Université Pierre et Marie Curie M1 théorie des nombres Année 2007-2008

Feuille d'exercices 3

Remarque : Tous les exercices ne seront pas traités en séance de TD, j'indiquerai au fur et à mesure sur la page du forum (http ://cours-jussieu-nombres.monforum.com/cours-et-td-2008-vf7.html) les exercices que nous aurons abordés.

1 Corps finis

Exercice 1.1. *Montrer les isomorphismes suivant et donner un générateur du groupe des inversibles des corps en question :*

(i) $\mathbf{F}_4 \simeq \mathbf{F}_2[X]/(X^2+X+1)$ *;*

(ii) $\mathbf{F}_8 \simeq \mathbf{F}_2[X]/(X^3+X+1)$ *;*

(iii) $\mathbf{F}_{16} \simeq \mathbf{F}_2[X]/(X^4+X+1)$ *; donner dans cet isomorphisme l'image de* $\mathbf{F}_4 \subset \mathbf{F}_{16}$ *et en déduire* $\mathbf{F}_{16} \simeq \mathbf{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y)$.

(iv) $\mathbf{F}_9 \simeq \mathbf{F}_3[X]/(X^2+X-1)$.

Exercice 1.2. *On dira d'une extension de corps* $k \subset \bar{k}$ *qu'elle est une clôture algébrique si :*

(a) tout élément $x \in \bar{k}$ *est algébrique sur* k*, i.e. il existe une polynôme* $P \in k[X]$ *tel que* $P(x) = 0$ *;*

(b) tout polynôme $P \in \bar{k}[X]$ *est totalement décomposé dans* $\bar{k}$.

Pour tout n *divisant* n' *on fixe une injection* $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^{n'}}$. *Montrez alors que* $\bar{\mathbb{F}}_p := \bigcup_{n>1} \mathbb{F}_{p^{n!}}$ *est une cloture algébrique de* $\mathbf{F}_p$.

Exercice 1.3. *(i) Donner tous les polynômes irréductibles de degré inférieur à* 4 *sur* $\mathbf{F}_2$.

(ii) Quelle est la factorisation sur $\mathbb{F}_4$ *d'un polynôme de* $\mathbb{F}_2[X]$ *irréductible de degré* 4 *?*

(iii) Déduire des questions précédentes, le nombre de polynômes irréductibles de degré 2 *sur* $\mathbf{F}_4$.

(iv) Expliciter les polynômes irréductibles de degré 2 *sur* $\mathbb{F}_4$.

Exercice 1.4. *Polynômes irréductibles sur* $\mathbb{F}_q$. *soient* $A(n,q)$ *l'ensemble des polynômes irréductibles unitaires de degré* n *sur* $\mathbb{F}_q$ *et* $I(n,q)$ *le cardinal de cet ensemble.*

(a) Montrer que si $d|n$ *alors si* $P \in A(d,q)$ *on a* P *qui divise* $X^{q^n} - X$.

(b) Montrer que si $P \in A(d,n)$ *divise* $X^{q^n} - X$ *alors* d *divise* n.

(c) En déduire la formule

$$\sum_{d|n} dI(d,q) = q^n,$$

puis en appliquant la formule d'inversion de Moebius

$$I(n,q) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) q^d.$$

(d) Montrer que pour tout $n \geq 1$, $I(n,q) \geq 1$ *et trouver un équivalent de* $I(n,q)$ *quand* n *tend vers* $+\infty$.

Exercice 1.5. *(1) Le nombre* 2 *est-il un carré dans* $\mathbf{F}_5$ *? Montrer que* X^2+X+1 *est irréductible sur* $\mathbf{F}_5$.

(2) *Soit* $P(X) \in \mathbf{F}_5[X]$ *un polynôme unitaire irréductible de degré deux . Montrer que le quotient*

$$\frac{\mathbf{F}_5[X]}{(P(X))}$$

est isomorphe au corps $\mathbf{F}_{25}$ *et que* P *a deux racines dans* $\mathbf{F}_{25}$.

(3) *On note* α *une racine de* X^2+X+1 *dans* $\mathbf{F}_{25}$. *Montrer que tout* $\beta \in \mathbf{F}_{25}$ *peut s'écrire* $a\alpha + b$ *avec* a *et* b *dans* $\mathbf{F}_5$.

(4) *Soit* $P = X^5 - X + 1$. *Montrer que pour tout* $\beta \in \mathbf{F}_{25}$, *on a* $P(\beta) \neq 0$. *En déduire que* P *est irréductible sur* $\mathbf{F}_5$. P *est-il irréductible sur* $\mathbf{Q}$ *?*

Exercice 1.6. *On considère le polynôme* $Q(X) = X^9 - X + 1$ *sur* $\mathbf{F}_3$.

(a) *Montrer que le polynôme* Q *n'a pas de racines dans* $\mathbb{F}_3, \mathbb{F}_9$.

(b) *Montrer que* $\mathbb{F}_{27} \simeq \frac{\mathbb{F}_3[X]}{(X^3-X-1)}$.

(c) *Montrer que toute racine* $\alpha \in \mathbb{F}_{27}$ *du polynôme* X^3-X-1 *est une racine du polynôme* Q.

(d) *Déterminer toutes le racines de* Q *dans* $\mathbb{F}_{27}$.

(e) *Factoriser le polynôme* Q *sur le corps* $\mathbb{F}_3$.

Exercice 1.7. *A quelle condition un polynôme* P *à coefficients dans* $\mathbf{F}_p$ *de degré* n *est-il irréductible sur* $\mathbf{F}_{p^m}$ *? Dans le cas où* P *est irréductible sur* $\mathbf{F}_p$, *on donnera des précisions sur les degrés des facteurs irréductibles de* P *sur* $\mathbf{F}_{p^m}$. *En particulier pour* $n = 5$, *donner* m *minimal tel que tout polynôme de degré* 5 *à coefficients dans* $\mathbf{F}_p$ *soit totalement décomposé (resp. possède une racine) sur* $\mathbf{F}_{p^m}$.

