La preuve géométrique mal comprise qu'a faite Eisenstein de la loi de réciprocité quadratique

R.C. Laubenbacher, D.J.Pengelley,
traduction : D. Chemla

30/8/2011

1 Introduction

La Loi de Réciprocité Quadratique a joué un rôle central dans le développement de la théorie des nombres et a constitué la première loi profonde gouvernant les nombres premiers. Ses nombreuses preuves de nombreux points de vue distincts attestent de sa position au coeur de ce sujet. Le théorème a été découvert par Euler et reformulé par Legendre en utilisant le symbole qui porte maintenant son nom mais a été prouvé pour la première fois par Gauss. Les huit preuves différentes de ce théorème, que Gauss publia au début des années 1800, en appellant la Loi de Réciprocité Quadratique le théorème fondamental, furent suivies de douzaines d'autres avant que ce dix-neuvième siècle ne s'achève, en incluant quatre de Gotthold Eisenstein dans les années 1844-1845. Notre but est de porter un nouveau regard sur la preuve géométrique d'Eisenstein, dans laquelle il présente une adaptation particulièrement belle et économique de la troisième preuve de Gauss et d'amener ainsi l'attention sur tous les avantages de sa preuve sur celle de Gauss, la plupart de ces avantages n'ayant apparemment pas été perçus jusqu'à présent.
Il est difficile d'imaginer aujourd'hui la sensation causée par Eisenstein quand il surgit dans le monde mathématique. A l'automne 1843, à 20 ans, ce mathématicien autodidacte avait tout juste reçu son certificat de Hautes Etudes et était entré à l'université de Berlin lorsqu'il produisit un flot de publications faisant immédiatement de lui un des mathématiciens majeurs du début du dix-neuvième siècle. Le 14 juillet 1844, Gauss écrivit à C.Gerling :

> *J'ai récemment fait la connaissance d'un jeune mathématicien, Eisenstein de Berlin, qui est venu ici avec une lettre de recommandation de Humboldt. Cet homme, qui est encore très jeune, montre un talent remarquable et il fera certainement de grandes choses.*

En 1844, Eisenstein contribua à pas moins de 16 des 27 articles mathématiques du volume 27 du Journal de Crelle et lors de son troisième semestre en tant qu'étudiant, il avait reçu un doctorat honorable de Breslau. Gauss et le grand scientifique et explorateur Alexandre Von Humboldt tous deux firent de gros efforts, pour la plupart en vain, pour obtenir la reconnaissance et la sécurité financière d'Eisenstein appauvri. Gauss écrivit à Humboldt que le talent d'Eisenstein était de ceux que la Nature ne crée que quelques fois dans un siècle. Il obtint un poste de Privatdozent (assistant non rémunéré) à l'université de Berlin et fut finalement admis à l'Académie des Sciences de Berlin début 1852. Mais sa santé s'étant alors sérieusement détériorée, il mourut la même année à l'âge de 29 ans, de la tuberculose. Gotthold Eisenstein reste avec Abel et Galois un autre génie mathématique du dix-neuvième siècle à avoir eu une vie courte et tragique.
La preuve géométrique d'Eisenstein parut dans le Journal de Crelle sous le titre *Démonstration géométrique du théorème fondamental des restes quadratiques.* Elle est très liée à la troisième preuve de Gauss. Plusieurs exposés de la preuve d'Eisenstein ont observé seulement un de ses trois aspects géométriques et ont omis les autres différences importantes entre les deux preuves. Le résultat en a été un échec à reconnaître et apprécier pleinement la manière dont Eisenstein organise grandement et éclaire la preuve de Gauss et ce-faisant révèle l'essence de cette troisième démonstration de Gauss. Par exemple, la troisième démonstration est basée sur un résultat appelé le Lemme de Gauss. Eisenstein était particulièrement satisfait du raccourci qu'il a trouvé pour éviter la technique nécessitée par l'application de ce Lemme.

