Séminaire de philosophie et mathématiques

G. Lachaud

Irrationnels et formes quadratiques binaires, de Platon à Gauss

Séminaire de Philosophie et Mathématiques, 1991, fascicule 1
« $b^2 - 4ac > 0$ », , p. 1-15

<http://www.numdam.org/item?id=SPHM_1991___1_A1_0>

Table des Matières

Table chronologique

Théodore	fl. – 400	Wallis	1616 – 1703
Euclide	fl. – 300	Lord Brouncker	1620 – 1684
Archimède	– 287 – – 212	Euler	1707 – 1783
Théon de Smyrne	ca. + 100	Lagrange	1736 – 1813
Diophante	ca. + 200	Legendre	1752 – 1833
Bhaskhara	1114 – ?	Gauss	1777 – 1855
Fermat	1601 – 1665	.....	.....

§1. les racines historiques

1.1. la genèse

Mis à part le nombre π, les irrationnels que l'on rencontre de prime abord sont les irrationnels quadratiques. Par exemple, **Platon**, dans le Théétète (147 d)[1] affirme que Théodore connaissait l'irrationnalité de $\sqrt{n}$ pour $n = 3, 5, \ldots, 17$. L'omission de la valeur $n = 2$ laisse penser que c'est là une affaire classée ; et pourtant **Aristote** (ca.- 350) prend soin d'évoquer des arguments de parité à propos de l'irrationnalité de $\sqrt{2}$. En fait, tout revient à montrer que l'équation $p^2 = 2q^2$ n'a pas de solution $(p, q) \in \mathbf{Z}^2$. Faute de pouvoir résoudre l'équation

$$p^2 - 2q^2 = 0,$$

on va chercher des solutions de

$$p^2 - 2q^2 = 1,$$

ce qui revient à

$$\frac{p^2}{q^2} - 2 = \frac{1}{q^2},$$

et plus le nombre q est grand, meilleure sera l'approximation de $\sqrt{2}$ par le nombre rationnel p/q. C'est ce que fait **Théon de Smyrne** (ca. + 50) en construisant deux suites (p_n) et (q_n) de nombres entiers dont les quotients approchent $\sqrt{2}$: si on pose

$$p_0 = 1, \quad q_0 = 1,$$
$$p_{n+1} = p_n + 2q_n, \quad q_{n+1} = p_n + q_n,$$

on a

$$p_n^2 - 2q_n^2 = (-1)^{n-1}.$$

On peut aussi interpréter certains passages de Platon dans la même direction[2].
La même démarche peut être accomplie pour le nombre d'or φ : si on pose cette fois-ci

$$p_0 = 1, \quad p_1 = 2,$$
$$p_{n+1} = p_n + p_{n-1}, \quad q_n = p_n,$$

on a

$$p_n^2 - p_n q_n - q_n^2 = (-1)^{n-1},$$

la suite des nombres $\varphi_n = p_n/q_n$ vérifie

---

[1] cf. en particulier l'étude de Kahane (1986)

[2] cf. Van der Waerden, (1983), p. 134-136.

$$\varphi_n^2 = \varphi_n + 1 \pm \frac{1}{\varphi_n^2},$$

et cette suite converge vers un nombre φ tel que

$$\varphi^2 = \varphi + 1.$$

On vient de contourner l'obstacle de la façon suivante : puisque la résolution de l'équation $x^2 = 2$ (comme celle de l'équation $\varphi^2 = \varphi + 1$) est sans espoir, on a essayé de résoudre les équation $x^2 \approx 2$ et $\varphi^2 \approx \varphi + 1$, i. e. de trouver des solutions approchées ; le plus surprenant est qu'il existe des procédés **arithmétiques** de résolution de telles équations approchées.

Citons encore Archimède qui affirme sans explication que

$$\frac{265}{153} < \sqrt{3} < \frac{1351}{780};$$

en notant x et y le numérateur et le dénominateur de ces fractions, on a

$$x^2 - 3y^2 = 1,$$

$$x^2 - 3y^2 = -2;$$

et le problème des boeufs porte sur la résolution de l'équation

$$x^2 - Ny^2 = 1, \text{ avec } N = 4\,729\,494.$$

Plus près de nous, Bhaskara a donné un algorithme de construction de solutions de telles équations dans certains cas, basé sur l'identité

$$(x^2 - Ny^2)(z^2 - Nt^2) = (xz \pm Nyt)^2 - N(xt \pm yz)^2.$$

1.2. les calculs de Diophante.

