Prérequis. Symbole de Legendre.

Lemme 0.0.1 (critère d'Euler)**.** *Soient p un nombre premier impair et $a \in \mathbf{Z}$. On a alors :*

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

Démonstration. Si p divise a c'est évident. Sinon, le petit théorème de Fermat donne $a^{p-1} = 1$ dans $\mathbf{F}_p^\times$, donc $a^{(p-1)/2} = \pm 1$. Si $a = b^2$ alors $a^{(p-1)/2} = b^{p-1} = 1$, et seuls les carrés non nuls vérifient ceci puisqu'il y en a $(p-1)/2$, degré du polynôme $X^{(p-1)/2} - 1$. □

Théorème 0.0.2 (loi de réciprocité quadratique)**.** *Pour tous nombres premiers impairs $p \neq q$, on a :*

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

Démonstration. Notons $A = \{2, 4, 6, \ldots, p-1\}$ et $\overline{A}$ sa réduction modulo p. Pour $a \in A$, on note aussi r_a le reste de la division euclidienne de qa par p.

Étape 1. L'application

$$\begin{aligned} A &\longrightarrow \overline{A} \\ a &\longmapsto (-1)^{r_a}\overline{r_a} \end{aligned}$$

est bien définie et bijective. En effet, si r_a est pair alors $r_a \in A$, sinon $p - r_a \in A$ avec $p - r_a \equiv -r_a \ [p]$. Elle est injective car si $(-1)^{r_a} r_a \equiv (-1)^{r_b} r_b \ [p]$ alors $qa \equiv \pm qb \ [p]$ donc $a \equiv \pm b \ [p]$. Comme $0 < a + b < 2p$, si $a \neq b$ alors $a + b = p$. C'est impossible car p est impair. Enfin, puisque $|\overline{A}| \leqslant |A|$, l'application est bien bijective.

Étape 2. On a $\left(\frac{q}{p}\right) = (-1)^{\sum_{a\in A} r_a}$. En effet, par définition :

$$\prod_{a\in A} r_a \equiv q^{\frac{p-1}{2}} \prod_{a\in A} a \ [p]$$

et l'étape 1 montre que :

$$\prod_{a\in A} a \equiv (-1)^{\sum_{a\in A} r_a} \prod_{a\in A} r_a \ [p].$$

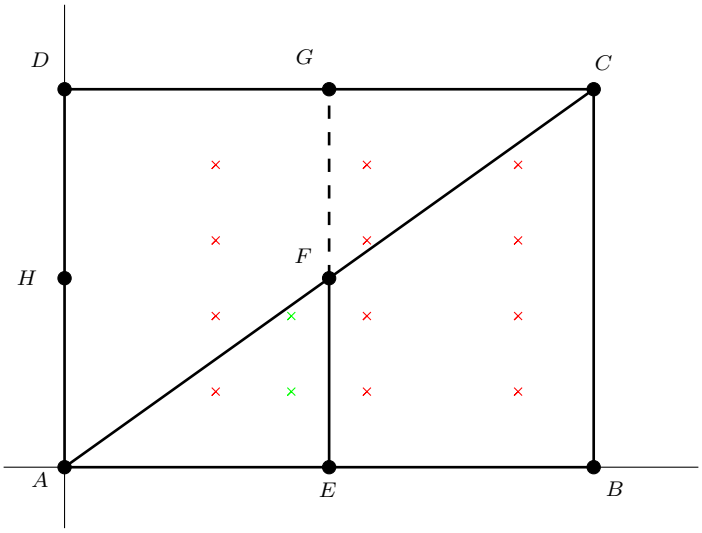
Ainsi $q^{\frac{p-1}{2}} \equiv (-1)^{\sum_{a\in A} r_a} \ [p]$, et le critère d'Euler conclut.

Étape 3. Comme r_a est le reste de la division euclidienne de qa par p, on peut écrire $qa = p\left\lfloor \frac{qa}{p} \right\rfloor + r_a$ et en déduire que :

$$\sum_{a\in A} r_a \equiv \sum_{a\in A} \left\lfloor \frac{qa}{p} \right\rfloor \ [2].$$

Il reste seulement à calculer ce membre de droite, ce que l'on fait par dénombrement.

On construit les points suivants dans $\mathbf{R}^2$: A est l'origine, $B = (p, 0)$, $C = (p, q)$ et $D = (0, q)$. E, F, G et H sont les milieux respectifs de $[AB]$, $[AC]$, $[DC]$ et $[AD]$. On s'intéresse au nombre (modulo 2) de points entiers d'abscisse paire à l'intérieur (strict) du rectangle $ABCD$.



