EVPHKA! num = Δ + Δ + Δ

Marc Guinot

(première partie)

C'est par cette exclamation passablement énigmatique que Gauss exprima dans son Journal, à la date du 10 juillet 1796, sa satisfaction d'être parvenu à démontrer rigoureusement que, comme l'avait prétendu Fermat quelques 158 ans plus tôt, tout entier naturel est une somme de trois nombres triangulaires, c'est à dire de trois nombres de la forme $\frac{k(k+1)}{2}$. A cette date, Gauss n'avait que dix-neuf ans.

En fait, le problème posé par Fermat était plus général : dans sa correspondance, il affirmait en effet que tout entier est non seulement une somme de trois "triangles", mais aussi une somme de quatre carrés, une somme de cinq nombres "pentagonaux", et ainsi de suite.

On sait que le problème relatif aux quatre carrés fut résolu par Lagrange en 1772, mais qu'il fut puissamment aidé en cela par Euler qui avait découvert, dès 1748, l'identité qui porte son nom et selon laquelle le produit de deux sommes de quatre carrés est une somme du même genre. Pour plus de détails sur toute cette histoire, on pourra consulter le livre d'André Weil (cité [WEI] dans toute la suite), *Number Theory, An approach through history*, Birkhäuser, 1984 et dont on ne verra sans doute jamais de traduction française. Il est à noter, à ce propos, que les Allemands, se jugeant sans doute trop nuls en anglais, ont traduit le livre de Weil dans leur dialecte. Mais, c'est bien connu, les Français ont le don des langues!

Comme on le verra à la fin de cette étude, l'assertion de Fermat concernant les nombres triangulaires peut être tirée du fait que tout nombre entier naturel de la forme $8n+3$ est une somme de trois carrés. On attribue généralement à Legendre le mérite d'avoir le premier caractérisé les entiers susceptibles de se décomposer en trois carrés, mais dans ses raisonnements Legendre n'hésitait pas à mélanger allègrement les résultats dûment démontrés et ceux qu'il avait obtenus par "induction", c'est à dire pas de simples vérifications numériques et c'est à juste titre, semble-t-il (cf [WEI, p.331, 332), que Gauss dénonça les prétentions de Legendre à avoir donné une démonstration satisfaisante.

Gauss exposa le résultat de ses travaux dans ses célèbres *Disquisitiones Arithmeticae* (Recherches arithmétiques), publiées en 1801, mais il faut beaucoup de bonne volonté pour comprendre entièrement sa démarche, même en se référant à la traduction française (citée [GAU] dans toute la suite) de son ouvrage, écrit et publié en latin.

Ayant travaillé de longues heures sur ce sujet (sacrifiant au passage mes maigres vacances) et aidé en sous-main par quelques auteurs plus modernes, je suis parvenu à la conviction que tant qu'on se limite aux entiers de la forme 8n+3 (les seuls dont on a réellement besoin pour les nombres triangulaires), on peut exposer aux lecteurs de *l'Ouvert* la démonstration complète du résultat qui nous intéresse ici. Mais pour cela, il nous faudra :

A/ répartir les "formes quadratiques binaires" en classes d'équivalence.
B/ définir et dénombrer les classes "primitives" en "ambiguës".
C/ apprendre à multiplier les classes entre elles, de façon à avoir un groupe.
D/ regrouper les classes en "genres" en fonction de leurs "caractères".
E/ donner un minimum d'information sur les formes quadratiques "ternaires".
F/ appliquer tous ces résultats aux sommes de trois carrés.

Les points A/, B/ et C/ seront traités dans le présent numéro, les points D/ E/ et F/ dans le suivant. En principe, aucune connaissance préalable d'arithmétique supérieure n'est requise pour aborder tous ces points, à l'exception des propriétés "bien connues" des résidus quadratiques sur lesquelles (que le lecteur se rassure!) nous donnerons cependant toutes les précisions utiles. Certains calculs et certaines parties élémentaires du raisonnement ne seront qu'esquissés. Le lecteur en détresse peut toujours nous écrire...

Evidemment, au lieu de se farcir un pareil programme, on peut préférer écouter, en se pâmant, l'ineffable voix de Léopold Simoneau[1]. Mais quand on a choisi de lire *l'Ouvert*, on doit s'attendre à tomber sur des mathématiques, non? Ou alors, on s'abonne à *Diapason* ou à *l'Avant Scène Opéra*.

A/ Formes et classes de formes.

1. La théorie des "formes quadratiques binaires" (qui va occuper l'essentiel de cette étude) n'est pas sortie brutalement du cerveau du jeune Gauss dans les dernières années du XVIII^{e} siècle. Au siècle précédent, les recherches de Fermat sur les sommes de deux carrés, puis sur les nombres de la forme x^2+2y^2 ou x^2+3y^2, avaient conduit celui-ci à de substantiels résultats qui furent démontrés, non sans mal, par Euler entre 1752 et 1772 (cf [WEI], p.179 et p.212). Ce dernier avait commencé à étendre ses réflexions à des cas plus généraux, comme les nombres de la forme $\lambda x^2+\mu y^2$ ou même, une fois au moins, aux nombres de la forme x^2+xy+y^2. Mais c'est Lagrange qui a le premier entrepris d'étudier le cas général des expressions de la forme $ax^2+bxy+cy^2+2$, l'idée principale de ses *Recherches arithmétiques* (publiées en 1775) étant qu'on ne change pas les nombres qui sont de la forme $ax^2+bxy+cy^2$ quand on fait un changement de variables du type $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$ avec des entiers α, β, γ, δ soumis à la condition $\alpha\delta-\beta\gamma=\pm 1$, condition qui garantit la "réversibilité" du changement de variables puisqu'on a alors

[1] Je profite de l'occasion pour dire que le grand spécialiste de ce grand ténor canadien habite Strasbourg. Pour tous renseignements complémentaires, écrire à l'IREM de Strasbourg qui transmettra.

x'=±(δx-βy) et y'=±(-γx+αy). C'est cette idée, légèrement modifiée par Gauss, que nous allons exposer ici.

2. Il y a plusieurs façons de définir, formellement parlant, une *forme quadratique binaire* (à coefficients entiers). Pour nous, ce sera simplement une application f de $\mathbb{Z}^2$ dans $\mathbb{Z}$ pour laquelle il existe des entiers a, b, c tels que $f(x,y)=ax^2+bxy+cy^2$ quels que soient $x,y\in\mathbb{Z}$. Les entiers a, b et c sont évidemment entièrement déterminés par f puisqu'on a les relations a=f(1,0), c=f(0,1), b=f(1,1)-a-c. On peut donc parler sans ambiguïtés des *coefficients* d'une forme f et même distinguer le *coefficient initial* a, le *coefficient final* c et le *coefficient médian* b.
Se donner une forme quadratique binaire f, à coefficients entiers, revient donc à se donner la suite (a,b,c) de ses coefficients, ce qui nous permettra d'écrire, sans trop de scrupules, à la manière de Gauss d'ailleurs f=(a,b,c).
Comme nous n'avons pas à envisager, sauf exception, d'autres formes que celles que nous venons de définir, nous nous permettrons d'omettre, assez souvent l'un ou l'autre des qualificatifs de "quadratique" ou de "binaire" qui font pourtant tout le charme des formes en question. L'exception est celui des formes ternaires qu'on verra dans le paragraphe D ; il sera bien temps de modifier notre langage à ce moment là.

3. Il résulte de ce qui précède qu'il ne faut pas confondre *a priori* la forme (a,b,c) et la forme (c,b,a). nous verrons plus loin l'importance de cette distinction et nous dirons dès maintenant que ces formes sont *inverses* l'une de l'autre (Gauss, de façon moins suggestive préférait parler de formes "associées"). Il ne faut pas confondre non plus, bien sûr, (a,b,c) et (-a,-b,-c). Nous dirons que ce sont des formes *opposées* (alors que Gauss préférait user de ce qualificatif pour les formes (a,b,c) et ... (a,-b,c)).
Puisque nous en sommes à critiquer Gauss, signalons que celui-ci voulait limiter l'étude des formes binaires à celles dont le coefficient médian b est pair. Pour mieux embrouiller ses lecteurs, il va jusqu'à noter (a,b,c) ce qu'on note ici (a,2b,c)! Curieusement, pour démontrer le théorème de Gauss sur les nombres triangulaires, nous n'aurons réellement besoin que des formes (a,b,c) où b est impair. Nous qualifierons ces dernières de *formes impaires* et nous parlerons de *formes paires* pour signifier que le coefficient médian b est un entier pair. Pour nous rattraper, il nous arrivera de parler, dans ce dernier cas, de *formes de Gauss*...
Parmi les formes paires, il y a (1,0,1) (qui "représente" les sommes de deux carrés) et la *forme nulle* (0,0,0) qui a surtout le mérite (ou l'inconvénient) d'exister.
On dira enfin qu'une forme quadratique binaire est *primitive* si ses coefficients sont premiers dans leur ensemble. En un sens facile à comprendre, toute forme non nulle "dérive" d'une forme primitive. De façon plus précise, on obtient cette dernière en mettant en facteur le PGCD des coefficients (a,b,c) de la forme initiale, qu'on appellera en abrégé le *PGCD* de la forme.

4. Le problème principal de la théorie est de savoir, pour une forme f=(a,b,c) donnée, quels sont les entiers qui sont "de cette forme", c'est à dire qui peuvent s'écrire $ax^2+bxy+cy^2$ avec des entiers x et y, puis, cela étant, de déterminer de combien de façons une telle écriture est possible. Dans le cas des sommes de deux carrés (c'est à dire dans le

cas de la forme (1,0,1)), on peut dire que le problème a été résolu par Fermat, en tenant compte du fait que les premières démonstrations connues sont dues à Euler (cf [WEI], p.178). Si j'ai bien compris ce que j'ai lu, ici et là, (cf par exemple [DIE], p.183) le problème général, c'est à dire le cas d'une forme (a,b,c) quelconque, n'est pas tout à fait réglé. Cela ne doit pas nous empêcher de fixer le vocabulaire avec toute la précision désirable. Nous dirons donc qu'un entier n est *représenté* par une forme f=(a,b,c) donnée (ou que f *représente* n) si n est de la forme $ax^2+bxy+cy^2$ (on notera le jeu de mot!) c'est à dire s'il existe deux entiers x et y tels que n=f(x,y). Tout couple (x,y) ayant cette propriété sera appelé une *représentation* de n par f.
Le nombre 0 est naturellement représenté par n'importe quelle forme ; les égalités x=0, y=0 en fournissent une représentation particulière, dite *triviale*. Certains auteurs excluent, dans le cas de 0, cette représentation là. Comme nous n'aurons pas besoin de faire cette restriction ici, on peut dire qu'en général les entiers représentés par f ne sont rien d'autres que les valeurs de f, f étant conçue, comme on l'a dit, comme une fonction sur $\mathbb{Z}^2$, à valeurs dans $\mathbb{Z}$.
Si la forme est nulle, seul le nombre 0 est représenté. Si f n'est pas nulle, au contraire, il existe une infinité d'entiers représentés par f, à savoir les nombres ax^2 si $a\neq 0$, les nombres cy^2 si $c\neq 0$ et les nombres bxy si a et c sont nuls simultanément.
Il peut être commode de dire enfin qu'une représentation (x,y) d'un entier n par une forme f est *propre* si x et y sont premiers entre eux. Un entier n qui admet au moins une représentation propre sera dit *proprement représenté* par f. Si (x,y) est une représentation quelconque de n par une forme f et si d est le PGCD de x et de y, alors d^2 divise n et le couple $\left(\frac{x}{d}, \frac{y}{d}\right)$ est une représentation propre de $\frac{n}{d^2}$ par f. Cela résulte immédiatement des définitions.

