Théorie des Nombres - TD3
Loi de réciprocité quadratique

Exercice 1 : Pour quels nombres premiers p la classe de l'entier 7 modulo p est-elle un carré ?

Solution de l'exercice 1. Tout d'abord, il est clair que 7 est un carré modulo 2 et modulo 7.
Soit maintenant un nombre premier impair $p \neq 7$. On écrit la loi de réciprocité quadratique :

$$\left(\frac{p}{7}\right)\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

On en déduit donc que $\left(\frac{7}{p}\right) = 1$ si et seulement si ($\left(\frac{p}{7}\right) = 1$ et $p \equiv 1$ [4]) ou ($\left(\frac{p}{7}\right) = -1$ et $p \equiv 3$ [4]).
Écrivons la liste des carrés non nuls modulo 7 : $1, 2, 4$ mod 7 sont les carrés non nuls modulo 7.
Alors la condition précédente s'écrit ainsi : $\left(\frac{7}{p}\right) = 1$ si et seulement si ($p \equiv 1, 2, 4$ [7] et $p \equiv 1$ [4]) ou ($p \equiv 3, 5, 6$ [7] et $p \equiv 3$ [4]).
Or le lemme chinois assure que l'on a un isomorphisme d'anneaux $\phi : \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/28\mathbb{Z}$, défini par $\phi(a \bmod 7, b \bmod 4) := 8a - 7b \bmod 28$ (puisqu'une relation de Bezout s'écrit $4.2 + 7.(-1) = 1$).
Donc les conditions précédentes se traduisent ainsi : $\left(\frac{7}{p}\right) = 1$ si et seulement si $p \equiv 1, 9, 25$ [28] ou $p \equiv 3, 19, 27$ [28].
Finalement, on a montré que pour tout nombre premier p, 7 est un carré modulo p si et seulement si

$$p \equiv 1, 2, 3, 7, 9, 19, 25, 27 \ [28],$$

si et seulement si

$$p = 2 \text{ ou } p = 7 \text{ ou } p \equiv 1, 3, 9, 19, 25, 27 \ [28].$$

Exercice 2 : Expliciter la fonction $p \mapsto \left(\frac{3}{p}\right)$.
En déduire que la condition "3 est un carré modulo p" ne dépend que de la classe de p modulo 12.

Solution de l'exercice 2. Notons pour simplifier $f(p) := \left(\frac{3}{p}\right)$. D'abord, il est clair que $f(3) = 1$ et $f(2) = 1$.
Soit maintenant un nombre premier $p \geq 5$.
La loi de réciprocité quadratique assure que $f(p) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$. Or les carrés modulo 3 sont exactement les classes de 0 et de 1. Par conséquent, on a $f(p) = 1$ si et seulement si ($p \equiv 1$ [3] et $p \equiv 1$ [4]) ou ($p \equiv 2$ [3] et $p \equiv 3$ [4]).
Le lemme chinois assure qu'il y a un isomorphisme $\varphi : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/12\mathbb{Z}$ donné par $\varphi(a \bmod 3, b \bmod 4) = 4a - 3b \bmod 12$. Donc les conditions précédentes sont équivalentes aux conditions suivantes : $f(p) = 1$ si et seulement si $p \equiv 1$ [12] ou $p \equiv 11$ [12].
Finalement, on a montré que :

$$\left(\frac{3}{p}\right) = 1 \text{ si et seulement si } p = 2, 3 \text{ ou } p \equiv 1, 11 \ [12]$$

et

$$\left(\frac{3}{p}\right) = -1 \text{ si et seulement si } p \equiv 5, 7 \ [12].$$

Exercice 3 : Soit $n \in \mathbb{Z}$. Montrer que l'entier n^2+n+1 n'admet aucun diviseur de la forme $6k-1$, avec $k \in \mathbb{Z} \setminus \{0\}$.
[Indication : on pourra montrer que si d est un diviseur de n^2+n+1, alors -3 est un carré mod. d.]

Solution de l'exercice 3. Soit d un diviseur positif de n^2+n+1. Alors d est impair et d divise $4(n^2+n+1)$. Or $4(n^2+n+1) = (2n+1)^2+3$, donc $(2n+1)^2 \equiv -3$ $[d]$, donc -3 est un carré modulo d. Supposons maintenant que $d=p$ est un diviseur premier de n^2+n+1, avec $p \neq 3$. Alors $\left(\frac{-3}{p}\right) = 1$, i.e. $\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$. Donc $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$. Or la loi de réciprocité quadratique assure que $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$. Donc on obtient $\left(\frac{p}{3}\right) = 1$, ce qui équivaut à $p \equiv 1$ [3]. Finalement, les facteurs premiers de n^2+n+1 sont soit 3, soit congrus à 1 modulo 3. Donc tout diviseur de n^2+n+1 est congru à 1 ou 3 modulo 6. Donc il n'existe aucun diviseur de la forme $6k-1$.

Exercice 4 : Soit p un nombre premier de Fermat, i.e. de la forme $p = 2^{2^n}+1$, avec $n \in \mathbb{N}$.
Montrer que la classe de 3 dans $\mathbb{Z}/p\mathbb{Z}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$ dès que $p \neq 3$. Même question en remplaçant 3 par 5, puis par 7.

