NOUVELLES ANNALES DE MATHÉMATIQUES

PAUL LAMBERT

Entiers imaginaires

Nouvelles annales de mathématiques 4^e série, tome 12 (1912), p. 408-421

<http://www.numdam.org/item?id=NAM_1912_4_12__408_1>

[15a]

ENTIERS IMAGINAIRES;

PAR M. PAUL LAMBERT,
Élève a l'Ecole Normale supérieure.

Gauss (1) a eu l'idée d'étendre aux imaginaires la notion de nombre entier. Un nombre complexe $a + bi$ sera entier si a et b sont tous deux entiers (positifs ou négatifs). Dans cette théorie, le module joue un rôle beaucoup moins important que son carré $a^2 + b^2$ qui est un entier réel et que Gauss appelle *norme*.

Dans la représentation géométrique classique, aux entiers imaginaires correspondront les sommets d'un quadrillage formé par les parallèles aux axes, dont les abscisses (ou les ordonnées) sont des entiers.

La somme, le produit de deux entiers imaginaires est aussi un entier. Il importe d'ailleurs de remarquer qu'en général une puissance entière complexe d'un nombre entier ne sera pas entière. Par exemple, si a est un nombre réel, on a

$$a^i = e^{i \operatorname{Log} a} = \cos(\operatorname{Log} a) + i \sin(\operatorname{Log} a)$$

et $\cos(\log a)$ et $\sin(\log a)$ ne sont pas entiers en général.

Pour obtenir les points correspondants aux mul-

(1) GAUSS, *Theoria residuorum biquadraticorum.*

tiples (entiers et complexes) d'une imaginaire z, il suffit évidemment de prendre l'homothétique du quadrillage primitif par rapport à l'origine dans le rapport $|z|$ puis de le faire tourner autour de O d'un angle égal à l'argument de z.

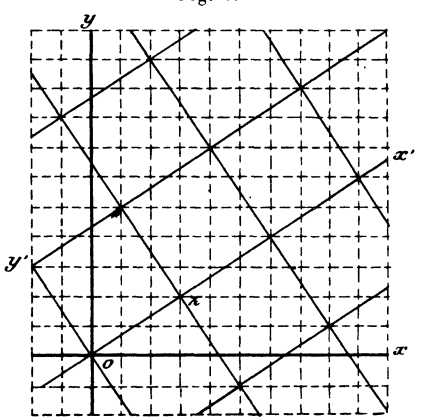
Le point (1,0) viendra au point z. Les équations cartésiennes des droites obtenues, en posant $z = a + bi$, seront

$$ax + by = k|z| \quad \text{et} \quad bx - ay = k'|z|$$

k et k' étant des entiers réels de signe quelconque.

On généralise de même la théorie de la division. Ici

Fig. 1.



il faut définir un reste. Soit $a + bi$ à diviser par $c + di$ et $x + yi$ le quotient entier. On devra avoir

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i$$

$$= (x+yi) + \left(\frac{ac+bd}{c^2+d^2} - x\right) + \left(\frac{bc-ad}{c^2+d^2} - y\right)i.$$

Posons

$$\frac{ac+bd}{c^2+d^2} - x = u \qquad \text{et} \qquad \frac{bc-ad}{c^2+d^2} - y = v.$$

Nous pouvons toujours déterminer les entiers réels x et y tels que $|u| \leq \frac{1}{2}$ et $|v| \leq \frac{1}{2}$. Or le reste de la division est ([illegible]) $(u + vi)$ puisque l'identité qui exprime la division peut s'écrire