Exercice 1.8. *Théorie de Galois des corps finis et version faible du théorème de Dirichlet : Soit* p *un nombre premier et* n *un entier premier avec* p. *On pose* $q = p^r$.

(1) *Décrire le groupe de Galois de l'extension* $\mathbb{F}_{q^n} : \mathbb{F}_q$ *et expliciter la théorie de Galois, i.e. montrer que l'application qui à un sous-groupe* H *de* $gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *associe le sous-corps de* $\mathbb{F}_{q^n}$ *des éléments fixés par tous les éléments de* H, *est une bijection entre les sous-groupes du groupe de Galois et les extensions intermédiaires* $\mathbb{F}_q \subset \mathbf{K} \subset \mathbb{F}_{q^n}$.

(2) *Soit* $L = Dec_{\mathbb{F}_p}(X^n - 1)$. *Montrer que* $\mathrm{Gal}(L/\mathbb{F}_p)$ *est isomorphe au sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$ *engendré par l'image de* p. *Montrer que le* n*-ième polynôme cyclotomique* $\Phi_n(X)$ *se décompose sur* $\mathbb{F}_p$ *en un produit de* $\phi(n)/k$ *facteurs irréductibles distincts, tous de degré* k. *Quel est cet entier* k *? En déduire une version faible du théorème de progression arithmétique, i.e. :*
pour tout entier n *il existe une infinité de nombres premiers* p *congrus à* 1 *modulo* n.

Exercice 1.9. *(i) Montrer que* X^4+1 *est irréductible sur* $\mathbb{Z}$ *et réductible modulo tout nombre premier* p. *(Indication : montrer que pour tout nombre premier impair* p, *le polynôme* X^4+1 *a une racine dans le corps* $\mathbb{F}_{p^2}$.

(ii) Soit n *un entier ne s'écrivant pas sous la forme* p^α *ou* $2p^\alpha$ *avec* p *premier impair. On sait que le* n*-ième polynôme cyclotomique* Φ_n *est irréductible sur* $\mathbb{Z}$. *Montrer en utilisant la question (ii) de l'exercice sur la théorie de Galois des corps finis, que* Φ_n *est réductible modulo tout nombre premier.*

Exercice 1.10. *Soit* $P(X) = X^4 - 10X^3 + 21X^2 - 10X + 11$

(a) *Décomposer* P *en facteurs irréductibles modulo 2,3,5.*

(b) *Montrer que* P *est irréductible sur* $\mathbb{Q}$.

Exercice 1.11. *Soient p et l deux nombres premiers impairs. On suppose que p engendre $(\mathbb{Z}/l\mathbb{Z})^*$ et que $l \equiv 2 \mod 3$. On note $P(X) = X^{l+1} - X + p$. On veut montrer que P est irréductible sur $\mathbb{Z}$.*

(i) Montrer que P n'a pas de racine rationnelle.

(ii) On raisonne par l'absurde et on suppose $P = QR$ avec $Q, R \in \mathbb{Z}[X]$ unitaire et de degré au moins 2. Montrer que $\bar{P} = X(X-1)\bar{\Phi}_l$ est la décomposition en polynômes irréductibles de $\bar{P}$ sur $\mathbf{F}_p$; en déduire alors que $\bar{Q} = \bar{\Phi}_l$ et $\bar{R} = X(X-1)$.

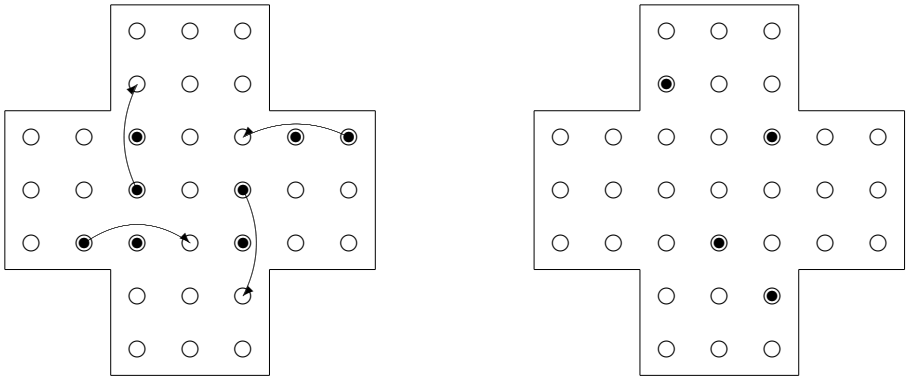
(iii) En passant modulo 2, en déduire une contradiction. Comme exemple on propose le polynôme $X^{72} - X + 47$.

Exercice 1.12. *Montrer l'existence d'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)* $p \equiv -1 \mod 10$.

Indication : on cherchera à faire des lemmes du genre : si p divise a^2+qb^2 et p premier avec b, alors $-q$ est un carré modulo p et donc d'après la loi de réciprocité quadratique p est congru à ? modulo q.

Exercice 1.13. *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. A 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*

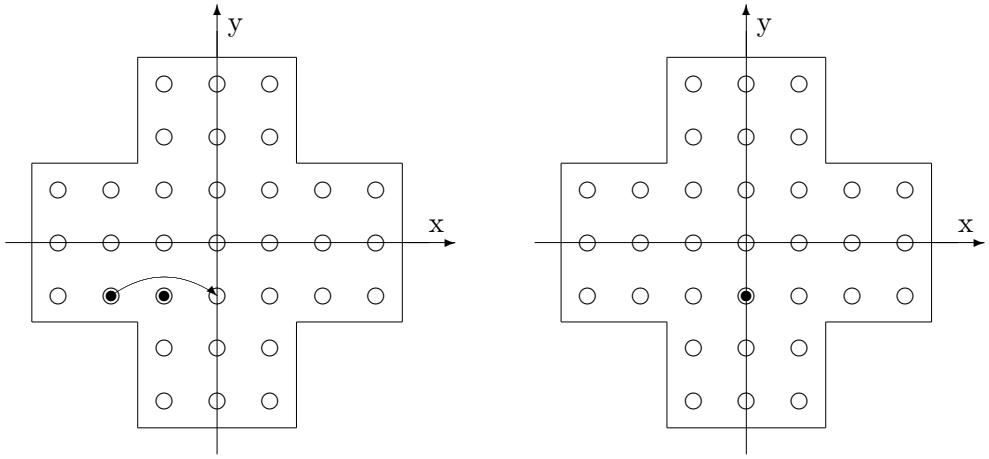


Soit alors O placé au centre du plateau et un repère (O, x, y) comme dans la figure suivante et pour une configuration $\mathcal{C}$ quelconque de billes sur le plateau on introduit

