INTRODUCTION A L'ANALYSE DIOPHANTIENNE

Autor(en): **Chatelet, François**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **6 (1960)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **10.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-36332

INTRODUCTION A L'ANALYSE DIOPHANTIENNE [1])

par François CHATELET

(Reçu le 20 juillet 1960)

Dans les exposés précédents, MM. CHABAUTY et PISOT ont déjà étudié plusieurs problèmes diophantiens ou indéterminés. M. PISOT a notamment rappelé qu'une des origines de la théorie des nombres algébriques se trouve dans la résolution en entiers (rationnels) x, y de l'équation diophantienne:

$$x^2 - dy^2 = m$$

où d et m sont des entiers (rationnels) donnés. Les méthodes qu'ils ont exposées ont été introduites au cours du XVIII^e et du XIX^e siècle.

Je me propose d'exposer des méthodes beaucoup plus anciennes puisqu'elles sont dues à DIOPHANTE et à FERMAT. Mais ces méthodes ont été développées récemment par POINCARÉ et plusieurs auteurs contemporains; elles ont permis d'étendre sensiblement des résultats obtenus par d'autres procédés et d'aborder des problèmes nouveaux. Il m'a semblé intéressant de détailler l'évolution des idées qui a conduit aux travaux les plus récents.

D'une manière générale, on appelle problème diophantien, tout problème qui peut être ramené à la recherche des systèmes d'entiers x, y, z, .., qui vérifient une ou plusieurs relations à coefficients entiers (rationnels). On exclut toutefois les systèmes de relations qui n'ont qu'un nombre fini de solutions en nombres réels ou complexes, c'est-à-dire les problèmes déterminés. C'est pourquoi l'ensemble des problèmes diophantiens, ou analyse diophantienne, est aussi appelée analyse indéterminée.

---

1) Conférence prononcée à Grenoble dans le cadre des « Journées Mathématiques de Grenoble », 21-22 mai 1960.

On peut se demander pourquoi DIOPHANTE et ses successeurs ont attaché une telle importance aux solutions en nombres entiers. Certains y ont vu une influence de l'école phytagoricienne qui attribuait aux nombres entiers une valeur magique. Mais il est possible que les raisons en soient beaucoup plus simples. Les mathématiciens grecs et romains, et même les mathématiciens du moyen âge ne possédaient pas de notations suffisamment simples pour faire des calculs sur les nombres irrationnels, ou même sur les nombres rationnels fractionnaires. Ce n'est guère qu'au cours de la renaissance que s'est dégagée l'idée de remplacer les calculs sur les nombres irrationnels par des calculs sur les valeurs rationnelles approchées, et les calculs sur les nombres fractionnaires par des calculs sur les valeurs décimales approchées. Les contemporains de DIOPHANTE avaient donc intérêt à connaître les solutions en entiers qu'ils savaient mieux utiliser. D'ailleurs on a retrouvé des traces de problèmes diophantiens dans les mathématiques égyptiennes et mésopotamiennes antérieures à PYTHAGORE, On a même retrouvé en Mésopotamie, l'étude des solutions en fractions de dénominateur 60; l'intérêt que ces solutions pouvaient présenter pour les mathématiciens de cette époque semble bien provenir du fait que le système de numération mésopotamien permet des calculs relativement simples sur les fractions de dénominateur 60.

On peut aussi se demander pourquoi l'intérêt des problèmes diophantiens s'est maintenu, malgré l'abandon des théories pythagoriciennes et le perfectionnement de l'arithmétique élémentaire. C'est certainement en raison de l'originalité et de l'élégance des méthodes nécessaires à la résolution de ces problèmes. Ces méthodes ont d'ailleurs grandement influencé les autres parties des mathématiques. La théorie des nombres algébriques, les premiers problèmes de la théorie des groupes ont été suggérés par des problèmes diophantiens.

