Feuille d'exercices 2

Avertissement : tous les exercices ne seront pas traités durant les séances ; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum*.

Loi de réciprocité quadratique

Exercice 1. — *Soient G un groupe fini, d'élément neutre e, et x un élément de G d'ordre m.*

1. *Montrer que pour tout entier k, l'ordre de x^k est $\frac{m}{(m\wedge k)}$.*
2. *Soit n un entier ≥ 1. Montrer que les conditions suivantes sont équivalentes :*
   - *on a $m = n$.*
   - *On a $x^n = e$ et pour tout diviseur premier p de n, on a $x^{\frac{n}{p}} \neq e$.*

Exercice 2. — 1. *Montrer que dans un groupe fini d'ordre impair, tout élément est un carré.*

Soient G un groupe cyclique d'ordre n pair, d'élément neutre e.

2. *Montrer que G possède exactement $\frac{n}{2}$ éléments qui sont des carrés.*
3. *Soit a un élément de G. Montrer l'équivalence*
$$a \text{ est un carré dans } G \iff a^{\frac{n}{2}} = e.$$
4. *Supposons que n soit une puissance de 2. Montrer que l'ensemble des générateurs de G est l'ensemble des éléments qui ne sont pas des carrés.*

Exercice 3. — ***Puissances dans un groupe cyclique*** *Soient G un groupe cyclique d'ordre n, d'élément neutre e, et a un élément de G.*

1. *Soit k un entier naturel. Montrer que pour qu'il existe $x \in G$ tel que $x^k = a$ il faut et il suffit que l'on ait*
$$a^{\frac{n}{d}} = e \quad \text{où} \quad d = (k \wedge n). \tag{1}$$
2. *Soit k un entier naturel tel que la condition (1) soit satisfaite. Soit x_0 un élément de G tel que $x_0^k = a$. Montrer que l'ensemble des éléments $x \in G$ tels que $x^k = a$ est*
$$\Big\{ x_0 z \;\Big|\; z \in G \text{ et } z^d = e \Big\},$$
et que son cardinal est d.
3. *On prend pour G le groupe additif $\mathbb{Z}/25\mathbb{Z}$. Déterminer dans G l'ensemble des solutions de l'équation $5x = \overline{15}$.*

Exercice 4. — 1. *Calculer le symbole de Legendre $\left(\frac{754}{7}\right)$.*

2. *Soit p un nombre premier impair. Démontrer l'égalité*
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$
En déduire que 2 est un carré dans $\mathbb{F}_p$ si et seulement si on a $p \equiv \pm 1 \mod 8$.

Indication *: soit A l'anneau quotient $\mathbb{F}_p[X]/(X^4+1)$. Il contient un sous-anneau isomorphe à $\mathbb{F}_p$. Soit α la classe de X modulo (X^4+1). C'est un élément inversible de A. Posons $y = \alpha + \alpha^{-1} \in A$. Montrer que l'on a $y^2 = 2$. Déterminer ensuite y^p et utiliser le critère d'Euler.*

3. *Soit p un nombre premier ≥ 5. Montrer que 3 est un carré dans $\mathbb{F}_p$ si et seulement si p est congru à 1 ou 11 modulo 12.*
4. *Montrer que tout résidu quadratique modulo p n'est pas un générateur de $\mathbb{F}_p^*$.*
5. *Les entiers 1236 et 1237 sont-ils des résidus quadratiques modulo 101 ?*
6. *Soit p un nombre premier distinct de 5. Trouver une condition nécessaire et suffisante portant sur le dernier chiffre décimal de p pour que 5 soit un carré dans $\mathbb{F}_p$.*

Exercice 5. — 1. *Calculer le symbole de Jacobi $\left(\frac{254}{1003}\right)$. Soit n un entier impair ≥ 1.*

2. *Montrer que l'on a*
$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \quad et \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$
3. *Soit a un entier relatif. Montrer l'implication*
$$\left(\frac{a}{n}\right) = -1 \implies a \text{ n'est pas un carré modulo } n,$$
et que la réciproque est fausse en général.
4. *Supposons n divisible par le carré d'un nombre premier. Trouver un entier b premier à n tel que l'on ait*
$$\left(\frac{b}{n}\right) = 1 \quad et \quad b^{\frac{n-1}{2}} \not\equiv 1 \mod n.$$

Exercice 6. — ***Carrés dans*** $\mathbb{Z}/p^r\mathbb{Z}$ *Soit p un nombre premier impair.*

1. *Soient n un entier ≥ 1 et a un entier. Montrer que l'on a les congruences*
$$(1+p^n a)^p \equiv 1 + p^{n+1}a \mod p^{n+2} \quad et \quad (1+pa)^{p^n} \equiv 1 + p^{n+1}a \mod p^{n+2}.$$
2. *Soit n un entier non divisible par p. Montrer que si n est un résidu quadratique modulo p, c'est aussi un résidu quadratique modulo toutes les puissances de p. Autrement dit, pour tout $r \geq 1$, on a l'implication*
$$\left(\frac{n}{p}\right) = 1 \implies \text{il existe } a \in \mathbb{Z} \text{ tel que } n \equiv a^2 \mod p^r.$$
3. *Soient n un entier impair et r un entier ≥ 3. Montrer que n est un résidu quadratique modulo 2^r si et seulement si on a $n \equiv 1 \mod 8$.*

Exercice 7. — *Posons $F = X^4 + 1 \in \mathbb{Z}[X]$.*

1. *Montrer que F est irréductible dans $\mathbb{Z}[X]$.*
2. *Montrer que pour tout nombre premier p, le polynôme de $\mathbb{F}_p[X]$ déduit de F en réduisant ses coefficients modulo p est réductible dans $\mathbb{F}_p[X]$.*
3. *Expliciter un polynôme de $\mathbb{Z}[X]$, sans racines dans $\mathbb{Z}$, et possédant une racine modulo p pour tout nombre premier p.*

