$\Delta = b^2 - 4ac$

par Jean-Pierre Serre

Professeur au Collège de France

La formule du titre est bien sûr familière ; il s'agit du *discriminant* du polynôme quadratique $ax^2 + bx + c$.

Le problème que je souhaite aborder aujourd'hui est le suivant : étant donné un entier Δ, *quels sont les polynômes possibles $ax^2 + bx + c$, à coefficients entiers a, b, c, pour lesquels $b^2 - 4ac$ est égal à Δ ?* Peut-on les classer ?

Ce problème a une longue histoire, remontant à Gauss (vers 1800) ; il n'est pas encore résolu, mais de nouveaux résultats assez intéressants ont été obtenus récemment, comme j'espère vous le montrer.

Remarquons d'abord qu'il existe une condition nécessaire évidente sur Δ ; notamment, Δ doit être congru à un carré modulo 4, c'est-à-dire,

$$\Delta \equiv 0, 1 \pmod 4.$$

Réciproquement, si cette congruence est vérifiée, il est facile de trouver $a, b, c \in \mathbb{Z}$ avec $\Delta = b^2 - 4ac$ (exercice). Ceci règle la question de l'*existence* des solutions de notre problème ; il ne reste plus (!) qu'à les classifier. Par exemple, existe-t-il des Δ pour lesquels il existe une solution unique ?

Sous cette forme grossière, la réponse est évidemment "non". En effet, la transformation $x \to x + 1$ laisse Δ invariant, mais change (a, b, c) en $(a, b + 2a, a + b + c)$. Ainsi, nous devons considérer deux polynômes quadratiques comme *équivalents* s'ils diffèrent de $x \to x + 1$, ou plus généralement, de $x \to x + n \quad (n \in \mathbb{Z})$. Mais cela ne suffit pas : il existe d'autres transformations possibles. Pour les voir, il est préférable d'utiliser une notation homogène et d'écrire nos polynômes quadratiques sous la forme $ax^2 + bxy + cy^2$. La transformation $x \to x + 1$ devient $\begin{cases} x \to x + y \\ y \to y \end{cases}$, que nous pouvons écrire sous la forme d'une matrice $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Puisque x et y jouent maintenant des rôles symétriques, nous devons également introduire la matrice $T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ qui correspond à la transformation $\begin{cases} x \to x \\ y \to x + y \end{cases}$ Et, puisque nous pouvons composer des transformations, nous devons considérer le groupe engendré par S et T, qui se trouve être le groupe $\mathbf{SL}_2(\mathbb{Z})$ des matrices 2×2 à coefficients entiers $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ et de déterminant 1.

Notre problème peut maintenant être reformulé comme suit :

Conférence organisée conjointement par la Société mathématique de Singapour et le Département de mathématiques de l'Université nationale de Singapour, et donnée le 14 février 1985. Notes prises par Daniel E. Flath

Étant donné un entier Δ, avec $\Delta \equiv 0, 1 \pmod 4$, classifier les classes d'équivalence $\mathbf{SL}_2(\mathbb{Z})$ *des formes quadratiques $ax^2 + bxy + cy^2$, avec $a, b, c \in \mathbb{Z}$ et $b^2 - 4ac = \Delta$.*

Pour le reste de cet exposé, nous considérerons *uniquement le cas où* $\Delta < 0$, c'est-à-dire les équations $ax^2 + bx + c = 0$ sans racine réelle. (Le cas d'un Δ positif est tout aussi intéressant, mais assez différent, et peu de progrès ont été réalisés à ce sujet depuis Gauss.) Cette restriction aux Δ négatifs impose que a et c aient le même signe. Par commodité, nous les prendrons toujours positifs, et nous noterons $\underline{h}(\Delta)$ le nombre de telles formes, modulo l'équivalence $\mathbf{SL}_2(\mathbb{Z})$; nous verrons plus loin que ce nombre est fini.

