Démonstration des lois de réciprocité quadratique et biquadratique

par Pierre KAPLAN
(Présenté par Y. Kawada)

Introduction

Le principe de cette démonstration est le suivant:

Soient p et q deux nombres premiers impairs distincts. Soit N_2 le nombre des solutions de la congruence $x_1^2+\cdots+x_q^2\equiv q \pmod p$. Soit, si $p\equiv 1 \pmod 4$, N_4 le nombre des solutions de $x_1^4+\cdots+x_q^4\equiv q \pmod p$. On peut d'une part calculer exactement N_2 et N_4, et d'autre part montrer que $N_2\equiv 2 \pmod q$ et $N_4\equiv 4 \pmod q$.

La première de ces relations donne immédiatement la loi de réciprocité quadratique, et de la seconde on déduit facilement la loi de réciprocité biquadratique.

Il existe trois démonstrations de la loi de réciprocité biquadratique:

Une démonstration de Gauss (a, Tome 10, pages 65-69) et Eisenstein (a), dont la notre est une interprétation. Le rapport entre ces deux démonstrations est expliqué dans la conclusion.

Une démonstration de Eisenstein (b), partant d'un lemme élémentaire de Gauss (a, Tome 2, page 141, b page 579), et utilisant la théorie des fonctions elliptiques. Gauss avait trouvé une démonstration élémentaire à partir du même lemme (a, Tome 2, pages 213 $\cdots$) mais elle est compliquée, et difficile à reconstituer; il doit être possible de trouver une démonstration élémentaire en interprétant convenablement cette démonstration d'Eisenstein, comme on peut le faire pour la démonstration analogue de la loi de réciprocité quadratique.

Enfin on peut déduire la loi de réciprocité biquadratique de la théorie du corps de classe et de la loi de réciprocité d'Artin. (Hasse - Tome 2 - pages 96 et 106).

Les idées nouvelles introduites ici sont le principle du raisonnement, et la notion d'ensemble de restes et d'ensemble de birestes, qui fait voir que ces raisonnements portent sur des nombre entiers, ce que l'usage des polynômes ou des nombres algébriques peut cacher.

Je suis reconnaissant à Monsieur le professeur Kawada de m'avoir permis d'exposer cette question dans un séminaire à l'Université de Tokyo. Cette article est une rédaction de ces exposés.

PREMIÈRE PARTIE

Cette partie est un exposé du premier mémoire de Gauss sur la loi de réciprocité biquadratique.

Bibliographie: Gauss [1] Tome 2 (en latin)
Gauss [2] pages 511-533 (en allemand)

Nous aurons besoin de la

PROPOSITION 1. *Un nombre premier ne peut être que d'une seule manière la somme de deux carrés.*

Démonstration (Euler).

Si le nombre premier p se décomposait de deux manières:

$$(1) \qquad p=a^2+b^2=c^2+d^2 \quad \text{avec} \quad 0<b<d<c<a$$

$$p(a^2-c^2)=a^2(c^2+d^2)-c^2(a^2+b^2)=a^2d^2-c^2b^2=(ad+bc)(ad-bc)\ ,$$

p divise un des deux nombres positifs $ad+bc$, $ad-bc$, donc est inférieur ou égal au plus grand:

$$p\leqslant ad+bc\ ,$$

d'où

$$0\geqslant 2p-2ad-2bc=a^2+b^2+c^2+d^2-2ad-2bc=(a-d)^2+(c-b)^2>0\ .$$

Donc (1) est impossible.

Soit p un nombre premier $\left(\frac{x}{p}\right)$ est le symbole de Legendre.

DÉFINITION. a est résidu biquadratique si la congruence $a\equiv x^4 \bmod p$ est résoluble, ou si a est puissance quatrième dans le corps des restes modulo p.

Pour abréger on désignera souvent par:

R les résidus quadratiques

N les non résidus quadratiques

A les résidus biquadratiques.

PROPOSITION 2. *Si* $p\equiv 3 \pmod 4$, *tout résidu quadratique est résidu biquadratique.*

Démonstration: $\left(\frac{x}{p}\right)=-1 \Rightarrow x\equiv y^2, \quad r\equiv y^4,$

$$\left(\frac{x}{p}\right)=-1 \Rightarrow \left(\frac{-x}{p}\right)=1, \quad -x\equiv y^2, \quad r\equiv y^4.$$

Dans la suite de ce chapitre nous supposons $p\equiv 1 \bmod 4$ (§ 2 excepté).

§ 1. Propriétés élémentaires des résidus biquadratiques modulo p.

On suppose $p\equiv 1 \bmod 4$. On a $\left(\frac{-1}{p}\right)=1$, donc $-1\equiv f^2 \bmod p$ est résoluble.

a) Les A sont obtenus en élevant les R au carré (mod p). Comme -1 est un R, les R sont symétriques par rapport à $p/2$, donc on obtient les A en élevant au carré les $\frac{p-1}{4}$ R compris entre 1 et $\frac{p-1}{2}$. Les A obtenus ainsi sont $\not\equiv \bmod p$: sinon $p|x^2-y^2=(x-y)(x+y) \Rightarrow p|x-y$ ou $x+y$, mais $0<|x-y|<|x+y|<p$ donc card (A)$=\frac{p-1}{4}$. Soit e un N. Considérons les quatre ensembles A, $Ae=$B, $Ae^2=$C, $Ae^3=$D. On montre, *en utilisant encore* $\left(\frac{-1}{p}\right)=1$, que ces quatre ensembles de $\frac{p-1}{4}$ restes mod p sont distincts, leur réunion est l'ensemble des restes mod p (sauf 0), donc C est l'ensemble des R qui ne sont pas A, et B$\cup$D$=$N.

REMARQUE. x, xf, $-x$, $-xf$ sont $\not\equiv \bmod p$, leur 4^e puissances sont congrues. Quand x parcourt $1 \cdots p-1$, x^4 parcourt 4 fois A $\left(\text{utiliser card(A)}=\frac{p-1}{4}\right)$.

b) Tout $x\not\equiv 0 \bmod p$ est solution de $x^{p-1}-1\equiv 0 \bmod p$, donc d'une des congruences:

$$(1)\quad x^{\frac{p-1}{4}}\equiv 1, \quad (2)\quad x^{\frac{p-1}{4}}\equiv -1, \quad (3)\quad x^{\frac{p-1}{4}}\equiv f, \quad (4)\quad x^{\frac{p-1}{4}}\equiv -f.$$

Les A sont les solutions de (1), car une congruence de degré n a au plus n solutions; pour la même raison les C sont les solutions de (2). e est solution de (3) ou de (4) comme le choix de e et f est arbitraire, nous conviendrons de choisir e et f de telle manière que e soit solution de (3). Alors B sont les solutions de (3) et D celles de 4. En résumé:

Nom	Numéro	Définition	Critère
A	0	Résidus biquadratiques	$x^{\frac{p-1}{4}}\equiv 1$
B	1	Ae	$x^{\frac{p-1}{4}}\equiv f$
C	2	Ae^2	$x^{\frac{p-1}{4}}\equiv -1$
D	3	Ae^3	$x^{\frac{p-1}{4}}\equiv -f$

(La classe B choisie dépend de e et f.)

§ 2. Énoncé du problème

Si on ajoute 1 aux restes d'une classe on obtient des reste qui peuvent se trouver dans les quatres classes, (et éventuellement 0, si -1 est dans la classe considérée). Le problème est de trouver combien de nombre de chaque classe on

obtient ainsi, c'est-à-dire de calculer les 16 nombres:

$$\begin{array}{cccc} (0,0) & (0,1) & (0,2) & (0,3) \\ (1,0) & (1,1) & (1,2) & (1,3) \\ (2,0) & (2,1) & (2,2) & (2,3) \\ (3,0) & (3,1) & (3,2) & (3,3) \end{array}$$

où par exemple (2, 3) signifie: le nombre de reste de la classe N°3 (D) obtenus en ajoutant 1 aux restes de la classe N°2 (C).

Pour mieux faire comprendre la méthode nous résoudrons le même problème pour le cas quadratique:

Trouver le tableau des quatre nombres $\begin{vmatrix} (0,0) & (0,1) \\ (1,0) & (1,1) \end{vmatrix}$ où (1, 0) par exemple est le nombre de résidus quadratiques obtenus en ajoutant 1 aux non résidus.

§ 3.1. **Cas quadratique** (dans ce §, p peut être $\equiv 3 \bmod 4$)

1ère Etape: Considérons la congruence (1) $1+n\equiv r \bmod p$. Par définition elle a (1, 0) solutions. Partant d'une solution, multiplions par l'inverse mod p de n, nous obtenons $n^{-1}+1\equiv n'$, c'est à dire une solution de (2) $n+1\equiv n'$. Cette correspondance entre les solutions de (1) et (2) est biunivoque: 2 solutions de (1) donnent 2 solutions de (2) et on obtient toutes les solutions de (2), car on peut aller en sens inverse.

Donc $(1,0)=(1,1)$: On obtient autant de résidus que de non résidus en ajoutant 1 aux non residus.

De là: le nombre de non résidus autres que -1 est pair. Le nombre de non résidus est $\frac{p-1}{2}$, si $\frac{p-1}{2}$ est pair -1 est résidu, et si $\frac{p-1}{2}$ est impair -1 est non résidu, d'où

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

2ème Etape. Ici on utilise le résultat $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$, et on distingue les cas $p\equiv 1$ et $p\equiv 3 \bmod 4$.

$p=4n+1$ $\quad -1$ étant résidu:

$$1+r=n \Longleftrightarrow 1+r+n=0 \Longleftrightarrow 1+n=r, \quad \text{donc } (1,0)=(0,1),$$

d'autre part: $(0,0)+(0,1)=2n-1$, $(1,0)+(1,1)=2n$

d'où $(1,0)=(1,1)=(0,1)=n$, $(0,0)=n-1$.

$p=4n+3$ $\quad -1$ étant non résidu:

$1+r=r' \Longleftrightarrow 1+r+n=0 \Longleftrightarrow 1+n=n'$ soit $(0,0)=(1,1)$

et $(0,0)+(0,1)=2n+1$,

$(1,0)+(1,1)=2n$.

Donc: $(0,0)=(1,1)=(1,0)=n$, $(0,1)=n+1$.