5. Les questions précédentes sont liées à la valeur de la quantité $\Delta=b^2-4ac$ que l'on peut associer à une forme f=(a,b,c). On dira évidemment que c'est le *discriminant* de la forme quadratique f. A cause des relations $4af(x,y)=(2ax+by)^2-\Delta y^2$ et $4cf(x,y)=(2cy+bx)^2-\Delta x^2$, on a trois grands cas à distinguer.
Si $\Delta=0$, la forme peut être transformée, au moyen d'une multiplication par un entier non nul, en le carré d'une "forme linéaire" mx+ny.
Si $\Delta<0$ (cas où on dira que la forme est *définie*), il est impossible que les coefficients extrèmes a et c soient nuls et ils sont nécessairement de même signe. On voit en outre aussitôt (à cause des relations ci-dessus) que ce signe commun est celui de tous les nombres f(x,y), le cas où f(x,y)=0 ne se produisant que si x=y=0. Il y a donc deux catégories de formes définies : les formes définies *positives* qui, en dehors de 0, ne représentent que des nombres >0 et les formes définies *négatives* qui ont la propriété contraire.
Enfin si $\Delta>0$ (cas où l'on dit que la forme est *indéfinie*), la forme représente une infinité d'entiers >0 et une infinité d'entiers <0. Comme $f(ux,uy)=u^2f(x,y)$, il suffit de démontrer que, dans ce cas, f représente au moins un entier >0 et au moins un entier <0. Ce résultat est évident si a=c=0 car alors f(x,y)=bxy avec $b\neq 0$. Si $a\neq 0$, on a $4af(x,y)=(2ax+by)^2-$

$\Delta y^2=4a^2>0$ si x=1 et y=0 et $4af(x,y)=(2ax+by)^2-\Delta y^2=-4a^2\Delta<0$ si x=-b et y =2a. On raisonne de même si $c\neq 0$.
Notons pour finir que les formes paires (respectivement impaires) dont nous avons parlé dans le n°3 ne sont rien d'autres que les formes de discriminant pair (respectivement impair) : la terminologie est donc on ne peut plus judicieuse!

6. Comme nous l'avons dit plus haut, c'est Lagrange qui a eu l'idée d'introduire les formes quadratiques les plus générales, sans doute en faisant la constatation que si on part d'une forme quadratique f(x,y) même aussi simple que x^2+y^2 ou x^2+2y^2, le remplacement de x et de y par des expressions du type $\alpha x+\beta y$ et $\gamma x+\delta y$ conduit à une forme g(x,y) a priori arbitraire. Si on part en fait d'une forme $f(x,y)=ax^2+bxy+cy^2$ quelconque, un calcul direct (laissé au lecteur) montre que les coefficients u, v, w de $g(x,y)=f(\alpha x+\beta y,\gamma x+\delta y)$ sont donnés par les relations

$$(1)\qquad \begin{cases} u=a\alpha^2+b\alpha\gamma+c\gamma^2=f(\alpha,\gamma) \\ v=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta \\ w=a\beta^2+b\beta\delta+c\delta^2=f(\beta,\delta) \end{cases}$$

Si on appelle τ l'application de $\mathbb{Z}^2$ dans lui-même : $(x,y)\to(\alpha x+\beta y,\gamma x+\delta y)$ (où $\alpha,\beta,\gamma,\delta$ sont supposés entiers), on voit que le "changement de variables" que l'on vient d'effectuer revient à composer τ : $\mathbb{Z}^2\to\mathbb{Z}^2$ et f : $\mathbb{Z}^2\to\mathbb{Z}$, donc à poser $g=f\circ\tau$. On exprimera cette dernière relation en disant que τ *transforme* f en g ou que τ *fait passer* de la forme f à la forme g. Si $f\circ\tau=f$, on dira aussi que f est *invariante* par τ.

7. Il est facile de voir que d'une manière générale, toute application τ de $\mathbb{Z}^2$ dans lui-même du type $(x,y)\to(\alpha x+\beta y,\gamma x+\delta y)$ (où $\alpha,\beta,\gamma,\delta$ sont des entiers) se prolonge d'une manière et d'une seule en une application $\overline{\tau}$ de $\mathbb{R}^2$ dans lui-même, qui est linéaire au sens des espaces vectoriels (ici sur $\mathbb{R}$).
Pour éviter des circonlocutions pénibles, on dira que l'application τ elle-même est *linéaire* (de $\mathbb{Z}^2$ dans lui-même) ou que c'est une *transformation linéaire* de $\mathbb{Z}^2$ et on attribuera à τ des propriétés qui, en fait, sont des propriétés de $\overline{\tau}$. C'est ainsi que la matrice $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ de $\overline{\tau}$ et son déterminant $\alpha\delta-\beta\gamma$ seront appelés respectivement la *matrice* et le *déterminant* de τ. Avec ces définitions, il est clair que si τ et τ' sont des transformations linéaires de $\mathbb{Z}^2$, il en est de même de la transformation composée $\tau'\circ\tau$, la matrice et le déterminant de cette dernière s'obtenant alors, de façon évidente, par multiplication.
Dans la pratique, il nous arrivera souvent d'identifier une transformation linéaire τ de $\mathbb{Z}^2$ avec sa matrice (au moins lorsqu'il s'agira de définir τ et donc d'écrire (abusivement)

$$\tau=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}.$$

8. Il est possible de donner aux relations (1) ci-dessus une forme plus maniable, en termes de matrices, à condition de dédoubler le terme *"rectangle"* bxy de f(x,y) et de représenter l'expression générale obtenue $ax^2 + \frac{1}{2}bxy + \frac{1}{2}byx + cy^2$ par la matrice symétrique $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ que l'on appellera la *matrice de la forme quadratique* f.

Si on considère un couple (x,y) d'entiers quelconques comme une matrice colonne et la matrice transposée comme une matrice ligne, on vérifie aussitôt que l'on a

$$(2) \qquad ax^2+bxy+cy^2=(x\ y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

en assimilant à un nombre pur et simple la matrice (à une ligne et à une colonne) du second membre.

Si on applique alors à f une transformation linéaire $\tau=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, on doit remplacer la matrice colonne $\begin{pmatrix} x \\ y \end{pmatrix}$ par $\begin{pmatrix} \alpha x+\beta y \\ \gamma x+\delta y \end{pmatrix}=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ et donc la matrice ligne (x y) par $(x\ y)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$. On en déduit que l'expression $ux^2+vxy+wy^2$ de la forme $f\circ\tau$ est donnée par le produit matriciel

$$(3) \qquad (x\ y)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

Comme le produit des matrices carrées placées au centre est symétrique, c'est donc la matrice de la forme $g=f\circ\tau$. Si on appelle alors F et G les matrices respectives des formes f et g, et T la matrice de la transformation τ, on a finalement

$$(4) \qquad G={}^tTFT$$

où ${}^tT$ désigne la matrice transposée de T. Il revient au même d'écrire les relations (1) sous la forme

$$(5) \qquad \begin{cases} u=(\alpha\ \gamma)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} \\ \frac{v}{2}=(\alpha\ \gamma)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \beta \\ \delta \end{pmatrix}=(\beta\ \delta)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} \\ w=(\beta\ \delta)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \beta \\ \delta \end{pmatrix} \end{cases}$$

comme on le vérifie immédiatement.

9. Comme Lagrange, nous allons nous intéresser essentiellement, dans la suite, aux transformations linéaires de déterminant ±1. Si $\tau=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est une transformation de ce genre, il est facile de vérifier que c'est une bijection, dont la bijection réciproque est une nouvelle transformation linéaire ayant pour matrice $\pm\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$. Comme le produit (c'est à dire la composée) de deux transformations linéaires de déterminant ±1 est encore une transformation du même genre, on en déduit que les transformations en question forment un groupe que les spécialistes notent $GL_2(\mathbb{Z})$.

Cela étant, on dira que deux formes quadratiques binaires f et g sont *équivalentes au sens de Lagrange* s'il existe une transformation linéaire $\tau \in GL_2(\mathbb{Z})$, donc de déterminant ± 1, telle que $g=f\circ\tau$. Comme $GL_2(\mathbb{Z})$ est un groupe, on définit ainsi, entre les formes quadratiques binaires, une relation d'équivalence au sens habituel du terme.
Mais d'un autre côté, on peut, comme le faisait Gauss, se limiter aux transformations linéaires de déterminant +1. elles forment aussi un groupe sous-groupe de $GL_2(\mathbb{Z})$, que l'on note $SL_2(\mathbb{Z})$. Cela permet alors de dire que deux formes quadratiques binaires f et g sont *équivalentes au sens de Gauss* s'il existe une transformation linéaire $\tau \in SL_2(\mathbb{Z})$, donc de déterminant +1, telle que $g=f\circ\tau$. Là encore, on obtient une relation d'équivalence au sens usuel du terme.

10. Deux formes équivalentes au sens de Gauss le sont évidemment au sens de Lagrange, mais la définition de Gauss peut paraître d'un raffinement bien inutile car il est facile de voir que bon nombre de notions attachées à une forme f ne changent pas lorsqu'on remplace f par une forme équivalente au sens de Lagrange. Il en est ainsi du discriminant, du PGCD (ce qui montre au passage que toute forme équivalente à une forme primitive est encore primitive), des entiers représentés par la forme et même des entiers admettant une représentation propre par la forme considérée.
Les démonstrations, faciles à déterminer sont laissées au lecteur. Toutefois, en ce qui concerne l'"invariance" du discriminant, on peut préférer à un calcul direct l'utilisation de la relation $G={}^tTFT$ (cf la relation (4) dans le n°8 ci-dessus). Avec des notations évidentes, le déterminant de la matrice G est donc à la fois $uw-\frac{v^2}{4}$ et le produit $(\det {}^tT)(\det F)(\det T)$.

Comme $\det {}^tT=\det T=\pm 1$, il ne reste dans ce produit que $\det F=ac-\frac{b^2}{4}$.

En multipliant tout par -4, on obtient l'égalité cherchée $v^2-4uw=b^2-4ac$.
On remarquera que le raisonnement précédent permet de voir que lorsque f est transformée en g par une transformation linéaire τ de déterminant d alors le discriminant de g s'obtient en multipliant celui de f par le carré d^2.

11. toutes les propriétés précédentes sont valables naturellement pour les formes équivalentes au sens de Gauss. Cela n'a pas empêché Gauss de persister dans son idée de limiter l'équivalence des formes comme on l'a dit dans le n°9. Pour aggraver son cas, il n'a pas craint d'indisposer Lagrange en qualifiant d'impropre l'équivalence de son prédécesseur. De façon précise, on dira (comme Gauss) que deux formes sont *proprement équivalentes*, si on passe de l'une à l'autre par une transformation linéaire de déterminant +1 et que ces deux formes sont *improprement équivalentes* si on passe de l'une à l'autre par une transformation de déterminant -1.
Pour voir la portée de cette distinction, considérons les formes (a,b,c) et (c,b,a) (formes inverses l'une de l'autre : n°3). Comme la seconde s'obtient à partir de la première en échangeant les variables, c'est à dire en appliquant la transformation τ : $(x,y)\to(y,x)$, et

que l'on a $\det\tau=\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}=-1$, ces formes sont improprement équivalentes. Mais comme on le verra un peu plus bas, il y a des cas où elles ne sont pas proprement équivalentes. En fait, dire que f est proprement équivalente à sa forme inverse revient à dire que f est improprement équivalente à elle-même. Nous traduirons cette propriété particulière (qui n'est pas toujours vraie) en disant que f est une *forme ambiguë*. S'il en est ainsi, toute forme équivalente à f (proprement ou non) est aussi ambiguë et les deux formes sont équivalentes entre elles tant proprement qu'improprement.
Nous reviendrons dans la prochaine section sur ce vocabulaire qui n'est ni celui de Gauss, ni celui de ses traducteurs (Gauss, rappelons-le, écrivait en latin).

