Université P. et M. Curie (Paris VI) date de mise à jour: 13/01/2009
Deuxième semestre 2008/2009

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : (12 ECTS)

Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Objectifs et descriptions

Ce cours vise à donner les bases de l'arithmétique, de la théorie algébrique des nombres et de la théorie analytique des nombres. Il est aussi utile en cryptographie et en théorie des codes.

Prérequis

Des connaissances en algèbre du niveau licence.

Contenu :

Arithmétique : factorisation, équations diophantiennes, fractions continues, approximation diophantienne, irrationalité et transcendance.

Extensions algébriques, corps de rupture et corps de décomposition, clôture algébrique, extentions normales et séparables, polynômes cyclotomiques.

Corps finis (existence, unicité, structure, construction, décomposition des polynômes cyclotomiques, loi de réciprocité quadratique, automorphisme de Frobenius et théorie de Galois). Polynômes à coefficients dans un corps fini. Applications : cryptographie, codes correcteurs d'erreurs.

Corps de nombres, norme, trace, discriminant ; entiers algébriques, unités et idéaux d'un corps de nombres, décomposition des idéaux premiers dans une extension.

Références

[1] H. Cohen – *Démonstration de la conjecture de Catalan*, `http ://www.math.polytechnique.fr/xups/xups05-01.pdf`

[2] H. Cohen – *A course in computational algebraic number theory*, Graduate texts in Math. **138**, Springer Verlag (1993).

[3] J.H. Conway & R.K. Guy – *The book of numbers*, Copernicus Books, Springer Science + Business Media, 2006.

[4] M. Demazure – *Cours d'algèbre. Primalité. Divisibilité. Codes*, Nouvelle Bibliothèque Mathématique Cassini, Paris, 1997.

[5] D.S. Dummit & R.M. Foote – *Abstract Algebra*, Prentice Hall 1991, 1999.

[6] D. Duverney – *Théorie des nombres : cours et exercices corrigés*, Paris : Dunod. viii, 244 p., 1998.

[7] G.H. Hardy & E.M. Wright – *An introduction to the theory of numbers*, Oxford University Press, 1938. Fifth Ed. 1979.

[8] M. Hindry – *Arithmétique*, Calvage et Mounet, Tableau Noir, Paris, 2008.

[9] S. Lang – *Algèbre*, Dunod, 2004.

[10] R. Lidl & H. Niederreiter – *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1994.
http ://www.amazon.com/gp/reader/0521460948/ref=sib_dp_ptu#reader-link

[11] W. Narkiewicz – *Classical problems in number theory*, PWN – Polish Scientific Publishers, Warszàwa, 1986.

[12] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[13] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.

[14] J-P. Serre – *Cours d'arithmétique*, Coll. SUP, Presses Universitaires de France, Paris, 1970.

[15] V. Shoup – *A Computational Introduction to Number Theory and Algebra* (Version 2) second print editon, Fall 2008. Version électronique téléchargeable intégralement :
http ://shoup.net/ntb/

De nombreux documents sont disponibles sur la toile. Voir notamment

MIT's open courseware
http ://ocw.mit.edu/OcwWeb/web/home/home/index.htm
Textbooks in Mathematics
http ://www.geocities.com/alex_stef/mylist.html
ainsi que la liste sur la page Online number theory lecture notes
http ://www.numbertheory.org/ntw/lecture_notes.html
du site du réseau de théorie des nombres
http ://www.numbertheory.org/ntw/web.html

Voir aussi
A.A. Pantchichkine, Magistère de Mathématiques (ENS Lyon), Algèbre 2, § 3.1.
http ://www-fourier.ujf-grenoble.fr/%7Epanchish/05ensl.pdf

Nils-Peter Skoruppa, *Théorie de Galois et Théorie Algébrique des Nombres*, Notes d'un cours de Maîtrise, UFR de Mathématiques et Informatique, Université de Bordeaux I, 2000.
http ://wotan.algebra.math.uni-siegen.de/∼countnumber/D/

Sur le site
http ://lib.org.by/
on trouve un grand nombre d'ouvrages à télécharger, ceux de théorie des nombres sont à la page
http ://lib.org.by/_djvu/M_Mathematics/MT_Number%20theory/

Des informations biographiques généralement fiables concernant un grand nombre de mathématiciens sont données sur le site internet
The MacTutor History of Mathematics archive
http ://www-gap.dcs.st-and.ac.uk/∼history/