Nous allons voir que l'on peut résoudre en nombres rationnels l'**équation de Pell**

(†) $\qquad y^2 - Nx^2 = 1,$

où N est un entier naturel, dans le cas "le plus simple" en un sens qui sera précisé, en utilisnat la méthode de la corde de Diophante. Le point P = (0, 1) appartient à l'hyperbole H d'équation (†) dans le plan affine ; il est à coordonnées rationnelles ; donc toute droite D issue de P rencontrera H en un autre point Q, qui sera nécessairement aussi à coordonnées rationnelles ; et si la droite est "générique", le point Q le sera aussi. L'équation d'une droite "générique" passant par P est

$$y = tx + 1,$$

où t est "générique" ; en reportant cette équation dans (†), il vient

(††) $\qquad x = \frac{2t}{N - t^2}, \qquad y = \frac{N + t^2}{N - t^2}$

On peut aussi voir la situation en coordonnées homogènes : en posant

$$x = \frac{Y}{X}, \qquad y = \frac{Z}{X}, \qquad t = \frac{U}{V},$$

on obtient l'équation

$$X^2 + NY^2 - Z^2 = 0;$$

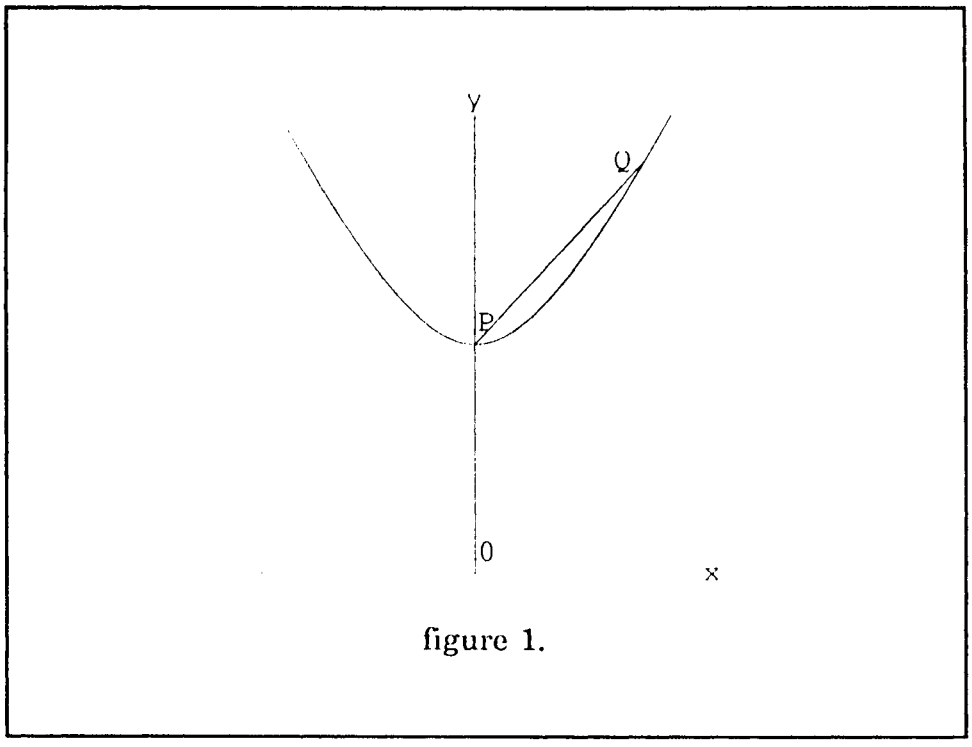


figure 1.

on déduit de (††) que les solutions à coefficients entiers avec pgcd(X, Y, Z) = 1 de cette équation s'écrivent

$$X = \pm (NU^2 - V^2), \quad Y = \pm 2UV, \quad Z = \pm (NV^2 + U^2),$$

avec des entiers (U, V) tels que pgcd(U, V) = 1. Si on fait N = 1, on retrouve l'**équation de Pythagore** et ses solutions classiques, qui figurent dans **Euclide** (Él., X. 28), mais remontent sans doute aux babyloniens (tablette **Plimpton 322**)[3]. En divisant par Y, on trouve les solutions rationnelles de l'équation

$$X^2 - Z^2 = N$$

qui sont exactement celles données par Diophante dans le Problème II. 10 des **Arithmétiques**[4], et qu'il a calculées par un procédé qui est celui décrit ici.

Le premier à avoir donné une interprétation géométrique des méthodes de Diophante semble bien être Isaac **Newton**, justement à propos des équations du second et du troisième degré (méthode de la corde et de la tangente) [Newton 1670's, 192-193 et 238-239].

1.3. application au calcul de $\sqrt{N}$

Soit $t \neq 0$; le nombre

$$z = \frac{y}{x} = \frac{N + t^2}{2t}$$

---

[3] cf. Weil (1984), p. 8, Van der Waerden, (1954), p. 78.