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

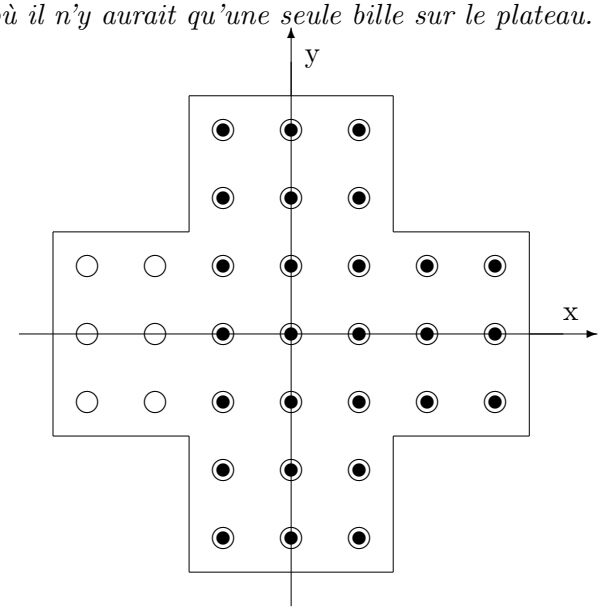
où j est un générateur de $\mathbb{F}_4^\times$.

(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.



Exercice 1.14. *Soit n un entier tel que pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p. Montrer que n est un carré dans $\mathbb{N}$.*

2 Codes correcteurs

Pour transmettre une information on utilise l'alphabet $\mathbb{F}_q$; on envoie des messages de n lettres. Le principe des codes correcteurs d'erreurs est de pouvoir corriger des erreurs de transmission (cf. les CD, les transmissions par satellite...). L'ensemble des mots $\mathbb{F}_q^n$ peut être muni de la distance de Hamming définie comme suit : pour $(x_1, \cdots, x_n)$ et $(x'_1, \cdots, x'_n)$ dans $\mathbb{F}_q^n$ alors

$$d(x, x') := \mathrm{card}\{i \in [1, n] \ / \ x_i \neq x'_i\}$$

On vérifie aisément qu'il s'agit bien d'une distance.

Un code est un sous-ensemble $\mathcal{C} \subset \mathbb{F}_q^n$ comportant au moins deux éléments de $\mathbb{F}_q^n$; on définit la distance d'un code comme

$$d(\mathcal{C}) := \min_{x \neq x' \in \mathcal{C}} d(x, x').$$

Le principe consiste, une fois choisi un code $\mathcal{C}$, à n'envoyer que des messages avec des mots appartenant à $\mathcal{C}$; on peut alors repérer jusqu'à $d(\mathcal{C}) - 1$ erreurs de transmission sur un mot en outre si le nombre d'erreurs commises t est tel que $2t + 1 \leq d(\mathcal{C})$, on voit qu'il existe un seul mot de $\mathcal{C}$ situé à une distance $\leq t$ du mot reçu. Le code permet donc de corriger $t := \lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$ erreurs. On introduit le taux de corrections $\frac{t}{n}$ et le taux d'information $\log \mathrm{card}(\mathcal{C})/n \log q$. La théorie de l'information développée par Shannon, indique que si l'on accepte d'envoyer des messages de plus en plus long, il existe des codes aussi sûrs que l'on veut avec un taux d'information proche de 1 : cependant le théorème de Shannon est un théorème d'existence, il ne dit pas comment construire les codes en question.

Exercice 2.15. *On considère des codes linéaires, i.e. $\mathcal{C} \subset \mathbb{F}_q^n$ est un sous-espace vectoriel. Pour tout $x \in \mathcal{C}$, on définit son poids $\omega(x)$ comme le nombre de composantes non nulles.*

(1) Montrer que $d(\mathcal{C}) = \min_{0 \neq x \in \mathcal{C}} \min \omega(x)$.

*(2) **exemple du bit de parité :** pour transmettre $(x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^{n-1}$ on envoie $x = (x_1, \cdots, x_{n-1}, x_1 + \cdots + x_{n-1}) \in \mathbb{F}_2^n$. Montrer qu'il s'agit d'un code cyclique qui permet de repérer une erreur mais pas de la corriger.*

*(3) **Code de Hamming :** 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 $x = m_0 e_0 + m_1 e_1 + m_2 e_2 + m_3 e_3$. Expliquez le décodage dans le cas où une erreur au plus est commise.

(4) Une matrice génératrice A d'un code $\mathcal{C}$ est une matrice dont les lignes forment une base. Une matrice vérificatrice B d'un code $\mathcal{C}$ est une matrice dont les lignes forment une base des formes linéaires s'annulant sur $\mathcal{C}$. Montrer que $A^t B = 0$ et que la distance du code $\mathcal{C}$ est le plus petit nombre d tel qu'il existe d vecteurs colonnes de B distincts et liés.

(5) Supposons un code $\mathcal{C}$ donné avec une matrice vérificatrice B et supposons que le code est 1-correcteur. Soit alors un message x' reçu différant du message envoyé x en au plus une coordonnée : on note $\epsilon = x' - x$ l'erreur commise. Montrer comment calculer ϵ à l'aide de B.

