DM 6 - Loi de réciprocité quadratique – corrigé

1 Symbole de Legendre

1. Soit $x \in [\![1, p-1]\!]$. Alors x^2 est un carré modulo p, donc $r_p(x^2) \in [\![1, p-1]\!]$. Réciproquement, si $y \in [\![1, p-1]\!]$ est un carré modulo p, il existe un $x \in \mathbb{Z}$ tel que $y \equiv x^2\,[p]$. On peut de plus supposer que $x \in [\![1, p-1]\!]$ (quitte à changer x en $r_p(x)$, ce qui ne change pas sa classe de congruence modulo p). Donc, l'image de θ_p est l'ensemble des $y \in [\![1, p-1]\!]$ qui sont des carrés modulo p.
   Soit $x \in [\![1, p-1]\!]$. Si $x' \in [\![1, p-1]\!]$, $\theta_p(x) = \theta_p(x')$ ssi $x^2 \equiv x'^2\,[p]$ ssi p divise $(x-x')(x+x')$. Par le lemme d'Euclide, c'est encore équivalent à demander que p divise $x + x'$ ou p divise $x - x'$.
   Comme $x, x' \in [\![1, p-1]\!]$, les seules solutions sont $x' = x$ et $x' = p - x$. De plus, $x \neq p - x$ car sinon p serait pair. Ainsi, $\theta_p(x)$ a exactement deux antécédents : x et $p - x$.

2. On a identifié l'image de θ_p et chaque élément de cette image a deux antécédents par θ_p. Par principe de division, on a donc :
$$p - 1 = 2 \times |\operatorname{Im}(\theta_p)|.$$
   Doncn il y a exactement $\dfrac{p-1}{2}$ carrés modulo p parmi les entiers de $[\![1, p-1]\!]$.

3. Soit $a \in [\![1, p-1]\!]$. Par le théorème de Fermat, $a^{p-1} \equiv 1\,[p]$. Donc, en notant $x = a^{\frac{p-1}{2}}$, $x^2 \equiv 1\,[p]$. Donc, p divise $(x-1)(x+1)$; donc p divise $x - 1$ ou p divise $x + 1$ (lemme d'Euclide). Donc,
$$a^{\frac{p-1}{2}} \equiv \pm 1\,[p].$$

4. **Critère d'Euler.**

   (a) Si $a \in [\![1, p-1]\!]$ est un carré modulo p, il existe $x \in [\![1, p-1]\!]$ tel que $a \equiv x^2\,[p]$. Alors, par le théorème de Fermat, $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1\,[p]$.
   Ceci montre que les $a \in [\![1, p-1]\!]$ qui sont des carrés modulo p vérifient $a^{\frac{p-1}{2}} \equiv 1\,[p]$. Or, on a admis qu'au plus $\dfrac{p-1}{2}$ éléments de $[\![1, p-1]\!]$ vérifient cette équation et il y a $\dfrac{p-1}{2}$ carrés modulo p dans $[\![1, p-1]\!]$. Ceci montre que
$$\forall a \in [\![1, p-1]\!], \left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1\,[p].$$

Comme pour $a \in [\![1, p-1]\!]$, les deux membres valent 1 ou -1 (modulo p à droite), on en déduit que :

$$\forall a \in [\![1, p-1]\!], \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \, [p].$$

L'égalité est encore vraie en $a = 0$ (les deux membres valent 0) ; comme les deux membres ne dépendent (modulo p à droite) que de la classe de a modulo p, on en déduit que l'égalité est vraie pour tout $a \in \mathbb{Z}$.

(b) Soient $a, b \in \mathbb{Z}$. On a

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}.$$

Avec la question précédente, on en déduit que pour tous $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Comme les deux membres valent -1, 0 ou 1, la congruence modulo p est en fait une égalité.

(c) On a $\frac{23-1}{2} = 11$. On cherche donc la valeur de 5^{11} modulo 23. Or, $5^2 \equiv 2\,[23]$, donc $5^4 \equiv 4\,[23]$ et $5^8 \equiv 16\,[23]$. D'où $5^11 = 5^8 \times 5^2 \times 5 \equiv 16 \times 2 \times 5 \equiv 160 \equiv -1\,[23]$. Donc, 5 n'est pas un carré modulo 23.