[4] cf. [4], tome III, p. CXII.

vérifie

$$z^2 - N = \varepsilon^2 \qquad \text{avec} \qquad \varepsilon = \frac{N - t^2}{2t} \ ;$$

autrement dit le nombre z est une **approximation (par excès) de $\sqrt{N}$, avec** une erreur sur les carrés exactement égale à ε^2. **Notons [x] la partie entière d'un nombre** x ; il est clair que la solution de l'équation **ci-dessus avec $N - t^2$ minimum est** obtenue en prenant $t = T = [\sqrt{N}]$; l'approximation **obtenue s'écrit**

$$z = \frac{N + T^2}{2T} = \frac{1}{2}\left(N + \frac{N}{T}\right)$$

Cette formule remonte sans doute aussi aux **babyloniens (tablette YBC 7289)**[5] et a été redonnée par **Héron** et même **Newton.**

1.4. solutions entières de l'équation de Pell

Lorsque $N - T^2$ divise $2T$, c'est-à-dire lorsque

$$N = T^2 + C \text{ avec } C = \frac{2T}{A} \ ,$$

alors la solution (††) de l'équation de Pell **est en nombres entiers :**

$$x = A, \qquad y = 1 + TA \ ;$$

l'approximation de $\sqrt{N}$ ainsi obtenue est

$$z = \frac{y}{x} = T + \frac{1}{A} \ .$$

d'autre part soit θ le nombre tel que

$$\sqrt{N} = T + \frac{1}{\theta} \ ;$$

on a

$$\theta = A + \frac{1}{T + \sqrt{N}} \ ;$$

autrement dit

$$\sqrt{N} = T + \cfrac{1}{A + \cfrac{1}{2T + \sqrt{N}}} \ ,$$

et l'approximation de $\sqrt{N}$ par z revient à "**négliger" la deuxième fraction** intérieure. Par exemple pour $N = 677 = 26^2 + 1$ on trouve

$$z = 26,019\,230 \ldots \qquad \text{et} \qquad \sqrt{N} = 26,019\,224 \ldots$$

On va voir que ce cas particulier est susceptible de **généralisation.**

---

5 cf. [VdW], p. 45.

§ 2. la théorie des formes quadratiques binaires[6]

2.1. fractions continues

Si $x \in \mathbf{R}$, le nombre **déduit** de x est par définition le nombre $\partial x \geq 1$ tel que

$$x = [x] + \frac{1}{\partial x} .$$

Si x_0 est un nombre réel, on note $x_n = \partial^n x$ la suite des déduits successifs de x ; ainsi

$$\begin{aligned}
x_0 &= r_0 + \frac{1}{x_1} , & r_0 &= [x_0], \\
x_1 &= r_1 + \frac{1}{x_2} , & r_1 &= [x_1], \\
&\dots & &\dots \\
x_{n-1} &= r_{n-1} + \frac{1}{x_n} , & r_{n-1} &= [x_{n-1}], \\
&\dots & &\dots
\end{aligned}$$

etc., et on peut poursuivre cette opération tant que $x_{n-1} \notin \mathbf{Z}$. Il ne s'agit de rien d'autre que de l'algorithme d'Euclide, qui consiste à itérer l'opération

$$\partial(a, b) = (b, a - b\,[\frac{a}{b}]),$$

de telle sorte que l'on obtient une **fraction continue** :

$$x = [\, r_0, r_1, \dots, r_{n-1}, x_n] = r_0 + \cfrac{1}{r_1 + \cfrac{1}{\dots + \cfrac{1}{r_{n-1} + \cfrac{1}{x_n}}}} .$$

Les entiers $r_0, r_1, \dots, r_{n-1}$ sont les **quotients partiels** de la fraction continue.

Le nombre x est rationnel si et seulement si sa fraction continue s'arrête, i.e. si $\partial^{m-1} x \in \mathbf{Z}$ pour un certain $m \geq 1$. Dans les **Additions**, Lagrange attribue la première apparition des fractions continues dans le traité de Lord Brouncker, et leur étude systématique à Huyghens.

