EVPHKA! num = $\Delta + \Delta + \Delta$

Marc Guinot

(deuxième partie)

Après avoir étudié dans une première partie les classes de formes quadratiques et leur composition, nous allons voir comment la notion de genre introduite par Gauss dans ses *Disquisitiones* permet, moyennant un petit détour par les formes ternaires et les sommes de trois carrés, de démontrer que tout nombre entier naturel est une somme de trois nombres triangulaires. Après les trois paragraphes A/, B/ et C/ de la première partie, voici donc la suite, c'est-à-dire D/, E/ et F/.

D/ Genre d'une forme quadratique.

1. C'est dans les articles 228 et suivants de ses *Disquisitiones Arithmeticae* que Gauss définit le genre d'une forme dans le but de caractériser autant que faire se peut les nombres représentés par cette forme. En se limitant aux formes primitives (ce qu'on peut toujours faire), il a découvert un ensemble de conditions nécessaires remplies par ces nombres. Ces conditions l'ont conduit à définir ce qu'il a appelé les «caractères» d'une forme, puis à ranger dans une même catégorie, appelée «genre», les formes de mêmes caractères, le résultat essentiel étant que deux formes qui ne sont pas rangées dans le même genre ne peuvent pas représenter les mêmes entiers. L'idéal serait que, réciproquement, deux formes rangées dans le même genre représentent les mêmes entiers; cela n'est malheureusement vrai que dans certains cas.
Il n'empêche que la notion de genre permet de résoudre un certain nombre de problèmes qui seraient inaccessibles sans celle–ci. Pour les besoins de notre cause (les nombres triangulaires!) nous pourrons nous contenter de définir le genre d'une forme f dans le cas où le discriminant Δ de cette forme est impair (cas où l'on dit que la forme est impaire). Rappelons que, paradoxalement, Gauss a écarté d'emblée ces formes dans son étude, ce qui l'a obligé à introduire, pour définir certains genres, la notion biscornue de formes «improprement équivalentes» (cf. [GAU], p.228). N'ayant pas les mêmes préjugés que Gauss, notre tâche en sera simplifiée.

2. Dans toute la suite, nous nous limiterons aux formes impaires, supposées en outre primitives.
Considérons d'abord un facteur premier p du discriminant Δ d'une forme f de cette sorte. Puisque Δ est supposé impair, on a $p \neq 2$. Parmi les entiers représentés par f, écartons ceux qui sont divisibles par p. Les entiers qui subsistent (et qui forment un ensemble non vide d'après un résultat vu dans la première partie, §C, n°7) ont alors une propriété commune liée à la notion de résidu quadratique modulo p. Cette notion, familière à Euler, Lagrange et Legendre, s'exprime en disant qu'un entier n, non divisible par p, est *résidu quadratique modulo p* (ou par abus de langage *résidu quadratique de p*) si n est congru à un carré modulo p. Dans le cas contraire, on dit que n est un *résidu non*

quadratique de p ou même parfois un *non résidu*. Si on remplace les entiers n par leurs classes modulo p, donc l'anneau $\mathbb{Z}$ par le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (corps fini à p éléments), les résidus quadratiques ne sont rien d'autres que les carrés du groupe $\mathbb{F}_p^*$.

3. On comprend mieux les propriétés des résidus quadratiques en introduisant ce qu'on appelle le *symbole de Legendre*, noté $\left(\frac{n}{p}\right)$, qui vaut +1 si n est un résidu quadratique de p, et −1 sinon, le nombre n étant dans tous les cas un entier non divisible par p. On dit parfois que $\left(\frac{n}{p}\right)$ est le *caractère quadratique* de n par rapport à p.

Il est immédiat, en premier lieu que

$$(1) \qquad \left(\frac{n}{p}\right) = +1 \text{ si n est un carré parfait}$$

que

$$(2) \qquad \left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right) \text{ si } n \equiv n' \pmod{p}$$

et facile de voir (à cause des propriétés des carrés dans $\mathbb{F}_p^*$) que

$$(3) \qquad \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right) = \left(\frac{nn'}{p}\right)$$

étant entendu que dans toutes ces relations ni n ni n' ne sont divisibles par p.

Les travaux d'Euler sur les sommes de deux carrés ont conduit ce dernier à démontrer que −1 est résidu quadratique de tout nombre premier p de la forme 4k+1 et non résidu de tout nombre premier p de la forme 4k+3. Avec le symbole de Legendre, on peut exprimer ce résultat par la relation

$$(4) \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

puisque $\frac{p-1}{2} = 2k$ dans le premier cas et $\frac{p-1}{2} = 2k+1$ dans le second.

Plus compliquée est la détermination du caractère quadratique de 2. On a en fait la formule

$$(5) \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

qui signifie, si on regarde bien, que 2 est résidu quadratique des nombres premiers de la forme 8k±1 et non résidu des nombres premiers de la forme 8k±3.

4. Mais la propriété la plus importante, subodorée par Euler et énoncée explicitement par Legendre, est la *loi de réciprocité quadratique* selon laquelle deux nombres premiers distincts p et q ont, l'un par rapport à l'autre, le même caractère quadratique sauf si p et q sont tous deux de la forme 4k+3. En d'autres termes, on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ si l'un au moins des nombres p ou q est de la forme 4k+1 et $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ sinon.

Cette propriété peut s'exprimer aussi par la relation

$$(6) \qquad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Malgré ses efforts, Legendre ne parvint pas à démontrer convenablement cette loi et c'est Gauss qui en donna les deux premières démonstrations dans ses *Disquisitiones* ([GAU], p.136 et p.298). Par la suite, il en imagina plusieurs autres : la troisième (assez élémentaire) et la quatrième (fondée sur les «sommes de Gauss») sont les plus connues.
On trouvera une démonstration de la loi de réciprocité quadratique, assez simple et apparentée à la troisième démonstration de Gauss, dans [ITA], p.76.

5. Le symbole de Legendre a été étendu par Jacobi de manière à laisser inchangées la plupart des relations précédentes, tout en facilitant les calculs. Ce *symbole de Jacobi*, défini pour tout entier impair a>0 et tout entier n non nul premier à a, s'obtient en décomposant a en facteurs premiers, donc en écrivant $a = p_1 \ldots p_r$ où tous les nombres p_i sont premiers (impairs) mais non nécessairement distincts, et en faisant le produit des symboles de Legendre correspondants, ce qui donne $\left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_r}\right)$. Si a est réduit à un seul facteur premier, on retrouve ainsi le symbole de Legendre – ce qui fait qu'il n'y a aucun inconvénient à noter $\left(\frac{n}{a}\right)$ le symbole de Jacobi en général.

Comme le symbole de Legendre, le symbole de Jacobi vaut +1 ou −1, mais s'il vaut +1 lorsque n est congru à un carré modulo a, la réciproque n'est pas nécessairement vraie comme on le voit facilement, de sorte que la relation $\left(\frac{n}{a}\right) = +1$ ne caractérise pas les «résidus quadratiques» de a.

6. Cela étant, les relations (1) et (6) se généralisent facilement (mais c'est un peu fastidieux à démontrer) pour donner les relations analogues suivantes :

$$(1') \qquad \left(\frac{n}{a}\right) = +1 \text{ si n (premier avec a) est un carré}$$

$$(2') \qquad \left(\frac{n}{a}\right) = \left(\frac{n'}{a}\right) \text{ si } n \equiv n' \pmod{a}$$

$$(3') \qquad \left(\frac{n}{a}\right)\left(\frac{n'}{a}\right) = \left(\frac{nn'}{a}\right)$$

$$(4') \qquad \left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}$$

$$(5') \qquad \left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$$

étant entendu que dans (2') et (3'), n et n' sont premiers avec a. Enfin, la loi de réciprocité quadratique se généralise le plus naturellement du monde :

$$(6') \qquad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

si a et b sont des entiers impairs positifs premiers entre eux.

7. Il nous sera commode de généraliser encore un tout petit peu cela en posant $\left(\frac{n}{-a}\right)=\left(\frac{n}{a}\right)$. Avec cette convention, on a $\left(\frac{n}{a}\right)=\left(\frac{n}{|a|}\right)$ si a est un entier impair de signe quelconque et si n est un entier non nul premier avec a. Les formules (1'), (2'), (3') et (5') restent alors valables sans changement, alors que (4') prend la forme

$$(7) \qquad \left(\frac{-1}{a}\right)=(-1)^{\frac{|a|-1}{2}}$$

Quant à la loi de réciprocité quadratique, elle devra s'écrire désormais

$$(8) \qquad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

si l'un au moins des entiers a ou b est >0, et

$$(9) \qquad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=-(-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

sinon – étant entendu que a et b sont des entiers impairs premiers entre eux.
Pour établir ces formules, à partir de celles énoncées dans le n°6, le lecteur vérifiera que $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\frac{|b|+1}{2}}$ si a>0 et b<0 et que $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{|a|-1}{2}\frac{|b|-1}{2}+\frac{|a|-1}{2}\frac{|b|-1}{2}}$ si a<0 et b<0

8. Revenons aux formes primitives de discriminant impair et aux entiers non divisibles par p représentés par ces formes. La propriété commune de ces entiers est qu'ils ont le même caractère quadratique vis–à–vis de p, ce qui veut dire que si f est une forme donnée (ayant les propriétés indiquées), alors $\left(\frac{n}{p}\right)=\left(\frac{n'}{p}\right)$ pour tout couple (n,n') d'entiers non divisibles par p, représentés par f.
En d'autres termes, ou bien les entiers en question sont tous des résidus quadratique de p, ou bien ce sont tous des non résidus.
La démonstration de ce résultat est facile, en partant de l'hypothèse qu'il existe des entiers α, γ et β, δ tels que $n = f(\alpha,\gamma)$ et $n' = f(\beta,\delta)$. Si on considère, en effet, la transformation linéaire $\tau = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, celle–ci transforme f en une forme g dont le premier coefficient est $f(\alpha,\gamma) = n$ et le dernier $f(\beta,\delta) = n'$. On voit que g est du type (n,ℓ,n'). Mais on sait en outre, en vertu d'une remarque faite à la fin du n°10, §A, que le discriminant de g est égal à Δd^2 où d est le déterminant de τ. On a donc $\ell^2-4nn' = \Delta d^2$, ce qui prouve, entre autres choses, que $\ell^2 \equiv 4nn' \pmod p$. On en déduit que $\left(\frac{4nn'}{p}\right) = +1$. Comme $\left(\frac{4nn'}{p}\right)=\left(\frac{4}{p}\right)\left(\frac{n}{p}\right)\left(\frac{n'}{p}\right)$ et que $\left(\frac{4}{p}\right)=+1$, on en déduit que $\left(\frac{n}{p}\right)=\left(\frac{n'}{p}\right)$. CQFD.

9. Ainsi, le symbole de Legendre $\left(\frac{n}{p}\right)$ d'un entier n (non divisible par p) représenté par f est un nombre, valant +1 ou −1, qui ne dépend pas de n, mais seulement de la forme f (et

aussi, bien sûr, du facteur premier p de Δ considéré). On le notera $\chi_p(f)$ et on dira que c'est le *caractère de* f *relatif à* p.
On peut calculer ce caractère assez simplement en observant que parmi les nombres n en question, il y a l'un au moins des coefficients extrêmes a ou c de la forme : ces deux entiers sont en effet représentés par p et s'ils étaient tous les deux divisibles par p, b le serait aussi (à cause de la relation $b^2 = 4ac+\Delta$), en contradiction avec le fait que f est une forme primitive par hypothèse.

