \alpha^{q^{r-1}}\}$ avec $\alpha^{q^r} = \alpha$ est une racine de P. Dans le cas où P est un facteur irréductible de X^n-1 ces racines sont des racines n-ème de l'unité lesquelles, une fois choisie une racine primitive, peuvent être vues comme des éléments de $\mathbb{Z}/n\mathbb{Z}$ de sorte que si α s'envoie sur k, α^q s'envoie sur qk, ce qui donne le résultat en considérant tous les facteurs irréductibles du polynôme générateur. □

En général la distance minimal d'un code linéaire cyclique n'est pas facile à calculer, on dispose cependant de la minoration élémentaire suivante.

Proposition 5.14. — *Soit C un code linéaire cyclique de longueur n sur $\mathbb{F}_q$ associé à $I \subset \mathbb{Z}/n\mathbb{Z}$ et supposons qu'il existe i et s tels que $\{i+1, i+2, \cdots, i+s\} \subset I$. La distance minimale d de C est $\geq s+1$.*

Preuve : Soient donc $0 \leq l_1 < \cdots < l_s < n$ et $\lambda_1, \cdots, \lambda_s \in \mathbb{F}_q$ tels que, avec $R(X) = \sum_{i=1}^s \lambda_i X^{l_i}$, on ait $R(\alpha^k) = 0$ pour tout $i+1 \leq k \leq i+s$. Ces équations s'écrivent matriciellement en faisant intervenir une matrice de Vandermonde qui est inversible de sorte que les λ_i sont tous nuls ce qui prouve le résultat. □

Remarque : notons $g(X) = a_0 + a_1 X + \cdots + a_{r-1} X^{r-1} + X^r$ le polynôme générateur du code cyclique C ; une matrice génératrice est alors

$$G = \begin{pmatrix} a_0 & \cdots & a_{r-1} & 1 & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{r-1} & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & \cdots & a_{r-1} & 1 & 0 \\ 0 & \cdots & \cdots & 0 & a_0 & \cdots & a_{r-1} & 1 \end{pmatrix}$$

En particulier toute code cyclique est systématique. Notons alors $h(X) = \frac{X^n-1}{g(X)} = b_0 + b_1 X + \cdots + b_{k-1} X^{k-1} + X^k$ ce qui se traduit matriciellement par l'égalité $G^t H = 0$ où

$$H = \begin{pmatrix} 1 & b_{k-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & b_{k-1} & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & b_{k-1} & \cdots & b_0 & 0 \\ 0 & \cdots & \cdots & 0 & 1 & b_{k-1} & \cdots & b_0 \end{pmatrix}$$

autrement dit H est une matrice de contrôle de C. Une autre façon équivalente de vérifier qu'un polynôme $m(X) \in C$ est de vérifier que $m(X)h(X)$ est divisible par X^n-1 ou encore si et seulement si $m(\alpha^i) = 0$ pour tout $i \in I$.

5.4. Codes BCH. — Les codes BCH (Bose-Chaudhuri-Hocquenghem) sont des codes cycliques particuliers qui contiennent les fameux codes de Redd-Solomon servant dans la lecture des CD. Pour q et r donné on prend n un diviseur de q^r-1 de sorte que l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est un diviseur de r. On note alors $\zeta_n \in \mathbb{F}_{q^r}$ une racine primitive n-ème de l'unité et pour $\delta \geq 2$, on considère le morphisme d'anneau

$$\mathbb{F}_q[X]/(X^n-1) \longrightarrow \mathbb{F}_{q^r}^{\delta-1}$$

qui à P associe $\Big(P(\beta), P(\beta^2), \cdots, P(\beta^{\delta-1})\Big)$. Le noyau de ce morphisme est le code $BCH(q,n,\delta)$ dont le polynôme générateur est le ppcm des polynômes minimaux sur $\mathbb{F}_q$ des éléments $\beta, \beta^2, \cdots, \beta^{\delta-1}$.
Remarque : il y a plusieurs cas selon que q est premier ou pas, que $r=1$ ou $r>1$ et que n est un diviseur strict ou pas de q^r-1. On notera bien que le code ne dépend pas du choix de r. De manière équivalente, le code $BCH(q,n,\delta)$ est le code linéaire cyclique associé au plus petit sous-ensemble Σ de $\mathbb{Z}/n\mathbb{Z}$ contenant $1, 2, \cdots, \delta-1$ et stable par multiplication par q.

Proposition 5.15. — *Un polynôme $c = x_1X^{n-1} + \cdots + x_n$ appartient à ce code si et seulement si*

$$c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{\delta-1}) = 0$$

où α désigne une racine primitive n-ème de l'unité dans $\mathbb{F}_{q^r}$.

Remarque : pour $\delta = 2t+1$, on peut d'après ce qui précède corriger t erreurs, expliquons comment s'y prendre dans le cas $q=2$. Supposons que le mot reçu soit $u = c + \epsilon$ et que le nombre d'erreurs est $\mu \leq t$ de sorte que

$$\epsilon = X^{l_1} + \cdots + X^{l_\mu}$$

avec $0 \leq l_\mu < \cdots < l_1 \leq n-1$. Le calcul des $u(\alpha_i) = \epsilon(\alpha^i)$ pour $i = 1, \cdots, 2t$ permet de connaître les sommes de Newton S_k des $(\alpha^{l_i})_{1\leq i\leq \mu}$ et donc, cf. ci après, le polynôme localisateur d'erreur $\sigma(X) = \prod_{i=1}^{\mu}(1-\alpha^{l_i}X)$. On détermine alors les bits erronés en testant les i tels que $\sigma(\alpha^i) = 0$. Comme on est en caractéristique 2, on ne peut pas utiliser les relations de Newton habituelles ; une méthode consiste à utiliser la congruence suivante.

Proposition 5.16. — *Posons $S(X) = \sum_{i=1}^{2t} S_iX^{i-1}$; on a alors*

$$S(X)\sigma(X) \equiv \omega(X) \mod X^{2t}$$

où $\omega(X)$ est de degré $< t$.

Preuve : On a

$$S(X) = \sum_{i=1}^{2t}\sum_{j=1}^{\mu} \alpha^{il_j}X^{i-1} = \sum_{j=1}^{\mu} \alpha^{l_j}\frac{1-\alpha^{2tl_j}X^{2t}}{1-\alpha^{l_j}X}$$

ce qui donne le résultat en prenant $\omega(X) = \sigma(X)\sum_{j=1}^{\mu}\frac{\alpha^{l_j}}{1-\alpha^{l_j}X}$. □

Lemme 5.17. — *Soient σ' et ω' des polynômes de $\mathbb{F}_{q^m}[X]$ avec $\deg\sigma' \leq t$ et $\deg w' < t$ et $S(X)\sigma'(X) \equiv \omega'(X) \mod X^{2t}$. Il existe alors $c(X) \in \mathbb{F}_{q^m}[X]$ tel que $\sigma' = c\sigma$ et $\omega' = c\omega$.*

Preuve : Modulo X^{2t}, on a

$$\omega\sigma' \equiv S\sigma\sigma' \equiv \omega'\sigma$$

de sorte que $\omega\sigma' - \omega'\sigma$ est divisible par X^{2t} et donc nul car de degré $< 2t$. Le résultat découle alors du lemme de Gauss en remarquant que σ et ω sont premiers entre eux car n'ayant pas de racines communes. □

On exécute ensuite l'algorithme d'Euclide étendu à partir de $P_0(X) = X^{2t}$ et $P_1 = S$ ce qui donne des suites (P_i), (A_i) et (B_i) avec $\deg P_i < \deg P_{i+1}$ et $p_i = A_i Z^{2t} + B_i S$ et donc $SB_i \equiv P_i \mod X^{2t}$. Il existe en outre un unique i tel que $\deg P_{i-1} \geq t$ et $\deg P_i < t$ de sorte que comme $\deg B_i = \deg P_0 - \deg P_{i-1} \leq 2t - t = t$, en posant $\sigma' = B_i$ et $\omega' = P_i$, on est dans les conditions du lemme précédent. Il existe donc $c(X) \in \mathbb{F}_{2^m}[X]$ tel que

$$B_i = C\sigma, \qquad P_i = C\omega$$

avec $\omega - S\sigma = AX^{2t}$ et donc $A_i = CA$. Or comme A_i et B_i sont premiers entre eux, le polynôme C est constant égal à $P_i(0)$ ce qui permet de calculer σ.
Remarque : dans le cas q quelconque, on obtient de la même façon le polynôme σ ; pour déterminer les coefficients il suffit ensuite de résoudre un système de Vandermonde.

5.18 — **Codes de Hamming** : on prend $n = \frac{q^r-1}{q-1}$ de sorte que q est d'ordre r dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et on prend $I := \{1, q, q^2, \cdots, q^{r-1}\}$. Montrons que $d \geq 3$: en effet s'il existe $a, b \in \mathbb{F}_q$ tel que $aX^i + bX^j$ appartient au code alors $a\beta^{q^s i} + b\beta^{q^s j} = 0$ de sorte que $a + b\beta^{q^s(j-i)} = 0$ et comme β est d'ordre n on voit que $a = b = 0$. Par ailleurs une matrice de contrôle $H \in \mathbb{M}_{r,n}(\mathbb{F}_q)$ est telle que ses colonnes forment n vecteurs de $\mathbb{F}_q^r$ qui sont donc 2 à 2 indépendantes ; comme $n = (q^r - 1)/(q - 1)$ on obtient exactement un vecteur dans chaque droite de $\mathbb{F}_q^r$. Ainsi pour e_1 et e_2 deux colonnes distinctes le vecteur $e_1 + e_2$ est nécessairement colinéaire à un des vecteurs colonnes de H et donc $d \leq 3$.
Remarque : les codes de Hamming sont 1-correcteur parfait qui ne sont MDS que pour $r = 2$. Soit $P(X) \in \mathbb{F}_q[X]$ est un polynôme irréductible de degré r qui est primitif, i.e. telle que la classe α de X dans $\mathbb{F}_q[X]/(P(X))$ engendre le groupe multiplicatif, autrement dit si $P(X)$ est un diviseur irréductible de $\Phi_n(X)$. A $(m_r, \cdots, m_{n-1})$ on associe $(m_0, \cdots, m_{r-1})$ tel que

$$m_0 + m_1\alpha + \cdots + m_{r-1}\alpha^{r-1} = -\sum_{k=r}^{n-1} m_k \alpha^k$$

et on transmet le mot de code $M = (m_0, \cdots, m_{n-1})$. On reçoit $M' = (m'_0, \cdots, m'_{n-1})$ dont la distance de Hamming à M est ≤ 1. Le mot $M' \in C$ si et seulement si $\sum_{k=0}^{n-1} m'_k \alpha^k = 0$ et sinon on retrouve $M = M' - (0, \cdots, 0, \lambda, 0, \cdots, 0)$ où λ est en i-ème position tel que $\lambda\alpha^i = \sum_{k=0}^{n-1} m'_k \alpha^k$.
Exemples le code du minitel, cf. l'exercice 5.3.