On a

---

[6] On trouvera dans Weil (1984) une analyse historique complète du sujet, dont nous nous sommes inspirés ; on trouvera dans Lachaud (1988) un exposé détaillé de ce qui suit.

$$[\, r_0, r_1, \dots, r_n] = \frac{p_n}{q_n} \ ,$$

où les suites (p_n) et (q_n) sont définies par les relations de récurrence suivantes :

$$p_{-1} = 1, \quad p_0 = r_0, \qquad q_{-1} = 0, \quad q_0 = 1,$$

$$p_n = r_n\, p_{n-1} + p_{n-2}, \qquad q_n = r_n\, q_{n-1} + q_{n-2}.$$

Les nombres $[\, r_0, r_1, \dots, r_n]$ convergent vers x ; par exemple

$$\pi = [3, 7, 15, 1, 292, 1, 1, \dots\,] .$$

2.2. l'algorithme de base pour l'équation de Pell

Soit N un entier donné, non carré. L'équation de Pell

$$x^2 - Ny^2 = \pm 1, \qquad (x, y) \in \mathbf{Z}^2.$$

a été proposée en 1657 par Fermat (cf. Weil (1977), Weil (1984)) aux mathématiciens anglais ; et ceux-ci (Wallis, Brouncker) la résolurent en fournissant les solutions. On trouvera l'algorithme de Wallis décrit dans Weil (1977) ; un algorithme voisin est donné par Euler (1770), IIe partie, Ch. VII.

Un algorithme de résolution voisin repose sur l'énoncé suivant[7]. Posons $x_0 = \sqrt{N}$, et pour $n \geq 1$ posons

$$x_{n-1} = r_{n-1} + \frac{1}{x_n} \qquad \text{avec } r_{n-1} = [x_{n-1}] \ ;$$

définissons les suites (p_n) et (q_n) comme ci-dessus.

Théorème 1. On a

$$p_{m-1}^{\,2} - N q_{m-1}^{\,2} = +1$$

pour un certain entier $m \geq 1$.

Exemple (Wallis) N = 13 : voir la figure 2.

Fermat a toujours affirmé qu'il manquait aux anglais "la démonstration générale". Pour comprendre un tel résultat, il a fallu attendre Lagrange (1774) ; et pour l'exposer, il nous faut venir à la théorie générale des formes quadratiques binaires, développée par Gauss dans la cinquième section des Disquisitiones Arithmeticae.

---

[7] ceci est l'algorithme de base ; en fonction de la forme de N, ou de l'allure de la fraction continue de $\sqrt{N}$, on peut souvent donner des algorithmes plus rapides ; cf. Richaud (1866), etc.

N = 13 $\qquad n_i = p_i^2 - 13\,q_i^2$

$x_0 = \sqrt{13},$	$r_0 = 3,$	$p_0 = 3,$	$q_0 = 1,$	$n_0 = -4,$
$x_1 = \dfrac{3+\sqrt{13}}{4},$	$r_1 = 1,$	$p_1 = 4,$	$q_1 = 1,$	$n_1 = 3,$
$x_2 = \dfrac{1+\sqrt{13}}{3},$	$r_2 = 1,$	$p_2 = 7,$	$q_2 = 2,$	$n_2 = -3,$
$x_3 = \dfrac{2+\sqrt{13}}{3},$	$r_3 = 1,$	$p_3 = 11,$	$q_3 = 3,$	$n_3 = 4,$
$x_4 = \dfrac{1+\sqrt{13}}{4},$	$r_4 = 1,$	$p_4 = 18,$	$q_4 = 5,$	$n_4 = -1,$
$x_5 = 3+\sqrt{13},$	$r_5 = 6,$	$p_5 = 119,$	$q_5 = 33,$	$n_5 = 4,$
$x_6 = \dfrac{3+\sqrt{13}}{4},$	$r_6 = 1,$	$p_6 = 137,$	$q_6 = 38,$	$n_6 = -3,$
$x_7 = \dfrac{1+\sqrt{13}}{3},$	$r_7 = 1,$	$p_7 = 256,$	$q_7 = 71,$	$n_7 = 3,$
$x_8 = \dfrac{2+\sqrt{13}}{3},$	$r_8 = 1,$	$p_8 = 393,$	$q_8 = 109,$	$n_8 = -4,$
$x_9 = \dfrac{1+\sqrt{13}}{4},$	$r_9 = 1,$	$\mathbf{p_9 = 649,}$	$\mathbf{q_9 = 180,}$	$\mathbf{n_9 = 1,}$

$(x, y) = (649, 180) \qquad x^2 - 13y^2 = 1 \qquad m = 10$

figure 2.

2.3. formes quadratiques indéfinies

Le trinôme[8]

$$Q(X, Y) = aX^2 + bXY + cY^2,$$

où a, b, c sont dans **Z** est appelé une forme quadratique binaire **entière**[9] et de discriminant

$$D = b^2 - 4ac.$$

On a $D \equiv 0$ ou $1 \pmod 4$. On suppose que (a, b, c) = 1 (i.e. que Q est une forme **primitive**) et que D n'est pas un carré (i.e. que Q est **irréductible**). On note Q = [a, b, c] la forme ci-dessus[10]. On note **Quad**(D) l'ensemble des formes quadratiques binaires entières primitives et irréductibles de discriminant D.

