Correction feuille 1

1 Nombres premiers

Exercice 1. *Soient p et q des nombres premiers distincts.*

(a) Quel est le cardinal de $(\mathbb{Z}/pq\mathbb{Z})^*$? Combien y a-t-il d'éléments de $(\mathbb{Z}/pq\mathbb{Z})^*$ égaux à leur inverse ?

(b) Montrer la congruence :

$$\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}} \equiv 1 \bmod pq$$

(même méthode que pour le théorème de Wilson: $(p-1)! \equiv -1 \mod p$).

Preuve : (a) D'après le lemme chinois, on a $(\mathbb{Z}/pq\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ de sorte que ce dernier est de cardinal $(p-1)(q-1)$. Les éléments x égaux à leur inverse sont ceux qui vérifient $x^2 = 1$, i.e. ce sont ceux d'ordre divisant 2, ce qui donne 4 éléments à savoir $(\pm 1, \pm 1)$ soit $x = \pm 1, x_1, x_2$ avec $x_i \equiv (-1)^i \mod p$ et $x_i \equiv (-1)^{i-1} \mod q$, pour $i = 1, 2$.

(b) On considère alors le produit de tous les éléments de $(\mathbb{Z}/pq\mathbb{Z})^\times$ soit le produit des $pq-1$ premiers entiers auxquels il faut enlever tous les multiples de p ainsi que tous les multiples de q. Les multiples de p (resp. q) sont $p, 2p, \cdots, (q-1)p$ (resp. $q, 2q, \cdots, (p-1)q$), de sorte que le produit en question est $\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}}$. Par ailleurs en regroupant les nombres distincts de $\pm 1, x_1, x_2$ avec leur inverse ce produit est égal à $a = 1(-1)x_1x_2$. Or par le lemme chinois, on a $a \equiv 1 \mod p$ et $a \equiv 1 \mod q$ de sorte que $a \equiv 1 \mod pq$, d'où le résultat.

Exercice 2. *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.

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 $p \equiv 1, 5 \mod 8$. 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.

Exercice 3. *Etude des premiers nombres de Fermat.*
On pose pour tout $n\in\mathbb{N}$, $F_n=2^{2^n}+1$; F_n est par définition le n-ième nombre de Fermat.

(a) Soit $m\in\mathbb{N}\backslash\{0\}$. En utilisant la factorisation

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

prouver que si 2^m+1 est premier alors m est une puissance de 2.

(b) Calculer F_n pour $n\leq 4$ et vérifiez qu'ils sont tous premiers.

(c) Montrer que tout diviseur premier de F_5 est de la forme $64k+1$.

(d) Montrer que F_5 est divisible par $641=1+5.2^7=5^4+2^4$.

(e) Montrer que pour $n\neq m$, F_n et F_m sont premiers entre eux et en déduire l'existence d'une infinité de nombres premiers.

(f) Soit $p=F_n$ premier; montrer qu'un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ est générateur si et seulement s' il n'est pas un carré. En utilisant la loi de réciprocité quadratique, montrer que $3,5,7$ sont des générateurs de $(\mathbb{Z}/p\mathbb{Z})^*$ pour $n\geq 2$. En déduire alors le critère de Pépin : $p=F_n$ est premier si et seulement si $3^{(p-1)/2}\equiv -1 \mod p$.

Preuve :
(a) On écrit m sous la forme 2^nk avec k impair. Si $k>1$, on a alors l'égalité

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

On obtient alors un diviseur propre $2^{2^n}+1$ d'où la contradiction, soit $k=1$ et m est une puissance de 2.

(b) On trouve $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$ et $F_4=65537$ et l'on vérifie aisément qu'ils sont tous premiers.

(c) Soit p premier divisant F_5, on a alors $2^{2^5}=-1$ dans $\mathbb{Z}/p\mathbb{Z}$ et 2^6 est l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Or l'ordre d'un élément divise le cardinal du groupe de sorte que 2^6 divise $p-1$, d'où le résultat.