(6) Soit $\mathcal{C}$ un code de longueur n sur $\mathbb{F}_q$. 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** : $\bar{\mathcal{C}} := \{(x_1, \cdots, x_{n+1}) \in \mathbb{F}_q^{n+1} \ / \ (x_1, \cdots, x_n) \in \mathcal{C} \text{ et } x_1 + \cdots + x_{n+1} = 0\}$.*

*(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.*

(7) Soit $\mathcal{C}$ un code de dimension k et de longueur n sur $\mathbb{F}_q$, montrer que $d(\mathcal{C}) \leq n + 1 - k$ et que si $\mathcal{C}$ est t-correcteur alors

$$1 + C_n^1(q-1) + C_n^2(q-1)^2 + \cdots + C_n^t(q-1)^t \leq q^{n-k}$$

Un code tel que $d(\mathcal{C}) = n + 1 - k$ sera dit MDS maximal distance separable. Un code t-correcteur tel que $\mathcal{C} = \bigcup_{x \in \mathcal{C}} B(x, t)$ est dit t-correcteur parfait.

Montrer que le code de Hamming de longueur 7 est 1-correcteur parfait mais qu'il n'est pas MDS.

Exercice 2.16. ***Codes linéaires cycliques*** *Un code linéaire cyclique est un code $\mathcal{C}$ linéaire de longueur n, stable par la permutation $T(a_1, \cdots, a_n) = (a_n, a_1, \cdots, a_{n-1})$.*

(1) En utilisant l'isomorphisme naturel d'espace vectoriel $\psi : \mathbb{F}_q^n \simeq \mathbb{F}_q[X]/Q(X)$ où $Q = X^n - 1$, montrer que $\mathcal{C} \subset \mathbb{F}_q^n$ est stable par T si et seulement si son image par ψ est un idéal. En déduire alors qu'il existe une bijection entre les codes cycliques de longueur n et les polynômes unitaires divisant $X^n - 1$.

(2) Rappeler la factorisation en irréductibles des polynômes cyclotomiques Φ_n dans $\mathbb{F}_q$, et en déduire une bijection entre les codes cycliques de longueur n et les parties $I \subset (\mathbb{Z}/n\mathbb{Z})^\times$ stables par la multiplication par q.

(3) Soit C un code linéaire cyclique de longueur n sur $\mathbb{F}_q$ associé à $I \subset (\mathbb{Z}/n\mathbb{Z})^\times$ et supposons qu'il existe i et s tels que $\{i+1, i+2, \cdots, i+s\} \subset I$. Montrer alors que $d(\mathcal{C}) \geq s + 1$.

*(4) **Codes de Hamming** : soit $n = \frac{q^r - 1}{q-1}$ et $I := \{1, q, q^2, \cdots, q^{r-1}\}$. Montrer que $d(\mathcal{C}) = 3$ ou 4 et qu'il est parfait 1-correcteur.*

Remarque : Pour $r = 3$, $q = 2$ et $n = 7$ on retrouve le code étudié précédemment.

En construisant une matrice vérificatrice montrer qu'en fait on a $d(\mathcal{C}) = 3$.

*(5) **Codes de Reed-Solomon** : ce code est utilisé dans les CD. Soit $n = q - 1$ et soit α un générateur de $\mathbb{F}_q^\times$. Pour k fixé on pose*

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

Montrer que le code linéaire cyclique correspondant est MDS et que pour $q = 2^f$, on a $2t + 1 \leq d(\mathcal{C}) = q - k$.

*(6) **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).*

(7) ***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* $d(\mathcal{G}_{2^n}) = 5, 6, 7$ *puis que* $\mathcal{G}_{23}$ *est "-correcteur parfait.*

Exercice 2.17. ***Code du minitel***

(a) Montrez que le polynôme $X^7 + X^3 + 1$ *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.*

(i) Expliquez pour quoi si $a'_0\alpha^{126} + \cdots + a'_{125}\alpha + a'_{126} = 0$ *alors il est raisonnable de penser qu'il n'y a pas eu d'erreurs de transmission. Quel est alors le message ?*

(ii) On suppose que les erreurs de transmissions 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 trouver* k *et donc le message initial.*

(iii) Commentez le choix de 128*.*

Exercice 2.18. ***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 auquels 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*-ième 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).*

3 Solutions

1.1 (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 $X+1$.

(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 ; il nous faut montrer que X^4+X+1 n'a pas de racines dans $\mathbb{F}_4$. Soit donc $x \in \mathbb{F}_4$ n'appartenant pas à $\mathbb{F}_2$; on a alors $x^3=1$ de sorte que $x^4+x+1 = x+x+1 = 1 \neq 0$. Ainsi X^4+X+1 n'a pas de racines dans les extensions de degré $\leq 4/2$ de $\mathbb{F}_2$ et est donc irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^4+X+1)$ est un corps de cardinal 16 qui est donc isomorphe à $\mathbb{F}_{16}$.

Pour savoir si X est un générateur du groupe multiplicatif, il suffit de vérifier qu'il n'est pas d'ordre 3 ou 5. Or dans la base $1, X, X^2, X^3$, $X^3-1 \neq 0$ et $X^5-1 = X^2+X+1 \neq 0$.

On cherche les éléments de $\mathbb{F}_4$ autres que $0,1$, i.e. des éléments d'ordre 3. Un candidat naturel est $X^5 = X^2+X =: \chi$, on a alors $\chi^2 = X^4+X^2$ et $\chi^2+\chi+1 = 0$ et $\chi^3 = 1$ de sorte que le sous ensemble $\{0, \chi, \chi^2, \chi^3\}$ de $\mathbb{F}_{16}$ correspond au sous-corps $\mathbb{F}_4$. En outre $X^2+\chi X+1$ n'a pas de racines dans $\mathbb{F}_2[\chi]$ et il y est donc irréductible de sorte que $\mathbb{F}_{16} \simeq \mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+YX+1)$.

(iv) A 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 $\psi(8)=4$ 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 $\mathbb{F}_9^\times$.

1.2 Evidemment $\bigcup_{n=1}^N \mathbb{F}_{p^{n!}} = \mathbb{F}_{p^{N!}}$ de sorte que $k = \bigcup_{n=1}^\infty \mathbb{F}_{p^{n!}}$ est une réunion croissante de corps et est donc 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 k 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 k 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 : En général il est pratique de fixer une clôture algébrique $\bar{\mathbb{F}}_p$ et de noter pour tout n, $\mathbb{F}_{p^n}$ **le** corps de décomposition dans $\bar{\mathbb{F}}_p$ du polynôme $X^{p^n}-X$.