$$a + bi = (x + yi)(c + di) + (u + vi)(c + di).$$

Le module du reste sera égal au module du diviseur $c + di$ multiplié par $\sqrt{u^2 + v^2}$, quantité au plus égale à $\frac{1}{\sqrt{2}}$. Donc le module du reste ainsi défini est inférieur au module du diviseur. Cette condition peut d'ailleurs être réalisée pour deux ou même quatre valeurs du système (x, y), au cas où les inégalités qui déterminent u et v se transformeraient en égalités. Géométriquement, si la division ne se fait pas exactement, le point $A(a, b)$ tombe à l'intérieur d'un carré du grand quadrillage formé par les multiples de $c + di$. Notre condition revient à prendre pour point représentatif du quotient le sommet de ce carré le plus rapproché de A. Il y aura indétermination si le point A est équidistant de deux ou même quatre sommets. Dans ce cas, il faudra faire une convention : prendre, par exemple, parmi les sommets possibles le plus rapproché de l'origine. Cela se peut toujours : deux sommets consécutifs ne peuvent être équidistants de O sans que la perpendiculaire au milieu du côté qu'ils déterminent soit un axe ox' ou oy', ce qui est *absurde; si deux sommets opposés sont équidistants de* O, des deux sommets restants, l'un en est *évidemment plus rapproché*, et c'est *celui-là qu'on* prendra.

On peut achever comme pour les nombres réels la théorie élémentaire des entiers imaginaires, théorie

qu'esquisse M. Cahen dans une Note à la fin de son Ouvrage sur la *Théorie des Nombres;* et c'est de cette théorie que je vais essayer de tirer quelques conséquences. Un fait important pour la divisibilité est que nous devrons considérer quatre unités différentes : $+1$, -1, $+i$, $-i$. A ce point de vue nous considérerons comme identiques quatre nombres tels que $a+bi$, $a-bi$, $-b+ai$, $b-ai$. Nous pourrions démontrer ainsi sur les entiers complexes tous les théorèmes qu'on démontre pour les entiers réels, en particulier le théorème suivant, dont nous aurons à nous servir : *un entier complexe n'est décomposable que d'une seule manière en facteurs premiers.*

Remarques. — 1° Quand une imaginaire admet certains diviseurs, sa conjuguée admet les diviseurs conjugués. Si elle est première, sa conjuguée l'est aussi.

2° Quand une imaginaire $a+bi$ n'admet pas de diviseur réel, a et b sont premiers entre eux, et réciproquement.

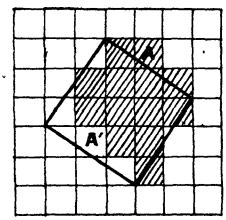
3° Un nombre premier réel peut ne pas être premier au sens imaginaire. Dans ce cas, il est la somme de deux carrés, donc de la forme $4h+1$. Exemple :

$$13=(2+3i)(2-3i).$$

4° La divisibilité la plus fréquente est la divisibilité par $1+i$. Si $a+bi$ est divisible par $1+i$, a et b sont de même parité. En effet, soit $c+di$ le quotient de $a+bi$ par $1+i$. On a $a=c-d$ et $b=c+d$, et l'on voit que $a-b$ est un multiple de 2. Nous pouvons comme Gauss appeler de tels nombres *semi-pairs* en réservant le nom de *pairs* pour ceux où a et b sont pairs séparément.

Système de restes incongrus. — La congruence étant définie comme pour les nombres réels, je reviens au quadrillage dont les sommets représentent les multiples d'un entier complexe $a + bi$; j'en considère un carré quelconque C que je déplace par une translation arbitraire. Parmi les points représentant *tous* les entiers imaginaires, j'isole l'ensemble de ceux qui tombent soit à l'intérieur de C soit sur un certain de ses quatre sommets (je me suis fixé arbitrairement l'un des quatre), soit sur les deux côtés qui y aboutissent (extrémités opposées non comprises). Je dis que ces points correspondent à un système de restes incongrus par rapport à $a + bi$. En effet, deux des nombres obtenus ne peuvent être congrus sans être, soit deux sommets du carré, et je n'en ai pris qu'un, soit sur deux côtés opposés, et je n'ai pris que deux sommets consécutifs. D'autre part, à tout entier complexe z est congru un nombre de ce système, car si je fais subir à tout le quadrillage des multiples de $a + bi$ la même translation qu'à C, le point correspondant à z tombe dans un autre carré C′ et je n'aurai qu'à prendre dans mon système le point semblablement placé dans C. En particulier, dans ce système de restes incongrus se trouve un et un seul multiple de $a + bi$.