Solution de l'exercice 4. On suppose $p \neq 3$. Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre 2^{2^n}. Donc 3 engendre ce groupe si et seulement si 3 n'est pas un carré modulo p, si et seulement si $\left(\frac{3}{p}\right) = -1$ si et seulement si $\left(\frac{p}{3}\right) = -1$ si et seulement si $p \equiv 2$ [3]. Or on a $p = 2^{2^n}+1$ et $2^{2^n} \equiv (-1)^{2^n} \equiv 1$ [3] car $n \geq 1$, donc $p \equiv 2$ [3], donc 3 engendre $(\mathbb{Z}/p\mathbb{Z})^*$.
On fait le même raisonnement en remplaçant 3 par un nombre premier impair q : supposons $p \neq q$. Alors q engendre $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si q n'est pas un carré modulo p, si et seulement si $\left(\frac{q}{p}\right) = -1$ si et seulement si $\left(\frac{p}{q}\right) = -1$. Or pour $q=5$, on trouve $\left(\frac{p}{5}\right) = \left(\frac{4^{2^{n-1}}+1}{5}\right)$, et $4^{2^{n-1}} \equiv 1$ [5] dès que $n \geq 2$. Donc pour $q=5$ et $n \geq 2$, on trouve que $\left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$, donc 5 engendre $(\mathbb{Z}/p\mathbb{Z})^*$.
De même, pour $q=7$ et $n \geq 3$, on trouve $\left(\frac{p}{7}\right) = \left(\frac{3}{7}\right)$ ou $\left(\frac{5}{7}\right)$ selon la parité de n, donc $\left(\frac{p}{7}\right) = -1$, d'où le résultat.

Exercice 5 : Soit p un nombre premier impair.

a) Montrer que
$$\sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) = 0\,.$$

b) Soit K un corps et soit $\zeta_p \in K$ une racine primitive p-ième de l'unité. On pose $G(\zeta_p) := \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right)\zeta_p^x$. Montrer que $G(\zeta_p)^2 = \left(\frac{-1}{p}\right)p$.
[Indication : on pourra montrer que $G(\zeta_p)^2 = \left(\frac{-1}{p}\right)G(\zeta_p)G(\zeta_p^{-1})$, ou alors que $G(\zeta_p)^2 = \sum_{x,y \in \mathbb{F}_p^*}\left(\frac{y}{p}\right)\zeta_p^{x(1+y)}$]

c) En considérant un corps K de caractéristique $q \neq p$ (q premier impair), calculer $G(\zeta_p)^q$ de deux façons différentes et en déduire la loi de réciprocité quadratique.

d) En considérant le corps $K = \mathbb{C}$, déduire de la question b) que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique (i.e. de la forme $\mathbb{Q}(\zeta_n)$, où ζ_n est une racine primitive n-ième de l'unité).

Solution de l'exercice 5.

a) On note $S := \sum_{x \in \mathbb{F}_p^*}\left(\frac{x}{p}\right)$. Puisque $p > 2$, il existe $y \in \mathbb{F}_p^*$ tel que $\left(\frac{y}{p}\right) = -1$. Alors le morphisme $x \mapsto yx$ est une bijection de $\mathbb{F}_p^*$ dans lui-même, donc
$$S = \sum_{x \in \mathbb{F}_p^*}\left(\frac{x}{p}\right) = \sum_{x \in \mathbb{F}_p^*}\left(\frac{yx}{p}\right) = \sum_{x \in \mathbb{F}_p^*}\left(\frac{y}{p}\right)\left(\frac{x}{p}\right) = -\sum_{x \in \mathbb{F}_p^*}\left(\frac{x}{p}\right) = -S\,.$$
Donc $2S = 0$, donc $S = 0$.

b) On a

$$G(\zeta_p)^2 = \sum_{x\in\mathbb{F}_p^*}\sum_{y\in\mathbb{F}_p^*}\left(\frac{xy}{p}\right)\zeta_p^{x+y}\,.$$

Or pour tout $x \in \mathbb{F}_p^*$, l'application $y \mapsto xy$ est une bijection de $\mathbb{F}_p^*$ dans lui-même. Donc pour tout $x \in \mathbb{F}_p^*$, on a

$$\sum_{y\in\mathbb{F}_p^*}\left(\frac{xy}{p}\right)\zeta_p^{x+y} = \sum_{y'\in\mathbb{F}_p^*}\left(\frac{x^2y'}{p}\right)\zeta_p^{x+xy'} = \sum_{y'\in\mathbb{F}_p^*}\left(\frac{y'}{p}\right)\zeta_p^{x(1+y')}\,.$$

Par conséquent, on en déduit que

$$G(\zeta_p)^2 = \sum_{x,y\in\mathbb{F}_p^*}\left(\frac{y}{p}\right)\zeta_p^{x(1+y)} = \sum_{y\in\mathbb{F}_p^*}\left(\frac{y}{p}\right)\sum_{x\in\mathbb{F}_p^*}\left(\zeta_p^{1+y}\right)^x = \sum_{x\in\mathbb{F}_p^*}\left(\frac{-1}{p}\right) + \sum_{y\in\mathbb{F}_p^*\setminus\{-1\}}\left(\frac{y}{p}\right)\sum_{x\in\mathbb{F}_p^*}\left(\zeta_p^{1+y}\right)^x\,,$$

où la dernière égalité est obtenue en isolant le terme correspondant à $y = -1$. Or pour tout $y \neq -1$, ζ_p^{1+y} est une racine primitive p-ième de l'unité, donc $\sum_{x\in\mathbb{F}_p^*}\left(\zeta_p^{1+y}\right)^x = -1$, d'où

$$G(\zeta_p)^2 = (p-1)\left(\frac{-1}{p}\right) - \sum_{y\in\mathbb{F}_p^*\setminus\{-1\}}\left(\frac{y}{p}\right) = p\left(\frac{-1}{p}\right) - \sum_{y\in\mathbb{F}_p^*}\left(\frac{y}{p}\right)\,.$$

