Vieilles sorcelleries numériques

El. Math., *47*, (1992)

0013-6018/92/020076-06$1.50 + 0.20/0

Vieilles sorcelleries numériques

Manuel Ojanguren
Université de Lausanne

Manuel Ojanguren wurde 1940 in Lugano geboren. Nach der Matur am Liceo Cantonale di Lugano studierte er an der ETH Zürich Mathematik und Physik. Hier doktorierte er 1968 mit einer Arbeit in algebraischer Topologie. Nach Aufenthalten am Tata Institute in Bombay, dem Battelle Institut in Genf und an der Queen's University in Kingston wurde er 1974 Professor an der Universität Münster. Seit 1977 ist er Professor an der Université de Lausanne. Seine Hauptinteressen liegen im Gebiete der Algebra und der algebraischen Geometrie. In seinen Forschungsarbeiten beschäftigt er sich unter anderem mit der Brauer Gruppe und mit Quadratischen Formen.

Cet article a pour but d'illustrer la thèse selon laquelle les théorèmes sont faits pour expliquer les exemples; il s'adresse aux profanes car tout ce qu'il contient est bien connu depuis longtemps des mathématiciens.

Il y a, en mathématique, deux nombres dont on ne pourrait exagérer l'importance: le premier, noté π, est le rapport entre la circonférence et le diamètre d'un cercle; il vaut, de

Albert Einstein sagte einmal: "Das Schönste ... ist das Geheimnisvolle, das an der Wiege wahrer Kunst und Wissenschaft steht. Wer es nicht mehr kennt und sich nicht mehr wundern, nicht mehr staunen kann, der ist sozusagen tot und sein Auge erloschen." Die *Vieilles Sorcelleries Numériques* beginnen mit einer zahlentheoretischen Tatsache, die uns ohne weiteres zum Wundern und Staunen bringen kann:

$e^{\pi\sqrt{163}}$ *ist mit ausserordentlich grosser Genauigkeit eine ganze Zahl.*

"Wundersame" Tatsachen wie diese wollen erklärt und deren Gründe entdeckt werden. In seinem Beitrag stellt Manuel Ojanguren dar, weshalb $e^{\pi\sqrt{163}}$ diese überraschende Eigenschaft hat. Dazu müssen tiefere und abstrakte Begriffsbildungen wie quadratische Formen, Diskriminante, modulare Funktion, Klassenzahl usw benützt und entsprechende allgemeine Sätze der Zahlentheorie herangezogen werden. Ist es überraschend, dass die Erklärung am Ende zu neuen "wundersamen" Tatsachen und zu weiteren offenen Fragen führt?

Es handelt sich bei diesem Text um das Manuskript eines Vortrages; es erscheint hier ohne nachträgliche Änderungen, um die Unmittelbarkeit des gesprochenen Wortes zu bewahren. – Am Schluss des Beitrages findet sich eine Liste weiterführender Literatur. *ust*

nos jours, à peu près 3,14159265.... Je dis "de nos jours" car au temps du roi Salomon sa valeur était apparemment égale à 3 (I Rois VII, 23). Certains savants expliquent cet écart par l'hypothèse d'un changement de la métrique de l'univers. Mais je divague. R. à nos m. Le deuxième nombre, noté e, est défini par la somme infinie

$$1+\frac{1}{1}+\frac{1}{1\cdot 2}+\frac{1}{1\cdot 2\cdot 3}+\frac{1}{1\cdot 2\cdot 3\cdot 4}+\cdots$$

et vaut à peu près 2,71828182.... A première vue, π et e n'ont rien à faire l'un avec l'autre. Mais Leonhard Euler, le mathématicien dont les billets de dix francs ont l'honneur de porter l'effigie, découvrit la relation étonnante