1.3 (i) Les polynômes irréductibles de degré 1 sont X et $X-1$; ceux de degré 2 sont tels que $X^4-X = X(X-1)P$ ce qui donne X^2+X+1. Pour ceux de degré 3, on a $X^8-X = X(X-1)P_1P_2$ et on trouve X^3+X+1 et X^3+X^2+1. Enfin pour ceux de degré 4, on a $X^16-X = (X^4-X)Q_1Q_2Q_3$ et on trouve X^4+X+1, $X^4+X^3+X^2+X+1$ et X^4+X^3+1. En effet ceux-ci sont irréductibles car un élément j de $\mathbb{F}_4$ qui n'est pas dans $\mathbb{F}_2$ vérifie $j^3=1$ de sorte qu'il ne peut être racine des polynômes en question.

(ii) Tout polynôme de $\mathbb{F}_2[X]$ de degré 4, irréductible sur $\mathbb{F}_2$, possède une racine dans $\mathbb{F}_{2^4}$ qui est une extension de degré 2 de $\mathbb{F}_4$; on en déduit donc que sur $\mathbb{F}_4$ il se factorise en un produit de 2 polynômes irréductibles de degré 2.

(iii) Les 3 polynômes de degré 4, irréductibles dans $\mathbb{F}_2[X]$ fournissent 6 polynômes de $\mathbb{F}_4[X]$ irréductibles de degré 2 ; ceux-ci sont distincts deux à deux car les 3 polynômes de degré 4 du départ sont premiers deux à deux dans $\mathbb{F}_2$ et donc dans $\mathbb{F}_4$.

Par ailleurs étant donné un polynôme de $\mathbb{F}_4[X]$ irréductible de degré 2, en le multipliant par son conjugué par l'unique élément non trivial du groupe de Galois de $\mathbb{F}_4 : \mathbb{F}_2$, qui échange j et j^2 avec les notations précédentes, on obtient un polynôme de degré 4 à coefficient dans $\mathbb{F}_2$, car les coefficients sont invariants par le groupe de Galois, et irréductible.

(iv) On note $0, 1, j, j^2$ les éléments de $\mathbb{F}_4$ avec $1 + j + j^2 = 0$. Les polynômes de degré 1 sont $X, X-1, X-j, X-j^2$ de produit $X^4 - X$. En ce qui concerne le degré 2, $X^4 + X + 1$, $X^4 + X^3 + X^2 + X + 1$ et $X^4 + X^3 + 1$ doivent s'écrire comme le produit de 2 polynôme irréductible de degré sur $\mathbb{F}_4$. On trouve alors $X^4 + X + 1 = (X^2 + X + j)(X^2 + X + j^2)$, $X^4 + X^3 + 1 = (X^2 + jX + j)(X^2 + j^2X + j^2)$ et $X^4 + X^3 + X^2 + X + 1 = (X^2 + jX + 1)(X^2 + j^2X + 1)$.

1.4 (a) Soit d divisant n et $P \in A(d, q)$. Soit alors $K = \mathbb{F}_q[x]$ un corps de rupture de P sur $\mathbb{F}_q$; on a $[K : \mathbb{F}_q] = d$ et $K \simeq \mathbb{F}_{q^d}$ où $\mathbb{F}_{q^d}$ est **le** corps de décomposition de $X^{q^d} - X$ dans une clôture algébrique $\bar{\mathbb{F}}_q$ fixée une fois pour toute. Comme $\mathbb{F}_{q^d}$ est l'ensemble des racines de $X^{q^d} - X$, on a $x^{q^d} = x$ et comme d divise n alors x est racine de $X^{q^n} - X$. Or l'ensemble des polynômes Q de $\mathbb{F}_q[X]$ tels que $Q(x) = 0$ est l'idéal de $\mathbb{F}_q[X]$ engendré par le polynôme irréductible $P(X)$ de sorte que P divise $X^{q^n} - X$.

(b) Soit P un facteur irréductible de $X^{q^n} - X$ de degré d. Soit alors $x \in \bar{\mathbb{F}}_q$ une racine de P qui est aussi une racine de $X^{q^n} - X$ et donc $x \in \mathbb{F}_{q^n}$ et $K = \mathbb{F}_q[x]$ est un sous-corps de $\mathbb{F}_{q^n}$ de degré d. Le théorème de la base télescopique on a $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q]$ soit donc d divise n.

(c) Les racines de $X^{q^n} - X$ sont simples de sorte que les facteurs irréductibles de $X^{q^n} - X$ sont de multiplicité 1. D'après ce qui précède on a donc $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$ soit $q^n = \sum_{d|n} dI(d, q)$. La formule d'inversion de Möebius donne alors $I(n, q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$. où μ est la fonction de Möebius.

(d) On pose $nI(n, q) = q^n + \alpha_n$ avec $|\alpha_n| \leq \sum_{d=1}^{[n/2]} q^d \leq q^{n/2}/(q-1)$ qui est donc négligeable devant q^n d'où l'équivalent $I(n, q) \sim \frac{q^n}{n}$. En outre on a facilement $r_n < q^n$ et donc $I(n, q) > 0$ et donc $I(n, q) \geq 1$ de sorte qu'il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_q$.

1.5 (1) On écrit la table des carrés de $\mathbb{F}_5$, soit

x	0	1	2	-2	-1
x^2	0	1	-1	-1	1

et on remarque que 2 n'est pas un carré dans $\mathbb{F}_5$.

On vérifie rapidement que pour $P(x) := X^2 + X + 1$, $P(0)$, $P(\pm 1)$ et $P(\pm 2)$ ne sont pas nuls de sorte que P n'a pas de racine dans $\mathbb{F}_5$, étant de degré 2 il y est donc irréductible.