(d) On vérifie que 641 est premier. Dans le corps $\mathbb{Z}/641\mathbb{Z}$, on a $0=641=1+5.2^7$ soit $2^7=-5^{-1}$. 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 $F_5=(-5^{-1})^4.2^4+1=(2^4+5^4)/5^4=0$.

(e) Supposons $n=m+r$ avec $r>0$. 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 que $\mathcal{P}$ est infini.

(f) Soit x un générateur de $\mathbb{Z}/p\mathbb{Z}$; s'il existe y tel que $x=y^2$ alors y est aussi un générateur mais alors y^2 serait d'ordre $(p-1)/2$ et donc non générateur. Réciproquement si x n'est pas un résidu quadratique alors $x^{(p-1)/2}\equiv -1 \mod p$ et puisque l'ordre de x est une puissance de 2 alors cet ordre est exactement $p-1$.

D'après la loi de réciprocité quadratique, pour $p\neq 3$, 3 est résidu quadratique modulo p si et seulement si p est résidu quadratique modulo 3; or $p\equiv 2 \mod 3$ qui n'est pas résidu quadratique modulo 3. De même pour $p\neq 5$, 5 est résidu quadratique modulo p si et seulement si p est résidu quadratique modulo 5; or $p=4^{2^{n-1}}+1\equiv 2$

mod 5 et 2 n'est pas résidu quadratique modulo 5. De même pour $p \neq 3, 7$ est résidu quadratique modulo p si et seulement si p est résidu quadratique modulo 7; or $p \equiv 3, 5 \mod 7$ qui ne sont pas résidus quadratiques.

Supposons la congruence vérifiée; $3^{p-1} \equiv 1 \mod p$, de sorte que l'ordre de 3 modulo p est exactement $p-1$, soit $\mathbb{Z}/p\mathbb{Z}$ est un corps. Réciproquement supposons $p \neq 3$ premier, il suffit alors de montrer que 3 n'est pas un résidu quadratique modulo p; or $p \equiv 2 \mod 3$ qui n'est pas résidu quadratique modulo 3 et donc 3 n'est pas résidu quadratique modulo p.

Exercice 4. *Le but de cet exercice est d'étudier les nombres de Mersenne $M_p = 2^p - 1$ pour p premier. On veut en particulier montrer le test de primalité de Lucas-Lehmer: M_q est premier ($q \geq 3$ premier) si et seulement si $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$.*

(i) Montrez que si $a^n - 1$ est premier alors $a = 2$ et n est premier.

(ii) Montrez que l'anneau $A = \mathbb{Z}[\sqrt{3}]$ est euclidien et caractérisez les unités.

(iii) Remarquez que pour q impair, $2^q - 1 \equiv 7 \mod 12$ et en déduire qu'il existe un premier $p \not\equiv \pm 1 \mod 12$ divisant $2^q - 1$ et remarquer que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. Montrez que si M_q vérifie la congruence ci-dessus, alors $p = M_q$.

(iv) En utilisant la loi de réciprocité quadratique, montrez que 3 est un résidu quadratique modulo $p \neq 2, 3$ si et seulement si $p \equiv \pm 1 \mod 12$. Pour $p > 3$ premier non congru à ± 1 modulo 12, montrez le petit théorème de Fermat suivant dans $\mathbb{Z}[\sqrt{3}]$: $(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \mod p$.

On suppose désormais M_q premier. En remarquant que 2 est un carré modulo M_q, on définit dans $\mathbb{Z}[\sqrt{3}]/(M_q)$: $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$ et $\bar{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$. A partir des relations $\tau^2 = 2+\sqrt{3}$ et $\tau\bar{\tau} = -1$, en déduire la congruence de l'énoncé.

(v) Montrez le test de primalité suivant sur M_q pour $q \geq 3$ premier: 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 $L_{q-2} \equiv 0 \mod M_q$.