$$e^{\pi\sqrt{-1}}=-1.$$

Comme la racine carrée d'un nombre négatif a un peu l'air d'une escroquerie, tâchons de trouver une relation encore plus jolie en remplaçant le -1 sous la racine et le -1 à droite du signe d'égalité par des entiers positifs. Si nous calculons $e^{\pi\sqrt{163}}$ avec 6 décimales exactes, nous trouvons

$$e^{\pi\sqrt{163}}\sim 262537412640768743,999999.$$

Le plus scrupuleux des banquiers n'hésiterait pas à arrondir. Mais soyons prudents et calculons encore quelques chiffres:

$$e^{\pi\sqrt{163}}\sim 262537412640768743,999999999999.$$

A ce point, même un mathématicien pourrait se laisser tenter. Faisons encore un petit effort:

$$e^{\pi\sqrt{163}}\sim 262537412640768743,9999999999992....$$

Zut! Pour avoir la photographie sur les billets de banque, il faudra mijoter autre chose. Mais y a-t-il une bonne raison pour que ce nombre bizarre soit si près d'un entier? En faisant quelques détours par la théorie des formes quadratiques et l'analyse, nous verrons qu'il y en a une. Commençons par les formes quadratiques. Il y a des nombres premiers qui sont sommes de deux carrés: $2=1^2+1^2$, $5=1^2+2^2$, $29=2^2+5^2$. Faisons la liste des premiers de ce type compris entre 3 et 100:

$$5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97;$$

et voici la liste des autres:

$$3,\ 7,\ 11,\ 19,\ 23,\ 31,\ 43,\ 47,\ 59,\ 67,\ 71,\ 79,\ 83.$$

Nous constatons que ceux de la première liste sont tous égaux à un multiple de 4 augmenté de 1, ceux de la deuxième à un multiple de 4 diminué de 1. Cette constatation expérimentale nous suggère la conjecture suivante: un premier impair est somme de deux carrés si et seulement s'il est égal à un multiple de 4 augmenté de 1. Ceci revient à dire

qu'on obtient tous les premiers de la forme $4n + 1$ et, à part 2, aucun autre, comme valeurs de $x^2 + y^2$ pour des valeurs entières de x et y. Pour démontrer des conjectures comme celle-ci (qui, soit dit en passant, est vraie, comme nous le verrons plus loin), on étudie les *formes quadratiques binaires*, c'est-à-dire les polynômes à deux variables du type

$$f(x,y) = ax^2 + bxy + cy^2,$$

où a, b et c sont des entiers fixés. Pour étudier les valeurs prises par f quand on attribue des valeurs entières à x et y (nous dirons que ce sont des valeurs *représentées* par f), nous pouvons nous permettre des substitutions du type $x = \alpha u + \beta v$, $y = \gamma u + \delta v$ où u et v sont de nouvelles variables et α, β, γ, δ des entiers tels que $\alpha\delta - \beta\gamma = 1$. En effet, un petit calcul montre que $u = \delta x - \beta y$ et $v = \alpha y - \gamma x$; par conséquent, toutes les valeurs entières de x, y s'obtiennent en donnant des valeurs entières à u, v. En remplaçant x par $\alpha u + \beta v$ et y par $\gamma u + \delta v$ dans $f(x,y)$, nous obtenons une forme quadratique

$$g(u,v) = Au^2 + Buv + Cv^2,$$

où A, B et C sont encore des entiers. On dit que g est *équivalente* à f, ou encore que f et g sont *dans la même classe*. Le but de cette opération est de trouver une forme équivalente à f qui soit plus facile à étudier que f. Par exemple, pour démontrer la conjecture sur les sommes de carrés, on peut procéder en deux étapes.

