Problèmes ouverts en Théorie des nombres

Henri Cohen

Institut de Mathématiques de Bordeaux

4 juin 2009, Bordeaux

Introduction

La théorie des nombres (ou arithmétique) s'occupe principalement des propriétés des nombres entiers. Bien que son sujet d'étude soit tout à fait élémentaire, les outils qu'elle utilise proviennent de toutes les branches des mathématiques, sont souvent très profonds, et assez fréquemment les outils sont en fait créés dans le but de résoudre des problèmes de théorie des nombres : l'un des exemples les plus frappants est la théorie des groupes, anneaux, corps, qui s'est principalement dévelopé sous l'impulsion de problèmes de théorie des nombres.

La TN a ceci de paradoxal que la plupart de ses problèmes peuvent être énoncés de manière tout à fait élémentaire, mais que les outils nécessaires pour leur résolution (quand on les résoud !) sont en général très sophistiqués. Dans cet exposé, je vais donner un aperçu d'un certain nombre de problèmes ouverts, dans certains cas des méthodes d'approche, et également des commentaires de nature plus philosophiques.

Introduction

La théorie des nombres (ou arithmétique) s'occupe principalement des propriétés des nombres entiers. Bien que son sujet d'étude soit tout à fait élémentaire, les outils qu'elle utilise proviennent de toutes les branches des mathématiques, sont souvent très profonds, et assez fréquemment les outils sont en fait créés dans le but de résoudre des problèmes de théorie des nombres : l'un des exemples les plus frappants est la théorie des groupes, anneaux, corps, qui s'est principalement dévelopé sous l'impulsion de problèmes de théorie des nombres.

La TN a ceci de paradoxal que la plupart de ses problèmes peuvent être énoncés de manière tout à fait élémentaire, mais que les outils nécessaires pour leur résolution (quand on les résoud !) sont en général très sophistiqués. Dans cet exposé, je vais donner un aperçu d'un certain nombre de problèmes ouverts, dans certains cas des méthodes d'approche, et également des commentaires de nature plus philosophiques.

Problème Infaisable (1)

Bien évidemment, les problèmes ouverts interessants sont innombrables, et il faut donc faire une sélection. La mienne ne sera évidemment pas la même que celle d'un collègue.

• Le problème de la "normalité". Considérons un nombre réel qui apparait naturellement en mathématiques, tel que $\sqrt{2}$, π, e, etc... On l'écrit en décimal (toute autre base ferait l'affaire). Par exemple

$$\sqrt{2} = 1.41421356237309504880168872420969807856967187537 69\cdots$$

Il est naturel de penser que chaque chiffre apparait avec la même probabilité de $1/10$, chaque séquence de 2 chiffres avec la probabilité de $1/100$, etc... Et pourtant on ne sait rien démontrer à ce sujet. Comme $\sqrt{2}$ est irrationnel, les décimales ne peuvent pas être périodiques à partir d'un certain rang, ce qui exclut en particulier le fait qu'à partir d'un certain rang on n'ait qu'un seul chiffre. Par contre rien n'empêche qu'à partir d'un certain rang il n'y ait que des 8 et des 9 par exemple. Commentaire :

Problème Infaisable (2)

• Le problème des grands écarts entre deux nombres premiers consécutifs : étant donné x, quelle taille doit on prendre pour y en fonction de x pour être sûr que pour x assez grand il y ait un nombre premier dans l'intervalle $[x, x + y]$? Un résultat élémentaire (le "postulat de Bertrand") affirme que $y = x$ convient : il y a toujours un premier entre x et $2x$. Ceci a été grandement amélioré avec des méthodes toujours plus sophistiquées, et le record actuel dû à Baker–Harman–Pintz est $y = x^{0.525\cdots}$. En admettant l'hypothèse de Riemann, qui est l'une des plus célèbres conjectures des mathématiques (voir plus loin), on peut montrer que $y = x^{1/2} = \sqrt{x}$ convient. Et pourtant ! On pense qu'en vérité $y = 1.5 \log^2(x)$ devrait convenir. Commentaire :