(d) Ainsi, -1 est un carré modulo p ssi $(-1)^{\frac{p-1}{2}} \equiv 1\,[p]$ ssi $(-1)^{\frac{p-1}{2}} = 1$ ssi $\frac{p-1}{2}$ est pair ssi $p \equiv 1\,[4]$.

5. **Un (autre) lemme de Gauss.**

(a) L'intervalle $I = [\![\frac{1-p}{2}, \frac{p-1}{2}]\!]$ est de cardinal p ; donc tout entier est congru à exactement un entier dans cet intervalle. De plus, l'ensemble des entiers qui s'écrivent $\varepsilon \times k$, avec $\varepsilon = \pm 1$ et $k \in S_p$ est $I - \{0\}$ (et cette écriture est unique).
Si $s \in S_p$, as n'est pas divisible par p et donc as est congru modulo p à un unique élément de $I - \{0\}$, qui s'écrit donc de façon unique sous la forme $\varepsilon \times k$, avec $\varepsilon = \pm 1$ et $k \in S_p$.

(b) Comme S_p est un ensemble fini, il suffit de montrer que f est injective pour montrer qu'elle est bijective. Soient $s, s' \in S_p$ tels que $f(s) = f(s')$. Avec la définition de f, on en déduit que $as \equiv \pm as'\,[p]$; comme a est premier avec p, on a donc $s \equiv s'\,[p]$ ou $s \equiv -s'\,[p]$. Comme s et s' sont dans S_p, la seule possibilité est $s = s'$.
Donc, f est injective ; donc elle est bijective.

(c) Notons P ce produit. La question précédente permet d'effectuer le changement de variable $s = f(t)$ (avec $s, t \in S_p$) dans le produit. On a donc :

$$P = \prod_{t \in S_p} f(t) \equiv \prod_{t \in S_p} \big(e_t(a) a t\big) \equiv a^{\frac{p-1}{2}} P \prod_{t \in S_p} e_t(a)\,[p].$$

On peut simplifier par P car P, produit d'éléments premiers avec p, est premier avec p. On a donc

$$1 \equiv a^{\frac{p-1}{2}} \prod_{s \in S_p} e_s(a)\,[p].$$

L'égalité souhaitée s'en déduit, en remarquant que $\prod_{s\in S_p} e_s(a) = \pm 1$.

(d) D'après la question précédente et la formule d'Euler, on a la congruence $\left(\frac{a}{p}\right) \equiv \prod_{s\in S_p} e_s(a)\,[p]$. Comme les deux membres valent 1 ou -1, ils sont en fait égaux, et pas seulement congrus modulo p.

6. (a) Soit $s \in S_p$. Alors, $2s \in [\![0, p-1]\!]$ et $2s \in S_p \iff s \le \frac{p-1}{4}$.
Si au contraire u est tel que $\frac{p-1}{4} < u \le \frac{p-1}{2}$, alors $\frac{p-1}{2} < 2u \le p-1$;alors $2u$ est congru modulo p à un entier dans $-S_p$. Donc, $e_s(2) = 1$ si $s \in [\![0, \frac{p-1}{4}]\!]$ et $e_s(2) = -1$ si $\frac{p-1}{4} < s \le \frac{p-1}{2}$. Par la question précédente, on en déduit que $\left(\frac{2}{p}\right) = (-1)^{n(p)}$, où $n(p)$ est défini comme dans l'énoncé.

(b) Supposons que p est congru à 1 modulo 4. Alors, $\frac{p-1}{4}$ est un entier et $n(p) = \frac{p-1}{2} - \frac{p-1}{4} + 1 - 1 = \frac{p-1}{4}$ (on a retranché 1 car l'inégalité de gauche est stricte).
Pour un tel p, on a donc $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$. Ceci vaut 1 si $p \equiv 1\,[8]$ et -1 si $p \equiv -3\,[8]$.
Supposons que p est congru à 3 modulo 4. Alors l'inégalité $\frac{p-1}{4} < u$ est équivalente à l'inégalité $\frac{p+1}{4} \le u$ (car $\frac{p+1}{4}$ est le plus petit entier strictement plus grand que $\frac{p-1}{4}$). Donc, dans ce cas, $n(p) = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4}$. Pour un tel p, $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$.
Ceci vaut 1 si $p \equiv -1\,[8]$ et -1 si $p \equiv 3\,[8]$.