12. Comme toute relation d'équivalence, l'équivalence au sens de Gauss détermine dans l'ensemble des formes quadratiques binaires (à coefficients entiers), des classes d'équivalence qu'on appellera les *classes de Gauss*. Mais il en est de même de l'équivalence au sens de Lagrange, ce qui permet de définir les *classes de Lagrange*.
Toute classe de Gauss est évidemment contenue dans une classe de Lagrange, nécessairement unique, mais l'inclusion réciproque n'a pas toujours lieu. Il est en fait facile de voir que si f est une forme ambiguë (cf n°11), alors la classe de Lagrange de f coïncide avec la classe de Gauss de f, alors que si f n'est pas ambiguë, la classe de Lagrange de f est la réunion de deux classes de Gauss distinctes ; celle de f et celle de la forme inverse.
En fait, l'équivalence de Gauss a sur l'équivalence de Lagrange de nombreux avantages. elle est même indispensable pour définir ce qu'on appellera, dans la section C, la "composition des classes de formes". C'est pourquoi, dans la suite, nous donnerons la préférence à l'équivalence au sens de Gauss. Quand nous parlerons désormais, de formes équivalentes, il sera entendu, sauf précision contraire, qu'il s'agit de formes équivalentes au sens de Gauss et quand il sera question d'une classe de formes, c'est d'une classe de Gauss dont il s'agira. Enfin, pour abréger, nous écrirons f~g l'équivalence de deux formes.

13. Une méthode assez générale pour trouver des formes équivalentes à une forme donnée est d'utiliser la transformation $\tau=\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ (dont le déterminant est +1) avec un entier n quelconque.
Si $f(x,y)=ax^2+bxy+cy^2$, $f(\tau(x,y))=a(x+ny)^2+b(x+ny)y+cy^2=ax^2+(2an+b)xy+(an^2+bn+c)y^2$.
En d'autres termes, si $f=(a,b,c)$, $f\circ\tau=(a,2an+b,an^2+bn+c)$.
Les formes ainsi obtenues, lorsque n parcourt $\mathbb{Z}$, seront dites *parallèles* à f (cf [VEN], p.125). elles sont toutes équivalentes à f. On notera que le coefficient médian de la nouvelle forme est congru au coefficient médian b de l'ancienne modulo a. Lorsque n parcourt $\mathbb{Z}$, on obtient même, de cette manière, tous les entiers possibles congrus à b modulo 2a. Lorsque a n'est pas nul, on peut donc s'arranger pour que l'entier b' obtenu soit le "reste minimal" de b modulo 2a, autrement dit pour $-|a|\leq b'\leq|a|$.

14. Une autre façon d'avoir des formes équivalentes est d'utiliser les transformations $\tau=\begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix}$ (dont le déterminant est encore +1) avec un entier n quelconque.
Cette fois, on vérifie que si f=(a,b,c), $f\circ\tau=(c,-b+2cn,a-bn+cn^2)$.
Les formes obtenues lorsque n parcourt $\mathbb{Z}$ sont dites *contiguës* (cf [GAU], p.125) ou *adjacentes* (cf [BUE], p.23) à f. elles sont toutes équivalentes à f.
On notera en particulier, en prenant n=0, que (a,b,c)~(c,-b,a).
Dans le cas général, lorsque n parcourt $\mathbb{Z}$, on obtient, pour le coefficient médian b' de la nouvelle forme, tous les entiers congrus à -b modulo 2c.
Lorsque c n'est pas nul, on peut donc s'arranger pour que b' soit le reste minimal de -b modulo 2c, autrement dit pour que $-|c|\leq b'\leq|c|$.

D'une manière générale, lorsque f=(a,b,c) et que $c\neq 0$, il est facile de vérifier si une forme g donnée est adjacente à f : pour qu'il en soit ainsi il faut et il suffit que g soit du type (c,d,e) avec $d^2-4ec=b^2-4ac$ et $b+d\equiv 0 \pmod{2c}$.
Grâce à cette méthode, on vérifie aussitôt que

(-1,6,-3)~(-3,0,2)~(2,8,5)~(5,12,6)~(6,12,5)

15. On aura encore une idée de la diversité des formes équivalentes à une forme f donnée en prenant connaissance du résultat suivant : pour qu'un entier n soit proprement représenté par f il faut et il suffit qu'il existe une forme g équivalente à f dont le coefficient initial soit n.
Supposons en effet qu'il existe deux entiers x et y premiers entre eux tels que n=f(x,y). D'après le théorème de Bézout, il existe deux entiers u et v tels que ux-vy=1. si on applique à f la transformation $\begin{pmatrix} x & v \\ y & u \end{pmatrix}$ on obtient une forme g équivalente à f (au sens de Gauss!) dont le premier coefficient est f(x,y) (cf n°6), c'est à dire n.
Réciproquement, si n est le coefficient initial d'une forme g équivalente à f, n est évidemment proprement représenté par g, donc aussi par f comme on l'a vu ci-dessus dans le n°10.

16. De nombreuses propriétés s'appliquant aux formes s'appliquent en fait aux classes. C'est ainsi qu'on peut parler des entiers représentés par une classe, du discriminant d'une classe, d'une classe primitive ou d'une classe ambiguë. On ne se privera pas d'user de ce vocabulaire commode.
En fait, nous nous intéresserons spécialement aux classes de formes (éventuellement primitives ou ambiguës) de discriminant donné.
Commençons par observer que si Δ est un entier arbitraire, ce n'est pas nécessairement le discriminant b^2-4ac d'une forme (donc d'une classe). Comme on a $b^2-4ac\equiv 0 \pmod 4$ si b est pair, et $b^2-4ac\equiv 1 \pmod 4$ si b est impair, un entier Δ qui est congru à 2 ou à 3 modulo 4 ne peut pas être un discriminant.

Par contre, si Δ est divisible par 4 (respectivement si $\Delta \equiv 1 \pmod 4$), la forme $\left(1,0,-\frac{\Delta}{4}\right)$ (respectivement la forme $\left(1,1,\frac{1-\Delta}{4}\right)$) est une forme de discriminant Δ. Cette forme particulière s'appelle la *forme principale* (de discriminant Δ) et sa classe la *classe principale* (de discriminant Δ). Forme et classe principales sont évidemment primitives.

17. Mais le principal résultat qui nous reste à voir est que si Δ est un entier non nul, il n'existe qu'un nombre fini de classes de formes de discriminant Δ. Cet important théorème, démontré en fait par Lagrange, ne s'étend pas aux classes de formes de discriminant 0 car il est facile de voir que si $a \neq a'$, les formes (a,0,0) et (a',0,0) ne représentent pas les mêmes nombres ; elles ne sont donc pas équivalentes.
Pour établir le théorème de Lagrange, on distingue d'ordinaire deux cas selon que Δ est ou non un carré parfait.

18. Si Δ n'est pas un carré parfait, on commence par démontrer que toute forme f=(a,b,c) de discriminant Δ est équivalente à une forme f'=(a',b',c') pour laquelle on a $|b'| \leq |a'| \leq |c'|$. L'hypothèse que Δ n'est pas un carré implique en effet que $a \neq 0$ et $c \neq 0$. Cette dernière permet de considérer une forme adjacente (a',b',c') (avec donc a'=c) telle que $|b'| \leq |c| = |a'|$ (cf n°14). Si $|a'| \leq |c'|$, on obtient la forme f cherchée. Si cette inégalité est fausse, on a $|a'| > |c'|$, c'est à dire $|c| > |c'|$; mais comme c'est différent de 0 (sinon $\Delta = b'^2 - 4a'c'$ serait un carré), on peut affirmer, comme dans le cas précédent, qu'il existe une forme (a",b",c"), adjacente à (a',b',c') (avec donc, en particulier, a"=c') telle que $|b''| \leq |c'| = |a''|$. Si $|a''| \leq |c''|$, on obtient la forme cherchée (du moins sous la forme f"=(a",b",c")). Sinon, on a $|a''| > |c''|$, c'est à dire $|c'| > |c''|$, avec $c'' \neq 0$ et on recommence le processus précédent avec (a",b",c"). Tant qu'on n'obtient pas une forme satisfaisant aux inégalités voulues, on continue.
Comme on a successivement $|c| > |c'| > |c''| > \ldots$, le processus ne peut se poursuivre indéfiniment. D'où immanquablement, au bout d'un nombre fini d'étapes, la forme cherchée.
On reconnaît là un exemple typique du raisonnement *par descente* inventé par Fermat.
Cela étant, le théorème complet se déduira du fait que les formes (a,b,c) obtenues à l'issue du processus précédent sont nécessairement en nombre fini.

En effet, si on a $|b|\leq|a|\leq|c|$, on a $|\Delta|=|4ac-b^2|\geq|4ac|-b^2\geq 4a^2-a^2=3a^2$ d'où la relation $a^2\leq\frac{|\Delta|}{3}$ ou $|a|\leq\sqrt{\frac{|\Delta|}{3}}$ qui montre déjà qu'il n'y a qu'un nombre fini de valeurs de a possibles.

Comme $|b|\leq|a|\leq\sqrt{\frac{|\Delta|}{3}}$, il en est de même des valeurs de b.

Enfin, une fois a et b choisis, la relation $\Delta=b^2-4ac$ montre qu'il n'y a plus qu'une valeur possible pour c égale à $\frac{b^2-\Delta}{4a}$ (où, rappelons-le $a\neq 0$). CQFD.

19. Le cas où Δ est un carré parfait non nul (qu'on peut écrire m^2 où $m>0$) se traite différemment. On commence par démontrer que pour une forme f=(a,b,c) de discriminant Δ, il existe des entiers u et v, premiers entre eux, tels que $au^2+buv+cv^2=0$.

En effet, si $a\neq 0$, le polynôme at^2+bt+c a deux racines rationnelles $\frac{-b\pm m}{2a}$. Si on écrit l'une d'elles sous la forme d'une fraction irréductible $\frac{u}{v}$, on a alors le résultat cherché.

Si $c\neq 0$, on raisonne de même, mais avec le polynôme ct^2+bt+a.
Enfin si a=c=0, on a la relation cherchée $au^2+buv+cv^2=0$ avec u=1 et v=0.
Le résultat obtenu signifie que 0 est proprement représenté par f. D'après le n°15, il existe une forme f'=(a',b',c') équivalente à f telle que a'=0.
Si on considère ensuite une forme parallèle à f', on obtient une forme f"=(a",b",c"), équivalente à f, telle que a"=a'=0, b"=2a'n+b'=b' et $c"=a'n^2+b'n+c'=b'n+c'$ où n est un entier quelconque. Cette dernière relation montre que c" peut être choisi parmi n'importe quel entier congru à c' modulo b'. comme |b'|=m on peut s'arranger pour que c" soit le reste de c' modulo m, donc pour que $0\leq c"\leq m-1$. Aux notations près, on a ainsi démontré que toute forme de discriminant $m^2>0$ est équivalente à une forme du type (a,b,c) avec a=0, b=±m et $0\leq c\leq m-1$. Le nombre de classes possibles est donc au maximum 2m.

20. Lorsque Δ est un discriminant non nul, on notera C(Δ), ou simplement C, l'ensemble des classes de formes de discriminant Δ et c(Δ), ou simplement c, le nombre de ces classes.
Lorsque Δ<0, on peut distinguer les classes de formes positives et les classes de formes négatives. On notera $C^+(\Delta)$ et $C^-(\Delta)$ (ou simplement C^+ et C^-) les sous-ensembles de C(Δ) correspondants. Parallèlement, on pourra noter $c^+(\Delta)$ et $c^-(\Delta)$ (ou c^+ et c^-) les nombres de classes que l'on trouve dans ces ensembles. Pour des raisons évidentes (passage de (a,b,c) à la forme opposée (-a,-b,-c), on a $c^+=c^-=\frac{1}{2}c$.