Exercice 8. — ***Racines carrées dans*** $\mathbb{F}_p$ *Soient p un nombre premier et a un élément de $\mathbb{F}_p^*$ qui soit un carré dans $\mathbb{F}_p$. Cet exercice concerne la détermination d'une racine carrée x de a dans $\mathbb{F}_p$.*

1. *Si $p \equiv 3 \mod 4$, montrer que $x = \pm\, a^{\frac{p+1}{4}}$.*
2. *Supposons $p \equiv 5 \mod 8$. Justifier l'égalité $a^{\frac{p-1}{4}} = \pm 1$. Montrer que l'on a*
$$x = \pm a^{\frac{p+3}{8}} \quad si \quad a^{\frac{p-1}{4}} = 1 \quad et \ que \quad x = \pm\, 2a(4a)^{\frac{p-5}{8}} \quad si \quad a^{\frac{p-1}{4}} = -1.$$
Le cas où $p \equiv 1 \mod 8$ est moins simple. En toute généralité, on peut procéder comme suit, que p soit ou non congru à 1 modulo 8. On écrit $p-1$ sous la forme
$$p - 1 = 2^e q \quad avec \quad q \text{ impair.}$$
Soit G la partie 2-primaire du groupe $\mathbb{F}_p^*$, i.e. le sous-groupe de $\mathbb{F}_p^*$ formé des éléments d'ordre une puissance de 2. Le groupe G est cyclique d'ordre 2^e. Soit z l'un de ses générateurs.
3. *Montrer que a^q appartient à G et que a^q est un carré dans G.*
4. *Montrer qu'il existe un entier pair k tel que $a^q z^k = 1$ avec $0 \leq k < 2^e$. En déduire que $x = a^{\frac{q+1}{2}} z^{\frac{k}{2}}$ est une racine carrée de a dans $\mathbb{F}_p$.*
5. *Application : montrer que 5 est un carré dans $\mathbb{F}_{29}$ et déterminer ses racines carrées.*

Exercice 9. — ***Symbole de Zolotarev*** *Pour m premier avec n, soit $\binom{m}{n}_Z$ le symbole de Zolotarev défini comme la signature de la permutation $s_n(m)$ correspondant à la multiplication par m dans $\mathbb{Z}/n\mathbb{Z}$.*

1. *Montrer que le symbole de Zolotarev est multiplicatif en la variable m, $\binom{mm'}{n}_Z = \binom{m}{n}_Z \binom{m'}{n}_Z$.*

2. *Pour p premier et n non divisible par p, en utilisant les involutions de $\mathbb{Z}/p\mathbb{Z}$*
$$\alpha : \begin{cases} 0 \mapsto 0 \\ x \mapsto x^{-1} \text{ si } x \neq 0 \end{cases} \quad ; \quad \beta : \begin{cases} 0 \mapsto 0 \\ x \mapsto nx^{-1} \text{ si } x \neq 0. \end{cases}$$
montrez que le symbole de Zolotarev $\binom{n}{p}_Z$ est égal au symbole de Legendre $\binom{n}{p}$.

3. *On fixe n et m des entiers impairs premiers entre eux. On range de trois manières différentes les entiers de 0 à $mn-1$ en définissant trois matrices de taille (m,n) notés V, H et D :*
   - *V correspond à un remplissage vertical soit $V = (v_{i,j}$ avec $v_{i,j} = m(j-1)+i-1$;*
   - *H correspond à un remplissage horizontal soit $H = (h_{i,j})$ avec $h_{i,j} = n(i-1)+j-1$;*
   - *D correspond à un remplissage diagonal soit $D = (d_{i,j})$ où $d_{i,j}$ est l'unique entier compris entre 0 et $mn-1$ congru à $i-1$ modulo m et $j-1$ modulo n.*

   On considère les permutations suivantes :
   - *$\sigma_{D,V} : v_{i,j} \mapsto d_{i,j}$;*
   - *$\sigma_{H,D} : d_{i,j} \mapsto h_{i,j}$;*
   - *$\sigma_{V,H} : h_{i,j} \mapsto v_{i,j}$.*

   Montrer que :
   (a) *$\sigma_{V,H} \circ \sigma_{H,D} \circ \sigma_{D,V} = id$;*
   (b) *$\epsilon(\sigma_{D,V}) = \binom{m}{n}_Z$;*
   (c) *$\epsilon(\sigma_{H,D}) = \binom{n}{m}_Z$;*
   (d) *$\epsilon(\sigma_{V,H}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.*

4. *Déduire de ce qui précède la loi de réciprocité quadratique.*

5. *Montrer que le symbole de Zolotarev est égal au symbole de Jacobi et en déduire la loi de réciprocité quadratique du symbole de Jacobi.*

6. *Montrer que pour tout n impair le symbole de Jacobi $\binom{2}{n} = (-1)^{\frac{n^2-1}{8}}$.*

Exercice 10. — ***Réciprocité quadratique via les résultants*** *L'idée est d'utiliser la relation*
$$\mathrm{Res}(P,Q) = (-1)^{\deg P . \deg Q}\mathrm{Res}(Q,P)$$
et de choisir des polynômes P et Q de degré respectifs $\frac{p-1}{2}$ et $\frac{q-1}{2}$, où p et q sont des premiers impairs distincts, de sorte que
$$\mathrm{Res}(P,Q) = (\frac{p}{q}) \text{ et } \mathrm{Res}(Q,P) = (\frac{q}{p}).$$

1. *Pour tout p premier impair, montrer qu'il existe un polynôme $Q_p \in \mathbb{Z}[X]$ tel que*
$$X^{p-1} + X^{p-2} + \cdots + X + 1 = X^{(p-1)/2} Q_p(X + \frac{1}{X}).$$