10. Lorsque p parcourt l'ensemble P des diviseurs premiers de Δ, les nombres $\chi_p(f)$ forment une famille finie (qu'on peut considérer comme une suite en rangeant les nombres $p\in P$ d'une certaine manière), que certains auteurs appellent le *système des caractères* de f, que Gauss nomme le «caractère complet» de la forme, et que nous appellerons plus volontiers la *signature* de f (les valeurs +1 et −1 des différents caractères de f pouvant être symbolisés par les signes + et −). Cela étant, on dira que deux formes primitives f et g, de même discriminant impair Δ, sont *du même genre* si elles ont la même signature, autrement dit, en bref, si elles ont les mêmes caractères.
Considérons à titre d'exemples les formes f = (1,1,16), g = (2,1,8) et h = (4,1,4) toutes primitives et de discriminant −63 (cf. §B, n°10). Comme $-63 = -3^2\times 7$, chacune de ces formes a deux caractères, l'un relatif à 3, l'autre relatif à 7. Comme elles représentent les entiers 1, 2 et 4 respectivement, et que ces nombres ne sont ni divisibles par 3 ni divisibles par 7, on a

$$\chi_3(f) = \left(\frac{1}{3}\right) = +1 \qquad \chi_7(f) = \left(\frac{1}{7}\right) = +1 \qquad \text{à cause de (1)}$$

$$\chi_3(g) = \left(\frac{2}{3}\right) = -1 \qquad \chi_7(g) = \left(\frac{2}{7}\right) = +1 \qquad \text{à cause de (5)}$$

$$\chi_3(h) = \left(\frac{4}{3}\right) = +1 \qquad \chi_7(h) = \left(\frac{4}{7}\right) = +1 \qquad \text{à cause de (1)}$$

Cela montre que f et h sont du même genre, alors que g est d'un genre différent. Si on remplace f par −f = (−1,−1,−16), on a

$$\chi_3(-f) = \left(\frac{-1}{3}\right) = -1 \qquad \chi_7(-f) = \left(\frac{-1}{7}\right) = -1 \qquad \text{à cause de (4)}$$

ce qui donne un troisième genre, différent des deux autres.

11. Si on revient au cas général, on constate que la définition des différents caractères d'une forme ne fait intervenir que les nombres représentés par cette forme, du moins à un détail près, lié au discriminant, ce qui n'empêche pas de pouvoir affirmer que deux formes de même discriminant qui représentent les mêmes nombres ont la même signature, donc le même genre.
En particulier, deux formes primitives équivalentes (de discriminant impair) sont du même genre.
On peut dire aussi, pour exprimer ce résultat général, que deux formes qui ne sont pas du même genre ne peuvent pas représenter les mêmes entiers.
On notera cependant que les formes f = (1,1,16) et h = (4,1,4) vues ci–dessus (n°10), bien que du même genre, ne représentent pas les mêmes nombres car la seconde

représente 7 (avec x = 1 et y = −1) alors que si on avait $x^2+xy+16y^2 = 7$, on aurait $\left(x+\frac{1}{2}y\right)^2 + \frac{63}{4}y^2 = 7$, d'où nécessairement y = 0 et $x^2 = 7$, ce qui est absurde.
Tout cela est conforme à ce que nous avions dit en introduction (n°1).

12. La relation qui exprime que deux formes primitives impaires de même discriminant Δ sont du même genre est évidemment une relation d'équivalence. On peut donc définir *le genre d'une forme* f donnée comme la classe de f pour cette relation d'équivalence et les *genres* en général comme les classes d'équivalence se rapportant à cette relation. Ces genres forment donc une partition de l'ensemble des formes primitives de discriminant Δ.
D'après ce qu'on a expliqué dans le précédent numéro, la relation d'équivalence en question est «moins fine» que l'équivalence au sens de Gauss. Cela entraîne 1°/ que toute classe de formes primitives de discriminant Δ (au sens de Gauss) est contenue dans un genre et dans un seul : cela permet de parler sans ambiguïté *du genre* d'une classe ou si on préfère, *de la signature* de cette classe, 2°/ que n'importe quel genre de formes (primitives et de discriminant Δ) est la réunion d'un certain nombre de classes, ce nombre étant d'ailleurs nécessairement fini d'après ce qu'on a vu dans le §A, 3°/ que le nombre total de genres relatifs à un discriminant (impair) donné est lui–même fini (ce qui peut se voir aussi directement à partir des définitions).
L'exemple des formes f = (1,1,16) et h = (4,1,4) (qui ne sont pas équivalentes car ce sont des formes réduites distinctes : §B, n°10) montre qu'un genre peut contenir plusieurs classes. Dans certains cas, cependant, il peut n'y en avoir qu'une seule.

13. Considérons maintenant, pour un discriminant Δ impair fixé (donc un entier $\equiv 1 \pmod 4$), la forme principale de discriminant Δ. Cette forme s'écrit, par définition, $f = \left(1,1,\frac{1-\Delta}{4}\right)$, ce qui montre qu'elle est primitive et qu'elle représente 1. Comme 1 n'est divisible par aucun nombre premier p divisant Δ, on peut s'en servir pour déterminer la signature de f. On a en fait $\chi_p(f) = \left(\frac{1}{p}\right) = +1$ en vertu de (1) (n°3). En d'autres termes, la signature de la forme principale de discriminant Δ n'est constituée que de signes +.
On appelle *genre principal* de discriminant Δ le genre de la forme principale. C'est donc aussi l'ensemble des formes de discriminant Δ dont la signature n'est constituée que de signes +. Le genre principal contient la classe principale, mais comme le montre un exemple déjà vu, il peut en contenir d'autres.

14. Si f = (a,b,c) est une forme primitive quelconque (de discriminant Δ impair) il peut être intéressant de comparer le genre de f avec celui de la forme inverse f^{-1} = (c,b,a) (on prendra garde à la notation, particulièrement audacieuse) et celui de la forme opposée −f = (−a,−b,−c). Dans le premier cas, il n'y a rien de bien transcendant : comme f et f^{-1} représentent les mêmes nombres (ce sont des formes équivalentes au sens de Lagrange : cf. §A, n°10), ces formes sont du même genre. Dans le second cas, il s'agit de comparer $\chi_p(f)$ et $\chi_p(-f)$ pour tout nombre premier p divisant Δ. Si n est un entier représenté par f

et non divisible par p, −n est représenté par −f (tout en restant non divisible par p). On a donc $\chi_p(f) = \left(\frac{n}{p}\right)$ et $\chi_p(-f) = \left(\frac{-n}{p}\right)$. Comme $\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{n}{p}\right)$, on voit d'après (4), n°3, que $\chi_p(-f) = \chi_p(f)$ si p est de la forme 4k+1 et que $\chi_p(-f) = -\chi_p(f)$ si p est de la forme 4k+3.
En d'autres termes, pour passer de la signature de f à celle de −f, on change les signes correspondant aux caractères relatifs aux facteurs premiers de Δ de la forme 4k+3, mais pas les autres. Bien sûr, il se peut que Δ n'ait pas de facteurs premiers de la forme 4k+3, auquel cas f et −f sont à ranger dans le même genre. Mais le phénomène ne se produit pas si Δ<0 car comme la décomposition en facteurs premiers de Δ s'écrit alors $\Delta = -p_1^{n_1}\ldots p_r^{n_r}$, on a $p_1^{n_1}\ldots p_r^{n_r} = -\Delta \equiv 3 \pmod 4$, ce qui rend impossible l'absence de nombre $p_1, \ldots, p_r$ de la forme 4k+3. Pour Δ<0, les formes f et −f sont donc dans deux genres différents.
On notera que ce résultat n'interdit pas, *a priori*, l'existence dans un même genre de formes positives et de formes négatives. Nous verrons cependant plus loin (cf. n°19) que cela est impossible.

15. Considérons pour finir deux formes impaires primitives composables f et f'. Il est alors normal de chercher à calculer la signature de la forme composée (primitive et de même discriminant) f∗f'.
Si p est un diviseur premier de Δ et si n (resp. n') est un entier non divisible par p, représenté par f (resp. par f'), on a $\chi_p(f) = \left(\frac{n}{p}\right)$ et $\chi_p(f') = \left(\frac{n'}{p}\right)$ par définition. Mais on sait (cf. §C, n°5) que nn' (qui est un entier également non divisible par p) est représenté par f∗f'. On a donc, toujours par définition, $\chi_p(f*f') = \left(\frac{nn'}{p}\right)$. Comme $\left(\frac{nn'}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right)$, on a alors la remarquable relation $\chi_p(f*f') = \chi_p(f)\chi_p(f')$.
On peut donc dire, en général, que lorsque f et f' sont des formes primitives composables, la signature de f∗f' s'obtient à partir des signatures de f et de f' en multipliant celles-ci terme à terme.

16. Il serait criminel de ne pas tirer le maximum de renseignements de ce dernier théorème. Pour cela, rappelons que la notion de signature peut être attachée à une classe de formes au lieu de l'être à une forme seule (cf. n°12) ; observons que si P désigne l'ensemble des diviseurs premiers de Δ, la signature en question, qui se présente sous la forme d'une famille $(\chi_p(f))_{p\in P}$ d'entiers égaux à +1 ou à −1, est un élément de l'ensemble produit $\{-1,+1\}^P$, ensemble que l'on peut identifier à $\{-1,+1\}^r$ où r est le nombre d'éléments de P, et qui est naturellement doté d'une structure de groupe multiplicatif ; souvenons-nous enfin que l'ensemble G = G(Δ) des classes de formes primitives de discriminant Δ est lui-même un groupe, pour une multiplication qui dérive de la composition des formes.
Bref, le lecteur l'aura compris, si on associe à toute classe primitive de discriminant Δ sa signature, on définit de cette manière un homomorphisme u du groupe G dans le groupe $\{-1,+1\}^P$.

On en déduit que
1°/ les classes contenues dans le genre principal constituent un sous–groupe G' de G, noyau de l'homomorphisme précédent : cela résulte de la définition même du genre principal (n°13) ;
2°/ les classes contenues dans un genre donné constituent, au sens de la théorie des groupes, une classe dans G modulo G' : c'est une propriété bien connue selon laquelle si $h:\Gamma\to\Gamma'$ est un homomorphisme de groupes, alors les ensembles non vides de la forme $h^{-1}(x')$ (où $x'\in\Gamma'$) sont les classes modulo Ker h dans Γ ;
3°/ le nombre de classes contenues dans un genre donné (de discriminant Δ) est le même pour tous les genres ; c'est en particulier le nombre de classes du genre principal, autrement dit l'ordre du groupe G' et par conséquent un diviseur $g' = g'(\Delta)$ de l'ordre g de G : on sait en effet que dans un groupe fini, le nombre d'éléments d'une classe modulo un sous–groupe H est égal à l'ordre de H ;
4°/ le nombre $\gamma = \gamma(\Delta)$ de genres relatifs à un discriminant Δ est une puissance de 2. De façon plus précise, si r désigne le nombre d'éléments de P c'est–à–dire le nombre de diviseurs premiers de Δ, γ est un diviseur de 2^r, égal à l'ordre du groupe quotient G/G', donc égal à g/g' : en effet, le nombre γ de tous les genres possibles de discriminant Δ est égal au nombre de signatures distinctes de toutes les formes (ou de toutes les classes) primitives de discriminant Δ ; c'est donc le nombre d'éléments de u(G) = Im u. Comme Imu est un sous–groupe du groupe $\{-1,+1\}^P$ donc l'ordre est 2^r, le nombre en question est bien un diviseur de 2^r, égal à l'ordre g/g' de G/G' puisque G/G' = G/Ker u est isomorphe, comme il est bien connu, à Im u.
Tous ces résultats figurent peu ou prou dans les *Disquisitiones Arithmeticae*, mais évidemment dans un langage qui n'est pas et qui ne pouvait pas être celui de la théorie des groupes. Néanmoins, certains des raisonnements que fait Gauss à cette occasion sont des anticipations assez nettes de raisonnements classiques de cette théorie (voir par exemple [GAU], p.277).