Fig. 2.



Cela posé, je dis que ce système comprend $a^2 + b^2$ nombres. En effet, à chacun de ces points j'adjoins le

carré de côté 1 qui se trouve par exemple en haut et à droite. (Ce sont les carrés couverts de hachures sur la figure. Le sommet particulier de C que j'ai choisi est celui du bas.) L'aire de l'ensemble de ces petits carrés est égale à l'aire du grand, car ce qu'il y a en trop au bord en A, par exemple, manque au bord opposé en A' : il suffit pour le voir d'amener par translation l'un des côtés sur le côté opposé. L'aire du grand carré étant $a^2 + b^2$, il y aura $a^2 + b^2$ petits carrés, donc $a^2 + b^2$ restes incongrus.

RELATIONS ENTRE LES ENTIERS IMAGINAIRES ET LEURS NORMES.

Je dirai, pour abréger, qu'une norme est première quand elle l'est en tant que nombre réel, comme 13, par exemple. Comme une norme n'est jamais première en tant qu'imaginaire, il ne saurait y avoir de confusion.

THÉORÈME I. — *Quand un entier imaginaire n'est pas premier, sa norme n'est pas première.* Ce fait est évident.

THÉORÈME II. — *Quand un entier imaginaire est premier, sa norme est première.* Dans cette hypothèse, en effet, l'égalité

$$a^2 + b^2 = (a + bi)(a - bi)$$

représente la décomposition de $a^2 + b^2$ en facteurs premiers. Cette décomposition n'étant possible que d'une seule manière, $a^2 + b^2$ n'admet pas d'autre diviseur, en particulier pas de diviseur réel.

Cela suppose essentiellement a et b tous deux différents de zéro.

De ces deux théorèmes je peux conclure aux réciproques.

Si les deux termes d'un entier complexe sont différents de zéro :

I. *Il est premier si sa norme est première;*

II. *Il n'est pas premier si sa norme ne l'est pas.*

Quand l'un des deux termes est nul, l'imaginaire se confond, à une de nos quatre unités près, avec son module, d'où les trois cas suivants :

a. Le module n'est pas premier (en tant que nombre réel) } l'imaginaire n'est pas première.

b. Le module est premier { et somme de deux carrés } l'imaginaire n'est pas première.
{ et n'est pas somme de deux carrés } l'imaginaire est première.

Cette correspondance réciproque entre les entiers complexes et leurs normes peut servir, par exemple, dans la recherche du plus grand commun diviseur ou du plus petit commun multiple puisqu'on peut ramener ce problème au problème correspondant sur des nombres réels.

APPLICATIONS DE LA THÉORIE ÉLÉMENTAIRE DES ENTIERS IMAGINAIRES.

La théorie précédente permet de simplifier certaines démonstrations d'Arithmétique concernant les nombres réels. On démontre facilement, par exemple, que le produit de deux sommes de deux carrés est aussi une somme de deux carrés; mais la réciproque offre plus de difficulté.