(c) Soit p un diviseur premier impair de N. Comme $2 \equiv (4p_1 \ldots {}^{p}_{n})^2\,[N]$, 2 est un carré modulo p. D'après le calcul du symbole de Legendre, on en déduit que $p \equiv \pm 1\,[8]$.

(d) L'entier $\frac{N}{2}$ est impair et a les mêmes facteurs premiers impairs que N. Tous ses facteurs premiers sont donc congrus à $\pm 1\,[8]$. Mais comme $\frac{N}{2} = 8p_1^2 \ldots p_n^2 - 1$, $\frac{N}{2}$ n'a aucun diviseur premier parmi les p_i (sinon p_i diviserait 1). Donc, tous les diviseurs premiers impairs de N sont congrus à 1 modulo 8. Comme $\frac{N}{2}$ est un produit de tels diviseurs premiers, on obtient $\frac{N}{2} \equiv 1\,[8]$; c'est absurde : $\frac{N}{2} \equiv -1\,[8]$.

7. Soit p un nombre premier impair, différent de 3. On remarque que 1 est un carré modulo 3 mais pas 2. Donc, $\left(\frac{p}{3}\right) = 1$ ssi $p \equiv 1\,[3]$, -1 sinon. De plus, par la loi de

réciprocité quadratique, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ si $\equiv 1\,[4]$ et $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ si $p \equiv 3\,[4]$. Pour conclure, on regarde la congruence de p modulo 12 :

- Si $p \equiv 1\,[12]$, $\left(\frac{3}{p}\right) = 1$.
- Si $p \equiv 7\,[12]$, $\left(\frac{3}{p}\right) = -1$.
- Si $p \equiv 5\,[12]$, $\left(\frac{3}{p}\right) = -1$.
- Si $p \equiv 11\,[12]$, $\left(\frac{3}{p}\right) = 1$.

8. On calcule le symbole de Legendre $\left(\frac{101}{641}\right)$.

$$\left(\frac{101}{641}\right) = \left(\frac{641}{101}\right) = \left(\frac{35}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{7}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{7}\right) = 1 \times \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

Donc, 101 n'est pas un carré modulo 641.

2 Une démonstration de la loi de réciprocité quadratique

9. (a) Soit $x \in \mathbb{R} \setminus \pi\mathbb{Z}$. On linéarise $\sin(mx)$:

$$\begin{aligned}
\sin(mx) &= \operatorname{Im}\big((\cos x + i \sin x)^m\big) \\
&= \operatorname{Im}\Big(\sum_{k=0}^{m} \binom{m}{k} (i \sin x)^k (\cos x)^{m-k}\Big) \\
&= \frac{1}{i} \sum_{j=0}^{n} \binom{m}{2j+1} (i \sin x)^{2j+1} (\cos x)^{m-(2j+1)} \\
&= \sum_{j=0}^{n} \binom{2n+1}{2j+1} (-1)^j (\sin^{2j+1} x)(1-\sin^2 x)^{n-j}.
\end{aligned}$$

D'où, en divisant par $\sin x \neq 0$:

$$\frac{\sin(mx)}{\sin x} = \sum_{j=0}^{n} \binom{2n+1}{2j+1} (-1)^j (\sin^2 x)^j (1-\sin^2 x)^{n-j}.$$

(b) La question précédente montre que pour tout $x \in \mathbb{R} \setminus \pi\mathbb{Z}$, $P(\sin^2 x) = \dfrac{\sin(mx)}{\sin x}$. Avec $x = \dfrac{2\pi j}{m}$, pour un $j \in [\![1, n]\!]$, on obtient donc :

$$P\left(\sin^2 \frac{2\pi j}{m}\right) = \frac{\sin(2\pi j)}{\sin x} = 0.$$

Donc, les réels $\sin^2 \dfrac{2\pi j}{m}$ sont des racines de P. De plus, ces réels sont distincts. En effet, les angles étant entre 0 et π, les sinus sont positifs ; s'il y a égalité entre deux valeurs, on a deux indices $i, j \in [\![1, n]\!]$ tels que $\dfrac{2\pi j}{m} = \dfrac{2\pi i}{m}$ ou $\dfrac{2\pi j}{m} = \pi - \dfrac{2\pi i}{m}$. La première égalité implique que $i = j$, la deuxième est impossible car on aurait $2(i + j) = m$, mais m est impair.