17. La question qui reste pendante est celle du calcul du nombre exact γ de genres. Le mieux serait que celui–ci soit 2^r, mais on va démontrer qu'à cause de la loi de réciprocité quadratique, cela n'est pas toujours vrai.
Quoi qu'il en soit, dire que le nombre de genres est égal à 2^r revient à dire que l'homomorphisme $u : G\to\{-1,+1\}^P$ défini dans le numéro précédent est surjectif, autrement dit que tout système de r "signes" $(\varepsilon_p)_{p\in P}$ (avec $\varepsilon_p = \pm 1$) peut être considéré comme la signature d'une forme de discriminant Δ, donc comme définissant un genre. Nous verrons plus loin (en fait dans le §E) que ce théorème d'existence pour les genres est valables si $\Delta<0$ (et impair).
Auparavant, pour comprendre le rôle joué par la loi de réciprocité quadratique dans cette question, considérons à côté d'un discriminant Δ impair et d'une forme primitive f de discriminant Δ, un entier n, premier avec 2Δ (donc impair), et représenté proprement par f : l'existence d'au moins un entier de ce genre est assuré comme on l'a vu dans le n°7 du §C. Par construction, si $p\in P$, n ne peut être divisible par p. On a donc $\chi_p(f) = \left(\frac{n}{p}\right)$. D'un

autre côté, comme n est représenté proprement par f il existe une forme f' équivalente à f et qu'on peut écrire (n,n',n") où n' et n" sont des entiers dont on ne sait pas grand chose sinon qu'ils vérifient la relation $n'^2-4nn" = \Delta$. Cela montre cependant que Δ est un carré modulo n. D'après les propriétés du symbole de Jacobi, généralisé à des entiers de signes quelconques, on a $\left(\frac{\Delta}{n}\right) = +1$. Appliquons alors à ce symbole de Jacobi la loi de réciprocité, c'est-à-dire les formules (8) et (9) du n°7 : compte tenu du fait que Δ est congru à 1 modulo 4, on voit que $\left(\frac{\Delta}{n}\right) = \left(\frac{n}{\Delta}\right)$ si l'un au moins des nombres n et Δ est positif et que $\left(\frac{\Delta}{n}\right) = -\left(\frac{n}{\Delta}\right)$ si les deux nombres sont négatifs. On a donc $\left(\frac{n}{\Delta}\right) = -1$ si n et Δ sont tous deux négatifs (ce qui veut dire que f est une forme définie négative) et $\left(\frac{n}{\Delta}\right) = +1$ dans tous les autres cas. Or $\left(\frac{n}{\Delta}\right)$ peut être calculé en décomposant Δ (ou plutôt |Δ| en facteurs premiers). Si on écrit cette décomposition sous la forme $p_1^{n_1}...p_r^{n_r}$, avec les conventions habituelles, on a $\left(\frac{n}{\Delta}\right) = \left(\frac{n}{|\Delta|}\right) = \left(\frac{n}{p_1}\right)^{n_1}...\left(\frac{n}{p_r}\right)^{n_r}$. Lorsque l'exposant n_i est pair, le facteur correspondant $\left(\frac{n}{p_i}\right)^{n_i}$ vaut +1, de sorte qu'on peut le supprimer. Il ne reste alors dans le produit, que les facteurs $\left(\frac{n}{p_i}\right)^{n_i}$ avec n_i impair, facteurs qui se réduisent d'ailleurs eux-mêmes à $\left(\frac{n}{p_i}\right)$. Si on appelle Q l'ensemble des diviseurs premiers p de Δ apparaissant avec un exposant impair dans la décomposition de Δ en facteurs premiers, on voit donc que $\left(\frac{n}{\Delta}\right) = \prod_{p\in Q}\left(\frac{n}{p}\right)$. Cela donne, en définitive, entre les caractères de f une «relation de dépendance» qu'on peut présenter sous la forme

$$(10) \qquad \prod_{p\in Q}\chi_p(f) = \begin{cases} -1 \text{ si f est une forme définie négative} \\ +1 \text{ dans tous les autres cas} \end{cases}$$

18. Cette «relation de dépendance» peut être parfaitement illusoire car il n'est pas interdit que Q soit vide. Cela ne se produit cependant pas si f est une forme définitive négative car un produit vide ne saurait être égal à −1. Plus généralement, cela ne peut se produire si $\Delta<0$ car en prenant pour f la forme $(-1,-1,\frac{\Delta-1}{4})$ (qui est négative), on obtient le premier cas de (10).

En revanche, si on suppose que $\Delta>0$, il n'est pas interdit que Q soit vide. Mais cela n'arrive que si tous les exposants de la décomposition en facteurs premiers de Δ sont pairs, donc seulement si Δ est un carré parfait.

Ainsi, en dehors de ce dernier cas, la relation (10) prend tout son sens.

19. La relation (10) a deux conséquences remarquables.
La première est que comme nous l'avions annoncé, un genre de discriminant impair Δ négatif ne peut renfermer à la fois une forme positive et une forme négative. en effet, si $(\varepsilon_p)_{p\in P}$ est la signature de la forme en question, l'existence des deux types de formes dans le genre impliquerait à la fois $\prod_{p\in Q}\varepsilon_p = -1$ et $\prod_{p\in Q}\varepsilon_p = +1$.
La seconde conséquence que l'on peut tirer de (10) est que si Δ est un discriminant impair positif, sans être un carré parfait, alors le nombre γ des genres relatifs à Δ est inférieur ou égal à 2^{r-1} (r étant comme ci–dessus, le nombre des diviseurs premiers de Δ). En effet, dans ce cas, la relation (10), qui s'écrit ici $\prod_{p\in Q}\chi_p(f) = +1$, et le fait que Q n'est pas vide empêchent d'avoir comme signature n'importe quelle famille $(\varepsilon_p)_{p\in P}$. D'où le résultat puisque γ est un diviseur de 2^r.

20. Dans le cas où Δ est >0, nous ne pourrons pas aller plus loin. Lorsque Δ est <0, par contre, la formule (10) est double, de sorte qu'elle n'entraîne *a priori* aucune obstruction particulière. D'ailleurs comme on l'a annoncé, il y a dans ce cas un théorème d'existence pour les genres tout à fait général. Toutefois, la méthode de Gauss que nous allons utiliser pour établir ce théorème fait un détour par les formes quadratiques ternaires, de sorte que le résultat ne pourra être obtenu qu'après le prochain paragraphe.
Cependant, nous allons voir tout de suite que le problème se réduit à une pure question d'algèbre concernant le groupe G' des classes primitives contenues dans le genre principal (cf. n°16). Rappelons que les classes de ce genre (attention : jeu de mot !) sont caractérisées par le fait que leur signature n'est constituée que de +. Or il y a dans le groupe G de toutes les classes, des classes simples ayant ce type de signature : ce sont les carrés des différents éléments de G car quelle que soit la signature d'une classe Φ, la signature de Φ^2 ne peut être constituée que de signes +. Si on note G^2 pour simplifier l'ensemble de tous ces carrés, on obtient ainsi un sous–groupe de G, qui est en fait un sous–groupe de G'. Bien mieux, si on associe à tout élément $\Phi\in G$ son carré Φ^2, on obtient un homomorphisme v du groupe G dans le groupe G', dont l'image est G^2 et dont le noyau est l'ensemble des classes Φ de G telles que $\Phi^2 = 1$. On reconnaît dans ce dernier cas le groupe A des classes primitives ambiguës (de discriminant Δ) (cf. §C, n°12). On en déduit que G/A est isomorphe à G^2.
Mais il se trouve que dans le cas d'un discriminant Δ impair <0 (juste celui qui nous intéresse!) on connaît exactement le nombre d'éléments de A : c'est 2^r (où r est encore et toujours le nombre de diviseurs premiers de Δ, cf. §B, n°11 et §C, n°12). On voit donc que le nombre d'éléments de G^2 est égal à $\frac{g}{2^r}$ (où g est le nombre d'éléments de G). Par suite, l'inclusion de G^2 dans G' signifie que l'on a $\frac{g}{2^r} \le g'$ (en appelant, comme on l'a déjà fait, g' le nombre d'éléments de G'). De façon plus précise, on a $\frac{g}{2^r} = g'$ si $G^2 = G'$ et

$\frac{g}{2^r} < g'$ sinon. Cela veut dire aussi, si on préfère, que l'on a $\frac{g}{g'} = 2^r$ si $G^2 = G'$ et $\frac{g}{g'} < 2^r$ sinon. Comme ce quotient $\frac{g}{g'}$ représente le nombre γ de genres de formes de discriminant Δ (n°16) on voit que $\gamma = 2^r$ si et seulement si $G^2 = G'$. il revient au même de dire que l'on a $G' \subset G^2$.
En d'autres termes, pour démontrer (dans le cas d'un discriminant impair négatif) que toute famille $(\varepsilon_p)_{p\in P} \in \{-1,+1\}^P$ peut être considérée comme la signature d'un genre (ou d'une forme primitive), on peut se contenter de démontrer que *toute classe contenue dans le genre principal est le carré d'une classe*. C'est ce qu'on fera §F, n°2 à 11!

E/ Petite théorie des formes quadratiques ternaires.

1. En fait de théorie, on se limitera plutôt à des «pièces détachées» en demandant au lecteur de compléter nos propos d'après le §A.
Comme il se doit, une *forme quadratique ternaire* peut être considérée comme une application f de $\mathbb{Z}^3$ dans $\mathbb{Z}$ pour laquelle il existe des entiers a, b, c, r, s, t tels que l'on ait

$$f(x,y,z) = ax^2+by^2+cz^2+rxy+syz+txz$$

quels que soient les entiers x, y, z.
Les entiers a, b, c et r, s, t sont évidemment uniques, ce qui permet de parler sans ambiguïté des *coefficients* de f et d'identifier f à la suite de ses coefficients, et donc d'écrire f = (a,b,c,r,s,t) ou, comme Gauss, $f = \begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix}$.
Il nous arrivera assez souvent aussi de confondre f avec f(x,y,z) et donc de définir une forme ternaire en se donnant l'expression générale $ax^2+by^2+cz^2+rxy+syz+txz$. Ce sera un abus de notation!

2. A partir d'une forme quadratique ternaire f, on définit de manière évidente les entiers *représentés* par f et en particulier les entiers *représentés proprement* par f. Pour un entier donné, on pourra donc parler des diverses *représentations*, éventuellement *propres*, de cet entier par la forme. Il y a des formes qui ne représentent que des entiers positifs, telles par exemple $x^2+y^2+z^2$: on dira que ce sont des *formes positives* ; il y en a d'autres (comme $-x^2-y^2-z^2$) qui ne représentent que des nombres négatifs : on dira que ce sont des *formes négatives*. Dans les deux cas, les mots "négatif" et "positif" sont à prendre au sens de Bourbaki, c'est-à-dire au sens large.
Lorsqu'une forme n'est ni positive ni négative (donc lorsqu'elle n'a pas de signe défini), on dira que c'est une *forme indéfinie*. Par définition, une forme de ce genre prend au moins une fois une valeur >0 et au moins une valeur <0. En fait, il y a une infinité de cas de chaque sorte à cause de la relation $f(cx,cy,cz) = c^2f(x,y,z)$.

3. Contrairement à ce qui se passe pour les formes binaires, il n'est pas possible de séparer les formes indéfinies des formes positives ou négatives au moyen d'une seule quantité simple analogue au discriminant. Il est cependant possible de considérer une

quantité numérique qui s'en rapproche, mais en définissant d'abord convenablement la «matrice» d'une forme ternaire. Comme dans le cas d'une forme binaire, on y parvient en dédoublant les termes «rectangles». De façon précise, si f = (a,b,c,r,s,t), la *matrice* de f est par définition la matrice symétrique

$$\begin{pmatrix} a & r/2 & t/2 \\ r/2 & b & s/2 \\ t/2 & s/2 & c \end{pmatrix}$$

Si on note a_{ij} le nombre situé à l'intersection de la i–ème ligne et de la j–ème colonne, on a alors $f(x_1,x_2,x_3) = \sum_{i=1}^{3}\sum_{j=1}^{3} a_{ij}x_ix_j$, ce qui est tout à fait satisfaisant.

Cela étant, le déterminant D de la matrice obtenue peut remplacer dans le cas des formes ternaires le discriminant. On dira que c'est le *déterminant* de la forme quadratique ternaire considérée. Son expression est évidemment assez compliquée car l'application de la règle de Sarrus donne $D = abc + \frac{rst}{4} - a\frac{s^2}{4} - b\frac{t^2}{4} - c\frac{r^2}{4}$. Lorsque $f(x,y,z) = x^2+y^2+z^2$ on obtient ainsi D = 1 et lorsque $f(x,y,z) = x^2-yz$, $D = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{vmatrix} = -\frac{1}{4}$

4. Si on revient à une forme binaire $ax^2+bxy+cy^2$, la matrice correspondante $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ donne comme déterminant $d = ac - \frac{b^2}{4}$. On peut appeler cette quantité le *déterminant* de la forme binaire. Par rapport au discriminant Δ, on a évidemment Δ = –4d. Dans le cas d'une forme ternaire, on pourrait sur le même modèle remplacer le déterminant D par –4D, ce qui donnerait un entier analogue à Δ qui pourrait s'appeler le «discriminant» de la forme ternaire. Mais cela ne se fait pas, sans doute parce que cela n'apporte pas grand chose par rapport au déterminant et que dans le cas d'une forme à plus de trois variables, il faudrait utiliser un autre facteur multiplicatif que –4. Bien plus, certains auteurs (et non des moindres) appellent «discriminant» d'une forme ternaire ce qu'on a appelé plus haut le déterminant. On comprend qu'il y en ait qui s'embrouille! Pour notre part, nous nous en tiendrons au point de vue exposé ci–dessus qui consiste à séparer nettement déterminant et discriminant pour les formes binaires et à ne parler que de déterminant dans le cas des formes ternaires.