Conséquence — Caractère quadratique de 2 — c'est celui de $\frac{p+1}{2}$

$$1 \cdots \frac{p+1}{2} \qquad \frac{p+1}{2} \cdots p-1$$

$p=4n+1$: $\left(\frac{-1}{2}\right)=1$ $\frac{p-1}{2}$ a aussi le caractère de 2, et deux nombre symétriques ont le même caractère — donc 2 résidu $\Longleftrightarrow$ le nombre de passage RR en ajoutant 1 est impair $\Longleftrightarrow (0,0)=n-1$ impair $\Longleftrightarrow$ $p\equiv 1 \bmod 8$ et 2 non résidu $p\equiv 5 \bmod 8$

$p=4n+3$ $\frac{p-1}{2}$ a le caractère opposé à 2, et deux nombres symétrique ont des caractères opposés

2 résidu $\Longleftrightarrow$ le nombres des possages NR est impair $\Longleftrightarrow n$ impair

2 non résidu $\Longleftrightarrow$ le nombre des passages RN est impair $\Longleftrightarrow n$ pair

§ 3.2. Cas biquadratique $(p=4n+1)$

Il y a aussi les deux étapes, et la conséquence (caractère biquadratique de 2), mais en plus une troisième étape (α désigne un reste de la classe A, β de la classe B, $\cdots$).

1ère Etape. Le raisonnement du cas quadratique montre que les couples de congruences ont le même nombre de solutions:

$$1+\beta\equiv\alpha \longleftrightarrow 1+\delta\equiv\delta \quad \text{soit} \quad (1,0)=(3,3)$$

$$1+\beta\equiv\beta \longleftrightarrow 1+\delta\equiv\alpha \quad " \quad (1,1)=(3,0)$$

$$1+\beta\equiv\gamma \longleftrightarrow 1+\delta\equiv\beta \quad " \quad (1,2)=(3,1)$$

$$1+\beta\equiv\delta \longleftrightarrow 1+\delta\equiv\gamma \quad " \quad (1,3)=(3,2)$$

$$1+\gamma\equiv\alpha \longleftrightarrow 1+\gamma\equiv\gamma \quad " \quad (2,0)=(2,2)$$

$$1+\gamma\equiv\beta \longleftrightarrow 1+\gamma\equiv\delta \quad " \quad (2,1)=(2,3)$$

(On voit facilement que ce raisonnement ne peut donner d'autres relations).

2e Etape (1ère partie). On utilise le caractère de -1, et il faut distinguer les cas $p\equiv 1$ et $p\equiv 5 \bmod 8$.

$p=8n+1$ — Le tableau des 16 nombres est symétrique: -1 étant un A, deux restes opposés sont dans la même classe, donc, par exemple, les 3 congruences $1+\beta\equiv\delta$, $1+\beta+\delta\equiv 0$, $1+\delta=\beta$ ont les mêmes solutions, donc $(1,3)=(3,1)\cdots$

D'où les nouvelles relations:

$$h=(0,0)$$
$$i=(0,1)=(1,0)=(3,3)$$
$$k=(0,2)=(2,0)=(2,2)$$
$$l=(0,3)=(3,0)=(1,1)$$
$$m=(1,2)=(2,1)=(2,3)=(3,2)=(1,3)=(3,1)$$

et le tableau:

$$\begin{vmatrix} h & i & k & l \\ i & l & m & m \\ k & m & h & m \\ l & m & m & i \end{vmatrix}.$$

Comme -1 est un A est que chaque classe contient n restes:

(1) $h+i+k+l=2n-1$

(2) $i+l+2m=2n$

(3) $k+m=n$.

Ces trois relations ne suffisent pas à déterminer les 5 nombres, d'où la

3e Etape ($p=8n+1$).

Considérons la congruence (C) $1+\alpha+\beta+\gamma\equiv 0 \bmod p$. On calcule de deux manières le nombre de ses solutions.

1) Quand α parcourt A, $1+\alpha$ est h fois un A, i fois un B, k fois un C, l fois un D, et une fois 0. Quand

$1+\alpha=\alpha_0$: $\alpha_0+\beta+\gamma\equiv 0 \Longleftrightarrow 1+\beta\alpha_0^{-1}+\gamma\alpha_0^{-1}\equiv 0 \Longleftrightarrow 1+\beta'\equiv\gamma'$ $a(1,2)=m$ solutions

$1+\alpha=\beta_0$: $\beta_0+\beta+\gamma\equiv 0 \Longleftrightarrow 1+\beta\beta_0^{-1}+\gamma\beta_0^{-1}\equiv 0 \Longleftrightarrow 1+\alpha'\equiv\beta'$ $a(0,1)=i$ solutions

$1+\alpha=\gamma_0$: $\gamma_0+\beta+\gamma\equiv 0 \Longleftrightarrow 1+\beta\gamma_0^{-1}+\gamma\gamma_0^{-1}\equiv 0 \Longleftrightarrow 1+\delta'=\alpha'$ $a(3,0)=l$ solutions

$1+\alpha=\delta_0$: $\delta_0+\beta+\gamma\equiv 0 \Longleftrightarrow 1+\beta\delta_0^{-1}+\gamma\delta_0^{-1}\equiv 0 \Longleftrightarrow 1+\gamma'\equiv\delta'$ $a(2,2)=m$ solutions

$1+\alpha=0$ $\quad\beta+\gamma\equiv 0 \Longleftrightarrow \beta\equiv\gamma'$ est impossible

donc (C) a $mh+i^2+kl+lm$ solutions.

2) Quand β parcourt B, $1+\beta$ est i fois un A, $\cdots$.
Chaque fois on raisonne comme dans le cas 1), et on trouve:

$$ik+lm+mk+m^2 \quad \text{solutions.}$$

D'où la nouvelle relation

III $$hm+i^2+kl-ik-mk-m^2=0\ ,$$

de (1) et (2) on déduit

$$h=2m-k-1\ ,$$

d'où en portant dans (III)

$$m(2m-k-1)+i^2+kl-ik-mk-m^2=0\ .$$

Soit, en regroupant,

$$(m-k)^2+i^2-k^2+kl-ik-m=0\ .$$

En comparant (2) et (3) on voit que $k=\dfrac{i+l}{2}$. D'ou

$$(m-k)^2+i^2-\frac{(i+l)^2}{4}+\frac{i+l}{2}(l-i)-m=0\ .$$

En réduisant, et multipliant par 4:

$$4(m-k)^2+(l-i)^2-4m=0\ .$$

En utilisant (3)

$$-4m=-2(m+k)+2(k-m)=-2n+2(k-m)\ .$$

On en déduit:

$$4(k-m)^2+2(k-m)+(l-i)^2=2n\ .$$

Cela nous permet de calculer p:

(d) $$p=8n+1=16(k-m)^2+8(k-m)+1+4(l-i)^2=[4(k-m)+1]^2+[2(l-i)]^2\ .$$

p est donc la somme de deux carrés — $p=a^2+b^2$. D'après la proposition 1 cette décomposition est unique et, $|a|$ (impair) et $|b|$ (pair) sont bien déterminés. Dans la décomposition $a=4(k-m)+1$ a le signe tel qu'il soit $\equiv 1 \bmod 4$.

On pose $b=2(l-i)$. Le signe de b dépend du choix de la classe B (car si on échange B et D, l et i s'échangent.), c'est à dire de f ou de e.

2e Etape (2e partie — Calcul de $h\ i\ k\ l\ m$).

$$h=2n-1-i-l-k \qquad (1)$$

$$i+l+2m=n \qquad (2)$$

$$k+m=n \qquad (3)$$

$$4(k-m)+1=a \qquad (4)$$

$$2(l-i)=b \qquad (5)$$

de (3) et (4) on déduit $\begin{cases} 4(k+m)=4n \\ 4(k-m)=a-1 \end{cases}$ d'où $\begin{cases} 8k=4n+a-1 \\ 8m=4n-a+1 \end{cases}$

de (2), (3) et (5) : $\begin{cases} 2(l+i)=4k \\ 2(l-i)=b \end{cases}$ d'où $\begin{cases} 8l=8k+2b=4n+a+2b-1 \\ 8i=8k-2b=4n+a-2b-1 \end{cases}$

et $8h=16n-8-3(8k)=4n-3a-5$.

Donc en fonction de $p=2(4n)+1$, a et b

$$16\times\begin{cases} h=p-6a-11 \\ i=p+2a-4b-3 \\ k=p+2a-3 \\ l=p+2a+4b-3 \\ m=p-2a+1 \end{cases}.$$

4e Etape: Détermination du signe de b.

PROPOSITION 3. $\sum_{z=1\cdots p-1} z^k \equiv \begin{cases} -1 \\ 0 \end{cases} \bmod p \begin{cases} \text{si } k \text{ est multiple de } p-1 \\ \text{si } k \text{ n'est pas multiple de } p-1. \end{cases}$

Démonstration. Si $p-1|k$, $z^k\equiv 1$, $(p-1)z^k\equiv -1$,

si $p-1\nmid k$, soit g une racine primitive mod p, $z\equiv g^u \bmod p$

$$\sum_{z=1\cdots p-1} z^k = \sum_{u\ 0\cdots p-2} g^{uk}.$$

Donc $$(1-g^k)\sum_{u=0\cdots p-2}(g^k)^u \equiv 1-(g^k)^{p-1}\equiv 0.$$

Comme $$1-g^k\not\equiv 0, \qquad \sum_{1\cdots p-1} z^k \equiv 0. \qquad \text{C. Q. F. D.}$$

Considérons $s=\sum_{z=1\cdots p-1}(z^4+1)^{\frac{p-1}{4}}$. D'après la proposition 3 $s\equiv -2 \bmod p$. Quand z parcourt $1,\cdots,p-1$, z^4 parcourt 4 fois A, et $(z^4+1)^{\frac{p-1}{4}}$ est donc mod p 4(0, 0) fois 1, 4(0, 1) fois f, 4(0, 2) fois -1, 4(0, 3) fois $-f$. Donc

$$-2\equiv 4(h-k)+4f(i-l)\equiv \frac{4}{16}(p-6a-11-p-2a+3)-2fb\equiv -2a-2-2fb.$$

$$\boxed{a+bf\equiv 0 \bmod p}$$

Cas de $p=8n-5$ (Différences de raisonnement et résultats). Ici -1 est dans C.

2e Etape, 1ère partie. Dans le tableau des 16 nombres, on obtient le même nombre en ajoutant 2 aux deux indices, puis en les permutant: car -1 étant dans C il faut augmenter de 2 le numéro d'une classe en le faisant sauter par dessus le signe $=$

$$\begin{aligned} \text{d'ou} \quad h &= (0,0)=(2,2)=(2,0) \\ i &= (0,1)=(3,2)=(1,3) \\ k &= (0,2) \\ l &= (0,3)=(1,2)=(3,1) \\ m &= (1,0)=(3,3)=(1,1)=(3,0)=(2,1)=(2,3) \end{aligned}$$

et le tableau:

$$\begin{vmatrix} h & i & k & l \\ m & m & l & i \\ k & m & h & m \\ m & l & i & m \end{vmatrix}$$

(Par exemple les trois congruences $1+\beta\equiv\gamma$, $1+\beta+\alpha\equiv 0$, $1+\alpha\equiv\delta$ ont les mêmes solutions d'ou $(1,2)=(0,3)$).