Je ne me reposai pas tant que je ne réussis pas à libérer cette preuve géométrique du lemme dont elle dépendait encore et cela est maintenant si simple qu'on peut le communiquer en deux lignes.

Nous croyons que l'élégance de la preuve d'Eisenstein mérite une large attention et nous la présentons ci-dessous en la comparant à la troisième preuve de Gauss.

2 Preuve d'Eisenstein

Pour commencer, nous rappelons quelques conséquences du fait que les classes de restes modulo un nombre premier p forment un corps Z_p. Le Petit Théorème de Fermat $b^{p-1} \equiv 1 \ (mod\ p)$ pour tout entier b non divisible par p découle du fait que les classes de restes non-nulles forment un groupe (cyclique) d'ordre $p-1$ selon la multiplication. Quand p est impair, l'application $x \to x^2$ a comme noyau $\{-1, 1\}$ et donc son image, les carrés (ou résidus quadratiques) modulo p, forment un sous-groupe d'ordre $\frac{p-1}{2}$ et les non-résidus forment son coset. Le caractère de résiduosité quadratique d'une classe de restes $b \in Z_p^*$ est spécifié en utilisant le symbole de Legendre : $\left(\frac{b}{p}\right) = 1$ si b est un résidu quadratique mod p et $\left(\frac{b}{p}\right) = -1$ sinon. De $\left(b^{\frac{p-1}{2}}\right)^2 = 1$, il résulte que $b^{\frac{p-1}{2}} = \pm 1$ pour tout $b \in Z_p^*$. Mais si $b = c^2$, alors $b^{\frac{p-1}{2}} = c^{p-1} = 1$, et alors les résidus quadratiques sont toutes les racines du polynome $x^{\frac{p-1}{2}} = 1$. Puisque ce polynome ne peut avoir plus de $\frac{p-1}{2}$ racines dans le corps Z_p, nous concluons que ses racines sont exactement les résidus quadratiques. C'est à dire que nous avons le *critère d'Euler* : $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}}$ pour tout b non divisible par p. Le théorème de la réciprocité quadratique compare le caractère quadratique de deux nombres premiers l'un par rapport à l'autre.
Loi de Réciprocité Quadratique : Si p et q sont deux nombres premiers impairs distincts alors

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

Voici la preuve d'Eisenstein, en suivant au plus près ses propre langage et notation (dont il a lui-même abusé avec convenance et succès).

Considérons l'ensemble $a = 2, 4, 6, \ldots, p-1$. Appelons r le reste modulo p d'un multiple arbitraire qa. Alors il apparaît clairement que la liste des nombres $(-1)^r r$ concorde avec la liste des nombres a, jusqu'aux multiples de p (car clairement chacun des nombres $(-1)^r r$ a un plus petit résidu positif pair et que s'il y avait une duplication parmi ces restes, on aurait

$$(-1)^{qa}.qa = (-1)^{qa'}.qa',$$

mais alors $a \equiv \pm a'$. Puisque les a sont distincts, on en déduit que $a + a' \equiv 0$ ce qui ne peut avoir lieu puisque $0 < a + a' < 2p$ et $a + a'$ est pair). Mais alors :

$$q^{\frac{p-1}{2}} \prod a \equiv \prod r \ (mod\ p) \ \ et \ \ \prod a \equiv (-1)^{\sum r} \prod r \ (mod\ p),$$

d'où il résulte que $q^{\frac{p-1}{2}} \equiv (-1)^{\sum r} \ (mod\ p)$. En rappelant que selon le critère d'Euler $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \ (mod\ p)$, cela entraîne que