Reste le problème des fractions qui apparaissent dans la matrice et dans le déterminant. Il n'y a pas de solution sauf à se limiter comme Gauss aux formes ternaires dont tous les termes rectangles sont affectés de coefficients pairs. Nous dirons alors que l'on a affaire à des *formes de Gauss*. Mais cette limitation est pour nous impossible : on a déjà pu le constater dans le cas binaire. Toutefois, pour simplifier les calculs nous n'hésiterons pas à remplacer certaines formes ternaires f par la forme de Gauss 2f – quitte à rediviser par 2 à la fin!

5. Nous allons d'ailleurs tout de suite appliquer ce principe pour introduire une forme binaire dans l'expression générale d'une forme ternaire f. Supposons donc que cette dernière soit une forme de Gauss et écrivons f(x,y,z) sous la forme $ax^2+by^2+cz^2+2uxy+2vyz+2wxz$ où u, v et w sont des entiers. On peut voir alors dans les derniers termes de cette expression une série de doubles produits susceptibles de provenir du développement d'un carré. Si on développe, pour voir, le carré $(ax+uy+wz)^2$, on obtient $a^2x^2+u^2y^2+w^2z^2+2auxy+2uwyz+2awxz$. On en déduit que $af(x,y,z)-(ax+vy+wz)^2 = (ab-u^2)y^2+(2av-2uw)yz+(ac-w^2)z^2$, ce qui définit une forme binaire $\varphi(y,z)$ dont la matrice est

$$\begin{pmatrix} ab-u^2 & av-uw \\ av-uw & ac-w^2 \end{pmatrix}$$

et dont le déterminant est $d=(ab-u^2)(ac-w^2)-(av-uw)^2=a(abc+uvw+uvw-bw^2-cu^2-av^2)$. On reconnaît dans la parenthèse le déterminant de la matrice de f, développée selon la règle de Sarrus.

Ainsi, pour toute forme de Gauss $f(x,y,z) = ax^2+by^2+cz^2+2uxy+2vyz+2wyz$, on a l'identité

$$(1) \qquad af(x,y,z) = (ax+uy+wz)^2+\varphi(y,z)$$

où φ est une forme binaire dont les coefficients sont $ab-u^2$, $2av-2uw$, $ac-w^2$ et dont le déterminant d est égal à aD où D est le déterminant de f.

En utilisant des méthodes de calculs analogues, le lecteur démontrera de même les identités

$$(2) \qquad bf(x,y,z) = (ux+by+vz)^2+\psi(x,z)$$

et

$$(3) \qquad cf(x,y,z) = (wx+vy+cz)^2+\theta(x,y)$$

où ψ et θ sont des formes binaires dont les déterminants respectifs sont bD et cD.

6. Nous allons utiliser ces relations pour caractériser convenablement les formes ternaires positives. Il y a en fait plusieurs caractérisations possibles équivalentes. Nous n'en donnerons qu'une seule et nous laisserons de côté le cas des formes de déterminant nul que nous n'aurons pas l'occasion de rencontrer.

Considérons donc une forme ternaire $f(x,y,z)=ax^2+by^2+cz^2+rxy+syz+txz$, de déterminant D non nul. Nous allons alors démontrer que cette forme est positive si et seulement si on a à la fois

$$a>0 \qquad \begin{vmatrix} a & r/2 \\ r/2 & b \end{vmatrix}>0 \qquad \begin{vmatrix} a & r/2 & t/2 \\ r/2 & b & s/2 \\ t/2 & s/2 & c \end{vmatrix}>0$$

On notera que les trois nombres qui interviennent dans ces relations sont des déterminants extraits de la matrice de la forme f : on les appelle parfois les *mineurs principaux* de cette matrice.

Comme on ne change pas le problème en remplaçant f par 2f (car cela ne change ni le signe de f ni celui des mineurs principaux), on supposera que f est une forme de Gauss, ce qui nous permettra de poser $f(x,y,z) = ax^2+by^2+cz^2+2uxy+2vyz+2wxz$ (donc de remplacer r/2, s/2, t/2 par u, v et w) et d'appliquer les identités (1), (2) et (3) ci-dessus.

7. Prenons d'abord pour hypothèse que f est une forme positive, c'est-à-dire une forme à valeurs positives, et utilisons la condition auxiliaire $D\neq 0$ pour démontrer que l'un au moins des coefficients a, b, c n'est pas nul. Si ce n'était pas le cas, on aurait $f(x,y,z) = 2uxy+2vyz+2wxz$. Comme f ne peut être la forme nulle (sinon on aurait $D = 0$), on peut affirmer que l'un au moins des coefficients u, v, w n'est pas nul.
Sans que cela restreigne la généralité, on peut supposer que c'est u. Mais alors on aurait $f(x,y,0) = uxy \geq 0$ quels que soient x et y, ce qui est manifestement impossible.
Nous allons maintenant démontrer que chacune des relation $a\neq 0$, $b\neq 0$, $c\neq 0$ implique les deux autres.
Supposons d'abord $a\neq 0$. Comme $a = f(1,0,0)$ et que f est positive, on a en fait $a>0$. Remplaçons alors y par ay, z par az et x par $-uy-wz$ dans la relation (1) du n°5. Comme $ax+uy+wz$ est remplacé par $a(-uy-wz)+auy+awz = 0$, on déduit de (1) et des hypothèses que $\varphi(ay,az) = a^2\varphi(y,z)$ est toujours un nombre positif. Il en est donc de même de $\varphi(y,z)$. Comme le déterminant d de φ est égal à aD, c'est un nombre non nul. Il en est de même, par conséquent, de son discriminant $\Delta = -4d$. On en déduit que φ est une forme définie positive au sens du §A. On a donc $\varphi(y,z)>0$ à chaque fois que $(y,z)\neq(0,0)$. Cela montre, en particulier, que

$$(4) \qquad ab = af(0,1,0) = u^2+\varphi(1,0)\geq\varphi(1,0)>0$$

et

$$(5) \qquad ac = af(0,0,1) = w^2+\varphi(0,1)\geq\varphi(1,0)>0$$

en utilisant deux fois la relation (1). D'où le résultat souhaité pour b et c.
Les deux autres cas se démontreraient de même, mais en utilisant systématiquement les identités (2) et (3).
En fait, on a donc toujours $a\neq 0$, c'est-à-dire le premier cas. La relation $a>0$ est donc évidente. Mais les autres relations $\begin{vmatrix} a & u \\ u & b \end{vmatrix}>0$ et $D>0$ qui restent à établir découlent facilement de ce qui précède. La première se déduit de (4) (qui a toujours lieu) et la seconde vient de ce que si Δ est le discriminant de la forme φ utilisée ci-dessus, alors $D = \frac{d}{a} = \frac{-\Delta}{4a}$ avec $\Delta<0$ et $a>0$. CQFD.

8. La réciproque reprend en partie les arguments ci-dessus. On suppose réalisées les trois conditions du n°6 et il s'agit d'en déduire que l'on a $f(x,y,z) \geq 0$ quels que soient x,y,z. Comme $a>0$, le problème revient à vérifier que $af(x,y,z) \geq 0$. Mais d'après l'identité (1), il suffit de démontrer que $\varphi(y,z) \geq 0$ quels que soient y et z, ou simplement de s'assurer que φ est une forme définie positive au sens du §A. Mais cela découle aisément des hypothèses car le discriminant Δ de φ est $-4aD$, donc un nombre <0, et que l'on a $\varphi(1,0) = ab-u^2 = ab-\frac{r^2}{4} > 0$ puisque $\varphi = (ab-u^2, 2av-uw, ac-w^2)$ (cf. n°5).

9. Reste à expédier en quelques lignes le problème des formes ternaires équivalentes. En premier lieu, nous dirons qu'une forme ternaire est *équivalente* à une forme ternaire f s'il existe des entiers α, β, γ, α', β', γ', α'', β'', γ'', formant une matrice carrée

$$\begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$$

de déterminant +1, tels que $g(x,y,z) = f(\alpha x+\beta y+\gamma z, \alpha' x+\beta' y+\gamma' z, \alpha'' x+\beta'' y+\gamma'' z)$. En un sens évident, il revient au même de dire qu'il existe une «transformation linéaire» τ de $\mathbb{Z}^3$, de déterminant +1 (ayant d'ailleurs pour matrice la matrice ci-dessus) telle que $g = f\circ\tau$.
En s'inspirant de ce qu'il a vu dans le §A, le lecteur n'aura pas de mal à vérifier qu'on définit ainsi une relation d'équivalence entre les formes ternaires, que deux formes ternaires équivalentes représentent les mêmes nombres et qu'elles ont aussi même déterminant. Pour démontrer ce dernier résultat, nous lui conseillons de démontrer la relation matricielle

$$G = {}^tTFT$$

analogue à celle que l'on a vue §A, n°8. Cette même relation devrait le convaincre aussi que toute forme équivalente à une forme de Gauss est encore une forme de Gauss...

10. Nous aurions quelques scrupules cependant à laisser le lecteur se dépatouiller avec un résultat dont nous aurons absolument besoin et selon lequel si une forme ternaire f représente proprement un entier m donné, alors il existe une forme g équivalente à f et dont le tout premier coefficient est m.
L'hypothèse signifie en effet qu'il existe des entiers u, v, w premiers dans leur ensemble tels que $f(u,v,w) = m$. tout repose alors sur le fait qu'il existe des entiers α, β, α', β', α'', β'' tels que

$$\begin{vmatrix} u & \alpha & \beta \\ v & \alpha' & \beta' \\ w & \alpha'' & \beta'' \end{vmatrix} = 1$$

car une fois ce résultat acquis il est facile de vérifier que l'on dispose ainsi d'une transformation linéaire τ transformant f en une forme g équivalente et dont le tout premier coefficient (celui de x^2) est $f(u,v,w)$, c'est-à-dire m.
Pour trouver α, β, α', β', α'', β'', utilisons le fait que selon le théorème de Bézout il existe des entiers u_0, v_0 et w_0 tels que $uu_0+vv_0+ww_0 = 1$.
Cette relation implique évidemment que l'un des nombres u_0, v_0, w_0 n'est pas nul. Supposons que ce soit u_0. Alors le PGCD g de u_0 et de v_0 n'est pas nul non plus et les nombres $u_1 = \frac{u_0}{g}$ et $v_1 = \frac{v_0}{g}$ sont premiers entre eux. Par suite, il existe des entiers u_2 et v_2 tels que $u_1u_2+v_1v_2 = 1$, de sorte que si on pose $u' = -u_2w_0$ et $v' = -v_2w_0$, on a $u_1u'+v_1v' = -u_1u_2w_0-v_1v_2w_0 = -w_0$. Avec les nombres ainsi introduits, on a

$$\begin{vmatrix} u & -v_1 & u' \\ v & u_1 & v' \\ w & 0 & g \end{vmatrix} = u\begin{vmatrix} u_1 & v' \\ 0 & g \end{vmatrix} - v\begin{vmatrix} -v_1 & u' \\ 0 & g \end{vmatrix} + w\begin{vmatrix} -v_1 & u' \\ u_1 & v' \end{vmatrix}$$

$$= uu_1g+vv_1g+w(-v_1v'-u_1u') = uu_0+vv_0+ww_0 = 1$$

ce qui correspond au résultat cherché.
On raisonne de manière semblable si $v_0 \neq 0$ ou si $w_0 \neq 0$.

11. Nous allons appliquer tout cela à la détermination de certaines formes de faible déterminant et en premier lieu pour démontrer que toute forme de Gauss positive de déterminant +1 est équivalente à la forme $x^2+y^2+z^2$. Nous commencerons par deux lemmes relatifs aux formes binaires.

Lemme 1 : Toute forme binaire définie positive de déterminant +1 (donc de discriminant −4) est équivalente à la forme x^2+y^2.

On sait en effet que toute forme définie positive de discriminant Δ est équivalente à une forme (a,b,c) pour laquelle on a $|b|\leq a\leq c$, $b\neq -a$ et $a \leq \sqrt{\frac{-\Delta}{3}}$ (§A, n° et §B, n°). Si $\Delta = -4$, on a donc $a \leq \sqrt{\frac{4}{3}}$ et par conséquent $a = 1$ et $-1<b\leq 1$. Comme b est nécessairement pair, on a $b = 0$ et par conséquent $c = 1$. CQFD.

Lemme 2 : Toute forme binaire définie positive de discriminant Δ représente au moins un entier n tel que $0<n \leq \sqrt{\frac{|\Delta|}{3}}$.