5.19 — **Codes de Reed-Solomon** : on prend $q = 2^m$ et $n = q-1$. Soit alors α un générateur de $\mathbb{F}_q^\times$. Pour k fixé on pose

$$g(X) := \prod_{i=1}^{q-1-k} (X - \alpha^i)$$

de sorte que g est le générateur d'un code cyclique sur $\mathbb{F}_q$ de longueur $q - 1$ et de dimension k. Sa distance minimale est $\geq q - k$ d'après la proposition 5.14 et $\leq q - k$ d'après la borne du singleton. Ses paramètres sont donc $(q - 1, k, q - k)$.
Exemples le code pour les CD, cf. l'exercice 5.4.

5.20 — Citons quelques cas où l'on considère pour n un diviseur strict de $q^r - 1$:

- **Code ternaire de Golay** : on a $3^5 - 1 = 11.23$; on choisit $q = 3$, $n = 11$ et la partie de$(\mathbb{Z}/11\mathbb{Z})^\times$ engendrée par 3, i.e. $i = \{1, 3, 4, 5, 9\}$. On note $\mathcal{G}_{11}$ le code linéaire cyclique correspondant. Montrer que $d(\mathcal{G}_{11}) = 4, 5$ puis que $\mathcal{G}_{11}$ est 2-correcteur parfait (il n'est pas MDS).
- **Code binaire de Golay** : on a $2^{11} - 1 = 23.89$, on choisit $q = 2$, $n = 23$ et $I = (2) \subset (\mathbb{Z}/23\mathbb{Z})^\times$.On note $\mathcal{G}_{23}$ le code linéaire cyclique correspondant. Montrer que $d(\mathcal{G}_{23}) = 5, 6, 7$ puis que $\mathcal{G}_{23}$ est "-correcteur parfait.

5.5. Exercices. —

Exercice 5.1. — *On code un nombre à* 10 *chiffres* $a_1, \cdots, a_{10}$ *en ajoutant deux clés :*
- *la première est le reste* a_{11} *modulo* 11 *de la somme des dix chiffres ;*
- *la seconde est le reste* a_{12} *modulo* 11 *de* $\sum_{k=1}^{10} k a_k$.

Montrez que ce code permet de détecter et de corriger une erreur.

Exercice 5.2. — *Donnez la distance et des matrices génératrices et vérificatrices des codes suivants :*

(i) ***Code raccourci*** *: soit* $d(\mathcal{C}) \leq l \leq n$, *on pose* $\mathcal{C}^{(l)} := \{x \in \mathbb{F}_q^l \ / \ (x; 0, \cdots, 0) \in \mathcal{C}\}$.

(ii) ***Code étendu*** $: \bar{\mathcal{C}} := \{(x_1, \cdots, x_{n+1}) \in \mathbb{F}_q^{n+1} \ / \ (x_1, \cdots, x_n) \in \mathcal{C}$ *et* $x_1 + \cdots + x_{n+1} = 0\}$.

(iii) ***Code dual*** $: \mathcal{C}^* := \{x' \in \mathbb{F}_q^n \ / \ \forall x \in \mathcal{C}, \ < x, x' >= 0\}$ *où* $<,>$ *est le produit scalaire canonique.*

Exercice 5.3. — ***Code du minitel***

(a) Montrez que le polynôme $P(X) = X^7 + X^3 + 1$ *est irréductible sur* $\mathbb{F}_2$ *et en déduire que* $\mathbb{F}_{128} \simeq \mathbb{F}_2[X]/(X^7 + X^3 + 1)$ *et montrez que* X *est un générateur du groupe multiplicatif.*

(b) Pour envoyer un message de 15 *octets (soit 120 bits) de la forme* $M = a_0 a_1 \cdots a_{119}$ *où les* a_i *sont des éléments de* $\mathbb{F}_2$ *(des bits), on considère l'élément suivant de* $\mathbb{F}_{128}$

$$\beta = a_0\alpha^{126} + \cdots + a_{119}\alpha^7 = a_{120}\alpha^6 + \cdots + a_{125}\alpha + a_{126}$$

On envoie alors le message $a_0 a_1 \cdots a_{126} a_{127}$ *où* a_{127} *est un bit de parité, soit* 16 *octets. Le message reçu est* $a'_0 \cdots a'_{127}$ *où certains* a'_i *sont distincts de* a_i *à cause d'une erreur de transmission. On suppose toutefois que les erreurs de transmission sont suffisamment rares pour qu'au plus une erreur se soit produite, par exemple au bit* k, *i.e.* $a_i = a'_i$ *pour* $i \neq k$ *et* $a'_k = a_k + 1$. *Expliquez comment décoder le message et commentez le choix de* 128.

Exercice 5.4. — ***Les disques compacts***

(a) Montrez que $P(X) = X^8 + X^7 + X^6 + X^5 + X^4 + X^2 + 1$ *est irréductible sur* $\mathbb{F}_2$ *et en déduire que* $\mathbb{F}_{256} \simeq \mathbb{F}_2[X]/(P(X))$. *Montrez que* α, *l'image de* X, *est un générateur du groupe multiplicatif.*

(b) On représente un octet par un élément de $\mathbb{F}_{256}$. *Considérons un mot* $M = a_0 \cdots a_{250}$ *constitué de* 251 *octets, i.e.* $a_i \in \mathbb{F}_{256}$. *On considère*

$$(\sum_{i=0}^{250} a_i X^i)(X + \alpha)(X + \alpha^2)(X + \alpha^3)(X + \alpha^4) = \sum_{i=0}^{254} b_i X^i$$

et on transmet le message $M = b_0 \cdots b_{255} b_{256}$ *où* b_{256} *est un bit de parité.*

(i) Supposons que deux erreurs au plus se produisent dans la lecture de M. *Comment savoir s'il y a eu zéro, une ou deux erreurs et expliquez comment les corriger.*

(ii) On suppose désormais que quatre octets quelconques de M sont illisibles. Expliquez comment retrouver les bonnes valeurs.

(iii) Dans un CD, on code les informations musicales par paquets de 24 octets auxquels on adjoint 4 octets comme précédemment afin de pouvoir corriger deux erreurs ou 4 effacements. On obtient ainsi des mots de 28 octets, dont le $i$ème mot est noté M_i de k-ème octet est $M_i(k)$. Les mots sont alors entrelacés comme suit : chaque sillon est constitué de 28 octets, le i-ème sillon contient alors les octets suivants

$$M_i(1)\ M_{i-4}(2)\ M_{i-8}(3)\cdots M_{i-108}(28)$$

ou de manière équivalente M_i est constitué de $S_i(1)S_{i+4}(2)\cdots S_{i+108}(28)$. Chaque sillon de 28 octets est complété de 4 octets comme précédemment. Expliquez comment nos lecteurs de CD se jouent des rayures (de 2mm de large).

6. Correction des exercices

6.1. du chapitre 1. —

1.2 Raisonnons par l'absurde et supposons qu'il existe $\sqrt{n/3} \leq l \leq n-2$ tel que l^2+l+n ne soit pas premier ; on prend l minimal. Soit alors q le plus petit diviseur premier de l^2+l+n ; on a $q \leq 2l$ car sinon on aurait $(2l+1)^2 \leq q^2 \leq l^2+l+n$ et donc $l \leq \sqrt{n/3}$. On écrit alors q sous la forme $l-k$ ou $l+k+1$ avec $0 \leq k \leq l-1$; de la factorisation

$$(l^2+l+n)-(k^2+k+n) = (l-k)(l+k+1)$$

on en déduit que q divise k^2+k+n lequel par minimalité de l est premier soit $q = k^2+k+n$. La relation $q^2 \leq l^2+l+n$ implique

$$(k^2+k+n)^2 \leq (n-2)^2+(n-2)+n < n^2$$

ce qui est absurde.

1.3 Il s'agit de vérifier que pour tout $x, y \in \mathcal{E}$, le nombre $\frac{x+y}{2}$ n'appartient pas à $\mathcal{E}$. Dans le cas contraire $x+y$ ne s'écrirait qu'avec des 0 et des 2 en base trois ce qui n'est le cas que si $x = y$, d'où le résultat.

Comme $2^11 = 2048$ et que $\sum_{i=0}^{10} 3^i = 88573$, l'exercice suggéré par la remarque aura une réponse positive jusqu'en 2048.

1.4

1.5 On rappelle que les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$; l'inclusion $48\mathbb{Z} \subset n\mathbb{Z}$ impose que n divise 48 soit $n = 1, 2, 3, 4, 6, 8, 12, 16, 18, 24, 48$ avec les inclusions

$$\begin{array}{ccccccccc} (16) & \subset & (8) & \subset & (4) & \subset & (2) & \subset & (1) = \mathbb{Z} \\ \cup & & \cup & & \cup & & \cup & & \cup \\ (48) & \subset & (24) & \subset & (12) & \subset & (6) & \subset & (3) \end{array}$$

1.6 (i) Cela découle de l'observation que les deux derniers chiffres de tout multiple de 20, sont pairs.