2. *Pour $p \neq q$ des nombres premiers impairs, montrer que le résultant de Q_p et Q_q est égal à ± 1.*

3. *Pour $p \neq q$ des nombres premiers distincts, montrer que*
$$\mathrm{Res}(Q_p, Q_q) = (\frac{q}{p}).$$

4. *Déduire de ce qui précède la loi de réciprocité quadratique.*

Exercice 11. — *Soient n un entier tel que pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p. Montrer alors que n est un carré dans $\mathbb{Z}$.*

1. Solutions

1 1) Soit d le plus grand commun diviseur de m et k. On a d'abord $(x^k)^{\frac{m}{d}} = (x^m)^{\frac{k}{d}} = e$, où e est l'élément neutre de G (car $x^m = e$). Considérons alors un entier u tel que $(x^k)^u = e$. L'entier m divise uk (car m est l'ordre de x) et donc m/d divise aussi uk/d. Les entiers m/d et k/d étant premiers entre eux, il en résulte que m/d divise u, ce qui prouve notre assertion.

2) La première condition entraîne la seconde car m est le plus petit entier $k \geq 1$ tel que $x^k = e$. Inversement, supposons la condition 2 réalisée. Il existe un entier $k \geq 1$ tel que l'on ait $n = mk$: on a $n = mk + r$ avec $k \in \mathbb{Z}$ et $0 \leq r < m$, d'où $x^r = e$ puis $r = 0$. Supposons $k \geq 2$. Soit p un diviseur premier de k. On a alors les égalités

$$x^{\frac{n}{p}} = \left(x^m\right)^{\frac{k}{p}} = e,$$

ce qui contredit l'hypothèse faite. Par suite, on a $k = 1$, puis $m = n$.

2 1) Soit G un groupe fini d'ordre $2n-1$. Pour tout élément $x \in G$, on a $x^{2n-1} = e$ (e est l'élément neutre de G), d'où $x = x^{2n} = (x^n)^2$. 2) Soit $f : G \to G$ l'application définie par $f(x) = x^2$. C'est un morphisme de groupes. Puisque G est cyclique, G a un unique élément d'ordre 2, et le noyau de f est donc d'ordre 2. Par suite, l'ensemble G^2 des carrés de G est un groupe d'ordre $\frac{n}{2}$. 3) Soit H le sous-groupe de G formé des éléments x tels que $x^{\frac{n}{2}} = e$. Puisque G est cyclique, H est l'unique sous-groupe d'ordre $\frac{n}{2}$ de G. D'après la question précédente, G^2 et H ont le même ordre. On en déduit que $G^2 = H$, d'où l'équivalence annoncée. **Remarque.** Si x est un élément de G qui ne soit pas un carré, $x^{\frac{n}{2}}$ est l'unique élément d'ordre 2 de G. 4) Supposons $n = 2^t$ avec $t \geq 1$. Dans ce cas, G^2 est de cardinal 2^{t-1} et son complémentaire aussi. Par ailleurs, il y a exactement $\varphi(2^t) = 2^{t-1}$ générateurs dans G (φ est la fonction indicatrice d'Euler). De plus, un générateur de G n'est évidemment pas un carré. Cela entraîne le résultat. [On peut aussi procéder comme suit : soit x un élément de G qui n'est pas un carré dans G. Si y est un générateur de G, il existe m tel que $x = y^m$. D'après l'hypothèse faite, m est impair, donc x est un générateur, car les générateurs de G sont précisément les éléments de la forme y^k avec k impair (ce sont les entiers k premiers avec l'ordre de G)].

3 1) Considérons le morphisme de groupes $\psi : G \to G$ défini par $\psi(x) = x^k$. Vérifions que son noyau est d'ordre d. Soit x un élément de $\mathrm{Ker}(\psi)$. On a $x^k = e$ et $x^n = e$, d'où en utilisant le théorème de Bézout, $x^d = e$. On en déduit que les éléments de $\mathrm{Ker}(\psi)$ sont exactement les éléments $x \in G$ pour lesquels on a $x^d = e$. Puisque G est cyclique, on a donc $|\mathrm{Ker}(\psi)| = d$ et l'ordre de l'image de ψ est n/d. Par suite, si a est dans l'image de ψ, on a $a^{n/d} = e$. Inversement, si on a l'égalité $a^{n/d} = e$, puisque G est cyclique, a appartient à l'unique sous-groupe de G d'ordre n/d, qui est précisément l'image de ψ, d'où la condition (1) de l'énoncé. 2) Si $x \in G$ vérifie l'égalité $x^k = a$, on a $(xx_0^{-1})^k = e$, d'où $x = x_0 z$ avec $z^k = e$, et comme on l'a constaté ci-dessus, on a alors $z^d = e$. Inversement, pour tout $z \in G$ tel que $z^d = e$, on a $(x_0 z)^k = a$ car d divise k, d'où l'ensemble des solutions annoncé. Par ailleurs, G étant cyclique, il y a exactement d éléments $z \in G$ tels que $z^d = e$. Cela établit le résultat. 3) On remarque que $x_0 = \overline{3}$ est une solution particulière. Par ailleurs, les éléments $x \in G$ qui vérifient $5x = \overline{0}$ sont les classes de 0, 5, 10, 15 et 20. L'ensemble des solutions cherché est donc $\left\{\overline{3}, \overline{8}, \overline{13}, \overline{18}, \overline{23}\right\}$.