3e Etape. On calcule de deux maniéres le nombre de solutions de $1+\alpha+\beta+\gamma\equiv 0 \bmod p$. (Il faut ici remarquer que -1 est un c).

On trouve $$m^2+hl+im-il-ik-lm=0\,.$$

Ensuite $$p=[4(h-m)+1]^2+[2(i-l)]^2\,.$$

On pose $a=4(h-m)+1$, $b=2(i-l)$, et on trouve, d'une part

$$16\times\begin{cases} h=p+2a-7 \\ i=p+2a+4b+1 \\ k=p-6a+1 \\ l=p+2a-4b+1 \\ m=p-2a-3 \end{cases}$$

et d'autre part, *grâce à ce choix de* b, $a+bf\equiv 0 \bmod p$.

Conséquence — caractère biquadratique de 2.

1) $p=8n+1$ $\quad a=4q+1$ $\quad b=4r$ (car $(4q+1)^2\equiv 1 \bmod 8$)

Dans ce cas -1 est résidu biquadratique

$$1 \ \dots \ \frac{p-1}{2} \qquad \frac{p+1}{2} \ \dots \ p-1\,.$$

Si x et $x+1$ sont dans une même classe $p-x-1$ et $p-x$ sont dans la même. Donc parmi les quatre nombres (0, 0), (1, 1), (2, 2), (3, 3), est impair celui correspondant à la classe de 1/2 et $-1/2$

$$(0,0)=h=\frac{1}{16}(p-6a-11)=\frac{1}{16}(16q^2-16q+16r^2-16)=q^2-q+r^2-1\equiv r^2-1 \bmod 2\,,$$

$$(2,2)=k=\frac{1}{16}(p+2a-3)=\frac{1}{16}(16q^2+16q+16r^2)\equiv r^2 \bmod 2\,,$$

donc si r est pair, 1/2 est dans A, donc 2 est dans A

si r est impair, 1/2 est dans C, donc 2 est dans C

(comme r est toujours soit pair, soit impair, 1/2 ne peut être ni dans B ni dans D, et (1, 1) et (3, 3) sont toujours pair, et on retrouve le caractère quadratique de 2).

2) $p=8n+5 \qquad a=4q+1 \qquad b=4r+2$

Ici -1 est dans C, donc les classes de $\frac{p-1}{2}$ et $\frac{p+1}{2}$ différent de 2, comme toutes les classes de deux nombres opposés. Si les classes de x et $x+1$ ont les numéros u et $u+2$ celles de $p-x-1$ et $p-x$ auront aussi les numéros u et $u+2$.

Donc 1/2 est dans la «classe d'arrivée» de celui des quatres nombres (0, 2) (1, 3) (2, 0) (3, 1) qui est impair.

$$(1,3)=i=\frac{1}{16}(p+2a+4b+1)=\frac{1}{16}(16q^2+16q+16r^2+16r+16r+16)\equiv r+1 \bmod 2\,.$$

$$(3,1)=l=\frac{1}{16}(p+2a+4b+1)=\frac{1}{16}(16q^2+16q+16r^2+16r-16r)\equiv -r\equiv r \bmod 2.$$

Donc 1/2 est dans la classe D, et 2 dans la classe B si r est pair, i,e, $b\equiv 2 \bmod 8$

1/2 est dans la classe B, et 2 dans la classe D si r est impair, i.e. $b\equiv 6 \bmod 8$.

En résumé

2 est dans la classe	A	B	C	D	I
suivant que, mod 8, $b\equiv$	0	2	4	6	

I s'écrit, puisque $a\equiv 1 \bmod 4$

$$2^{\frac{p-1}{4}}\equiv f^{\frac{b}{2}}\equiv f^{\frac{ab}{2}}\equiv\left(\frac{b}{a}\right)^{\frac{ab}{2}}, \quad \bmod p\,.$$

Remplaçons b par $b'=-b$ dans cette formule.

$$2^{\frac{p-1}{4}}\equiv f^{-\frac{ab'}{2}}=(f)^{-\frac{ab'}{2}}(-1)^{-\frac{ab'}{2}}\,.$$

Si $\frac{ab'}{2}$ est pair, $(-1)^{-\frac{ab'}{2}}=1$, et $(-f)^{-\frac{ab'}{2}}\equiv(-f)^{\frac{ab'}{2}}$ car la différence des exposants, ab', est $\equiv 0 \bmod 4$.

Si $\frac{ab'}{2}$ est impair, $(-1)^{-\frac{ab'}{2}}=-1$, $(-f)^{-\frac{ab'}{2}}\equiv-(-f)^{\frac{ab'}{2}}$ car la différence des exposants est $\equiv 2 \bmod 4$.

Donc dans les deux cas

$$2^{\frac{p-1}{4}}\equiv\left(\frac{b'}{a}\right)^{\frac{ab'}{2}}.$$

On peut aussi changer le signe de a. Donc on peut choisir $|a|$ et $|b|$. D'où

si $p=a^2+b^2$, a et b positifs, a impair

$$a^{\frac{ab}{2}}\,2^{\frac{p-1}{4}}\equiv b^{\frac{ab}{2}} \qquad \text{II}$$

De II on déduit le résultat I par un raisonnement analogue.

§ 4. Autre méthode pour les première et troisième étapes

a) Pour résoudre l'equation (1) $x^p=1$ (ou la congruence (2) $x^p\equiv 1 \bmod q$, où $p|q-1$). Gauss a découvert la méthode suivante.

Soit s une solution autre que 1. Les autres solutions autres que 1 sont

$$s,\ s^2,\ \cdots,\ s^{p-1},$$

soit, si g est une racine primitive mod p

$$s^0,\ s^g,\ s^{g^2},\ \cdots,\ s^{g^{p-2}}.$$

Soit $p-1=ef$. Les nombres suivants (cas de (1)) ou les restes mod q (cas (2))

$$s+s^{g^e}+s^{g^{2e}}+\cdots+s^{g^{(f-1)e}},$$

$$s^g+s^{g^{e+1}}+s^{g^{2e+1}}+\cdots+s^{g^{(f-1)e+1}},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$s^{g^{e-1}}+s^{g^{2e-1}}+\cdots+s^{g^{ef-1}},$$

sont les périodes à f termes (Les exposants de g vont de e en e). Si f' divise f, chaque période à f terme se décompose en somme de f/f' périodes à f' termes. Gauss prouve deux théorèmes:

DA § 345. Le produit de deux périodes à f termes est une combinaison linéaire (non homogène) à coefficients entiers des périodes à f termes.

DA § 350. Soit $p-1=\alpha\beta\gamma$. Un polynôme symétrique en les β périodes à γ termes dont la somme est une période à $\beta\gamma$ termes est une combinaison linéaire (non homogène) à coefficients entiers des périodes à $\beta\gamma$ termes.

Grâce à ces deux résultats on peut résoudre (1) (ou (2)) par une suite d'équations dont les degrés sont les facteurs premiers de $p-1$. (La théorie de Galois montre que ce sont les degrés minimum possible.)

En utilisant ces résultats Gauss prouve aussi des résultats de théorie des nombres, par exemple que l'on obtient autant de résidus que de non résidus quadratiques en ajoutant 1 aux non résidus.

Les résultats cités, et leurs conséquences arithmétiques s'obtiennent en considérant *l'ensemble des exposants de s* (considérés comme restes modulo p) dans le produit de deux périodes:

b) Sur les ensembles de restes modulo p définissons deux opérations:

Somme: réunion

Produit A×B: on prend un reste dans A et un reste dans B, de toutes les manières possibles, et on les ajoute mod p.

Les périodes, considérées comme ensembles de restes mod p, sont:

$$g^0=1,\ g^e,\ g^{2e},\ \cdots,\ g^{(f-1)e},$$
$$g,\ g^{1+e},\ g^{1+2e},\ \cdots,\ g^{1+(f-1)e},$$
$$\cdots\cdots\cdots\cdots$$
$$g^{e-1},\ g^{2e-1},\ \cdots,\ g^{fe-1}.$$

Formule générale: $g^a,\ g^{a+e},\ g^{a+2e},\ \cdots,\ g^{a+(f-1)e}$ désigné par (g^a, f) où g^a est un terme de la période, et f sa longueur. Calculons le produit de deux périodes $(g^a, f)\times(g^b, f)$. Nous ajoutons g^i à tous les termes de (g^b, f) puis g^{a+e}, $\cdots$, et en même temps chaque fois nous permutons circulairement les termes de (g^b, f):

$$\begin{array}{rcl}
g^a+ & g^b, \quad g^{b+e}, \quad \cdots, & g^{b+e(f-1)} \\
g^{a+e}+ & g^{b+e}, \quad g^{b+2e}, \quad \cdots, & g^{b+ef}=g^b \\
\cdots\cdots & \cdots\cdots\cdots\cdots\cdots & \\
g^{a+(f-1)e}+ & g^{b+(f-1)e}, \quad g^b, \quad \cdots, & g^{b+(f-2)e}
\end{array}$$

Les termes de la première colonne sont g^a+g^b, $g^{a+e}+g^{b+e}=(g^a+g^b)g^e$, $\cdots$, $(g^a+g^b)g^{(f-1)e}$ c'est à dire (g^a+g^b, f). De même pour la 2^e: (g^a+g^{b+e}, f). Donc en tout on obtient

$$(g^a+g^b, f)\cup(g^a+g^{b+e}, f)\cup\cdots(g^a+g^{b+(f-1)e}, f),$$

(De là résulte immédiatement le résultat du § 345).

Mais on peut permuter a et b; cela revient à grouper autrement les restes du produit:

$$(g^b+g^a, f)\cup(g^b+g^{a+c}, f)\cup\cdots .$$

La comparaison de ces résultats donne la 1ère Etape:

c) *Cas quadratique*: $f=\frac{p-1}{2}$ $e=2$.

Les périodes sont l'ensemble des résidus $\mathrm{R}=\left(1, \frac{p-1}{2}\right)$ et des non résidus $\mathrm{N}=\left(g, \frac{p-1}{2}\right)$

$$\mathrm{R}\times\mathrm{N}=(1, f)\times(g, f)=\begin{cases}(1+g, f), & (1+g^3, f), \cdots \\ (g+1, f), & (g+g^2, f), \cdots .\end{cases}$$

Dans le résultat chaque période est $(1, f)$, si le premier terme est un résidu, (g, f) si le premier terme est un non résidu, ou $f=\frac{p-1}{2}$ fois 0 si le terme écrit est 0. Les premiers termes des périodes dela première ligne sont les restes $1+\mathrm{N}$, ceux de la 2e ligne sont $g+\mathrm{R}$, soit $g(1+\mathrm{N})$.