Preuve : (i) On a la factorisation $a^{pq} - 1 = (a^p - 1)(a^{p(q-1)} + \cdots + a^p + 1)$ de sorte que si M_n irréductible alors $a = 2$ et n premier.

(ii) On considère le sthasme $v : x + y\sqrt{3} \mapsto |x^2 - 3y^2|$, soit la valeur absolue de la norme N. Soient alors $\alpha, \beta \in\in \mathbb{Z}[\sqrt{3}]$; $\alpha/\beta = r + s\sqrt{3}$ avec $r, s \in \mathbb{Q}$ que l'on approxime par des entiers x, y avec une erreur inférieure à $1/2$: $|x-r| \leq 1/2$ et $|y-s| \leq 1/2$. On obtient alors $-3/4 \leq (r-x)^2 - 3(s-y)^2 \leq 1/4$ soit $v(\alpha/\beta - (x+y\sqrt{3})) \leq 3/4$ et donc $v(\alpha - \beta(x+y\sqrt{3})) < v(\beta)$.

Si $z \in \mathbb{Z}[\sqrt{3}]$ est inversible alors $N(zz^{-1}) = N(z)N(z^{-1})$ et donc $N(z) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement si $N(x + y\sqrt{3}) = \epsilon = \pm 1$ alors $\epsilon(x - y\sqrt{3})$ est son inverse. En particulier $2 + \sqrt{3}$ est inversible d'inverse $2 - \sqrt{3}$. On remarquera par ailleurs que $a^2 - 3b^2$ est un carré modulo 3 de sorte qu'il ne peut pas être congru à -1 modulo 3. Ainsi $a + b\sqrt{3}$est inversible si et seulement si $a^2 - 3b^2 = 1$.
Remarque: Il s'agit d'une équation de Pell-Fermat que l'on étudiera dans la feuille 4.

(iii) On a $2^q - 1 \equiv 7 \mod 12$ si et seulement si il est congru à 1 modulo 3 et -1 modulo 4. Modulo 3, on a $2^q - 1 = (-1)^q - 1 = -2 = 1 \mod 3$; modulo 4 pour $q > 2$, $2^q - 1 \equiv -1 \mod 4$.

Remarquons que 2 et 3 ne divise pas M_q pour q impair, de sorte que si p divise M_q alors $p \equiv \pm 1, \pm 5 \mod 12$; tous les diviseurs p de M_q ne peuvent pas être congrus à $\pm 1 \mod 12$ car sinon il en serait de même de M_q. Soit donc p premier divisant M_q avec $p \not\equiv \pm 1 \mod 12$ et montrons que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. On raisonne par l'absurde: $p = \alpha\beta$ soit $p^2 = N(\alpha)N(\beta)$ et $p = \pm N(\alpha)$ car β n'est pas inversible. On en déduit alors $p = \pm(x^2 - 3y^2)$; or comme $x^2 - 3y^2$ est un nombre premier distinct de $\pm 2, \pm 3$, on a alors $x^2 - 3y^2 \equiv 1 \mod 3$ et $x^2 - 3y^2 \equiv 1 \mod 4$ soit $p \equiv \pm 1 \mod 12$ ce qui n'est pas.
Remarque: Une autre façon de voir le résultat est la suivante: p est irréductible si et seulement si $\mathbb{Z}[\sqrt{3}]/(p)$ est un corps. Or cet anneau est isomorphe à $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 - 3)$: c'est un corps si et seulement si $X^2 - 3$ est irréductible ce qui revient à dire qu'il n'a pas de racines; autrement dit p est irréductible si et seulement si 3 n'est pas un carré modulo p, i.e. si et seulement si $p \neq \pm 1 \mod 12$.