4 1) On a $754 \equiv 5 \mod 7$ et 5 n'est pas un carré dans $\mathbb{F}_7$. On a donc $\left(\frac{754}{7}\right) = -1$. 2) L'application $\mathbb{F}_p \to A$ qui à λ associe $\lambda + (X^4 + 1)$ est un morphisme injectif d'anneaux, donc A contient un sous-anneau isomorphe à $\mathbb{F}_p$. En particulier, A est de caractéristique p [on a $p1_A = 0$, donc le noyau du morphisme $\mathbb{Z} \to A$ qui à n associe $n1_A$ est $p\mathbb{Z}$]. On a $\alpha^4 + 1 = 0$, d'où $\alpha^2 + \alpha^{-2} = 0$, puis $y^2 = 2$. Par ailleurs, A étant de caractéristique p, on a

$$y^p = \alpha^p + \alpha^{-p}.$$

Supposons $p \equiv \pm 1 \mod 8$. L'égalité $\alpha^8 = 1$ entraîne alors $y^p = y$. Puisque p est impair, 2 est inversible dans A, et l'égalité $y^2 = 2$ entraîne qu'il en est de même de y. On en déduit que l'on a $y^{p-1} = 1$. Par suite, on obtient dans A les égalités

$$2^{\frac{p-1}{2}} = (y^2)^{\frac{p-1}{2}} = y^{p-1} = 1.$$

D'après le critère d'Euler, on a

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \mod p,$$

d'où il résulte que l'on a $\left(\frac{2}{p}\right) = 1$.

Supposons $p \equiv \pm 5 \mod 8$. Dans ce cas, on a

$$y^p = \alpha^5 + \alpha^{-5} = -\big(\alpha + \alpha^{-1}\big) = -y.$$

On a donc $y^{p-1} = -1$, ce qui entraîne par le même argument que celui utilisé ci-dessus, que $\big(\frac{2}{p}\big) = -1$.

L'égalité à démontrer est alors une conséquence de ce qui précède, vu que $p^2 - 1$ est multiple de 16 si et seulement si $p \equiv \pm 1 \mod 8$. En particulier, 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$. 3) D'après la loi de réciprocité quadratique, on a

$$\Big(\frac{3}{p}\Big)\Big(\frac{p}{3}\Big) = (-1)^{\frac{p-1}{2}} \quad \text{i.e.} \quad \Big(\frac{3}{p}\Big) = \Big(\frac{p}{3}\Big)(-1)^{\frac{p-1}{2}}.$$

On a donc l'équivalence

$$\Big(\frac{3}{p}\Big) = 1 \Longleftrightarrow \Big(p \equiv 1 \mod 4 \text{ et } p \equiv 1 \mod 3\Big) \quad \text{ou} \quad \Big(p \equiv 2 \mod 3 \text{ et } p \equiv 3 \mod 4\Big).$$

On en déduit que l'on a

$$\Big(\frac{3}{p}\Big) = 1 \Longleftrightarrow p \equiv \pm 1 \mod 12,$$

d'où l'assertion. 4) Soit a un entier résidu quadratique modulo p. On peut supposer a non divisible par p. D'après le critère d'Euler, on a

$$a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

L'ordre de a modulo p divise donc $(p-1)/2$, il est en particulier distinct de $p-1$. 5) On a $1237 = 12 \times 101 + 25$. On a donc

$$\Big(\frac{1237}{101}\Big) = \Big(\frac{5^2}{101}\Big) = 1.$$

Par ailleurs, on a

$$\Big(\frac{1236}{101}\Big) = \Big(\frac{24}{101}\Big) = \Big(\frac{3}{101}\Big)\Big(\frac{8}{101}\Big) = \Big(\frac{3}{101}\Big)\Big(\frac{2}{101}\Big).$$

On a $101 \equiv 5 \mod 8$ et $101 \equiv 5 \mod 12$. Compte tenu des questions 1 et 2, on a ainsi

$$\Big(\frac{3}{101}\Big) = \Big(\frac{2}{101}\Big) = -1 \quad \text{d'où} \quad \Big(\frac{1236}{101}\Big) = 1.$$

6) D'après la loi de réciprocité quadratique, on a

$$\Big(\frac{5}{p}\Big) = \Big(\frac{p}{5}\Big).$$

Par suite, on a

$$\Big(\frac{5}{p}\Big) = 1 \Longleftrightarrow p \equiv \pm 1 \mod 5 \quad \text{i.e.} \quad p \equiv \pm 1 \mod 10.$$

Ainsi, 5 est un carré dans $\mathbb{F}_p$ si et seulement si le dernier chiffre décimal de p est 1 ou 9.

5 1) On a $1003 = 17 \times 59$. On a donc

$$\Big(\frac{254}{1003}\Big) = \Big(\frac{254}{17}\Big)\Big(\frac{254}{59}\Big).$$

Par ailleurs, on a $254 \equiv -1 \mod 17$ et $254 \equiv 18 \mod 59$. On en déduit l'égalité

$$\Big(\frac{254}{1003}\Big) = \Big(\frac{-1}{17}\Big)\Big(\frac{18}{59}\Big) = \Big(\frac{-1}{17}\Big)\Big(\frac{2}{59}\Big).$$

Puisque l'on a $17 \equiv 1 \mod 4$ et $59 \equiv 3 \mod 8$, il en résulte que

$$\Big(\frac{254}{1003}\Big) = -1.$$

2) Les égalités à démontrer sont vraies si $n = 1$. Supposons donc $n \geq 3$. On considère l'application f définie sur l'ensemble des entiers impairs positifs à valeurs dans $\{\pm 1\}$, par l'égalité

$$f(m) = (-1)^{\frac{m-1}{2}}.$$

Pour tous a et b impairs, on vérifie, en examinant les classes de a et b modulo 4, que l'on a

$$f(ab) = f(a)f(b).$$

Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition en facteurs premiers de n. On a ainsi

$$f(n) = \prod_{i=1}^{r} f(p_i)^{n_i}.$$

Par ailleurs, pour tout $i = 1, \cdots, r$, on a $f(p_i) = \left(\frac{-1}{p_i}\right)$, d'où l'égalité $f(n) = \left(\frac{-1}{n}\right)$ par définition du symbole de Jacobi. On procède de même pour l'autre égalité, en posant pour tout m impair

$$g(m) = (-1)^{\frac{m^2-1}{8}}.$$

Pour tous a et b impairs, on vérifie, en examinant les classes de a et b modulo 8, que l'on a $g(ab) = g(a)g(b)$, et l'on conclut comme ci-dessus. 3) Supposons que l'on a $\left(\frac{a}{n}\right) = -1$. On a $n \geq 3$. Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition en facteurs premiers de n. Par définition du symbole de Jacobi, on a