DIOPHANTE a vécu vers le III^e^ siècle de notre ère à Alexandrie. S'il n'est pas le premier à avoir étudié des problèmes indéterminés, il en a résolu un grand nombre, sans d'ailleurs les distinguer nettement des problèmes déterminés, dans son «Arithmétique».

Il a donné notamment une solution du problème des triangles pythagoriciens. Il s'agit de trouver les triangles rectangles dont

les longueurs des côtés sont des entiers, donc encore de trouver les entiers (rationnels) a, b, c qui vérifient la relation:

$$a^2 + b^2 = c^2.$$

DIOPHANTE se limitait aux solutions en entiers positifs. D'ailleurs les solutions en entiers positifs ou négatifs se déduisent sans peine des solutions en entiers positifs; nous nous limiterons, comme DIOPHANTE, à la recherche de ces dernières.

Remarquons d'abord que, si a, b, c ont un même facteur d, les quotients de a, b, c par d sont aussi solutions du problème. Nous chercherons donc seulement les solutions « primitives » telles que a, b, c, soient premiers dans leur ensemble. Mais, si a et b ont un facteur commun premier p, il doit diviser c^2, donc aussi c; ainsi a et b sont premiers entre eux. De même a et c, ainsi que b et c sont premiers entre eux.

En particulier, un seul des entiers a, b, c est pair. Mais le carré d'un nombre impair est un multiple de 4 plus une unité; en effet:

$$(1 + 2n)^2 = 1 + 4n + 4n^2.$$

Ainsi, si a et b étaient tous deux impairs, la somme de leurs carrés serait un multiple de 4 plus 2 unités et ne pourrait être un carré; car le carré d'un nombre impair est impair et le carré d'un nombre pair est un multiple de 4. Donc c est impair et un et un seul des entiers a et b est pair. Désignons par b le côté pair et écrivons la relation de Pythagore sous la forme:

$$b^2 = c^2 - a^2 = (c + a)\ (c - a).$$

Les facteurs communs à $c + a$ et à $c - a$ divisent leur somme et leur différence, soit:

$$2c, \qquad 2a.$$

Puisque a et c sont premiers entre eux, le p.g.c.d. de $c + a$ et de $c - a$ ne peut être que 1 ou 2. Mais, puisque a et c sont impairs, leur somme et leur différence sont paires; donc le p.g.c.d. de $c + a$ et de $c - a$ est 2. Enfin le produit de ces deux derniers nombres est un carré (b^2) et l'un d'eux au moins ($c + a$) est positif. Pour que leur p.g.c.d. soit égal à 2, il est

nécessaire que chacun d'eux soit le produit de 2 et du carré d'un entier; soit:

$$c + a = 2\alpha^2, \quad c - a = 2\beta^2$$

avec α et β premiers entre eux. D'où:

$$a = a^2 - \beta^2$$
$$b = 2\alpha\beta$$
$$c = \alpha^2 + \beta^2.$$

Réciproquement, un système d'entiers a, b, c de la forme précédente avec $\alpha \geqslant \beta$ est une solution primitive de la relation de Pythagore.

Les solutions imprimitives sont exprimées par les formules:

$$a = (a^2 - \beta^2)\,\gamma$$
$$b = 2\alpha\beta\gamma$$
$$c = (\alpha^2 + \beta^2)\,\gamma$$

où γ est un entier arbitraire positif ou négatif.

DIOPHANTE a étudié plusieurs problèmes concernant les triangles pythagoriciens, dont voici un exemple:

Trouver un triangle rectangle (à côtés entiers) dont l'aire, diminuée de six unités, forme un carré. C'est-à-dire résoudre en entiers rationnels positifs le système:

$$a^2 + b^2 = c^2$$
$$ab - 12 = 2\alpha^2.$$

Il a également étudié d'autres problèmes indéterminés, dont voici un exemple:

Trouver deux entiers tels que leur produit, augmenté soit de leur somme, soit de chacun d'eux, forme un carré. C'est-à-dire trouver les solutions en nombres entiers du système:

$$ab + a + b = \alpha^2,$$
$$ab + a = \beta^2,$$
$$ab + b = \gamma^2.$$

Il faut toutefois remarquer que, pour beaucoup de ces problèmes, DIOPHANTE ne savait pas obtenir toutes les solutions en entiers.