Premier fascicule: 12/01/2009 – Introduction

Introduction

0.1 Équations Diophantiennes

Historiquement, la principale source du développement de la théorie algébrique des nombres est le problème de la résolution des équations en nombres entiers ou rationnels. Traditionnellement, on appelle *équation Diophantienne* une équation polynomiale $f(x_1, \ldots, x_n) = 0$, où f est un polynôme à coefficients rationnels, que l'on cherche à résoudre en nombres entiers ou rationnels. *Résoudre* une telle équation signifie d'abord décider si elle a ou non des solutions, quand elle en a il faut ensuite dire si leur ensemble est fini ou non, et pour la résoudre complètement il faut enfin déterminer toutes les solutions.

Un exemple simple est l'équation $y(y-1) = x^2$. Elle a 2 solutions en nombres entiers, à savoir $(x, y) = (0, 0)$ et $(0, 1)$, tandis qu'elle a une infinité de solutions en nombres rationnels : pour chaque nombre rationnel t distinct de ± 1 le couple

$$(x, y) = \big(t/(t^2-1)\ ,\ t^2/(t^2-1)\big) \in \mathbf{Q} \times \mathbf{Q}$$

est solution, et on les obtient toutes ainsi à part $(0, 1)$ (qu'on retrouverait en passant en coordonnées projectives, ce qui revient à prendre $t = \infty$).

Un des premiers mathématiciens à avoir considéré ce genre de question est Diophante d'Alexandrie (325–409). La traduction, par Bachet de Méziriac (1581–1638), de la partie des œuvres de Diophante qui était parvenue dans le monde occidental grâce aux mathématiciens arabes, a été la source d'inspiration de Fermat (1601–1665). Beaucoup d'énoncés formulés par Fermat, et bien d'autres, ont été démontrés par Euler (1707–1783). La théorie des équations quadratiques fait l'objet de nombreux travaux à partir du XVIIIè siècle, notamment par Lagrange (1736–1813) et Gauss (1777-1855). Le "dernier théorème de Fermat", selon lequel l'équation $x^n + y^n = z^n$ n'a pas de solution en nombres rationnels non nuls x, y, z dès que l'entier n est supérieur ou égal à 3, reste un défi jusqu'en 1994 où A. Wiles en donnera enfin une démonstration complète. Cette question a motivé les recherches de Kummer (1810–1893), Dedekind (1831–1916), Dirichlet (1805–1859) et bien d'autres ; c'est ce problème qui est à l'origine des principaux concepts dont il sera question dans ce cours.

Jusque vers la fin du XIXème siècle les méthodes employées seront spécifiques aux équations considérées. Il faudra attendre les contributions de Hurwitz (1859–1919) et Poincaré (1854–1912) pour disposer d'énoncés portant sur des classes générales d'équations. Le début du XXème siècle verra apparaître d'abord les méthodes d'approximation diophantienne avec les travaux de Thue (1863–1922), puis, grâce à ces outils puissants, les résultats de Siegel (1896–1981) sur les points entiers sur des courbes algébriques (il s'agit de décider si une équation $f(x, y) = 0$ a une infinité de solution entières, Siegel donne en 1929 des conditions nécessaires et suffisantes sur le polynôme $f \in \mathbf{Z}[X]$). Un énoncé semblable pour les points rationnels a été proposé par Mordell (1888–1972) et démontré par G. Faltings en 1983.

Étant donné un polynôme non nul explicite $f \in \mathbf{Z}[X, Y]$, on sait maintenant répondre aux questions suivantes :

– L'équation Diophantienne $f(x, y) = 0$ a-t-elle une infinité de solutions rationnelles $(x, y) \in \mathbf{Q} \times \mathbf{Q}$?

– L'équation Diophantienne $f(x,y)=0$ a-t-elle une infinité de solutions entières $(x,y)\in\mathbf{Z}\times\mathbf{Z}$?

Dans le cas où la réponse est qu'il n'y a qu'un nombre fini de solutions, on sait aussi en majorer le nombre. Mais dans ce cas il n'existe pas encore d'algorithme permettant de déterminer toutes les solutions.