(ii) Notons $A = \bar{a} = \overline{a_k \cdots a_0} = \sum_{i=0}^{k} a_i 10^i$ un multiple alterné de n avec a_k impair. Si a_1 est impair, on se ramène à a_1 pair en considérant $\overline{a_k \cdots a_0 0}$. Pour tout $r \geq 1$, le nombre

$$\overline{a \cdots a} = (10^k)^r A + (10^k)^{r-1} A + \cdots + 10^k A + A = A\frac{(10^k)^{r+1}-1}{10^k-1}$$

est alterné ; il suffit alors de prendre r tel que m divise $\frac{(10^k)^{r+1}-1}{10^k-1}$ ce qui est le cas pour $r+1=\psi(m(10^n-1))$ car 10^k étant premier avec $m(10^k-1)$, d'après le théorème d'Euler, on a $(10^k)^{r+1}\equiv 1 \mod m(10^k-1)$.

(iii) On raisonne par récurrence sur n ; le cas $n=1$ étant trivial, supposons le résulta acquis jusqu'au rang n et traitons le cas $n+1$. Soit $A=\overline{a_{n-1}\cdots a_0}=\lambda 5^n$ alors 5^{n+1} divise $A'=\overline{a_n\cdots a_0}$ si et seulement si $5|a_n 2^n+\lambda$, i.e. $a_n\equiv -\lambda 3^n \mod 5$. Or il existe nécessairement deux éléments a_n vérifiant cette congruence dans $[0,9]$ et ils sont de parité différente ce qui permet de choisir a_n tel que A' soit alterné.

(iv) On raisonne comme dans (iii) : $A=\overline{a_{n-1}\cdots a_0}=\lambda 2^n$ avec $\lambda\equiv n \mod 2$. Alors 2^{n+1} divise $A'=\overline{a_n\cdots a_0}$ si et seulement si $2|a_n 5^n+\lambda$, i.e. $a_n\equiv\lambda \mod 2$. En outre $\overline{a_n\cdots a_0}/2^{n+1}=(a_n 5^n+\lambda)/2\equiv n+1 \mod 2$ si et seulement si $a_n+\lambda\equiv 2(n+1) \mod 4$. Il existe une solution a_n aux deux équations précédentes : si a_n vérifie la première alors a_n ou a_n+2 vérifie la deuxième. Le nombre A' est bien alterné puisque $a_n\equiv\lambda \mod 2$ et donc par hypothèse de récurrence de même parité que n donc distincte de celle de a_{n-1}.

(v) Posons $n=2^s 5^t m$ avec $m\wedge 10=1$:
- si $s=t=0$ d'après (ii), n possède un multiple alterné ;
- si $s=0$ ou 1, d'après (iii) 5^t admet un multiple alterné de dernier chiffre impair, supposé, quitte à lui rajouter 10^t, de premier chiffre impair. D'après (ii), $5^t m$ admet un multiple alterné $\overline{a}$ de dernier chiffre impair par construction de sorte que $\overline{a0}$ est un multiple alterné de n ;
- si $t=0$ d'après (iv) 2^s admet un multiple alterné de dernier chiffre pair et, quitte à lui ajouter 10^s, de premier chiffre impair. D'après (ii), $n=2^s m$ admet un multiple alterné ;
- dans les autres cas on a $t\geq 1$ et $s\geq 2$ et donc $20|n$ et d'après (i), n'admet pas de multiple alterné.

1.7 Pour tout $k>0$, l'ensemble $[1,n]$ contient $\lfloor n/p^k\rfloor$ multiples de p^k de sorte qu'il y a exactement $\lfloor n/p^k\rfloor-\lfloor n/p^{k+1}\rfloor$ éléments i tels que $v_p(i)=k$ ce qui donne le résultat.

En ce qui concerne la valuation 2-adique de $\binom{b}{a+b}$ elle découle directement de la formule de Legendre en remarquant que

$$\lfloor\frac{a+b}{2^k}\rfloor-\lfloor\frac{a}{2^k}\rfloor-\lfloor\frac{b}{2^k}\rfloor$$

est non nulle si et seulement si $a_k=b_k=1$.

1.8 On raisonne par l'absurde ; on prend (a,b) tel que $\max\{a,b\}$ soit minimal avec $\frac{a^2+b^2}{ab+1}=k$ qui n'est pas un carré parfait. Remarquons déjà que si $a=b$ alors $a=b=k=1$ ne convient pas. Supposons donc $0<a<b$ et écrivons l'égalité précédente sous la forme

$$b^2-(ka)b+a^2-k=0$$

de sorte que b est une racine du polynôme $X^2-(ka)X+a^2-k$, lequel possède une deuxième racine b' telle que $b+b'=ka$ et donc $b'\in\mathbb{Z}$. Par ailleurs on a :
- $bb'=a^2-k$ et donc $b'=(a^2-k)/b<a$;
- $b'>0$: en effet si $b'<0$ alors $k=(a^2+(b')^2)/(ab'+1)<0$ ce qui n'est pas et si $b'=0$ alors $k=a^2$ ce qui n'est pas non plus.

En résumé le couple (a,b') avec $0<b'<a$ est plus petit que (a,b) vérifie les mêmes hypothèses ce qui contredit la minimalité de (a,b).

1.9 (i) On raisonne par récurrence sur $k=v_3(n)$; pour $k=0$ comme 3 ne divise pas n et qu'il est impair, on a $n\equiv\pm 1 \mod 6$ et comme $2^6\equiv 1 \mod 9$, on a $2^n+1\equiv 3,6 \mod 9$ d'où la

propriété au rang $k = 0$. Supposons alors le résultat acquis jusqu'au rang k et montrons la au rang $k+1$: on écrit $n = 3^{k+1}m$ avec$3 \wedge m = 1$ et m impair. Pour $x = 2^{3^k m}$, on a

$$2^n + 1 = x^3 + 1 = (x+1)(x^2 - x + 1)$$

de sorte que $v_3(2^n+1) = v_3(x+1) + v_3(x^2-x+1) = k + v_3(x^2-x+1)$. Or $2^3 \equiv -1 \mod 9$ et donc $x \equiv -1 \mod 9$ et $x^2 - x + 1 \equiv 3 \mod 9$ d'où le résultat.

(ii) D'après (i) si $n^2 | 2^n + 1$ alors n est impair et d'après (i), on a $2v_3(n) \leq v_3(2^n+1) = v_3(n) + 1$ et donc $v_3(n) = 0, 1$ ce qui donne $n = 1$ ou 3.

On raisonne par l'absurde et supposons que n n'est pas une puissance de 3 : notons $p \neq 3$ le plus petit facteur premier de n. Comme n est nécessairement impair, $p \geq 5$. On note alors δ l'ordre de 2 dans $\mathbb{Z}/p\mathbb{Z}$ qui comme $2^n \equiv -1 \mod p$ est un diviseur pair de $2n$ et de $p-1$ d'après le petit théorème de Fermat. Ecrivons alors $p = 2k$ avec $k|n$ et $k < p$. Par minimalité de p, k est une puissance de 3 et donc $k = 1$ ou 3. Dans le premier cas on obtient $2^2 \equiv 1 \mod p$ soit $p = 3$ et dans le second $2^6 \equiv 1 \mod p$ et donc $p = 3$ ou 7 soit $p = 7$; or l'ordre de 2 dans $\mathbb{Z}.7\mathbb{Z}$ est 3 et non 6 d'où la contradiction.

1.10 A tout élément n de $\mathcal{E}$, on associe bijectivement un vecteur $(n_1, \cdots, n_9) \in \mathbb{Z}^9$ tel que $n = 2^{n_1}3^{n_2}\cdots 23^{n_9}$; il s'agit alors de démontrer que l'on peut trouver 4 vecteurs de $\mathbb{Z}^9$ dont la somme appartient à $4\mathbb{Z}^9$. Remarquons déjà que d'après le principe des tiroirs, étant donnés 2^9+1 vecteurs de $\mathbb{Z}^9$, il en existe 2 dont la somme est dans $2\mathbb{Z}^9$. L'idée est alors la suivante : construire des a_k, b_k deux à deux distincts pour $1 \leq k \leq 2^9+1$ tels que $s_k = a_k + b_k \in 2\mathbb{Z}^9$ de sorte que l'on pourra trouver $i \neq j$ avec $(s_i/2)$ et $(s_j/2)$ de somme appartenant à $\mathbb{Z}^9$. Pour cela il suffit d'avoir au départ $(2^9+1)+2.2^9 = 1537 < 2008$ éléments distincts : on commence par prendre $a_1 + b_1 \in 2\mathbb{Z}^9$, puis ainsi de suite. S'il existe $i \neq j$ tels que $s_i = s_j$ c'est gagné, sinon on réapplique ce qui précède à l'ensemble de 2^9+1 éléments distincts constitués des $s_i/2$.