Appelons en effet n le plus petit entier >0 représenté par la forme considérée φ. Si (a,b,c) est une forme équivalente à φ telle que $a \leq \sqrt{\frac{|\Delta|}{3}}$ (ce qui est possible d'après ce qu'on a rappelé plus haut), on a $n\leq a \leq \sqrt{\frac{|\Delta|}{3}}$ puisque a est un entier >0 représenté par φ. D'où le lemme.

Cela étant, considérons une forme de Gauss ternaire positive f de déterminant +1. Parmi tous les entiers >0 représentés par f, appelons m celui qui est le plus petit. On a donc $m = f(x,y,z)$ pour des entiers x,y,z particuliers. A cause du caractère minimal de m, il est facile de voir que x, y et z sont premiers dans leur ensemble. On peut donc dire que m est représenté proprement par f. D'après le n°10, il existe une forme g équivalente à f dont le terme en x^2 s'écrit en fait mx^2. Comme c'est une forme de Gauss (n°9), on peut écrire d'après (1), n°4

$$(6) \qquad mg(x,y,z) = (mx+py+qz)^2+\varphi(y,z)$$

où p et q sont des entiers et où φ est une forme binaire de déterminant m. Cette dernière propriété veut dire aussi que le discriminant de φ est le nombre strictement négatif −4m, donc que φ est une forme définie négative ou définie positive. C'est en fait le second cas qui a lieu car d'après (6), $\varphi(m,0) = mg(-p,m,0)\geq 0$.

D'après le lemme 2 ci−dessus, il existe alors des nombres entiers y_0 et z_0 tels que $0<\varphi(y_0,z_0)<\sqrt{\frac{4m}{3}}$. Ces nombres y_0 et z_0 étant fixés, les nombres $mx+py_0+qz_0$ parcourent toute une classe de congruence modulo m lorsque x varie dans $\mathbb{Z}$. On peut donc choisir un entier x_0 tel que l'on ait $|mx_0+py_0+qz_0| \leq \frac{m}{2}$. Comme d'autre part, on a $g(x_0,y_0,z_0)>0$ (car $mg(x_0,y_0,z_0) = (mx_0+py_0+qz_0)^2+\varphi(y_0,z_0)\geq\varphi(y_0,z_0)>0$), il résulte de la minimalité de m que $g(x_0,y_0,z_0)\geq m$ (on rappelle que f et g représentent les mêmes nombres). On a donc $mg(x_0,y_0,z_0)\geq m^2$.

Si on rassemble toutes les inégalités obtenues, on voit que

$$m^2 \le mg(x_0,y_0,z_0) = (mx_0+py_0+qz_0)^2+\varphi(y_0,z_0) \le \frac{m^2}{4}+\sqrt{\frac{4m}{3}}$$

d'où successivement $m^2 \le \frac{m^2}{4}+\sqrt{\frac{4m}{3}}$, $\frac{3m^2}{4} \le \sqrt{\frac{4m}{3}}$, $m^2 \le \frac{4}{3}\sqrt{\frac{4}{3}}\,m$, $m^4 \le \frac{16}{9}\left(\frac{4}{3}m\right) = \frac{64}{27}m$, $m^3 \le \frac{64}{27}$ et donc $m \le \frac{4}{3}$.

On en déduit que m = 1 et donc que la relation (6) est en réalité

$$(7) \qquad g(x,y,z) = (x+py+qz)^2+\varphi(y,z)$$

où le discriminant de φ est −4. Cette dernière propriété implique, d'après le lemme 1, que $\varphi(y,z) \sim y^2+z^2$, autrement dit qu'il existe des entiers α, β, γ, δ vérifiant la relation $\alpha\delta-\beta\gamma = 1$ tels que $\varphi(\alpha y+\beta z,\gamma y+\delta z) = y^2+z^2$. Considérons alors l'application linéaire $\tau : (x,y,z) \to (x,\alpha y+\beta z,\gamma y+\delta z)$ dont la matrice est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \gamma & \delta \end{pmatrix}$ et dont le déterminant est 1.

Si on applique τ aux deux membres de (7), on obtient d'un côté une forme h(x,y,z) équivalente à g(x,y,z) – donc à f(x,y,z) – et de l'autre une expression du type $(x+ry+sz)^2+y^2+z^2$ où r et s sont deux nouveaux entiers. D'où la nouvelle relation

$$(8) \qquad h(x,y,z) = (x+ry+sz)^2+y^2+z^2$$

Si on applique maintenant à cette forme ternaire la transformation $\tau' = \begin{pmatrix} 1 & -r & -s \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ de déterminant 1, on voit que le premier membre est une forme équivalente à h, donc à f, égale à $x^2+y^2+z^2$. CQFD.

12. Pour le déterminant 2, nous nous intéresserons aux seules formes indéfinies et nous démontrerons de façon précise que toute forme de Gauss indéfinie de déterminant 2 est équivalente soit à la forme $x^2-y^2-2z^2$, soit à la forme $-2x^2+2yz$.

Nous demanderons d'abord au lecteur d'établir le lemme suivant, analogue au lemme 1 du n°11 et dont la démonstration se fait selon les mêmes principes.

Lemme 3 : Toute forme quadratique binaire définie positive de discriminant −8 est équivalente à la forme x^2+2y^2. Toute forme binaire définie positive de discriminant −16 (resp. −24) est équivalente à l'une des deux formes x^2+4y^2, $2x^2+2y^2$ (resp. x^2+6y^2, $2x^2+3y^2$).

Ce lemme étant acquis, la démonstration que l'on va exposer est compliquée par le fait que l'on part d'une forme indéfinie (de Gauss et de déterminant 2). Comme f représente par définition au moins un entier >0 et au moins un entier <0, on peut appeler m le plus petit entier >0 représenté par f. Comme dans le n°11, m est en fait représenté proprement et par suite, il existe une forme g équivalente à f (donc de Gauss, et indéfinie) dont le tout premier terme est mx^2. On peut donc écrire cette fois

$$(9) \qquad mg(x,y,z) = (mx+py+qz)^2+\varphi(y,z)$$

où p et q sont deux entiers et où φ est une forme binaire de déterminant 2m, donc de discriminant −8m. Mais ici, puisque g est indéfinie, φ ne peut pas être positive. Comme

cependant $-8m<0$, c'est une forme définie négative, qu'on préférera écrire $-\psi(y,z)$ où ψ est une forme définie positive (de discriminant $-8m$). D'où la nouvelle relation, plus claire

$$(9') \qquad mg(x,y,z) = (mx+py+qz)^2-\psi(y,z)$$

D'après le lemme 2 du n°11, il existe des entiers y_0 et z_0 tels que $0<\psi(y_0,z_0)\leq\sqrt{\frac{8m}{3}}$. Ces entiers étant fixés, les nombres $mx+py_0+qz_0$ forment une classe de congruence modulo m, de sorte qu'on peut choisir x de telle façon que $0\leq mx+py_0+qz_0\leq m$. Si $mx+py_0+qz_0$ est dans l'intervalle $\left[\frac{m}{2},m\right]$, on posera $x_0 = x$, sinon on posera $x_0 = x-1$. Ainsi, dans ce dernier cas, on aura $-m\leq mx_0+py_0+qz_0\leq-\frac{m}{2}$. dans tous les cas, on a alors $\frac{m}{2}\leq\left|mx_0+py_0+qz_0\right|\leq m$, c'est-à-dire

$$\frac{m^2}{4}\leq(mx_0+py_0+qz_0)^2\leq m^2$$

On a donc en particulier $mg(x_0,y_0,z_0) = (mx_0+py_0+qz_0)^2-\psi(y_0,z_0)<(mx_0+py_0+qz_0)^2\leq m^2$. On en déduit que $g(x_0,y_0,z_0)<m$. Vu le choix de m comme valeur minimum >0 de f (ou de g), on a nécessairement $g(x_0,y_0,z_0)\leq 0$, c'est-à-dire $(mx_0+py_0+qz_0)^2\leq\psi(y_0,z_0)$.

D'où la relation $\frac{m^2}{4}\leq(mx_0+py_0+qz_0)^2\leq\psi(y_0,z_0)\leq\sqrt{\frac{8m}{3}}$, ce qui implique successivement

$\frac{m^2}{4}\leq\sqrt{\frac{8m}{3}}$, $\frac{m^4}{16}\leq\frac{8m}{3}$, $m^3\leq\sqrt{\frac{128}{3}}$, donc $m\leq\sqrt[3]{\frac{128}{3}}\leq 3,5$.

Il n'y a donc que trois possibilités pour m (mais trois quand même!) et trois relations qui remplacent (9) ou (9') :

$$(10) \qquad g(x,y,z) = (x+px+qy)^2-\psi(y,z)$$
$$(10') \qquad 2g(x,y,z) = (2x+py+qz)^2-\psi(y,z)$$
$$(10'') \qquad 3g(x,y,z) = (3x+py+qz)^2-\psi(y,z)$$

où ψ est une forme définie positive de discriminant -8 dans la relation (10), -16 dans la relation (10') et -24 dans la relation (10'').

Dans le premier cas, on sait, d'après le lemme 3, que $\psi(y,z)\sim y^2+2z^2$, dans le second que $\psi(y,z)\sim y^2+4z^2$ ou $\psi(y,z)\sim 2y^2+2z^2$, dans le troisième que $\psi(y,z)\sim y^2+6z^2$ ou $\psi(y,z)\sim 2y^2+3z^2$. Ainsi, en appliquant aux deux membres des relations (10), (10') et (10'') une transformation convenable du type $\begin{pmatrix}1&0&0\\0&\alpha&\beta\\0&\gamma&\delta\end{pmatrix}$ avec $\alpha\delta-\beta\gamma = 1$, obtient-on une forme ternaire h équivalente à g telle que

$$(11) \qquad mh(x,y,z) = (mx+ry+sz)^2-\chi(y,z)$$

avec $\chi(y,z) = y^2+2z^2$ si $m = 1$, $\chi(y,z) = y^2+4z^2$ ou $\chi(y,z) = 2y^2+2z^2$ si $m = 2$, $\chi(y,z) = y^2+6z^2$ ou $\chi(y,z) = 2y^2+3z^2$ si $m = 3$.

Appliquons enfin à cette nouvelle relation une transformation de matrice $\begin{pmatrix} 1 & k & \ell \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. On obtient dans le premier membre de (11) une nouvelle forme équivalente à g (et à f) (qu'on continuera à appeler h) et dans le second membre une expression égale à

$$[mx+(mk+r)y+(m\ell+s)z]^2-\chi(y,z).$$

En choisissant convenablement k et ℓ, il est possible d'avoir $0\leq mk+r\leq m-1$ et $0\leq m\ell+s\leq m-1$ (restes de r et de s modulo m). Bref, sans changer inutilement de notation, on peut supposer que dans la relation (11), on a $0\leq r,\ s\leq m-1$.

Si m = 1, cette dernière condition implique r=s=0 et par conséquent $h(x,y,z)=x^2-y^2-2z^2$, ce qui est une des conclusions souhaitées.

Si m = 2, on a

$$2h(x,y,z) = (2x+ry+sz)^2-y^2-4z^2 \text{ ou } 2h(x,y,z) = (2x+ry+sz)^2-2y^2-2z^2$$

Le premier membre de ces égalités est toujours pair. Il en résulte que dans le premier cas, on ne peut avoir r = 0 (car en faisant x = 0, y = 1, z = 0, il resterait −1 dans le second membre) ni s = 1 (car en faisant x = 0, y = 0, z = 1, on obtiendrait −3). On a donc, en fait, pour cette première égalité, r = 1, s = 0, c'est-à-dire $2h(x,y,z) = (2x+y)^2-y^2-4z^2 = 4x^2+4xy-4z^2$, donc $h(x,y,z) = 2x^2+2xy-2z^2$. Si on remplace x par y, y par z−y et z par x, on définir alors une transformation de $\mathbb{Z}^3$, dont la matrice est $\begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, donc de déterminant +1, qui transforme $2x^2+2xy-2z^2$ en $2y^2+2y(z-y)-2x^2 = 2yz-2x^2$, ce qui est encore conforme à la conclusion cherchée.

Dans le second cas, on ne peut avoir r = 1 (prendre sinon x = 0, y = 1, z = 0) ni s = 1 (prendre x = 0, y = 0, z = 1). On a donc r = s = 0, c'est-à-dire $2h(x,y,z) = (2x)^2-2y^2-2z^2$, donc $h(x,y,z) = 2x^2-y^2-z^2$, mais cette dernière égalité est impossible car on aurait alors h(1,1,0) = 1, alors que par hypothèse le minimum des valeurs >0 de h (ou de f) doit être égal à m = 2.