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

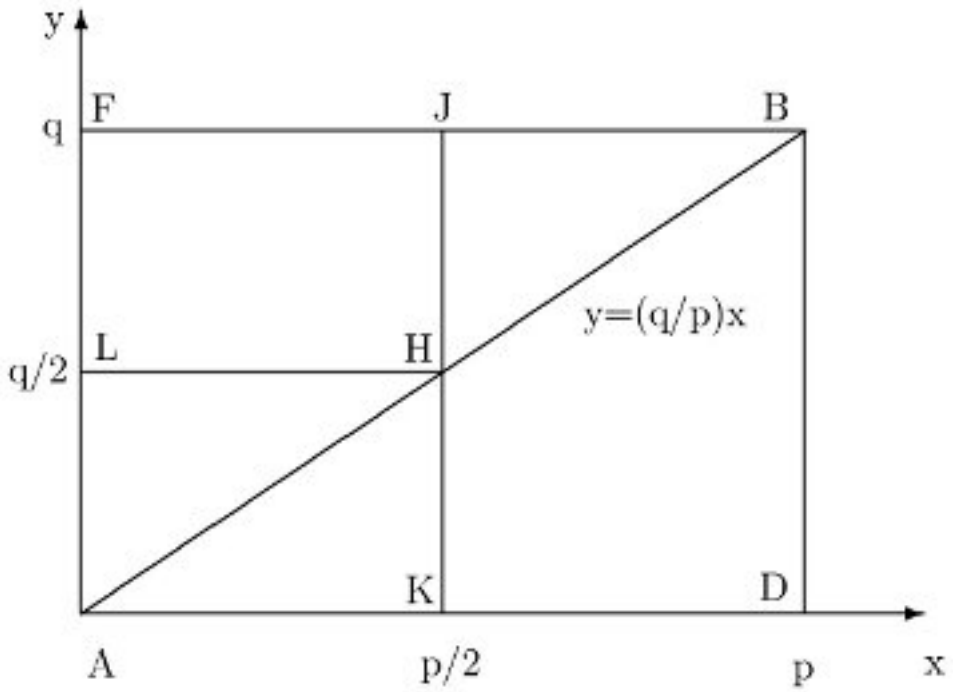
ainsi on peut se concentrer seulement sur la parité de l'exposant. Clairement,

$$\sum qa = p \sum \left[\frac{qa}{p}\right] + \sum r, \qquad (2)$$

où $[\,]$ est la fonction *plus grand entier inférieur à*. Puisque les éléments a sont tous pairs, et que p est impair, il s'ensuit que $\sum r \equiv \sum [\frac{qa}{p}] \ (mod\ 2)$ et donc que

$$\left(\frac{q}{p}\right) = (-1)^{\sum [\frac{qa}{p}]}.$$

(Ici, Eisenstein remarque que puisque jusque là, q ne nécessite pas d'être un nombre premier impair, mais plutôt un nombre premier à p, on peut facilement obtenir le caractère de résiduosité de 2 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ de la formule ci-dessus. On laisse ceci en exercice au lecteur.)



Eisenstein utilise alors une représentation géométrique de l'exposant dans cette dernière équation pour la transformer deux fois en étudiant sa parité : cet exposant est précisément le nombre de points entiers du réseau d'abscisses paires à l'intérieur du triangle ABD sur la Figure (notez qu'il n'y a aucun point du réseau sur la ligne AB). Considérons une abscisse paire $a > p/2$. Puisque le nombre de points du réseau associé à chaque abscisse à l'intérieur du rectangle $ADBF$ est pair, le nombre $[\frac{qa}{p}]$ de points du réseau d'abscisse sous AB a la même parité que le nombre de points du réseau au-dessus de AB. Celui-ci en retour est le même que le nombre de points du réseau sous AB d'abscisse impaire $p - a$. Cette correspondance un-à-un entre les abscisses paires dans le triangle BHJ et les abscisses impaires dans AHK implique maintenant que $\sum \left[\frac{qa}{p}\right] \equiv \mu \ (mod\ 2)$, où μ est le nombre de points à l'intérieur du triangle AHK, et donc $\left(\frac{q}{p}\right) = (-1)^{\mu}$.