En fait, pour un discriminant Δ de signe quelconque donné, on s'intéressera surtout aux classes de formes primitives. On notera G(Δ), ou simplement G, leur ensemble et g(Δ), ou simplement g, leur nombre.

On verra plus loin que cet ensemble est en fait un groupe, ce qui justifie, par anticipation, la notation utilisée.
Si $\Delta<0$, on définit de façon évidente des ensembles $G^+(\Delta)$ et $G^-(\Delta)$ (notées aussi simplement G^+ et G^-) et des nombres $g^+(\Delta)$ et $g^-(\Delta)$ (qu'on écrira aussi g^+ et g^-). On a en fait $g^+=g^-=\frac{1}{2}g$.
Signalons que lorsque les spécialistes de la théorie des formes binaires parlent du "nombre de classes" relatif à un discriminant donné Δ, ils entendent généralement par là un nombre noté h ou $h(\Delta)$, égal au nombre g si $\Delta>0$ et égal à $g^+=\frac{1}{2}g$ si $\Delta<0$. Pour nous, qui n'avons en vue que les nombres triangulaires, le nombre $g=g(\Delta)$ fera l'affaire. Il serait d'ailleurs odieux de faire de l'ostracisme à l'égard des formes définies négatives!
Indiquons pour finir que $g(\Delta)$ est fini, même lorsque $\Delta=0$. Il est en effet facile de vérifier que, comme on l'a fait dans le n°19, une forme f de discriminant nul représente proprement 0. Elle est donc équivalente à une forme du type (a,b,0) où b est nécessairement nul. Si elle est primitive, il n'y a que deux possibilités : a=1 et a=-1. D'où $g(\Delta)=g(0)=2$ si $\Delta=0$.

B/ Classes ambiguës primitives de discriminant donné.

1. Ce paragraphe sera bien plus court que le précédent, d'autant plus court qu'on ne traitera pas le cas général, mais celui où Δ est un nombre négatif impair.
Rappelons cependant qu'une forme de discriminant quelconque est dite ambiguë si elle est improprement équivalente à elle-même, autrement dit s'il existe une transformation linéaire de $\mathbb{Z}^2$, de déterminant -1, laissant cette forme invariante (cf §A, n°10).
En fait, pour une forme quelconque, les propriétés suivantes sont équivalentes
(i) f est une forme ambiguë.
(ii) f est équivalente à une forme du type (a',b',c') où b' est un multiple de a'.
(iii) f est équivalente à une forme du type (a',0,c') ou à une forme du type (a',a',c').

2. Démontrons d'abord l'implication (i)⇒(ii). Considérons une forme ambiguë (a,b,c) et écartons le cas ou f est nulle pour laquelle la conclusion est évidente. Compte tenu des relations (1), §A, n°6 vues plus haut, il existe par hypothèse des nombres α, β, γ, δ entiers tels que

$$\begin{aligned} &a\alpha^2+b\alpha\gamma+c\gamma^2=a \\ (1)\quad &2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta=b \\ &a\beta^2+b\beta\delta+c\delta^2=c \end{aligned}$$

avec $\alpha\delta-\beta\gamma=-1$. Cette dernière relation permet de simplifier la seconde des trois égalités données ci-dessus car si on écrit celle-ci sous la forme $2a\alpha\beta+b(\alpha\delta+\beta\gamma-1)+2c\gamma\delta=0$ et si on remplace -1 par $\alpha\delta-\beta\gamma$, on obtient après simplification par 2

(2) $a\alpha\beta+b\alpha\delta+c\gamma\delta=0$

Nous allons déduire de là qu'on a toujours

(3) $\alpha+\delta=0$

De la relation $a=a\alpha^2+b\alpha\gamma+c\gamma^2$ on tire en effet $a\delta=a\alpha^2\delta+b\alpha\gamma\delta+c\gamma^2\delta=a\alpha^2\delta+\gamma(b\alpha\delta+c\gamma\delta)$. Comme $b\alpha\delta+c\gamma\delta=-a\alpha\beta$ d'après (2), on obtient $a\delta=a\alpha^2\delta-a\alpha\beta\gamma=a\alpha(\alpha\delta-\beta\gamma)=-a\alpha$ puisque $\alpha\delta-\beta\gamma=-1$. D'où le résultat annoncé si $a\neq0$.
De la même façon, de la relation $c=a\beta^2+b\beta\delta+c\delta^2$, on tire $c\alpha=a\alpha\beta^2+b\alpha\beta\delta+c\alpha\delta^2=\beta(a\alpha\beta+b\alpha\delta)+c\alpha\delta^2=\beta(-c\gamma\delta)+c\alpha\delta^2=c\delta(-\beta\gamma+\alpha\delta)=-c\delta$, ce qui conduit à la même conclusion si $c\neq0$.
Reste le cas où $a=c=0$ (et où donc $b\neq0$). dans ce cas, les diverses relations ci-dessus se réduisent à $b\alpha\gamma=0$, $b\alpha\delta=0$ et $b\beta\delta=0$, donc à $\alpha\gamma=\alpha\delta=\beta\delta=0$. comme en outre $\alpha\delta-\beta\gamma=-\beta\gamma=-1$, β et γ ne peuvent être nuls. On a donc $\alpha=\delta=0$ et par conséquent $\alpha=-\delta$.
La relation (3) étant établie, supposons d'abord $\gamma=0$. On a alors d'après (2), $a\alpha\beta+b\alpha\delta=0$, c'est à dire, puisque $\alpha\delta=-1$, $b=a\alpha\beta$. Cela démontre l'assertion (ii) cherchée en prenant pour (a',b',c') la forme f=(a,b,c) elle-même.
Supposons maintenant $\gamma\neq0$ et considérons une transformation $\tau=\begin{pmatrix}\lambda & \mu\\ \nu & \rho\end{pmatrix}$ arbitraire de déterminant +1. Appelons f' la forme $f\circ\tau$: c'est une forme équivalente à f qu'on écrira aussi (a',b',c'). Si on note σ la transformation $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ utilisée ci-dessus, il est facile de voir que f' est invariante par la transformation $\tau^{-1}\sigma\tau$ car
$f'\circ(\tau^{-1}\sigma\tau)=f\circ\tau\circ\tau^{-1}\circ\sigma\circ\tau=f\circ\sigma\circ\tau=f\circ\tau=f'$ (puisque par hypothèse $f\circ\sigma=f$). Mais $\tau^{-1}\sigma\tau$ est évidemment une transformation linéaire de $\mathbb{Z}^2$ de déterminant -1, de sorte que si on pose $\tau^{-1}\sigma\tau=\begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}$, on voit par le raisonnement précédent que $\alpha'+\delta'=0$ (ce qui ne nous servira pas!) et surtout que b' est un multiple de a' si en outre $\gamma'=0$. tout le problème est donc de montrer qu'on peut choisir $\tau=\begin{pmatrix}\lambda & \mu\\ \nu & \rho\end{pmatrix}$ de façon à avoir $\gamma'=0$.
Comme la matrice de $\tau^{-1}\sigma\tau$ est $\begin{pmatrix}\rho & -\mu\\ -\nu & \lambda\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}\lambda & \mu\\ \nu & \rho\end{pmatrix}$, un calcul facile (laissé au lecteur) montre que $\gamma'=\gamma\lambda^2-2\alpha\lambda\nu-\beta\nu^2$. On a donc
$\gamma\gamma'=\gamma^2\lambda^2-2\alpha\gamma\lambda\nu-\beta\gamma\nu^2=\gamma^2\lambda^2-2\alpha\gamma\lambda\nu+\alpha^2\nu^2-\alpha^2\nu^2-\beta\gamma\nu^2=(\gamma\lambda-\alpha\nu)^2-\nu^2(\alpha^2+\beta\gamma)=(\gamma\lambda-\alpha\nu)^2-\nu^2$
car $\alpha^2+\beta\gamma=-\alpha\delta+\beta\gamma=+1$.
Par suite, la relation $\gamma'=0$ équivaut à la relation $(\gamma\lambda-\alpha\nu)^2=\nu^2$ (on rappelle que $\gamma\neq0$). Elle est vérifiée si $\gamma\lambda-\alpha\nu=\nu$, c'est à dire si $\gamma\lambda=(\alpha+1)\nu$. Pour avoir cette relation, il suffit d'écrire $\frac{\alpha+1}{\gamma}$ sous la forme $\frac{\lambda}{\nu}$, ce qui est toujours possible. Mais si on choisit en outre λ et ν premiers entre eux, on peut trouver μ et ρ tels que $\lambda\rho-\mu\nu=1$ (Bézout) et le tour est joué!

3. La fin de la démonstration est beaucoup plus simple : pour démontrer que (ii) implique (iii), il suffit d'utiliser la notion de forme parallèle (§A, n°13) et pour démontrer que (iii) implique (i) il suffit de démontrer que toute forme du type (a,0,c) ou du type (a,a,c) est

ambiguë, ce qui se voit en faisant appel soit à la transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ soit à la transformation $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. Les détails sont laissés au lecteur.

Gauss n'a pas donné de nom aux formes invariantes par une transformation de déterminant -1 mais il a qualifié d'"anceps" (ce qui parait-il veut dire "à deux têtes" : cf [BUE], p.7) les formes du type (a,b,c) où b est un multiple de a. Ce terme a été traduit pas "ambigu" dans [GAU], p.132. Vu nos choix terminologiques, cette traduction est inacceptable ; c'est pourquoi nous parlerons plutôt de *formes ancipitales*. Cette notion est très utile à Gauss pour développer sa théorie de la réduction des formes indéfinies. Pour nous, nous aurons surtout besoin des formes ancipitales du type (a,0,c) ou (a,a,c) ; nous les appellerons les *formes élémentaires*.

4. D'après ce qu'on a dit dans le n°1, dire qu'une forme est ambiguë c'est dire qu'elle est équivalente à une forme élémentaire. Par suite, pour déterminer toutes les classes ambiguës possibles, il suffit de déterminer toutes les formes élémentaires. Si l'on fixe le discriminant Δ et si on suppose $\Delta \neq 0$ la méthode est d'autant plus facile à mettre en œuvre que tout revient à avoir les relations $-4ac=\Delta$ et $a^2-4ac=\Delta$. Comme a est dans les deux cas un diviseur de Δ, cela ne fait qu'un nombre fini de formes possibles. Si on impose en outre aux formes d'être primitives, on voit que se donner une forme de ce type revient à se donner deux entiers a et c premiers entre eux, vérifiant soit la relation $-4ac=\Delta$, soit la relation $a(a-4c)=\Delta$. Le cas général est un peu délicat du fait de l'existence de deux espèces de formes élémentaires et à cause de subtils problèmes de divisibilité que nous ne pouvons pas détailler ici (cf [CAS], p.342). Mais on peut traiter sans difficultés le cas où Δ est impair - le seul qui, finalement, nous servira. Lorsque Δ est impair, seules apparaissent les formes du type (a,a,c).

Si a et c sont des entiers premiers entre eux tels que $a^2-4ac=\Delta$, a est un diviseur de Δ (donc un nombre impair), premier avec a-4c, donc premier avec son "diviseur complémentaire". On traduira cette propriété bien particulière en disant que a est un *diviseur libre* de Δ.

Réciproquement, si a est un diviseur libre de Δ, la relation $a(a-4c)=\Delta$ définit un nombre c et un seul, égal à $\frac{a^2-\Delta}{4a}$. Ce nombre est en fait un entier car a divise $a^2-\Delta$, tout en étant premier avec 4, et que 4 divise $a^2-\Delta$: cette dernière propriété résulte de ce que, avec les hypothèses, on a $a^2 \equiv \Delta \equiv 1 \pmod 4$. Il est ensuite facile de vérifier que c est premier avec a.

En résumé, lorsque Δ est un discriminant impair, on obtient toutes les formes primitives élémentaires de discriminant Δ en considérant les formes (a,a,c) où a parcourt l'ensemble des diviseurs libres de Δ et où $c=\frac{a^2-\Delta}{4a}$.