Enfin, si m = 3, on a

$$3h(x,y,z) = (3x+ry+sz)^2-y^2-6z^2 \text{ ou } 3h(x,y,z) = (3x+ry+sz)^2-2y^2-3z^2 \text{ avec } 0\leq r,s\leq 2$$

Cette fois, c'est par 3 que le premier membre est divisible. Il doit donc en être de même du second membre. Or si x = 0, y = 0, z = 1, on obtient dans le premier cas s^2-6 et dans le second s^2-3, de sorte que s doit être divisible par 3, donc nul, et si x = 0, y = 1, z = 0, on obtient r^2-1 dans le premier cas (ce qui suppose r = 1 ou r = 2) et r^2-2 dans le second, ce qui est franchement impossible. On a donc en fait $3h(x,y,z) = (3x+y)^2-y^2-6z^2$ ou $3h(x,y,z) = (3x+2y)^2-y^2-6z^2$, c'est-à-dire, après développement et simplification par 3

$$h(x,y,z) = 3x^2+2xy-2z^2 \text{ ou } h(x,y,z) = 3x^2+4xy+y^2-2z^2$$

Mais ces deux cas sont en réalité impossible car le "minimum" de h serait 1 et non 3 (prendre x = 1, y = −1, z = 0 dans un cas et x = 0, y = 1, z = 0 dans l'autre).

Bref, comme prévu, il ne reste, à équivalence près, que les deux formes $x^2-y^2-2z^2$ et $2yz-2x^2$. On notera que ce sont deux formes indéfinies et de déterminant +2, et qu'elles

ne sont pas équivalentes entre elles car l'une représente des nombres impairs et l'autre en est bien incapable.

13. En fait, pour ce que nous voulons faire, nous aurons besoin de savoir que toute forme ternaire indéfinie de déterminant $-\frac{1}{4}$ est équivalente à la forme x^2-yz.

Cela découle de ce qui précède car si on appelle f une forme ternaire indéfinie de déterminant $-\frac{1}{4}$, il est clair que $g = -2f$ est une forme de Gauss indéfinie de déterminant 2. On a donc $g(x,y,z)\sim x^2-y^2-2z^2$ ou $g(x,y,z)\sim 2yz-2x^2$. Mais seul le second cas peut avoir lieu puisque g ne peut pas représenter des nombres impairs. D'où le résultat.

Cela étant, il convient de considérer tout ce qui précède (je parle des paragraphes A, B, C, D et E) comme une série de préliminaires (en fait volontairement limités) nécessaires pour aborder enfin le vif du sujet – le vif du sujet que voici!

F/ Nombres triangulaires et sommes de trois carrés.

1. Pour qu'un entier naturel n soit une somme de trois nombres triangulaires il faut et il suffit que 8n+3 soit une somme de trois carrés.
La démonstration de ce résultat est facile. Supposons d'abord que n soit la somme de trois nombres triangulaires. Cela veut dire qu'il existe des entiers positifs a, b, c tels que $n = \frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2}$.
Alors $8n = 4a^2+4a+4b^2+4b+4c^2+4c$, et donc $8n+3 = (2a+1)^2+(2b+1)^2+(2c+1)^2$.
Réciproquement, supposons que 8n+3 soit une somme de trois carrés. Alors, ou bien un seul de ces carrés est impair, ou bien tous le sont. En fait, le premier cas ne peut avoir lieu car comme un carré impair est congru à 1 modulo 8 et qu'un carré pair est un multiple de 4, la somme des trois carrés serait, dans ce premier cas, ou congrue à 1 ou congrue à 5 modulo 8, ce qui n'est pas. Il y a donc trois carrés impairs, ce qu'on peut écrire $8n+3=(2a+1)^2+(2b+1)^2+(2c+1)^2$. On en déduit aussitôt que $n = \frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2}$.
Bref, le résultat contenu dans l'exclamation qui sert de titre à ce passionnant article sera obtenu en démontrant que tout entier naturel de la forme 8n+3 est une somme de trois carrés.

2. Pour parvenir à ce résultat définitif, il nous faut établir le théorème de l'existence des genres que nous avons laissé en suspens à la fin du §D, donc démontrer que si Δ est un discriminant impair négatif (dont P est l'ensemble des diviseurs premiers) et si $(\varepsilon_p)_{p\in P}$ est un élément quelconque du produit $\{-1,+1\}^P$, alors il existe au moins une forme de discriminant Δ dont la signature est la famille $(\varepsilon_p)_{p\in P}$. Comme nous l'avons dit dans le n°20 du §D, il suffit de prouver que dans le groupe $G(\Delta)$ des classes de formes primitives de discriminant Δ toute classe du genre principal est un carré.

Considérons donc une classe Φ du genre principal et, pour fixer les idées, une forme f de ce genre. Il s'agit donc d'une forme quadratique binaire primitive, de discriminant Δ, dont la signature n'est formée que de signes +. Il s'agit d'en déduire qu'il existe des formes primitives φ et ψ de discriminant Δ, contenues dans une même classe Θ (donc équivalentes), composables entre elles, et telles que $f \sim \varphi * \psi$; on aura alors $\Phi = \Theta^2$.
Comme on le verra au cours de la démonstration, on peut s'arranger pour que l'on ait $\psi = \varphi$, donc pour que φ soi composable avec elle–même et que l'on ait $f \sim \varphi * \varphi$.

3. Cette démonstration consiste à établir un lien entre la forme binaire f – qu'on écrira (a,b,c) – et la forme ternaire x^2–yz introduite à la fin du précédent paragraphe. Ce lien résultera, comme on va le voir de l'étude des congruences simultanées

$$(1) \qquad M^2 \equiv c,\ 2MN \equiv -b,\ N^2 \equiv a \pmod{\Delta}.$$

Nous ne pouvons pas aborder ici, faute de place, les raisons qui expliquent l'intervention plus ou moins inéluctable de ce système de congruences : voir pour cela [GAU], p.326. Il nous suffira de démontrer que ce système est résoluble, autrement dit qu'il admet au moins une solution M et N.

4. Nous aurons besoin du lemme suivant :
Lemme : Si p est un nombre premier impair et si a est un résidu quadratique de p (non divisible par p), alors, pour tout entier $\alpha \geq 1$, la congruence $x^2 \equiv a \pmod{p^\alpha}$ est résoluble.
Le raisonnement se fait par récurrence sur α. Lorsque $\alpha = 1$, l'existence d'un entier x tel que $x^2 \equiv a \pmod{p}$ résulte de la définition même d'un résidu quadratique (cf. §D, n°2).
Supposons que le résultat ait été démontré pour un exposant $\alpha \geq 1$ fixé, donc qu'il existe un entier x tel que $x^2 \equiv a \pmod{p^\alpha}$ et montrons qu'il existe un entier y tel que $y^2 \equiv a \pmod{p^{\alpha+1}}$. Cherchons en fait un nombre y qui soit de la forme $x+kp^\alpha$ où k est un entier à trouver. Comme $y^2 = (x+kp^\alpha)^2 = x^2+2xkp^\alpha+k^2p^{2\alpha}$ et que x^2 est de la forme $a+mp^\alpha$, on a $y^2 = a+(m+2kx)p^\alpha+k^2p^{2\alpha}$. Comme $\alpha+1 \leq 2\alpha$ (puisque $\alpha \geq 1$), le dernier terme de cette somme est divisible par $p^{\alpha+1}$. Tout le problème est donc de voir qu'on peut choisir k de telle sorte que m+2kx soit divisible par p. Il revient au même d'étudier la congruence $2xk \equiv -m \pmod{p}$. Or il est bien connu (ça traîne dans tout traité d'arithmétique digne de ce nom) que cette congruence (d'inconnue k) est résoluble (quel que soit m) si 2x est premier avec p. Mais cette propriété résulte d'une part du fait que p est impair, de l'autre de ce que x, comme a, est premier avec p.

5. Revenons alors aux congruences du système (1). Si on décompose Δ en facteurs premiers, en écrivant $\Delta = -p_1^{\alpha_1}\ldots p_r^{\alpha_r}$, il est normal de commencer par étudier la résolubilité du système

$$(2) \qquad M^2 \equiv c,\ 2MN \equiv -b,\ N^2 \equiv a \pmod{p_i^{\alpha_i}}.$$

Observons d'abord que p_i ne peut diviser à la fois a et c à cause du caractère primitif de la forme (cf. §D, n°9).

Si on suppose que p_i ne divise pas a, on peut commencer l'étude de (2) par la congruence $N^2 \equiv a \pmod{p_i^{\alpha_i}}$. Sinon, p_i ne divise pas c et on pourrait procéder dans l'autre sens, en commençant par la congruence $M^2 \equiv c \pmod{p_i^{\alpha_i}}$.

Pour établir que la congruence $N^2 \equiv a \pmod{p_i^{\alpha_i}}$ admet au moins une solution N_i, il suffit d'après le lemme du n°4 de vérifier que a est un résidu quadratique de p. Mais cela résulte de l'hypothèse faite sur la signature de f qui implique en particulier $\chi_{p_i}(f) = +1$ c'est-à-dire (avec le symbole de Legendre) $\left(\frac{a}{p_i}\right) = +1$.

Avec le nombre N_i ainsi obtenu, on voit ensuite que la congruence

$$2MN_i \equiv -b \pmod{p_i^{\alpha_i}}$$

admet au moins une solution M_i : cela résulte du fait que $2N_i$ est un entier premier avec le module $p_i^{\alpha_i}$, c'est-à-dire non divisible par p_i.

Reste à vérifier que la congruence

$$M^2 \equiv c \pmod{p_i^{\alpha_i}}$$

est assurée lorsqu'on prend $M = M_i$. pour cela, on tire de la congruence $2M_iN_i \equiv -b \pmod{p_i^{\alpha_i}}$, la relation $4M_i^2N_i^2 \equiv b^2 \equiv 4ac \pmod{p_i^{\alpha_i}}$, soit $4aM_i^2 \equiv 4ac \pmod{p_i^{\alpha_i}}$. Il n'y a plus qu'à diviser par 4a, ce qui est possible puisque 4a est premier avec le module mod $p_i^{\alpha_i}$.

6. Le système (2) ayant une solution M_i, N_i connue, utilisons le théorème chinois : les nombres mod $p_i^{\alpha_i}$ étant deux à deux premiers, il existe un entier M (resp. un entier N) tel que l'on ait $M \equiv M_i \pmod{p_i^{\alpha_i}}$ (resp. $N \equiv N_i \pmod{p_i^{\alpha_i}}$) quel que soit i.

On a alors $M^2 \equiv M_i^2 \equiv c \pmod{p_i^{\alpha_i}}$ quel que soit i. D'où $M^2 \equiv c \pmod{\Delta}$.

On vérifie de même que $N^2 \equiv a \pmod{\Delta}$ et que $2MN \equiv -b \pmod{\Delta}$.

D'où l'existence d'au moins une solution M, N pour le système (1).

7. On peut donc dire, en explicitant ce que veut dire ce système qu'il existe des entiers A, B et C tels que

$$(3) \qquad M^2+C\Delta = c,\ 2MN-B\Delta = -b \text{ et } N^2+A\Delta = a$$

les signes étant choisis pour rendre les calculs qui vont suivre suffisamment lisibles. On aura en effet besoin de calculer 2aM+bN, 2cN+bM et $\Delta = b^2-4ac$ en utilisant (3). Cela donne

$2aM+bN = 2(N^2+A\Delta)M+(B\Delta-2MN)N = 2N^2M+2AM\Delta+BN\Delta-2MN^2 = \Delta(2AM+BN)$

$2cN+bM = 2(M^2+C\Delta)N+(B\Delta-2MN)M = 2M^2N+2CN\Delta+BM\Delta-2M^2N = \Delta(2CN+BM)$

$\Delta = b^2-4ac = (2MN-B\Delta)^2-4(N^2+A\Delta)(M^2+C\Delta) = 4M^2N^2-4MNB\Delta+B^2\Delta^2-4N^2M^2$
$-4N^2C\Delta-4AM^2\Delta-4AC\Delta^2 = \Delta^2(B^2-4AC)-4\Delta(BMN+AM^2+CN^2)$

Le premier calcul permet de définir un entier m (unique) tel que

$$(4) \qquad m = 2AM+BN \text{ et } \Delta m = 2aM+bN$$

le second de définir un entier n tel que

$$(4') \qquad n = 2CN+BM \text{ et } \Delta n = 2cN+bM$$

et le troisième donne, après simplification par Δ

$$\Delta(B^2-4AC)-4(BMN+AM^2+CN^2) = 1$$

Mais $4(BMN+AM^2+CN^2)=2BMN+4AM^2+2BMN+4CN^2=2M(BN+2AM)+2N(BM+2CN) = 2Mm+2Nn$ d'après (4) et (4').

