La loi de réciprocité quadratique

Alexandre Junod, Lycée Denis-de-Rougemont (Neuchâtel), alexandre.junod@rpn.ch

Véritable chef d'oeuvre de la théorie des nombres, la *loi de réciprocité quadratique* a été découverte indépendamment par Leonhard Euler en 1783 et Adrien-Marie Legendre en 1785. Carl Friedrich Gauss en donna une première démonstration complète en 1801 et on compte aujourd'hui plus de 200 preuves recensées sur la page internet `http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`. Nous présentons ici une des preuves de Gotthold Eisenstein (1823−1852) qui nécessite peu de pré-requis.

1 Le lemme de Gauss et le petit théorème de Fermat

$$\begin{array}{c|c} kq & p \\ \cline{2-2} \vdots & a_k \\ r_k & \end{array}$$

On considère un nombre premier $p \neq 2$, un entier q non divisible par p et un entier $k \in \{1, 2, \ldots, N\}$ avec $N = \frac{p-1}{2}$. Par division euclidienne, on peut trouver des nombres $a_k = \lfloor kq/p \rfloor$ et $r_k \in \{1, 2, \ldots, p-1\}$ tels que $kq = a_k p + r_k$.

On pose alors $\widehat{r}_k = r_k$ si $r_k \leqslant N$, $\widehat{r}_k = r_k - p$ si $r_k > N$ et on note n le nombre de valeurs de k pour lesquelles $\widehat{r}_k < 0$.

Effectuons le produit modulo p de tous les nombres $kq \equiv r_k$ (pour $k = 1, 2, \ldots, N$) :

$$q^N N! \;\equiv\; \prod_{k=1}^{N} r_k \;\equiv\; \prod_{k=1}^{N} \widehat{r}_k \;=\; (-1)^n \prod_{k=1}^{N} |\widehat{r}_k|.$$

Les N nombres entiers $|\widehat{r}_k|$ vérifient clairement $1 \leqslant |\widehat{r}_k| \leqslant N$ et ils sont tous différents : si $\widehat{r}_k = \widehat{r}_s$, on aurait $r_k = r_s$, donc $(k - s)q = (a_k - a_s)p$, mais p ne divise ni q ni $|k - s| < N$, sauf si $k = s$. De même, si $\widehat{r}_k = -\widehat{r}_s$, on aurait $r_k + r_s = p$, donc $(k + s)q = (1 + a_s + a_k)p$, mais comme p ne divise ni q ni $k + s \in \{2, 3, \ldots, p - 1\}$, la supposition initiale est absurde. Ainsi l'ensemble $\{|\widehat{r}_k| : 1 \leqslant k \leqslant N\}$ est simplement $\{1, 2, \ldots, N\}$ et la congruence ci-dessus devient $q^N N! \;\equiv\; (-1)^n N!$. Comme p ne divise pas $N!$, on en déduit que $q^N \equiv (-1)^n \pmod{p}$. Cette congruence constitue le *lemme de Gauss* et le *petit théorème de Fermat* en découle immédiatement : p divise $(q^N - 1)(q^N + 1) = q^{p-1} - 1$, autrement dit $q^{p-1} \equiv 1$ modulo p (lorsque, rappelons-le, q n'est pas divisible par le nombre premier p).

Lemme d'Eisenstein. Supposons que l'entier q soit impair et effectuons la somme des nombres kq :

$$q \sum_{k=1}^{N} k \;=\; p \sum_{k=1}^{N} a_k + \sum_{k=1}^{N} r_k \;=\; p \sum_{k=1}^{N} a_k + \sum_{k=1}^{N} \widehat{r}_k + np.$$

Modulo 2, on a $p \equiv q \equiv 1 \equiv -1$, donc on peut écrire $\sum k \;\equiv\; \sum a_k + \sum |\widehat{r}_k| - n$. Comme les ensembles $\{|\widehat{r}_k| : 1 \leqslant k \leqslant N\}$ et $\{1, 2, \ldots, N\}$ coïncident, on a $n \;\equiv\; \sum a_k \pmod{2}$, ce qui permet de réécrire le lemme de Gauss sous la forme $q^N \equiv (-1)^S \pmod{p}$ avec $S = \sum_{k=1}^{N} a_k = \sum_{k=1}^{N} \left\lfloor \frac{kq}{p} \right\rfloor$.

