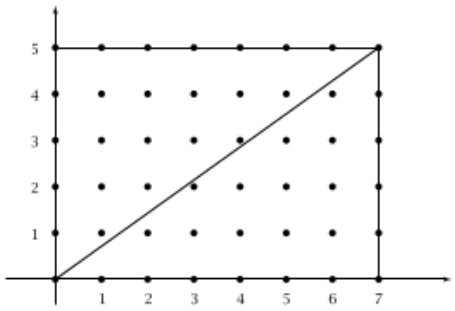
Traduction de l'explication de la preuve géométrique par Eisenstein de la loi de réciprocité quadratique de Gauss trouvée dans le livre Topologie des nombres de Allen Hatcher

On rappelle la loi de réciprocité quadratique de Gauss (si on note $\left(\frac{p}{q}\right)$ le caractère de résiduosité quadratique de p à q, qui exprime que p est un carré modulo q) :

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

1. Ici notre but est d'exprimer le symbole de Legendre $\left(\frac{p}{q}\right)$ en termes géométriques.

Pour commencer, considérons un rectangle dans le premier quadrant du plan cartésien qui est de largeur égale à p unités et de hauteur égale à a unités, avec un coin à l'origine et l'autre coin au point (p, a). Par exemple pour $p = 7$ et $a = 5$, on a le schéma



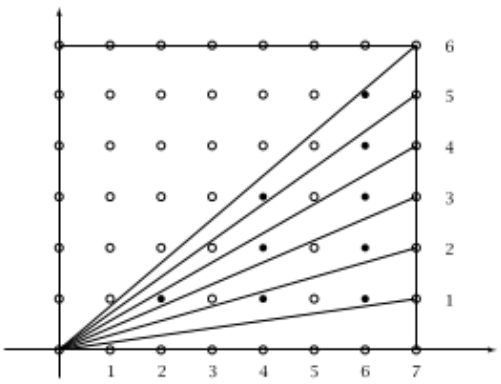
Nous allons nous intéresser aux points qui sont strictement à l'intérieur du rectangle dont les coordonnées sont entières. Les points satisfaisant cette dernière condition sont appelés *points du réseau*. Le nombre de points du réseau à l'intérieur du rectangle est donc $(p-1)(a-1)$ puisque leur abscisse est comprise entre 1 et $p-1$ and leur ordonnée est comprise entre 1 et $a-1$, indépendamment.

La diagonale du rectangle de $(0, 0)$ à (p, a) ne passe par aucun point du réseau intérieur au rectangle puisque nous avons supposé que p ne divise pas a, ainsi la fraction a/p, qui est la pente de la diagonale, est irréductible (s'il y avait un point intérieur du réseau sur la diagonale, la pente de la diagonale serait une fraction avec un numérateur et un dénominateur plus petits que a et p). Puisqu'il n'y a pas de points intérieurs au réseau sur la diagonale, exactement la moitié des points du réseau à l'intérieur du rectangle sont de chaque côté de la diagonale, et du coup, le nombre de points du réseau sous la diagonale est $\frac{1}{2}(p-1)(a-1)$. Ce nombre est un entier puisque p est impair, ce qui rend $p-1$ pair.

librement téléchargeable ici https://pi.math.cornell.edu/ hatcher/TN/TNbook.pdf.

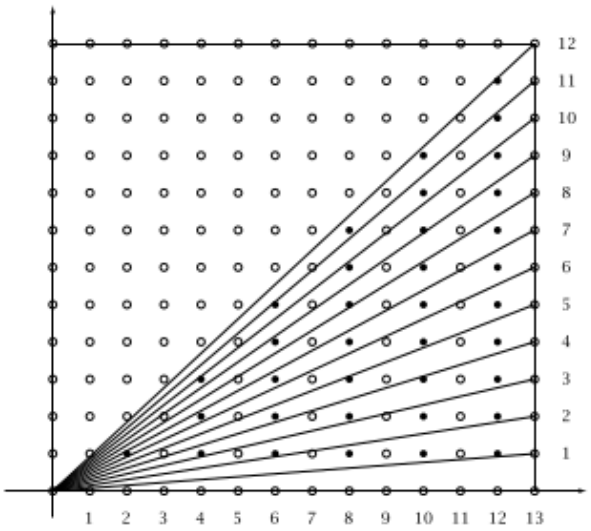
Une question plus précise que l'on peut se poser est de savoir combien de points du réseau sous la diagonale ont une abscisse (coordonnée x) paire et combien ont une abscisse impaire. Ici, il n'y a pas de garantie que ces deux nombres doivent être égaux, et si par exemple ils étaient égaux, ils devraient être égaux à $\frac{1}{4}(p-1)(a-1)$ mais cette fraction pourrait ne pas être entière, par exemple quand $p = 7$ et $a = 4$.