1.11 On décompose a et b en facteurs premiers

$$a = \epsilon(a) \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \qquad b = \epsilon(b) \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$$

où $\mathcal{P}$ est un système de représentant de l'ensemble des nombres premiers. Si on a la bonne idée de choisir chaque représentant dans $\mathbb{N}$, les signes $\epsilon(a)$ et $\epsilon(b)$ sont alors égaux à 1. Les familles d'entiers $(\nu_p(a))_{p\in\mathcal{P}}$ et $(\nu_p(b))_{p\in\mathcal{P}}$ sont presque nulles, i.e. l'ensemble des $p \in \mathcal{P}$ tels que $\nu_p(a)$ ou $\nu_p(b)$ est non nul, est fini. Soit alors $u \in \mathbb{N}$ tel que $ab = u^k$. On écrit de même $u = \epsilon(u)\prod_{p\in\mathcal{P}} p^{\nu_p(u)}$ avec pour tout $p \in \mathcal{P}$

$$\nu_p(a) + \nu_p(b) = k\nu_p(u)$$

L'hypothèse a et b premier entre eux signifie que pour tout $p \in \mathcal{P}$, $\nu_p(a)$ et $\nu_p(b)$ ne sont pas tous deux non nuls. On en déduit donc que pour tout $p \in \mathcal{P}$, $\nu_p(a)$ et $\nu_p(b)$ sont divisibles par k : $\nu_p(a) = k\alpha_p$ et $\nu_p(b) = k\beta_p$ avec à nouveau α_p et β_p non tous deux non nuls. En posant $\alpha = \prod_{p\in\mathcal{P}} p^{\alpha_p}$ et $\beta = \prod_{p\in\mathcal{P}} p^{\beta_p}$, on en déduit $a = \alpha^k$ et $b = \beta^k$.

1.12 Le but est de faire des combinaisons pour faire descendre le degré ; concrètement appelons $\delta(n)$ ce pgcd. On a $n^3 + n^2 + 1 = (n^2 + 2n - 1)(n-1) - (n+1)$ de sorte que $\delta(n) = (n^2+2n-1, n+1)$. De même $n^2+2n-1 = (n+1)^2 - 2$ et donc $\delta(n) = (n+1, 2)$ soit $\delta(n) = 2$ si $n \equiv 1 \mod 2$ et $\delta(n) = 1$ si $n \equiv 0 \mod 2$.

1.13 On procède comme dans l'exercice précédent au détail près que l'on ne divise plus par un polynôme unitaire ; appelons $\delta(n)$ le pgcd cherché et $\delta_1(n) = (2n^3+2n^2-12n+4, 2n^2+5n-3)$;

de manière générale on a $\delta_1(n) = \delta(n)$ si la multiplicité de 2 [5] dans $n^3 + n^2 - 6n + 2$ est supérieure ou égale à celle dans $2n^2 + 5n - 3$, sinon $\delta_1(n) = 2\delta(n)$: en particulier si $n \equiv 0 \mod 2$ alors $2n^2 + 5n - 3$ est impair et donc $\delta(n) = \delta_1(n)$. De l'égalité $2n^3 + 2n^2 - 12n + 4 = n(2n^2 + 5n - 1) - (3n^2 + 9n - 4)$ on en déduit $\delta_1(n) = (2n^2 + 5n - 3, 3n^2 + 9n - 4) = (2n^2 + 5n - 3, n^2 + 4n - 1) = (n^2 + 4n - 1, 3n + 1)$ par simples soustractions. On introduit à nouveau $\delta_2(n) = (3n^2 + 12n - 3, 3n + 1)$ et comme $3n + 1$ n'est pas divisible par 3, on a $\delta_1(n) = \delta_2(n)$ et de l'égalité $3n^2 + 12n - 3 = (3n + 1)(n + 3) + 2n - 6$, on en déduit $\delta_2(n) = (2n - 6, 3n + 1)$. On introduit $\delta_3(n) = (n - 3, 3n + 1)$ avec $\delta_3(n) = \delta_2(n)$ si la multiplicité de 2 dans $n-3$ est supérieure ou égale à celle dans $3n+1$ et sinon $\delta_2(n) = 2\delta_3(n)$. On a $\delta_3(n) = (n - 3, 10)$ de sorte que

$$\delta_3(n) = \begin{cases} 10 \text{ si } n \equiv 3 \mod 10 \\ 5 \text{ si } n \equiv 3 \mod 5 \text{ et } n \equiv 0 \mod 2 \\ 2 \text{ si } n \equiv 1 \mod 2 \text{ et } n \not\equiv 3 \mod 5 \\ 1 \text{ si } n \equiv 0 \mod 2 \text{ et } n \not\equiv 3 \mod 5 \end{cases}$$

On traite alors les cas un par un :

(a) Si $\delta_3(n) = 1$ ou 5 soit $n \equiv 0 \mod 2$, soit $3n + 1 \equiv 1 \mod 2$ et donc $\delta_3(n) = \delta_2(n) = \delta_1(n)$; on a de même $2n^2 + 5n - 3 \equiv 1 \mod 2$ soit $\delta(n) = \delta_1(n)$;

(b) si $\delta_3(n) = 2$ ou 10 soit $n \equiv 1 \mod 2$ et $n \not\equiv 3 \mod 5$, alors si $n \equiv 3 \mod 4$ on a $3n + 1 \equiv 2 \mod 4$ et $\delta_2(n) = \delta_3(n) = \delta_1(n)$; en outre $2n^2 + 5n - 3 \equiv 2 \mod 4$ et $n^3 + n^2 - 6n + 2 \equiv 0 \mod 4$ et donc $\delta(n) = \delta_1(n)$. Si on a $n \equiv 1 \mod 4$ alors de même $3n+1 \equiv 0 \mod 4$ et $n-3 \equiv 2 \mod 4$ soit $\delta_1(n) = \delta_2(n) = 2\delta_3(n)$; $2n^2+5n-3 \equiv 0 \mod 4$ et $n^3 + n^2 - 6n + 2 \equiv 2 \mod 4$ de sorte que $\delta_1(n) = 2\delta(n)$;

Ainsi on a toujours $\delta(n) = \delta_3(n)$.

1.14 On factorise $(y - 2)(y + 2) = x^3$; notons $d = (y - 2) \wedge (y + 2)$ qui est aussi égal à $(y - 2) \wedge 4$ et donc égal à $1, 2, 4$. Si $d = 1$ alors d'après l'exercice 1.11 appliqué au cas des cubes, on obtient que $y \pm 2 = t_\pm^3$ avec $t_+ \wedge t_- = 1$ et $x = t_+t_-$. On obtient alors $4 = t_+^3 - t_-^3 = (t_+ - t_-)(t_+^2 + t_+t_- + t_-^2)$

Si $d = 2$ alors $(y - 2)(y + 2)$ est divisible par 4 mais par pas 8 ; ainsi x est pair et x^3 est divisible par 8 ce qui donne une contradiction à l'égalité $y^2 - 4 = x^3$. Si $d = 4$ alors $y - 2 = 4k$ et $y + 2 = 4(k + 1)$ ce qui donne $x^3 = 16k(k + 1)$. Ainsi x est pair $x = 4t$ avec $4t^3 = k(k + 1)$

1.15 Soit $2 \leq m \leq n$ tel que $m \wedge n = 1$; prendre par exemple $m = n - 1$. On a alors

- $m|(mn-n) \vee \cdots \vee (mn-1)$ car l'un de ces entiers consécutifs est nécessairement divisible par $m \leq n$;
- $n|(mn - n) \vee \cdots \vee (mn - 1)$ car $n|mn - n$.

Ainsi comme $m \wedge n = 1$, d'après le lemme de Gauss, on en déduit que mn divise $(mn - n) \vee \cdots \vee (mn - 1)$ d'où le résultat.

1.16 Une façon agréable de faire des calculs est d'écrire matriciellement

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Le résultat découle alors directement de la multiplication de cette égalité pour n et m. On en déduit alors que $F_{n+m} \wedge F_m = F_nF_{m-1} \wedge F_m = F_n \wedge F_m$ car par une récurrence immédiate $F_m \wedge F_{m-1} = 1$. En appliquant l'algorithme d'Euclide (soustractif, i.e. on ne fait pas de division euclidienne mais on soustrait simplement), on obtient le résultat.

5. i.e. le plus grand entier r tel que 2^r divise le nombre en question

1.17 (a) On remarque tout d'abord que $650 = 2.325$ et $66 = 2.33$. On va appliquer l'algorithme d'Euclide à 325 et 33 puis on multipliera par deux, ce qui nous permet de gagner quelques lignes de calculs (on n'est pas un ordinateur...)

$$\begin{aligned} 325 &= 33.9 + 28 \\ 33 &= 28 + 5 \\ 28 &= 5.5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

On remonte alors les calculs :

$$\begin{aligned} 1 &= 3 - 2 \\ 1 &= 3 - (5 - 3) = 2.3 - 5 \\ 1 &= 2.(28 - 5.5) - 5 = 2.28 - 11.5 \\ 1 &= 2.28 - 11.(33 - 28) = 13.28 - 11.33 \\ 1 &= 13.(325 - 9.33) - 11.33 = 13.325 - 128.33 \end{aligned}$$

Finalement la relation de Bezout est $2 = 13.650 - 128.66$, c'est la plus "simple" ; on rappelle que les autres sont données par

$$2 = (13 + k.66)650 - (128 - k.650)66$$

pour $k \in \mathbb{Z}$.

(b) (i) D'après la relation de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $1 = ua + vb$, i.e. si on nous rend la monnaie (u ou v est forcément négatif), pouvant payer la somme 1, on peut payer n'importe quelle somme entière.

(ii) On écrit $m = ax + by$ et $n = au + bv$ de la façon la plus simple possible, i.e. $0 \leq x, u \leq b - 1$, de sorte que l'écriture est unique ; en effet on rappelle que $m = a(x - bt) + b(y + at)$, de sorte qu'il existe un unique t tel que $0 \leq x - bt < b$. L'égalité $m + n = ab - a - b$ donne alors $ab = a(x + u + 1) + b(v + y + 1)$: a et b étant premier entre eux, "le" théorème de Gauss nous dit que b divise $x + u + 1$. Or on a $1 \leq x + u + 1 \leq 2b - 1$, le seul multiple de b dans cet intervalle est b lui-même, soit $x + u + 1 = b$ et donc $v + y + 1 = 0$. Les nombres y et v étant des entiers, exactement un parmi eux deux est positif ou nul, l'autre étant strictement négatif. En language clair exactement une somme parmi m et n est payable sans rendu de monnaie. En remarquant que 0 est payable, alors $ab - a - b$ n'est pas payable. De même une somme négative n'est pas payable de sorte que si $m > ab - a - b$, la somme m est payable.