2 Résidus quadratiques

Modulo p, les nombres $1^2, 2^2, \dots, N^2$ (avec $N = \frac{p-1}{2}$) représentent tous les carrés non nuls (car $(p-a)^2 \equiv a^2$) et sont tous différents : si $a^2 \equiv b^2 \pmod{p}$, alors p divise $a^2 - b^2 = (a-b)(a+b)$ mais ne pouvant diviser $a+b \in \{2, 3, \dots, 2N\}$, il divise $|a-b| \in \{0, 1, \dots, N-1\}$, donc $a = b$. Ces N nombres distincts $1^2, 2^2, \dots, N^2$ sont exactement les racines (modulo p) du polynôme $P(x) = x^N - 1$ de degré N. Toujours par le petit théorème de Fermat, les nombres qui ne sont pas congrus à des carrés d'entiers annulent le polynôme $x^{p-1} - 1 = (x^N - 1)(x^N + 1)$ mais comme ils n'annulent pas $x^N - 1$ (dont les racines non nulles viennent d'être recensées), ils annulent $x^N + 1$. Pour résumer, q^N est congru à 1 ou à -1 selon que q est congru ou non à un carré. Legendre a défini le symbole

$$\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{s'il existe } x \text{ tel que } p \text{ divise } q - x^2 \\ -1 & \text{sinon} \end{cases}$$

On a alors $\left(\frac{q}{p}\right) \equiv q^N \pmod{p}$ et on peut remarquer que $\left(\frac{q+kp}{p}\right) = \left(\frac{q}{p}\right)$ pour tout entier $k \in \mathbb{Z}$.
De plus, si q est impair, alors $\left(\frac{q}{p}\right) \equiv q^N \equiv (-1)^S \pmod{p}$, donc $\left(\frac{q}{p}\right) = (-1)^S$ avec $S = \sum_{k=1}^{N} \left\lfloor \frac{kq}{p} \right\rfloor$.

Exemples

1) $\left(\frac{-1}{p}\right) = \left(\frac{2p-1}{p}\right)$ dépend de la parité de la somme

$$S = \sum_{k=1}^{N} \left\lfloor \frac{k(2p-1)}{p} \right\rfloor = \sum_{k=1}^{N} \left\lfloor 2k - \frac{k}{p} \right\rfloor = \sum_{k=1}^{N} (2k-1) = N^2 = \left(\frac{p-1}{2}\right)^2.$$

On a les équivalences $\left(\frac{-1}{p}\right) = 1$, S est paire, $\frac{p-1}{2} \in 2\mathbb{N}$, $p \in (4\mathbb{N}+1)$.

2) $\left(\frac{2}{p}\right) = \left(\frac{p+2}{p}\right)$ dépend de la parité de la somme

$$S = \sum_{k=1}^{N} \left\lfloor \frac{k(p+2)}{p} \right\rfloor = \sum_{k=1}^{N} \left\lfloor k + \frac{2k}{p} \right\rfloor = \sum_{k=1}^{N} k = \frac{N(N+1)}{2}.$$

On a les équivalences $\left(\frac{2}{p}\right) = 1$, S est paire, $N \in 4\mathbb{N}$ ou $N+1 \in 4\mathbb{N}$, $\frac{p-1}{2} \in 4\mathbb{N}$ ou $\frac{p+1}{2} \in 4\mathbb{N}$, $p \in (8\mathbb{N}+1)$ ou $p \in (8\mathbb{N}-1)$.

3) Le symbole de Legendre est *multiplicatif* : $\left(\frac{m_1 m_2}{p}\right) \equiv (m_1 m_2)^N = m_1^N m_2^N \equiv \left(\frac{m_1}{p}\right)\left(\frac{m_2}{p}\right)$ modulo p, si bien que les deux extrémités, qui valent 1 ou -1, sont égales.

En particulier, $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ vaut 1 uniquement dans les cas suivants.

- $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$, c'est-à-dire $p \in (4\mathbb{N}+1) \cap \big((8\mathbb{N}+1) \cup (8\mathbb{N}+7)\big) = (8\mathbb{N}+1)$
- $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$, c'est-à-dire $p \in (4\mathbb{N}+3) \cap \big((8\mathbb{N}+3) \cup (8\mathbb{N}+5)\big) = (8\mathbb{N}+3)$

On peut également déterminer $\left(\frac{-2}{p}\right) = \left(\frac{p-2}{p}\right) = (-1)^{(N-1)N/2}$ comme dans le deuxième exemple.