Considérons une forme $ax^2 + bxy + cy^2$, avec $a, c > 0$ et $b^2 - 4ac = \Delta$, avec $\Delta < 0$. On dit qu'une telle forme est *presque réduite* si $a \leq c$ et $|b| \leq a$. *Toute forme peut être transformée en une forme presque réduite* par un élément de $\mathbf{SL}_2(\mathbb{Z})$. En effet, on peut faire en sorte que $a \leq c$ en appliquant la transformation $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ dans le cas où $c < a$ et on peut s'assurer que $|b| \leq a$ en appliquant un décalage $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ qui laisse a invariant et remplace b par $b + 2an$. Si cela détruit l'inégalité $a \leq c$, on applique à nouveau $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, et ainsi de suite. Il est facile de vérifier que ce processus s'arrête après un nombre fini d'étapes et donne une forme presque réduite.

Théorème. Le nombre de formes presque réduites avec un discriminant donné $\Delta < 0$ est fini.

Preuve. Si $ax^2 + bxy + cy^2$ est presque réduit, nous avons

$$4a^2 \leq 4ac = b^2 - \Delta \leq a^2 - \Delta,$$

donc $3a^2 < -\Delta$; ceci montre que a ne peut prendre qu'un nombre fini de valeurs. Il en va de même pour b puisque $|b| \leq a$, et c est déterminé par a, b et Δ. □

Corollaire. $\underline{h}(\Delta)$ est fini.

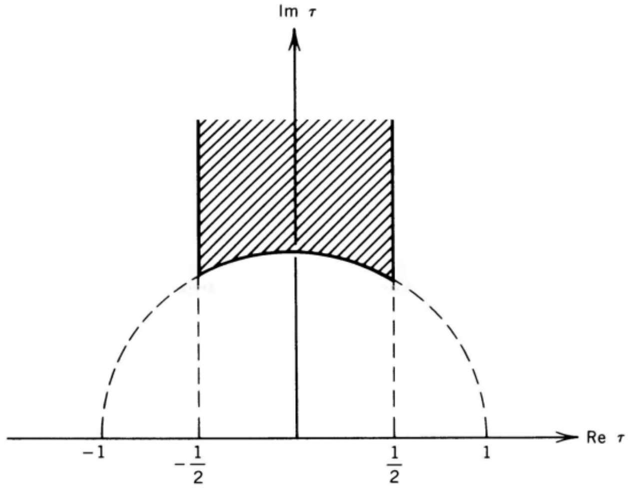

Figure A1

Pour aller plus loin, nous devons examiner si chaque classe d'équivalence $\mathbf{SL}_2(\mathbb{Z})$ contient une forme presque réduite *unique*. Il s'avère que c'est presque toujours vrai. Je souhaite expliquer les exceptions à l'aide d'une image dans le plan complexe : écrivons $ax^2+bxy+cy^2$ comme $a(x+\tau y)(x+\overline{\tau}y)$ avec un certain nombre complexe τ. Nous pouvons supposer que $\mathfrak{Im}\ \tau > 0$ puisque τ et $\overline{\tau}$ jouent des rôles symétriques. La condition $|b| \leq a$ est équivalente à $|\tau+\overline{\tau}| \leq 1$, c'est-à-dire $|\mathfrak{Re}\ \tau| \leq \frac{1}{2}$. La condition $a \leq c$ se traduit par $\tau\overline{\tau} \geq 1$, c'est-à-dire $|\tau| \geq 1$. En d'autres termes, $ax^2+bxy+cy^2$ est presque réduit précisément lorsque τ se trouve dans la fameuse région ombrée représentée (frontière incluse) sur la figure A1.

Les exceptions mentionnées proviennent de la frontière. La transformation $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ changent τ en $\tau+1$ reliant deux points sur les frontières verticales. La transformation $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ relie deux points symétriques τ et $-1/\tau = -\overline{\tau}$ sur l'arc frontière.