Supposons que $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$, on va alors montrer que $p = M_q$. Comme $\mathbb{Z}[\sqrt{3}]$ est principal, et p est irréductible, alors le quotient $(\mathbb{Z}[\sqrt{3}]/(p))^\times$ est un corps de cardinal p^2. La congruence $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$ montre alors que l'ordre de $2 + \sqrt{3}$ est d'ordre 2^q dans $(\mathbb{Z}[\sqrt{3}]/(p))^\times$; donc 2^q divise $p^2 - 1$. On écrit

$M_q = pa$, soit $p^2 \equiv 1 \mod M_q$ et $ap \equiv -1 \mod 2^q$ soit $ap \equiv -p^2 \mod 2^q$. Comme p est inversible modulo 2^q, on obtient $a + p \equiv 0 \mod 2^q$, or $ap < 2^q \leq a + p$ soit $(a-1)p \leq a - 1$ soit $a = 1$ et $p = M_q$.

(iii) La loi de réciprocité quadratique donne $(\frac{3}{p})(\frac{p}{3}) = (-1)^{(p-1)/2}$; donc 3 est résidu quadratique modulo p si et seulement si $(\frac{p}{3}) = (-1)^{(p-1)/2}$. Le seul carré modulo 3 autre que 0 est 1, soit $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$ ou bien $p \equiv 2 \mod 3$ et $p \equiv 3 \mod 4$, soit en définitive $p \equiv \pm 1 \mod 12$.

Par hypothèse 3 n'est pas un carré modulo p et par conséquent $\sqrt{3}^p = 3^{(p-1)/2}\sqrt{3} \equiv -\sqrt{3} \mod p$ et donc $(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \mod p$. On considère les éléments $\tau, \bar{\tau}$ de l'énoncé; $\tau^p = \bar{\tau}$ soit $\tau^{p+1} = -1$ ce qui donne la congruence de l'énoncé $(\tau^2)^{(p+1)/2} \equiv -1 \mod p$ car $\tau^2 = 2 + \sqrt{3}$.

(iv) En posant $\alpha = 2 + \sqrt{3}$ et $\bar{\alpha} = 2 - \sqrt{3}$, en remarquant que $\alpha\bar{\alpha} = 1$, on montre aisément par récurrence que $L_i = \alpha^{2^i} + \bar{\alpha}^{2^i}$; la congruence $L_i \equiv 0 \mod n$ est ainsi équivalente à $\alpha^{2^{i+1}} \equiv -1 \mod n$, d'où le résultat.

Exercice 5. *Un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \mod n$.*

(a) Montrez que $n = 105 = 3.5.7$ est pseudo-premier de base 13 mais qu'il ne l'est pas de base 2.

(b) Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p. Réciproquement un nombre n est dit de Carmichael s'il est pseudo-premier de base b pour tout b premier avec n, sans être premier. Montrez que $n = 561 = 3.11.17$ est un nombre de Carmichael.

(c) 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:

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

(i) Montrez que si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leq b < n$ et qui si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b.

(ii) Montrez que $n = 561$ n'est pas fortement pseudo-premier de base 2.

(iii) Pour n impair soit

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

On veut montrez le théorème de Rabin: si n est non premier alors $\frac{|B_n|}{\phi(n)} \leq 1/4$ sauf pour $n = 9$. Sous une autre forme, si $|B_n| \geq \phi(n)/4$ alors n est premier.

(α) Considérons $p_1 \equiv 3 \mod 4$ premier tel que $p_2 = 2p_1 - 1$ soit premier (exemple $p_1 = 40039, 41011, 42727$) Montrez alors que pour $n = p_1 p_2$, on a $4|B_n| = \phi(n)$.

(β) Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en facteurs premiers de $n = 1 + 2^k q$, q impair; on écrit $p_i = 1 + 2^{k_i} q_i$ avec q_i impair et $k_1 \leq \cdots \leq k_r$. Montrez alors que

$$|B_n| = (q, q_1) \cdots (q, q_r)(1 + \sum_{j=0}^{k_1 - 1} 2^{jr})$$

En déduire que $\frac{|B_n|}{\phi(n)} \leq \frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{k_1 r}} K$, avec $K = \prod_{i=1}^r \frac{(q, q_i)}{q_i p_i^{\alpha_i - 1}}$. En outre si tous les k_i ne sont pas tous égaux, on peut améliorer l'inégalité précédente d'un facteur 2.