3 La loi de réciprocité quadratique

Si $q \neq 2$ est aussi un nombre premier (différent de p), on peut échanger les rôles de p et q. On a alors

$$\left(\frac{q}{p}\right) = (-1)^S \text{ avec } S = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor \quad \text{et} \quad \left(\frac{p}{q}\right) = (-1)^T \text{ avec } T = \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor.$$

On voit ainsi que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S+T}$ ne dépend que de la parité de $S+T$.

L'ensemble $E = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \times \left\{1, 2, \ldots, \frac{q-1}{2}\right\}$ contient $\frac{(p-1)(q-1)}{4}$ éléments que l'on peut répartir en deux catégories : le sous-ensemble E_1 qui contient les éléments $(x; y)$ vérifiant $y < \frac{q}{p}x$ et le sous ensemble E_2 qui contient ceux vérifiant $y > \frac{q}{p}x$, c'est-à-dire $x < \frac{p}{q}y$ (on ne peut pas avoir $y = \frac{q}{p}x$ car la fraction $\frac{q}{p}$ est irréductible). Le nombre d'éléments de ces sous-ensembles est respectivement

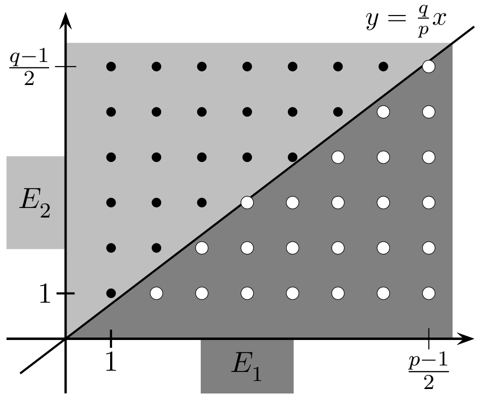
$$\sum_{(x;y)\in E_1} 1 = \sum_{x=1}^{(p-1)/2} \sum_{y<\frac{q}{p}x} 1 = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor = S \quad \text{et} \quad \sum_{(x;y)\in E_2} 1 = \sum_{y=1}^{(q-1)/2} \sum_{x<\frac{p}{q}y} 1 = \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor = T.$$

Comme E est réunion disjointe de E_1 et E_2, on a

$$S + T = \frac{(p-1)(q-1)}{4}.$$

Cette relation peut aussi être expliquée par l'illustration ci-contre (avec $p = 17$ et $q = 13$) et démontre la *loi de réciprocité quadratique* :

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



Pour être plus explicite, on peut envisager deux situations.

- Si les nombres p et q sont tous les deux congrus à 3 modulo 4, alors $\frac{(p-1)(q-1)}{4}$ est impair, S et T ont des parités différentes, et donc $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.
- Si l'un (au moins) des nombres p et q est congru à 1 modulo 4, alors $\frac{(p-1)(q-1)}{4}$ est pair, S et T ont la même parité, et donc $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Exemple. En utilisant la réduction modulaire (R), la loi de réciprocité quadratique (L) et la multiplicativité du symbole de Legendre (M), on a

$$\left(\frac{23}{13}\right) \overset{(R)}{=} \left(\frac{10}{13}\right) \overset{(M)}{=} \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) \overset{(L)}{=} \left(\frac{2}{13}\right)\left(\frac{13}{5}\right) \overset{(R)}{=} \left(\frac{2}{13}\right)\left(\frac{3}{5}\right) \overset{(L)}{=} \left(\frac{2}{13}\right)\left(\frac{5}{3}\right) \overset{(R)}{=} \left(\frac{2}{13}\right)\left(\frac{2}{3}\right).$$

Comme 3 et 13 ne sont pas congrus à ± 1 modulo 8, on a $\left(\frac{2}{13}\right) = \left(\frac{2}{3}\right) = -1$, et donc $\left(\frac{23}{13}\right) = 1$. Ainsi, il existe un entier x tel que $x^2 - 23$ est divisible par 13 (en fait $x = 6$ convient).