(c) On écrit $48x + 20y + 15z = 3(16x + 5z) + 20y$. D'après ce qui précède tout nombre de la forme $60 + t$ avec $t \geq 0$ peut s'écrire sous la forme $16x + 5Z$. De même tout nombre de la forme $38 + s$ avec $s \geq 0$, peut s'écrire sous la forme $3t + 20y$. Finalement toute somme supérieure ou égale à 218 est payable. Étudions le cas de 217 : $217 = 20y + 3u$, $217 \equiv -3 \mod 20$, on en déduit que $-3(u + 1)$ doit être divisible par 20, soit $u = 20k - 1$ et $220 = 20(y + 3k)$ soit $11 = y + 3k$ ce qui donne $u = 19, 39, 59$ et on vérifie aisément qu'aucune de ses possibilités ne s'écrit sous la forme $16x + 5z$ avec x, y positifs.

(d) Soit $n > 2abc - bc - ac - ab$. D'après le théorème de Bezout, il existe $0 \leq x < a$ avec $n \equiv x \mod xbc \mod a$; soit $y' \in \mathbb{Z}$ tel que $n = xbc + y'a$ de sorte que

$$y'a = n - xbc > 2abc - bc - ac - ab - (a - 1)bc = (bc - b - c)a$$

et donc $y' > bc - b - c$. D'après (b), il existe $y, z \geq 0$ tel que $y' = zb + yc$ et donc $n = xbc + yac + zab$.

Supposons par l'absurde que $2abc - bc - ac - ab = xbc + yac + zab$ avec $x, y, z \geq 0$; on aurait alors $a|(x+1)bc$ et donc $a|x+1$ d'après le lemme de Gauss, soit $x \geq a - 1$. De même on aurait $y \geq b - 1$ et $z \geq c - 1$ si bien que

$$xbc + yac + zbc \geq 3abc - bc - ac - ab > 2abc - bc - ac - ab$$

ce qui n'est pas.

(e) D'après ce qui précède la propriété est vraie pour $n = 2, 3$; on la suppose vraie jusqu'au rang $n-1$ et prouvons la au rang n. Soit $k > M = a_1 \cdots a_n\Big(n - 1 - \sum_{i=1}^n \frac{1}{a_i}\Big)$; comme a_n est premier avec $a_1 \cdots a_{n-1}$, d'après le théorème de Bezout, il existe $0 \leq x_n < a_n$ tel que $k \equiv x_n a_1 \cdots a_{n-1} \mod a_n$; notons $q_n = (k - x_n a_1 \cdots a_{n-1})/a_n$ de sorte que

$$N > \frac{a_1 \cdots a_n\Big(n - 1 - \sum_{i=1}^n \frac{1}{a_i}\Big) - (a_n - 1)a_1 \cdots a_{n-1}}{a_n} = a_1 \cdots a_{n-1}\Big(n - 2 - \sum_{i=1}^{n-1} \frac{1}{a_i}\Big).$$

D'après l'hypothèse de récurrence $N = \sum_{i=1}^{n-1} \prod_{j \neq i} a_j$ avec $x_i \geq 0$ pour tout $i = 1, \cdots, n-1$ et donc $k = \sum_{i=1}^n x_i \prod_{j \neq i} a_j$.

Supposons désormais que $M = \sum_{i=1}^n x_i \prod_{j \neq i} a_j$ avec $x_i \geq 0$ pour tout $i = 1, \cdots, n$. Alors comme dans (d), le lemme de Gauss donne que $a_i|(x_i + 1)$ et donc $x_i \geq a_i - 1$ et finalement que

$$M \geq \sum_{i=1}^n (a_i - 1) \prod_{j \neq i} a_j > a_1 \cdots a_n\Big(n - 1 \sum_{i=1}^n \frac{1}{a_i}\Big) = M$$

d'où la contradiction.

1.18 Comme $4 \equiv -3 \mod 7$ et que 105 est impair, on a $4^{105} \equiv -3^{105}$ d'où le résultat.

1.19 Le sens $\Rightarrow$ est évident ; en ce qui concerne l'autre sens, il suffit de faire un petit tableau des sommes $a^2 + b^2$ avec $a, b \in \mathbb{Z}/3\mathbb{Z}$ pour s'apercevoir que $a^2 + b^2 \equiv 0 \mod 3 \Rightarrow a, b \equiv 0 \mod 3$.

1.20 L'entier n est congru au mois M de naissance modulo 13 ce qui le détermine parfaitement ; il suffit alors de calculer le jour directement à partir de $n - 14M$.

1.21 On a $n \equiv A \mod 9$; il reste alors à déterminer A exactement ce qui est aisé puisque $k < 9$ de sorte que l'ordre de grandeur de n fixe A.

1.22 Notons pour tout entier e, A_e (resp. B_e) l'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z})^2$ d'ordre e (resp. d'ordre divisant e) et soit a_e (resp. b_e) son cardinal. Un élément (x, y) appartient à A_e si et seulement si x et y sont d'ordre divisant e dans $\mathbb{Z}/n\mathbb{Z}$, de sorte que pour tout e, $b_e = (e \wedge n)^2$. Par ailleurs B_d est la réunion disjointe de $A_d \coprod A_p \coprod A_q \coprod A_1$, où A_1 est réduit à l'élément nul. De même B_p (resp. B_q) est la réunion disjointe de $A_p \coprod A_1$ (resp. $A_q \coprod A_1$). En prenant les cardinaux, on obtient alors :

- $b_d = (n \wedge d)^2 = a_d + a_p + a_q + 1$,
- $b_p = (n \wedge p)^2 = a_p + 1$ et $b_q = (n \wedge q)^2 = a_q + 1$;

soit $a_d = (n \wedge (pq))^2 - (n \wedge p)^2 - (n \wedge q)^2 + 1$.

1.23 On rappelle que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont indexés par les diviseurs d de n ; concrètement l'application $d|n \mapsto (n/d)$ qui à un diviseur d de n associe le sous groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré

par n/d, est une bijection. Rappelons rapidement l'argument ; soit $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique et soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$; $\pi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ de la forme $d\mathbb{Z}$ qui contient $\operatorname{Ker}\pi = n\mathbb{Z}$ soit d divise n de sorte que π étant surjective H est engendré par l'image de d. En outre le sous-groupe engendré par un élément m est celui étiqueté par (n, m) ; en effet (m) est clairement inclu dans (m, n). L'inclusion réciproque se déduit de la relation de Bezout $un + vm = (n, m)$.

Pour $n = 24$, les sous-groupes sont ceux engendrés par $1, 2, 3, 4, 6, 8, 12, 0$ avec les relations d'inclusion

$$\begin{array}{ccccccc} (8) & \subset & (4) & \subset & (2) & \subset & (1) \\ \cup & & \cup & & \cup & & \cup \\ (0) & \subset & (12) & \subset & (6) & \subset & (3) \end{array}$$

On a en outre $(16) = (8)$ et $(18) = (6)$ de sorte que les sous-groupes contenant (8) et (6) sont (2) et (1) et qu'il n'y en a aucun contenant (8) inclus dans (6).

De manière générale les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ contenant (m_1) et inclus dans (m_2) sont les (d) avec (m_2, n) divisant d et d divisant (m_1, n).

1.24 On rappelle qu'un morphisme d'un groupe cyclique de cardinal n dans un groupe G est complètement déterminé par l'image g d'un générateur quelconque telle $g^n = 1_G$, soit g d'ordre divisant n. Dans le premier cas comme 3 et 4 sont premiers entre eux, les seuls éléments d'ordre divisant 3 dans $\mathbb{Z}/4\mathbb{Z}$ sont le seul d'ordre 1 à savoir 0 de sorte que tout morphisme $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ est nul.

Dans $\mathbb{Z}/15\mathbb{Z}$ les éléments d'ordre divisant 12 sont donc d'ordre divisant $12 \wedge 15 = 3$ et sont donc $0, 5, 10$, ce qui donne 3 morphismes distincts.

D'après les raisonnements ci-dessus, on en déduit donc qu'une CNS pour qu'il n'y ait pas de morphisme non nul $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ est donc $n \wedge m = 1$.

1.25 Il suffit de remarquer que $a^3 - a$ est divisible par 2 et 3 et donc 6 divise $(a^3 - a) + (b^3 - b) + (c^3 - c)$ et donc $a^3 + b^3 + c^3 \equiv a + b + b \mod 6$.

1.26 On rappelle que 700 n'étant pas premier, 429 est inversible dans $\mathbb{Z}/700\mathbb{Z}$ si et seulement si il est premier avec 700 et son inverse est donné par la relation de Bezout, i.e. si $1 = 700a + 429b$ alors l'inverse cherché est b. Il suffit alors d'appliquer l'algorithme d'Euclide :

$$\begin{aligned} 700 &= 429 + 271 \\ 429 &= 271 + 158 \\ 271 &= 158 + 113 \\ 158 &= 113 + 45 \\ 113 &= 2.45 + 23 \\ 45 &= 23 + 22 \\ 23 &= 22 + 1 \end{aligned}$$

On remonte alors les calculs et on obtient la relation de Bezout : $1 = 19.700 - 31.429$ de sorte que l'inverse de 429 dans $\mathbb{Z}/700\mathbb{Z}$ est -31.