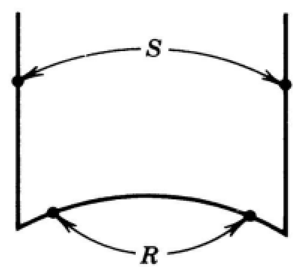

Figure A2

Pour éliminer les formes presque réduites redondantes, nous supprimons la moitié de la frontière. Notamment :

Définition. $ax^2+bxy+cy^2 = a(x+\tau y)(x+\overline{\tau}y)$ est *réduit* si τ se trouve dans la région représentée sur la figure A3 :

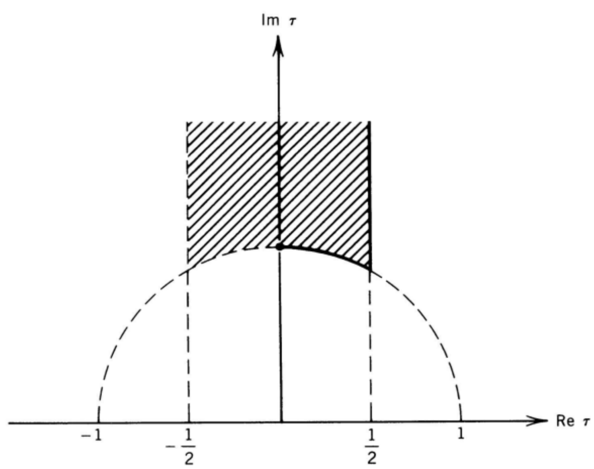

Figure A3

De manière équivalente, si $|b| \leq a \leq c$ et dans le cas $a = |b|$, alors $b = a$ et dans le cas $a = c$, alors $b \geq 0$.

Cette définition a été choisie de sorte qu'il existe une forme réduite *unique* dans chaque classe d'équivalence $\mathbf{SL}_2(\mathbb{Z})$. Par conséquent, $\underline{h}(\Delta)$ est le nombre de formes réduites du discriminant Δ. Cela conduit à une procédure pour calculer $\underline{h}(\Delta)$ pour un Δ donné, notamment à lister toutes les formes réduites comme dans le tableau A1. (La preuve de la finitude de $\underline{h}(\Delta)$ donnée ci-dessus montre comment établir cette liste.)

Remarquons que les formes $2(x^2 + xy + y^2)$ et $2(x^2 + y^2)$ pour les discriminants -12 et -16 sont des multiples de formes qui apparaissent plus tôt dans le tableau sous $\Delta = -3, -4$. Pour éviter ce doublon, nous modifions le jeu. Définissons une forme $ax^2 + bxy + cy^2$ comme primitive si a, b et c n'ont aucun facteur commun supérieur à 1, et définissons $h(\Delta)$, le nombre de classes de Δ, comme le nombre de formes réduites *primitives* du discriminant Δ. Gauss a fait une découverte remarquable : l'ensemble C_Δ des formes réduites primitives du discriminant Δ est un groupe abélien de manière naturelle, mais nous n'entrerons pas dans les détails ici [1].

TABLEAU A1

Δ	$\underline{h}(\Delta)$	Formes reduites du Discriminant Δ		
-3	1	$x^2 + xy + y^2$		
-4	1	$x^2 + y^2$		
-7	1	$x^2 + xy + 2y^2$		
-8	1	$x^2 + 2y^2$		
-11	1	$x^2 + xy + 3y^2$		
-12	2	$x^2 + 3y^2$	$2(x^2 + xy + y^2)$	
-15	2	$x^2 + xy + 4y^2$	$2(x^2 + xy + 2y^2)$	
-16	2	$x^2 + 4y^2$	$2(x^2 + y^2)$	
-19	1	$x^2 + xy + 5y^2$		
-20	2	$x^2 + 5y^2$	$2x^2 + 2xy + 3y^2$	
-23	3	$x^2 + xy + 6y^2$	$2x^2 - xy + 3y^2$	$2x^2 + xy + 3y^2$

TABLEAU A2

Δ	-3	-4	-7	-8	-11	-12	-15	-16	-19	-20
$h(\Delta)$	1	1	1	1	1	1	2	1	1	2
Δ	-23	-31	-43	-47	-59	-67	-71	-79	-83	-163
$h(\Delta$	3	3	1	5	3	1	7	5	3	1

Grâce à l'assistance informatique, ces tableaux ont maintenant été étendus à des millions.