M. Borel (1) a démontré que :

Si un nombre premier divise la somme de deux

(1) Borel et Drach, *Introduction à la Théorie des Nombres et a l'Algèbre superieure*, p. 105.

carrés sans les diviser tous deux, il est lui-même la somme de deux carrés, ou, ce qui revient au même, *si un nombre divise la somme de deux carrés premiers entre eux, il est lui-même la somme de deux carrés.*

La même démonstration s'applique d'ailleurs au cas de quatre carrés. La voici en quelques mots :

p divise a^2+b^2. Je suppose $p>2$. Soient a' et b' les résidus minima absolus de a et b par rapport à p, c'est-à-dire deux nombres compris entre $-\frac{p}{2}$ et $\frac{p}{2}$ et congrus respectivement à a et à $b \pmod p$. J'ai

$$(1) \qquad a'^2+b'^2 \leqq 2\left(\frac{p}{2}\right)^2 \qquad \text{ou} \qquad a'^2+b'^2=pp',$$

p' étant un entier inférieur à p. Si $p'=1$, le théorème est démontré. Sinon, soient $a'-\alpha p'$ et $b'-\beta p'$ les résidus minima absolus de a' et β' par rapport à p'. J'aurai de la même façon

$$(2) \quad (a'-\alpha p')^2+(b'-\beta p')^2=p'p'' \qquad \text{avec} \qquad p''<p'<p.$$

En multipliant (1) et (2) membre à membre, il vient

$$A^2+B^2=pp'^2p'',$$

A et B contenant p' en facteur, je pose $A=p'a''$, $B=p'b''$, donc

$$(3) \qquad a''^2+b''^2=pp''.$$

Si $p''\neq 1$ je recommence. Les multiplicateurs successifs de p sont des entiers qui décroissent constamment. L'un d'eux finira par être égal à 1 et l'égalité correspondante exprimera p comme somme de deux carrés.

On peut démontrer ce théorème plus simplement

par l'intermédiaire des entiers imaginaires. Je suppose qu'un entier p divise $a^2 + b^2$, et que p, a, b sont premiers entre eux dans leur ensemble. Dans ces conditions p est une somme de deux carrés. En effet, je décompose $a + bi$ en facteurs premiers imaginaires :

$$(1) \qquad a + bi = (c + di)\dots(e + fi).g\dots h.ki\dots li,$$

g, h, k, l sont les diviseurs communs à a et à b.

L'égalité correspondante entre les normes est

$$(2) \qquad a^2 + b^2 = (c^2 + d^2)\dots(e^2 + f^2)g^2\dots h^2k^2\dots l^2$$

et elle exprime la décomposition de $a^2 + b^2$ en facteurs premiers réels, d'après la correspondance établie plus haut. Or comme p ne contient par hypothèse aucun des facteurs $g\dots h$, $k\dots l$, il se réduit à un produit de sommes du genre de $(c^2 + d^2)$, donc à une somme de deux carrés.

L'égalité (2) montre en même temps que *les diviseurs premiers d'une somme de deux carrés sont soit des sommes de deux carrés, soit des nombres quelconques, mais affectés alors d'un exposant pair.*

Remarque. — Le produit de deux sommes de deux carrés $c^2 + d^2$ et $e^2 + f^2$ étant une somme de deux carrés $a^2 + b^2$, si c et d sont premiers entre eux ainsi que e et f, on peut affirmer que a et b sont aussi premiers entre eux; car l'une des quatre égalités suivantes

$$(3) \qquad a + bi = (c \pm di)(e \pm fi)$$

est vraie et montre que si $c \pm di$ et $e \pm fi$ n'admetteut pas de diviseur réel (ce qui équivaut à avoir ses termes premiers entre eux), $a + bi$ ne peut en admettre.

Réciproquement, si a et b sont premiers entre eux,

les facteurs premiers que j'ai appelés $g \dots h$, $k \dots l$ n'existent pas; les imaginaires $(c + di) \dots (e + fi)$ de l'égalité (1) n'admettent pas de diviseur réel; donc p, qui est le produit de certaines de ces imaginaires, est, d'après la première partie de cette remarque, la somme de deux carrés premiers entre eux.