D'où la relation $\Delta(B^2-4AC) = 2Mm+2Nn+1$, qui permet d'affirmer l'existence d'un entier s tel que

$$(4'') \qquad s = B^2-4AC \text{ et } \Delta s = 2Mm+2Nn+1$$

8. Considérons dans ces conditions la matrice symétrique d'ordre 3

$$\begin{pmatrix} a & b/2 & m \\ b/2 & c & n \\ m & n & s \end{pmatrix}$$

Elle définit naturellement une forme quadratique ternaire dont l'expression générale est $ax^2+cy^2+sz^2+bxy+2mxy+2nyz$ et dont le déterminant (développé par rapport à la troisième ligne de la matrice) est égal à $m\left(\frac{bn}{2}-cm\right)-n\left(an-\frac{bm}{2}\right)+s\left(ac-\frac{b^2}{4}\right)$. Si on multiplie ce résultat par 2Δ, on obtient $\Delta m(bn-2cm)+\Delta n(bm-2am)-\frac{\Delta^2 s}{2}$.

D'où, en remplaçant Δm par $2aM+bN$ et Δn par $2cN+bM$:

$$(2aM+bN)(bn-2cm)+(2cN+bM)(bm-2an)-\frac{\Delta^2 s}{2}$$

$$= 2aMbn+4acMm+b^2Nn-2bNcm+2cNbm-4cNan+b^2Mm-2bMan-\frac{\Delta^2 s}{2}$$

Après élimination des quatre termes qui s'annulent, il reste

$$b^2(Mm+Nn)-4ac(Mm+Nn)-\frac{\Delta^2 s}{2} = (Mm+Nn)\Delta-\frac{\Delta^2 s}{2}$$

$$= \frac{1}{2}\Delta(2Mm+2Nn-\Delta s) = -\frac{1}{2}\Delta$$

puisque $2Mm+2Nn-\Delta s = -1$ d'après (4'').

Si on redivise par 2Δ, on en déduit que le déterminant de la matrice (ou de la forme correspondante) est, miraculeusement, égal à $-\frac{1}{4}$. Comme les "mineurs principaux" de la matrice ne sont ni tous >0 ni tous <0 (ce sont a, $ac-\frac{b^2}{4} = -\frac{\Delta}{4}$ qui est >0 et $-\frac{1}{4}$ qui est <0), la forme est indéfinie (§E, n°6). On déduit de tout cela que la forme ternaire considérée est équivalente à la forme x^2-yz (§E, n°13). Cela veut dire qu'il existe des entiers $\alpha, \beta, \gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ tels que

$$(5) \qquad \begin{vmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{vmatrix} = +1$$

et $ax^2+cy^2+sz^2+bxy+2mxz+2nyz = (\alpha x+\beta y+\gamma z)^2-(\alpha' x+\beta' y+\gamma' z)(\alpha'' x+\beta'' y+\gamma'' z)$.

En faisant $g = 0$, on en déduit que

$$(6) \quad f(x,y) = ax^2+bxy+cy^2 = (\alpha x+\beta y)^2-(\alpha' x+\beta' y)(\alpha'' x+\beta'' y)$$

ce qu'on exprime en disant que *la forme binaire* f *est représentée par la forme ternaire* x^2-yz.

9. Comme le montre un calcul facile, laissé généreusement au lecteur, la relation (6) signifie aussi que

(6') $a = \alpha^2-\alpha'\alpha''$ $b = 2\alpha\beta-\alpha'\beta''-\alpha''\beta'$ $c = \beta^2-\beta'\beta''$

Si on pose alors $u = \alpha\beta'-\alpha'\beta$, $v = \alpha'\beta''-\alpha''\beta'$ et $w = \alpha''\beta-\alpha\beta''$, il est possible de démontrer en utilisant la notion gaussienne de «forme adjointe» que $v^2-4uw = b^2-4ac = \Delta$. Comme je ne veux pas me lancer dans ces considérations (cf. [GAU], p.306], je propose une vérification directe, bête mais efficace :

$$\begin{aligned} v^2-4uw &= (\alpha'\beta''-\alpha''\beta')^2-4(\alpha\beta'-\alpha'\beta)(\alpha''\beta-\alpha\beta'') \\ &= \alpha'^2\beta''^2-2\alpha'\alpha''\beta'\beta''+\alpha''^2\beta'^2-4\alpha\alpha''\beta\beta'+4\alpha^2\beta'\beta''+4\alpha'\alpha''\beta^2-4\alpha\alpha'\beta\beta'' \\ b^2-4ac &= (2\alpha\beta-\alpha'\beta''-\alpha''\beta')^2-4(\alpha^2-\alpha'\alpha'')(\beta^2-\beta'\beta'') \\ &= 4\alpha^2\beta^2+\alpha'^2\beta''^2+\alpha''^2\beta'^2-4\alpha\alpha'\beta\beta''-4\alpha\alpha''\beta\beta'+2\alpha'\alpha''\beta'\beta''-4\alpha^2\beta^2+4\alpha^2\beta'\beta'' \\ &\quad +4\alpha'\alpha''\beta^2-4\alpha'\alpha''\beta'\beta''. \end{aligned}$$

L'égalité cherchée s'obtient alors en remarquant que dans ce dernier résultat il y a deux termes qui s'annulent ($4\alpha^2\beta^2$ et $-4\alpha^2\beta^2$) et deux qui se simplifient ($2\alpha'\alpha''\beta'\beta''$ et $-4\alpha'\alpha''\beta'\beta''$).

On déduit de là que ni u ni w ne sont nuls car s'il en était autrement, on aurait $\Delta = v^2$, ce qui est faux car par hypothèse Δ est <0.

Notons au passage que les nombres u, v et w sont aussi premiers dans leur ensemble, car la relation (5) montre que $\gamma v+\gamma' w+\gamma'' u = +1$.

10. Si on prend alors $x = \beta'$ et $y = -\alpha'$ dans la relation (6) ci–dessus, il vient $f(x,y) = f(\beta',-\alpha') = (\alpha\beta'-\alpha'\beta)^2 = u^2$. En d'autres termes, f représente un carré non nul. Quitte à diviser par un PGCD convenable (en l'occurence le PGCD de α' et de β' – qui n'est pas nul puisque $u\neq 0$), on peut supposer que cette représentation est propre. Appelons n^2 le carré non nul représenté proprement par f ainsi obtenu.

D'après un résultat bien connu, vu dans le premier paragraphe, il existe alors des entiers ℓ et m tels que $f\sim(n^2,\ell,m)$. On a alors $\ell^2-4mn^2 = \Delta$. Si on pose $\varphi = (n,\ell,mn)$, on obtient une nouvelle forme binaire de discriminant Δ, composable avec elle–même (car $4n^2$ est un entier non nul qui divise $\ell^2-\Delta = 4mn^2$: cf. §C, n°3) et pour laquelle $\varphi*\varphi = (n^2,\ell,m)\sim f$.

Le résultat serait alors à notre portée (que dis–je? dans la poche) si la forme φ avait le bon goût d'être primitive. Mais ce n'est malheureusement pas sûr car ce n'est pas parce que n^2, ℓ et m sont premiers dans leur ensemble (ce qu'on sait) que n, ℓ et mn le sont! En fait, pour que n, ℓ et mn soient premiers dans leur ensemble, il est nécessaire que n et ℓ soient premiers entre eux. Cette condition nécessaire est aussi suffisante et revient à dire que n est premier avec $\Delta = \ell^2-4mn^2$. Mais il est bien difficile de savoir si cette condition est réalisée avec le nombre n défini ci–dessus à partir de la seule matrice

$$S = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$$

dont on ne sait pas grand chose. Heureusement, comme on va le voir, on a toujours la possibilité de remplacer S par une matrice analogue ayant les mêmes propriétés et pour laquelle le nombre n correspondant soit premier avec Δ.

11. Pour cela, considérons un entier r quelconque et la matrice

$$T = \begin{pmatrix} 1 & 0 & r \\ 2r & 1 & r^2 \\ 0 & 0 & 1 \end{pmatrix}$$

de déterminant +1 et qui laisse invariante la forme x^2-yz car on a $(x+rz)^2-(rx+y+r^2z)z = x^2+2rxz+r^2z^2-2rxz-yz-r^2z^2 = x^2-yz$.

Si on pose alors $S_1 = TS = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_1' & \beta_1' & \gamma_1' \\ \alpha_1'' & \beta_1'' & \gamma_1'' \end{pmatrix}$, on en déduit que S_1, comme S, transforme la forme x^2-yz en $ax^2+cy^2+sz^2+bxy+2mxz+2nyz$.

L'entier u ci-dessus (égal à $\alpha\beta'-\alpha'\beta$) doit être alors remplacé par $u_1 = \alpha_1\beta_1'-\alpha_1'\beta_1$. Comme $\alpha_1 = \alpha+\alpha''r$, $\beta_1 = \beta+\beta''r$, $\alpha_1' = 2\alpha r+\alpha'+\alpha''r^2$ et $\beta_1' = 2\beta r+\beta'+\beta''r^2$, on voit que $u_1 = (\alpha+\alpha''r)(2\beta r+\beta'+\beta''r^2)-(2\alpha r+\alpha'+\alpha''r^2)(\beta+\beta''r)$, ce qui donne, après développement, $(\alpha\beta'-\alpha'\beta)+(\alpha''\beta'-\alpha'\beta'')r+(\alpha''\beta-\alpha\beta'')r^2 = u-vr+wr^2$.

Il suffit alors de voir qu'on peut choisir r de façon que $u-vr+wr^2$ soit premier avec Δ. Le lecteur vérifiera qu'il en est bien ainsi si on pose $r = \prod_{p\in R} p$ où R est l'ensemble des diviseurs premiers de Δ.

Cela clôt la démonstration du théorème énoncé ci-dessus dans le n°2.

12. Nous pouvons enfin nous attaquer à la phase finale de notre propos en démontrant que tout entier de la forme 8k+3 est une somme de trois carrés (cf. n°1).

Cette conclusion se déduit en fait de ce qu'il existe une forme positive f = (a,b,c), définie positive, de discriminant Δ = −8k−3 et pour laquelle le système de congruences

$$(7) \qquad M^2 \equiv -2c \qquad MN \equiv b \qquad N^2 \equiv -2a \pmod{2a}$$

est résoluble.

Supposons l'existence de f établie et associons à une solution (M,N) de (7) des entiers A, B et C tels que

$$(8)\ M^2-C\Delta = -2c,\ MN+B\Delta = b \text{ et } N^2-A\Delta = -2a$$

En s'inspirant des calculs faits ci-dessus dans le n°7, le lecteur vérifiera qu'il existe des entiers m, n et s tels que

$$(9) \qquad m = AM+BN \text{ et } \Delta m = 2aM+bN$$
$$(9') \qquad n = CN+BM \text{ et } \Delta n = 2cN+bM$$
$$(9'') \qquad s = AC-B^2 \text{ et } \Delta s = Mm+Nn+1$$

Dans ces conditions, la matrice symétrique

$$\begin{pmatrix} 2a & b & m \\ b & 2c & n \\ m & n & s \end{pmatrix}$$

définit une forme quadratique ternaire (de Gauss) dont l'expression générale est $2ax^2+2cy^2+sz^2+2bxy+2mxz+2nyz$ dont le déterminant, calculé selon la même méthode que le n°8, est égal à +1.