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{n_i}.$$

Il existe donc un indice i tel que l'on ait $\left(\frac{a}{p_i}\right) = -1$. Par suite, a n'est pas un carré modulo p_i, en particulier, a n'est pas un carré modulo n.

La réciproque de l'implication précédente est fausse en général : on a par exemple $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1$, bien que 2 ne soit pas un carré modulo 15, vu que 2 n'est pas un carré modulo 3. 4) Soit p un nombre premier tel que p^2 divise n. On a $n \geq 3$. Vérifions que l'entier $b = 1 + \frac{n}{p}$ convient. D'abord, pour tout nombre premier q divisant n, on a $b \equiv 1 \mod q$, en particulier, on a $\left(\frac{b}{q}\right) = 1$, ce qui entraîne l'égalité $\left(\frac{b}{n}\right) = 1$. Par ailleurs, étant donné un entier $j \geq 1$, on a l'équivalence

$$b^j \equiv 1 \mod n \Longleftrightarrow j \equiv 0 \mod p.$$

En effet, on a

$$b^j = 1 + j\frac{n}{p} + \sum_{k=2}^{j} C_j^k \left(\frac{n}{p}\right)^k.$$

Puisque p^2 divise n, on a donc

$$b^j = 1 + j\frac{n}{p} + \sum_{k=2}^{j} C_j^k \frac{n}{p^2}\left(\frac{n}{p}\right)^{k-2} n \equiv 1 + j\frac{n}{p} \mod n,$$

d'où l'équivalence annoncée. Puisque l'entier $j = \frac{n-1}{2}$ n'est pas multiple de p, on a donc $b^{\frac{n-1}{2}} \not\equiv 1 \mod n$.

6 1) On a

$$(1 + p^n a)^p = \sum_{j=0}^{p} C_p^j p^{nj} a^j = 1 + p^{n+1}a + C_p^2 p^{2n} a^2 + \cdots + p^{np} a^p.$$

L'entier C_p^2 est divisible par p et l'on a $2n + 1 \geq n + 2$ et $3n \geq n + 2$, cela entraîne la première congruence. On démontre la seconde par récurrence sur n. Elle est vraie si $n = 1$. Soit alors n un entier ≥ 2 tel qu'elle soit vraie pour l'entier $n - 1$. On a donc

$$(1 + pa)^{p^{n-1}} = 1 + p^n a + p^{n+1} b \quad \text{où } b \in \mathbb{Z}.$$

En utilisant la première congruence (avec l'entier $a + pb$), on en déduit que

$$(1 + pa)^{p^n} = \left(1 + p^n(a + pb)\right)^p \equiv 1 + p^{n+1}(a + pb) \mod p^{n+2},$$

d'où le résultat. 2) Soit r un entier ≥ 1. Puisque p est impair, le groupe $\left(\mathbb{Z}/p^r\mathbb{Z}\right)^*$ est cyclique d'ordre $p^{r-1}(p-1)$. Supposons $\left(\frac{n}{p}\right) = 1$. D'après le critère d'Euler, on a

$$n^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Autrement dit, il existe $a \in \mathbb{Z}$ tel que l'on ait $n^{\frac{p-1}{2}} = 1 + pa$. D'après la seconde congruence démontrée ci-dessus, on a donc

$$n^{\frac{p^{r-1}(p-1)}{2}} = (1+pa)^{p^{r-1}} \equiv 1 + p^r a \mod p^{r+1}.$$

En particulier, on a

$$n^{\frac{p^{r-1}(p-1)}{2}} \equiv 1 \mod p^r.$$

D'après la question 3 de l'exercice 11, cela entraîne que n est un carré dans $\big(\mathbb{Z}/p^r\mathbb{Z}\big)^*$. 3) Supposons qu'il existe un entier a tel que $n \equiv a^2 \mod 2^r$. On a $r \geq 3$, d'où en particulier $n \equiv a^2 \mod 8$. L'entier a étant impair, on $a^2 \equiv 1 \mod 8$, d'où $n \equiv 1 \mod 8$.
Inversement, supposons $n \equiv 1 \mod 8$. Compte tenu du paragraphe 10 du chapitre I du cours, il existe $t \in \mathbb{N}$ tel que l'on ait

$$n \equiv \pm 5^t \mod 2^r.$$

Par ailleurs, si t est pair on a $5^t \equiv 1 \mod 8$, et si t est impair on a $5^t \equiv 5 \mod 8$. D'après l'hypothèse faite sur n, on en déduit que t est pair et que l'on a $n \equiv 5^t \mod 2^r$, ce qui prouve que n est carré modulo 2^r.