Problème Infaisable (2)

• Le problème des grands écarts entre deux nombres premiers consécutifs : étant donné x, quelle taille doit on prendre pour y en fonction de x pour être sûr que pour x assez grand il y ait un nombre premier dans l'intervalle $[x, x + y]$? Un résultat élémentaire (le "postulat de Bertrand") affirme que $y = x$ convient : il y a toujours un premier entre x et $2x$. Ceci a été grandement amélioré avec des méthodes toujours plus sophistiquées, et le record actuel dû à Baker–Harman–Pintz est $y = x^{0.525\cdots}$. En admettant l'hypothèse de Riemann, qui est l'une des plus célèbres conjectures des mathématiques (voir plus loin), on peut montrer que $y = x^{1/2} = \sqrt{x}$ convient. Et pourtant ! On pense qu'en vérité $y = 1.5 \log^2(x)$ devrait convenir. Commentaire :

Nombres Premiers, encore

• Si on s'occupe maintenant de petits écarts entre nombres premiers, la situation change radicalement, bien que de nombreux et célèbres problemes subsistent. Le plus connu est celui des nombres premiers jumeaux : existe-t-il une infinité de couples de nombres premiers $(p, p+2)$, dits jumeaux ? Cette fois ci ce n'est plus un problème infaisable et on sait beaucoup de choses (mais on ne connait toujours pas la réponse). Le meilleur résultat, dû à Chen dans les années 60, est qu'il existe une infinité de nombres premiers p tels que $p+2$ ait au plus deux facteurs premiers. On connait aussi depuis longtemps une estimation précise, évidemment aussi conjecturale, du nombre de jumeaux $(p, p+2)$ avec $p \leq X$.

• Le problème de Goldbach. Tout nombre pair (supérieur à 4) est-il la somme de deux nombres premiers ? C'est un problème très voisin du précédent, les mêmes méthodes s'appliquent avec les mêmes résultats. Ce qui est frustrant c'est que le nombre de décompositions en somme de deux premiers devient très vite grand, mais on ne sait pas démontrer qu'il est non nul !

Nombres Premiers, encore

• Si on s'occupe maintenant de petits écarts entre nombres premiers, la situation change radicalement, bien que de nombreux et célèbres problemes subsistent. Le plus connu est celui des nombres premiers jumeaux : existe-t-il une infinité de couples de nombres premiers $(p, p+2)$, dits jumeaux ? Cette fois ci ce n'est plus un problème infaisable et on sait beaucoup de choses (mais on ne connait toujours pas la réponse). Le meilleur résultat, dû à Chen dans les années 60, est qu'il existe une infinité de nombres premiers p tels que $p+2$ ait au plus deux facteurs premiers. On connait aussi depuis longtemps une estimation précise, évidemment aussi conjecturale, du nombre de jumeaux $(p, p+2)$ avec $p \leq X$.

• Le problème de Goldbach. Tout nombre pair (supérieur à 4) est-il la somme de deux nombres premiers ? C'est un problème très voisin du précédent, les mêmes méthodes s'appliquent avec les mêmes résultats. Ce qui est frustrant c'est que le nombre de décompositions en somme de deux premiers devient très vite grand, mais on ne sait pas démontrer qu'il est non nul !

Problèmes Diophantiens

A partir de maintenant, je ne vais mentionner que des problèmes diophantiens, c'est à dire essentiellement des équations que l'on souhaite résoudre en nombres entiers ou rationnels. Attention ! entier signifie toujours entier relatif. Dans les problèmes précédents, du moins ceux qui ne sont pas infaisables, l'outil principal est l'analyse. Pour les équations diophantiennes on utilise en plus de l'algèbre et de la géométrie algébrique.