Pour les équations Diophantiennes faisant intervenir un plus grand nombre de variables, Yu.V. Matiyasevich a résolu par la négative en 1970 à une question posée par Hilbert en 1900 : *il n'y a pas d'algorithme général permettant de déterminer si une équation en nombres entiers $f(x_1,\ldots,x_n)$ a ou non une infinité de solutions dans $\mathbf{Z}^n$.*

Une extension de la notion d'équation Diophantienne est celle *d'équation Diophantienne exponentielle*, dans laquelle certains exposants sont considérés comme des inconnues. Une des plus connues est celle proposée en 1844 par Catalan $x^p-y^q=1$, où les inconnues (x,y,p,q) sont des entiers tous ≥ 2. Catalan (1814-1894) a conjecturé que la seule solution était $(3,2,2,3)$ correspondant à $3^2-2^3=1$. Cette conjecture a été démontrée en 2003 par P. Mihailescu. Une démonstration complète et détaillée est donnée par H. Cohen [1].

Une question plus vaste que celle de Catalan a été posée par S.S. Pillai (1901–1950) en 1945 :

Conjecture 0.1 (S.S. Pillai)**.** *Pour chaque entier $k>0$, l'équation $x^p-y^q=k$ n'a qu'un nombre fini de solutions en entiers (x,y,p,q) tous ≥ 2.*

Il n'y a que le cas $k=1$ qui soit résolu. La conjecture de Pillai signifie que la distance entre deux termes consécutifs de la suite

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125,\ 128,\ 144,\ \ldots$$

des puissance parfaites tend vers l'infini.

Considérons pour commencer la plus simple des équations Diophantiennes en deux variables : on fixe deux entiers a et b et on cherche à résoudre l'équation $ax+by=0$ où les inconnues x, y sont dans $\mathbf{Z}$. Si on note d le pgcd de a et b, et $a'=a/d$, $b'=b/d$, alors la solution générale est $(x,y)=(tb',-ta')$, $t\in\mathbf{Z}$. Cet exemple élémentaire se généralise aisément aux systèmes de m équations en n inconnues : on se donne une matrice de format $m\times n$ à coefficients entiers et on cherche les vecteurs colonnes $X={}^t(x_1,\ldots,x_n)$ à coefficients dans $\mathbf{Z}$ qui satisfont $AX=0$. L'algèbre linéaire permet de résoudre la question.

Si maintenant on se donne, en plus, un vecteur colonne B (matrice $m\times 1$) et que l'on veut résoudre $AX=B$, pour en obtenir la solution générale il suffit d'ajouter à une solution particulière de cette équation la solution générale de l'équation homogène associée $AX=0$.

Revenant au cas particulier d'une équation en deux inconnues ($m=1$, $n=2$), pour résoudre l'équation de Bézout $ax+by=c$ on utilise l'algorithme d'Euclide : cette équation a une solution $(x,y)\in\mathbf{Z}\times\mathbf{Z}$ si et seulement si le pgcd de a et b divise c.

Après les équations *linéaires* (de degré 1), passons aux équations *quadratiques* (de degré 2). La plus célèbre est sans doute celle de Pythagore (VIème siècle avant J.-C) : $x^2+y^2=z^2$. Comme elle est homogène, la résoudre en nombres entiers revient à résoudre en nombres rationnels l'équation $x^2+y^2=1$, c'est-à-dire à déterminer les points rationnels sur un cercle. La méthode géométrique, qui permet plus généralement de trouver les points rationnels sur une conique (c'est-à-dire de résoudre en nombres rationnels une équation $f(x,y)=0$ où f est un polynôme en deux variables de degré 2), consiste à tracer une droite passant par un point rationnel : elle coupe la courbe en question en un autre point et cela fournit une paramétrisation des solutions. Pour le cercle on peut

partir par exemple du point $(x, y) = (-1, 0)$ et considérer la droite $y = t(x + 1)$ de pente $t \in \mathbf{Q}$. Le second point d'intersection est obtenu en résolvant l'équation

$$x^2 + t^2(x + 1)^2 - 1 = 0$$

qui possède bien entendu la solution $x = -1$. On peut donc mettre $x+1$ en facteur dans le membre de gauche : si $x \neq -1$ alors on peut diviser par $x + 1$ et l'équation devient linéaire

$$x - 1 + t^2(x + 1) = 0,$$

ce qui donne

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}.$$

Pour chaque $t \in \mathbf{Q}$ ces formules donnent un point rationnel (x, y) sur le cercle, et inversement tout point rationnel sur le cercle distinct de $(-1, 0)$ est de cette forme. On retrouve le point exceptionnel $(-1, 0)$ en autorisant $t = +\infty$, c'est-à-dire en passant en coordonnées projectives. En écrivant $t = a/b$ on retrouve les formules