7 1) Soit G le polynôme $F(X+1)$. On a

$$G = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

D'après le critère d'Eisenstein[(1)], G est irréductible dans $\mathbb{Z}[X]$ et il en est de même de F. [(1)] Démontrons ce critère. Tout d'abord, dans un anneau commutatif, un élément a est irréductible s'il n'est pas inversible et si l'égalité $a = bc$ entraîne que b ou c est inversible. Le polynôme F n'est pas inversible dans $\mathbb{Z}[X]$ car $n \geq 1$. Supposons qu'il existe deux polynômes g et h dans $\mathbb{Z}[X]$ tels que $F = gh$. Il s'agit alors de prouver que g ou h vaut ± 1. Notons $s : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la surjection canonique et $\varphi : \mathbb{Z}[X] \to \big(\mathbb{Z}/p\mathbb{Z}\big)[X]$ l'application définie par

$$\varphi\Big(\sum u_i X^i\Big) = \sum_i s(u_i) X^i.$$

C'est un morphisme d'anneaux. Il résulte des hypothèses faites que l'on a

$$\varphi(F) = \varphi(g)\varphi(h) = s(a_n)X^n.$$

On en déduit qu'il existe des entiers λ, μ et $k \geq 0$ tels que l'on ait

$$\varphi(g) = s(\lambda)X^k \quad \text{et} \quad \varphi(h) = s(\mu)X^{n-k}.$$

Prouvons que l'on a $k = 0$ ou $k = n$. Supposons pour cela que l'on ait $0 < k < n$. Le polynôme $g - \lambda X^k$ appartient à $p\mathbb{Z}[X]$. Puisque $k > 0$, le terme constant de g est divisible par p. De même, puisque $k < n$ le terme constant de h est aussi divisible par p. Cela contredit le fait que p^2 ne divise pas a_0, d'où l'assertion. Supposons $k = 0$. On a $\varphi(g) = s(\lambda)$. Si le degré de g est ≥ 1, le coefficient dominant de g est donc divisible par p, ce qui entraîne que p divise a_n, d'où une contradiction. Par suite, le degré de g est nul, autrement dit, g est un entier. Puisque g divise F et que les a_i sont premiers entre eux, on a donc $g = \pm 1$. De même si $k = n$, on montre que l'on a $h = \pm 1$. Cela établit le critère annoncé.

2) Notons encore F le polynôme de $\mathbb{F}_p[X]$ que l'on obtient par réduction modulo p. Si $p = 2$, on a $F = (X+1)^4$, d'où l'assertion dans ce cas. Supposons $p \geq 3$. Si l'on a $p \equiv 1 \mod 4$, alors -1 est un carré dans $\mathbb{F}_p$. En posant $-1 = a^2$ où $a \in \mathbb{F}_p$, on obtient l'égalité $F = (X^2 - a)(X^2 + a)$. Supposons $p \equiv 3 \mod 4$. Si $p \equiv 7 \mod 8$. Dans ce cas, 2 est un carré dans $\mathbb{F}_p$. En écrivant F sous la forme $F = (X^2+1)^2 - 2X^2$, on constate de nouveau que F est réductible dans $\mathbb{F}_p[X]$. Il reste le cas où $p \equiv 3 \mod 8$. On a alors

$$\Big(\frac{-2}{p}\Big) = -(-1)^{\frac{p^2-1}{8}} = 1,$$

par suite, -2 est un carré dans $\mathbb{F}_p$, et l'égalité $F = (X^2-1)^2 - (-2)X^2$ entraîne l'assertion.

---

1. Le critère d'Eisenstein sur $\mathbb{Z}$ est le suivant. Soit $F = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ un polynôme de degré $n \geq 1$ tel que les coefficients a_i soient premiers entre eux dans leur ensemble. Soit p un nombre premier. On suppose que

$$a_i \equiv 0 \mod p \quad \text{si} \quad i = 0, \cdots, n-1, \quad a_0 \not\equiv 0 \mod p^2 \quad \text{et} \quad a_n \not\equiv 0 \mod p.$$

Alors, F est irréductible dans $\mathbb{Z}[X]$.

3) Soient a et b deux entiers relatifs tels que a, b et ab ne soient pas des carrés dans $\mathbb{Z}$. Le polynôme

$$(X^2-a)(X^2-b)(X^2-ab)\in\mathbb{Z}[X]$$

satisfait alors à la condition demandée. En effet, on peut supposer p impair et ab non divisible par p. Il suffit ensuite de remarquer que l'un des entiers a, b et ab est un carré modulo p : si a et b ne sont pas des carrés modulo p, on a

$$a^{\frac{p-1}{2}}\equiv b^{\frac{p-1}{2}}\equiv -1 \mod p,$$

de sorte que l'on a

$$(ab)^{\frac{p-1}{2}}\equiv 1 \mod p \quad \text{i.e.} \quad \left(\frac{ab}{p}\right)=1.$$

8 1) D'après le critère d'Euler, on a dans $\mathbb{F}_p^*$ l'égalité $a^{\frac{p-1}{2}}=1$. Il en résulte que l'on a

$$\left(a^{\frac{p+1}{4}}\right)^2=a^{\frac{p+1}{2}}=a^{\frac{p-1}{2}}a=a,$$

ce qui entraîne l'assertion. 2) Parce que $\mathbb{F}_p$ est un corps, l'égalité $a^{\frac{p-1}{2}}=1$ entraîne $a^{\frac{p-1}{4}}=\pm 1$ (p est congru à 1 modulo 4).

Si l'on a $a^{\frac{p-1}{4}}=1$, en posant $x=\pm a^{\frac{p+3}{8}}$, on obtient $x^2=a^{\frac{p+3}{4}}=a$.