Les groupes $\Gamma = PGL(2, \mathbf{Z})$ et $\Gamma_0 = PSL(2, \mathbf{Z})$ opèrent sur **Quad**(D) par

$$Q \circ S(\mathbf{X}) = Q(S\mathbf{X}),$$

ce qui permet de parler de **classes** de formes équivalentes : **équivalence au sens strict** ou **étroit** si $S \in PSL(2, \mathbf{Z})$ et **équivalence au sens large**[11] si $S \in PGL(2, \mathbf{Z})$.

On note H(D) l'ensemble quotient **Quad**(D)/Γ des classes d'équivalence larges, et h(D) le nombre d'éléments de H(D) ; c'est le **nombre de classes** de **Quad**(D).

On ne s'occupe ici que du cas D > 0.

On va montrer que le nombre de classes est fini ; mais nous avons besoin de résultats intermédiaires.

Si D > 0 la forme Q est **indéfinie** ou **isotrope** sur le corps **R** des nombres réels : on a

$$Q(X, Y) = a\,(X - Yx^+)\,(X - Yx^-),$$

avec

$$x^+ = \frac{-b + \sqrt{D}}{2a} = \frac{2c}{-b - \sqrt{D}}, \quad x^- = \frac{-b - \sqrt{D}}{2a} = \frac{2c}{-b + \sqrt{D}}.$$

Le nombre x est un irrationnel quadratique réel, et son équation minimale s'écrit

$$ax^2 + bx + c = 0.$$

Le groupe Γ agit aussi sur les irrationnels quadratiques réels :

$$\gamma x = \frac{ax+b}{cx+d} \qquad \text{pour} \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

---

[8] Pour une introduction à la théorie des formes quadratiques binaires , on renvoie à Borevitch & Chafarevitch (1967), ou encore à Weil (1984).

[9] Il s'agit de formes entières au sens naïf, i. e. les coefficients de la forme Q sont dans **Z**. Les formes entières au sens de Gauss sont celles pour lesquelles b/2 est entier, i. e celles dont la forme bilinéaire associée est à coefficients dans **Z**.

[10] C'est à peu près la notation de Gauss.

[11] Dans la terminologie de Gauss (cf. Gauss (1801), n° 158, p. 122), les formes Q et $Q \circ \gamma$ sont dites **proprement** équivalentes si $\det \gamma = +1$ et **improprement** équivalentes si $\det \gamma = -1$.

Le nombre ∂x est équivalent à x : on a

$$x = \gamma.\partial x \text{ avec } \gamma = \begin{pmatrix} r & 1 \\ 1 & 0 \end{pmatrix}, \; r = [x] .$$

L'opération ∂ applique l'ensemble des nombres irrationnels quadratiques réels dont l'équation minimale a pour discriminant D dans lui-même.

On dit qu'un irrationnel quadratique réel est **réduit** s'il satisfait à la condition :

$$x > 1 \qquad \text{et} \qquad -1 < x' < 0.$$

Les résultats de Lagrange[12] s'énoncent comme suit :

Théorème 2 (IQR). Pour tout irrationnel quadratique réel x, le nombre $\partial^n x$ est réduit pour n assez grand.

Théorème 3 (IQR). le nombre x est réduit si et seulement si la fraction continue de x est purement périodique.

Les théorèmes 2 et 3 impliquent que tout irrationnel quadratique réel a un développement en fraction continue périodique à partir d'un certain rang :

$$x = [\, s_1, \ldots, s_l ; \overline{r_1, \ldots, r_m}] = s_1 + \cfrac{1}{\ddots + \cfrac{1}{s_l + \cfrac{1}{r_1 + \cfrac{1}{\ddots + \cfrac{1}{r_m + \cfrac{1}{r_1 + \cfrac{1}{\ddots}}}}}}}$$

Si x est réduit, l'application $n \to \partial^n x$ est périodique ; le plus petit entier $m(x) = m > 0$ tel que $\partial^m x = x$ s'appelle le **calibre** de x, et la suite d'entiers naturels $(r_1, \ldots, r_m)$ est la **période** (primitive) de x.

Par exemple, si

$$N = T^2 + C \text{ avec } C = \frac{2T}{A} ,$$

on a

$$\sqrt{N} = [T, A, 2T, A, 2T, A, \ldots] ,$$

avec un calibre égal à 2, et même égal à 1 si C = 1.

---

[12] cf. Lagrange (1774).