En inversant les rôles de p et q, on aboutit à $\left(\frac{p}{q}\right) = (-1)^{\nu}$, où ν est le nombre de points à l'intérieur du triangle AHL. Puisque le nombre total de points à l'intérieur des deux triangles est simplement $\frac{p-1}{2}.\frac{q-1}{2}$, on peut maintenant conclure que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\nu+\mu} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}. \qquad \square$$

Même l'habituellement modeste Eisenstein ne put retenir sa joie face à cette démonstration :

> *Comme Euler se serait trouvé chanceux s'il avait été en possession de ces lignes il y a quelques soixante-dix ans.*

3 Eisenstein contre Gauss

Gauss lui-même considérait sa troisième preuve comme la plus directe et la plus naturelle de ses démonstrations. En l'introduisant, il disait :

Une année entière, ce théorème m'a tourmenté et a absorbé mes plus gros efforts jusqu'à ce qu'enfin j'obtienne une démonstration... Plus tard, je trouvai trois autres preuves qui étaient construites sur des principes complètement différents... Je n'hésite pas à dire que jusqu'à présent, aucune preuve naturelle n'a été produite. Je laisse les autorités juger si la preuve suivante que j'ai été assez chanceux de découvrir mérite cette description.

Tandis qu'Eisenstein suit essentiellement la même structure que Gauss, chaque caractéristique de son approche est d'une grande clarté, et offre une vision élégante tout en raccourcissant le chemin pris par Gauss.
La troisième preuve de Gauss commence par son Lemme, qui dit que :

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}, \qquad (3)$$

avec α obtenu de la manière suivante. Posons

$$A = 1, 2, \ldots, \frac{p-1}{2} \; et \; B = \frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1.$$

Alors α est défini comme le nombre de *résidus minima absolus* positifs de l'ensemble qA qui appartiennent à B.
Plutôt que d'utiliser le Lemme de Gauss, Eisenstein dérive l'équation (1), avec l'expression algébrique $\sum r$ en exposant, qui est alors plus facilement convertie en l'équation clef

$$\left(\frac{q}{p}\right) = (-1)^{\sum[\frac{qa}{p}]}, \qquad (4)$$

commune aux deux démonstrations, ce qui n'est pas le cas de l'équation (3). Alors que l'exposant algébrique d'Eisenstein est facilement transformé en l'exposant dans (4) via (2), Gauss doit établir un certain nombre de propriétés de la fonction plus grand entier et les appliquer pour relier α à l'exposant dans (4). L'utilisation par Eisenstein de l'ensemble $a = 2, 4, 6, \ldots, p-1$, par opposition à l'ensemble A de Gauss, lui permet de compter les mêmes éléments que le Lemme de Gauss, mais via l'expression $\sum r$, l'amenant rapidement à (4) :

La principale différence entre mon argument et celui de Gauss est que je ne divise pas les nombres moindres que p en ceux moindres que $p/2$ et ceux supérieurs à $p/2$, mais plutôt en pairs et impairs.

Eisenstein applique maintenant ses deux intelligentes transformations géométriques pour convertir l'exposant $\sum[\frac{qa}{p}]$ en nombre de points du réseau dans le triangle AHK (*mod* 2). Après avoir fait la même chose pour $\left(\frac{p}{q}\right)$, calculant le nombre de points du réseau du triangle AHL, la preuve est complétée en comptant le nombre de points du réseau du rectangle $AKHL$[1]. Gauss, de son côté, fait essentiellement les deux mêmes transformations, et calculs, sans avoir recours à l'approche géométrique. Il compte vraiment les points en utilisant des propriétés algébriques de la fonction plus grand entier. Cela rend le reste de la preuve longue et non-intuitive, et le force à considérer des cas séparés dépendant des classes de congruence de p et q (mod 4).

[1]La plupart des exposés modernes de la preuve d'Eisenstein présentent seulement cet argument de comptage final, en remplaçant ses deux transformations géométriques par de l'algèbre.