(3) Le corps $\mathbb{F}_5[X]/(P(X))$ est de cardinal 25 et donc isomorphe à $\mathbb{F}_{25}$ qui est un corps de décomposition de $X^{25} - X$. Par ailleurs la classe x de X dans $\mathbb{F}_5[X]/(P(X))$ vérifie $P(x) = 0$ de sorte que x est une racine de P qui étant de degré 2, y est alors totalement décomposé. On en déduit alors que P admet deux racines dans $\mathbb{F}_{25}$.

(3) Un isomorphisme $f : \mathbb{F}_5[X]/(X^2+X+1) \simeq \mathbb{F}_{25}$ étant fixée, l'image $\alpha \in \mathbb{F}_{25}$ de X par f vérifie alors $\alpha^2+\alpha+1=0$ et est donc une racine de X^2+X+1. Le sous-espace vectoriel sur $\mathbb{F}_5$ de $\mathbb{F}_{25}$ engendré par 1 et α est de dimension 2 car $\alpha \notin \mathbb{F}_5$ et est donc égal à $\mathbb{F}_{25}$ de sorte que tout élément $\beta \in \mathbb{F}_{25}$ s'écrit sous la forme $a\alpha+b$ avec $a, b \in \mathbb{F}_5$.

(4) On vérifie rapidement que P n'a pas de racine dans $\mathbb{F}_5$. Soit alors $\beta = a\alpha+b \in \mathbb{F}_{25}$; on a $\beta^5 = a^5\alpha^5+b^5 = a\alpha^5+b$. Or on a $\alpha^2 = -\alpha-1$ soit $\alpha^4 = \alpha^2+2\alpha+1 = \alpha$ et donc $\alpha^5 = \alpha^2 = -\alpha-1$. Ainsi $\beta^5-\beta+1 = \alpha(-a-a)+(b-b-a+1) \neq 0$ car $\alpha \notin \mathbb{F}_5$ soit P n'a pas de racine dans $\mathbb{F}_{25}$ de sorte qu'il est irréductible sur $\mathbb{F}_5$.

Par ailleurs, P en tant que polynôme de $\mathbb{Z}[X]$ unitaire, y est irréductible. En effet une factorisation $P = QR$ dans $\mathbb{Z}[X]$ induit par réduction modulo 5 une factorisation $\bar{P} = \bar{Q}\bar{R}$ dans $\mathbb{F}_5[X]$. Comme P est unitaire, Q et R le sont aussi, de sorte que $\deg Q = \deg \bar{Q}$ et $\deg R = \deg \bar{R}$; $\bar{P}$ étant irréductible, on en déduit que $\bar{Q}$, ou $\bar{R}$, est un polynôme constant donc, étant unitaire, égal à $\bar{1}$ et donc Q, ou R, est le polynôme constant égal à 1. Ainsi P est irréductible sur $\mathbb{Z}$ et donc irréductible sur $\mathbb{Q}$ d'après le lemme de Gauss.

1.6 (a) on vérifie rapidement que Q n'a pas de racine dans $\mathbb{F}_3$. On cherche alors ses racines dans $\mathbb{F}_9$. Pour $a \in \mathbb{F}_9$, on a $a^9 = a$ de sorte que $a^9-a+1 = 1$ et donc Q n'a pas de racine dans $\mathbb{F}_9$.

(b) Afin de calculer dans $\mathbb{F}_{27}$, on commence par le décrire concrètement : on vérifie aisément que X^3-X-1 n'a pas de racines dans $\mathbb{F}_3$ et est donc irréductible sur $\mathbb{F}_3$ et $\mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(X^3-X-1)$.

(c) Soit alors $\alpha \in \mathbb{F}_{27}$ tel que $\alpha^3 = \alpha+1$. On a alors $\alpha^9 = \alpha^3+1 = \alpha+2 = \alpha-1$ et donc finalement α est une racine de Q dans $\mathbb{F}_{27}$ de sorte que Q possède un facteur irréductible de degré 3 sur $\mathbb{F}_3$, à savoir X^3-X-1, soit $X^9-X+1 = (X^3-X-1)(X^6+X^4+X^3+X^2-X-1)$.

(d) Cherchons de manière générale toutes les racines dans $\mathbb{F}_{27}$; un élément quelconque s'écrit sous la forme $x = a\alpha^2+b\alpha+c$ avec $a, b, c \in \mathbb{F}_3$. On a alors $x^9 = a\alpha^{18}+b\alpha^9+c$ avec $\alpha^9 = \alpha-1$ et donc $\alpha^{18} = \alpha^2+\alpha+1$ de sorte que $x^9-x+1 = a\alpha+a-b+1$ ce qui impose $a = 0$ et $b = 1$ soit $x = \alpha, \alpha+1, \alpha-1$.

(e) On en déduit alors que $X^6+X^4+X^3+X^2-X-1$ n'a pas de racines dans $\mathbb{F}_{27}$ comme il n'en avait pas non plus dans $\mathbb{F}_9$, il est donc irréductible.

1.7 Si P est réductible sur $\mathbb{F}_p$, il l'est sur toute extension $\mathbb{F}_{p^m}$. Supposons donc P irréductible sur $\mathbb{F}_p$ de sorte que toutes les racines de P, vues dans $\bar{\mathbb{F}}_p$, sont dans $\mathbb{F}_{p^n}$ et aucune n'appartient à un sous-corps strict. On regarde alors P comme un polynôme dans $\mathbb{F}_{p^m}[X]$ dont on se demande s'il est encore irréductible. Il faut regarder s'il possède ou non des racines dans $\mathbb{F}_{p^{mr}}$ pour $r \leq n/2$ et donc si $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{mr}}$, soit n divise mr ce qui est possible si et seulement si n et m ne sont pas premiers entre eux. En outre en notant $d = n \wedge m$, les facteurs irréductibles sont alors de degré r un multiple de n/d.

Pour $n = 5$, la décomposition en facteur irréductible donne en prenant les degrés les décompositions suivantes de 5 : $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$. Si on veut être sur d'avoir toutes les racines (resp. au moins une racine) il faut donc se placer dans $\mathbb{F}_{p^{60}}$ (resp. $\mathbb{F}_{p^{10}}$) avec $60 = 5.4.3$ (resp. $10+5.2$).