L'œuvre de DIOPHANTE fut étudiée par les mathématiciens arabes pendant le Moyen-Age, mais fut ignorée par les mathématiciens d'Europe. C'est seulement au XIII^e^ siècle qu'un Italien, LÉONARD DE PISE, dit FIBONACCI, retrouve une partie des résultats de DIOPHANTE, en étudiant les mathématiques arabes. Plusieurs Italiens, Français et Anglais poursuivent les recherches et les études de LÉONARD, notamment BACHET DE MÉZIRAC, qui édite les manuscrits de DIOPHANTE. C'est l'étude de cette édition qui engage Pierre DE FERMAT, au début du XVII^e^ siècle, dans des recherches arithmétiques. Ce dernier résout plusieurs problèmes nouveaux et surtout introduit des méthodes très originales. Mais, occupé par ses fonctions juridiques, il ne publie aucun travail d'ensemble et ses résultats ne sont connus que par sa correspondance avec divers mathématiciens et par l'édition d'une partie de ses notes, faites après sa mort par son fils SAMUEL. Plusieurs propriétés sont énoncées sans explication et c'est seulement EULER, LAGRANGE ou LEGENDRE qui les démontreront au cours du XVIII^e^ en précisant et en développant les méthodes de FERMAT.

Comme exemple, établissons la propriété suivante: la somme de deux bi-carrés ne peut être un carré; c'est-à-dire, il n'existe pas d'entiers a, b, c tous différents de zéro, vérifiant la relation:

$$a^4 + b^4 = c^2 .$$

S'il existe de tels entiers, a^2, b^2, c sont les côtés entiers d'un triangle rectangle. Comme précédemment supprimons les facteurs communs de ces trois entiers; après cette simplification, a, b, c sont premiers deux à deux. Si a^2 est impair, a^2 et b^2 sont de la forme:

$$a^2 = \alpha^2 - \beta^2 , \qquad b^2 = 2\,\alpha\beta ,$$

avec α, β premiers entre eux et $\alpha > \beta$. Mais la première de ces relations s'écrit:

$$a^2 + \beta^2 = \alpha^2$$

et a, α et β sont premiers 2 à 2; a est impair, donc β est pair et α et β sont de la forme:

$$\alpha = \lambda^2 + \mu^2 \qquad \beta = 2\,\lambda\mu$$

avec λ, μ premiers entre eux. En comparant les résultats précédents, nous obtenons:

$$b^2 = 2\alpha\beta = 4\lambda\mu(\lambda^2 + \mu^2).$$

Mais λ, μ sont premiers entre eux, donc aussi sont premiers avec $\lambda^2 + \mu^2$. Les produits de ces trois nombres premiers 2 à 2 et positifs ne peut être un carré que si chacun d'eux est carré. Donc

$$\lambda = \rho^2 \qquad \mu = \sigma^2 \qquad \lambda^2 + \mu^2 = \tau^2$$

Et par suite:

$$\rho^4 + \sigma^4 = \tau^2.$$

Ainsi, d'une solution en entiers a, b, c de la relation proposée, nous avons déduit une nouvelle solution en entiers ρ, σ, τ. Nous pouvons ensuite, par le même procédé, déduire de cette seconde solution une troisième solution. Et ainsi de suite, indéfiniment. C'est le procédé de « descente infinie » de FERMAT.