Par la question précédente, la dernière somme est nulle, donc finalement

$$G(\zeta_p)^2 = \left(\frac{-1}{p}\right)p\,.$$

c) On a

$$G(\zeta_p)^q = \left(\sum_{x\in\mathbb{F}_p^*}\left(\frac{x}{p}\right)\zeta_p^x\right)^q = \sum_{x\in\mathbb{F}_p^*}\left(\frac{x}{p}\right)\zeta_p^{qx}$$

puisque le corps K est de caractéristique q. Autrement dit, en faisant le changement de variables $y := qx$, on a montré que

$$G(\zeta_p)^q = \sum_{x\in\mathbb{F}_p^*}\left(\frac{x}{p}\right)\zeta_p^{qx} = \sum_{y\in\mathbb{F}_p^*}\left(\frac{qy}{p}\right)\zeta_p^{y} = \left(\frac{q}{p}\right)G(\zeta_p)\,.$$

En outre, on a

$$G(\zeta_p)^q = G(\zeta_p)\left(G(\zeta_p)^2\right)^{\frac{q-1}{2}}\,,$$

donc grâce à la question b), on en déduit que

$$G(\zeta_p)^q = G(\zeta_p)\left(\frac{-1}{p}\right)p^{\frac{q-1}{2}}\,.$$

En comparant les deux écritures de $G(\zeta_p)^q$, on obtient, puisque $G(\zeta_p) \neq 0$ (voir question a)) :

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

Or on sait que dans K, on a $p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right)$, donc on en déduit

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

d'où l'on déduit facilement la loi de réciprocité quadratique, puisque $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

d) Cela se fait en plusieurs étapes. Remarquons d'abord que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ et que $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$.

Soit maintenant un nombre premier impair p. La question b) assure que $\left(\frac{-1}{p}\right) p$ est un carré dans le corps $\mathbb{Q}(\zeta_p)$ (c'est le carré de $s \in \mathbb{Q}(\zeta_p)$). Par conséquent, p est un carré dans le corps $\mathbb{Q}(i, \zeta_p) = \mathbb{Q}(\zeta_{2p})$. Donc finalement, pour tout p premier impair, $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{2p})$.

Soit maintenant une extension quadratique quelconque $K/\mathbb{Q}$. On sait qu'il existe un entier sans facteur carré $d \in \mathbb{Z}$ tel que $K = \mathbb{Q}(\sqrt{d})$. On décompose d en facteurs premiers : il existe $\epsilon \in \{\pm 1\}$, $s \in \{0, 1\}$ et $p_1, \ldots, p_r$ des nombres premiers impairs distincts, tels que $d = \epsilon 2^s p_1 \ldots p_r$. Grâce à l'étude précédente, on a les inclusions suivantes :

$$\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{\epsilon}, \sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_r}) \subset \mathbb{Q}(\zeta_8, \zeta_{2p_1}, \ldots, \zeta_{2p_r})\,.$$

Finalement, on remarque que $\mathbb{Q}(\zeta_8, \zeta_{2p_1}, \ldots, \zeta_{2p_r}) = \mathbb{Q}(\zeta_n)$, où $n = 8p_1 \ldots p_r$, et on a bien montré que

$$K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_n)\,.$$

Exercice 6 : Soit p un nombre premier impair.

a) Soit $n \in \mathbb{N}$ premier à p. Montrer qu'il existe $x, y \in \mathbb{Z}$ premiers entre eux tels que $p | x^2 + ny^2$ si et seulement si $\left(\frac{-n}{p}\right) = 1$.

b) Vérifier la formule suivante pour tout $w, x, y, z, n \in \mathbb{Z}$:

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2\,.$$

c) En déduire que si un entier N s'écrit $N = x^2 + ny^2$, et si un nombre premier $q | N$ s'écrit $q = z^2 + nw^2$ $(w, x, y, z \in \mathbb{Z})$, alors l'entier $\frac{N}{q}$ s'écrit aussi $\frac{N}{q} = a^2 + nb^2$ $(a, b \in \mathbb{Z})$.

d) On suppose que $n = 1, 2, 3$ et qu'il existe $a, b \in \mathbb{Z}$ premiers entre eux tels que $p | a^2 + nb^2$.

i) Montrer que l'on peut supposer que $|a|, |b| < \frac{p}{2}$ et $a^2 + nb^2 < p^2$.

ii) En déduire qu'il existe $x, y \in \mathbb{Z}$ tels que $p = x^2 + ny^2$.

e) En déduire les énoncés suivants :

i) un nombre premier impair p est somme de deux carrés d'entiers si et seulement si $p \equiv 1$ [4].

ii) un nombre premier impair p s'écrit sous la forme $x^2 + 2y^2$ $(x, y \in \mathbb{Z})$ si et seulement si $p \equiv 1, 3$ [8].

iii) un nombre premier p s'écrit sous la forme $x^2 + 3y^2$ $(x, y \in \mathbb{Z})$ si et seulement si $p = 3$ ou $p \equiv 1$ [3].