1.8 (1) On considère le morphisme de Frobenius

$$\mathrm{Fr}_q : x \in \mathbb{F}_{q^n} \longmapsto x^q \in \mathbb{F}_{q^n}$$

dont on vérifie aisément que c'est un morphisme de corps car $\mathrm{Fr}_q(x+y) = (x+y)^q = x^q+y^q$ et $\mathrm{Fr}_q(xy) = x^q y^q$, qui laisse le corps $\mathbb{F}_q$ invariant car pour tout $x \in \mathbb{F}_q$ on a $x^q = x$. En outre

il est immédiat que le groupe engendré par Fr_q est d'ordre n de sorte que $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est de cardinal supérieur ou égal à n. Pour montrer l'inégalité inverse, soit χ un générateur de $\mathbb{F}_{q^n}^\times$ et soit μ_χ son polynôme minimal unitaire sur $\mathbb{F}_q$; on a alors $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(\mu_\chi(X))$ de sorte que μ_χ est irréductible de degré n. Ainsi tout élément $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est déterminée par $\sigma(\chi)$ qui doit être une racine de μ_χ ce qui donne au plus n choix. On en déduit ainsi $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) =< \mathrm{Fr}_q >\simeq \mathbb{Z}/n\mathbb{Z}$.

Un sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $\mathbb{Z}/r\mathbb{Z}$ pour r un diviseur de n, un générateur étant n/r. On considère alors le sous-groupe de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ engendré par $\mathrm{Fr}_q^{n/r}$; le sous-corps fixé est alors l'ensemble des éléments x de $\mathbb{F}_{q^n}$ tels que $x^{q^{n/r}} = x$ ce qui correspond au corps $\mathbb{F}_{q^{n/r}} \subset \mathbb{F}_{q^n}$. D'après l'exercice précédent, l'application de la théorie de Galois est bien une bijection.

(2) Le corps L est isomorphe à $\mathbb{F}_{p^r}$ pour un certain r et $\mathrm{Gal}(L/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$ engendré par Fr_p. En outre on a $L = \mathbb{F}_p[\chi]$ pour $\chi \in L$ une racine primitive n-ième de l'unité. Ainsi un élément $\sigma \in \mathrm{Gal}(L/\mathbb{F}_p)$ est déterminé par $\sigma(\chi)$ qui doit être une racine primitive n-ième de l'unité et donc de la forme χ^k pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. On obtient ainsi une application injective naturelle

$$\sigma \in \mathrm{Gal}(L/\mathbb{F}_p) \longmapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$$

l'image étant le groupe engendré par la classe de p. Ainsi r est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Soit $\bar{\Phi}_n(X) = P_1 \cdots P_s$ la décomposition en irréductibles de la réduction modulo p de Φ_n. Soit χ une racine de P_1 de sorte que $L = \mathbb{F}_p[\chi]$ et donc P_1 est le polynôme minimal de χ sur $\mathbb{F}_p$ et donc $\deg P_1 = [L : \mathbb{F}_p]$. En conclusion tous les P_i sont de même degré $[L : \mathbb{F}_p]$ et donc $s = \frac{\psi(n)}{[L:\mathbb{F}_p]}$ où l'on rappelle que $[L : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ainsi $p \equiv 1 \mod n$ est équivalent à demander que $\bar{\Phi}_n$ est totalement décomposé sur $\mathbb{F}_p$ ce qui on vient de le voir, est équivalent à demander que $\bar{\Phi}_n$ a une racine dans $\mathbb{F}_p$. Soit donc p premier divisant $\Phi_n(N!) \equiv 1 \mod N!$ soit $p > N$ et $p \equiv 1 \mod n$ car $\bar{\Phi}_n$ a pour racine $\bar{N}!$. On vient donc de montrer une version faible du théorème de progression arithmétique dont l'énoncé fort est que pour tout a premier avec n, il existe une infinité de premiers congrus à a modulo n, ceux-ci se répartissant de manière uniforme en un sens que l'on ne précise pas ici, sur les $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

1.9 (i) Le polynôme $X^4 + 1$ est le huitième polynôme cyclotomique Φ_8 qui est irréductible. On peut aussi le voir directement en considérant $\Phi_8(X + 1)$ qui est un polynôme d'Eisenstein pour 2.

Modulo 2, on a $X^4 + 1 = (X + 1)^4$ et pour $p \neq 2$, $\mathbb{F}_{p^2}^\times$ est cyclique d'ordre $p^2 - 1$ qui est divisible par 8. Soit alors $x \in \mathbb{F}_{p^2}^\times$ d'ordre 8, on a $x^8 = (x^4)^2 = 1$ et $x^4 \neq 1$ soit $x^4 = -1$ de sorte que Φ_8 a une racine dans $\mathbb{F}_{p^2}$ et donc Φ_8 est réductible modulo p.

(ii) Avec les hypothèses de l'énoncé $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique. D'après loc. cit., la réduction modulo p de ψ_n est un produit de polynômes irréductibles qui ont tous le même degré à savoir l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi ψ_n est irréductible modulo p si et seulement si p engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ ce qui ne se peut pas si ce dernier groupe n'est pas cyclique.
Remarque : On a ainsi une famille d'exemples de polynômes irréductibles sur $\mathbb{Z}$ et réductible modulo tout premier p.

1.10 modulo 2, on a $\bar{P} = X^4 + X^2 + 1 = (X^2 + X + 1)^2$, modulo 3, $\bar{P} = X^4 + 2X^3 + 2X + 2 = (X^2 + 1)(X^2 + 2X + 2)$ et modulo 5, $\bar{P} = X^4 + X^2 + 1$ qui n'a pas de racine dans $\mathbb{F}_5$; regardons dans $\mathbb{F}_{25}$. Comme $\mathbb{F}_{25}^\times \simeq \mathbb{Z}/24\mathbb{Z}$, soit x un élément d'ordre 6 : $x^6 = 1$ avec $x^2 \neq 1$ et $x^3 \neq 1$.