Mais la relation:

$$b^2 = 4\lambda\mu(\lambda^2 + \mu^2) = 4\rho^2\sigma^2(\rho^4 + \sigma^4)$$

montre que:

$$b > \text{Max}(\rho, \sigma).$$

Et la relation:

$$\begin{aligned} a^2 &= \alpha^2 - \beta^2 = (\lambda^2 + \mu^2)^2 - 4\lambda^2\mu^2 \\ &= (\lambda^2 - \mu^2)^2 = (\rho^4 - \sigma^4)^2 \\ &= (\rho^2 + \sigma^2)^2(\rho^2 - \sigma^2)^2 \end{aligned}$$

montre que:

$$a > \text{Max}(\rho, \sigma).$$

Ainsi, si la descente infinie de FERMAT est possible, le maximum de la valeur absolue des entiers a, b diminue à chaque étape de la descente. Il y a donc incompatibilité entre les propriétés des entiers finis et la possibilité d'une descente infinie. La descente infinie est impossible, ce qui entraîne qu'il n'existe pas de solution en entiers a, b, c tous différents de zéro.

Le résultat que nous venons d'établir montre *a fortiori* que: la somme de deux bicarrés ne peut être un bicarré; c'est-à-dire

qu'il n'existe pas d'entiers a, b, c non tous nuls vérifiant la relation:

$$a^4 + b^4 = c^4 .$$

Ce nouveau résultat est un cas particulier d'une propriété générale, connue sous le nom de « théorème de FERMAT » ou « hypothèse de FERMAT ». Elle affirme qu'il n'existe pas d'entiers a, b, c non nuls vérifiant la relation:

$$a^n + b^n = c^n ,$$

où n est un entier positif arbitrairement donné. Cette propriété est énoncée dans les notes de FERMAT publiées par son fils. Elle a donné lieu à de nombreux travaux, mais n'a pu encore être démontrée que pour certaines valeurs de n, dont les entiers inférieurs à 100. Sauf pour les très petites valeurs de n, les démonstrations utilisent des propriétés difficiles des entiers algébriques. On s'est souvent étonné que FERMAT ait pu deviner et peut-être démontrer une propriété aussi difficile. Il faut toutefois remarquer que nous ne possédons pas l'original de la note de FERMAT, mais seulement des exemplaires de l'édition faite par son fils. L'énoncé est d'ailleurs donné explicitement seulement pour les valeurs $n = 3$ et 4 et suggéré pour les valeurs plus élevées de n. Il est donc fort possible que Samuel FERMAT ait mal recopié le texte de son père et que celui-ci ne prétendait démontrer cette propriété que pour certaines valeurs de l'exposant. Quoi qu'il en soit, il faut être reconnaissant à Pierre ou Samuel FERMAT d'avoir provoqué des travaux importants qui ont contribué au développement de l'arithmétique.

Il est bien connu que C.-F. GAUSS a poursuivi pendant toute sa vie des travaux d'arithmétique, en alternance avec des recherches dans d'autres domaines des mathématiques. Mais il a abandonné presque complètement les méthodes de DIOPHANTE et de FERMAT pour introduire les problèmes et les procédés qui allaient conduire au développement de la théorie des entiers algébriques pendant le XIX^e ou le XX^e siècle. C'est seulement vers 1900 qu'Henri POINCARÉ retourne aux méthodes de FERMAT et en provoque, pendant les années suivantes, un nouveau développement. Il faut toutefois remarquer, comme nous allons le

voir, que ces nouvelles applications utilisent les propriétés des entiers algébriques, préalablement établies.

On peut résumer l'idée essentielle de POINCARÉ de la façon suivante: il remarque que la « descente infinie » de FERMAT utilise des transformations simplement rationnelles à coefficients rationnels sur une courbe ou une variété algébrique associée au problème diophantien considéré. Une pareille transformation permet de déduire d'une solution en nombres rationnels du problème une nouvelle solution; dans certaines conditions, elle permet même de déduire d'une solution en entiers une autre solution en entiers. POINCARÉ recherche aussi méthodiquement que possible ces transformations et leurs conséquences arithmétiques. Pour cela, lui-même et ses successeurs complètent la théorie géométrique des correspondances entre courbes ou variétés algébriques par l'étude de celles de ces transformations dont les coefficients sont rationnels, ou plus généralement appartiennent à un corps de base déterminé.