(γ) Montrez le résultat dans le cas où n est une puissance d'un nombre premier, puis traitez le cas général.

Remarque: 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.

Preuve : (a) 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 $2^{104} = (2^6)^{17} \times 2^2 \equiv 4 \mod 7$.

(b) Il suffit de remarquer que 560 est multiple de $2, 10, 15$ et par suite $x^{560} \equiv 1$ dans $(\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$, dans $(\mathbb{Z}/11\mathbb{Z})^\times \simeq \mathbb{Z}/10\mathbb{Z}$ et dans $(\mathbb{Z}/17\mathbb{Z})^\times \simeq \mathbb{Z}/16\mathbb{Z}$ et donc dans $(\mathbb{Z}/561\mathbb{Z})^\times$ d'après le lemme chinois.

(c) (i) Si n est premier alors $b^{2^k q} \equiv 1 \mod n$ 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 $x = \pm 1$.
Si n est fortement premier de base b, 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 $b^{n-1} \equiv 1 \mod n$.

(ii) On a vu que $n = 561$ est pseudo-premier de base 2 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 $2^{352^2} \equiv 67 \mod 561$.

(iii) (α) On écrit $p_1 = 1 + 2q_1$ et $p_2 = 1 + 4q_1$ avec q_1 impair; $n - 1 = 2q_1(3 + 4q_1) = 2^k q$, soit $k = 1$ et $q = q_1(3 + 4q_1)$. L'ensemble B_n est la réunion disjointe de

$$P_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^q = 1\} \qquad Q_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^q = -1\}$$

Le théorème chinois donne avec des notations évidentes $|P_n| = |P_{p_1}||P_{p_2}|$ et $|Q_{p_1}||Q_{p_2}|$. Or comme $(\mathbb{Z}/p_1\mathbb{Z})^\times$ est cyclique d'ordre $p_1 - 1$, on a $|P_{p_1}| = (q, p_1 - 1) = (q, 2q_1) = (q, q_1) = q_1$. On calcule de même les autres cardinaux et on obtient $|B_n| = 2q_1^2$ et $\phi(n) = 8q_1^2$ d'où le résultat.

(β) L'ensemble B_n est la réunion disjointe de $P_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^q = 1\}$ et des $Q_n(j) = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^{2^j q} = -1\}$ pour $0 \leq j < k$.
- *calcul de* $|P_n|$: le théorème chinois donne $P_n \simeq \prod_{i=1}^r P_{p_i^{\alpha_i}}$ avec $|P_{p_i^{\alpha_i}}| = (q, \psi(p_i^{\alpha_i})) = (q, q_i)$.
- *cacul de* $|Q_n(j)|$: à nouveau le théorème chinois nous ramène à calculer le cardinal de $Q_{p_i^{\alpha_i}}(j)$: or ce dernier ensemble est non nul si et seulement si $(-1)^{\frac{\psi(p_i^{\alpha_i})}{(2^j q, \psi(p_i^{\alpha_i}))}} = 1$ ce qui est équivalent à $\frac{2^{k_i} q_i}{2^{\inf(j,k_i)}(q,q_i)}$ car $(2^j q, \psi(p_i^{\alpha_i})) = 2^{\inf(j,k_i)}(q, q_i)$; en effet comme p_i divise n, et que n est premier avec $n - 1 = 2^k q$ alors p_i est premier avec $n - 1$. Ainsi $Q_{p_i^{\alpha_i}}(j)$ est non vide si et seulement si $j < k_i$ et dans ce cas son cardinal est $2^j(q, q_i)$. Finalement si $j \geq k_1$ alors $Q_n(j)$ est vide et si $j < k_1$ alors $|Q_n(j)| = 2^{jr}(q, q_1) \cdots (q, q_r)$. En outre comme $p_i \equiv 1 \mod 2^{k_i}$ alors $n \equiv 1 \mod 2^{k_1}$ soit $k_1 \leq k$. Ainsi on obtient