$$x = \frac{b^2 - a^2}{b^2 + a^2}, \quad y = \frac{2ab}{b^2 + a^2}$$

qui conduisent à la solution générale en nombres entiers de l'équation de Pythagore $x^2 + y^2 = z^2$. On remarque d'abord que si x, y, z sont des entiers positifs qui satisfont $x^2 + y^2 = z^2$, et si d est leur pgcd, alors le triplet (x', y', z') défini par $x' = x/d$, $y' = y/d$, $z' = z/d$ satisfait encore l'équation de Pythagore, et en plus ces trois entiers x', y', z' sont premiers entre eux dans leur ensemble (ils sont même premiers entre eux deux-à-deux). De plus z' est impair. On en déduit facilement que l'un des deux nombres x', y' est pair, l'autre bien entendu est impair. Voici l'énoncé auquel on aboutit (voir par exemple [12], § 1.2, Th.1 ou [6], Th. 5.9).

Théorème 0.2. *L'application*

$$(a, b) \ \rightarrow \ (x = b^2 - a^2, \ y = 2ab, \ z = b^2 + a^2)$$

établit une bijection entre
• *l'ensemble des couples (a, b) d'entiers positifs premiers entre eux*
et
• *l'ensemble des triplets (x, y, z) formés d'entiers positifs premiers entre eux dans leur ensemble, avec y pair, qui vérifient l'équation de Pythagore $x^2 + y^2 = z^2$.*

Le procédé géométrique de la corde et de la tangente que nous venons de voir est utile aussi pour les équations *cubiques* (de degré 3) : si on dispose de deux points rationnels sur une courbe $f(x, y) = 0$ où f est un polynôme de degré 3, alors la droite joignant ces deux points coupe *généralement* la cubique en un autre point rationnel. On le vérifie de la façon suivante. Si les deux points sur la courbe sont (x_0, y_0) et (x_1, y_1), la droite qui passe par ces deux points a pour équation

$$y - y_0 = \frac{y_1 - y_0}{x_1 - x_0}(x - x_0),$$

le polynôme

$$f\left(X, \frac{y_1 - y_0}{x_1 - x_0}(X - x_0) + y_0\right) \in \mathbf{Q}[X]$$

est *généralement* de degré 3, il a deux racines rationnelles x_0 et x_1, donc sa troisième racine est aussi rationnelle. Bien entendu pour enlever le mot *généralement* il suffit de passer en coordonnées projectives (ce qui revient à tenir compte des points à l'infini).

De même si on dispose d'un point rationnel sur une telle courbe, la tangente à la courbe en ce point coupe *généralement* la cubique en un autre point. Si le premier est rationnel alors le second l'est aussi : on est amené à résoudre une équation de degré 3 en x, qui a une racine double, donc se décompose sur $\mathbf{Q}$ en un produit d'un terme linéaire au carré par un autre terme linéaire.

C'est la base de la théorie des courbes elliptiques.

Ce processus géométrique permet de paramétrer les solutions rationnelles d'une équation de degré 2 en 2 inconnues. Il ne donne pas forcément d'information sur les solutions entières. Par exemple si d est un entier positif qui n'est pas un carré, les points rationnels $\neq (0,0)$ sur la courbe $x^2 - dy^2 = 1$ sont paramétrés par

$$x = \frac{dt^2+1}{dt^2-1}, \quad y = \frac{2t}{dt^2-1}.$$

Mais ce n'est pas la bonne voie pour trouver les points entiers !

Quand d est un entier positif qui n'est pas un carré, l'équation $x^2 - dy^2 = \pm 1$, où les inconnues x et y sont dans $\mathbf{Z}$, porte le nom de Pell–Fermat. Pourtant elles ont été étudiées par le mathématicien indien Brahmagupta (598–670) bien avant Pell (1611–1685) et Fermat. Il a trouvé la plus petite solution en entiers positifs de l'équation $x^2 - 92y^2 = 1$, qui est $(x, y) = (1151\ ,\ 120)$. On peut noter que l'équation $x^2 - 23y^2 = 1$ possède la solution $(x, y) = (24, 5)$, puisque $24^2 = 576$ et $5^2 \cdot 23 = 575$. En développant $(24 + 5\sqrt{23})^2 = 1151 + 120\sqrt{23}$ on retrouve la solution donnée par Brahmagupta.