1.27 Il s'agit de redémontrer le théorème chinois, i.e. que $\operatorname{Ker}\pi = (n \vee m)$ où $n \vee m$ est le ppcm de n et m, et $\operatorname{Im}\pi = \{(a, b) \ / \ (n \wedge m) | b - a \ \}$. Il est tout d'abord évident que π est un morphisme de groupes ; en outre si $k \in \operatorname{Ker}\pi$, alors il est divisible d'après le lemme de Gauss par $n \vee m$ de sorte que $\operatorname{Ker}\pi \subset (n \vee m)$, l'inclusion réciproque étant évidente. Soit maintenant a, b tels que $b - a$ est divisible par le pgcd (n, m). On écrit une relation de Bezout

$un + vm = (n, m)$ et on pose $k = u\frac{n}{(n,m)}b + v\frac{m}{(n,m)}b$. On a alors $k = un\frac{(b-a)}{(n,m)} + a \equiv a \mod n$; de même on a $k = vm\frac{(a-b)}{(n,m)} + b \equiv b \mod m$, de sorte que l'ensemble donné est inclus dans l'image de π. La réciproque est évidente car $k = a + \lambda n = b + \mu m$ soit $(b-a) = \lambda n - \mu m$ qui est donc divisible par (n, m). En particulier lorsque n et m sont premiers entre eux, π induit un isomorphisme $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(i) 5 et 7 sont premiers entre eux, on trouve la solution particulière $k = 32$, l'ensemble des solutions est alors $32 + \lambda 35$ avec $\lambda \in \mathbb{Z}$;

(ii) $(6, 10) = 2$ or 2 ne divise pas $3 - 2 = 1$, il n'y a donc pas de solutions ;

(iii) cette fois-ci $2 = (6, 10)$ divise $4 - 2$; une solution particulière est $k = 14$, l'ensemble des solutions est alors $14 + 30l$ avec $\lambda \in \mathbb{Z}$.

D'après ce qui précède si $k \equiv 3 \mod 6$, on a alors $k \equiv a \mod 10$ avec $a - 3$ divisible par 2, soit $a = 1, 3, 5, 7, 9$.

1.28 (i) 3 étant premier avec 7, il est inversible dans $\mathbb{Z}/7\mathbb{Z}$; on calcule rapidement que $3.5 \equiv 1 \mod 7$, i.e. $5 = 1/3$ dans $\mathbb{Z}/7\mathbb{Z}$ de sorte que l'équation s'écrit $x \equiv 20 \mod 7$ soit $x \equiv -1 \mod 7$;

(ii) d'après le théorème chinois, il suffit de vérifier l'équation modulo 3 et 7. Modulo 3 l'équation s'écrit $0.x \equiv 0 \mod 3$ et est donc toujours vérifiée. Modulo 7, on obtient $2x \equiv -2 \mod 7$; l'inverse de 2 dans $\mathbb{Z}/7\mathbb{Z}$ est -3, soit donc $x \equiv -1 \mod 7$. Le résultat final est donc $x \equiv -1 \mod 7$;

(iii) on calcule rapidement $676 = 2^2.13^2$; par le théorème chinois, on est donc ramené à résoudre $-x \equiv 0 \mod 4$ et $103x \equiv 105 \mod 169$. L'algorithme d'euclide fournit $64.103 - 39.169 = 1$ soit donc $x \equiv 64.105 \mod 69$ soit $x \equiv -40 \mod 169$ et donc $x \equiv -40 \mod 676$.

On peut aussi résoudre la congruence $103x \equiv 105 \mod 13^2$ de proche en proche, de la façon suivante. On la résoud tout d'abord modulo 13 soit $2x \equiv 4 \mod 13$ soit $x \equiv 2 \mod 13$. On écrit alors $x = 2 + 13k$ et on est donc ramené à résoudre $206 + 13.103k \equiv 105 \mod 13^2$ soit $13.103k \equiv -13.8 \mod 13^2$ soit en simplifiant par 13, $103k \equiv -8 \mod 13$, soit $2k \equiv -8 \mod 4$ et donc $k \equiv -4 \mod 13$ et donc finalement $x \equiv 2 - 4.13 \mod 13^2$.

1.29 On a $1035125 \equiv 12 \mod 17$. On pourrait maintenant calculer l'ordre de 12 dans $\mathbb{Z}/17\mathbb{Z}$. D'après le petit théorème de Fermat on a $12^16 \equiv 1 \mod 17$. Or $5642 \equiv 10 \mod 16$; la réponse est alors 12^10 modulo 17. Or $12 \equiv -5 \mod 17$ et $12^2 \equiv 8 \mod 17$ soit $12^4 \equiv -4$ soit $12^8 \equiv -1$ de sorte que l'ordre de 12 est 16. Finalement $12^10 = 12^8 12^2 = -12^2 = -8 = 9 \mod 17$.

1.30 On a $1823 \equiv 5 \mod 18$; or $5 \in (\mathbb{Z}/18\mathbb{Z})^\times$ on peut donc utiliser le petit théorème de Fermat avec $\varphi(18) = \varphi(2)\varphi(9) = 1.6 = 4$ soit $5^6 \equiv 1 \mod 18$. Or on a $242 \equiv 2 \mod 6$ soit $1823^{242} \equiv 5^2 = 7 \mod 18$. De même $2222 \equiv 2 \mod 20$ avec $2 \notin (\mathbb{Z}/20\mathbb{Z})^\times$; on ne peut donc pas utiliser le petit théorème de Fermat (2^8 est pair et ne peut donc pas être congru à 1 modulo 20). On étudie alors la suite $u_n = 2^n$ modulo 20 pour $n \in \mathbb{Z}$: $u_0 = 1$, $u_1 = 2$, $u_2 = 4$, $u_3 = 8$, $u_4 = -4$, $u_5 = -8$, $u_6 = 4$. On remarque qu'à partir de $n \geq 2$ la suite est périodique de période 4 : $u_{n+4} = u_n$. Or $321 \equiv 1 \mod 4$ de sorte que $u_{321} = u_5 = -8$ et donc $2222^{321} \equiv -8 \mod 20$.

La bonne façon de comprendre le phénomène est d'utiliser le lemme chinois. On a $2222 \equiv 2 \mod 4$ de sorte que $2222^n \equiv 0 \mod 4$ dès que $n \geq 2$. On a aussi $2222 \equiv 2 \mod 5$ et $321 \equiv 1 \mod 4$ et donc d'après le petit théorème de Fermat $2222^{321} \equiv 2 \mod 5$ et donc $2222^{321} \equiv 12 \mod 20$.

Remarque : On comprend ainsi que de manière générale la suite $u_n = a^n \mod m$ pour a non premier avec m est périodique à partir d'un certain rang (le temps que pour les premiers p divisant $a \wedge m$, $a^k \equiv 0 \mod m$ soit $k\alpha_a(p) \geq \alpha_m(p)$ où $\alpha_a(p)$ (resp. $\alpha_m(p)$) est la multiplicité de p dans a (resp. dans m)). Une autre façon de le remarquer et de dire qu'elle ne prend qu'un nombre fini de valeurs de sorte qu'il existe n_0 et $n_0 + r$ tels que $u_{n_0} = u_{n_0+r}$ ce qui implique que $u_{n_0+r+k} = u_{n_0+k}$ et donc la périodicité de u_n à partir d'un certain rang.

1.31 On a $42 = 2.3.7$, il suffit alors de verifier la congruence modulo 2, 3 et 7. Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.

1.32 On rappelle que p étant premier, $(\mathbb{Z}/p\mathbb{Z}, +, *)$ est un corps. Ainsi dans $\mathbb{Z}/p\mathbb{Z}$, on a $\bar{a}^2 + \bar{b}^2 = 0$ soit $(\bar{a}/\bar{b})^2 = -1$, car $\bar{b} \neq 0$. Ainsi -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$: $-1 = x^2$, soit $x^4 = 1$. Or d'après le petit théorème de Fermat, on a $x^{p-1} = 1$, soit $4|p-1$ car 4 est l'ordre de x dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

1.33 On a $42 = 2.3.7$, il suffit alors de verifier la congruence modulo 2, 3 et 7. Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.

1.34 Le nombre Σ est une somme de $x_{i_1}^{a_{i_1}} \cdots x_{i_k}^{a_{i_k}}$, les i_r étant distincts deux à deux et $\sum_{r=1}^{k} a_{i_r} = p-1$; pour que ce terme apparaisse il faut que I contienne les k indices $i_1, \cdots, i_k$ ce qui arrive dans $\binom{p-k}{2p-1-k}$ cas de sorte que le nombre de fois où le terme précédent apparait dans Σ est divisible par ce coefficient binomial lequel est divisible par p : en effet il est égal à $\frac{(2p-1-k)\cdots p}{(p-k)!}$ et comme p est premier p ne divise pas $(p-k)!$ pour tout $1 \leq k \leq p$.

Par ailleurs si aucun des S_I n'était divisible par p alors d'après le petit théorème de Fermat, on aurait $S_I^{p-1} \equiv 1 \mod p$ et donc $\Sigma \equiv \binom{p}{p-1} \not\equiv 0 \mod p$.

Le cas n quelconque s'en déduit immédiatement en remarquant que si le résultat est vrai pour n et m, il l'est pour mn.

1.35 (i) Comme $1+p+\cdots+p^{p-1} \equiv 1 \mod 2$, ses facteurs premiers sont tous impairs ; en outre comme il est congru à $1+p \mod p^2$, il possède au moins un diviseur premier non congru à 1 modulo p^2.

(ii) Raisonnons par l'absurde : soit n tel que $n^p \equiv p \mod q$; on a alors $n^{p^2} \equiv p^p \equiv 1 \mod q$ car $p^p - 1 = (p-1)(1+p+\cdots+p^{p-1}$. Comme q est un nombre premier ne divisant pas n, il est premier avec n et donc d'après le petit théorème de Fermat, on a $n^{q-1} \equiv 1 \mod q$. On en déduit donc, d'après le théorème de Bezout, que $n^{(q-1)\wedge p^2} \equiv 1 \mod q$ et comme ce pgcd est égal à 1 ou p, le cas p^2 étant exclu par le fait que $q \not\equiv 1 \mod p^2$, on a $n^p \equiv 1 \mod q$. Ainsi comme $n^p \equiv p \mod q$, on a $p \equiv 1 \mod q$ et donc $1+p+\cdots+p^{p-1} \equiv p \mod q$ et donc q divise aussi p soit $q = p$ ce qui ne se peut pas car $q|p^p - 1$.