Il y a donc autant de $1+\mathrm{N}$ résidus que de $g(1+\mathrm{N})$ résidus c'est-à-dire de $1+\mathrm{N}$ non résidus. C. Q. F. D.

Conséquence. Equation vérifiée par les périodes à $\frac{p-1}{2}$ termes (au sens a)

$$p+p'=-1 .$$

Si $p\equiv 1 \bmod 4$ l'ensemble des exposants de pp' est $\frac{p-1}{4}\mathrm{R}\cup\frac{p-1}{4}\mathrm{N}$ donc $\frac{p-1}{4}(\mathrm{R}+\mathrm{N})$. Or à $\mathrm{R}+\mathrm{N}$ correspond la somme de toutes les racines, sauf 1, i.e. -1. Donc $pp'=-\frac{p-1}{4}$.

Si $p\equiv 3 \bmod 4$ l'ensemble des exposants de pp' est $\frac{p-3}{4}(\mathrm{R}+\mathrm{N})\cup\frac{p-1}{2}$ fois 0, car ici -1 est non résidu, donc on obtient une fois 0 comme premier terme.

Donc $$\frac{p-1}{2}-\frac{p-3}{4}=\frac{p+1}{4} .$$

D'où les équations

$$X^2+X\begin{cases}-\frac{p-1}{4}=0 & \text{si } p\equiv 1 \bmod 4 \\ +\frac{p-1}{4}=0 & \text{si } p\equiv 3 \bmod 4 .\end{cases}$$

d) *Cas biquadratique*: $p=4n+1$, $f=\dfrac{p-1}{4}=n$, $e=4$.

Les quatre périodes sont $(1, n)=A$, $(g, n)=B$, $(g^2, n)=C$, $(g^3, n)=D$. On calcule les produits deux à deux, des deux manières:

$$A\times B=(1, n)(g, n)=\begin{cases}(1+g, n),\ (1+g^5, n), \cdots \\ \qquad =(1, 0)A\cup(1, 1)B\cup(1, 2)C\cup(1, 3)D\ , \\ (g+1, n),\ (g+g^4, n)\cdots =(g(1+g^{p-2}), n),\ (g(1+g)^3), n)\cdots\ , \\ \qquad =(3, 0)B\cup(3, 1)C\cup(3, 2)D\cup(3, 3)A\ .\end{cases}$$

Donc $(1, 0)=(3, 3)$, $(1, 1)=(3, 0)$, $(1, 2)=(3, 1)$, $(1, 3)=(3, 2)$.

On obtient toujours les mêmes relations en faisant le produit de périodes dont les numéros différent de 1 ou de 3

$$A\times C=\left\{\begin{array}{l}(1+g^2, n)(1+g^6, n)\cdots \\ \qquad =(2, 0)A\cup(2, 1)B\cup(2, 2)C\cup(2, 3)D \\ (g^2+1, n)(g^2+g^4, n)\cdots =(g^2(1+g^{p-3}), n)(g^2(1+g^2), n)\cdots \\ \qquad =(2, 0)C\cup(2, 1)D\cup(2, 2)A\cup(2, 3)B\end{array}\right\}$$

et éventuellement n fois 0, si $-1\in C$. D'où $(2, 2)=(2, 0)$ et $(2, 1)=(2, 3)$.

On retrouve bien les résultats de la 1ère étape.

Par cette méthode on peut calculer tous les produits deux à deux, y compris $A\times A\cdots$; mais ceux ci ne donnent pas de relation.

La deuxième étape se fait comme dans l'autre méthode.

e) *Troisième étape* — (Il faut distinguer les cas $p\equiv 1$ et $p\equiv 5 \bmod 8$)

La méthode consiste à calculer le produit ABC des deux manières:

$$(A\cdot B)C=A(B\cdot C)\ .$$

Par exemple, si $p\equiv 1 \bmod 8$,

$$(A\cdot B)C=(iA\cup lB\cup mC\cup mD)\times C\ .$$

Connaissant les produits deux à deux, on calcule (AB)C. Puis on calcule A(BC). On trouve 5 égalités: les coefficients de A, B, C, D et du reste 0. On trouve que ces égalités sont soit III, soit des identités. Si au lieu de ABC on prend un autre produit de trois périodes, on trouve aussi soit III soit des identités.

DEUXIÈME PARTIE

Démonstration de la loi de réciprocité quadratique et de la loi de réciprocité biquadratique.

§ 1. Nombre des solutions d'une congruence modulo p

Soit $f(x)=f(x_1 \cdots x_n)$ un polynôme à coefficients entiers, et soit N le nombre des solutions de la congruence $f(x)\equiv 0 \bmod p$.

Si t parcourt un ensemble complet de restes modulo p:

si $f(x)\equiv 0 \pmod p$ $tf(x)$ est p fois 0 mod p

si $f(g)\not\equiv 0 \pmod p$ $tf(x)$ parcourt un ensemble complet de restes modulo p.

Donc:

> Quand $x_1, \cdots, x_n, t$ parcourent independamment chacun un ensemble de restes complet, $tf(x)$ parcourt des ensembles de restes complets, et Np fois le reste 0.

§ 2. Birestes et ensembles de birestes

Définition 1) Cas «quadratique»: couples formes d'un reste modulo 2 et d'un reste modulo p.

2) Cas «biquadratique»: couples formés d'un reste modulo 4 et d'un reste modulo p.

Notation. (u, x) où u est un reste modulo 2 ou 4, et x un reste modulo p.

Nous ferons deux opérations sur les *ensembles de birestes.*

Réunion

Produit $S\times S'$.

C'est l'ensemble de birestes obtenu ainsi. On prend de toutes les manières un bireste de S et un de S', et on ajoute séparément leurs composantes (modulo 2 ou 4 et modulo p respectivement). L'ensemble produit est la réunion des birestes obtenus ainsi.

Il est clair que $A\times(B\cup C)=(A\times B)\cup(A\times C)$.

Ensembles de birestes complets. (Désignés par FS «full set»)

Réunion d'ensembles de birestes de la forme $\bigcup_{x\equiv 0,\cdots,p-1}(u, x)$, où u est fixe, et x parcourt un ensemble complet de restes modulo p.

Ensembles de birestes opposés deux à deux. (Notés OS «opposite set»)

Cas quadratique: Réunion d'ensembes $(0, x)(1, x)$; chaque fois qu'il a le bireste (u, x) il y a aussi le bireste $(u+1, x)$.

Cas biquadratique: Réunion d'ensembles $(u, x)(u+2, x)$; chaque fois qu'il y a le bireste (u, x) il y a aussi le bireste $(u+2, x)$.

Deux ensembles de birestes sont *opposés* si leur réunion est un OS.

PROPOSITION. *Le produit d'un ensemble quelconque par un*

1) *un ensemble complet est un ensemble complet*
2) *un ensemble opposé deux à deux est un ensemble opposé deux à deux*

$$S \times FS = FS \qquad S \times OS = OS .$$

Démonstration. 1) Si on ajoute successivement un ensemble complet de restes modulo p à un reste fixe on obtient un ensemble complet.

2) Chaque fois que dans le résultat il y a le bireste (u, x) il y a aussi le bireste $(u+1, x)$ (respectivement $(u+2, x)$).

§ 3. Nombre de solutions de la congruence

$$f(x) = a_1 x_1^2 + \cdots + a_n x_n^2 - b \equiv 0 \pmod p \text{ où } (a_i, p) = 1, \ \prod_i a_i = A .$$

a) D'après le § 1: $\quad S_0 = \bigcup_{t, x} (0, tf(x)) = Np(0, 0) \cup FS .$

Les termes où $t \equiv 0$ donnent les birestes:

$$\bigcup_{x \bmod p} (0, 0) = p^n (0, 0) .$$

Donc, d'après la définition du produit des ensembles de birestes:

$$S_0 = p^n (0, 0) \bigcup_{\substack{t \not\equiv 0 \\ x \bmod p}} (0, a_1 t x_1^2 + \cdots + a_n t x_n - bt) = p^n (0, 0) \bigcup_{t \not\equiv 0} (0, -bt) \prod_i \{ \bigcup_{x_i} (0, a_i t x_i^2) \} .$$

Posons ici:

$$R = \bigcup_{\left(\frac{r}{p}\right) = 1} (0, r), \quad N = \bigcup_{\left(\frac{n}{p}\right) = -1} (0, n) \text{ — Alors } R = \bigcup_r (1, r), \quad -N = \bigcup_n (1, n)$$

et $R \cup -R$, $N \cup N$ sont des OS.

Suivant que $\left(\frac{a_i t}{p}\right) = \begin{cases} +1 \\ -1 \end{cases}$:

$$\bigcup_{x_i \bmod p} (0, a_i t x_1^2) = \begin{cases} 0 \cup 2R \equiv 0 \cup R \cup N \cup R \cup -N \pmod{OS} \equiv R \cup -N \bmod (OS, FS) \\ 0 \cup 2N \equiv 0 \cup R \cup N \cup N \cup -R \pmod{OS} \equiv N \cup -R \bmod (OS, FS) \end{cases}$$

Donc $\quad \boxed{Np(0, 0) \equiv p^n (0, 0) \bigcup_{t \not\equiv 0} (0, -bt) \left(\frac{At^n}{p}\right) (R \cup -N)^n \bmod (OS, FS)}$

b) *Calcul de* $(R \cup -N)^2$. Il sera commode de noter multiplicativement les premières composantes:

$0 \to 1$
$A \to -1$ et addition mod $2 \to$ multiplication

$R \cup -N = \bigcup_{(x,p)=1} \left(\left(\frac{x}{p}\right), x\right)$, donc:

$$(R \cup -N) \bigcup_{x \neq 0} \left(\left(\frac{xy}{p}\right), x+y\right) \bigcup_{\substack{x,z\neq 0 \\ xz=y}} \left(\frac{z}{p}, x(1+z)\right) = \bigcup_{z\neq 0} \left(\left(\frac{z}{p}\right), 0\right) \left\{ \bigcup_{x} (1, x(1=z)) \right\}.$$

Si $1+z \equiv 0$, ou $z \equiv -1$ $\therefore \left(\left(-\frac{p}{1}\right), 0\right)((p-1)(1,0)) = (p-1)\left(\left(\frac{-1}{p}\right), 0\right)$.

Si $1+z \not\equiv 0$, $\bigcup_x (1, x(1+z))$ est un FS auquel manque $(1,0)$. En y ajoutant l'OS: $(1,0)$, $(-1,0)$ on obtient FS $\cup(-1,0)$. Donc $\bigcup_x (1, x(1+z)) \equiv (-1,0) \bmod (OS, FS)$.