Au XIIème siècle, Bhaskara II a trouvé pour l'équation $x^2 - 61y^2 = 1$ (qui sera plus tard considérée par Fermat) la solution

$$(x, y) = (1\,766\,319\,049\ ,\ 226\,153\,980).$$

Plus tard Narayana (∼1340–∼1400) a obtenu pour $x^2 - 103y^2 = 1$ la solution

$$(x, y) = (227\,528\ ,\ 22\,419).$$

Un algorithme pour résoudre une équation de Pell–Fermat consiste à développer $\sqrt{d}$ en *fraction continue* (1.1) (voir par exemple [6] Chap. 3 et 4). La résolution de l'équation $x^2 - dy^2 = \pm 1$ est étroitement liée à la recherche des *unités* du corps quadratique $\mathbf{Q}(\sqrt{d})$. L'algèbre classique enseigne que les unités d'un corps sont les éléments non nuls du corps, et aussi que les seuls idéaux d'un corps sont les deux idéaux triviaux (0) et (1). Mais en théorie algébrique des nombres on travaille avec des *corps de nombres* (cf. § 2), qui sont par définition les extensions *finies* de $\mathbf{Q}$. Un corps de nombres a un *anneau d'entiers* (cf § 4.2) ; ce que l'on appelle *unité d'un corps de nombres* (cf. § 4.4) ou *idéal d'un corps de nombres* (cf. § 4.5) est une unité ou un idéal de cet anneau.

0.2 Quelques problèmes ouverts en théorie des nombres

Un des attraits de la théorie des nombres réside dans le contraste entre la simplicité de certains énoncés et leur profondeur. En particulier de nombreux problèmes ouverts sont faciles à énoncer. Nous en donnons un échantillon, les exemples ne manquent pas. On pourra consulter notamment [7] et [11] pour en savoir plus.

Conjecture 0.1 de Pillai

La conjecture de Catalan, datant de 1844, a été résolue en 2003 : *les seules puissances parfaites (c'est-à-dire de la forme a^b avec a et b entiers ≥ 2) qui soient consécutives sont $8 = 2^3$ et $9 = 3^2$.* En 1945 S.S. Pillai a posé le problème plus difficile cité plus haut (Conjecture 0.1).

Conjecture de Beal

Considérons l'équation diophantienne

$$x^p + y^q = z^r$$

en entiers x, y, z, p, q, r, tous positifs, avec les conditions supplémentaires que x, y, z sont premiers entre eux et que p, q, r satisfont

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

On connaît dix solutions :

$$1 + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$

$$3^5 + 11^4 = 122^2, \qquad 17^7 + 76271^3 = 21063928^2, \qquad 1414^3 + 2213459^2 = 65^7,$$

$$9262^3 + 15312283^2 = 113^7, \qquad 43^8 + 96222^3 = 30042907^2, \qquad 33^8 + 1549034^2 = 15613^3.$$

On conjecture qu'*il n'y en a pas d'autres* que celles qu'on déduit trivialement de celles-ci par symétries.

Conjecture *abc*

On désigne par $R(n)$ le *radical* ou *partie sans facteurs carrés* d'un entier positif n : si $n = p_1^{a_1} \cdots p_s^{a_s}$ avec des nombres premiers p_i deux-à-deux distincts et des exposants a_i tous ≥ 1, alors $R(n) = p_1 \cdots p_s$. On écrit

$$R(n) = \prod_{p \mid n} p,$$

où p décrit l'ensemble des nombres premiers.

Une forme faible de la conjecture *abc* est qu'*il existe une constante absolue ϑ telle que, pour tout triplet (a, b, c) d'entiers positifs premiers entre eux satisfaisant $a + b = c$, on ait $c < R(abc)^{\vartheta}$.* Une telle inégalité aurait beaucoup de conséquences. La forme plus précise de la conjecture *abc* est la suivante :

Conjecture 0.3 (Conjecture *abc*)**.** *Pour tout $\epsilon > 0$, il existe une constante $\kappa(\epsilon) > 0$ telle que, pour tout triplet (a, b, c) d'entiers positifs premiers entre eux satisfaisant $a + b = c$, on ait*

$$c < \kappa(\epsilon) R(abc)^{1+\epsilon}.$$

Un analogue de cette conjecture *abc*, dans laquelle on remplace l'anneau $\mathbf{Z}$ des entiers rationnels par l'anneau des polynômes en une variable sur un corps K, est le théorème suivant dû à R. Mason ([9], Chap. IV § 7).