1.36 Il suffit de trouver les n premiers, on obtiendra alors les n généraux en prenant des produits finis de tels premiers. Remarquons déjà que comme $2+3+6-1 \equiv 0 \mod 2$, le premier 2 ne convient pas. De même comme $2^2+3^2+6^2-1 \equiv 0 \mod 3$ alors 3 non plus. Soit alors $p \geq 5$; d'après le petit théorème de Fermat on a

$$6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) = 32^{p-1} + 23^{p-1} + 6^{p-1} - 6 \equiv 0 \mod p$$

et comme $p \wedge 6 = 1$, on a $2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 0 \mod p$ et donc p ne convient pas non plus. Finalement 1 est le seul entier qui convient.

1.37 Considérons un pgcd δ de (x^2-9) et (x^2-16) ; celui-ci divise $(x^2-9)-(x^2-16) = 7$, soit $\delta = 1, 7$.

Supposons $\delta = 1$: d'après loc. cit., on en déduit que $x^2 - 9 = \epsilon t^2$ et $x^2 - 9 = \epsilon s^2$ avec $\epsilon = \pm 1$ et $t, s \geq 0$ premiers entre eux. On obtient alors $7 = \epsilon(t^2 - s^2) = \epsilon(t-s)(t+s)$ d'où

$t+s=7$ et $t-s=\epsilon$. Si $\epsilon=1$, on a $t=4$ et $s=3$ ce qui donne $x=\pm 5$ et $y=\pm 12$. Si $\epsilon=-1$ alors $t=3$ et $s=4$ ce qui donne $x=0$ et $y=\pm 12$.
Remarque : Il nous faut bien sûr vérifier à chaque fois que les solutions obtenues conviennent, car on a simplement raisonné par implication.

Supposons $\delta=7$: $x^2-9=7u$, $x^2-16=7v$ et $y^2=7^2uv$ avec u et v premiers entre eux. On a alors $uv=(y/7)^2$ de sorte que $u=\epsilon t^2$ et $v=\epsilon s^2$ avec $\epsilon=\pm 1$ et $s,t\geq 0$ premiers entre eux. On trouve alors les solutions $x=\pm 3,4$ et $y=0$, qui conviennent.

1.38 (i) Si x est pair, on a $y^2\equiv -1 \mod 8$. En écrivant y impair sous la forme $2k+1$, on obtient $y^2=1+4k(k+1)\equiv 1 \mod 8$ contradiction.
(ii) On a $x^3+8=(x+2)(x^2-2x+4)$ avec x impair de la forme $2k+1$; $(x^2-2x+4)=4k^2+3$. On en déduit donc qu'il existe un p premier divisant x^2-2x+4 avec $p\equiv 3 \mod 4$. Or si p premier divise y^2+1 alors $p\equiv 1 \mod 4$, d'où la contradiction.

1.39 Il s'agit donc de déterminer n et m tels que $2008^n\equiv 2008^m \mod 1000$ avec $1000=2^3 5^3$ ce qui d'après le théorème chinois est équivalent aux congruences

$$2008^n\equiv 2008^m \mod 8 \qquad 2008^n\equiv 2008^m \mod 5^3.$$

Comme $2008\equiv 0 \mod 8$, la première congruence est toujours valable, tandis que comme $2008\equiv 8 \mod 5^3$, la deuxième s'écrit $8^{n-m}\equiv 1 \mod 5^3$. Calculons alors l'ordre de 8 dans $(\mathbb{Z}/5^3\mathbb{Z})^\times$ qui est un diviseur de $\varphi(125)=100$. Or modulo 5, on a $8^{50}\equiv(-1)^{25}\equiv -1 \mod 5$ de sorte que cet ordre n'est pas un diviseur de 50.

1.40 Modulo3, on a $x^3\equiv x \mod 3$ de sorte que l'équation donne $x+y\equiv 2 \mod 3$. On est donc dans l'une des situations suivantes :
- $x\equiv y\equiv 1 \mod 3$ de sorte que modulo 9, on a $x^3-3xy^2+y^3\equiv 1-3+1\equiv -1 \mod 9$ alors que $2891\equiv 2 \mod 9$;
- $x\equiv 0 \mod 3$ et $y\equiv 2 \mod 3$ de sorte que $x^3-3xy^2+y^3\equiv 0-0-1 \mod 9$ ce qui est absurde ;
- $x\equiv 2 \mod 3$ et $y\equiv 0 \mod 3$ et donc $x^3-3xy^2+y^3\equiv -1-0+0 \mod 9$ ce qui est encore absurde.

1.41 Essayons de factoriser $P(x)=(x+1)^7-x^7-1$ en regardant ses racines : on remarque qu'outre 0 et 1, le nombre complexe $j=e^{2i\pi/3}$ est aussi racine car $j+1=-j^2$ de sorte que $P(x)$ est divisible par $x(x+1)(x^2+x+1)$ le quotient étant égal à x^2+x+1 et donc

$$(a+b)^7-a^7-b^7=7ab(a+b)(a^2+ab+b^2)^2.$$

On est ainsi amené à résoudre $a^2+ab+b^2\equiv 0 \mod 7^3$ qui s'écrit encore

$$(a+\frac{b}{2})^2\equiv -3(\frac{b}{2})^2 \mod 7^3$$

laquelle possède des solutions si et seulement si le symbole de Legendre $(\frac{-3}{7^3})=1$ ce que l'on vérifie aisément en utilisant la loi de réciprocité quadratique.

6.2. du chapitre 2. —

2.1

6.3. du chapitre 3. —

3.1 (1) Le polynôme $\sum_{i=0}^{n-1} P(i)L_i(X) - P(X)$ est dans $\mathbb{Q}_{n-1}[X]$ et appartient à l'intersection des noyaux $\operatorname{Ker} f_i$ où f_i est la forme linéaire $Q \in \mathbb{Q}_n[X] \mapsto Q(i) \in \mathbb{Q}$. Or la famille des $(f_i)_{0\leq i\leq n-1}$ est libre ; en effet étant donnée une relation $\sum_i \lambda_i f_i = 0$, en la testant sur L_i, on obtient $\lambda_i = 0$. Ainsi l'espace vectoriel $\bigcap_{i=0}^{n-1} \operatorname{Ker} f_i$ est de dimension nulle de sorte que $P(X) = \sum_{i=0}^{n-1} P(i)L_i(X)$.

(2) Comme précédemment soit $Q \in \mathbb{Q}_{n-1}[X]$ tel que $Q(i) = P(i)$ pour tout $0 \leq i \neq i_0 \leq n-1$. Ainsi $P - Q$ appartient à $\bigcap_{\substack{0\leq i\leq n-1 \\ i\neq i_0}} \operatorname{Ker} f_i$ qui est de dimension 1 engendré par $\prod_{0\leq i\neq i_0\leq n-1}(X-i)$ de sorte qu'il existe $\lambda \in \mathbb{Q}$ tel que $Q(X) = P(X) + \lambda \prod_{i\neq i_0}(X-i)$; or Q est à coefficients dans $\mathbb{Z}$ de sorte que $\lambda \in \mathbb{Z}$. Ainsi pour le coefficient constant de Q on obtient $s_0 + (-1)^{n-1}\lambda\frac{n!}{i_0}$ où $\lambda \in \mathbb{Z}$ est non déterminé ; on connaît alors s_0 à un multiple de $\frac{n!}{i_0}$ près. Si $p < \frac{n!}{i_0}$, alors s_0 est connu.

(3) l'indication correspond à dire que $\frac{n!}{i_0}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$, on le prouve en écrivant une relation de Bezout...

Comme précédemment on a $s_0+\lambda\frac{n!}{i_0}$ or $\frac{n!}{i_0}$ est inversible, de sorte que lorsque λ décrit $\mathbb{Z}/p\mathbb{Z}$, $s_0 + \lambda\frac{n!}{i_0}$ aussi ; bref on ne sait rien sur s_0.

(4) Le code est s_0. On tire au sort les s_i, et on transmet $P(i)$ modulo p à la personne numérotée i. D'après (2), les n personnes réunies peuvent reconstituer s_0 alors que d'après (3), $n-1$ quelconques ne le peuvent pas.

(5) De la même façon soit $P(X) = \sum_{i=0}^{k-1} s_i X^i$ et on transmet $P(i)$ à la personne i pour $1 \leq i \leq n$. Comme précédemment, k personnes quelconques peuvent reconstituer P et donc s_0 alors que $k-1$ quelconques ne le peuvent pas

Remarque : Si une personne malintentionnée i_0 transmet une mauvaise valeur distincte de $P(i_0)$ alors que toutes les autres transmettent leur $P(i)$, la personne i_0 sera la seule à connaître le code s_0. Bien sur s'il y a deux qui trichent, personne ne sait rien.