Nous dénotons le nombre de points du réseau qui sont sous la diagonale et ont une abscisse paire par la lettre e. La figure ci-dessous montre les valeurs de e quand $p = 7$ et quand a est compris entre 1 et 6.



a	e	$\left(\frac{a}{7}\right)$
6	9	−1
5	7	−1
4	6	+1
3	3	−1
2	2	+1
1	0	+1

Un exemple un petit peu plus compliqué pour p = 13 et a compris entre 1 et 12



a	e	$\left(\frac{a}{13}\right)$
12	36	+1
11	33	−1
10	30	+1
9	26	+1
8	23	−1
7	21	−1
6	15	−1
5	13	−1
4	10	+1
3	6	+1
2	3	−1
1	0	+1

La manière dont e varie en fonction de a semble quelque peu imprévisible. Ce que nous allons montrer c'est que connaître simplement la parité de e suffit déjà pour déterminer la valeur du symbole de Legendre via la formule

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

Pour prouver cela, on trouve d'abord une formule pour e. Le segment de la ligne verticale $x = u$ allant de l'axe des abscisses jusqu'à la diagonale a pour longueur $\frac{ua}{p}$ puisque la pente de la diagonale est a/p. Si u est un entier positif, le nombre des points du réseau sur ce segment de droite est $\left\lfloor \frac{ua}{p} \right\rfloor$, le plus grand entier $n \leq \frac{ua}{p}$. Maintenant si on ajoute ces nombres de points du réseau pour l'ensemble des nombres pairs $E = \{2, 4, \ldots, p-1\}$, on obtient

$$e = \sum_E \left\lfloor \frac{ua}{p} \right\rfloor .$$

La manière de calculer $\left\lfloor \frac{ua}{p} \right\rfloor$ est d'appliquer l'algorithme de division entière en divisant ua par p pour obtenir $\left\lfloor \frac{ua}{p} \right\rfloor$ comme quotient et un reste que nous notons $r(u)$. Du coup, nous avons la formule

$$ua = p \left\lfloor \frac{ua}{p} \right\rfloor + r(u) \tag{1}$$

Cette formule implique que le nombre $\left\lfloor \frac{ua}{p} \right\rfloor$ a la même parité que $r(u)$ puisque u est pair et p est impair. Cette relation entre les parités implique que le nombre $(-1)^e$ qui nous intéresse peut aussi être calculé comme

$$(-1)^e = (-1)^{\sum_E \left\lfloor \frac{ua}{p} \right\rfloor} = (-1)^{\sum_E r(u)} \tag{2}$$

Avec cette dernière expression à l'esprit, nous allons nous focaliser sur les restes $r(u)$.

Le nombre $r(u)$ est strictement compris entre 0 et p et peut être soit pair soit impair, mais dans les deux cas, nous pouvons dire que $(-1)^{r(u)} r(u)$ est congruent à un nombre pair dans l'intervalle $(0, p)$ puisque si $r(u)$ est impair, $(-1)^{r(u)} r(u)$ l'est aussi et alors en ajoutant p à cela, on obtient un nombre pair entre 0 et p. Ainsi, il y a toujours un nombre pair $s(u)$ entre 1 et p qui est congruent à $(-1)^{r(u)} r(u)$ $mod\ p$. De façon évidente, $s(u)$ est unique puisqu'il n'y a pas deux nombres dans l'intervalle $(0, p)$ qui sont congruents mod p.

Un fait clef à propos de ces nombres pairs $s(u)$ est qu'ils sont tous distincts lorsque u varie dans l'ensemble E. Car supposons que nous ayons $s(u) = s(v)$ pour un autre nombre pair v dans E. Alors $r(u) = \pm r(v)$ $mod\ p$, ce qui implique $au = \pm av$ $mod\ p$ au regard de l'équation (1) ci-dessus. Nous pouvons éliminer les a des deux côtés de la congruence pour obtenir $u \equiv \pm v$. Pourtant, nous ne pouvons avoir $u \equiv -v$ parce que le nombre entre 0 et p qui est congruent à $-v$ est $p - v$, du coup, nous devrions avoir $u = p - v$ ce qui est impossible puisque ce sont des nombres strictement compris entre 0 et p. Cela montre que les nombres $s(u)$ sont tous distincts.