Théorème 0.4 (Mason)**.** *Soient K un corps, A, B, C trois polynômes de $K[X]$ premiers entre eux vérifiant $A + B = C$ et a, b, c leurs degrés. Soit r le nombre de zéros sans multiplicités du produit ABC. Alors*

$$\max\{a, b, c\} \leq r - 1.$$

Le nombre r est le degré du *radical* R de ABC, c'est-à-dire du produit des facteurs irréductibles unitaires de ABC :

$$R = \prod_{P|ABC} P$$

où P décrit l'ensemble des polynômes irréductibles unitaires de $K[X]$. C'est ce qui explique l'analogie avec la conjecture *abc*.

Démonstration du théorème 0.4 de Mason. Posons $f = A/C$, $g = B/C$, de sorte que la relation $A + B = C$ devient $f + g = 1$. En dérivant on obtient $f' + g' = 0$, relation que l'on peut écrire

$$\frac{A}{B} = \frac{f}{g} = -\frac{g'/g}{f'/f}.$$

Soit R le radical du produit ABC : son degré est r, comme nous l'avons vu. On remarque que $A_1 = -Rg'/g$ et $B_1 = Rf'/f$ sont deux polynômes de degrés $r - 1$, qui vérifient

$$\frac{A}{B} = \frac{A_1}{B_1}.$$

Comme A/B est une fraction rationnelle irréductible, il en résulte que les polynômes A et B sont tous deux de degré $\leq r - 1$. □

Problème de Waring

Soit $k \geq 2$ un entier rationnel. On définit $g(k)$ comme le plus petit des entiers $g \geq 1$ tels que tout entier positif soit somme d'au plus g puissances k-ièmes. Par exemple $g(4) \geq 19$ car pour écrire le nombre 79 comme somme de puissances 4-ièmes (bicarrés) il faut au moins 19 termes (comme $79 = 4 \times 16 + 15$, le plus économique est d'ajouter 4 fois 2^4 et 15 fois 1).

Divisons 3^k par 2^k, ce qui veut dire qu'on écrit $3^k = 2^k q + r$ avec $0 < r < 2^k$. Ainsi $q = [(3/2)^k]$ (où $[\cdot]$ désigne la partie entière). Le nombre $I(k) = 2^k + q - 2$ est appelé *constante de Waring idéale*. L'écriture de $2^k q - 1$ comme somme de puissances k-ième nécessite au moins $I(k)$ termes, à savoir $q - 1$ termes 2^k et $2^k - 1$ termes 1, donc $g(k) \geq I(k)$. L'égalité $g(k) = I(k)$ est vérifiée pour de nombreuses valeurs de k (notamment toutes les valeurs de k "suffisamment grandes" ainsi que pour $2 \leq k \leq 4,716 \cdot 10^8$), mais on ne sait pas démontrer qu'elle est vraie pour tout $k \geq 2$.

Nombres parfaits

Un nombre parfait est un entier positif qui est égal à la moitié de la somme de ses diviseurs. Par exemple 6 a pour diviseurs 1, 2, 3, et 6, dont la somme est 12. De même 28 a pour diviseurs 1, 2, 4, 7, 14 et 28, la somme étant 56. Il est assez facile de démontrer qu'un nombre pair est parfait si et seulement s'il s'écrit $2^{p-1}M_p$, avec p premier tel que le *nombre de Mersenne* $M_p = 2^p - 1$ soit également premier. La principale question ouverte concerne l'*existence de nombre parfaits impairs*. On n'en connaît pas et on serait surpris qu'il en existe !