Solution de l'exercice 6.

a) Il existe $x, y \in \mathbb{Z}$ premiers entre eux tels que $p | x^2 + ny^2$ si et seulement si il existe $x, y \in \mathbb{Z}$ premiers entre eux tels que $x^2 \equiv -ny^2$ $[p]$ si et seulement si il existe $x, y \in \mathbb{Z}$ premiers entre eux tels que $\left(\frac{x}{y}\right)^2 \equiv -n$ $[p]$ (car p ne divise pas y : dans le cas contraire, p divise aussi x, ce qui contredit le fait que x et y sont premiers entre eux). Cela équivaut à dire que $-n$ est un carré modulo p, i.e. à $\left(\frac{-n}{p}\right) = 1$.

b) Il suffit de développer.

c) Par la question précédente, on remarque qu'il suffit de trouver $a, b \in \mathbb{Z}$ tels que

$$x = za \pm nwb\ , y = \mp wa + zb\,. \tag{1}$$

En résolvant ce système, on voit qu'il suffit de montrer que quitte à changer les signes de x, y, z, w, q divise $xz - nyw$ et $xw + yz$.

Or, on calcule

$$(xw+yz)(xw-yz) = x^2w^2 - y^2z^2 = (N-ny^2)w^2 - y^2(q-nw^2) = Nw^2 - qy^2\,,$$

donc q divise $xw+yz$ ou $xw-yz$.

Quitte à changer le signe de w, on peut supposer que q divise $xw-yz$. Il existe donc $b \in \mathbb{Z}$ tel que $yz - xw = bq$. Montrons qu'alors z divise $x+nbw$. Puisque z et w sont premiers entre eux, il suffit de montrer que z divise $(x+nbw)w = yz - bq + nbw^2 = yz - bz^2$, ce qui est clair. Il existe donc $a \in \mathbb{Z}$ tel que $x + nbw = az$.

On déduit alors des calculs précédents que $azw = yz - bz^2$, donc $y = aw + bz$. Finalement, on a construit $a, b \in \mathbb{Z}$ tels que $x = za - nwb$ et $y = wa + zb$, ce qui est bien la formule souhaitée (1).

Remarquons au passage que si x, y sont premiers entre eux, alors a et b sont premiers entre eux.

d) i) Posons $a' := a + rp$ et $b' := b + sp$, avec $r, s \in \mathbb{Z}$. On constate que l'on a toujours $p|a'^2 + nb'^2$. Par conséquent, on peut supposer que $|a|, |b| < \frac{p}{2}$, mais a et b peuvent alors avoir un facteur commun. Quitte à diviser alors a et b par $\mathrm{PGCD}(a,b)$ (ce PGCD n'est pas divisible par p), on obtient que $p|a^2 + nb^2$, $|a|, |b| < \frac{p}{2}$ et $\mathrm{PGCD}(a,b) = 1$.

Enfin, on a $a^2 + nb^2 < \left(\frac{p}{2}\right)^2 + 3\left(\frac{p}{2}\right)^2 \leq p^2$, ce qui conclut cette question.

ii) On raisonne par l'absurde : supposons la propriété fausse en général. Il existe alors un nombre premier p minimal tel que p divise un entier N qui s'écrit $a^2 + nb^2$, mais p lui-même ne s'écrit pas sous la forme $x^2 + ny^2$. Grâce à la question précédente, on peut supposer que $a^2 + nb^2 = N$, avec $N = pk$, $k \in \mathbb{N}$, $|a|, |b| < \frac{p}{2}$ et $N < p^2$. Soit $l \neq p$ un facteur premier de N. Nécessairement, $l < p$, et $l|a^2 + nb^2$, donc par minimalité de p, il existe $z, w \in \mathbb{Z}$ premiers entre eux tels que $l = z^2 + nw^2$. Grâce à la question c), il existe $c, d \in \mathbb{Z}$ premiers entre eux tels que $\frac{N}{l} = c^2 + nd^2$. On recommence ainsi pour tous les facteurs premiers de N distincts de p, et on obtient finalement que le quotient de N par $\frac{N}{p}$ est de la forme souhaitée. Par conséquent, la question c) assure que p s'écrit sous la forme $x^2 + ny^2$, avec $x, y \in \mathbb{Z}$ premiers entre eux, ce qui est contradictoire.

D'où la conclusion.

e) i) Les questions a) et d) assurent que p est une somme de deux carrés si et seulement si $\left(\frac{-1}{p}\right) = 1$ si et seulement si $p \equiv 1$ [4].

ii) Les questions a) et d) assurent que p est de cette forme si et seulement si $\left(\frac{-2}{p}\right) = 1$ si et seulement si $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)$ si et seulement si (loi de réciprocité quadratique) $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}}$ si et seulement si $p \equiv 1$ [8] ou $p \equiv 3$ [8]. Finalement, p s'écrit sous la forme $x^2 + 2y^2$ si et seulement si $p \equiv 1, 3$ [8].

iii) Les questions a) et d) assurent que p est de cette forme si et seulement si $p = 3$ ou $\left(\frac{-3}{p}\right) = 1$ si et seulement si $p = 3$ ou $\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)$ si et seulement si (en utilisant l'exercice 2) $p = 3$ ou $p \equiv 1$ [12] ou $p \equiv 7$ [12]. Finalement, p s'écrit sous la forme $x^2 + 3y^2$ si et seulement si $p = 3$ ou $p \equiv 1, 7$ [12] si et seulement si $p = 3$ ou $p \equiv 1$ [3].

Exercice 7 : Une autre preuve de la loi de réciprocité quadratique.