La première application faite par POINCARÉ lui-même de cette méthode concerne les points rationnels des courbes de genre nul, c'est-à-dire des solutions en entiers de l'équation homogène d'une telle courbe. Un raisonnement relativement simple lui permet de montrer qu'une telle courbe peut être remplacée par une transformation birationnelle à coefficients rationnels, soit en une conique, soit en une droite (à coefficients rationnels). La transformation utilisée permet de déduire les points rationnels de la courbe considérée de ceux de la courbe réduite. Or la recherche des points rationnels sur une conique (ou sur une droite) résulte des travaux de LAGRANGE, LEGENDRE et GAUSS. La méthode de POINCARÉ permet donc d'augmenter considérablement le champ d'application de ces derniers résultats.

POINCARÉ applique également cette méthode aux courbes de genre un, pour lesquelles il n'obtient que des résultats incomplets, mais qui seront améliorés par ses successeurs: L. J. MORDELL, A. WEIL, T. NAGELL, ... Nous allons donner une idée de ces résultats à propos d'un exemple particulier qui est d'ailleurs intimement lié au problème de FERMAT précédemment traité.

Considérons la cubique C d'équation non homogène:

$$z^2 = x\,(x^2 + 1)$$

ou d'équation homogène:

$$z^2 t = x(x^2 + t^2) .$$

Divisions x, z, t par leur p.g.c.d.; nous obtenons ainsi une nouvelle solution avec x, z, t premiers dans leur ensemble. Désignons par d le p.g.c.d. de x et t; ainsi:

$$x = x_1 d , \qquad t = t_1 d ,$$

avec x_1 et t_1 premiers entre eux. De plus z et t sont premiers entre eux, puisque x, z et t sont premiers dans leur ensemble. L'équation homogène de C s'écrit encore:

$$t_1 z^2 = x_1 (x_1^2 + t_1^2) d^2 .$$

Puisque t_1 est premier avec x_1, donc aussi avec $x_1^2 + t_1^2$, il doit diviser d^2. Puisque x, z, t sont premiers dans leur ensemble. z est premier avec le p.g.c.d. de x et t, soit d; donc d^2 divise t_1. C'est-à-dire

$$d^2 = t_1$$

et par suite:

$$z^2 = x_1 (x_1^2 + d^4) .$$

Avec un léger changement de notations, tout point rationnel de la cubique C correspond ainsi à une solution de la relation:

$$z^2 = x(x^2 + y^4)$$

en entiers x, y, z, avec y premier à x et à z. Pour abréger, appelons ces entiers x, y, z « coordonnées arithmétiques » du point considéré.

POINCARÉ utilise alors la représentation classique de la cubique C par des fonctions elliptiques et le théorème d'addition de ces fonctions; il remarque en outre que, pour un choix convenable de la représentation, les formules d'addition, qui sont rationnelles, ont également leurs coefficients rationnels. Ce qui peut être exprimé géométriquement de la façon suivante: les coordonnées du troisième point d'intersection M_3 de la cubique C et de la droite qui joint deux points M_1 et M_2 de C peuvent être calculées par des formules rationnelles à coefficients rationnels

à partir des coordonnées de M_1 et de M_2. Ces formules définissent donc une loi de composition L à l'intérieur de l'ensemble des points rationnels sur C. Cette loi de composition L n'organise pas l'ensemble des points rationnels sur C en groupe, car elle n'est pas associative. On peut montrer que la loi de composition L_1, Obtenue en effectuant L sur deux points M_1, M_2 variables puis sur le résultat obtenu et un point fixe M_0 est associative pour toute cubique de genre un. Si de plus M_0 est un point d'inflexion de cette cubique, en particulier si M_0 est le point à l'infini pour une cubique de la forme:

$$y^2 = x^3 + Ax + B\,,$$

M_0 est un élément neutre pour la loi L_1 et l'ensemble des points rationnels forme bien un groupe pour cette loi.