Nombres premiers de Mersenne et de Fermat

Une autre question ouverte sur les nombres parfaits consiste à savoir s'il y en a une infinité. On soupçonne que la réponse est positive, et plus précisément qu'*il existe une infinité de nombres premiers p tels que le nombre de Mersenne $M_p = 2^p - 1$ soit également premier*. Mais on ne sait pas non plus démontrer qu'*il existe une infinité de p tels que le nombre $M_p = 2^p - 1$ ne soit pas premier.*

Dans le même ordre d'idée il est facile de voir qu'un entier de la forme $2^m + 1$ ne peut être premier que si m est une puissance de 2. Un nombre premier de la forme $F_n = 2^{2^n} + 1$ est appelé *nombre premier de Fermat*. On ne sait pas s'il y en a une infinité, on soupçonne que non, mais on ne sait même pas démontrer qu'*il y a une infinité de n tels que le nombre* $2^{2^n} + 1$ *ne soit pas premier.*

Nombres premiers jumeaux

Y a-t-il une infinité de nombres premiers p tels que $p + 2$ *soit aussi premier ?*

Hypothèse H de Schinzel

Y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$ *?* Plus généralement A. Schinzel a formulé une hypothèse qui répond aux questions analogues que l'on peut se poser sur la représentation d'une infinité de nombre premiers par des polynômes.

Conjecture de Goldbach

Goldbach a conjecturé que *tout entier pair* ≥ 6 *est somme de deux nombres premiers impairs* et que *tout entier impair* ≥ 9 *est somme de trois nombres premiers impairs.*

Sur le petit théorème de Fermat

Si p est un nombre premier alors $2^{p-1} \equiv 1 \pmod{p}$. On connaît deux nombres premiers tels que $2^{p-1} \equiv 1 \pmod{p^2}$, ce sont 1 093 et 3 511. On ignore s'il y en a d'autres, on ignore s'il y en a une infinité, mais on ne sait pas non plus démontrer qu'il y a une infinité de p qui ne satisfont pas cette congruence.

Conjecture d'Artin

Y a-t-il une infinité de p premiers tels que la classe de 2 *modulo p soit un générateur du groupe cycle* $(\mathbf{Z}/p\mathbf{Z})^\times$ *?* Le même problème se pose si on remplace 2 par un nombre entier rationnel qui n'est pas un carré et qui n'est pas -1.

Spectre de Markoff

L'équation

$$x^2 + y^2 + z^2 = 3xyz \tag{0.5}$$

en nombres entiers positifs possède une infinité de solutions, et il est facile de donner un algorithme qui les fournit toutes. Mais la question suivante est actuellement l'objet de travaux en cours : *si z est un entier* ≥ 3 *tel qu'il existe x et y avec* $x < y < z$ *et* (x, y, z) *solution de l'équation de Markoff, alors le couple* (x, y) *est unique.*

Problèmes d'irrationalité et de transcendance

On ignore la nature arithmétique (déterminer si le nombre donné est rationnel, ou bien irrationnel algébrique, ou bien transcendant) de la plupart des constantes de l'analyse. Il serait plus rapide de donner la liste de celles pour lesquelles on connaît la réponse. Parmi les principaux défis citons la *Constante d'Euler* (voir [7] Th. 422 § 22.5 p. 347)

$$\gamma = \lim_{N\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N}\right) - \log N = 0,577\,215\,664\,901\,532\,860\,60\ldots, \tag{0.6}$$

celle de *Catalan*

$$\sum_{n\geq 0} \frac{(-1)^n}{(2n+1)^2} = 0,915\,965\,594\,177\,219\,015\,05\ldots,$$

la valeur aux points entiers impairs ≥ 5 de la fonction zêta de Riemann (0.7), la valeur au point $1/5$ de la fonction Gamma d'Euler

$$\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}dt = \frac{1}{ze^{\gamma z}\prod_{n\geq 1}\left(1+\frac{z}{n}\right)e^{-z/n}} = \lim_{n\to\infty}\frac{(n-1)!}{z(z+1)\cdots(z+n-1)}n^z.$$

Une des principales conjectures du sujet est due à Schanuel : *si $x_1, \ldots, x_n$ sont des nombres complexes linéairement indépendants sur le corps des nombres rationnels, alors parmi les nombres $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$ il y en a au moins n qui sont algébriquement indépendants.*