Donc $$(R \cup -N)^2 \equiv (p-1)\left(\left(\frac{-1}{p}\right), 0\right) \bigcup_{\substack{z\neq 0 \\ z\neq -1}} \left(-\left(\frac{z}{p}\right), 0\right) \bmod OS, FS .$$

Considérons donc $$\bigcup_{z=1,\cdots,p-2} \left(-\left(\frac{z}{p}\right), 0\right).$$

Si $\left(-\frac{1}{p}\right) = 1$ parmi ces birestes il y en a

$$\frac{p-1}{2} \text{ où } -\left(\frac{z}{p}\right) = +1 \text{ et } \frac{p-1}{2} - 1 \text{ où } -\left(\frac{z}{p}\right) = -1 .$$

Si $\left(-\frac{1}{p}\right) = -1$ parmi ces birestes il y en a

$$\frac{p-1}{2} - 1 \text{ où } -\left(\frac{z}{p}\right) = +1 \text{ et } \frac{p-1}{2} \text{ où } -\left(\frac{z}{p}\right) = -1 .$$

Donc cet ensemble bireste est $\equiv \left(\left(-\frac{p}{1}\right), 0\right) \bmod OS$, et finalement:

$$\boxed{(R \cup -N)^2 \equiv p\left(\left(\frac{-1}{p}\right), 0\right) \bmod (FS, OS)}$$

c) *Cas où n est pair* (inutile pour la loi de réciprocité quadratique). En tenant compte du résultat de b), et du fait que n est pair le résultat de a) est ici:

$$Np(1,0) \equiv p^n(1,0) \cup \left(\frac{A}{p}\right) p^{n/2} \left(\left(-\frac{p}{1}\right)^{n/2}, 0\right) \left\{ \bigcup_{t\neq 0} (1, -bt) \right\} \bmod (OS, FS) .$$

Si $b \not\equiv 0 \bigcup_{t \not\equiv 0} (1, -bt) \equiv (-1, 0) \bmod (OS, FS)$ (Se voit en ajoutant l'OS: $(-1, 0)$, $(1, 0)$).

Donc $$Np(1, 0) \equiv p^n(1, 0) \cup p^{n/2}\left(-\left(\frac{(1-1)^{n/2}A}{p}\right), 0\right) \bmod (OS, FS) .$$

Cette relation montre que nécessairement

$$Np = p^n - p^{n/2}\left(\frac{(-1)^{n/2}A}{p}\right).$$

D'où $$\boxed{N = p^{n-1} - p^{(n/2)-1}\left(\frac{(-1)^{n/2}A}{p}\right)} .$$

Si $b \equiv 0$, $\bigcup_{t \not\equiv 0} (1, -bt) = (p-1)(1, 0)$, d'où résulte:

D'où $$\boxed{N = p^{n-1} + p^{(n/2)-1}(p-1)\left(\frac{(-1)^{n/2}A}{p}\right)} .$$

d) *Cas où n est impair*

Ici le résultat de a) devient:

$$Np(1, 0) \equiv p^n(1, 0 \cup \left(\frac{A}{p}\right)p^{\frac{n-1}{2}}\left(\left(\frac{-1}{p}\right)^{\frac{n-1}{2}}, 0\right)(R \cup -N)\left\{\bigcup_t \left(\left(\frac{t}{p}\right), -bt\right)\right\} \bmod (OS, FS),$$

si $b \not\equiv 0$: Posons $-bt = 0$, d'où $\left(\frac{t}{p}\right) = \left(\frac{-b}{p}\right)\left(\frac{u}{p}\right)$. Il vient:

$$Np(1, 0) \equiv p^{-n}(1, 0) \cup \left(\frac{-Ab}{p}\right)p^{\frac{n-1}{2}}\left(\left(\frac{-1}{p}\right)^{\frac{n-1}{2}}, 0\right)(R \cup -N)\left\{\bigcup_u \left(\left(\frac{u}{p}\right), u\right)\right\} .$$

Il y a donc encore une fois le facteur $(R \cup -N)^2$, et donc:

$$Np(0, 0) = p^n(0, 0)\left(\frac{-Ab}{p}\right)p^{\frac{n-1}{2}}\left(\left(\frac{-1}{p}\right)^{\frac{n+1}{2}}, 0\right) \bmod (OS, FS) .$$

Le seul ensemble de $(0, 0)$ congru au terme de droite modulo des OS, FS étant

$$\left[p^n + \left(\frac{(-1)^{\frac{n-1}{2}}Ab}{p}\right)p^{\frac{n-1}{2}}\right](0, 0) ,$$

on trouve:

$$\boxed{N = p^{n-1} + \left(\frac{(-1)^{\frac{n-1}{2}}Ab}{p}\right)p^{\frac{n-1}{2}}}$$

(Si $b \equiv 0 \bmod p$, $\bigcup_t \left(\left(\frac{t}{p}\right), 0\right)$ est un OS, d'où $N = p^{n-1}$) .

e) *Démonstration de la loi de réciprocité quadratique*

q étant un autre nombre premier, nous appliquons le résultat de d) à la congruence

$$(c) \quad x_1^2 + \cdots + x_q^2 \equiv q \bmod p .$$

Parmi les solutions de (c) il y a celles où les x_i sont tous égaux. Cela donne:

$$qx^2 \equiv q \quad \text{ou} \quad x^2 \equiv 1 \quad \text{ou} \quad x \equiv \pm 1 \bmod p \quad \text{soit deux solutions.}$$

Si dans une solution tous les x_i ne sont pas égaux, par permutation circulaire on obtient q solutions *distinctes*. En effet (Gauss *DA* § 41) si deux solutions obtenues par permutation circulaires étaient identiques, il existerait $k \neq q$ tel que, pour tout i, $x_i = x_{i+k} = x_{i+2k} = \cdots = x_{i+mk} = \cdots$. Comme q est premier, il existe toujours m tel que $mk \equiv 1 \bmod q$, et par conséquent $x_i = x_{i+1} = \cdots = x_{i+q}$, tous les x_i seraient égaux.

Donc $N \equiv 2 \bmod q$, soit:

$$p^{q-1} + \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) p^{\frac{q-1}{2}} \equiv 2 \bmod q .$$

Mais $p^{q-1} \equiv 1 \bmod p$, et $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \bmod q$

$$\text{d'où} \quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right) = (-1)^{\frac{q-1}{2}\,\frac{q-1}{2}} \qquad \text{C. Q. F. D.}$$

§ 4. Entiers de Gauss (rappels)

Les nombres premiers π sont les nombres premiers réels $q \equiv 3 \bmod 4$, les facteurs complexes $a \pm bi$ des nombres premiers réels $p \equiv a^2 + b^2 \equiv 1 \bmod 4$, et $1+i$, avec $(1+i)^2 = 2i$. La décomposition d'un nombre en facteurs premiers est unique, aux unités près. Si $\pi \neq 1+i$, le nombre de classes modulo π est soit q^2, soit p, donc toujours $\equiv 1$ modulo 4. Donc les raisonnements, résumés page 4 s'appliquent aussi. Ici $i^2 \equiv -1 \bmod \pi$.

Nom	Numéro	Critère	Propriété
A	0	$x^{\frac{p-1}{4}} \equiv 1$	Résidus biquadratiques
B	1	$x^{\frac{p-1}{4}} \equiv i$	
C	2	$x^{\frac{p-1}{4}} \equiv -1$	Résidus quadratiques non biquadratique
D	3	$x^{\frac{p-1}{4}} \equiv -i$	

π détermine complètement les quatre classes A, B, C, D. La puissance de i à laquelle est congru $x^{\frac{p-1}{4}}$ est notée $\left(\frac{x}{\pi}\right)_4$.

Cas des nombres premiers $m=a+bi$, $p=(a+bi)(a-bi)=mm'$.

En utilisant le fait que a et b sont premiers entre eux on voit facilement que toute classe mod m a un représentant mod p. On peut donc séparer grâce à m, l'aide du critère précédent, les classes mod p en quatre classes. On peut aussi le faire comme à la page 4, en es fixant à priori la classe B.

Si B (*ou e, ou f*) *est choisi de manière à ce que le b obtenu par la théorie de la première partie soit le b de* $m=a+bi$, *les classes* B *pour p et m coincident.* En effet nous avons alors $a+bf\equiv 0 \bmod p$ donc $a+bf\equiv 0 \bmod p$ donc $a+bf\equiv 0 \bmod m$, donc $b(f-i)\equiv 0 \bmod m$, donc $f\equiv i \bmod m$, donc le critère pour le classe B est le même dans les deux cas.

Si $(x, y)=1$, et si $y=\pi_1\pi_2\cdots\pi_n$ (les π_n non forcément distincts, et $\neq 1+i$) nous posons $\left(\frac{x}{y}\right)_4=\prod_{i=1\to n}\left(\frac{\pi_i}{x}\right)_4$.

§ 5. Énoncé de la loi de réciprocité biquadratique

1) Soit q un nombre premier réel, congru à 3 modulo 4, l un entier réel premier à q alors $\left(\frac{l}{q}\right)_4=1$, ($l$ est résidu biquadratique *complexe* de q).

En effet $l^{\frac{q^2-1}{4}}=l^{q-1}\cdot^{\frac{q+1}{4}}\equiv 1 \bmod q$, car $\frac{q+1}{4}$ est entier.

2) Soit m un nombre premier complexe, $m=a+bi$, $a^2+b^2=p$ $a\equiv 1 \bmod 4$. Soit q un nombre premier congru à 3 modulo 4. Alors

$$\left(\frac{m}{q}\right)_4=\left(\frac{-q}{m}\right)_4.$$

La même démonstration fournit aussi le résultat: Soit $p_1=m_1m_1'$ un autre nombre premier congru à 1 modulo 4. Alors

$$\left(\frac{m}{p_1}\right)_4=\left(\frac{m}{m_1}\right)_4\left(\frac{m}{m_1'}\right)_4=\left(\frac{p_1}{m}\right)_4.$$

En combinant ces deux résultats: Soit k un nombre réel, premier à m, congru à 1 modulo 4. Alors

$$\left(\frac{k}{m}\right)_4=\left(\frac{m}{k}\right)_4. \qquad \text{II}$$

3) Si m et M sont deux nombres premiers complexes

$$m=a+bi \quad M=A+Bi \quad p=a^2+b^2 \quad P=A^1+B^2 \quad a\equiv A\equiv 1 \bmod 4$$

$$\left(\frac{m}{M}\right)_4=(-1)^{\frac{p-1}{4}\cdot\frac{P-1}{4}}\left(\frac{M}{m}\right)_4. \qquad \text{III}$$

REMARQUES. 1) La partie la plus difficile est le résultat 2).