En regardant les tableaux, on constate que les valeurs de $h(\Delta)$ sont très irrégulières, mais qu'avec de grandes valeurs de $|\Delta|$, $h(\Delta)$ tend également à être grand. Rendre cette dernière observation

1. Appelons R_Δ l'anneau $\mathbb{Z}[\frac{1}{2}\sqrt{\Delta}]$ si $\Delta \equiv 0 \pmod 4$ et l'anneau $\mathbb{Z}[(1+\sqrt{\Delta})/2]$ si $\Delta \equiv 1 \pmod 4$. Alors C_Δ est isomorphe au "groupe de classes" $\mathrm{Pic}(R_\Delta)$ de R_Δ. Lorsque Δ est un discriminant fondamental, alors R_Δ est l'anneau des entiers du corps quadratique $\mathbb{Q}(\sqrt{\Delta})$, et $h(\Delta)$ est le nombre de classes de ce corps.

précise a été un problème fondamental.

Pour des raisons techniques, nous limitons notre considération pour le reste de cet exposé aux “discriminants fondamentaux”. Un discriminant Δ est *fondamental* s'il *ne peut pas* être écrit $\Delta = \Delta_0 f^2$ avec Δ_0 un discriminant (c'est-à-dire congru à 0 ou 1 modulo 4) et f un entier supérieur à 1. Par exemple, -12 et -16 ne sont pas fondamentaux. Cette restriction n'est pas importante car on sait comment calculer tous les $h(\Delta)$ à partir des seules valeurs des discriminants fondamentaux Δ.

Les discriminants fondamentaux $\Delta < 0$ avec un nombre de classes $h(\Delta) = 1$ sont particulièrement intéressants : ce sont ceux pour lesquels notre problème initial (trouver les équations quadratiques avec un Δ donné) a une solution essentiellement unique. On en trouve facilement 9 : $\Delta = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Vers 1800, Gauss a conjecturé qu'il n'y en avait pas d'autres. Comme nous le verrons, c'est vrai (mais il a fallu plus de 150 ans pour le prouver).

Ces discriminants Δ avec $h(\Delta) = 1$ ont des propriétés remarquables. Permettez-moi d'illustrer cela avec le cas $\Delta = -163$.

En 1772, Euler (*Mémoires de l'Académie de Berlin*, extrait d'une lettre à M. Bernoulli) a découvert une propriété curieuse du polynôme

$$x^2 + x + 41 \quad \text{(de discriminant } \Delta = -163).$$

notamment, si vous regardez le tableau de ses valeurs pour $x = 0, 1, \ldots,$

x	0	1	2	3	4	5	6	7	...	39
$x^2 + x + 41$	41	43	47	53	61	71	83	97	...	1601

vous ne trouvez que *des nombres premiers*, jusqu'à $x = 39$ (mais $x = 40$ n'est pas un nombre premier, car $40^2 + 40 + 41 = 41^2$) ! Le fait que ce polynôme produise autant de nombres premiers est équivalent à l'égalité $h(-163) = 1$. En effet, le théorème suivant n'est pas difficile à démontrer, en utilisant les propriétés élémentaires des corps quadratiques imaginaires :

Théorème. *Pour un nombre premier p supérieur à 3 et congru à 3 modulo 4, les trois propriétés suivantes sont équivalentes :*

a. $h(-p) = 1$.

b. $x^2 + x + (p + 1)/4$ *est un nombre premier pour tout entier x tel que* $0 \leq x \leq (p - 7)/4$.

c. $x^2 + x + (p + 1)/4$ *est premier pour* $0 \leq x < (\sqrt{p/3} - 1)/2$

(Pour une démonstration de l'équivalence (b) et (c), voir, par exemple, G. Frobenius, *Gesammelte Abhandlungen* III, n° 94.)