$$\sum_{0 \leq j < k} |Q_n(j)| = \sum_{0 \leq j < k_1} |Q_n(j)| = \prod_{i=1} r(q, q_i) \sum_{0 \leq j < k_1} 2^{jr}$$

d'où le résultat en y ajoutant le calcul du cardinal de P_n.
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 $\frac{|B_{561}|}{\psi(561)} = 1/32$ est relativement faible.

On obtient ainsi

$$\frac{|B_n|}{\psi(n)} = \frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{k_1 + \cdots + k_r}} K$$

si l'on minore $k_1 + \cdots + k_r$ par rk_1, on obtient l'inégalité demandée; si en outre tous les k_i ne sont pas égaux k_1, on peut minorer $k_1 + \cdots + k_r$ par $rk_1 + 1$.

(γ) Dans le cas où $n = p^\alpha$, on obtient alors $\frac{|B_n|}{\psi(n)} \leq (q, q_1)/q_1 \leq 1/p_1^{\alpha_1 - 1}$ ce qui donne si $p_1 \geq 5$, $\frac{|B_n|}{\psi(n)} \leq 1/5$ et si $p_1 = 3$, $\frac{|B_n|}{\psi(n)} \leq 1/9$ sauf pour $\alpha = 2$, i.e. $n = 9$ auquel cas $B_9 = \{1, -1\}$ et $\psi(9) = 6$ soit $\frac{|B_9|}{\psi(9)} = 1/3$.

Dans le cas général, le rapport $\frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{rk_1}}$ qui intervient dans la majoration, est décroissant en k_1; on peut donc le remplacer par $1/2^{r-1}$, soit

$$\frac{|B_n|}{\psi(n)} \leq \frac{1}{2^{r-1}} \prod_{i=1}^r \frac{1}{p_i^{\alpha_i}}$$

Si l'un des α_i est supérieur ou égal à 2, alors $\prod_{i=1}^r \frac{1}{p_i^{\alpha_i - 1}} \leq 1/3$ et donc $\frac{|B_n|}{\psi(n)} \leq 1/6$. On suppose donc dans la suite que tous les α_i sont égaux à 1:
cas $r \geq 3$: l'inégalité $\frac{|B_n|}{\psi(n)} \leq 1/4$ est alors immédiate et l'égalité est obtenue pour $r = 3, k_1 = k_2 = k_3 = 1$ et $q_i | q$ autrement dit si la décomposition primaire de n est $(1 + 2q_1)(1 + 2q_2)(1 + 2q_3)$.
cas $r = 2$ *et* $k_1 < k_2$ d'après ce qui précède on a la majoration $\frac{|B_n|}{\psi(n)} \leq \frac{1}{2^2} \prod_{i=1}^2 \frac{(q, q_i)}{q_i} \leq 1/4$, l'égalité étant obtenue si et seulement si $k_1 = 1, k_2 = k_1 + 1 = 2$, q_1 et q_2 divisent q soit $q_1 = q_2$ et la décomposition primaire de n est $(1 + 2q_1)(1 + 4q_1)$, ce qui est le cas étudié plus haut.

cas $r = 2$ *et* $k_1 = k_2$ on a la majoration $\frac{|B_n|}{\psi(n)} \leq \frac{1}{2}\prod_{i=1}^{2}\frac{(q,q_i)}{q_i}$. Or q_1 et q_2 ne peuvent pas tous deux diviser q; en effet on a

$$n-1 = 2^k q = p_1p_2 - 1 = (1+2^{k_1}q_1)(1+2^{k_1}q_2) - 1 = 2^{k_1}(q_1+q_2) + 2^{2k_1}q_1q_2$$

et si $q_1|q$ (resp. $q_2|q$) entraine $q_1|q_2$ (resp. $q_2|q_1$) soit $q_1 = q_2$ puis $p_1 = p_2$ ce qui n'est pas. On en déduit alors $\frac{(q,q_i)}{q_i} \leq 1/3$ pour $i = 1$ ou 2 soit $\frac{|B_n|}{\psi(n)} \leq 1/6$.