Soient p, q deux nombres premiers impairs distincts. On définit le groupe G par $G := (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. On note U le sous-groupe de G formé des deux éléments $(1,1)$ et $(-1,-1)$. Enfin, on définit H comme le quotient $H := G/U$. On pose alors $\pi := \prod_{x \in H} x \in H$.

a) Montrer qu'un système de représentants de H dans G est donné par les éléments $(i,j) \in G$, avec $i = 1, 2, \ldots, p-1$ et $j = 1, 2, \ldots, \frac{q-1}{2}$.

b) En déduire que

$$\pi = \left((p-1)!^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \bmod U\,.$$

c) Montrer qu'un système de représentants de H dans G est donné par les éléments $(k,k) \in G$, où k décrit les entiers entre 1 et $\frac{pq-1}{2}$ premiers à pq.

d) En déduire que

$$\pi = \left((p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \right) \bmod U\,.$$

e) En déduire la loi de réciprocité quadratique :

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

Solution de l'exercice 7.

a) Il est clair que deux éléments distincts du sous-ensemble $E_1 := \{(i,j) \in G : i = 1,\dots,p-1 \text{ et } j = 1,\dots,\frac{q-1}{2}\}$ de G ont une image distincte dans H : il ne peuvent être opposés l'un de l'autre dans G (regarder la seconde composante). Par conséquent, le morphisme quotient $G \to H$ induit une injection $E_1 \to H$. Or E_1 et H sont deux ensembles finis de même cardinal $\frac{(p-1)(q-1)}{2}$, donc le morphisme quotient induit une bijection $E_1 \xrightarrow{\cong} H$. Donc E_1 est bien un ensemble de représentants de H dans G.

b) On déduit de la question précédente que

$$\pi = \prod_{(i,j)\in E_1} (i,j) \bmod U\,.$$

Par conséquent, un calcul simple assure que

$$\pi = \left((p-1)!^{\frac{q-1}{2}}, \left(\prod_{j=1}^{\frac{q-1}{2}} j \right)^{p-1} \right) \bmod U\,.$$

Or la seconde composante de ce couple s'identifie à

$$\left(\prod_{j=1}^{\frac{q-1}{2}} j \right)^{p-1} = \left(\prod_{j=1}^{\frac{q-1}{2}} j^2 \right)^{\frac{p-1}{2}} = \left((-1)^{\frac{q-1}{2}} \prod_{j=1}^{\frac{q-1}{2}} j(-j) \right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\prod_{j=1}^{q-1} j \right)^{\frac{p-1}{2}} \quad [q]\,,$$

et donc on obtient bien

$$\pi = \left((p-1)!^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (q-1)!^{\frac{p-1}{2}} \right) \bmod U\,.$$

c) Montrons d'abord que le morphisme quotient $G \to H$ restreint à l'ensemble E_2 (le sous-ensemble de G défini dans cette question) est injectif : si deux éléments distincts $(k,k), (l,l) \in E_2$ s'envoient sur la même image dans H, alors $(k,k) = (-l,-l)$ dans G. Donc on en déduit que pq divise $k+l$. Or $0 < k+l < pq$, donc ceci n'est pas possible. Par conséquent, E_2 s'injecte dans H via le morphisme quotient. En outre, le cardinal de E_2 est égal à $\frac{pq-1}{2} - \frac{q-1}{2} - \frac{p-1}{2}$ puisqu'il y a exactement $\frac{q-1}{2}$ multiples de p entre 1 et $\frac{pq-1}{2}$ (de même pour les multiples de q). Donc $\#E_2 = \frac{(p-1)(q-1)}{2} = \#H$, d'où le résultat.

d) On déduit de la question précédente que

$$\pi = \prod_{1\le k\le \frac{pq-1}{2}, (k,pq)=1} (k,k) \bmod U\,.$$

Or on a

$$\prod_{1\leq k\leq \frac{pq-1}{2},(k,pq)=1} k = \frac{1.2\dots(p-1)(p+1)\dots(2p-1)(2p+1)\dots(\frac{q-1}{2}p-1)(\frac{q-1}{2}p+1)\dots\frac{pq-1}{2}}{q(2q)\dots\frac{p-1}{2}q},$$

donc

$$\prod_{1\leq k\leq \frac{pq-1}{2},(k,pq)=1} k \equiv \frac{(p-1)!^{\frac{q-1}{2}}.\frac{p-1}{2}!}{q^{\frac{p-1}{2}}.\frac{p-1}{2}!} \equiv (p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right)\ [p]\,.$$

Par symétrie, en échangeant les rôles de p et q, on obtient

$$\prod_{1\leq k\leq \frac{pq-1}{2},(k,pq)=1} k \equiv (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\ [q]\,.$$

Donc finalement, on a montré que

$$\pi = \left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right),(q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right)\ \text{mod}\ U\,.$$

e) En comparant les résultats obtenus dans les questions b) et d), on obtient que

$$\left((p-1)!^{\frac{q-1}{2}},(-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}}\right) = \left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right),(q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right)\ \text{mod}\ U\,,$$

ce qui implique que

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

d'où le résultat.