2) On énonce souvent le résultat 3 en choisissant les associés m_1 et M_1 congrus à 1 mod $2+2i$, c'est-à-dire $\frac{a-1}{2}$ et $\frac{b}{2}$ de même parité, cela revient à prendre $m_1=m$ si $\frac{b}{2}$ est pair ou $p\equiv 1 \bmod 8$ et $m_1=-m$ si $p\equiv 5 \bmod 8$ (Même choix pour M_1). Que se passe-t-il si dans III on remplace m et M par m_1 et M_1?
1) Si p et P sont $\equiv 1 \bmod 8$, $m_1=m$, $M_1=M$, donc rien n'est changé dans III.
2) Si $p\equiv 5$ et $P\equiv 1 \bmod 8$, $m_1=-m$, $M_1=M$. Le membre de droite n'est pas changé, et le membre de gauche non plus, car -1 est dans la classe A de M.
3) Si p et $P\equiv 5 \bmod 8$, $m_1=-m$, $M_1=-M$, et -1 est dans les classes C,

$$\text{donc } \left(\frac{m_1}{M_1}\right)_4=-\left(\frac{m}{M}\right)_4 \text{ et } \left(\frac{M_1}{m_1}\right)_4=-\left(\frac{M}{m}\right)_4 .$$

Donc III est vrai aussi.

§ 6. Calcul de certaines ensembles de birestes

Soit p un nombre premier, congru à 1 modulo 4. Nous définissons quatre fonctions de x modulo p à valeur entier modulo 4.

$x\in$	A	B	C	D	Définition de k_i
$k_0(x)$	0	0	0	0	0
$k_1(x)$	0	1	2	3	Numéro de la classe de x
$k_2(x)$	0	2	0	2	$2k_1(x)$
$k_3(x)$	0	3	2	11	$3k_1(x)=-k_1(x)$

Les classes A B C D sant définies comme dans la première partie. Ces fonctions vérifient:

$$k_i(xy)=k_i(x)+k_i(y) .$$

Considérons les ensembles de birestes (biquadratiques)

$$T=\bigcup_{x\not\equiv 0 \bmod p}(k_1(x), x) \qquad \bar{T}=\bigcup_{x\not\equiv 0 \bmod p}(k_3(x), x) \qquad V=\bigcup_{x\equiv 0}(k_2(x), x) .$$

Dans ce paragraphes nous proposons de trouver une expression simple pour les ensembles $T\bar{T}$, V^2 et T^4, modulo des OS et FS.

a) *Calcul de* $T\bar{T}$. (On pose $k_1(x)=k(x)$)

$$T\bar{T}=\bigcup_{\substack{x,y\\ x,y \text{ 1ers à } p}}(k(x)-k(y), x+y). \text{ Posons } xy=z \text{—alors } k(x)-k(y)=k(z) \text{ d'où}$$

$$T\bar{T}=\bigcup_{y,z}(k(z), y(1+z))=\bigcup_{z}(k(z), 0)\bigcup_{y}(0, y(1+z)) .$$

Si $z\equiv -1$ on obtient $(p-1)(k(-1),0)$.

Si $z\not\equiv -1$ on obtient $(k(z),0)\times(\mathrm{FS}-0)\equiv(k(z)+2,0) \bmod \mathrm{FS}, \mathrm{OS}$.

(l'OS ici étant $(k(z)+2,0), (k(z),0)$.)

$$\mathrm{T}\bar{\mathrm{T}}\equiv(p-1)(k(-1),0) \bigcup_{z\not\equiv 1,0} (k(z)+2,0) \bmod \mathrm{OS}, \mathrm{FS} .$$

Ajoutons l'OS $(k(-1)+2,0)(k(-1),0)$:

$$\mathrm{T}\bar{\mathrm{T}}\equiv p(k(-1),0) \bigcup_{z\not\equiv 0} (k(z)+2,0)=p(k(-1),0) \bmod (\mathrm{OS}, \mathrm{FS})$$

car $\bigcup (k(z)+2,0)$ est un OS

$$\boxed{\mathrm{T}\bar{\mathrm{T}}=(-1)^{\frac{p-1}{4}} p(0,0) \bmod \mathrm{OS}, \mathrm{FS}} .$$

b) *Calcul de* V^2. On peut considérer V comme un ensemble de birestes quadratiques:

$0\to 0$
$2\to 1$, addition mod $4\to$ addition mod 2 pour les premières composantes.

Donc, d'après p. 18, et comme $p\equiv 1 \bmod 4$,

$$\boxed{\mathrm{V}^2\equiv p(0,0) \bmod (\mathrm{FS}, \mathrm{OS})} .$$

(Les OR modulo lesquels on a calculé étant ici de la forme $\bigcup_x (0,x),(2,x)$).

c) *Calcul de* T

$$\mathrm{T}^2= \bigcup_{\substack{x,y \\ x,y \text{ premiers entre eux } p}} (k(x)+k(y), x+y)= \bigcup_{\substack{x,z \\ xz=y}} (2k(x)+k(z), x(1+z)) .$$

D'où, en regroupant:

$$\mathrm{T}^2= \bigcup_{(z,p)=1} (k(z),0) \bigcup_{\substack{x \\ (x,p)=1}} (2k(x), x(1+z)) .$$

Si $z\equiv -1$: $(k(-1),0) \bigcup_{\substack{x \\ (x,p)=1}} (2k(x),0)=\dfrac{p-1}{2}\cdot[(k(-1),0),(k(-1)+2,0)]=\mathrm{OS}$.

Si $z\not\equiv -1$, posons $x(1+z)=t$ — Alors $2k(x)=2k(t)-2k(1+z)=2k(t)+2k(1+z) \bmod 4$.

Donc, mod OS

$$\mathrm{T}^2 \equiv \bigcup_{\substack{(z,p)=1 \\ z\not\equiv -1}} (k(z)+2k(1+z,0)\times(2k(t),t)=\mathrm{V}\times \bigcup_{\substack{(z,p)=1 \\ z\not\equiv -1}} (k(z)+2k(1+z),0)=\mathrm{V}\times\mathrm{W} .$$

Il reste à déterminer W, c'est à dire à trouver combien de fois $k(z)+2k(1+z)$ vaut

repsectivement 0, 1, 2 et 3. Pour cela nous utilisons le tableau des 16 nombres de la première partie.

Si z est un A, $k(z)=0$ et

$$(z\neq -1)\ 1+z \text{ est dans } \begin{bmatrix} \text{A } (0,0) & \text{fois} \\ \text{B } (0,1) & \text{"} \\ \text{C } (0,2) & \text{"} \\ \text{D } (0,3) & \text{"} \end{bmatrix} \text{ donc } 2k(1+z) \text{ vaut } \begin{cases} 0\ (0,0)+(0,2) & \text{fois} \\ 2\ (0,1)+(0,3) & \text{"} \end{cases}$$

et, comme $k(z)=0$

$$k(z)+2k(1+z) \quad \text{vaut} \begin{cases} 0\ (0,0)+(0,2) & \text{fois} \\ 2\ (0,1)+(0,3) & \text{fois}. \end{cases}$$

En faisant le même raisonnement pour $z\in$ B, puis $z\in$ C, puis $z\in$ D on trouve finalement que

$$k(z)+2k(1+z) \quad \text{vaut} \left\{ \begin{array}{l} 0\ (0,0)+(0,2)+(2,1)+(2,3)=\alpha \\ 1\ (1,0)+(1,2)+(3,3)+(4,0)=\beta \\ 2\ (0,0)+(0,3)+(2,0)+(2,2)=\gamma \\ 3\ (3,0)+(3,3)+(1,1)+(1,3)=\delta \end{array} \right\} \text{ fois, et donc:}$$

$$T^2\equiv V\times\{\alpha(1,0)\cup\beta(1,0)\cup\gamma(2,0)\cup\delta(3,0) \mod OS.$$

Donc

$$T^2\equiv V\times\{(\alpha-\gamma)(0,0)\cup(\beta-\delta)(0,1)\} \mod OS.$$

(Où si par exemple $\alpha-\gamma$ est négatif, l'ensemble de birestes $(\alpha-\gamma)$ fois $(0,0)$ est l'ensemble de birestes opposé $(\gamma-\alpha)(2,1)$).

D'autre part on peut calculer $\alpha-\gamma$ et $\beta-\delta$ à l'aide des seize nombres. Dans ce calcul il faut distinguer les cas $p=8n+1$ et $p=8n+5$. Dans les deux cas on trouve

$\left.\begin{array}{l}\alpha-\gamma=-a \\ \beta-\delta=-b\end{array}\right|$ où a et b sont les nombres fournis par la théorie de la 1ère partie,

c'est à dire: $p=a^2+b^2$, $a\equiv 1 \mod 4$, $a+bf\equiv 0 \mod p$.

$$\text{Donc: } T^2\equiv V\times\{-a(0,0)\cup -b(1,0)\} \mod OS.$$

Un ensemble de birestes de deuxième composante nulle est égal modulo des OS a un et un seul ensemble $x(0,0)\cup y(1,0)$ (où x et y peuvent être négatifs).

Pour déterminer, modulo des OS, un produit de tels ensembles et exprimer le résultat sous la même forme on peut calculer le produit des nombres complexes $x+iy$ correspondants et remplacer le résultat $x+iy$ par $X(0,0)+Y(1,0)$. Cela

résulte de l'isomorphisme du groupe additif des entiers modulo 4 et du groupe multiplicatif des puissances de i.

Posons $m=a+bi\,,\quad m'=a-bi\,.$

Avec ces conventions le facteur $(k_1(q),0)$ doit être remplacé par $\left(\frac{q}{m}\right)_4$: On doit le remplacer par i élevé à la puissance: numéro de la classe de q modulo p; *mais les classes modulo p et m coincident.* De même $(k_2(q),0)$ devient $\left(\frac{q}{p}\right)$ et $(-k_1(q),0)$: $\left(\frac{q}{m}\right)_4^3$.

Par conséquent V^2 devient p mod OS, FS

$\overline{TT}$ devient $(-1)^{\frac{p-1}{4}}pp$ mod OS, FS

T^2 devient $-Vm$ mod OS, et donc T^4 devient pm^2 mod OS, FS.

§ 7. Démonstration du résultat 2.

a) Soit N le nombre de solutions de la congruence $f(x)=a_1x_1^4+\cdots a_nx_n^4-b\equiv 0 \bmod p$ où $(a_i,p)=1$.