5. D'après ce qu'on vient de dire, le nombre de formes primitives élémentaires de discriminant Δ est égal au nombre de diviseurs libres de Δ. Pour calculer ce dernier nombre, on peut faire appel à la décomposition en facteurs premiers de Δ ou plutôt du

nombre positif $|\Delta|$. Si on écrit celle-ci sous la forme $p_1^{\alpha_1}...p_r^{\alpha_r}$ avec des nombres premiers p_1, ..., p_r deux à deux distincts et des exposants α_1, ..., α_r entiers >0, on sait qu'on obtient tous les diviseurs de $\Delta_1^{\alpha_1}$en considérant les produits $\pm p_1^{\beta_1}...p_r^{\beta_r}$ où $0\leq\beta_1\leq\alpha_1$, ..., $0\leq\beta_r\leq\alpha_r$. Pour obtenir alors un diviseur libre de Δ (c'est à dire un diviseur premier avec son diviseur complémentaire) il faut que l'on ait $\beta_i=0$ ou $\beta_i=\alpha_i$ pour tout i car dans le cas contraire le nombre premier p_i diviserait à la fois le diviseur considéré et son diviseur complémentaire. Cette condition nécessaire est aussi suffisante.
Pour i fixé, il y a donc deux façons de choisir β_i. Comme ce choix doit se faire pour i=1, 2, ..., r et qu'il faut pour finir choisir le signe du diviseur libre cherché, on voit finalement que le nombre de diviseurs libres de Δ est égal à 2^{r+1} où r désigne, en fait, le nombre de diviseurs premiers de Δ.

6. Tout serait parfait si les formes obtenues étaient deux à deux non équivalentes. Ce n'est malheureusement pas le cas car si on applique à une forme (a,a,c) la transformation $\begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}$, évidemment de déterminant +1, on obtient, en développant $a(-x-y)^2+a(-x-y)(2x+y)+c(2x+y)^2$, la forme (4c-a,4c-a,c). C'est une forme équivalente à (a,a,c), du même type, et qui s'obtient finalement en remplaçant le diviseur libre a initial par $4c-a=-\frac{\Delta}{a}$, donc par un autre diviseur libre qui n'est autre que l'opposé du diviseur complémentaire de a.
Ces diviseurs libres "associés" jouent des rôles symétriques, sans jamais être égaux car si on avait a=4c-a, on aurait a=2c en contradiction avec le fait que a est impair. On pourrait donc supprimer sans grand dommage une forme sur deux et donc réduire le nombre de ces formes à 2^r. Mais on va voir que sauf dans le cas très particulier où Δ=1, un et un seul des deux nombres a, 4c-a appartient à l'intervalle $]-\sqrt{|\Delta|},\sqrt{|\Delta|}[$. Raisonnons par l'absurde en distinguant deux cas. Si on avait en même temps $|a|<\sqrt{|\Delta|}$ et $|4c-a|<\sqrt{|\Delta|}$, on aurait $|\Delta|=|a||4c-a|<|\Delta|$, ce qui est absurde. Si on avait en même temps $|a|\geq\sqrt{|\Delta|}$ et $|4c-a|\geq\sqrt{|\Delta|}$, l'une de ces inégalités serait stricte car s'il y avait égalité partout on aurait $|a|=\sqrt{|\Delta|}=|4c-a|$, donc soit $|a|=|2c|$, en contradiction avec le fait que a est impair, soit 4c=0, ce qui impliquerait a=±1 (à cause du caractère primitif de la forme (a,a,c)), donc $\Delta=a^2=1$, ce qu'on a exclu. On en déduit que $|a||4c-a|>|\Delta|$, ce qui est encore absurde.
Les résultats ainsi obtenus et ceux du n°1 vus ci-dessus montrent que si Δ est un discriminant impair ≠1, toute forme ambiguë primitive est équivalente à une forme du type (a,a,c) où a est un diviseur libre de Δ tel que $a^2<|\Delta|$, le nombre des formes de ce type étant égal à 2^r, où r désigne le nombre de diviseurs premiers de Δ.

7. Le résultat précédent implique que le nombre de classes ambiguës primitives de discriminant Δ (Δ impair $\neq 1$) est au plus égal à 2^r et qu'il est égal à 2^r exactement si et seulement si les formes du type (a,a,c) qui nous restent (donc avec $a^2<|\Delta|$) sont deux à deux non équivalentes. Sauf erreur de ma part (cf [VEN], p.126), cette dernière propriété est exacte si $\Delta<0$ (hypothèse qui élimine au passage l'exception $\Delta=1$ que nous n'avons pas traitée). Heureusement pour nous nous n'aurons pas besoin d'un autre cas!

8. Pour parvenir à nos fins, nous allons revenir sur un résultat vu plus haut (§A, n°18) selon lequel lorsque Δ n'est pas un carré parfait, toute forme f de discriminant Δ est équivalente à une forme (a,b,c) telle que $|b|\leq|a|\leq|c|$. Si $\Delta<0$ (ce qui exclut les carrés parfaits) et si la forme f est supposée positive, cette condition s'écrit $|b|\leq a\leq c$ puisque a et c sont alors des nombres >0. Il se trouve qu'avec toutes ces conditions, les formes obtenues sont rarement équivalentes. De façon plus précise, si on qualifie de *faiblement réduite* toute forme définie positive f=(a,b,c) pour laquelle $|b|\leq a\leq c$, alors on peut affirmer que deux formes définies positives distinctes et faiblement réduites ne sont jamais équivalentes sauf si l'une s'écrit (a,b,a) et l'autre (a,-b,a) ou si l'une s'écrit (a,a,c) et l'autre (a,-a,c).

9. La démonstration du résultat que l'on vient d'énoncer nous demandera un lemme en quatre cas :

Lemme : Si f=(a,b,c) est une forme définie positive faiblement réduite alors $f(x,y)\geq a(x^2-|xy|+y^2)$ quels que soient les entiers x et y. On a même une inégalité stricte si $y\neq 0$ et $c>a$ ou si $xy\neq 0$ et $|b|<a$.

Si on écrit $f(x,y)=ax^2+bxy+cy^2$ sous la forme $a\left(x^2+\frac{b}{a}xy+\frac{c}{a}y^2\right)$ on voit que l'on a l'inégalité "large" annoncée si on démontre que $\frac{b}{a}xy\geq -|xy|$ et $\frac{c}{a}y^2\geq y^2$. Comme on a $\left|\frac{b}{a}\right|\leq 1$ par hypothèse, on a aussi, $\left|\frac{b}{a}xy\right|\leq|xy|$. cela signifie aussi que $-|xy|\leq\frac{b}{a}xy\leq|xy|$, donc en particulier $\frac{b}{a}xy\geq -|xy|$, d'où la première inégalité cherchée. La seconde est plus immédiate car elle découle de l'hypothèse que $\frac{c}{a}\geq 1$.

Ce raisonnement montre aussi que l'on a l'inégalité stricte $f(x,y)>a(x^2-|xy|+y^2)$ à chaque fois que $\frac{b}{a}xy>-|xy|$ ou que $\frac{c}{a}y^2>y^2$. Le premier cas est réalisé si on suppose $\left|\frac{b}{a}\right|<1$ (c'est à dire $|b|<a$) et $xy\neq 0$; le second si on suppose $\frac{c}{a}>1$ (c'est à dire $c>a$) et $y\neq 0$. D'où le lemme.

Cela étant, supposons que f=(a,b,c) et f'=(a',b',c') soient deux formes définies positives équivalentes, faiblement réduites, donc pour lesquelles $|b|\leq a\leq c$ et $|b'|\leq a'\leq c'$.

Comme $x^2-|xy|+y^2$ est >0 si $(x,y)\neq(0,0)$ (cela résulte de ce que $x^2-|xy|+y^2 = (|x|-|y|)^2+|xy|$), le lemme ci-dessus permet de dire que $f(x,y)\geq a$ si $(x,y)\neq(0,0)$. Comme f(1,0)=a, on peut dire que a est la plus petite valeur non nulle prise par f.
Le même raisonnement pour f' montre que a' est, de son côté, la plus petite des valeurs non nulles prises par f'. Comme ces valeurs pour f et pour f' sont les mêmes (cela vient de ce que f et f' sont équivalentes), on a ici a=a'.
Cela étant, considérons une transformation $\tau=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ de déterminant +1 telle que $f'=f\circ\tau$.
Comme $a'=f'(1,0)=f(\tau(1,0))=f(\alpha,\gamma)$ et que a'=a, $a=f(\alpha,\gamma)$. Si on suppose alors que c>a, on a nécessairement $\gamma=0$ (et donc $\alpha\delta=1$) car si on avait $\gamma\neq0$, le lemme ci-dessus (appliqué avec $x=\alpha$ et $y=\gamma$) donnerait $a=f(\alpha,\gamma)>a(\alpha^2-|\alpha\gamma|+\gamma^2)\geq a$, donc a>a. Si on suppose que $|b|<a$, le même raisonnement montre que l'on a nécessairement $\alpha\gamma=0$, c'est à dire $\alpha=0$ (donc $\beta\gamma=-1$) ou $\gamma=0$ (donc $\alpha\delta=1$). On va alors distinguer plusieurs cas.

Premier cas. Supposons c>a
D'après ce qui précède, on a $\gamma=0$ et $\alpha\delta=1$, de sorte que la matrice $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ est égale à l'une des matrices $\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$ ou $\begin{pmatrix}-1 & \beta\\ 0 & -1\end{pmatrix}$. Quitte à remplacer β par -β dans le second cas, on peut dire que la matrice qui nous intéresse est de la forme $\pm\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$. Comme l'application composée $f\circ\tau$
(où $\tau=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$) ne dépend pas du signe en jeu (ainsi qu'on le vérifie immédiatement), on peut se contenter de calculer les coefficients a', b', et c' de f' en utilisant la seule relation $f'=f\circ\tau$ avec $\tau=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$, donc en développant $a(x+\beta y)^2+b(x+\beta y)+cy^2$. On voit aussitôt que a'=a (ce qu'on savait déjà) et que $b'=b+2a\beta$. Cette dernière relation signifie que l'on a $b'\equiv b \pmod{2a}$.
Comme b' et b sont tous deux, par hypothèse, dans l'intervalle [-a,a], cette congruence ne peut avoir lieu que si b'=b ou si $b=\pm a$ et b'=-b. Si b'=b, on a aussi c=c' (à cause des égalités a=a' et $b^2-4ac=b'^2-4a'c'$), donc f=f'. Si $b=\pm a$ et b'=-b, l'une des formes considérées est (a,a,c) et l'autre (a,-a,c), conformément à la conclusion souhaitée.

Deuxième cas. Supposons c=a et $|b|<a$. alors, d'après ce qu'on a vu plus haut, on a $\alpha\gamma=0$. Si $\gamma=0$, $\alpha\delta=1$ et on retrouve le cas traité juste ci-dessus, avec la même conclusion car la condition c>a du premier cas n'a pas été utilisée dans le calcul de a',b',c'.

Si $\alpha=0$, on a $\beta\gamma=-1$, de sorte que la matrice $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ est égale à $\begin{pmatrix}0 & 1\\ -1 & \delta\end{pmatrix}$ ou à $\begin{pmatrix}0 & -1\\ 1 & \delta\end{pmatrix}$. En suivant un raisonnement déjà fait dans le premier cas, on peut supposer que la matrice est simplement $\begin{pmatrix}0 & 1\\ -1 & \delta\end{pmatrix}$. Cela permet de calculer a', b', c' en développant

$ay^2+by(-x+\delta y)+c(-x+\delta y)^2$.