La géométrie algébrique est un outil extrêment puissant (et également très sophistiqué, lire difficile) qui permet d'obtenir de remarquables résultats dans beaucoup de domaines de la TN, mais aussi qui permet d'obtenir (facilement cette fois) une estimation intuitive de la difficulté d'un problème. Par exemple, pour ceux qui connaissent la notion, la difficulté d'une équation diophantienne donnée par une courbe se mesure à son genre : en genre supérieur ou égal à 2 le problème est très difficile voire infaisable, en genre 1 on peut espérer résoudre le problème (sans garantie), en genre 0 le problème est facile et même algorithmique.

Problèmes Diophantiens

A partir de maintenant, je ne vais mentionner que des problèmes diophantiens, c'est à dire essentiellement des équations que l'on souhaite résoudre en nombres entiers ou rationnels. Attention ! entier signifie toujours entier relatif. Dans les problèmes précédents, du moins ceux qui ne sont pas infaisables, l'outil principal est l'analyse. Pour les équations diophantiennes on utilise en plus de l'algèbre et de la géométrie algébrique.
La géométrie algébrique est un outil extrêment puissant (et également très sophistiqué, lire difficile) qui permet d'obtenir de remarquables résultats dans beaucoup de domaines de la TN, mais aussi qui permet d'obtenir (facilement cette fois) une estimation intuitive de la difficulté d'un problème. Par exemple, pour ceux qui connaissent la notion, la difficulté d'une équation diophantienne donnée par une courbe se mesure à son genre : en genre supérieur ou égal à 2 le problème est très difficile voire infaisable, en genre 1 on peut espérer résoudre le problème (sans garantie), en genre 0 le problème est facile et même algorithmique.

Problèmes Diophantiens

A partir de maintenant, je ne vais mentionner que des problèmes diophantiens, c'est à dire essentiellement des équations que l'on souhaite résoudre en nombres entiers ou rationnels. Attention ! entier signifie toujours entier relatif. Dans les problèmes précédents, du moins ceux qui ne sont pas infaisables, l'outil principal est l'analyse. Pour les équations diophantiennes on utilise en plus de l'algèbre et de la géométrie algébrique.
La géométrie algébrique est un outil extrêment puissant (et également très sophistiqué, lire difficile) qui permet d'obtenir de remarquables résultats dans beaucoup de domaines de la TN, mais aussi qui permet d'obtenir (facilement cette fois) une estimation intuitive de la difficulté d'un problème. Par exemple, pour ceux qui connaissent la notion, la difficulté d'une équation diophantienne donnée par une courbe se mesure à son genre : en genre supérieur ou égal à 2 le problème est très difficile voire infaisable, en genre 1 on peut espérer résoudre le problème (sans garantie), en genre 0 le problème est facile et même algorithmique.

La Conjecture *abc*

Probablement l'équation diophantienne la plus importante, car elle donne la solution à beaucoup d'autres (par exemple au célèbre "grand théorème de Fermat", démontré par Wiles), est la conjecture *abc*, due à Masser–Oesterlé. Définissons le radical $\mathrm{Rad}(N)$ d'un entier N comme le produit des nombres premiers divisant N. Par exemple, le radical de p^{1000} est égal à p si p est premier. Le radical de 1728 est égal à 6. Mais ceci sont des exceptions, et en général le radical de N n'est pas beaucoup plus petit que N (il est même égal à N si N est sans facteur carré, ce qui se produit avec une probabilité de $6/\pi^2$, supérieure à 60%).

La conjecture *abc* est la suivante : si a, b sont premiers entre eux et si on pose $c = a + b$, alors le radical du produit abc ne peut pas etre beaucoup plus petit que le maximum de $|a|$, $|b|$, ou $|c|$ (on exclut bien sur les cas triviaux où $abc = 0$). Plus précisément $\mathrm{Rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$ pour tout $\varepsilon > 0$. Commentaire :

La Conjecture *abc*

Probablement l'équation diophantienne la plus importante, car elle donne la solution à beaucoup d'autres (par exemple au célèbre "grand théorème de Fermat", démontré par Wiles), est la conjecture *abc*, due à Masser–Oesterlé. Définissons le radical $\mathrm{Rad}(N)$ d'un entier N comme le produit des nombres premiers divisant N. Par exemple, le radical de p^{1000} est égal à p si p est premier. Le radical de 1728 est égal à 6. Mais ceci sont des exceptions, et en général le radical de N n'est pas beaucoup plus petit que N (il est même égal à N si N est sans facteur carré, ce qui se produit avec une probabilité de $6/\pi^2$, supérieure à 60%).