Soit $y = x^2$ de sorte que $y^3 - 1 = (y-1)(y^2+y+1) = 0$ et $y \neq 1$ soit $y^2 + y + 1 = 0$ et donc x est une racine de $\bar{P} = (X^2+X+1)(X^2+4X+1)$.

Sur $\mathbb{Z}$, P n'a pas de racine car sinon il en aurait modulo 2 ce qui n'est pas. Si P était réductible, on aurait alors $P(X) = (X^2+aX+b)(X^2+cX+d)$ et donc

$$\begin{cases} a+c = 10 \\ b+d+ac = 21 \\ ad+bc = -10 \\ bd = 11 \end{cases}$$

Ainsi on obtient soit $\{b,d\} = \{1,11\}$ et donc $ac = 9$ et $\{a,c\} = \{-1,-9\}$ car $a+c = -10$, et $ad+bc \neq -10$; soit $\{b,d\} = \{-1,-11\}$ et $ac = 33$ et $a+c \neq -10$. Ainsi P est irréductible sur $\mathbb{Z}$.

1.11 (i) Si $x = a/b \in \mathbb{Q}$ avec $(a,b) = 1$, est une racine de P alors comme P est unitaire on a b divise 1 et donc $x \in \mathbb{Z}$. En outre modulo 2, $x^{l+1} - x + 1 \equiv 1 \mod 2$ de sorte que P n'a pas de racine modulo 2 et donc n'a pas de racine dans $\mathbb{Z}$.

(ii) Modulo p, on a $\bar{P} = X(X-1)\bar{\Phi}_l$; il suffit donc de prouver que $\bar{\Phi}_l$ est irréductible ce qui découle d'un exercice précédent car p engendre $(\mathbb{Z}/l\mathbb{Z})^\times$. On peut en donner une preuve directe en considérant pour $1 \leq n < (l+1)/2$, $x \in \mathbb{F}_{p^n}$ une racine de $\bar{\Phi}_l$. On a $x \neq 1$ car $\bar{\Phi}_l(1) = \bar{l} \neq 0$ et $x^{l+1} = x$ avec l premier implique que l est l'ordre de x dans $\mathbb{F}_{p^n}^\times$ et donc l divise $p^n - 1$ soit $p^n \equiv 1 \mod l$. Or comme p engendre $(\mathbb{Z}/l\mathbb{Z})^\times$, on en déduit que n est un multiple de $l-1$ ce qui contredit le fait que $n < (l+1)/2$.

(iii) Modulo 2, $\bar{P}$ admet donc un diviseur de degré 2 qui est donc irréductible car $\bar{P}$ n'a pas de racine. Or sur $\mathbb{F}_2$, il y a un unique polynôme irréductible de degré 2, à savoir X^2+X+1. Ainsi sur $\mathbb{F}_4$, on doit avoir $P(j) = 0$ où j est un générateur de $\mathbb{F}_4^\times$, soit $j^{l+1} = j+1 = j^2$ et donc $l+1 \equiv 2 \mod 3$ ce qui n'est pas.

1.12 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 $p \equiv 1, 5 \mod 8$. A 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 :

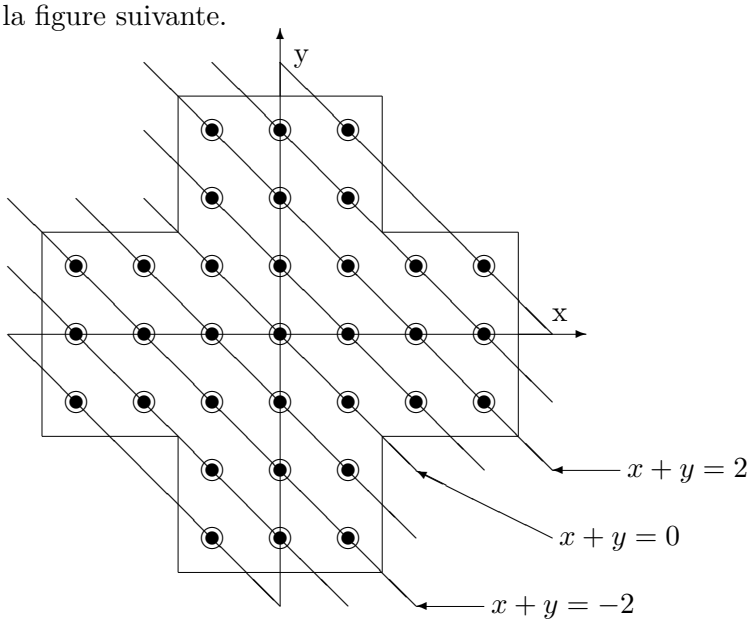
- $(\frac{p}{3}) = (-1)^{(p-1)/2} = 1$ soit $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$ soit $p \equiv 1 \mod 12$;
- $(\frac{p}{3}) = (-1)^{(p-1)/2} = -1$ soit $p \equiv -1 \mod 3$ et $p \equiv -1 \mod 4$ soit $p \equiv -1 \mod 12$;

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.

1.13 (1) Prenons par exemple le mouvement élémentaire de la figure (1.0.13). 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 $(j^{x_0+y_0}, j^{x_0-y_0})$.

1.14 Soit $p_1, \cdots, p_n$ tels que pour tout $p \neq p_i$, n est un carré modulo p. Supposons n sans facteur carré et distinct de $\pm 1, \pm 2$. On écrit $n = hl_1 \cdots l_k$ avec $h \in \{\pm 1, \pm 2\}$ et où les l_i sont premiers impairs distincts ($k \geq 1$). Il existe un entier naturel a tel que :

$$a \equiv 1 \mod 8p_1 \cdots p_n l_1 \cdots l_{k-1} \text{ et } a \equiv r \mod l_k$$

D'après la loi de réciprocité quadratique on a

$$(\frac{n}{a}) = (\frac{l_1 \cdots l_k}{a}) = \prod_i (\frac{a}{l_i}) = (\frac{1}{l_1}) \cdots (\frac{1}{l_{k-1}})(\frac{r}{l_k}) = -1$$

de sorte que a a un diviseur premier p distinct des p_i tel que $(\frac{n}{p}) = -1$, d'où la contradiction.