On démontre d'abord que si $p - 1$ est un multiple de 4, le nombre $(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2})^2 + 1$ est un multiple de p, donc égal à $p \cdot k$ où k est un certain entier. On démontre ensuite que la forme

$$g(x,y) = px^2 + 2\left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right)xy + ky^2$$

est équivalente à $x^2 + y^2$. Elle représente p, car $g(1,0) = p$. Donc f représente p. Ceci constitue la partie non banale de la conjecture, à savoir que tout premier p de la forme $4n + 1$ est somme de deux carrés. Mais comment décider si deux formes sont équivalentes? Prenons par exemple $p = 13$. En ce cas

$$g(x,y) = 13x^2 + 1440xy + 39877y^2$$

et on ne peut pas dire que l'équivalence entre $g(x,y)$ et $x^2 + y^2$ saute aux yeux! Il y a toutefois une fonction des coefficients de f qui est insensible aux changements de variables décrits plus haut: c'est le *discriminant*: $D = b^2 - 4ac$. Ainsi, deux formes équivalentes ont le même discriminant. Si on suspecte que deux formes sont équivalentes, il faut donc commencer par vérifier qu'elles ont le même discriminant. C'est le cas pour $x^2 + y^2$ et

$$px^2 + 2\left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right)xy + ky^2$$

car le discriminant de la première est

$$0^2 - 4 \cdot 1 \cdot 1 = -4$$

et celui de la deuxième

$$4\left(1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\right)^2 - 4pk = 4(pk-1) - 4pk = -4.$$

Si les formes en question passent ce premier test, on pousse l'analyse plus loin. Nous allons nous restreindre pour la suite aux formes *primitives* et *définies positives.*

Une forme est primitive si ses coefficients n'ont pas de diviseur commun. Elle est définie positive si elle ne prend que des valeurs strictement positives (sauf, bien entendu, pour $x = y = 0$). Ainsi, la forme x^2+y^2 est définie positive, tandis que les formes x^2-y^2, x^2, xy ne le sont pas. En bricolant un peu avec des changements de variables, on démontre qu'une forme f de cette espèce est toujours équivalente à une unique forme *réduite*

$$f^*(x,y) = ax^2 + bxy + cy^2$$

dont les coefficients satisfont les inégalités

$$0 < a \le \sqrt{\frac{|D|}{3}}, \qquad -a < b \le a \le c \quad \text{et si} \quad a = c,\ b \ge 0. \tag{*}$$

Si f et g ont même discriminant D, on calcule leurs réduites f^* et g^*. Celles-ci sont égales si et seulement si f et g sont équivalentes. Mais quelquefois les calculs sont superflus. Si, par exemple, $D = -4$, les coefficients d'une forme réduite doivent satisfaire les conditions

$$b^2 - 4ac = -4, \qquad |b| \le a \le c,\ a \le \sqrt{4/3}.$$

La seule possibilité est $a = 1$, $b = 0$, $c = 1$. Ceci prouve en particulier que la réduite de $px^2+2(1\cdot 2\cdot \ldots \cdot \frac{p-1}{2})xy+ky^2$ ne peut être que x^2+y^2. Ces deux formes sont donc bien équivalentes. Toutefois, il y a, en général, pour un même D, plusieurs formes réduites. Si, par exemple, $D = -23$, il y a trois formes réduites distinctes:

$$x^2 + xy + 6y^2,\ 2x^2 + xy + 3y^2,\ 2x^2 - xy + 3y^2.$$

Il est clair que, pour un D fixé, il n'y a qu'un nombre fini de ternes (a,b,c) satisfaisant les inégalités (*) et l'égalité $D = b^2 - 4ac$. Il ne peut donc y avoir qu'un nombre fini de formes réduites de discriminant D. Ce nombre, qui coïncide avec le nombre de classes de formes primitives, est noté $h(D)$ et s'appelle le *nombre de classes* de D.