D'après les § 1 et 2 de la 2e partie (p. 129).

$$Np(0,0)\mathrm{FS}=\bigcup_{t,x \bmod p}(0,tf(x))=p^n(0,0)\bigcup_{t\not\equiv 0}(0,-bt)\bigcup_{x}(0,a_1tx_1^4+\cdots+a_ntx_n^4)$$

$$=p^n(0,0)\bigcup_{t\not\equiv 0}(0,-bt)\coprod_{i}\Big(\bigcup_{x_i \bmod p}(0,a_itx_i^4)\Big)\,.$$

Les birestes introduits ici sont les birestes biquadratiques. On a isolé les termes où $t=0 \pmod p$, et utilisé la définition du produit des ensembles de birestes (p. 130). Maintenant on peut évaluer autrement les facteurs du produit $\coprod_i\big(\bigcup_{x_i \bmod p}(0,a_itx_i^4)\big)$:

LEMME. *Soit v un nombre fixe premier à p. $k_j(x)$ étant les fonctions introduites* p. 135:

$$\bigcup_{x \bmod p}(0,vx^4)\equiv\bigcup_{j=1,2,3}\bigcup_{y\not\equiv 0}(k_j(y),v_y) \bmod \mathrm{OS, FS}\,.$$

Démonstration 1) $\bigcup_{x\not\equiv 0}(0,vx^4)\equiv\bigcup_{j=0,1,2,3}\bigcup_{y\not\equiv 0}(k_j(y),vy) \bmod \mathrm{OS}\,.$

En effet, quand y parcourt A, le terme de droite fournit quatre fois les birestes $(0,vA)$, c'est à dire $\bigcup(0,vx^4)$. D'autre part

pour chaque $y\in\left\{\begin{matrix}B\\C\\D\end{matrix}\right\}$ on obtient $\left\{\begin{matrix}(0,y)(1,y)(2,y)(3,y)\\(0,y)(2,y)(0,y)(2,y)\\(0,y)(3,y)(2,y)(1,y)\end{matrix}\right\}$ c'est-à-dire un OS.

2) Ajoutons $(0, 0)$. A droite:

$$(0, 0) \bigcup_{y \not\equiv 0} (k_0(y), 0) = \bigcup_{y \bmod p} (0, y) = \mathrm{FS}\,. \qquad \text{C. Q. F. D.}$$

De ce lemme résulte:

$$Np(0, 0) \equiv p^n(0, 0) \bigcup_{t \not\equiv 0} (0, -bt) \prod_i \Big(\bigcup_{j=1,2,3} \{ \bigcup_{x \neq 0} (k_j(y), a_i t y) \} \bmod \mathrm{OS}, \mathrm{FS}\,.$$

Comme: $$\mathrm{A} \times (\mathrm{B} \cup \mathrm{C}) = \mathrm{A} \times \mathrm{B} \cup \mathrm{A} \times \mathrm{C}\,.$$

$$Np(0, 0) \equiv p^n(0, 0) \bigcup_{j=1,2,3} \mathrm{S}_j \bmod \mathrm{OS}, \mathrm{FS} \text{ avec}$$
$$\mathrm{S}_j = \bigcup_{t \neq 0} (0, -bt) \prod_i \{ \bigcup_y (k_j(y), a_i t y) \}\,.$$

b) A partir de maintenant nous supposerons $a_i = 1$, $u = b = q$, c'est à dire $f(x) = x_1^4 + \cdots + x_q^4 - q$ (où q est un nombre premier distinct de p). Posons $ty = z$. Alors $(t \not\equiv 0 \bmod p)$

$$\bigcup_{y \not\equiv 0} (k_j(y), ty) = (-k_j(t), 0) \bigcup_{z \not\equiv 0} (k_j(z), z)\,.$$

Donc

$$\mathrm{S}_j = \bigcup_{t \not\equiv 0} (0, -qt)(-k_j(t), 0)^q \{ \bigcup_{z \not\equiv 0} (k_j(z), z) \}^q\,.$$

On combine le facteur $(0, -qt)$ avec un des facteurs $(-k_j(t), 0)$:

$$(0, -qt)(-k_j(t), 0) = (-k_j(t), -qt) = (k_j(q), 0)(-k_j(qt), -qt)\,.$$

D'où

$$\mathrm{S}_j = (k_j(q), 0) \bigcup_{t \not\equiv 0} (-k_j(bt), -qt)(-k_j(t), 0)^{q-1} \{ \bigcup_z (k_j(z), z) \}^q\,.$$

Remarquons:

$$(-k_j(-u), u) = \begin{cases} (-k_j(u), u) \text{ si } j = 1, 3 \text{ et } p = 8n+1 \text{ car } -1 \in \mathrm{A} \\ (-k_j(\mathrm{u}), u)(2, 0) \text{ si } j = 1, 3 \text{ et } p = 8n+5 \text{ car } -1 \in \mathrm{C} \\ (k_2(u), u) \text{ si } j = 2, \text{ car } \left(\dfrac{-1}{p}\right) = 1 \text{ et } k_2(u) = -k_2(u) = = k_2(-u)\,. \end{cases}$$

Le facteur $(2, 0)$ qui peut apparaitre si $j = 1, 3$ a pour effet de transformer le résultat en l'ensemble opposé. (On peut le noter $(-1)^{\frac{p-1}{4}}$.)

$$\mathrm{T} = \bigcup_{z \not\equiv 0} (k_1(z), z) \qquad \bar{\mathrm{T}} = \bigcup_{z \not\equiv 0} (k_3(z), z) \qquad \mathrm{V} = \bigcup_{z \not\equiv 0} (k_1(z), z)\,.$$

1) S_2: $q-1$ étant pair $(-k_2(t), 0)^{q-1} = (0, 0)$. Donc, d'après la remarque

$$\mathrm{S}_2 = (k_2(q), 0)\mathrm{V}^{q+1} \equiv \left(\frac{p}{q}\right) p^{\frac{q+1}{2}} \; (0, 0) \bmod \mathrm{OS}, \mathrm{FS}\,.$$

(En utilisant les résultats et notations du § 3, p. 131).

Pour calculer S_1 et S_3 il faut distinguer les cas $q\equiv 1 \bmod 4$ et $q\equiv 3 \bmod 4$.

2) $q\equiv 1 \bmod 4$. $q-1$ étant multiple de 4, $(k_j(t), 0)^{q-1}=(0, 0)$.

D'après la remarque

$$\bigcup_{t\neq 0}(-k_j(qt), -qt)=\{(-1)^{\frac{p-1}{4}}\{\bigcup_{z\neq 0}(-k_j(z), z) \quad \text{si} \quad j=1, 3\ .$$

Donc

$$S_1=(k_1(q), 0)(-1)^{\frac{p-1}{4}}T^q\bar{T}\equiv\left(\frac{q}{m}\right)_4 m^{\frac{q-1}{2}}q^{\frac{q+3}{4}} \bmod \mathrm{OS}, \mathrm{FS}\ ,$$

et

$$S_3\equiv\left(\frac{q}{m}\right)_4^3 m'^{\frac{q-1}{4}}q^{\frac{q+3}{4}} \bmod \mathrm{OS}, \mathrm{FS}\ ,$$

en utilisant les résultats et conventions de la page 137.

L'ensemble de birestes $Np(0, 0)$ et celui représenté par le nombre complexe

$$p^q+\left(\frac{q}{p}\right)p^{\frac{q+1}{2}}+\left(\frac{q}{m}\right)_4 p^{\frac{q+3}{4}}m^{\frac{q-1}{2}}+\text{conjugué}\ ,$$

différent de OS et FS. Mais leur différence au sens ensembliste ne peut contenir de FS, et la représentation d'un ensemble de birestes de deuxièmes composantes nulles par un nombre complexe est unique. Donc, en divisant par p:

$$N=p^{q-1}+\left(\frac{q}{p}\right)p^{\frac{q-1}{2}}+\left(\frac{q}{m}\right)_4 p^{\frac{q-1}{4}}m^{\frac{q-1}{2}}+\text{conjugué}\ .$$

La congruence $x_1^4+\cdots+x_q^4\equiv q \bmod p$ a quatre solutions où les x_i sont tous égaux. Donc, d'après le raisonnement fait à propos de la loi de réciprocité quadratique: (page 133).

$$N\equiv 4 \bmod q\ .$$

Soit $q=nn'$ la décomposition de q en facteurs premiers complexes.

$$p^{q-1}\equiv 1 \bmod q, \quad \text{donc} \bmod n. \quad p^{\frac{q-1}{2}}\equiv\left(\frac{p}{q}\right) \bmod q, \text{ donc} \bmod n.$$

$$p^{\frac{q-1}{1}}m^{\frac{q-1}{2}}=(m^3m^1)^{\frac{q-1}{4}}\equiv\left(\frac{m}{n}\right)_4^3\left(\frac{m'}{n}\right)_4 \text{ modulo } n.$$

Donc:

$$4\equiv 1+\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)+\left(\frac{q}{m}\right)_4\left(\frac{m}{n}\right)_4^3\left(\frac{m'}{n}\right)_4+\text{conjugé} \quad \text{modulo } n.$$

Chacun des termes de cette somme est une puissance de i. Montrons que chacun vaut 1:

$$4\equiv 1\pm 1+i^r+i^{-r} \bmod n\ .$$

Si $r=1$ ou 3, $3\equiv\pm 1+0 \bmod n$, donc n divise 2 ou 4: impossible.
Si $r=2$ $3\equiv\pm 1-2 \bmod n$, donc n divise 4 ou 6: impossible.
Donc $r=0$, d'où $3\equiv\pm 1+2$, soit $1\equiv\pm 1$. Mais n ne divise pas 2, donc le signe est $+$.

Le deuxième terme donne $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=1$, c'est à dire la loi de réciprocité quadratique dans ce cas.

Le troisième terme donne:

$$\left(\frac{q}{m}\right)_4\left(\frac{m}{n}\right)_4^3\left(\frac{m'}{n}\right)_4=1 \quad \text{où} \quad \left(\frac{q}{m}\right)_4\left(\frac{m'}{n}\right)_4=\left(\frac{m}{n}\right)_4 .$$

Mais $\left(\frac{m'}{n}\right)_4\left(\frac{m}{n'}\right)_4=1$, car ces deux puissances de i sont conjuguées. Donc:

$$\boxed{\left(\frac{q}{m}\right)_4=\left(\frac{m}{n}\right)_4\left(\frac{m}{n'}\right)_4 .} \tag{1}$$

C'est le résultat 2) dans le cas ($q\equiv 1 \bmod 4$).

Cas où $q\equiv 3 \bmod 4$. $q-1$ étant congru à 2 modulo 4

$$(-k_j(t), 0)^{q-1}=(-k_j(t), 0)^2=(k_{2j}(t), 0) .$$

Donc:

$$S_1=(k_1(q), 0)\underset{t\neq 0}{\cup}(-k_1(qt), -qt)(k_2(t), 0)T^q .$$

Posons $y=-qt$

$$(k_2(t), 0)=(k_2(tq^2), 0)=(k_2(q), 0)(k_2(-y), 0)=(k_2(q), 0)(k_2(y), 0)$$

$$\left(\text{car } \left(\frac{-1}{p}\right)=1\right).$$

$$(-k_1(-y), y)=\{(-1)^{\frac{p-1}{4}}\}(-k_1(y), y) .$$

Donc

$$S_1=\{(-1)^{\frac{p-1}{4}}\}(k_3(q), 0)\underset{y\neq 0}{\cup}(-k_1(y), y)(k_2(y), 0)T^q=\{(-1)^{\frac{p-1}{4}}\}(k_3(q), 0)T^{q+1} .$$

De là nous déduisons, comme dans le cas où $q\equiv 1 \bmod 4$

$$N=p^{q-1}+\left(\frac{q}{p}\right)p^{\frac{q-1}{2}}+(-1)^{\frac{p-1}{4}}p^{\frac{q-3}{4}}\left(\frac{q}{m}\right)_4^3 m^{\frac{q+1}{2}}p^{\frac{q-3}{4}}+\text{conjugué}\equiv 4 \bmod q .$$

D'après le théorème de Fermat et la loi de réciprocité quadratique les deux

premiers termes sont congrus à 1 modulo q. Soient $C+Di$ et $C-Di$ les autres termes.