Exercice 8 : Encore une autre preuve de la loi de réciprocité quadratique.

a) Soit p un nombre premier impair, $a\in\mathbb{Z}$ tel que p ne divise pas a. Notons $r_1,\dots,r_{\frac{p-1}{2}}$ les restes des divisions euclidiennes de $a,2a,\dots,\frac{p-1}{2}a$ par p. Montrer que $\left(\frac{a}{p}\right)=(-1)^t$, où t est le nombre de r_i strictement supérieurs à $\frac{p-1}{2}$.

b) Soit q premier impair distinct de p. Avec les notations de la question précédente pour $a=q$, on note u la somme des $r_i\leq\frac{p-1}{2}$ et v la somme des $r_i>\frac{p-1}{2}$.

i) Montrer que $u+(pt-v)=\frac{p^2-1}{8}$.

ii) En déduire que $t\equiv\frac{p^2-1}{8}+\sum_{j=1}^{\frac{p-1}{2}}r_j\ [2]$.

iii) Montrer que $t\equiv\sum_{j=1}^{\frac{p-1}{2}}E(\frac{jq}{p})\ [2]$ (où $E(.)$ désigne la partie entière).

iv) En déduire la formule

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}}E(\frac{jq}{p})+\sum_{k=1}^{\frac{q-1}{2}}E(\frac{kp}{q})}\,.$$

v) En déduire la loi de réciprocité quadratique.

Solution de l'exercice 8.

a) On définit une partition de l'ensemble $\{1,\dots,\frac{p-1}{2}\}$ en deux sous-ensembles S et T définis par $S := \{i : r_i \leq \frac{p-1}{2}\}$ et $T := \{i : r_i > \frac{p-1}{2}\}$. Par définition, $t = \#T$. Considérons le produit $\Pi := \prod_{i=1}^{\frac{p-1}{2}} ia \in \mathbb{Z}$. Il est clair que

$$\Pi = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \,. \tag{2}$$

Or par définition des r_i, on a $\Pi \equiv \prod_{i=1}^{\frac{p-1}{2}} r_i \ [p]$. Pour tout $i \in T$, on pose $s_i := p - r_i$; alors $1 \leq s_i \leq \frac{p-1}{2}$. Par conséquent, on dispose de $\frac{p-1}{2}$ entiers dans l'ensemble $\{1,\dots,\frac{p-1}{2}\}$, donnés par les r_i pour $i \in S$ et les s_j pour $j \in T$. Montrons que ces nombres sont deux -à-deux distincts : si $i,j \in S$, on a $r_i = r_j$ si et seulement si $ia \equiv ja \ [p]$ si et seulement si p divise $i-j$ (car p ne divise pas a) si et seulement si $i = j$. De même, si $i,j \in T$, on a $s_i = s_j$ si et seulement si $i = j$. Enfin, si $i \in S$ et $j \in T$, on a $r_i = s_j$ si et seulement si $r_i = p - r_j$, ce qui implique que $p | i + j$, ce qui n'est pas possible car $2 \leq i + j \leq p - 1$.
Finalement, $\{1,\dots,\frac{p-1}{2}\}$ est la réunion (disjointe) de $\{r_i : i \in S\}$ et de $\{s_j : j \in T\}$. Or on a

$$\prod_{i=1}^{\frac{p-1}{2}} r_i \equiv \prod_{i\in S} r_i \prod_{j\in T} (p - s_j) \equiv \prod_{i\in S} r_i \prod_{j\in T} (-s_j) \equiv (-1)^t \prod_{i\in S} r_i \prod_{j\in T} s_j \ [p] \,.$$

Or par la remarque précédente, $\prod_{i\in S} r_i \prod_{j\in T} s_j = \left(\frac{p-1}{2}\right)!$, donc on obtient

$$\Pi \equiv (-1)^t \left(\frac{p-1}{2}\right)! \ [p] \,. \tag{3}$$

En combinant (2) et (3), on obtient $a^{\frac{p-1}{2}} \equiv (-1)^t \ [p]$. Or on sait que $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ [p]$, donc $\left(\frac{a}{p}\right) \equiv (-1)^t \ [p]$, d'où $\left(\frac{a}{p}\right) = (-1)^t$.

b) i) On a vu que $\{1,\dots,\frac{p-1}{2}\}$ est la réunion disjointe de $\{r_i : i \in S\}$ et de $\{s_j : j \in T\}$ (et les r_i, comme les s_j, sont deux-à-deux distincts). Donc

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i\in S} r_i + \sum_{j\in T} s_j = \sum_{i\in S} r_i + \sum_{j\in T} (p - r_j) = \sum_{i\in S} r_i + pt - \sum_{j\in T} r_j = u + (pt - v) \,,$$

or la somme de gauche vaut $\frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}$, d'où le résultat.

ii) On regarde l'égalité de la question b) i) modulo 2. On obtient $u + pt - v \equiv \frac{p^2-1}{8} \ [2]$, or p est impair, donc cette égalité devient $u + v + t \equiv \frac{p^2-1}{8} \ [2]$, d'où le résultat.

iii) Par définition, on a pour tout $1 \leq j \leq \frac{p-1}{2}$, $jq = pE(\frac{jq}{p}) + r_j$, donc en sommant sur tous les j, on obtient

$$q \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) + \sum_{j=1}^{\frac{p-1}{2}} r_j \,.$$

Or le terme de gauche vaut $q\frac{p^2-1}{8}$, donc modulo 2 cette égalité devient

$$q\frac{p^2-1}{8} \equiv p \sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) + \sum_{j=1}^{\frac{p-1}{2}} r_j \ [2] \,.$$

Or p et q sont impairs, donc on peut réécrire cette congruence sous la forme

$$\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) + \sum_{j=1}^{\frac{p-1}{2}} r_j \ [2] \,.$$