La conjecture *abc* est la suivante : si a, b sont premiers entre eux et si on pose $c = a + b$, alors le radical du produit abc ne peut pas etre beaucoup plus petit que le maximum de $|a|$, $|b|$, ou $|c|$ (on exclut bien sur les cas triviaux où $abc = 0$). Plus précisément $\mathrm{Rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$ pour tout $\varepsilon > 0$. Commentaire :

La Conjecture de Hall

Un cas particulier de *abc* est la conjecture dite de Hall. Ce cas particulier est important car réciproquement, elle entraine “presque” la conjecture générale. La conjecture de Hall est la suivante : étant donnés x et y tels que $y^2 - x^3 \neq 0$, $|y^2 - x^3|$ ne peut pas être beaucoup plus petit que la racine carrée de x, plus précisément le rapport

$$r = \frac{x^{1/2}}{|y^2 - x^3|}$$

doit être majoré par x^ε pour tout $\varepsilon > 0$.

Ce qui est amusant avec cette conjecture est qu’elle est facilement testable sur ordinateur. On sait que r peut être plus grand que 1.035 infiniment souvent (c’est le meilleur résultat connu). On appelle donc exemple de “bonne qualité” tout couple (x, y) tel que $r > 1.035$. On ne connait que 39 tels couples : leur recherche est un exercice amusant. Commentaire :

La Conjecture de Hall

Un cas particulier de *abc* est la conjecture dite de Hall. Ce cas particulier est important car réciproquement, elle entraine “presque” la conjecture générale. La conjecture de Hall est la suivante : étant donnés x et y tels que $y^2 - x^3 \neq 0$, $|y^2 - x^3|$ ne peut pas être beaucoup plus petit que la racine carrée de x, plus précisément le rapport

$$r = \frac{x^{1/2}}{|y^2 - x^3|}$$

doit être majoré par x^ε pour tout $\varepsilon > 0$.
Ce qui est amusant avec cette conjecture est qu’elle est facilement testable sur ordinateur. On sait que r peut être plus grand que 1.035 infiniment souvent (c’est le meilleur résultat connu). On appelle donc exemple de “bonne qualité” tout couple (x, y) tel que $r > 1.035$. On ne connait que 39 tels couples : leur recherche est un exercice amusant.
Commentaire :

Equations Superfermat (1)

Nous en arrivons maintenant à des équations plus spécifiques. Maintenant que le grand théorème de Fermat est résolu (! ! !) on peut s'interesser à l'équation superfermat qui est la généralisation suivante :

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

avec p, q, r entiers supérieurs ou égaux à 2, éventuellement différents. Il faut absolument supposer en plus que x, y et z sont sans facteurs communs (ce n'est pas nécessaire pour Fermat par homogénéité).
Exercice facile : Trouver une infinité de solutions (avec x, y et z avec facteurs communs) de l'équation $z^7 = x^3 + y^5$.

Equations Superfermat (1)

Nous en arrivons maintenant à des équations plus spécifiques. Maintenant que le grand théorème de Fermat est résolu (! ! !) on peut s'interesser à l'équation superfermat qui est la généralisation suivante :

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

avec p, q, r entiers supérieurs ou égaux à 2, éventuellement différents. Il faut absolument supposer en plus que x, y et z sont sans facteurs communs (ce n'est pas nécessaire pour Fermat par homogénéité).
Exercice facile : Trouver une infinité de solutions (avec x, y et z avec facteurs communs) de l'équation $z^7 = x^3 + y^5$.