2 Corps finis

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

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 $X+1$.

(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 $\mathbb{F}_9^\times$.

Exercice 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* $\mathbf{F}_p$.

Preuve : 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 $X^{p^n} - X$.

Exercice 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 $\mathbb{F}_4$.

Preuve : (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 $X^4+X^3+X^2+X+1 = (X^2+jX+1)(X^2+j^2X+1)$.

Exercice 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* $+\infty$.

Preuve : (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 $\mathbb{F}_q$.

Exercice 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 $\mathbf{Q}$?

Preuve :

(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 $P(x):=X^2+X+1$, $P(0)$, $P(\pm1)$ et $P(\pm2)$ 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.

Exercice 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 $\mathbb{F}_3$.

Preuve : (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.

Exercice 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 $\mathbf{F}_{p^m}$.*

Preuve : 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. $10 + 5.2$).

Exercice 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.

Preuve : (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 $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 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 ψ_n est irréductible sur $\mathbb{Z}$. Montrer en utilisant la question (ii) de l'exercice sur la théorie de Galois des corps finis, que ψ_n est réductible modulo tout nombre premier.

Preuve : (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.

Exercice 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 $\mathbb{Q}$.

Preuve : 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 $\mathbb{Z}$.

Exercice 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 $\bar{R} = X(X-1)$.

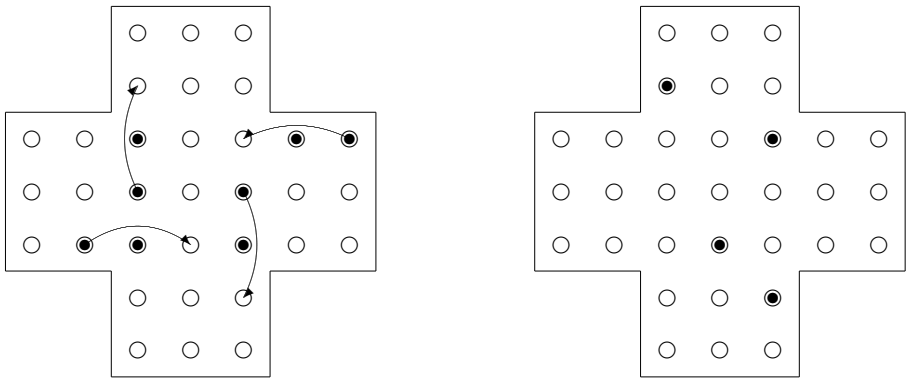
(iii) En passant modulo 2, en déduire une contradiction. Comme exemple on propose le polynôme $X^{72} - X + 47$.

Preuve : (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.

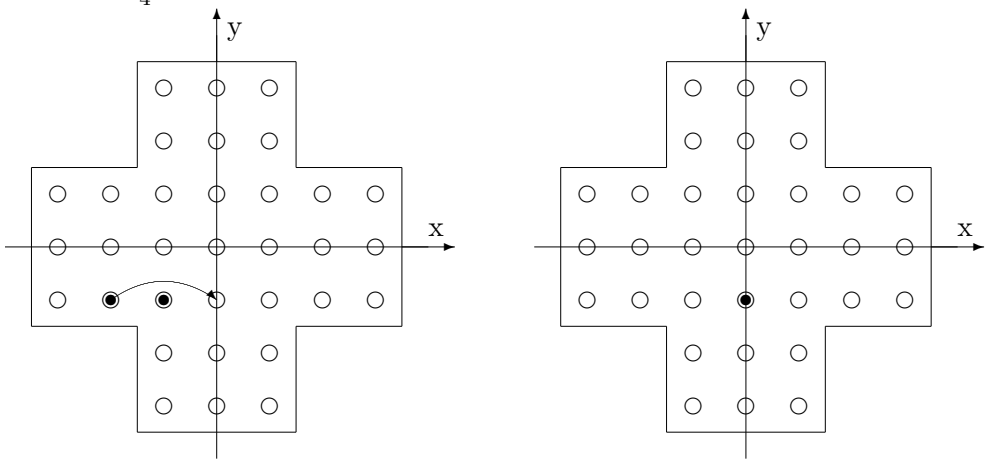
Exercice 12. *Le jeu du solitaire se joue sur un plateau disposant de 33 réceptacles (cercle vide) dans lesquels il peut y avoir des billes notés avec un cercle plein. A chaque étape on peut faire passer une bille au dessus d'une autre sur un axe vertical ou horizontal, pourvu que le réceptacle suivant 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