2.4. réduction des formes indéfinies

Si on écrit

$$Q(X, Y) = a\,(X - Yx)\,(X - Yx'),$$

avec $x > x'$, le nombre x est **réduit** si et seulement si la forme $Q = [a, b, c]$ satisfait aux conditions suivantes de Gauss[13] :

(R) $\quad a > 0, \quad b < 0, \quad c < 0, \quad |b| < \sqrt{D},$

$$\sqrt{D} - |b| < 2a < \sqrt{D} + |b|.$$

On dit qu'une telle forme est **réduite**.

Théorème 4. Il n'y a qu'un nombre fini de formes réduites de discriminant D.

En effet, le système de conditions (R) implique

$$\mathrm{Max}(|a|, |b|, |c|) < \sqrt{D}.$$

Si $Q = [a, b, c]$ est dans **Quad**(D), la **forme déduite** de Q est la forme

$$\partial Q(X, Y) = -\,Q(rX+Y, Y) \qquad \text{où } r = [x] ;$$

on obtient ainsi une application ∂ de **Quad**(D) dans lui-même ; et la forme ∂Q est équivalente à Q.

Puisque la première racine de ∂Q est égale à ∂x^+, en notant x^+ la première racine de Q, le théorème de Lagrange se reprend textuellement en termes de formes quadratiques[14] :

Théorème 2 (FQ). Pour toute forme $Q \in$ **Quad**(D), la forme $\partial^n Q$ est réduite pour n assez grand.

Théorème 3 (FQ). La forme Q est réduite si et seulement si il existe un entier $m > 0$ tel que $\partial^m Q = Q$.

Ces théorèmes vont nous permettre de démontrer le théorème 1. Prenons

$$Q_0 = X^2 - NY^2$$

et posons $Q_n = \partial^n Q = [a_n, b_n, c_n]$ pour $n \geq 0$; il est facile de voir que

$$Q_0(p_{n-1}, q_{n-1}) = (-1)^n\, Q_n(1, 0) = (-1)^n\, a_n ;$$

---

[13] cf. Gauss (1801), n° 183, p. 159.

[14] cf. Weil (1984)

la forme Q_1 est réduite ; par le théorème 3 (FQ), il y a un entier m tel que $Q_{m+1} = Q_1$, d'où l'on voit facilement que $a_m = 1$; on trouve donc

$$Q_0(p_{km-1}, q_{km-1}) = (-1)^{km},$$

ce qui prouve le théorème 1.
On peut montrer que ce sont là les seules solutions de l'équation de Pell ; A. Weil (1984) en a proposé une démonstration "comme Fermat aurait pu la faire".

On observera que m = 2 si

$$N = T^2 + C \text{ avec } C = \frac{2T}{A} ;$$

c'est en ce sens que les irrationnels de cette forme sont "les plus simples".

J.P. Kahane (cf. [Kahane 1985]) a cherché à expliquer pourquoi, dans ses démonstrations de l'irrationalité des racines, Théodore s'est arrêté à $\sqrt{17}$. On peut voir le calibre d'un nombre irrationnel comme une mesure de la **complexité** de ce nombre. Or les nombres $\sqrt{N}$, pour $2 \leq N \leq 17$, sont de calibre 5 au plus alors que $\sqrt{19}$ est de calibre 6. D'autre part, pour $N \leq 17$ on peut toujours trouver dans le corps $\mathbf{Q}(\sqrt{N})$ des irrationnels de calibre 1 ou 2 ; ce sont des solutions de l'équation de Pell, i.e. des unités de $\mathbf{Q}(\sqrt{N})$; la faisabilité de la preuve dépend de la valeur absolue de la plus petite solution de cette équation ; or pour $2 \leq N \leq 17$, ces raisons sont ≤ 30 alors que pour N = 19 cette raison est égale à $170 + 39\sqrt{19} \approx 340$ et toute figure devient impossible.

2.5. calibre

On tire du théorème 2 (FQ) que **toute forme est équivalente à une forme réduite** ; par suite :

Théorème 5. Le nombre de classes h(D) est fini.

Supposons $D = 4N$ où $N \equiv 2$ ou $3 \pmod 4$. On peut montrer que $h(D) = 1$ si et seulement si l'anneau $\mathbf{Z}[\sqrt{N}]$ est principal. Gauss pensait déjà qu'il y a une infinité de valeurs de D pour lesquelles $h(D) = 1$. On conjecture actuellement[15] que $h(D) = 1$ dans 75, 445 % des cas, alors qu'il n'y a que 9 valeurs de D pour lesquelles $h(-D) = 1$. On va montrer que le calibre joue pour les discriminants > 0 le rôle du nombre de classes pour les discriminants négatifs.