Problèmes d'approximation diophantienne

On ne connaît aucun exemple explicite de triplet (α, g, c) formé d'un nombre algébrique réel irrationnel $\alpha \in (0,1)$, d'un entier $g \geq 3$ et d'un *chiffre* $c \in \{0, 1, \ldots, g-1\}$ pour lequel on puisse affirmer que le chiffre c intervient une infinité de fois dans le développement en base g de α :

$$\alpha = c_1 g^{-1} + c_2 g^{-2} + \cdots + c_n g^{-n} + \cdots$$

avec $0 \leq c_i \leq g-1$. E. Borel a conjecturé en 1950 que la suite $(c_1, c_2, \ldots)$ de ces chiffres devrait se comporter comme une suite *aléatoire*, au sens où toute suite donnée de chiffres devrait apparaître une infinité de fois.
Dans le même ordre d'idées, on ne sait pas s'il existe un nombre algébrique réel α de degré ≥ 3 pour lequel la suite des *réduites* successives $(a_0, a_1, \ldots, a_n, \ldots)$ dans le développement en fraction continue (1.1)

$$\alpha = a_0 + \frac{1}{|a_1+}\ \frac{1}{|a_2+}\ \cdots\ \frac{1}{|a_n+}\ \cdots$$

est bornée. Et on ne sait pas non plus s'il en existe un pour lequel cette suite ne soit pas bornée. Le sentiment le plus généralement partagé est que cette suite n'est jamais bornée.

D'autres problèmes de théorie des nombres demandent un peu plus de connaissances pour pouvoir comprendre leurs énoncés. En voici quelques uns.

Hypothèse de Riemann

La fonction

$$\zeta(s) = \sum_{n\geq 1} n^{-s} \tag{0.7}$$

est bien définie par cette série de Dirichlet dans le demi–plan où la partie réelle $\Re e(s)$ de s est > 1. Elle a été étudiée par Euler pour les valeurs de s entières (Euler ne se limitait pas aux valeurs ≥ 2, il étudiait aussi les valeurs négatives) et par Riemann pour les valeurs complexes. Elle se prolonge en une fonction méromorphe dans le plan complexe, avec un unique pôle au point $s = 1$. Dans le demi–plan $\Re e(s) \leq 0$, cette fonction prolongée s'annule exactement aux entiers négatifs pairs :

$$\zeta(-2 = \zeta(-4) = \cdots = \zeta(-2n) = \cdots = 0$$

(ce sont les *zéros triviaux*). L'hypothèse, formulée par B. Riemann en 1859 dans l'unique article *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* (8 pages) qu'il ait écrit en théorie

des nombres, est que *les zéros de la fonction zêta dans la bande critique* $0 < \Re e(s) < 1$ *sont tous situés sur la droite critique* $\Re e(s) = 1/2$.

Il existe de nombreuses formulations équivalentes de l'Hypothèse de Riemann. Par exemple il est connu que la fonction $\pi(x)$ qui compte les nombres premiers $\leq x$

$$\pi(x) = \sum_{p \leq x} 1$$

satisfait

$$\pi(x) = \mathrm{Li}(x) + \mathcal{O}\left(xe^{-c\sqrt{\log x}}\right),$$

où la fonction *logarithme intégral* Li, définie par

$$\mathrm{Li}(x) = \int_2^\infty \frac{dt}{\log t},$$

vérifie

$$\mathrm{Li}(x) = \frac{x}{\log x} + \frac{1}{2} \cdot \frac{x}{(\log x)^2} + \mathcal{O}\left(\frac{x}{(\log x)^3}\right).$$

Une des formulations équivalentes de l'Hypothèse de Riemann est

$$\pi(x) = \mathrm{Li}(x) + \mathcal{O}\left(\sqrt{x}\log x\right).$$

Profitons-en pour indiquer quelques valeurs *spéciales* de la fonction zêta :

$$\zeta(0) = -\frac{1}{2}, \quad \zeta(-1) = -\frac{1}{12}, \quad \zeta(-3) = \frac{1}{120}, \quad \zeta(-5) = -\frac{1}{252}$$

et

$$\zeta(2) = \frac{\pi^2}{2}, \quad \zeta(4) = -\frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(8) = -\frac{\pi^8}{9450}.$$

On a aussi

$$\zeta'(0) = -\frac{1}{2}\log(2\pi) \quad \text{et} \quad \lim_{s \to 1}\left(\zeta(s) - \frac{1}{s-1}\right) = \gamma$$

où γ est la Constante d'Euler (0.6).

Nombre de classes 1

Existe-t-il une infinité de corps de nombres ayant un nombre de classes 1 *?* Les tables numériques semblent indiquer que cela devrait être vrai même si on se limite aux corps quadratiques réels.

Problème inverse de la théorie de Galois

Peut-on réaliser tout groupe fini comme groupe de Galois sur $\mathbf{Q}$ *d'un corps de nombres (= extension finie de* $\mathbf{Q}$*) ?*