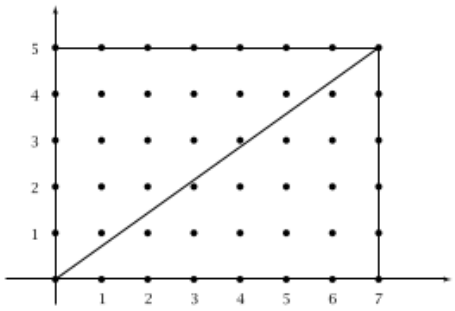
Traduction de l'explication de la preuve géométrique par Eisenstein de la loi de réciprocité quadratique de Gauss trouvée dans le livre Topologie des nombres de Allen Hatcher

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



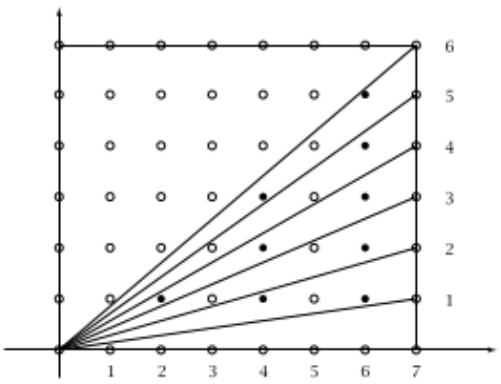
Nous allons nous intéresser aux points qui sont strictement à l'intérieur du rectangle dont les coordonnées sont entières. Les points satisfaisant cette dernière condition sont appelés *points du réseau*. Le nombre de points du réseau à l'intérieur du rectangle est donc $(p-1)(a-1)$ puisque leur abscisse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

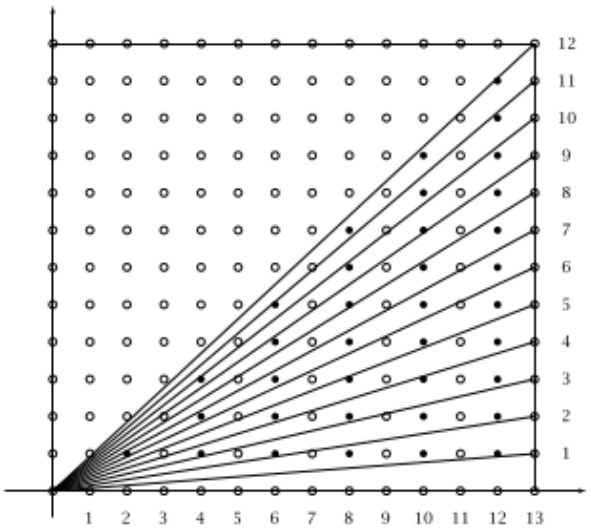
Une question plus précise que l'on peut se poser est de savoir combien de points du réseau sous la diagonale ont une abscisse (coordonnée x) paire et combien ont une abscisse impaire. Ici, il n'y a pas de garantie que ces deux nombres doivent être égaux, et si par exemple ils étaient égaux, ils devraient 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

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

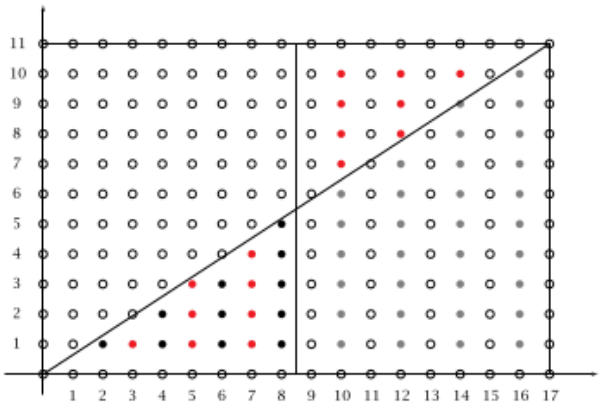
Nous pouvons éliminer les facteurs $2, 4, \ldots, p-1$ des deux côtés de la congruence pour obtenir

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

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.