On conclut alors en combinant cette congruence avec celle de la question b) ii), pour trouver

$$t \equiv \sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) \ [2]\,.$$

iv) Les questions a) et b) iii) assurent que $\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right)}$. En échangeant les rôles de p et q, on obtient de même que $\left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}} E\left(\frac{jp}{q}\right)}$. Finalement, en faisant le produit de ces deux égalités, il reste :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right)+\sum_{j=1}^{\frac{q-1}{2}} E\left(\frac{jp}{q}\right)}\,.$$

v) Pour obtenir la loi de réciprocité quadratique, il suffit de montrer que $\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) + \sum_{j=1}^{\frac{q-1}{2}} E\left(\frac{jp}{q}\right) = \frac{(p-1)(q-1)}{4}$. Pour cela, on remarque que la première somme est égale à la somme $\sum_{j=1}^{\frac{p-1}{2}} \sum_{k=1}^{\frac{jq}{p}} 1$. Or cette dernière somme est le cardinal de l'ensemble E_1 formé des points de $\mathbb{Z}^2 \cap [1, \frac{p-1}{2}] \times [1, \frac{q-1}{2}]$ situés sous la droite d'équation $y = \frac{q}{p}x$. Symmétriquement, la seconde somme est égale au cardinal de l'ensemble E_2 formé des points de $\mathbb{Z}^2 \cap [1, \frac{p-1}{2}] \times [1, \frac{q-1}{2}]$ situés au-dessus de la droite d'équation $y = \frac{q}{p}x$.
Or la droite $y = \frac{q}{p}x$ ne contient aucun point à coordonnées entières dans le rectangle $[1, \frac{p-1}{2}] \times [1, \frac{q-1}{2}]$, donc E_1 et E_2 réalisent une partition de $\mathbb{Z}^2 \cap [1, \frac{p-1}{2}] \times [1, \frac{q-1}{2}]$. Donc $\#E_1 + \#E_2 = \frac{p-1}{2}\frac{q-1}{2}$, d'où le résultat.

Exercice 9 : L'objectif est de montrer le résultat suivant. Soit p un nombre premier tel que $p \equiv 1$ [4]. Alors 2 est une puissance quatrième modulo p si et seulement si p s'écrit sous la forme $p = A^2 + 64B^2$ $(A, B \in \mathbb{Z})$.

a) Si $m \in \mathbb{Z}, n \in \mathbb{N}$ sont des entiers premiers entre eux avec n impair, et si $n = p_1^{a_1} \dots p_r^{a_r}$ est la décomposition de n en facteurs premiers, on définit $\left(\frac{m}{n}\right) := \left(\frac{m}{p_1}\right)^{\alpha_1} \dots \left(\frac{m}{p_r}\right)^{\alpha_r}$.

   i) En utilisant la loi de réciprocité quadratique usuelle, montrer que $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ et $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, et démontrer la formule $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$ si m et n sont impairs et premiers entre eux.

   ii) Montrer que si m est un carré modulo n, alors $\left(\frac{m}{n}\right) = 1$. Montrer que la réciproque est fausse.

b) On fixe $p \equiv 1$ [4]. On sait que $p = a^2 + b^2$, avec $a, b \in \mathbb{Z}$, a impair. Montrer que

   i) $\left(\frac{a}{p}\right) = 1$.

   ii) $\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$.
   [Indication : on pourra calculer $(a+b)^2 + (a-b)^2$.]

   iii) $(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}}$ [p].

c) Avec les notations de la question b), soit $f \in \mathbb{Z}$ tel que $b \equiv af$ [p]. Montrer que $f^2 \equiv -1$ [p] et que $2^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}}$ [p].

d) Conclure.

Solution de l'exercice 9.

a) i) Puisque pour tout $m, n \in \mathbb{Z}$ impairs, on a $\left(\frac{-1}{mn}\right) = \left(\frac{-1}{m}\right)\left(\frac{-1}{n}\right)$, il suffit de montrer que la fonction $f(n) := (-1)^{\frac{n-1}{2}}$ est multiplicative, i.e. que $f(mn) = f(m)f(n)$. Pour cela, il suffit de montrer que pour tout $m, n \in \mathbb{Z}$ impairs, $\frac{m-1}{2} + \frac{n-1}{2} \equiv \frac{mn-1}{2}$ [2]. Cela revient à montrer que l'entier $mn - (m+n) + 1 = (m-1)(n-1)$ est divisible par 4, ce qui est clair puisque m et n sont impairs. D'où le premier point, à savoir $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

De même, pour déduire le deuxième point de la loi de réciprocité quadratique, il suffit de montrer que la fonction $g(n) := (-1)^{\frac{n^2-1}{8}}$ est multiplicative sur les entiers n impairs. Cela revient à montrer que pour tout m, n impairs, l'entier $(mn)^2 - 1 - (m^2-1) - (n^2-1)$ est divisible par 16. Or cet entier est égal à $(m^2-1)(n^2-1) = (m-1)(m+1)(n-1)(n+1)$, qui est bien multiple de 16 comme produit de quatre entiers pairs. D'où le deuxième point : $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Pour le troisième point, puisque pour tout (p, q, r, s) impairs deux-à-deux premiers entre eux, on a $\left(\frac{pq}{r}\right)\left(\frac{r}{pq}\right) = \left(\left(\frac{p}{r}\right)\left(\frac{r}{p}\right)\right)\left(\left(\frac{q}{r}\right)\left(\frac{r}{q}\right)\right)$ et $\left(\frac{p}{rs}\right)\left(\frac{rs}{p}\right) = \left(\left(\frac{p}{r}\right)\left(\frac{r}{p}\right)\right)\left(\left(\frac{p}{s}\right)\left(\frac{s}{p}\right)\right)$, il suffit de montrer que la fonction $h(m, n) := (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$ vérifie la même propriété de multiplicativité, à savoir $h(pq, r) = h(p, r)h(q, r)$ et $h(p, rs) = h(p, r)h(p, s)$. Cela revient à montrer que pour p, q, r, s impairs et deux-à-deux premiers entre eux, les entiers $(pq-1)(r-1)-(p-1)(r-1)-(q-1)(r-1)$ et $(p-1)(rs-1)-(p-1)(r-1)-(p-1)(s-1)$ sont divisibles par 8. Or ces entiers sont exactement $(p-1)(q-1)(r-1)$ et $(p-1)(r-1)(s-1)$, donc ils sont divisibles par 8 comme produit de trois entiers pairs. D'où le troisième point : $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