Application à la détermination des systèmes d'entiers réels x, y, z tels qu'on ait

$$x^2 + y^2 = z^2.$$

On peut toujours supposer x et y premiers entre eux. Donc z qui divise $x^2 + y^2$ est aussi une somme de deux carrés premiers entre eux. Réciproquement, dans ce cas, z^2 est bien de la forme $x^2 + y^2$. Cela posé, connaissant z, on déterminera tous les systèmes correspondants de x et de y en se basant sur l'égalité

$$(x + yi)(x - yi) = z^2.$$

Or $x + yi$ est un carré parfait, car si un facteur premier $u + vi$ y figurait avec un exposant impair m, $u^2 + v^2$ serait un facteur de z^2, premier en tant que nombre réel, et y figurerait avec un exposant impair, ce qui est impossible ($x - yi$ ne peut contenir de son côté le facteur $u + vi$, sinon $x + yi$ serait divisible par $u - vi$ et admettrait par suite un diviseur réel $u^2 + v^2$). Donc

$$x + yi = (s + ti)^2 \qquad \text{et} \qquad z = (s + ti)(s - ti).$$

On aura donc tous les systèmes de nombres s et t en décomposant z en ses $2n$ facteurs premiers imaginaires conjugués deux à deux et en combinant de toutes les façons possibles n de ces facteurs, en ayant soin que les n facteurs restants soient bien les conjugués de ceux qu'on aura pris.

Exemples. — Cherchons à retrouver quelques systèmes de nombres x, y, z. Prenons d'abord $z = 5 = 2^2 + 1^2$. Ici $s + ti = 2 + i$; $x + yi = (s + ti)^2 = 3 + 4i$, d'où le système $3^2 + 4^2 = 5^2$.

Soient encore : $z = 13 = 3^2 + 2^2$; $s + ti = 3 + 2i$; $x + yi = (3 + 2i)^2 = 5 + 12i$:

$$13^2 = 12^2 + 5^2.$$

Continuons :

$$z = 17 = 4^2 + 1^2; \quad s + ti = 4 + i; \quad x + yi = (4 + i)^2 = 15 + 8i:$$
$$17^2 = 15^2 + 8^2,$$

et ainsi de suite. Pour compléter, il faut multiplier tous ces systèmes par des carrés parfaits.

Les théorèmes de Fermat, d'Euler et de Wilson s'étendent aussi au cas des entiers complexes. On trouve l'indicateur (c'est-à-dire le nombre des restes d'un système incongru qui sont premiers avec le module) en employant le procédé dont je me suis servi pour compter le nombre de restes incongrus. L'indicateur d'un nombre $a + bi$ dont les diviseurs sont de la forme $p + qi$, sera

$$N = (a^2 + b^2) \prod \left(1 - \frac{1}{p^2 + q^2}\right).$$

Théorème de Fermat. — Soient $a + bi$ et $q + ri$ deux entiers complexes, $q + ri$ étant premier et ne divisant pas $a + bi$. Le nombre des restes d'un système incongru par rapport à $q + ri$, le multiple du module mis à part, est $q^2 + r^2 - 1$. Le théorème de Fermat s'exprimera donc par la congruence

$$(a + bi)^{q^2 + r^2 - 1} - 1 \equiv 0 \pmod{q + ri}.$$

Si $q - ri$ ne divise pas non plus $a + bi$, le premier membre de la congruence se trouve aussi divisible

par $q - ri$, donc par $q^2 + r^2$:

$$(a + bi)^{q^2+r^2-1} - 1 \equiv 0 \qquad (\mathrm{mod}\, q^2 + r^2).$$

Le théorème de Fermat est donc vrai, non pas seulement d'un module p premier comme nombre complexe, mais encore quand p n'est premier que comme nombre réel (c'est-à-dire admet deux diviseurs conjugués premiers).