Appliquons en particulier la loi de composition L à deux points M_1 et M_2 confondus (en remplaçant la sécante M_1M_2 par la tangente en M_1 à C). Nous obtenons ainsi une transformation simplement rationnelle à coefficients rationnels R entre M_1 et M_3. Si M_1 est rationnel, son image M_3 est aussi rationnelle; mais inversement un point rationnel M_3 peut n'être l'image d'aucun point rationnel M_1 dans R. Pour abréger, nous dirons qu'un point rationnel M_3 est « pair » s'il est l'image dans R d'au moins un point rationnel M_1. Un calcul simple montre qu'une condition nécessaire et suffisante pour qu'un point rationnel soit pair est qu'il existe des entiers rationnels λ, μ, ν tels que les coordonnées arithmétiques x, y, z de M vérifient les relations:

$$x = \lambda^2\,, \qquad x + iy^2 = (\mu + i\nu)^2$$

ou encore:

$$x = \lambda^2 = \mu^2 - \nu^2\,, \qquad y^2 = 2\mu\nu\,.$$

D'autre part, on démontre que si deux points rationnels M_1 et M_2 de C sont pairs, leur composé M_3 dans L est pair. Plus généralement, la condition pour que le composé dans L de deux points rationnels sur C soit pair, définit une relation d'équivalence (ou congruence) dans l'ensemble des points rationnels sur C. Une classe de points pour cette congruence est obtenue en appliquant à l'ensemble des points pairs de C la transformation birationnelle à coefficients rationnels définie comme suit: on compose un point variable M de C avec un point fixe M_1 de C.

En utilisant la loi de composition L_1, on peut encore montrer que l'ensemble des points pairs est le sous-groupe 2G du groupe G des points rationnels pour L_1 formé par les composés d'un point avec lui-même. Une classe quelconque est un élément du groupe quotient de G par 2G.

Un calcul simple montre encore qu'une classe quelconque est formée par les points de C dont les coordonnées arithmériques x, y, z vérifient les relations:

$$x = a\lambda^2, \qquad x + iy^2 = (b + ic)(\mu + i\nu)^2,$$

ou

$$x = a\lambda^2 = b(\mu^2 - \nu^2) - 2c\mu\nu,$$
$$y^2 = 2b\mu\nu + c(\mu^2 - \nu^2)$$

où a, b, c sont des entiers fixes, où λ, μ, ν sont des entiers arbitraires et où i est l'imaginaire principale. Le triplet d'entiers a, b, c qui détermine une classe ne peut pas être choisi de façon arbitraire; il est nécessaire que le produit:

$$a(b^2 + c^2)$$

soit un carré parfait. D'autre part, si on multiplie a par un carré parfait et $b + ic$ par le carré d'un entier du corps de GAUSS engendré par i, on ne change pas la classe déterminée par a, b, c. Cette dernière propriété permet de supprimer tous les facteurs carrés de a, et aussi ceux de $b + ic$, puisque les entiers de GAUSS sont décomposables en produits de facteurs premiers.

Utilisons l'arithmétique des entiers de GAUSS. Pour que $a(b^2 + c^2)$ soit un carré parfait, a, $b + ic$ et $b - ic$ sans facteurs carrés, il faut que tout facteur de a divise $b^2 + c^2$, donc divise soit $b + ic$ soit $b - ic$. Mais les facteurs de a divisent x, ceux de $b + ic$ divisent $x + iy^2$ et x, y sont premiers entre eux. Donc les seuls facteurs possibles pour a sont les unités du corps de GAUSS soit $+1$, -1, $+i$ et $-i$. Mais a est entier rationnel et positif, puisque $a(b^2 + c^2)$ est le carré d'un entier rationnel. Donc:

$$a = 1.$$

Il est alors nécessaire que $b^2 + c^2$ soit un carré parfait et $b + ic$, $b - ic$ sans facteurs carrés. Tout facteur de $b + ic$ doit donc

diviser $b - ic$ et réciproquement; c'est-à-dire que ces deux entiers sont des unités de GAUSS.