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

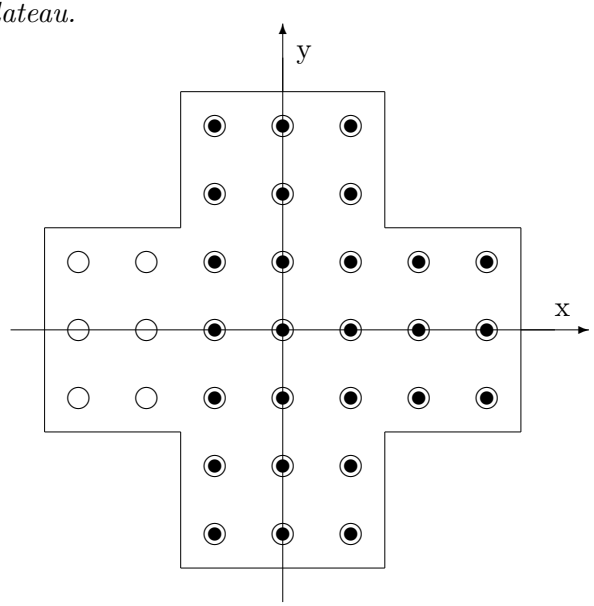
où j est un générateur de $\mathbb{F}_4^\times$.



(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.

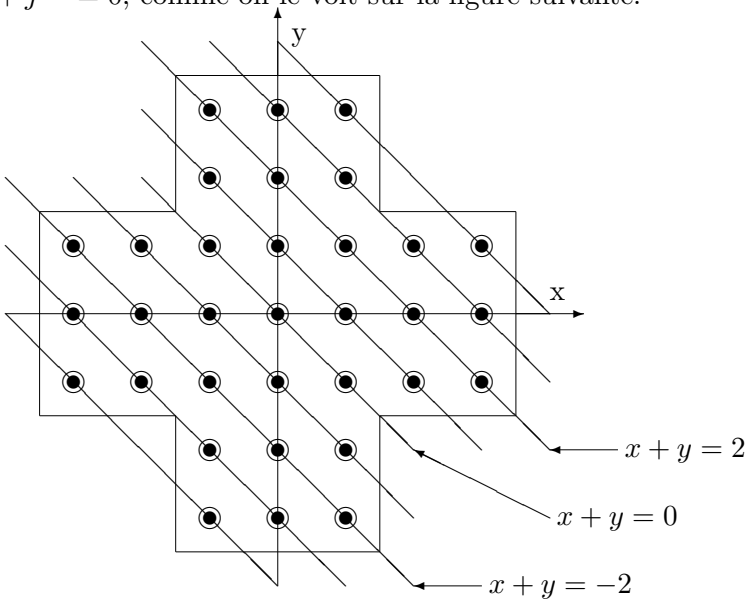


Preuve :

(1) Prenons par exemple le mouvement élémentaire de la figure (12). 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 $(j^{x_0+y_0}, j^{x_0-y_0})$.

Exercice 13. *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 $\mathbb{N}$.*

Preuve : 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.