Ceci s'applique à $p = 163$: d'après (c), il suffit de vérifier que $x^2 + x + 41$ est premier pour $x = 0, 1, 2, 3$; cela *implique* qu'il le sera jusqu'à $x = 39$.

Il existe d'autres faits intéressants concernant 163 qui sont liés au fait que $h(-163) = 1$. Considérons par exemple le nombre transcendant

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007...$$

Le fait qu'il soit si proche d'un entier peut être prouvé a priori à partir de $h(-163) = 1$!

[*Esquisse de démonstration.* On calcule la valeur de la fonction modulaire elliptique $j(z)$ pour $z = (1 + i\sqrt{163})/2$; en utilisant $h(-163) = 1$, on prouve que $j(z)$ est un entier ordinaire. D'autre part, le développement en série entière de $j(z)$ donne :

$$\begin{aligned} j(z) &= e^{-2\pi iz} + 744 + 196884e^{2\pi iz} + \dots \\ &= -e^{\pi\sqrt{163}} + 744 - 196884e^{-\pi\sqrt{163}} + \dots \end{aligned}$$

une expression dans laquelle tous les termes, sauf les deux premiers, contribuent très peu (moins de 10^{-12}). Par conséquent, $e^{\pi\sqrt{163}}$ est proche d'un entier.

Pour ces raisons et d'autres encore, il est très intéressant de déterminer tous les discriminants fondamentaux négatifs Δ avec un nombre de classe $h(\Delta) = 1$ (ou 2 ou 3 ou ...).

Dans la suite de cet exposé, je passerai en revue les travaux qui ont été effectués sur ce problème, certains assez récents, d'autres encore en cours.

Les tableaux suggèrent que le nombre de classe $h(\Delta)$ est approximativement de l'ordre de grandeur de $|\Delta|^{1/2}$. On peut en fait facilement prouver que $h(\Delta) < 3|\Delta|^{1/2}\log|\Delta|$.

Mais nous voulons vraiment une *borne inférieure* pour h, car nous voulons montrer que pour les grands discriminants Δ, $h(\Delta)$ doit également être grand.

Les travaux de Gronwall en 1913 et de Landau en 1918 ont montré que si la fonction zêta de $\mathbb{Q}(\sqrt{\Delta})$ n'a pas de zéro entre $\frac{1}{2}$ et 1, alors $h(\Delta) > C|\Delta|^{1/2}/\log|\Delta|$ pour une constante C qui peut en principe être calculée. Malheureusement, l'hypothèse sur la fonction zêta n'a jamais été prouvée (c'est un cas particulier de l'hypothèse de Riemann généralisée (HRG)).

En 1934, Heilbronn a terminé certains travaux antérieurs de Deuring et a prouvé que $\lim h(\Delta) = \infty$ lorsque $\Delta \to \infty$. Ce résultat a rapidement été précisé par Siegel (1936), qui a montré que pour tout $\epsilon > 0$, il existe une constante positive C_ϵ telle que $h(\Delta) \geq C_\epsilon|\Delta|^{1/2-\epsilon}$. En d'autres termes, le taux de croissance de $h(\Delta)$ est exactement comme prévu.

Cependant, la démonstration de Siegel donne moins que ce qu'on pourrait espérer : elle n'est pas "efficace" (en clair, la constante C_ϵ ne peut pas être calculée). La raison en est intéressante. On voudrait prouver que si un discriminant Δ est très grand [2], alors $h(\Delta)$ ne peut pas être trop petit. On ne sait pas comment faire. Ce que la démonstration de Siegel montre, en revanche, c'est que l'existence de *deux* grands discriminants Δ et Δ' avec $h(\Delta)$ et $h(\Delta')$ suffisamment petits conduit à une contradiction. Cela permet à $h(\Delta)$ d'être petit pour *un seul* grand Δ, ce qui est un de trop !

Par exemple, il découle des travaux de Siegel qu'il existe *au plus un* discriminant fondamental Δ_{10} ayant comme nombre de classe 1 au-delà des 9 précédemment listés comme déjà connus de Gauss.