L'unité $b + ic = +1$ détermine la classe des points pairs déjà étudiée. L'unité $b + ic = -1$ détermine la même classe puisque -1 est le carré de l'entier de GAUSS $+ i$. L'unité $b + ic = i$ détermine la classe:

$$x = \lambda^2, \qquad x + iy^2 = i(\mu + i\nu)^2$$

ou:

$$x = \lambda^2 = -2\mu\nu, \qquad y^2 = \mu^2 - \nu^2.$$

L'unité $b + ic = -i$ détermine la même classe puisque $-i$ est le produit de i par le carré d'un entier de GAUSS.

Finalement, il n'existe que deux classes. De plus, la seconde classe n'est pas vide, puisqu'elle contient notamment le point de coordonnées arithmétiques $x = z = 0$, y arbitraire.

Or, si un point rationnel M est pair, on peut en déduire un autre point rationnel, à savoir l'un des points N dont M est l'image dans R. Si un point rationnel M est dans la seconde classe, on peut en déduire un point pair M_1 en le composant avec le point fixe A de coordonnées arithmétiques $x = z = 0$. Du point M_1, on peut déduire un nouveau point rationnel N dont M_1 est l'image dans R. Ces constructions donnent de nouveau un procédé de descente infinie. Cette descente infinie vérifie des inégalités analogues à celles de l'exemple de FERMAT. Elles permettent de démontrer que les seuls points rationnels sur C sont le point de coordonnées arithmétiques $x = z = 0$ et le point à l'infini de coordonnées arithmétiques $y = 0$, $x = z = 1$.

En fait, cet exemple se réduit presque entièrement à celui de FERMAT. Nous avons en effet montré que si x, y, z sont les coordonnées arithmétiques d'un point rationnel sur C:

$$z^2 = x(x^2 + y^4),$$

il est nécessaire que x soit le carré d'un entier rationnel λ. La relation précédente montre donc que

$$\lambda^4 + y^4 = \rho^2$$

où ρ est un entier rationnel. C'est la relation de FERMAT considérée. De plus, on constate facilement que la composition de A

avec un point M de C conduit seulement à intervertir les valeurs de λ et y. Ce qui explique pourquoi le procédé de descente de FERMAT ne semble utiliser qu'une seule opération: il suppose une permutation possible des entiers a, b ou y, λ pour rendre a ou y pair.

Mais, si la méthode de POINCARÉ se réduit en fait à celle de FERMAT sur cet exemple particulier, elle s'applique encore à d'autres cubiques en faisant toutefois intervenir l'arithmétique des idéaux dans des corps algébriques plus compliqués que celui de GAUSS.

Pour conclure, donnons quelques indications sur les problèmes encore ouverts et pour lesquels on peut raisonnablement espérer des progrès. La recherche des points rationnels sur les courbes de genre supérieur à un a été abordée par A. WEIL. En fait A. WEIL étudie et obtient les points rationnels sur la jacobienne d'une courbe de genre g; ce qui revient à étudier les systèmes de g points (rationnels ou algébriques) sur la courbe considérée, tels que leur ensemble soit rationnel, c'est-à-dire que les fonctions symétriques à coefficients rationnels des coordonnées de ces g points prennent des valeurs rationnelles. Ces systèmes comprennent notamment les systèmes formés par g points tous rationnels. Mais on ne sait pas encore distinguer ces systèmes particuliers parmi les systèmes plus généraux obtenus par A. WEIL. Il semble d'ailleurs qu'on rencontre dans ce problème une difficulté essentielle.