Nous allons maintenant jeter un coup d'oeil sur les zéros d'une forme. Si $ax^2+bxy+cy^2 = 0$, x/y vaut, comme nous suggèrent nos souvenirs d'école, $(-b \pm \sqrt{D})/2a$. Puisque D est négatif, une racine carrée de D est le nombre imaginaire $i\sqrt{|D|}$. Nous dirons que "la" racine de f est le nombre complexe $\omega = \frac{-b+i\sqrt{|D|}}{2a}$, et nous ferons mine d'ignorer sa conjuguée $\bar{\omega} = \frac{-b-i\sqrt{|D|}}{2a}$. Il est facile de voir que les formes réduites sont précisément celles dont la racine est dans la région $\mathcal{R}$ du plan complexe (fig. 1, page suivante).

A toute forme f on peut donc associer un point ω de $\mathcal{R}$, qui ne dépend que de la classe de f: la racine de f^*. Si nous découpons dans le plan complexe la région $\mathcal{R}$ et

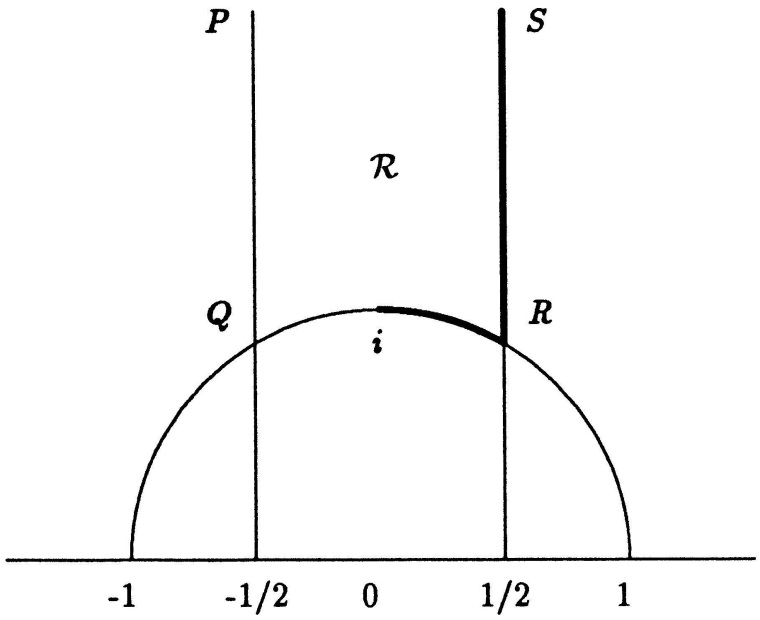

Fig. 1

si nous collons ensuite le bord PQi sur son symétrique SRi, nous obtenons une sorte de sac infiniment haut. En supposant que ce sac soit très élastique, nous pouvons élargir son ouverture et l'aplatir sur un deuxième plan complexe, de façon à faire coïncider le point $i = \sqrt{-1}$ avec le point 1728 et le point Q avec le point 0 (zéro). Or, la théorie des fonctions elliptiques nous fournit une fonction j, appelée fonction modulaire, qui réalise sur $\mathcal{R}$ les transformations que nous venons de décrire. Je renonce à en donner une définition explicite et je me contente de dire qu'elle a l'allure suivante: pour tout nombre complexe z dans $\mathcal{R}$, $j(z)$ est donné par une série:

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \ldots$$

où $q = e^{2\pi iz}$.

Il y a des liens profonds entre les formes quadratiques et la fonction modulaire. En voici un des exemples les plus frappants: si ω est le point de $\mathcal{R}$ qui correspond à une forme de discriminant D, $j(\omega)$ satisfait une équation