2. Je qualifie un discriminant négatif de "grand" lorsque sa valeur absolue est grande.

La question de l'existence de Δ_{10} a acquis une certaine notoriété sous le nom de "problème du dixième corps quadratique imaginaire".

Le progrès suivant est survenu en 1952 lorsque Heegner a publié une preuve que Δ_{10} *n'existe pas*. Cependant, cette preuve utilisait des propriétés des fonctions modulaires qu'il a énoncées sans justification suffisante. Les gens ne comprenaient pas son travail et n'y croyaient pas (j'ai moi-même essayé une fois de suivre ses arguments, mais je ne suis arrivé nulle part...). Par conséquent, la question de l'existence de Δ_{10} était toujours considérée comme ouverte.

En 1966, Stark étudia Δ_{10} dans sa thèse et prouva que, s'il existe, Δ_{10} est très grand : $|\Delta_{10}| > 10^{9000000}$. L'année suivante, il réussit à prouver que Δ_{10} n'existe pas, résolvant ainsi le problème du nombre de classes 1. Sa méthode semblait au premier abord assez différente de celle de Heegner ; il s'avéra plus tard que les deux méthodes sont étroitement liées (et que l'approche de Heegner était fondamentalement correcte, après tout).

La même année, A. Baker donna également une solution au problème du nombre de classes 1, en utilisant ses bornes effectives pour les formes linéaires dans les logarithmes des nombres algébriques.

Avec quelques travaux (de Baker lui-même et de Stark et Montgomery-Weinberger), cette méthode put également être appliquée à $h(\Delta) = 2$, et révéla qu'il existe exactement 18 discriminants fondamentaux négatifs de nombre de classes 2, le plus grand étant -427.

Cependant, ni la méthode de Stark ni celle de Baker ne s'appliquaient au problème de classe numéro 3 ou plus.

Pour aller plus loin, nous devons maintenant introduire de nouveaux objets. Rappelons qu'une *courbe elliptique* E sur $\mathbb{Q}$ est une cubique non singulière

$$y^2 = x^3 + ax + b, \qquad \text{avec } a, b \in \mathbb{Q} \ \text{ et } \ 4a^3 + 27b^2 \neq 0.$$

À une telle courbe est attachée une fonction analytique merveilleuse (et mystérieuse) $L_E(S)$, appelée sa série L ; on conjecture qu'elle s'étend analytiquement à tout le plan $\mathbb{C}$, qu'elle a une équation fonctionnelle similaire à celle de la fonction zêta de Riemann (mais par rapport à $s \mapsto 2 - s$), etc.

Cela ne semble rien avoir à voir avec $h(\Delta)$. Cependant, en 1976, Goldfeld a fait une découverte surprenante. Il a prouvé que l'existence d'une seule courbe elliptique E sur $\mathbb{Q}$ pour laquelle $L_E(s)$ satisfait les conjectures précédentes et a un zéro en $s = 1$ avec une multiplicité d'au moins 3 implique

$$h(\Delta) \geq C_E \log |\Delta|$$

pour tous[3] les Δ, avec un C_E positif qui est effectivement calculable. (Comment une hypothèse sur une courbe elliptique peut-elle impliquer quoi que ce soit sur $h(\Delta)$? Eh bien, c'est l'un des nombreux mystères de la théorie des nombres...)

3. Ceci est correct uniquement lorsque $h(\Delta)$ est impair ; l'énoncé général est légèrement différent, voir, par exemple, [1].

Le théorème de Goldfeld nous dit que *si* nous pouvons trouver une courbe elliptique E avec les propriétés requises, alors $h(\Delta)$ tend vers l'infini effectivement lorsque $\Delta \to \infty$. Il reste à trouver une telle courbe.