Supposons $a^{\frac{p-1}{4}}=-1$. D'après la congruence $p\equiv 5 \mod 8$, on a $\left(\frac{2}{p}\right)=-1$, autrement dit, on a dans $\mathbb{F}_p$ l'égalité

$$2^{\frac{p-1}{2}}=-1.$$

Posons $x=\pm 2a(4a)^{\frac{p-5}{8}}$. On vérifie alors que l'on a

$$x^2=4a^2(4a)^{\frac{p-5}{4}}=a^{\frac{p+3}{4}}2^{\frac{p-1}{2}}=-a^{\frac{p+3}{4}}=-a^{\frac{p-1}{4}}a=a.$$

On vérifie directement les assertions des questions 3 et 4 si $p=2$. On supposera donc $p\geq 3$. 3) Puisque a est un carré dans $\mathbb{F}_p$, on a les égalités

$$a^{\frac{p-1}{2}}=\left(a^q\right)^{2^{e-1}}=1.$$

Ainsi, l'ordre de $a^q\in\mathbb{F}_p^*$ est une puissance de 2, donc a^q appartient à G. Par ailleurs, l'ordre de a^q divisant 2^{e-1}, a^q n'est pas un générateur de G. D'après la question 4 de l'exercice 11, a^q est donc un carré dans G. 4) L'ensemble des carrés de G, qui est le complémentaire dans G de l'ensemble de ses générateurs, est formé des puissances paires de z. Il existe donc un entier pair u tel que l'on ait $0\leq u<2^e$ et $a^q=z^u$, ce qui entraîne l'assertion (si $u=0$, on prend $k=0$, sinon on prend $k=2^e-u$). On en déduit les égalités $x^2=a^{q+1}z^k=a(a^qz^k)=a$. 5) On a

$$\left(\frac{5}{29}\right)=\left(\frac{29}{5}\right)=\left(\frac{4}{5}\right)=1,$$

donc 5 est un carré dans $\mathbb{F}_{29}$. Le groupe $\mathbb{F}_{29}^*$ est d'ordre $28=2^2.7$. En reprenant les notations précédentes, on a $e=2$ et $q=7$, et G est cyclique d'ordre 4. Puisque l'on a $12^2\equiv -1 \mod 29$, on peut prendre $z=12$. Il existe donc un entier pair k tel que l'on ait $0\leq k<4$ et $5^7.12^k\equiv 1 \mod 29$, et l'on vérifie que $k=2$. Il en résulte que

$$x=5^4.12 \mod 29 = 18 \mod 29$$

est une racine carrée de 5 dans $\mathbb{F}_{29}$, l'autre racine carrée étant la classe de 11 modulo 29.

9 1) La multiplicativité du symbole de Zolotarev en la variable m provient du fait que la composition de la multiplication par m avec la multiplication par m' correspond à la multiplication par mm' et que la signature d'une composée est le produit des signatures.

2) Le cas $p=2$ étant évident, on suppose donc p impair. Si $n\equiv a^2 \mod p$, alors $\binom{n}{p}_Z=\binom{a}{p}_Z^2=\binom{n}{p}$. Supposons donc que n n'est pas un carré modulo p ; de l'égalité $s_p(n)=\beta\circ\alpha$ on en déduit que $\binom{n}{p}_Z=\epsilon(\beta)\epsilon(\alpha)$. Mais puisque une involution se décompose en produit de transpositions à supports disjoints, la signature d'une involution τ de $\mathbb{Z}/p\mathbb{Z}$ est égale à $(-1)^{p-\sharp\mathrm{Fix}(\tau)}$ où $\mathrm{Fix}(\tau)$ désigne l'ensemble des points fixes de τ. Or $\mathrm{Fix}(\alpha)=\{0,1,-1\}$ et $\mathrm{Fix}(\beta)=\{0\}$ car un point fixe $a\neq 0 \mod p$ de β vérifie $n=a^2$ ce qui est exclu. Ainsi $\binom{n}{p}_Z=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-3}{2}}=-1=\binom{n}{p}$.

Remarque : on peut aussi calculer explicitement la signature. Soit r l'ordre de m dans $(\mathbb{Z}/n\mathbb{Z})^\times$ qui est cyclique si n est premier ; ce groupe se décompose alors sous l'action de m en $(n-1)/r$ orbites chacune de longueur r et sur

ces orbites la multiplication par m y induit un cycle de longueur r. On en déduit alors que le symbole de Zolotarev est $(-1)^{(r-1)(n-1)/r}$. Ainsi

- si r est pair on a

$$m^{(n-1)/2} = (m^{r/2})^{(n-1)/r} \equiv (-1)^{(n-1)/r} \mod n$$

car m étant d'ordre r, $m^{r/2}$ est une racine carrée de 1 dans le corps $\mathbb{Z}/n\mathbb{Z}$ distincte de 1 donc égale à -1 ;

- si r est impair, $n-1$ est alors divisible par $2r$ et donc $m^{(n-1)/2} = (m^r)^{(n-1)/2r} \equiv 1 \mod n$ d'où le résultat.

3-a) C'est clair.

3-b) La permutation $\sigma_{D,V}$ conserve les lignes puisque

$$\{v_{i,j};\ j = 1, \cdots, n\} = \{0 \leq k \leq mn-1;\ k \equiv i-1 \mod m\} = \{d_{i,j},\ j = 1, \cdots, n\}.$$

Ainsi $\sigma_{D,V}$ est le produit de m permutations de n éléments, chacune correspondant à l'action de $\sigma_{D,V}$ sur une ligne. Fixons $1 \leq i \leq m$ et calculons la signature de la permutation ρ_i induit par $\sigma_{D,V}$ sur la i-ème ligne. Grâce au lemme chinois, un élément de la i-ème ligne de D ou de V est uniquement déterminé par sa classe dans $\mathbb{Z}.n\mathbb{Z}$. Ainsi ρ_i^{-1} est la permutation de $\mathbb{Z}/n\mathbb{Z}$ qui envoie $j-1$ sur $m(j-1)+i-1$, i.e. $\rho_i^{-1} = T_{i-1} \circ s_n(m)$ où T_a désigne la translation $k \in \mathbb{Z}/n\mathbb{Z} \mapsto k+a$. Mais pour tout a, $\epsilon(T_a) = 1$ car $T_a = \underbrace{T_1 \circ \cdots T_1}_{a}$ et $\epsilon(T_1) = 1$ car T_1 est un cycle de longueur impair n. Ainsi $\epsilon(\sigma_{D,V}) = \prod_{i=1}^m \epsilon(\rho_i) = \left(\binom{m}{n}_Z\right)^m = \binom{m}{n}_Z$ puisque m est impair.