---

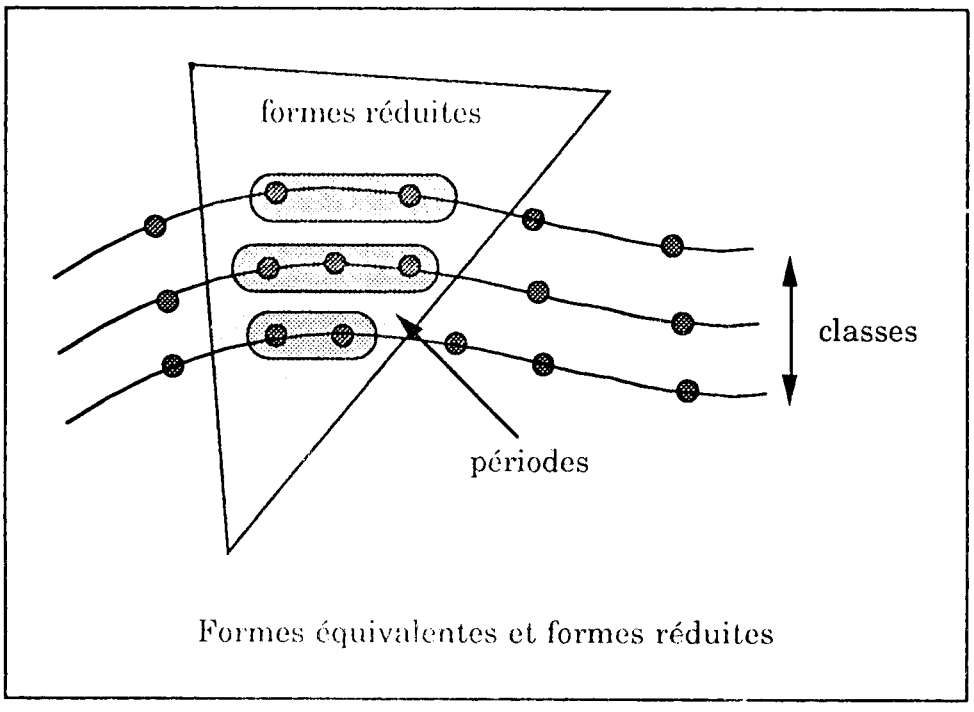
[15] cf. Cohen-Martinet (1987).

Si $Q \in$ **Quad**(D) a pour première racine x, la période de x ne dépend que de la classe d'équivalence large C de Q ; on appelera **calibre** de la classe C la longueur m(C) de cette période. Si le nombre x est réduit, on peut voir que les seuls nombres réduits qui lui sont équivalents sont exactement les $\partial^n x$, i.e. ceux que l'on obtient par une permutation circulaire de la période : ils sont donc en nombre égal au calibre de x. Par suite :

Théorème 6. Le nombre $\kappa(D)$ de formes réduites de discriminant D est égal à la somme des calibres des classes de formes de discriminant D :

$$\kappa(D) = \sum_{C \in H(D)} m(C).$$

Le nombre $\kappa(D)$ est le **calibre total** du discriminant D.



Formes équivalentes et formes réduites

Exemple. – Regardons le cas D = 40. Les formes réduites de discriminant 40 sont :

$Q_0 = [1, -6, -1]$; $x_0 = 3+\sqrt{10} = [\overline{6}]$ (calibre 1)

$Q_1 = [3, -2, -3]$; $x_1 = \dfrac{1+\sqrt{10}}{3} = [\overline{1}, \overline{2}, \overline{1}]$ (calibre 3)

$Q_2 = [2, -4, -3]$; $x_2 = \dfrac{2+\sqrt{10}}{2} = [\overline{2}, \overline{1}, \overline{1}]$ (calibre 3)

$Q_3 = [3, -4, -2]$; $x_3 = \dfrac{2+\sqrt{10}}{3} = [\overline{1}, \overline{1}, \overline{2}]$ (calibre 3)

par suite la classe principale est de calibre 1 et la classe de x_1 est de calibre 3 : on a

$h(40) = 2, \quad m(Q_0) = 1, \quad m(Q_1) = 3, \quad \kappa(40) = 4.$

Pour D > 0, le nombre $\kappa(D)$ joue un rôle analogue à celui joué par le nombre h(D) pour D < 0 : c'est le nombre de formes réduites dans les deux cas.
Frobenius (1912) a posé la question suivante : chercher les discriminants de calibre total 1, i.e. tels que $\kappa(D) = 1$; c'est une condition plus forte que la condition h(D) = 1.
Si D est un tel nombre, alors D = 2 ou $D = T^2 + 4$ avec T impair.
Lorsque $D \equiv 1 \pmod 4$, l'équation qui joue le rôle de l'équation de Pell est

$$Q_0(x, y) = x^2 + xy - \frac{D-1}{4} y^2 = \pm 1 ;$$

Lorsque $D = T^2 + 4$ avec T impair, la méthode de la corde donne la solution

$x_0 = T, y_0 = 1, Q_0(x_0, y_0) = -1.$

Théorème 7[16] . Si l'hypothèse de Riemann est satisfaite, les seuls discriminants de calibre 1 sont les sept valeurs suivantes :

D = 2, 5, 13, 29, 53, 173, 293.