Il existe des courbes elliptiques, dérivées de formes modulaires et appelées “courbes de Weil”, pour lesquelles l'holomorphie de la série L et l'équation fonctionnelle sont connues. Si nous choisissons pour E une telle courbe, la seule autre propriété requise est que $L_E(s)$ s'annule en $s = 1$ avec une multiplicité de 3 ou plus. La “conjecture de Birch et Swinnerton-Dyer” prédit quand cela devrait se produire, notamment lorsque le rang du groupe $E(\mathbb{Q})$ des points rationnels de E est ≥ 3. Il est facile de trouver de telles courbes E. Il faut ensuite prouver

$$L_E(1) = 0, \qquad L'_E(1) = 0, \qquad L''_E(1) = 0.$$

En utilisant l'équation fonctionnelle de L_E (que l'on peut fixer avec un signe moins), cela se réduit à prouver que $L'_E(1) = 0$. Mais comment le montrer ? Bien sûr, un ordinateur peut vérifier que

$$L'_E(1) = 0,0000000000\ldots$$

avec une précision de 10 décimales. Mais ce n'est pas suffisant : le théorème exige que $L'_E(1)$ soit *exactement* égal à 0.

Aucune solution à cette difficulté n'a été trouvée pendant environ 7 ans, et par conséquent, la méthode de Goldfeld n'a pas pu être appliquée.

Le progrès suivant a eu lieu en 1983, lorsque Gross et Zagier ont trouvé une formule fermée pour $L'_E(1)$. En l'utilisant, ils ont pu trouver une courbe de Weil E satisfaisant toutes les hypothèses de Goldfeld. La constante correspondante C_E a été calculée par Oesterlé et s'est avérée égale à $1/7000$.

Pour voir concrètement ce que cela signifie, appliquons ces idées au problème de la détermination des Δ avec $h(\Delta) = 3$. La borne de Goldfeld donne $|\Delta| \leq e^{21000} < 10^{9200}$. Il ne nous reste donc qu'un ensemble fini de Δ à étudier. Malheureusement, cet ensemble est trop grand.

Si la borne 10^{9200} pouvait être abaissée à 10^{2500}, on pourrait appliquer un résultat de Montgomery-Weinberger indiquant que, dans cet intervalle, le plus grand Δ négatif avec $h(\Delta) = 3$ est $\Delta = -907$. (Il est certainement possible d'étendre la méthode de Montgomery-Weinberger, mais cela nécessiterait beaucoup de calculs informatiques.)

Heureusement, il existe de meilleures courbes elliptiques que celle utilisée par Gross-Zagier. Récemment [4], Mestre a étudié la courbe de rang 3

$$y^2 + y = x^3 - 7x + 6.$$

Il a pu montrer qu'il s'agit d'une courbe de Weil (cela a également nécessité des calculs informatiques ; voir une note récente de lui, aux *Comptes Rendus de l'Académie des Sciences*), et, en

4. Ce travail de Mestre a été achevé peu après ma conférence à Singapour (février 1985).

utilisant le théorème de Gross-Zagier, que sa série L a un triple zéro en $s = 1$. Le constante C_E correspondant s'avère être $\geq 1/55$. Pour $h(\Delta) = 3$, cela donne

$$|\Delta| \leq e^{165} < 10^{72},$$

ce qui est bien inférieur à 10^{2500}, la valeur de Montgomery-Weinberger. Le problème du nombre de classes 3 est ainsi résolu. Nul doute que la même méthode fonctionnera pour d'autres petits nombres de classes, jusqu'à 100, par exemple.

Bien sûr, ce n'est pas la fin de l'histoire. Nous aimerions avoir des bornes inférieures effectives pour $h(\Delta)$ de l'ordre d'une certaine puissance de $|\Delta|$, plutôt que de $\log|\Delta|$. Mais comment les obtenir ? Devrons-nous attendre que l'hypothèse de Riemann généralisée (HRG) soit prouvée ? Cela pourrait prendre un certain temps...

Références

1. Oesterlé, J., Nombres de classes des corps quadratiques imaginaires, Séminaire Nicolas Bourbaki 1983-84, *Astérisque* 121-122, Exposé 631.

2. Zagier, D., Séries L de courbes elliptiques, conjecture de Birch-Swinnerton-Dyer et problème du nombre de classes de Gauss, *Notices of the American Mathematical Society* 31, 739-743 (1984).