Comme les trois mineurs principaux 2a, $\begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = 4ac-b^2 = -\Delta = 8k+3$ et $\begin{vmatrix} 2a & b & m \\ b & 2c & n \\ m & n & s \end{vmatrix} = +1$

sont >0 (on rappelle que f = (a,b,c) est une forme définie positive, ce qui entraîne a>0), la forme donné par la matrice ci–dessus est une forme positive (§E, n°6). Elle est donc équivalente à $x^2+y^2+z^2$ (§E, n°11), ce qui veut dire qu'il existe des entiers α, β, γ, α', β', γ', α'', β'', γ'' formant une matrice de déterminant +1, tels que

$$2ax^2+2cy^2+sz^2+2bxy+2mxz+2nyz = (\alpha x+\beta y+\gamma z)^2+(\alpha' x+\beta' y+\gamma' z)^2+(\alpha'' x+\beta'' y+\gamma'' z)^2$$

D'où en particulier, en faisant z = 0,

$$2ax^2+2bxy+2cy^2 = (\alpha x+\beta y)^2+(\alpha' x+\beta' y)^2+(\alpha'' x+\beta'' y)^2$$

relation qui veut dire que

$$2a = \alpha^2+\alpha'^2+\alpha''^2,\ b = \alpha\beta+\alpha'\beta'+\alpha''\beta'',\ 2c = \beta^2+\beta'^2+\beta''^2$$

Il est facile d'en déduire, par un calcul direct, que $-\Delta = 8k+3$ est la somme des trois carrés $(\alpha\beta'-\alpha'\beta)^2+(\alpha\beta''-\alpha''\beta)^2+(\alpha'\beta''-\alpha''\beta')^2$ car on a d'une part

$$(\alpha\beta'-\alpha'\beta)^2+(\alpha\beta''-\alpha''\beta)^2+(\alpha'\beta''-\alpha''\beta')^2$$
$$= \alpha^2\beta'^2+\alpha'^2\beta^2+\alpha^2\beta''^2+\alpha''^2\beta^2+\alpha'^2\beta''^2+\alpha''^2\beta'^2-2\alpha\alpha'\beta\beta'-2\alpha\alpha''\beta\beta''-2\alpha'\alpha''\beta'\beta''$$

alors que de l'autre

$$-\Delta = 4ac-b^2 = (\alpha^2+\alpha'^2+\alpha''^2)(\beta^2+\beta'^2+\beta''^2)-(\alpha\beta+\alpha'\beta'+\alpha''\beta'')^2$$
$$= \alpha^2\beta^2+\alpha^2\beta'^2+\alpha^2\beta''^2+\alpha'^2\beta^2+\alpha'^2\beta'^2+\alpha'^2\beta''^2+\alpha''^2\beta^2+\alpha''^2\beta'^2+\alpha''^2\beta''^2-\alpha^2\beta^2$$
$$-\alpha'^2\beta'^2-\alpha''^2\beta''^2-2\alpha\alpha'\beta\beta'-2\alpha\alpha''\beta\beta''-2\alpha'\alpha''\beta'\beta''$$

ce qui est la même chose, après simplification.

13. Reste à prouver l'existence de la forme f = (a,b,c)...

Faisons une analyse rapide en supposant, comme on disait autrefois, le problème résolu. Si on décompose $-\Delta = 8k+3$ en facteurs premiers, sous la forme $p_1^{\alpha_1}...p_r^{\alpha_r}$, on doit avoir pour tout i, $M^2 \equiv -2c$ et $N^2 \equiv -2a \pmod{p_i}$. Comme la forme f est primitive et que p_i divise $\Delta = b^2-4ac$, l'un des deux nombres a ou c est premier avec p_i. Supposons que ce soit a. On a donc, avec le symbole de Legendre, $\left(\frac{-2a}{p_i}\right) = +1$, c'est-à-dire $\left(\frac{a}{p_i}\right) = \left(\frac{-2}{p_i}\right)$. Mais $\left(\frac{a}{p_i}\right)$ est aussi le caractère de f relatif à p_i (§D, n°9), de sorte que la relation trouvée s'écrit $\chi_{p_i}(f) = \left(\frac{-2}{p_i}\right)$. La forme f cherchée doit donc être choisie dans le genre déterminé par le système de signes $\left(\frac{-2}{p_i}\right)$ obtenu lorsque i varie de 1 à r.

Cette analyse étant faite, le théorème de l'existence des genres (n°2 ci–dessus) garantit qu'il existe une forme primitive f = (a,b,c), de discriminant Δ = –8k–3, telle que $\chi_{p_i}(f) = \left(\frac{-2}{p_i}\right)$ pour tout i = 1, ..., r.

Pour démontrer dans ces conditions la résolubilité du système (7), on procède comme on a fait ci–dessus pour (1) (cf. n°3). Grâce au théorème chinois, on se contente de vérifier que

$$M^2 \equiv -2c,\ MN \equiv b,\ N^2 \equiv -2a \pmod{p_i^{\alpha_i}}$$

est résoluble quel que soit i.

Si a n'est pas divisible par p_i, on commence par $N^2 \equiv -2a \pmod{p_i^{\alpha_i}}$; si c'est c qui a cette propriété, par $M^2 \equiv -2c \pmod{p_i^{\alpha_i}}$.

Limitons–nous au premier cas. L'existence d'au moins une solution N_i à la congruence $N^2 \equiv -2a \pmod{p_i^{\alpha_i}}$ résulte du lemme vu n°4, compte tenu du fait que –2a est un résidu quadratique modulo p_i puisque $\left(\frac{-2a}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{-2}{p_i}\right) = \chi_{p_i}(f)\chi_{p_i}(f) = +1$. Il est facile ensuite de voir que la congruence $MN_i \equiv b \pmod{p_i^{\alpha_i}}$ a une solution M_i. Reste à voir que $M_i \equiv -2c \pmod{p_i^{\alpha_i}}$. Cela vient de la relation $b^2–4ac = \Delta$ qui donne $b^2 \equiv 4ac = (-2a)(-2c) \pmod{p_i^{\alpha_i}}$, donc $M_i^2N_i^2 \equiv N_i^2(-2c)$, congruence qui peut être simplifiée par N_i^2 puisque N_i est premier avec p_i, tout comme a.

La résolubilité de (7) étant acquise, il convient de s'assurer, pour finir, que f est bien une forme positive. On le voit en utilisant la relation (10) du §D, n°17. Autrement dit, si on appelle Q l'ensemble des diviseurs premiers de Δ ayant un exposant impair dans la décomposition de Δ en facteurs premiers, il s'agit de vérifier que $\prod_{p\in Q}\chi_p(f) = +1$.

On peut supposer, si on veut, que les éléments p de Q sont rangés au début de la suite p_1, ..., p_r utilisée plus haut, autrement dit que ces éléments sont p_1, ..., p_s avec s≤r. Dans ce cas, compte tenu de la parité des exposants (impairs si i≤s, pairs si i>s), on voit aussitôt que

$$\prod_{p\in Q}\chi_p(f) = \chi_{p_1}(f)\cdots\chi_{p_s}(f) = \left(\frac{-2}{p_1}\right)\cdots\left(\frac{-2}{p_s}\right) = \left(\frac{-2}{p_1}\right)^{\alpha_1}\cdots\left(\frac{-2}{p_s}\right)^{\alpha_s}$$

$$= \left(\frac{-2}{p_1}\right)^{\alpha_1}\cdots\left(\frac{-2}{p_r}\right)^{\alpha_r} = \left(\frac{-2}{p_1^{\alpha_1}\cdots p_r^{\alpha_r}}\right) = \left(\frac{-2}{|\Delta|}\right) = \left(\frac{-1}{|\Delta|}\right)\left(\frac{2}{|\Delta|}\right)$$

Comme |Δ| est de la forme 8k+3, on a $\left(\frac{-1}{|\Delta|}\right) = -1$ et $\left(\frac{2}{|\Delta|}\right) = -1$ d'après (4') et (5'), §D, n°6.

D'où le résultat, qui met un point final à cette interminable démonstration!

Epilogue.

Le premier paragraphe de cette étude est assez élémentaire et ne devrait pas poser de problèmes de compréhension au lecteur. Le second paragraphe ne présente pas non plus

de grandes difficultés dans la mesure où l'on s'est limité aux discriminants impairs négatifs. Lorsque le discriminant Δ est pair, le dénombrement des formes ancipitales élémentaires (a,0,c) et (a,a,c) est plus délicat et il y a de nombreux cas à envisager en fonction de l'exposant α de 2 dans la décomposition en facteurs premiers de Δ : voir [CAS], p.342. En outre, le passage des formes élémentaires (primitives) aux classes ambiguës (primitives) n'est pas facile lorsque $\Delta>0$; il faut soit connaître la théorie de la réduction des formes indéfinies de Gauss ([GAU], p.161), soit avoir procédé à une étude détaillée du sous-groupe de $SL_2(\mathbb{Z})$ laissant invariant une forme f donnée (groupe des automorphismes de f) (cf. [CAS], p.291).
La composition des formes selon Gauss est difficilement compréhensible (pour le commun des mortels que je suis). Ce qu'en dit Buell dans [BUE] est d'un faible secours. J'ai suivi de près la méthode de Cassels ([CAS], p.333) mais en modifiant son vocabulaire (au mépris de l'histoire de la théorie, il appelle «concordantes» les formes que j'appelle «composables»).
La notion de genre, étendue au cas d'un discriminant de parité quelconque est définie dans [BUE], p.52. Cassels part d'un tout autre point de vue, plus moderne, mais pas forcément plus compréhensible (cf. [CAS], p.139). Dans le cas général il y a une relation de dépendance entre les caractères dont il faut tenir compte pour énoncer le théorème de l'existence des genres.
Le paragraphe sur les formes ternaires a été réduit au strict minimum. Nous n'avons pas jugé utile de démontrer comme l'a fait Gauss, à l'aide d'une théorie de la réduction *ad hoc*, qu'il n'y a qu'un nombre fini de classes de déterminant donné (cf. [GAU], p.318 ou de façon indépendante, [ROS], p.156) – je me suis d'ailleurs inspiré de ce dernier pour établir les résultats des numéros 11 et 12 du §E.
Le dernier paragraphe, tel que je l'ai rédigé, est sans doute le moins satisfaisant, en particulier parce que les congruences (1) et (7) tombent du ciel comme des cheveux sur la soupe! Gauss est en principe plus explicite (surtout si on lit [VEN] en parallèle...), mais j'ai reculé devant la tâche d'exposer la théorie de la représentation des formes binaires par les formes ternaires qui explique pas mal de choses, mais que je n'ai pas entièrement comprise.

Pour tous renseignements complémentaires, voici la bibliographie qui m'a servi :
[BUE] Duncan A. 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 *Disquisitiones Arithmeticae*, par A.–C.–M. Poullet – Delisle), réimpression éditions Jacques Gabay, 1989.
[ITA] Jean ITARD, *Les nombres premiers*, P.U.F, Collection «Que sais–je?».
[ROS] H.E. ROSE, *A Course in Number Theory*, Oxford University Press, 1988.

[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.

Errata

Plusieurs erreurs se sont glissées dans le texte de la première partie de cet article, dont voici les corrections. Que l'auteur et les lecteurs veuillent bien nous en excuser.

p.22, ligne 8 : au lieu de «classes "primitives" en "ambiguës"» lire «classes "primitives" et "ambiguës"».
p.22, ligne 5 (en partant du bas) : supprimer «+2» dans «$ax^2+bxy+cy^2+2$».
p.28, ligne 4 (en partant du bas) : au lieu de «modulo a», lire «modulo 2a».
p.30, il manque le mot «propriété» tout à la fin de la 3ème ligne du n°18.
p.30, n°18 encore, 6ème ligne, le «c'» au milieu de la ligne représente un entier (différent de 0) et non un mot élidé.
p.31, ligne 4, à la fin : lire «montre qu'il n'y a, au plus, qu'une valeur».
p.35, ligne 3, au lieu de «$\Delta_1^{\alpha_1}$» lire «Δ».
p.36, passage sauté : il faut lire à partir de la ligne 4 «Sauf erreur de ma part (cf. [VEN], p.126), cette dernière propriété n'est pas vraie si Δ>0. En revanche, nous allons voir qu'elle est exacte si Δ<0».
p.36, n°9, 1ère ligne, tout à la fin, remplacer «en» par «et».
p.37, 10ème ligne en partant du bas : il s'agit de développer «$a(x+\beta y)^2+b(x+\beta y)y+cy^2$» et non «$a(x+\beta y)^2+b(x+\beta y)+cy^2$».
p.40, 1ère ligne au n°2 : lire «compilation» et non «composition».
p.42, ligne 9, «membre à membre» et non «nombre à nombre»...
p.42, 1ère ligne du n°6, supprimer le préfixe «dé» de «décomposer».
p.43, 3ème ligne avant la fin du n°8, «on aura f~(a,b,c) et f'~(a',b,c')» (pas d'accent à b). Mettre ensuite une majuscule au mot «comme».
p.45, ligne 13, «Comme $B^2-4\alpha\alpha'\Gamma''=\Delta$» (un accent à α).