(c) On connait n racines distinctes à P, qui est de degré n. Par un résultat sur les polynômes admis en début d'année, on sait qu'il existe $\lambda \in \mathbb{R}$ tel que $P = \lambda \displaystyle\prod_{j=1}^{n} \Big(X - \sin^2 \frac{2\pi j}{m}\Big)$.

(d) On cherche le coefficient dominant λ de P. On peut l'obtenir à partir de la définition de P en isolant le terme en X^n quand on développe P. On a

$$P = \sum_{j=0}^{n} \binom{2n+1}{2j+1} (-1)^j X^j \sum_{k=0}^{n-j} \binom{n-j}{k} (-1)^k X^k = \sum_{j=0}^{n} \sum_{k=0}^{n-j} \binom{2n+1}{2j+1} \binom{n-j}{k} (-1)^{j+k} X^{j+k}.$$

Les termes en X^n sont ceux pour lesquels $k = n - j$. Donc,

$$\lambda = \sum_{j=0}^{n} \binom{2n+1}{2j+1} \binom{n-j}{n-j} (-1)^n = (-1)^n \frac{2^{2n+1}}{2} = (-4)^n.$$

On a utilisé le fait bien connu que si $N \geq 1$, la somme des coefficients binomiaux $\dbinom{N}{\ell}$ pour ℓ pair ou impair vaut 2^{N-1}.

10. Avec les notations de la question 6, on a

$$\left(\frac{q}{p}\right) = \prod_{s \in S_p} e_s(q).$$

Soit $s \in S_p$. Avec les notations précédentes, $qs \equiv e_s(q) s_q \, [p]$. On multiplie par $\dfrac{2\pi}{p}$:

$$\frac{2\pi q s}{p} \equiv \frac{2\pi e_s(q) s_q}{p} \, [2\pi].$$

Par 2π-périodicité et imparité de sin (on rappelle que $e_s(q) = \pm 1$, on a donc :

$$\sin\left(\frac{2\pi q s}{p}\right) = e_s(q) \sin\left(\frac{2\pi s_q}{p}\right).$$

On a donc :

$$\left(\frac{q}{p}\right) = \prod_{s \in S_p} \frac{\sin \frac{2\pi q s}{p}}{\sin \frac{2\pi s_q}{p}}.$$

De plus, on a montré que $s \mapsto s_q$ est une bijection de S_p. Donc, $\displaystyle\prod_{s \in S_p} \sin \frac{2\pi s_q}{p} = \prod_{s \in S_p} \sin \frac{2\pi s}{p}$. On en déduit la formule annoncée.

11. Soit $s \in S_p$. On applique l'identité trigonométrique trouvée précédemment (avec $x = \dfrac{2\pi s}{p}$, $m = q$ et $n = \dfrac{q-1}{2}$) :

$$\frac{\sin \frac{2\pi q s}{p}}{\sin \frac{2\pi s}{p}} = (-4)^{\frac{q-1}{2}} \prod_{t=1}^{\frac{q-1}{2}} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{q} \right).$$

On remarque que t varie dans S_q. On a donc :

$$\left(\frac{q}{p}\right) = \prod_{s \in S_p} \frac{\sin \frac{2\pi q s}{p}}{\sin \frac{2\pi s}{p}} = \prod_{s \in S_p} (-4)^{\frac{q-1}{2}} \prod_{t \in S_q} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{q} \right).$$

12. Dans l'expression précédente, on change les termes dans les facteurs $\left(\sin^2 \dfrac{2\pi s}{p} - \sin^2 \dfrac{2\pi t}{q} \right)$; $\dfrac{q-1}{2}$ signes *moins* sortent du produit interne, donc :

$$\left(\frac{q}{p}\right) = \prod_{s \in S_p} 4^{\frac{q-1}{2}} \prod_{t \in S_q} \left(\sin^2 \frac{2\pi s}{q} - \sin^2 \frac{2\pi s}{p} \right).$$

Mais on a aussi :

$$\left(\frac{p}{q}\right) = \prod_{t \in S_q} (-4)^{\frac{p-1}{2}} \prod_{s \in S_q} \left(\sin^2 \frac{2\pi s}{q} - \sin^2 \frac{2\pi s}{p} \right),$$

en échangeant les rôles de p et q. Les membres de droite diffèrent par $(-1)^{\frac{(p-1)(q-1)}{4}}$. Donc,

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

Admirable formule.