Maintenant considérons le produit de tous les nombres $(-1)^{r(u)}r(u)$ lorsque u^r parcourt E. Ecrivons-le : c'est

$$\left[(-1)^{r(2)}r(2)\right]\left[(-1)^{r(4)}r(4)\right]\ldots\left[(-1)^{r(p-1)}r(p-1)\right] \tag{3}$$

Par l'équation (1), nous avons $r(u) = ua \ mod \ p$, du coup, ce produit est congruent mod p à

$$\left[(-1)^{r(2)}2a\right]\left[(-1)^{r(4)}4a\right]\ldots\left[(-1)^{r(p-1)}(p-1)a\right]$$

D'un autre côté, par la définition des nombres $s(u)$, le produit (3) est congruent mod p à

$$[s(2)][s(4)]\ldots[s(p-1)]$$

Il y a $\frac{p-1}{2}$ facteurs ici et ce sont tous des nombres pairs distincts de l'intervalle $[0..p]$ comme nous l'avons montré au paragraphe précédent, de telle façon qu'ils sont juste un réarrangement des nombres $2, 4, \ldots, p-1$. Ainsi nous avons la congruence

$$\left[(-1)^{r(2)}2a\right]\left[(-1)^{r(4)}4a\right]\ldots\left[(-1)^{r(p-1)}(p-1)a\right] \equiv (2)(4)\ldots(p-1) \ mod \ p$$

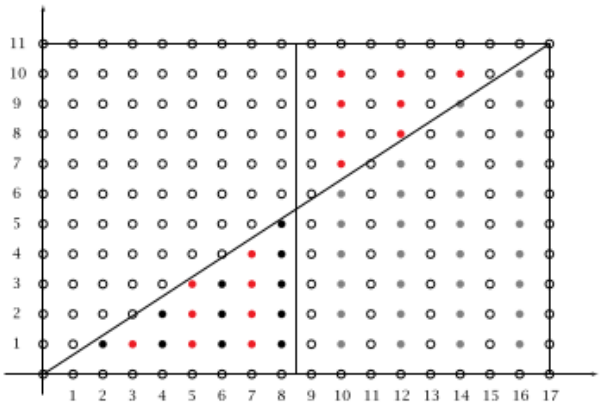
Nous pouvons éliminer les facteurs $2, 4, \ldots, p-1$ des deux côtés de la congruence pour obtenir

$$(-1)^{\sum_E r(u)} a^{\frac{p-1}{2}} \equiv 1 \ mod \ p$$

Les facteurs $(-1)^{\sum_E r(u)}$ et $a^{\frac{p-1}{2}}$ sont à la fois égaux à $\pm 1 \ mod \ p$ et leur produit est 1, ce qui fait qu'ils doivent être égaux mod p (en utilisant le fait que 1 et -1 ne sont pas congruents modulo un nombre premier impair). Par la formule d'Euler, on a $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \ mod \ p$, du coup, de la formule précédente (2), nous concluons que $\left(\frac{a}{p}\right) = (-1)^e$. Cela termine cette première étape de la preuve géométrique de la loi de réciprocité quadratique.

2. Maintenant nous traitons le cas où $a = q$ avec q un nombre premier impair distinct de p. Comme dans l'étape 1, nous considérons un triangle de taille $p \times q$.

Nous savons que $\left(\frac{a}{p}\right) = (-1)^e$ où e est le nombre de points du réseau d'abscisse paire à l'intérieur du rectangle et au-dessous de la diagonale. Supposons que nous divisions le rectangle en deux moitiés égales séparées par un ligne verticale $x = \frac{p}{2}$. Cette ligne ne passe par aucun point du réseau puisque p est impair Cette ligne verticale coupe deux triangles plus petits dans chacun des deux grands triangles au-dessus et au-dessous de la diagonale du rectangle. Appelons le petit triangle du bas L et celui du haut U, et les variables l et u pour le nombre de points du réseau d'abscisse paire dans L et U respectivement. On remarque que u a la même parité que le nombre de



points du réseau d'abscisse paire dans le quadrilatère sous U dans la moitié droite du rectangle puisque chaque colonne de points du réseau dans le rectangle contient $q-1$ points, un nombre pair. Du coup, e a la même parité que $l+u$, et par conséquent $(-1)^e = (-1)^{l+u}$.

La chose suivante à remarquer est qu'en tournant le rectangle U de 180 degrés autour du centre du rectangle l'amène sur le triangle L. Cette rotation amène les points du réseau dans U d'abscisse paire sur les points du réseau dans L sur les points d'abscisse impaire. Ainsi nous obtenons la formule $\left(\frac{q}{p}\right) = (-1)^t$ où t est le nombre total de points du réseau dans le triangle L.

En inversant les rôles de p et q, nous pouvons aussi dire que $\left(\frac{q}{p}\right) = (-1)^{t'}$ où t' est le nombre de points du réseau à l'intérieur du triangle L' au-dessus de la diagonale et au-dessous de la ligne horizontale $y = \frac{q}{2}$ qui coupe le rectangle en deux horizontalement. Alors $t + t'$ est le nombre des points du réseau dans le petit rectangle formé par L et L' ensemble. Ce nombre est juste $\frac{p-1}{2}.\frac{q-1}{2}$. Ainsi nous avons

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t(-1)^{t'} = (-1)^{t+t'} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$$

qui finalement termine la preuve de la loi de réciprocité quadratique.