On trouve alors a'=c, c'est à dire a'=a comme on le savait déjà, et $b'=-b-2c\delta$. Cette dernière relation permet de dire cette fois que $b'\equiv -b \pmod{2c}$, donc (puisque c=a) que $b'\equiv -b \pmod{2a}$. Comme b' et -b sont tous deux compris entre -a et a, la congruence précédente ne peut avoir lieu que si b'=-b ou si $b'=\pm a$ et -b=-b'. Dans ce dernier cas, on a b=b', donc c=c' (puisque $b^2-4ac=b'^2-4a'c'$) et par conséquent f=f'. Dans l'autre cas, on a encore c=c' (car $b^2=b'^2$ et $b^2-4ac=b'^2-4a'c'$), ce qui fait que les formes considérées sont respectivement (a,b,a) et (a,-b,a), conformément à la conclusion cherchée.

Troisième cas. Supposons c=a=b. Alors, comme la relation $a=f(\alpha,\gamma)$ s'écrit $a=a\alpha^2+b\alpha\gamma+c\gamma^2=a(\alpha^2+\alpha\gamma+\gamma^2)$, on a nécessairement $\alpha^2+\alpha\gamma+\gamma^2=1$. Cela n'est possible que si $\alpha\gamma=0$ ou $\alpha\gamma=-1$. En effet, dans le cas contraire, on aurait $\alpha\gamma\geq 1$ ou $\alpha\gamma\leq -2$. Cela est absurde car avec la première inégalité, on aurait $\alpha^2+\alpha\gamma+\gamma^2=(\alpha-\gamma)^2+3\alpha\gamma\geq 3\alpha\gamma\geq 3$ et avec la seconde, $\alpha^2+\alpha\gamma+\gamma^2=(\alpha+\gamma)^2-\alpha\gamma\geq -\alpha\gamma\geq 2$.

Le cas $\alpha\gamma=0$ se traite comme on l'a fait ci-dessus, dans le deuxième cas, en tenant compte du fait que lorsque $\alpha=0$ on a aussi, ici, a=c. Le cas $\alpha\gamma=-1$ donne $\alpha=1$, $\gamma=-1$ ou $\alpha=-1$, $\gamma=1$. Comme $\alpha\delta-\beta\gamma=1$, on voit que $\beta+\delta=1$ dans le premier cas et que $\beta+\delta=-1$ dans le second. D'où les deux matrices possibles pour $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, à savoir $\begin{pmatrix}1 & \beta\\ -1 & \delta\end{pmatrix}$ avec $\beta+\delta=1$ et $\begin{pmatrix}-1 & \beta\\ 1 & \delta\end{pmatrix}$ avec $\beta+\delta=-1$. Quitte à changer de notation, on peut dire que l'on a toujours une matrice de la forme $\pm\begin{pmatrix}1 & \beta\\ -1 & \delta\end{pmatrix}$ avec $\beta+\delta=1$, ce qui permet de limiter les calculs à $\begin{pmatrix}1 & \beta\\ -1 & \delta\end{pmatrix}$, donc à développer

$a(x+\beta y)^2+b(x+\beta y)(-x+\delta y)+c(-x+\delta y)^2$. D'où $a'=a-b+c=a$ (car a=b=c) et $b'=2a\beta+b\delta-b\beta-2c\delta=2a\beta+a\delta-a\beta-2a\delta=a(\beta-\delta)=a(2\beta-1)$. On a donc $b'=2a\beta-a$, soit $b'\equiv -b \pmod{2a}$.

En suivant un raisonnement déjà fait ci-dessus, on voit que b'=-b (donc c=c') ou que b'=b, ce qui correspond à la conclusion cherchée.

Quatrième cas. c=a=-b. On se ramène au cas précédent en observant que (a,-a,a)~(a,a,a).

Compte tenu des conditions initiales $|b|\leq a\leq c$, les quatre cas précédents épuisent toutes les possibilités. Comme les équivalences (a,b,a)~(a,-b,a) et (a,a,c)~(a,-a,c) sont évidentes ou presque, la démonstration est entièrement achevée.

10. On voit ainsi que, sauf exceptions, des formes définies positives faiblement réduites, définissent des classes deux à deux distinctes. Comme les exceptions sont (a,b,a)~(a,-b,a)

et (a,a,c)~(a,-a,c), on peut éviter les répétitions en choisissant positivement, dans ces deux cas, le coefficient médian, ce qui revient, dans le dernier cas, à éliminer (a,-a,c).
Cela explique la définition précise suivante (cf [BUE], p.17) : on dit qu'une forme définie positive (a,b,c) est *réduite* (on pourrait dire "fortement réduite") si on a la condition générale $|b|\leq a\leq c$, si $b\neq -a$ et si la relation $a=c$ implique $b\geq 0$. On complétera cette définition de la manière la plus naturelle qui soit en disant qu'une forme définie négative f est réduite si -f est réduite au sens précédent.
Avec ces définitions, des formes réduites distinctes sont deux à deux non équivalentes. Cela permet de compléter le résultat du §A, n°18 en notant que toute forme de discriminant $\Delta<0$ est équivalente à une forme réduite et à une seule. Lorsque $|\Delta|$ n'est pas très grand, la liste complète des formes réduites n'est pas difficile à obtenir, surtout si on tient compte du fait que $a\leq\sqrt{\frac{|\Delta|}{3}}$ (§A, n°16). dans le cas où $\Delta=-63$, cela donne $a\leq 4$. En essayant tous les cas possibles, on obtient 10 formes réduites dont les cinq positives sont (1,1,16), (2,1,8), (2,-1,8), (3,3,6) et (4,1,4).
On en déduit que le nombre des classes de formes de discriminant -63 est c=10, que celui des classes primitives est g=8 (il faut éliminer (3,3,6) et la forme opposée) et donc que le "nombre de classes" (cf §A, n°20) est h=4.

11. Mais revenons aux classes ambiguës primitives ou plutôt aux formes de discriminant Δ du type (a,a,c) où a est un diviseur libre de Δ tel que $a^2<|\Delta|$. Comme on l'a expliqué dans le n°7, il s'agit de vérifier que lorsque Δ est un nombre impair négatif, ces formes sont deux à deux non équivalentes. Un tout petit peu de réflexion (lecteur, dévoue-toi) montre qu'il suffit de prouver le résultat en question pour les seules formes positives. Malheureusement, les formes à examiner n'ont aucune raison d'être réduites. Pour nous ramener à celles-ci, nous conviendrons de noter f_a en général la forme (a,a,c), étant entendu que a est un diviseur libre >0 de Δ tel que $a^2<|\Delta|$ et que $c=\frac{a^2-\Delta}{4a}$, puis de poser $f'_a=f_a$ si $a\leq c$ et $f'_a=(c,2c-a,c)$ si $a>c$. Comme f'_a est adjacente à f_a dans ce dernier cas, on en déduit que f'_a est, quel que soit a, équivalente à f_a. Aussi, pour démonter que les formes f_a sont deux à deux non équivalentes il suffit de vérifier que les formes f'_a ont la même propriété. Comme ces dernières sont réduites (ainsi qu'on le vérifier facilement), tout revient à démontrer qu'elles sont deux à deux distinctes. La démonstration, très simple, est laissée au lecteur.
Ainsi, si Δ est un discriminant impair et négatif, le nombre de classes ambiguës et primitives que l'on peut définir à partir de Δ est égal à 2^r (où r est le nombre de diviseur premiers de Δ). Bien entendu, si on ne considère que les classes de formes positives, le nombre en question doit être divisé par 2, ce qui donne 2^{r-1}.
On peut illustrer ce qui précède par le cas où $\Delta=-63$. Les diviseurs libres de 63 sont ± 1, ± 9, ± 7 et les formes élémentaires correspondantes sont $\pm(1,1,16)$, $\pm(9,9,4)$, $\pm(7,7,4)$. En se limitant aux formes positives (a,a,c) pour lesquelles $a^2<|\Delta|$, on obtient les deux formes

(1,1,16) et (7,7,4). La première est réduite, donc laissée telle quelle, alors que la seconde doit être remplacée par (4,1,4). Les 4 classes ambiguës primitives de discriminant -63 sont donc les classes des formes (1,1,16), (4,1,4), (-1,-1,-16) et (-4,-1,-4).
Nous pouvons maintenant passer au troisième point de notre programme.

C/ Composition des classes de formes et groupes de classes.

1. L'idée de base de ce qu'on appelle, depuis Gauss, la composition des formes est de généraliser autant que faire se peut certaines identités bien connues comme l'identité de Fibonacci

$$(x^2+y^2)(x'^2+y'^2)=(xx'\pm yy')^2+(xy'\mp x'y)^2$$

l'identité de Brahmagoupta

$$(x^2+Ay^2)(x'^2+Ay'^2)=(xx'\pm Ayy')^2)+A(xy'\mp x'y)^2$$

ou certaines identités moins courantes, ou moins utiles comme l'identité

$$(2x^2+2xy+3y^2)(2x'^2+2x'y'+3y'^2)=(2xx'+xy'+x'y+3yy')^2+5(xy'-x'y)^2$$

qui a permis à Lagrange de résoudre certaines conjectures de Fermat et d'Euler sur les nombres de la forme x^2+5y^2.
Ce dernier exemple signifie que lorsqu'on multiplie deux nombres de la forme $2x^2+2xy+3y^2$, on obtient un nombre de la forme x^2+5y^2, ce qu'on exprime aussi, de manière quelque peu abusive en disant que lorsqu'on "compose" la forme $2x^2+2xy+3y^2$ avec elle-même, on obtient la forme x^2+5y^2.

2. A la fin du XVIII^e siècle, Legendre fit une composition de cas analogues déjà connus, ce qui le conduisit à dresser de véritables tables de composition. Mais c'est Gauss qui s'attaqua au cas général en se proposant, dans ses *Disquisitiones Arithmeticae* (cf [GAU], p.243) de rechercher tous les cas où l'on a, entre des formes quadratiques binaires f, g, et h, une relation du type

$$f(x,y)g(x',y')=h(X,Y)$$

où X et Y sont des fonctions bilinéaires, à coefficients entiers, des éléments x, y, x' et y' :

$$X=axx'+bxy'+cx'y+dyy'$$
$$Y=rxx'+sxy'+tx'y+uyy'$$

Moyennant certaines conditions portant sur les coefficients a, b, c, d, r, s, t, u de ces fonctions bilinéaires, il put montrer qu'en partant de deux formes f et g, il était toujours possible de définir une forme h unique à une équivalence près, ne dépendant en réalité que des classes de f et de g.
"On voit par là" ajoutait-il *"comment on peut définir la composition de deux classes"*. Il convient de noter que les classes en question doivent être prises au sens de Gauss et non au sens de Lagrange : comme le montrent d'ailleurs les tables de Legendre, la considération des seules classes de Lagrange conduit à une certaine ambiguïté due au fait que la "classe composée" n'est pas unique.

3. Malheureusement, si l'idée de Gauss est séduisante et générale, elle donne lieu à des calculs si complexes qu'on lui préfère souvent une méthode due à Dirichlet, qui apparaît déjà chez Legendre (et que Gauss lui-même ne méconnaissait pas) et qui consiste à limiter la composition à des formes qui s'adaptent bien, en quelque sorte, les unes aux

autres, et qu'on qualifie de "concordantes". En fait, pour les seuls besoins de la théorie, il n'est pas nécessaire de reprendre telle quelle la définition de Dirichlet et on peut finalement se borner à un type encore plus restreint de formes qu'on appellera ici des formes composables[2].
De façon précise, nous dirons que deux formes quadratiques binaires f et f' sont *composables* si elles ont même discriminant Δ, même coefficient central b et si, en appelant a et a' leurs coefficients initiaux, le produit 4aa' est un entier non nul divisant b^2-Δ.
Les deux premières conditions signifient que l'on peut poser f=(a,b,c) et f'=(a',b,c') avec $\Delta=b^2-4ac=b^2-4a'c'$. La dernière condition exprime que a et a' sont des entiers non nuls et que le quotient $\frac{b^2-\Delta}{4aa'}$ est un entier. Si on l'appelle c" et si on pose a"=aa', cela permet de considérer la forme f"=(a",b",c") qui a non seulement le même coefficient central que f et f' mais aussi le même discriminant Δ.
Cette nouvelle forme s'appelle alors la *composée* de f et de f' ; on l'écrira f*f'.
On notera tout de suite que f et f' jouent dans les définitions précédentes des rôles rigoureusement symétriques : si f et f' sont des formes composables, f' et f le sont aussi et on a f*f'=f'*f.