L'étude des points rationnels sur les surfaces et variété algébriques est à peine ébauchée. Les variétés homaloïdales, c'est-à-dire celles pour lesquelles on peut trouver des représentation birationnelles à coefficients algébriques, n'ont donné lieu qu'à quelques résultats isolés. Même l'étude des surfaces cubiques, abordée par B. SEGRE, est encore très incomplète. Il est probable qu'une utilisation convenable de la topologie algébrique, généralisant l'utilisation de la théorie des groupes, permette d'appliquer aux variétés homaloïdales les méthodes de POINCARÉ et d'obtenir dans un avenir proche des résultats importants.

Nous avons rencontré au cours de cette conférence la recherche des points entiers sur quelques variétés algébriques. Mais en fait cette recherche se ramenait chaque fois à la recherche des points

rationnels sur une autre variété. Par contre, les conférences de MM. CHABAUTY et PISOT ont donné des exemples de recherche de points entiers qui ne peuvent se ramener à une recherche de points rationnels pour un autre système diophantien. Il semble que les méthodes de DIOPHANTE, FERMAT et POINCARÉ ne suffisent plus et qu'il soit indispensable d'utiliser les méthodes d'HERMITE ou de MINKOWSKI pour traiter complètement ces problèmes.

Néanmoins les méthodes de POINCARÉ peuvent encore être utiles dans une première partie de l'étude. Ainsi, l'étude par POINCARÉ des points rationnels sur les courbes de genre zéro a servi de point de départ à l'étude des points entiers sur ces courbes, faite quelques années plus tard par MAILLET. L'étude par A. WEIL des points rationnels sur les jacobiennes des courbes de genre supérieur à un a permis à C.-L. SIEGEL de déterminer les courbes sur lesquelles existent un nombre infini de points entiers. L.-J. MORDELL a obtenu quelques surfaces cubiques contenant un nombre infini de points entiers. Il est possible que ses résultats puissent être généralisés par un emploi convenable de la topologie algébrique.

Enfin, il faut remarquer que certaines de ces recherches peuvent être abordées avec des moyens relativement élémentaires. Depuis FERMAT, de nombreux amateurs ont d'ailleurs poursuivi l'étude de l'analyse diophantienne. Et nous devons à certains d'entre eux des idées ou des résultats plus modestes mais non négligeables. Les fautes de raisonnement commises par d'autres, surtout à propos de l'hypothèse de FERMAT, ne doivent pas décourager les bonnes volontés. Il reste un vaste domaine où chacun peut trouver à satisfaire, quel que soit le degré de son érudition, son goût pour la recherché scientifique et pour l'esthétique mathématique.

BIBLIOGRAPHIE

R. D. CARMICHAEL: Analyse indéterminée. Presses universitaires, 1929. Livre élémentaire et ancien. L'auteur ne connaissait pas les méthodes de POINCARÉ, mais fait plusieurs suggestions qui s'en rapprochent. Exposés très clairs de plusieurs exemples élémentaires.

L. J. MORDELL: Le dernier théorème de FERMAT. Presses universitaires. Livre un peu ancien qui ne contient pas les importants résultats de WIEFERICH et MIRIMANOFF.

T. NAGELL: L'analyse indéterminée de degré supérieur. Mémorial des sciences mathématiques. Gauthier-Villars (1929). Exposé succinct de tous les travaux importants antérieurs à 1929. Ne contient pas le travail d'A. WEIL.

Th. SKOLEM: Diophantische Gleichungen, Ergebnisse der Mathematik. Springer, Berlin, 1943. Exposé d'ensemble le plus récent.

L. E. DICKSON: History of the theorie of numbers. Washington,1920. Ce n'est pas une histoire, mais une analyse de tous les travaux d'analyse indéterminée, importants ou non, antérieurs à 1920. Ne contient aucune vue d'ensemble, mais peut être utile pour retrouver des travaux peu connus.

B. SEGRE: Arithmetical questions on algebraic varieties. Londres, 1951. Contient des résultats récents et des suggestions fort intéressantes.

Professeur F. CHATELET,
Institut de Mathématiques,
Université de Besançon.