Pour D > 2, on a $D = T^2 + 4$ avec

T = 1, 3, 5, 7, 13, 17 ;

ce sont tous les entiers $T \leq 17$ tels que $D = T^2 + 4$ soit premier ; on revient à la limite de Théodore !

---

[16] cf. Lachaud (1987).

bibliographie

BOREVITCH, Z.I., CHAFAREVITCH, I.R., **Théorie des Nombres**, Gauthier-Villars, Paris, 1967.

COHEN, H., MARTINET, J., **Class Groups of Number Fields : Numerical Heuristics**, Math. Comp. **48** (1987), p. 123-137.

DAVENPORT, H, **The Higher Arithmetic**, 5th edition, Cambridge, Cambridge University Press, 1982.

DIOPHANTE, **Les Arithmétiques**, livre IV et livres V à VII (texte arabe), éd. par R. Rashed, notes math. par G. Lachaud et R. Rashed, Les Belles Lettres, Paris, 1984.

EULER, L., **Vollständige Anleitung zur Algebra**, St Petersburg 1770 ; Opera Omnia, Ser. I, vol. I, Teubner, Leipzig & Berlin, 1911 ; engl. trad., Longman, Orme & Co., London, 1840 ; reprint, Springer, New-York Heidelberg Berlin, 1984.

FROBENIUS, F.G., **Über quadratische Formen, die viele Primzahlen darstellen**, Sitz. König. Preußischen Akad. der Wiss. zu Berlin, (1912), 966-980 ; = Ges. Abhand., Band III, n° 94, p. 573-587, Springer, Berlin, 1968.

GALOIS, E., **Démonstration d'un théorème sur les fractions continues périodiques**, Ann. de M. Gergonne (1828-1829), p. 294 ; = Œuvres, Gauthier-villars, Paris, 1897, p.1-8.

GAUSS, C. F., **Disquisitiones arithmeticæ**, Fleisher, Lipsiae, 1801; = Werke Bd 1 ; engl. trans., Springer, New York, 1987

HARDY, G.H., WRIGHT, E. M. **An Introduction to The Theory of Numbers**, Oxford University Press, Oxford, 1938.

KAHANE, J.P., **La théorie de Théodore des corps quadratiques réels**, L'Enseignement Mathématique **31** (1985) 85-92.

LACHAUD, G., **On Real Quadratic fields**, Bull. Amer. Math. Soc. **17** (1987), p. 307-311.

LACHAUD, G., **Continued fractions, binary quadratic forms, quadratic fields, and zeta functions**, Proceedings of KIT Mathematics Workshop, K.I.T. Taejon, 1988, p.1-56.

LACHAUD, G., **Exactitude et Approximation en Analyse Diophantienne**, Actes du Colloque d'Urbino, "L'À peu près", Editions de l'E.H.E.S.S., Paris, & Il Lavoro Editoriale, Ancona, 1988, p. 27-45 ; à paraître dans Historia Mathematica.

LAGRANGE, J. L., **Additions à l'Analyse indéterminée [des éléments d'algèbre de M. Léonard Euler]** , Lyon, 1774 ; = in Euler (1770), etc.

NEWTON, I., (late 1670's) **The solutions of simple diophantine equations**, in Mathematical papers, vol. IV, pp. 74-75. University Press : Cambridge, 1971. **The generation of rational solutions from given instances**, De resolutione Qæstionum circa numeros, ibid., pp. 110-115.

RICHAUD, Casimir, **Sur la résolution des équations** $x^2 - Ay^2 = \pm 1$, Att. dell'Acc. Pont. de Nuovi Lincei (1866), p. 177-182.

VAN DER WAERDEN, B.L., **Science Awakening,** Wolters Noordhof Pub., Groningen, 1954.

VAN DER WAERDEN, B.L., **Geometry and Algebra in Ancient Civilisations**, Springer, Heidelberg, 1983.

WEBER, H., **Traité d'algèbre supérieure, t. I, tr. fr. Paris, Gauthier-Villars, 1898.**

WEIL, A., **Number Theory, An approach through history,** Birkhäuser, Boston, 1984.

WEIL, A., **Fermat et l'équation de Pell,** ΠΡΙΣΜΑΤΑ, Fr. Steiner Verlag, Wiesbaden 1977, p. 441-448 ; = Coll. Papers, [1977b], vol. III, p. 413-419.