4. Deux formes du type (a,b,c) et (a',b,c') de même discriminant sont par exemple composables si a et a' sont des entiers non nuls premiers entre eux. En effet, si on appelle Δ le discriminant commun des deux formes, la relation $b^2-\Delta=4ac=4a'c'$ montre que $\frac{b^2-\Delta}{4}$ (qui est un entier) est divisible par a et par a'. Si on suppose a et a' premiers entre eux, cet entier est divisible par aa'. Cela veut dire aussi que 4aa' divise b^2-Δ. CQFD.
Un autre exemple de formes composables est fourni par une forme (a,b,c) pour laquelle ac≠0, et la forme inverse (c,b,a). Cela résulte immédiatement des définitions puisque $b^2-\Delta=4ac$. On notera en outre que la composée de (a,b,c) et de (c,b,a) est la forme (ac,b,1).
En revanche, il est assez rare qu'une forme (a,b,c) soit composable avec elle-même car non seulement il faut que a et c soient différents de 0, mais aussi que $4a^2$ divise 4ac, donc que a divise c, condition qui n'est évidemment pas toujours réalisée.

5. Il est vrai que la définition que nous avons donnée de la composabilité pêche par son caractère artificiel. Pour la rattacher à la conception de Gauss, il est commode de la présenter autrement en démontrant que deux formes f et f' sont composables si et seulement si on peut trouver des entiers a, a', b et c, les deux premiers n'étant pas nuls, tels que f=(a,b,a'c) et f'=(a',b,ac). Dans ces conditions, f*f'=(aa',b,c).
La démonstration n'est pas difficile ; elle est donc laissée au lecteur.
Cela étant, la raison de cette nouvelle version de la composabilité réside dans le fait que si a, a', b et c sont des entiers quelconques, on a l'identité suivante

$$(ax^2+bxy+a'cy^2)(a'x'^2+bx'y'+acy'^2)=aa'X^2+bXY+cY^2$$

---

[2] Pour voir les différents points de vue possible (et les variations de vocabulaire), on consultera [GAU], *loc. cit.*, [VEN], p.127, [BUE], p.55 et 120 ainsi que [CAS], p.335.

avec X=xx'-cyy' et Y=axy'+a'x'y+byy'.
La démonstration de cette identité est facile quoique un peu fastidieuse. On peut me croire sur parole! Pour aller plus vite, au moins dans le cas où aa'≠0, on peut développer le produit $\left(ax+\frac{b+\sqrt{\Delta}}{2}y\right)\left(a'x'+\frac{b+\sqrt{\Delta}}{2}y'\right)$.
En menant les calculs intelligemment, cela donne

$$\left(ax+\frac{b+\sqrt{\Delta}}{2}y\right)\left(a'x'+\frac{b+\sqrt{\Delta}}{2}y'\right)=aa'X+\frac{b+\sqrt{\Delta}}{2}Y$$

où X et Y ont la signification ci-dessus. On a bien sûr aussi

$$\left(ax+\frac{b-\sqrt{\Delta}}{2}y\right)\left(a'x'+\frac{b-\sqrt{\Delta}}{2}y'\right)=aa'X+\frac{b-\sqrt{\Delta}}{2}Y$$

En multipliant nombre à nombre les deux égalités trouvées, on en déduit sans trop de problèmes l'identité cherchée. Le lecteur se débrouillera!
De toute façon l'identité en tant que telle ne nous sera utile que pour énoncer le résultat selon lequel si f et f' sont deux formes composables, représentant respectivement des entiers n et n' donnés, alors la forme composée f*f' représente le produit nn'. Compte tenu de tout ce qui précède, ce résultat est quasi évident...

6. Comme nous l'avons dit, le problème n'est pas tant de décomposer des formes que de composer des classes. Il s'agit donc de savoir si, étant données deux formes f et f' de même discriminant, il existe deux formes composables φ et φ' qui soient respectivement équivalentes à f et à f'. Notre bonheur sera complet, si on prouve en outre que la classe de la forme $\varphi*\varphi'$ ne dépend que des classes de φ et de φ' (ou de f et de f').
Nous allons voir que toutes ces propriétés sont satisfaites si les formes considérées sont primitives. A cause de cette limitation, il serait souhaitable que le lecteur établisse que si f et f' sont des formes primitives composables, alors f*f' est aussi primitive. Mais non ce n'est pas difficile!

7. En fait, l'essentiel de l'argumentation qui va suivre repose sur le lemme suivant que ni Gauss ni Cassels ne jugent utile de démontrer entièrement (cf [GAU], p.231 et [CAS], p.334) :

Lemme : Si f est une forme primitive et si m est un entier non nul quelconque, alors il existe un entier n non nul, premier avec m, et proprement représenté par f.

Posons f=(a,b,c) et partageons l'ensemble P des diviseurs premiers de m en trois ensembles disjoints : l'ensemble Q des diviseurs premiers de m ne divisant pas a, l'ensemble R des diviseurs premiers de m divisant a mais ne divisant pas c et l'ensemble S des diviseurs premiers de m divisant a et c. Comme m≠0, tous ces ensembles sont finis. Posons alors $x=\prod_{p\in R}p$ et $y=\prod_{p\in Q}p$. Comme $Q\cap R=\emptyset$, on obtient ainsi des entiers premiers entre eux. Mais le plus intéressant est que le nombre $n=ax^2+bxy+cy^2$ est alors premier avec m. Pour le voir il suffit de démontrer que n est premier avec p (donc non divisible par p) pour tout p∈P. Cela se fait très bien en considérant trois cas : p∈Q, p∈R, p∈S. C'est un excellent exercice d'arithmétique.

Après cela, il reste un dernier point à régler. Il n'est pas interdit en effet que n soit nul, mais si on remplace dès le début m par 2m, l'entier n que l'on obtient est premier avec m et impair, donc non nul. D'où le lemme.
On peut en tirer deux conséquences. La première est que toute forme primitive est équivalente à une forme (a,b,c) dont le coefficient initial a est un entier non nul qu'on peut choisir premier avec n'importe quel entier $m\neq 0$ donné à l'avance. On sait en effet (§A, n°15) que lorsqu'une forme f représente proprement un entier a, elle est équivalente à une forme dont le premier coefficient est a.
La seconde conséquence est que toute forme primitive est équivalente à une forme (a,b,c) pour laquelle a et c sont différents de 0. On peut en effet d'abord choisir $a\neq 0$ d'après ce qui précède. Ensuite, quitte à prendre des formes parallèles, on peut supposer qu'on dispose d'une forme du type $(a,b+2an,an^2+bn+c)$. D'où le résultat puisque le polynôme an^2+bn+c ne peut s'annuler plus de deux fois.

8. Ces préparatifs faits, nous allons voir d'abord que si f et f' sont des formes primitives de même discriminant, il existe des formes φ et φ' respectivement équivalentes à f et f', et composables entre elles. En outre, on peut s'arranger pour que les coefficients initiaux de ces formes soient des entiers non nuls, premiers entre eux, et premiers avec n'importe quel nombre m non nul donné à l'avance.
En effet, le nombre m étant donné, considérons un entier a non nul premier avec m et représenté proprement par f, puis un entier a' non nul premier avec am et représenté proprement par f' : on applique donc deux fois le lemme du n° précédent. Comme les représentations sont propres, il existe des entiers b, c et b', c' tels que f~(a,b,c) et f'~(a',b',c') (cf §A n°15). Il n'y a bien sûr aucune raison pour que b=b', mais sans changer les équivalences précédentes (ni a et a'), on peut remplacer b par n'importe quel nombre de la forme b+2ak et b' par n'importe quel nombre de la forme b'+2a'k' (cf §A, n°13 : formes "parallèles"). Nous allons voir qu'on peut choisir k et k' de telle façon que b+2ak=b'+2a'k'. Il revient au même de trouver un entier B tel que $B\equiv b \pmod{2a}$ et $B\equiv b' \pmod{2a'}$. Cet énoncé rappelle le théorème chinois sauf que si a et a' sont premiers entre eux, il n'en est pas de même de 2a et de 2a'. Heureusement pour nous, on sait que b et b' ont la même parité. On peut donc poser soit b=2β et b'=2β', soit b=2β+1 et b'=2β'+1, ce qui ramène aussitôt le problème à deux congruences simultanées de modules a et a', où le théorème chinois proprement dit fait merveille.
Moyennant quoi, en changeant de notation, on aura f~(a,b,c) et f'~(a',b',c'). comme a et a' sont des entiers non nuls premiers entre eux, les formes obtenues sont composables (n°4), tout en ayant les autres propriétés requises. CQFD.

9. Reste à voir que la forme composée φ*φ' se trouve dans une classe qui ne dépend que de la classe de φ et de la classe de φ'. Il revient au même de prouver que si f et f' sont des formes primitives composables, respectivement équivalentes à des formes (primitives) composables g et g', alors f*f' est équivalente à g*g'.
Nous aurons besoin d'un lemme.

Lemme : Soient (a_1,b,c_1) et (a_2,b,c_2) deux formes équivalentes de même coefficient central et soit d un diviseur commun non nul de c_1 et de c_2 tel que a_1, a_2 et d soient premiers dans leur ensemble. Alors les formes $(da_1,b,\frac{c_1}{d})$ et $(da_2,b,\frac{c_2}{d})$ sont équivalentes.

Les formes (a_1,b,c_1) et (a_2,b,c_2) étant équivalentes, il existe des entiers α, β, γ, δ tels que $\alpha\delta-\beta\gamma=1$ pour lesquels

$$\begin{pmatrix} a_2 & b/2 \\ b/2 & c_2 \end{pmatrix}=\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} a_1 & b/2 \\ b/2 & c_1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

(cf §A, n°8). En multipliant tout par 2 et par $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}^{-1}=\begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix}$, on obtient une nouvelle relation matricielle qui équivaut aux quatre égalités

$$(1)\quad \begin{cases} 2a_1\alpha+b\gamma=2a_2\delta-b\gamma \\ 2a_1\beta+b\delta=b\delta-2c_2\gamma \\ b\alpha+2c_1\gamma=-2a_2\beta+b\alpha \\ b\beta+2c_1\delta=-b\beta+2c_2\alpha \end{cases}$$

On tire des deux égalités du milieu $a_1\beta=-c_2\gamma$ et $a_2\beta=-c_1\gamma$. Comme d divise c_1 et c_2, d divise $a_1\beta$ et $a_2\beta$. Par suite, d divise le PGCD de ces deux derniers nombres, c'est à dire le produit de β et du PGCD de a_1 et de a_2. Comme d est premier avec ce PGCD par hypothèse, d divise β. Cela permet de considérer la matrice à coefficients entiers, et de déterminant +1

$$\begin{pmatrix} \alpha & \beta/d \\ d\gamma & \delta \end{pmatrix}$$

Le lemme sera établi si on démontre que

$$\begin{pmatrix} da_2 & b/2 \\ b/2 & c_2/d \end{pmatrix}=\begin{pmatrix} \alpha & d\gamma \\ \beta/d & \delta \end{pmatrix}\begin{pmatrix} da_1 & b/2 \\ b/2 & c_1/d \end{pmatrix}\begin{pmatrix} \alpha & \beta/d \\ d\gamma & \delta \end{pmatrix}$$

Un petit calcul (laissé au lecteur!) montre que cette relation équivaut à (1).