Application — I. Prenons

$$a + bi = \sqrt{2}\left(\cos\frac{\pi}{4} + i + \sin\frac{\pi}{4}\right) = 1 + i;$$

et pour $q + ri$ un entier imaginaire premier ne divisant pas $1 + i$, donc tel qu'on n'ait pas à la fois $q = \pm 1$, $r = \pm 1$. On démontre dans la *Théorie des nombres* que $p = q^2 + r^2$, nombre réel impair, doit être de la forme $4h + 1$. Le théorème devient

$$2^{2h}(\cos h\pi + i \sin h\pi) - 1 \equiv 0 \qquad (\mathrm{mod}\, p)$$

ou

$$2^{2h} \equiv (-1)^h,$$

h étant le quotient de la division de p par 4.

II. Prenons toujours $a + bi = 1 + i$, et pour module un nombre réel p premier en tant qu'imaginaire. p n'est pas une somme de deux carrés : alors il est de la forme $4h + 3$. Le théorème sera alors

$$(1 + i)^{16h^2+24h+8} - 1 \equiv 0 \qquad (\mathrm{mod}\, p).$$

Posons $16h^2 + 24h + 8 = 8m$:

$$2^{4m}(\cos 2m\pi + i \sin 2m\pi) = 2^{4m} \equiv 1 \qquad (\mathrm{mod}\, p),$$

$4m$ étant le quotient de la division de p^2 par 2.

Si p est de la forme $4h + 1$, on pose $16h^2 + 8h = 8m$, le résultat est le même.

Nous aurons finalement ce théorème pour les nombres réels :

Soit p un nombre premier. Si p est une somme de deux carrés et si j'appelle h le quotient de la division de p par $4, 2^{2h}$ *est congru à* $(-1)^h, (\mathrm{mod}\, p)$. *Si p n'est pas une somme de deux carrés et si j'appelle k le quotient de la division de* p^2 *par* 2, 2^k *est congru à* $1\ (\mathrm{mod}\, p)$.

Exemples. — I. Prenons par exemple $p = 4^2 + 1^2 = 17$. Ici $h = 4$; 2^8 ou 256 doit être congru à $1\ (\mathrm{mod}\, 17)$. Or $255 = 17 \times 15$.

Soit encore

$$p = 5^2 + 2^2 = 29.$$

Ici $h = 7$; 2^{14} ou 16.384 doit être congru à $-1\ (\mathrm{mod}\, 29)$. Or

$$16385 = 29 \times 565.$$

II. Soit $p = 7$; on a

$$k = 24 \qquad \text{et} \qquad 2^k = 2^{24} = 16777216.$$

On a bien

$$16777215 = 7 \times 2396745.$$

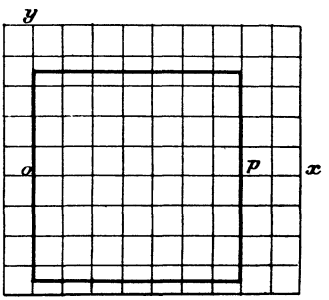
Théorème de Wilson. — Il s'énonce ainsi : le produit de tous les nombres d'un système incongru par rapport à un module premier p (les multiples du module mis à part) est congru à $-1\ (\mathrm{mod}\, p)$.

Application. — Je considère un entier réel positif p, premier en tant qu'imaginaire, et je cherche le système de restes incongrus contenus dans un carré de côtés parallèles aux axes et dont l'origine et le point représentatif de p occupent les milieux de deux côtés opposés. Un tel système est formé :

1° Des $p - 1$ points situés sur ox;

2° De tous les points situés à l'intérieur du carré et sur oy, à part le point o. Ces points sont deux à deux

Fig. 3



symétriques par rapport à ox. Les produits des imaginaires correspondantes sont des sommes de deux carrés. D'où le théorème :

Soit p un nombre premier non somme de deux carrés. Le produit par $(p-1)!$ *de toutes les sommes obtenues en ajoutant le carré d'un nombre inférieur à p au carré d'un nombre inférieur à* $\frac{p}{2}$ *est congru à* $-1 \pmod{p}$.

Dans ce produit, il faut évidemment laisser de côté la somme $o^2 + o^2$.