Soit $a \in A$. Le nombre de points d'abscisse a dans $ABCD$ est pair (il y en a $q-1$). Comme p et q sont premiers entre eux, il n'y a aucun tel point sur le segment $[AC]$. Ainsi, il y a autant de points d'abscisse paire dans le triangle FCG que dans le trapèze $EBCF$, modulo 2. Comme les points d'abscisse paire de FCG correspondent bijectivement avec les points d'abscisse impaire de AEF, le nombre de points d'abscisse paire dans le grand triangle ABC est égal modulo 2 au nombre total de points dans le triangle AEF.

Ce premier nombre vaut exactement $\sum_{a \in A} \left\lfloor \frac{qa}{p} \right\rfloor$ car pour chaque abscisse paire $a \in A$, il y a bien $\left\lfloor \frac{qa}{p} \right\rfloor$ points sous le segment $[AC]$ qui est de pente q/p. En notant μ le second nombre, on a donc $\left(\frac{q}{p}\right) = (-1)^\mu$. De même symétriquement, $\left(\frac{p}{q}\right) = (-1)^\nu$ où ν est le nombre de points entiers dans le triangle AFH. Au total, $\mu + \nu = \frac{p-1}{2} \cdot \frac{q-1}{2}$ d'où le résultat. □

Remarques.

— C'est trop long si l'on démontre le critère d'Euler, alors autant laisser celui-ci dans le plan (ou l'ignorer complètement, mais le dire quand on l'utilise). Et c'est plus facile de donner les idées de la preuve que de tout écrire.

— Il faut bien s'entraîner à donner à l'oral les justifications géométriques. Elles sont faciles, mais après avoir répété cinquante fois le mot abscisse, on peut perdre le jury. Et il ne faut pas s'emmêler entre les abscisses paires ou non.

— Le dessin fait très bonne figure au tableau. En plus il permet de voir un peu magiquement le symbole de Legendre : c'est -1 exposant le nombre de points

dans le petit triangle en bas à gauche. Une fois qu'on a vu ça, la réciprocité quadratique devient évidente ! C'est une bonne idée d'insister un peu sur cette visualisation.

— Il faut absolument savoir justifier pourquoi il n'y a aucun point sur $]AC[$. Un point entier non nul (x, y) sur (AC) vérifie $x/y = p/q$, donc $qx = py$, et comme p et q sont premiers entre eux, q divise y et p divise x, avec le même quotient. Donc c'est impossible que (x, y) soit sur le segment $]AC[$.

— Une fois que l'on a bien compris la démonstration, la partie difficile à retenir sont l'étape 2 et le début de l'étape 3. L'argument géométrie à la fin est le cœur de la démonstration, mais c'est aussi la partie la plus facile à retenir.

— Il faut bien retenir où apparaissent le fait que p et q doivent être impairs. Pour p, c'est quand on explique que les points d'abscisse paire de FCG sont en bijection avec les points d'abscisse impaire de AEF, par rotation centrale de centre F. C'est l'imparité de p qui fait changer la parité des abscisses. Pour q, c'est le fait que chaque colonne contienne un nombre pair de points, ce qui permet l'égalité modulo 2 entre les points d'abscisse paire dans FCG et ceux dans $EBCF$. On remarque que si l'on pose $p = 2$ ou $q = 2$, le dessin se casse la figure.

Recasages.

— 120 : L'étude des carrés dans les anneaux $\mathbf{Z}/n\mathbf{Z}$ est vraiment bien dans le thème, le théorème chinois y est obligatoire et les symboles de Legendre/Jacobi sont bienvenus. Le rapport de jury demande en plus de faire une section à propos du cas où n est premier, super nickel.

— 121 : On utilise le fait que $\mathbf{Z}/p\mathbf{Z}$ est un corps quand p est premier, on utilise le petit théorème de Fermat, tout tourne autour de nombres premiers. On peut même mettre l'accent sur le segment $]AC[$ qui ne contient aucun point entier, si l'on a vraiment peur de ce recasage.

— 123 : C'est vraiment parfait si on fait une partie sur les carrés dans les corps finis. Sinon, c'est un peu hors sujet !

— 126 : Les symboles de Legendre donnent une réponse directe à l'existence de solutions aux équations de la forme $x^2 \equiv a$ modulo n. En plus, le rapport de jury en parle en disant que c'est naturel.

— 190 : Difficile de faire mieux qu'une approche combinatoire à un théorème abstrait. On montre que l'on sait compter des choses, et l'on en déduit un joli théorème.