3-c) Même raisonnement que dans b) en remarquant que $\sigma_{H,D}$ conserve les colonnes.

3-d) Calculons le nombre d'inversions de $\sigma_{V,H}$. On a

$$(v_{i,j} < v_{k,l}) \Leftrightarrow \Big(m(j-1)+i-1 < m(k-1)+l-1\Big) \Leftrightarrow \Big(j < l \text{ ou } (j = l \text{ et } i < k\Big).$$

De même $(h_{i,} < h_{k,l} \Leftrightarrow (i < k$ ou $(i = k$ et $j < l))$. On a donc

$$(v_{i,j} < v_{k,l} \text{ et } h_{i,j} > h_{k,l}) \Leftrightarrow (j < l \text{ et } k < i).$$

Ainsi le nombre d'inversion est égal à $\binom{m}{2}\binom{n}{2} = \frac{m(m-1)}{2}\frac{n(n-1)}{2}$, et puisque mn est impair, on a $\epsilon(\sigma_{V,H}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

3-e) Immédiat d'après les questions précédentes.

4) La loi de réciprocité contient la multiplicativité en bas du symbole de Zolotarev :

$$\binom{a}{mn}_Z = \frac{a}{m}_Z \binom{a}{n}_Z$$

où m et n sont des entiers impairs et a est premier à mn. En effet si r est un entier congru à 1 modulo 4 et à a modulo mn, on a

$$\binom{a}{mn}_Z = \binom{r}{mn}_Z = (-1)^{\frac{r-1}{2}\frac{mn-1}{2}} \binom{mn}{r}_Z = \binom{m}{r}_Z \binom{n}{r}_Z = \binom{r}{m}_Z \binom{r}{n}_Z = \binom{a}{m}_Z \binom{a}{n}_Z.$$

On en déduit donc que le symbole de Zolotarev est égal au symbole de Jacobi défini pour les couples (m,n) d'entiers premiers entre eux avec n impair comme l'unique symbole multiplicatif en haut et en bas prolongeant le symbole de Legendre.

5) Comme n est impair, $n \wedge (n-2) = 1$ et donc

$$\binom{2}{n} = \binom{2}{n}_Z = \binom{-(n-2)}{n}_Z = \binom{-1}{n}_Z \binom{n-2}{n}_Z = (-1)^{\frac{n-1}{2}}(-1)^{\frac{n-1}{2}\frac{n-3}{2}} \binom{n}{n-2}_Z = (-1)^{\frac{n-1}{2}} \binom{2}{n-2}_Z.$$

En notant $n = 2k+1$, on a donc $\binom{2}{n}_Z = (-1)^{\frac{k(k+1)}{2}} = \begin{cases} 1 & \text{si } n \equiv \pm 1 \mod 8 \\ -1 & \text{sinon} \end{cases}$.

10 1) En posant $Y = X^{-1}$, le membre de gauche est égal à $X^{(p-1)/2} + \cdots + X + 1 + Y + \cdots + Y^{(p-1)/2}$, de sorte que d'après le théorème sur les polynômes symétriques, il existe $R \in \mathbb{Z}[X,Y]$ tel que le terme précédent est égal à $R(X+Y, XY)$, d'où le résultat en notant que $XY = 1$.

2) Raisonnons par l'absurde et considérons l premier divisant $\mathrm{Res}(Q_p, Q_q)$ de sorte que modulo l, $\bar{Q}_p$ et $\bar{Q}_q$ ont une racine commune $\beta \in \mathbb{F}_{l^n}$ pour $2n \leq \min\{p-1, q-1\}$. Soit alors $x \in \bar{\mathbb{F}}_l$ tel que $x^2 - \beta x + 1 = 0$ de sorte que

$$x^{p-1} + \cdots + x + 1 = x^{(p-1)/2} \bar{Q}_p(\beta) = 0.$$

En multipliant cette égalité par $x-1$, on en déduit que $x^p=1$ dans $\bar{\mathbb{F}}_l$. De la même façon on a aussi $x^q=1$ et comme $p\wedge q=1$, on en déduit $x=1$ et donc $p\equiv q\equiv 0 \mod l$ ce qui n'est pas car $p\wedge q=1$.

3) On raisonne modulo p de sorte que d'après le lemme précédent, il suffit de prouver que ce résultant est $\equiv q^{(p-1)/2} \mod p$:

$$X^{p-1}+\cdots+X+1\equiv (X-1)^{p-1}\equiv (X^2-2X+1)^{(p-1)/2}\equiv X^{(p-1)/2}(X+\frac{1}{X}-2)^{(p-1)/2} \mod p,$$

de sorte que $Q_p(X+\frac{1}{X})\equiv (X+\frac{1}{X}-2)^{(p-1)/2} \mod p$ et donc

$$Q_p(X)\equiv (X-2)^{(p-1)/2} \mod p.$$

Ainsi on en déduit que $\mathrm{Res}(Q_p,Q_q)\equiv Q_p(2)^{(p-1)/2}\equiv Q_q(1+\frac{1}{1})^{(p-1)/2}\equiv q^{(p-1)/2} \mod p$, d'où le résultat.

4) Immédiat.

11 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 $\pm1,\pm2$. On écrit $n=hl_1\cdots l_k$ avec $h\in\{\pm1,\pm2\}$ 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.