$$j(\omega)^h + a_1 j(\omega)^{h-1} + \ldots + a_h = 0$$

à coefficients *entiers*, de degré $h = h(D)$. Prenons $D = -163$ et calculons $h(D)$. Si $ax^2 + bxy + cy^2$ est une forme réduite de discriminant -163, on a $b^2 - 4ac = -163$, c'est-à-dire $4ac = b^2 + 163$, avec $|b| \leq a < \sqrt{163/3} \sim 7,37$ et $a \leq c$. En donnant à b les valeurs de 0 à 7, on trouve l'unique solution $a = 1$, $b = 1$, $c = 41$. La seule forme réduite de discriminant -163 est donc $x^2 + xy + 41y^2$. Sa racine est $\omega = \frac{-1+i\sqrt{163}}{2}$ et puisque $h(D)$ vaut 1, l'équation satisfaite par $j(\omega)$ est $j(\omega) + a_1 = 0$. Le nombre $j(\omega)$ est donc un *entier*. Calculons-le à l'aide de la série qui définit j. Nous obtenons d'abord, grâce à la relation d'Euler,

$$q = e^{\pi i(-1+i\sqrt{163})} = -e^{-\pi\sqrt{163}}$$

et ensuite

$$j(\omega) = \text{entier} = -e^{\pi\sqrt{163}} + 744 - \frac{196884}{e^{\pi\sqrt{163}}} + \frac{21493760}{e^{2\pi\sqrt{163}}} + \ldots,$$

d'où

$$e^{\pi\sqrt{163}} = \text{entier} - \frac{196884}{e^{\pi\sqrt{163}}} + \frac{21493760}{e^{2\pi\sqrt{163}}} - \ldots .$$

Le nombre $e^{\pi\sqrt{163}}$ étant énorme, une estimation grossière des coefficients de la série qui définit j montre que la somme

$$\frac{196884}{e^{\pi\sqrt{163}}} - \frac{21493760}{e^{2\pi\sqrt{163}}} + \ldots,$$

qui représente la différence entre $e^{\pi\sqrt{163}}$ et un certain entier, est très petite. Nous avons ainsi trouvé une réponse à la question qui nous intriguait. En cours de route, nous avons aussi construit la forme réduite $x^2 + xy + 41y^2$ de discriminant -163 qui, pour $y = 1$, devient le polynôme $P(x) = x^2 + x + 41$. On pourrait en calculer quelques valeurs: $P(0) = 41$, $P(1) = 43$, $P(2) = 47$, $P(3) = 53$, $P(4) = 61$. Tiens! Les premières valeurs sont des nombres premiers. Et puis? $P(5) = 71$, $P(6) = 83$, $P(7) = 97$, $P(8) = 113$, $P(9) = 131$, $P(10) = 151$. Encore des premiers! Ça devient inquiétant; $P(11) = 173$, $P(12) = 197$, et puis 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601, tous premiers jusqu'à $P(40) = 1681$. Bizarre. Est-ce un hasard? Ah non! Nous n'allons pas recommencer avec ce genre de questions!

Prof. Manuel Ojanguren
Institut de mathématiques
CH-1015 Lausanne-Dorigny

Aus der Menge von Literatur über die in diesem Beitrag angesprochenen zahlentheoretischen Begriffe und Sätze greifen wir die folgenden Bücher und Artikel heraus, die allesamt auch ohne grössere Vorbereitung mit Gewinn gelesen werden können:

- J-P. Serre: *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1970; (engl. Übersetzung: *A course in arithmetic*. Graduate Texts in Mathematics 7, Springer Verlag 1973).
- S. Borewicz, I. Šafarevič: *Zahlentheorie*. Birkhäuser 1966.
- H.M. Stark: Class-numbers of complex quadratic fields. In: *Modular functions of one variable I*. Springer Lecture Notes 320 (1973) 154–174.
- I. Stewart: Mathematische Unterhaltungen. Spektrum der Wisenschaft, Dezember 1990, 12–16.
- A. Weil: *Number theory, An approach through history*. Birkhäuser 1983.
- A. Weil: Two lectures on number theory, past and present. L'Enseignement Mathématique 20 (1974) 87–110.
- D. Zagier: A one-sentence proof that every prime $p \equiv 1 (\text{mod } 4)$ is a sum of two squares. Amer. Math. Monthly 97 (1990), 144.