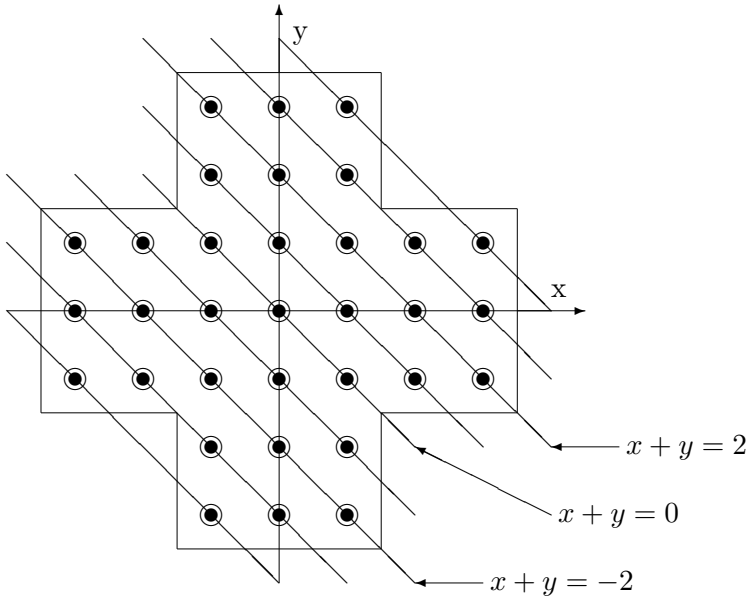
3.2 (1) Prenons par exemple le mouvement élémentaire de la figure (3.2). Dans le plateau de gauche on a $\alpha = j^{x_0+y_0}(1+j)$ (resp. $\beta = j^{x_0-y_0}(1+j)$) alors que dans le plateau de droite on a $\alpha = j^{x_0+y_0}.j^2$ (resp. $\beta = j^{x_0-y_0}j^2$), avec $(x_0, y_0) = (-2, -1)$. Le résultat découle alors de l'égalité $1 + j = j^2$ dans $\mathbb{F}_4$ (on rappelle que dans $\mathbb{F}_4$, on a $1 = -1$). Les autres mouvements élémentaires se traitent de manière strictement identique.

(2) Commençons par calculer (α, β) pour la configuration où tous les réceptacles contiennent une bille. La configuration étant invariante par la réflexion d'axe (Oy), on a $\alpha = \beta$, calculons donc α. Pour cela on propose de sommer sur les droites $x + y$ constantes, de sorte que ne contribuent que les droites où il y a un nombre impair de billes, ce qui donne $\alpha = j^0+j^2+j^{-2} = 0$, comme on le voit sur la figure suivante.

Notons alors avec un indice *tot* (resp. $\mathcal{C}_0$, resp. 0) ce qui fait référence à la configuration où tous les réceptacles sont remplis (resp. tous sauf en (x_0, y_0), resp aucun sauf en (x_0, y_0)). On a ainsi $(\alpha_{tot}, \beta_{tot}) = (\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) + (\alpha_0, \beta_0) = (0, 0)$ de sorte que $(\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) = (\alpha_0, \beta_0)$.

(3) On calcule comme précédemment les invariant (α, β) ce qui donne $(0, 0)$ qui ne peut pas être de la forme $(j^{x_0+y_0}, j^{x_0-y_0})$.

6.4. du chapitre 4. —



4.1 Le polynôme X^3+2X+1 n'a pas de racines dans $\mathbb{F}_3$, il y est donc irréductible. L'ordre de X est soit $1, 2, 13, 26$; les cas 1 et 2 sont clairement exclus calculons alors $X^{13} = X^9.X^3.X$. On a $X^3 = X - 1$ puis $X^9 = X^3 - 1 = X + 1$ et donc $X^{13} = -1$. On vérifie aussi que $X^{10} = X^2 + X$ et donc $i = 10$

4.2 Parmi les 5 cartes, il y en a forcément deux de la même famille (trèfle, carreau, coeur ou pique) ; pour fixer les idées supposons qu'il s'agisse du 4 et du roi de coeur. En numérotant les cartes de l'as, deux vers le roi circulairement (le successeur du roi est l'as) ces deux cartes sont espacés d'où plus 6 : ici c'est 4. Alice garde alors pose alors la carte à laquelle il faut rajouter ce nombre pour obtenir l'autre de la même famille ; ici elle pose le roi de coeur et garde le 4. Ainsi Bob sait que la carte cherchée est un coeur. Il faut alors avec les trois cartes restante savoir coder les nombres de 1 à 6. Une façon de faire est de positionner la carte de moindre valeur (les familles étant classées comme au bridge) à gauche (resp. au milieu, à droite) si le nombre est 1 ou 2 (resp. 3 ou 4, 5 ou 6) et celle de plus grande valeur à gauche (resp. à droite) parmi les places restantes s'il faut prendre la plus petite (resp. grande) des deux possibilités.

6.5. du chapitre 5. —

5.1 Notons $b_1, \cdots, b_{12}$ le nombre réceptionné et supposons qu'il existe $1 \leq i \leq 12$ tel que $b_i \neq a_i$ et $b_k = a_k$. Si $1 \leq i \leq 10$ alors

$$b_{11} - \sum_{k=1}^{10} b_k = a_i - b_i \not\equiv 0 \mod 11, \qquad b_{12} - \sum_{k=1}^{10} k b_k = i(a_i - b_i) \not\equiv 0 \mod 11$$

et donc les tests de b_{11} et b_{12} sont erronés ce qui permet de savoir si l'erreur s'est glissé dans les 10 premiers chiffres ou dans les deux clés. Si c'est dans les clés, un seul de ces tests est faux et on le corrige sinon comme 11 est premier $a_i - b_i \in (\mathbb{Z}/11\mathbb{Z})^\times$ de sorte qu'en divisant la deuxième ligne par la première on calcule i puis $a_i - b_i$.

5.2

5.3 (a) Le polynôme $P(X)$ n'a pas de racines dans $\mathbb{F}_2$, ni dans $\mathbb{F}_4$ car $P(j) = j$ et $P(j^2) = j^2$. Par ailleurs un élément α non nul de $\mathbb{F}_8$ vérifie $\alpha^7 = 1$ et donc $P(\alpha) = \alpha^3 + 1$ qui est non nul car dans $\bar{\mathbb{F}}_2$ seuls $j, j^2 \in \mathbb{F}_4$ vérifient $X^3 + 1 = 0$. Ainsi $\mathbb{F}_{2^7} \simeq \mathbb{F}_2[X]/(X^7 + X^3 + 1)$ et l'ordre de la classe α de X est un diviseur de 127 qui est premier de sorte que α est un générateur du groupe multiplicatif.

(b) Il s'agit d'un code de Hamming ; si $\sum_{i=0}^{126} a'_i \alpha^i = 0$ alors le mot reçu appartient au code et s'il y a au plus une erreur, il s'agit du mot initial. Sinon k est l'unique entier entre 0 et 126 tel que $\alpha^k = \sum_{i=0}^{126} a'_i \alpha^i$.
Remarque : on se sert du bit de parité pour tester s'il y a deux erreurs auquel cas on demande à renvoyer le message. Au final on peut corriger une erreur et détecter s'il y a deux erreurs.

5.4 (a) On écrit $P(X) = \frac{X^9+1}{X+1} + X(X^2 + 1)$; celui-ci n'a pas de racines dans $\mathbb{F}_2$ ni dans $\mathbb{F}_4$ puisque $j^9 + 1 = 0$ et $j^3 + j = 1 \neq 0$. Dans $\mathbb{F}_8$, on a $X^9 = X^2$ et donc $P(X) = X + 1 + X^3 + X = X^3 + 1$ qui n'a pas de racines dans $\mathbb{F}_8$. Si $\alpha \in \mathbb{F}_{16} - \mathbb{F}_4$, est tel que $P(\alpha) = 0$ alors $\alpha^9 + 1 = \alpha(\alpha + 1)^3$ et donc en prenant la puissance cinquième et en utilisant $(\alpha + 1)^{15} = 1$ car $\alpha \neq 1$, on obtient

$$(\alpha^9 + 1)^5 = \alpha^{45} + \alpha^{36} + \alpha^9 + 1 = \alpha^5$$

ce qui donne $\alpha^9 + \alpha^6 + \alpha^5 = 0$ soit $\alpha^4 + \alpha + 1 = 0$. Ainsi en réinjectant l'égalité $\alpha + 1 = \alpha^4$ on obtient $\alpha^9 + 1 = \alpha^1 3$ ce qui après multiplication par α^3 donne $\alpha^{12} = \alpha^3 + \alpha$ avec

$$\alpha^{12} = (\alpha^4)^3 = (\alpha + 1)^3 = \alpha^3 + \alpha^2 + \alpha + 1$$

et donc $\alpha = \alpha^{12} + \alpha^3 = \alpha^2 + \alpha + 1$ ce qui donne $\alpha^2 = 1$ et comme 2 ne divise pas 15, on obtient α d'ordre $1 = 2 \wedge 15$ soit $\alpha = 1$ qui ne convient pas.

(b-i) Il s'agit d'un code de Reed-Solomon qui est donc 2-correcteur. Si on suppose qu'il y a au plus deux erreurs, on teste si $\alpha, \alpha^2, \alpha^3$ et α^4 sont racines du polynôme $\sum_{i=0}^{254} b_i X^i$: si oui alors il n'y a pas eu d'erreurs sinon le bit de parité permet de savoir s'il y a eu 1 ou 2 erreurs et on calcule les α^k puis les $\alpha^i + \alpha^j$ pour savoir quels bits corriger.

(b-ii) Notons i_1, i_2, i_3, i_4 les indices des bits en question ; il s'agit alors de trouver quelle somme $\sum_{k=1}^{4} \epsilon_k X^{i_k} = 0$ avec $\epsilon_i = 0, 1$ prend en α^j pour $j = 1, 2, 3, 4$, la valeur $\sum_{i=0}^{254} b_i X^i$ où pour $k = 1, \cdots, 4$ on a posé $b_{i_k} = 0$. Si on avait 2 quadruplets de ϵ_k distincts, alors par soustraction, on aurait un polynôme formé d'au plus 4 monômes ayant α^j pour $j = 1, \cdots, 4$ comme racines et donc multiple de $(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4) = X^4 + \beta_1 X^3 + \beta_2 X^2 + \beta_3 X + \beta_4$ avec $\beta_j \neq 0$ pour tout $j = 1, \cdots, 4$ de sorte que le polynôme a forcément 5 termes non nuls, d'où la contradiction.

(b-iii) Si moins de 16 sillons sont illisibles, d'après (ii) on peut alors reconstituer le mot qui rappelons le est constitué de lettres de 8 bits...

Boyer Pascal