D'une part: $C^2+D^2=p^{\frac{q+1}{2}+2\frac{q-3}{4}}=p^{q-1}\equiv 1 \pmod q$.

D'autre part: $C+Di+C-Di=2C\equiv 2 \bmod q$, d'où $C\equiv 1 \bmod q$.

Donc $$D\equiv 0 \bmod q .$$

D'où en tenant compte du caractère biquadratique de -1:

$$\boxed{\left(\frac{-q}{m}\right)_4^3 m^{\frac{q+1}{2}} p^{\frac{p-3}{4}} \equiv 1 \bmod q .} \qquad (2)$$

Élevons à la puissance $\frac{q-1}{2}$:

$$p^{\frac{q-3}{4}\cdot\frac{q-1}{2}} m^{\frac{q^2-1}{4}} \equiv \left(\frac{-q}{m}\right)_4^{\frac{q-1}{2}} \bmod q .$$

Soit

$$p^{\frac{q-3}{4}\cdot\frac{q-1}{2}} \left(\frac{m}{q}\right)_4 \equiv \left(\frac{-q}{m}\right)_4^{\frac{q-1}{2}} \bmod q .$$

a) Si $q=8r+3$, $\frac{q-3}{4}$ est pair, et $\frac{q-1}{2}=4r+1$. Donc:

$$\left(\frac{m}{q}\right)_4 = \left(\frac{-q}{m}\right)_4 .$$

b) Si $q=8r+7$, $\frac{q-1}{2}=4r+3$. D'autre part $m^q\equiv m' \bmod q$.

En effet $(a+ib)^q\equiv a^q+b^q\equiv a-ib \bmod q$, d'après le théorème de Fermat (p, donc a et b sont premiers à q), et parce que $q\equiv 3 \bmod 4$. Donc:

$$p^{\frac{q-1}{2}} = (mm')^{\frac{q-1}{2}} = (m^{1+q})^{\frac{q-1}{2}} = m^{\frac{q^2-1}{2}} \equiv \left(\frac{m}{q}\right)_4^2 \bmod q .$$

D'où résulte:

$$\left(\frac{m}{q}\right)_4^{1+2\cdot\frac{q-3}{4}} = \left(\frac{m}{q}\right)_4^{1+4r+2} = \left(\frac{m}{q}\right)_4^3 \equiv \left(\frac{-q}{m}\right)^3 \bmod q .$$

Comme il s'agit maintenant de puissances de i:

$$\left(\frac{m}{q}\right)_4 = \left(\frac{-q}{m}\right)_4 .$$

Cela achève démonstration du résultat 2).

Démonstration du resultat 3.

a) k et l réels, premiers entre eux, l impair. Alors $\left(\frac{k}{l}\right)_4 = 1$.

En effet, pour les facteurs premiers $4n+1$:

$$\left(\frac{k}{p}\right)_4 = \left(\frac{k}{m}\right)_4 \left(\frac{m'}{k}\right)_4 = 1,$$

pour les facteurs premiers $4n+3$:

$$\left(\frac{k}{q}\right)_4 = 1 \text{ d'après le résultat 1)}.$$

b) l réel, $l \equiv 1 \bmod 4$ — Alors $\left(\frac{i}{l}\right) = (-1)^{\frac{l-1}{4}}$:

l est produit de nombres premiers $4n+1$, et de carrés de nombres premiers $4n+3$

$$\left(\frac{i}{p}\right)_4 = \left(\frac{i}{m}\right)_4 \left(\frac{i}{m'}\right)_4 = (i)^{\frac{p-1}{4}} \cdot (i)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}}.$$

$$\left(\frac{q^2}{i}\right) = \left(\frac{i}{q}\right) \cdot \left(\frac{i}{q}\right) = i^{\frac{q^2-1}{4}} i^{\frac{q^2-1}{4}} = (-1)^{\frac{q^2-1}{4}}.$$

D'autre part $\frac{l-1}{4} + \frac{l'-1}{4} \equiv \frac{l'-1}{4}$. D'où le résultat.

c) Ces remarques préliminaires faites, soient $m = a+bi$ et $M = A+Bi$ deux nombres premiers complexes.

$$a^2+b^2 = p \quad a \equiv 1 \bmod 4 \quad A^2+B^2 = P \quad A \equiv 1 \bmod 4 \quad b \text{ et } B \text{ pairs.}$$

$$\left(\frac{A}{A+Bi}\right)_4 \left(\frac{a+bi}{A+Bi}\right)_4 = \left(\frac{Aa+Abi+(A+Bi)(-bi)}{A+Bi}\right)_4 = \left(\frac{Aa+Bb}{A+Bi}\right)_4 = \left(\frac{A+Bi}{Aa+Bb}\right)_4.$$

En effet: $(a+bi)$ et A sont premiers à $A+Bi$, donc aussi $Aa+Bb$, et $Aa+Bb \equiv 1 \bmod 4$ donc on peut appliquer le résultat 2). De même:

$$\left(\frac{A}{A+Bi}\right)_4 = \left(\frac{A+Bi}{A}\right)_4 = \left(\frac{B}{A}\right) \cdot \left(\frac{i}{A}\right) = 1 \cdot (-1)^{\frac{A-1}{4}} \text{ d'après a) et b).}$$

Donc $\left(\frac{m}{M}\right)_4 = \left(\frac{A+Bi}{Aa+Bb}\right)_4 (-1)^{\frac{A-1}{4}}$ et: $\left(\frac{M'}{m'}\right)_4 = \left(\frac{a-bi}{Aa+Bb}\right)_4 (-1)^{\frac{a-1}{4}}$. Donc:

$$\left(\frac{m}{M}\right)_4 \left(\frac{M'}{m'}\right)_4 = \left(\frac{(A+Bi)(a-bi)}{Aa+Bb}\right)_4 (-1)^{\frac{A-1}{4}+\frac{a-1}{4}}$$

$$= \left(\frac{Aa+Bb+i(aB-Ab)}{Aa+Bb}\right)_4 (-1)^{\frac{A+1}{4}+\frac{a-1}{4}}$$

$$\left(\frac{m}{M}\right)_4\left(\frac{M'}{m'}\right)_4 = (-1)^{\frac{Aa+Bb-1}{4}+\frac{A-1}{4}+\frac{a-1}{4}} \text{ d'après a) et b).}$$

$$\frac{Aa+Bb-1}{4}+\frac{A-1}{4}+\frac{a-1}{4} \equiv \frac{Aa+Bb-1}{4}-\frac{A-1}{4}-\frac{B-1}{4}$$

$$\equiv \frac{(A-1)(a-1)}{4}+\frac{Bb}{4} \equiv \frac{Bb}{4} \mod 2.$$

D'autre part $\frac{b}{2} \equiv \frac{b^2}{4} \equiv \frac{a^2-1+b^2}{4} \mod 2$ car b est pair, et a^2-1 est multiple de 8).

D'où $$\left(\frac{m}{M}\right)_4 = (-1)^{\frac{P-1}{4}\frac{p-1}{4}}\left(\frac{M}{m}\right)_4 . \qquad \text{C. Q. F. D.}$$

Conclusion

En utilisant la notion d'ensemble de birestes la démonstration de Gauss est la suivante:

Pour la loi de réciprocité quadratique on calcule l'ensemble de birestes V^2, puis V^{q-1}, puis V^q. On trouve, par le calcul des pages 131-132.

$$V^q = p^{\frac{q-1}{2}}((-1)^{\frac{q-1}{2}}, 0)\,V \qquad \mod (OS, FS) .$$

Le calcul direct de V^q donne:

D'une part les termes où on prend le même bireste dans les ensembles, soit, (q était impair):

$$\bigcup_x \left(\left(\frac{x}{p}\right)^q, qx\right) = \bigcup_x \left(\left(\frac{x}{p}\right), qx\right) = \left(\left(\frac{q}{p}\right), 0\right)V .$$

D'autre part les termes où tous les birestes pris ne sont pas les mêmes. Par permutation circulaire on obtient q combinaisons *distinctes* qui donnent le même bireste dans le résultat. Le raisonnement qui prouve que les q combinaisons sont distinctes est celui de la page 133. Donc:

$$p^{\frac{q-1}{2}}((-1)^{\frac{q-1}{2}}, 0)\,V = \left(\frac{q}{p}, 0\right)V \qquad \mod (OS, FS, q) .$$

De là, après avoir multiplié par V on déduit:

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

Pour démontrer la loi de réciprocité biquadratique le raisonnement est analogue. On calcule T^4, et $T\bar{T}$, puis $T^q\bar{T}$ ou T^{q+1} d'une part, et d'autre part $T^q \pmod q$ directement. On arrive ainsi aux formules (1) page 141 et (2) page 142. La fin

du raisonnement est la même.

Gauss présente ces démonstrations à l'aide de polynômes, et son raisonnement porte en fait sur les restes des polynômes modulo X^p-1. Cela est calculer dès le départ modulo les OS. On peut aussi présenter cette démonstration comme un calcul dans les corps $\boldsymbol{Q}(\sqrt[p]{1})$ ou $\boldsymbol{F}_q(\sqrt[p]{1})$. Cela est calculer dès le départ modulo les OS, FS, q.

Le calcul du nombre des solutions des congruences est présenté d'habitude à l'aide de sommes de Gauss.

Maison Franco-japonaise
Universités de Tokyo et de Nancy

Bibliographie

C.F. Gauss [1] Werke.
[2] Untersuchungen über höhere Arithmetik, Leipzig, 1889, Chelsea 1965.
G. Eisenstein [1] Lois de réciprocité, Journal de Crelle 28, page 53.
[2] Mathematische Abhandlungen, Aerlin, 1847, page 121.
C. L. Siegel, Werke, Springer, 1966.
A. Weil, Number of solutions of équations in finite fields, Bulletin of the American Mathematical Society 55, p. 497-508.
S. I. Borevitch et I. R. Shafarevitch, Théorie des nombres.
H. Hasse Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Physica-Verlag, Würzburg-Wien, 1965.

(Reçu le 1 mars 1969)