10. Ce lemme étant établi, plaçons-nous dans les hypothèses du résultat à démontrer : f et f' composables, g et g' composables, f~g et f'~g', ce qui implique que toutes les formes considérées ont le même discriminant Δ.

Posons f=(a,b,c), f'=(a',b,c'), g=(u,v,w), g'=(u',v,w').

D'après le n°8 ci-dessus, il existe deux autres formes composables $\varphi=(\alpha,\beta,\gamma)$ et $\varphi'=(\alpha',\beta,\gamma')$, respectivement équivalentes à f et f' (donc aussi à g et g') dont les coefficients initiaux α et α' sont des entiers non nuls, premiers entre eux et premiers avec aa'uu' (il résulte des hypothèses que aa'uu'≠0).

Nous allons démontrer que $\varphi*\varphi'\sim f*f'$ et $\varphi*\varphi'\sim g*g'$, ce qui établira la conclusion cherchée $f*f'\sim g*g'$.

Comme le problème est symétrique, on peut se contenter de démontrer que $\varphi*\varphi'\sim f*f'$, c'est à dire que

$$\left(\alpha\alpha',\beta,\frac{\beta^2-\Delta}{4\alpha\alpha'}\right)\sim\left(aa',b,\frac{b^2-\Delta}{4aa'}\right)$$

Comme αα' est premier avec aa' et que b et β ont la même parité, on démontre, comme on l'a fait plus haut (en distinguant deux cas et en appliquant le théorème chinois) qu'il existe un entier B tel que

$B\equiv\beta \pmod{2\alpha\alpha'}$ et $B\equiv b \pmod{2aa'}$

Comme ces congruences sont aussi valables modulo 2α, 2α', 2a et 2a', on peut affirmer en utilisant la notion de formes parallèles (cf §A, n°12) qu'il existe des entiers Γ, Γ', Γ'' et C, C', C'' tels que

$$(\alpha,\beta,\gamma)\sim(\alpha,B,\Gamma) \quad (\alpha',\beta,\gamma')\sim(\alpha',B,\Gamma') \quad (\alpha\alpha',\beta,\frac{\beta^2-\Delta}{4\alpha\alpha'})\sim(\alpha\alpha',B,\Gamma'')$$

$$(a,b,c)\sim(a,B,C) \quad (a',b,c')\sim(a',B,C') \quad (aa',b,\frac{b^2-\Delta}{4aa'})\sim(aa',B,C'')$$

toutes ces formes ayant Δ pour discriminant.

Il résulte des hypothèses que $(\alpha,B,\Gamma)\sim(a,B,C)$ et $(\alpha',B,\Gamma')\sim(a',B,C')$ et tout le problème est de faire voir que $(\alpha\alpha',B,\Gamma'')\sim(aa',B,C'')$.

Comme $B^2-4\alpha\alpha\Gamma''=\Delta$, on voit que $4\alpha\alpha'$ divise $B^2-\Delta$, donc en particulier $4\alpha'\Gamma'$ et $4a'C'$. On en déduit que α divise $\alpha'\Gamma'$ et $a'C'$. Comme α est premier avec α' et avec a', α divise Γ' et C', tout en étant premier avec le PGCD de α' et de a'.

On est donc dans les conditions d'application du lemme du n°9 : puisque $(\alpha',B,\Gamma')\sim(a',B,C')$, on en déduit que $(\alpha\alpha',B,\frac{\Gamma'}{\alpha})\sim(\alpha a',B,\frac{C'}{\alpha})$ c'est à dire, puisque $(\alpha\alpha',B,\frac{\Gamma'}{\alpha})$ est nécessairement identique à $(\alpha\alpha',B,\Gamma'')$, que l'on a

(2) $\quad(\alpha\alpha',B,\Gamma'')\sim(\alpha a',B,\frac{C'}{\alpha})$

On voit de la même façon (puisque $B^2-4aa'C''=\Delta$) que 4aa' divise $B^2-\Delta$. Si on remarque que

$B^2-\Delta=4\alpha\Gamma=4aC$, on en déduit que a' divise C et αΓ, donc Γ seul puisque a' est premier avec α. Comme a' est à fortiori premier avec le PGCD de α et de a, on peut appliquer le lemme aux formes (α,B,Γ) et (a,B,C) : on a $(\alpha a',B,\frac{\Gamma'}{a'})\sim(aa',B,\frac{C}{a'})$.

Comme $(aa',B,\frac{C}{a'})=(aa',B,C'')$ et $(\alpha a',B,\frac{\Gamma}{a'})=(\alpha a',B,\frac{C'}{\alpha})$ puisqu'il y a partout le même discriminant, on voit que

(3) $\quad(\alpha a',B,\frac{C'}{\alpha})\sim(aa',B,C'')$

Le rapprochement de (2) et de (3) donne le résultat cherché. CQFD.

11. Comme on l'a énoncé, les résultats précédents permettent de définir sans ambiguïté le composé de deux classes Φ et Φ' de formes primitives de discriminant Δ, lorsque Δ est un entier $\equiv 0,1 \pmod 4$ donné : on choisit une forme f dans Φ et une forme f' dans Φ' de telle sorte que f et f' soient composables (n°8) et on considère la classe de la forme composée f*f'. Comme cette classe ne dépend que de Φ et de Φ', on dira que c'est la classe composée de Φ et de Φ' ; on la notera provisoirement Φ*Φ'. Comme ce résultat est une classe de formes primitives de discriminant Δ (n°6), cela définit dans l'ensemble

$G(\Delta)$ de ces classes une loi de composition qu'on appellera en abrégé la *composition des classes*.

Le résultat fondamental est, bien sûr, que, pour cette loi très spéciale, $G(\Delta)$ est un groupe commutatif. Dans ce groupe, l'élément neutre est la classe principale (de discriminant Δ) et le symétrique de la classe d'une forme (a,b,c) est la classe de la forme inverse (c,b,a). La commutativité est évidente.

Pour démontrer l'associativité, considérons comme il se doit trois classes Φ, Φ' et Φ'' appartenant à $G(\Delta)$. Choisissons une première forme $f=(a,b,c)$ dans Φ dont le coefficient initial a n'est pas nul, puis une forme $f'=(a',b',c')$ dans Φ' dont le coefficient initial a' est un entier non nul premier avec a et enfin une forme $f''=(a'',b'',c'')$ dans Φ'' dont le coefficient initial a'' est un entier non nul premier avec aa'. Tout cela est possible en faisant appel aux résultats exposés ci-dessus dans le n°7. En appliquant ensuite un raisonnement fait plus haut (mais ici avec trois congruences), on peut démontrer qu'il existe un entier B tel que $B\equiv b \pmod{2a}$, $B\equiv b' \pmod{2a'}$ et $B\equiv b'' \pmod{2a''}$ (cf n°8).

Sans changer alors les classes Φ, Φ' et Φ'', on peut donc supposer que les formes f, f' et f'' ont le même coefficient central B qu'on écrira en fait b, de sorte que

$$f=(a,b,c),\ f'=(a',b,c'),\ f''=(a'',b,c'')$$

En utilisant alors les résultats du début du n°4, on voit aisément que f et f' sont composables et que $f*f'=(aa',b,\frac{b^2-\Delta}{4aa'})$, puis que f*f' est composable avec f'' et que $(f*f')*f''=(aa'a'',b,\frac{b^2-\Delta}{4aa'a''})$.

Mais un raisonnement semblable conduit à montrer que la composée $f*(f'*f'')$ est définie et que l'on a aussi $f*(f'*f'')=(aa'a'',b,\frac{b^2-\Delta}{4aa'a''})$

D'où l'égalité $(f*f')*f''=f*(f'*f'')$ et, en passant aux classes, la relation $(\Phi*\Phi')*\Phi''=\Phi*(\Phi'*\Phi'')$ qu'il fallait démontrer.

Le reste de la démonstration n'est pas difficile (donc laissée au lecteur) : on aura simplement à représenter la classe principale par une forme du type $(1,b,\frac{b^2-\Delta}{4})$ et dans le cas des formes inverses (a,b,c) et (c,b,a) à se ramener au cas où $ac\neq 0$ (cf la fin du n°7).

12. Le groupe $G=G(\Delta)$ obtenu est fini, d'ordre $g=g(\Delta)$ (cf §A, n°20). Dans la suite, on notera multiplicativement la composition des classes dans $G(\Delta)$, ce qui permettra de parler du "produit" $\Phi\Phi'$ de deux classes, de la classe "unité" et de la classe "inverse" Φ^{-1} d'une classe Φ donnée.

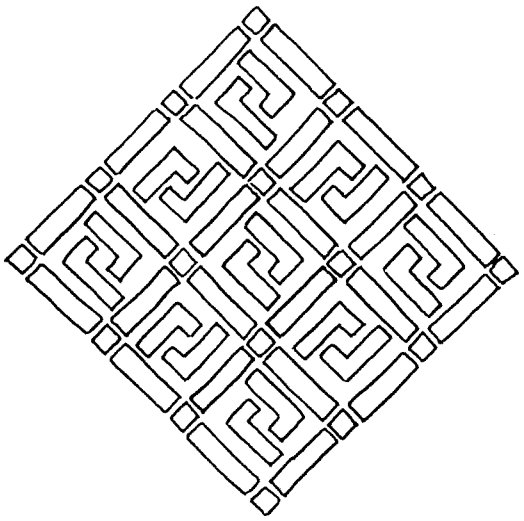
Il est alors clair qu'une classe ambiguë primitive de discriminant Δ apparaît maintenant comme un élément $\Phi\in G(\Delta)$ tel que $\Phi=\Phi^{-1}$ (cf §A, n°11). Il revient au même de dire que $\Phi^2=1$.

Ces éléments Φ de $G(\Delta)$ forment évidemment un sous-groupe qu'on notera $A(\Delta)$ et dont on a calculé l'ordre, du moins dans le cas où Δ impair et négatif : il est égal à 2^r où r est le nombre de diviseurs premiers de Δ (cf §B, n°11).

Tous ces résultats nous serviront dans l'étude de ce que Gauss a appelé les "genres de formes" - mais cela est une autre histoire qu'on verra dans un prochain numéro!
Pour le lecteur qui voudrait un exemple concret de groupes de classes de formes primitives de discriminant Δ (on dira simplement "groupe de classes"...), nous lui conseillons de reprendre le cas où Δ=-63 (cf §B, n°10 et n°11). Il devrait trouver un groupe d'ordre 8 produit direct d'un groupe d'ordre 2 (engendré par (-1,-1,-16) et d'un groupe cyclique d'ordre 4 (engendré par (2,1,8)).

Livres cités dans le texte :

[BUE] Duncan E. BUELL, *Binary Quadratic Forms, Classical Theory and Modern Computations*, Springer Verlag, 1989.
[CAS] J.W.S. CASSELS, *Rational Quadratic Forms*, Academic Press, 1978.
[DIE] Jean DIEUDONNE (sous la direction de), *Abrégé d'histoire des mathématiques*, 1700-1900, vol.I, Hermann, 1978. Il y a maintenant une nouvelle édition regroupant les deux volumes de 1978.
[GAU] Carl Friedrich GAUSS, *Recherches arithmétiques* (traduction française de *Disquisitionnes Arithmeticae*, par A.-C.-M. Poullet - Delisle), réimpression éditions Jacques Gabay, 1989.
[VEN] B.A. VENKOV, *Elementary number Theory*, Walters - Noordhoff Publishing Groningen, 1970.
[WEI] André WEIL, *Number Theory, An approach through history, From Hammurapi to Legendre*, Birkhäuser, 1984.



Motif utilisé dans l'art 'bakuba'
(extrait du livre de Claudia Zaslavsky "Africa counts"
Boston, Prindle, Weber & Schmidt, 1973).