ii) Si m est un carré modulo n, alors m est un carré modulo p pour tout p premier divisant n, donc $\left(\frac{m}{p}\right) = 1$ pour tout facteur premier de n, donc $\left(\frac{m}{n}\right) = 1$.

La réciproque est fausse : par exemple, $\left(\frac{-1}{21}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right) = (-1)(-1) = 1$, mais -1 n'est pas un carré modulo 21 car ce n'est pas un carré modulo 3.

b) i) Modulo a, on a $p \equiv b^2$ [a], donc $\left(\frac{p}{a}\right) = 1$ par a) ii). Par a) i), on a $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)$ puisque $p \equiv 1$ [4]. Donc finalement, $\left(\frac{a}{p}\right) = 1$.

ii) Comme indiqué, on calcule $(a+b)^2+(a-b)^2 = 2(a^2+b^2) = 2p$. Donc $2p \equiv (a-b)^2$ [$a+b$], donc par a) ii), on a $\left(\frac{2p}{a+b}\right) = 1$. Or par a) i), on a $\left(\frac{2p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{p}{a+b}\right)$, et $\left(\frac{p}{a+b}\right) = \left(\frac{a+b}{p}\right)$ (il est clair que p ne divise pas $a+b$). Donc on a $\left(\frac{a+b}{p}\right) = \left(\frac{2}{a+b}\right)$. Or par a) i), on a $\left(\frac{2}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$, d'où finalement $\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$.

iii) Puisque $(a+b)^2 = a^2 + b^2 + 2ab = p + 2ab$, on a $(a+b)^2 \equiv 2ab$ [p]. On élève à la puissance $\frac{p-1}{4}$, et on trouve bien $(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}}$ [p].

c) Puisque $p = a^2 + b^2$, on a $b^2 \equiv -a^2$ [p]. Or $b^2 \equiv f^2a^2$ [p], et p ne divise pas a, donc $f^2 \equiv -1$ [p]. On remarque d'abord que

$$(ab)^{\frac{p-1}{4}} \equiv (a^2 f)^{\frac{p-1}{4}} \equiv a^{\frac{p-1}{2}} f^{\frac{p-1}{4}} \equiv \left(\frac{a}{p}\right) f^{\frac{p-1}{4}} \equiv f^{\frac{p-1}{4}},$$

où la dernière égalité utilise la question b) i).

Donc on a

$$2^{\frac{p-1}{4}} f^{\frac{p-1}{4}} \equiv (2ab)^{\frac{p-1}{4}} \equiv (a+b)^{\frac{p-1}{2}} \equiv \left(\frac{a+b}{p}\right) \ [p]$$

où la deuxième congruence utilise la question b) iii). Donc

$$2^{\frac{p-1}{4}} f^{\frac{p-1}{4}} \equiv (-1)^{\frac{(a+b)^2-1}{8}} \ [p]$$

par la question b) ii). Or $f^2 \equiv -1\ [p]$, donc $(-1)^{\frac{(a+b)^2-1}{8}} \equiv f^{\frac{(a+b)^2-1}{4}}\ [p]$. Or $\frac{(a+b)^2-1}{4} = \frac{p-1}{4} + \frac{ab}{2}$, donc $f^{\frac{(a+b)^2-1}{4}} \equiv f^{\frac{p-1}{4}} f^{\frac{ab}{2}}\ [p]$. Finalement, on a donc

$$2^{\frac{p-1}{4}} f^{\frac{p-1}{4}} \equiv f^{\frac{p-1}{4}} f^{\frac{ab}{2}}\ [p]\,,$$

donc en simplifiant,

$$2^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}}\ [p]\,.$$

d) On sait qu'un entier $x \in \mathbb{Z}$ premier à p est une puissance quatrième modulo p si et seulement si $x^{\frac{p-1}{4}} \equiv 1\ [p]$ (puisque le morphisme de groupes $\mathbb{F}_p^* \to \mathbb{F}_p^*$ défini par $t \mapsto t^4$ a un noyau d'ordre 4 formé des racines 4-ièmes de l'unité). Donc 2 est une puissance quatrième modulo p si et seulement si $2^{\frac{p-1}{4}} \equiv 1\ [p]$. Par la question c), ceci équivaut à $f^{\frac{ab}{2}} \equiv 1\ [p]$. Or f est d'ordre 4 dans $\mathbb{F}_p^*$, donc $f^{\frac{ab}{2}} \equiv 1\ [p]$ si et seulement si 4 divise $\frac{ab}{2}$ si et seulement si 8 divise ab. Or a est impair, donc cette dernière condition équivaut à 8 divise b. Finalement, on a bien l'équivalence souhaitée, en prenant $A = a$ et $b = 8B$.