Equations Superfermat (2)

Pour superfermat, le principe philosophique concernant le genre s'applique parfaitement : posons $\chi = 1/p + 1/q + 1/r$. Si $\chi > 1$ (genre 0) c'est très facile, il y a une infinité de solutions que l'on sait parfaitement décrire. Si $\chi = 1$ (genre 1) ce n'est pas trop dur, mais si on mettait des coefficients devant x^p, y^q, ou z^r, cela pourrait le devenir. Enfin si $\chi < 1$ (genre ≥ 2) c'est très difficile. Il n'y a qu'un nombre fini de solutions pour chaque (p, q, r), et si *abc* est vraie il n'y en a qu'un nombre fini en tout (on en connait 10, et il n'y en a peut être pas d'autres).

Au prix de gros efforts, on a réussi à résoudre certaines de ces équations avec $\chi < 1$, la plus spectaculaire étant $z^7 = x^2 + y^3$, qui a (aux signes près) 5 solutions, la plus grande étant

$$17^7 = 21063928^2 + (-76271)^3 .$$

Conjecture (voir plus haut) : il n'y a pas de solution à l'exemple ci-dessus $z^7 = x^3 + y^5$ si on suppose x, y, z sans facteur commun. Ceci est totalement hors de portée pour l'instant.

Equations Superfermat (2)

Pour superfermat, le principe philosophique concernant le genre s'applique parfaitement : posons $\chi = 1/p + 1/q + 1/r$. Si $\chi > 1$ (genre 0) c'est très facile, il y a une infinité de solutions que l'on sait parfaitement décrire. Si $\chi = 1$ (genre 1) ce n'est pas trop dur, mais si on mettait des coefficients devant x^p, y^q, ou z^r, cela pourrait le devenir. Enfin si $\chi < 1$ (genre ≥ 2) c'est très difficile. Il n'y a qu'un nombre fini de solutions pour chaque (p, q, r), et si *abc* est vraie il n'y en a qu'un nombre fini en tout (on en connait 10, et il n'y en a peut être pas d'autres).

Au prix de gros efforts, on a réussi à résoudre certaines de ces équations avec $\chi < 1$, la plus spectaculaire étant $z^7 = x^2 + y^3$, qui a (aux signes près) 5 solutions, la plus grande étant

$$17^7 = 21063928^2 + (-76271)^3 .$$

Conjecture (voir plus haut) : il n'y a pas de solution à l'exemple ci-dessus $z^7 = x^3 + y^5$ si on suppose x, y, z sans facteur commun. Ceci est totalement hors de portée pour l'instant.

Equations Superfermat (2)

Pour superfermat, le principe philosophique concernant le genre s'applique parfaitement : posons $\chi = 1/p + 1/q + 1/r$. Si $\chi > 1$ (genre 0) c'est très facile, il y a une infinité de solutions que l'on sait parfaitement décrire. Si $\chi = 1$ (genre 1) ce n'est pas trop dur, mais si on mettait des coefficients devant x^p, y^q, ou z^r, cela pourrait le devenir. Enfin si $\chi < 1$ (genre ≥ 2) c'est très difficile. Il n'y a qu'un nombre fini de solutions pour chaque (p, q, r), et si *abc* est vraie il n'y en a qu'un nombre fini en tout (on en connait 10, et il n'y en a peut être pas d'autres).
Au prix de gros efforts, on a réussi à résoudre certaines de ces équations avec $\chi < 1$, la plus spectaculaire étant $z^7 = x^2 + y^3$, qui a (aux signes près) 5 solutions, la plus grande étant

$$17^7 = 21063928^2 + (-76271)^3 .$$

Conjecture (voir plus haut) : il n'y a pas de solution à l'exemple ci-dessus $z^7 = x^3 + y^5$ si on suppose x, y, z sans facteur commun. Ceci est totalement hors de portée pour l'instant.

Equations de type Catalan (1)

L'équation de Catalan est $y^n - x^m = \pm 1$ avec $xy \neq 0$, qui a la solution évidente $3^2 - 2^3 = 1$.

Exercice (pas trop difficile, résolu par V.-A. Lebesgue au 19ème siècle) : la seule solution de $y^2 = x^p - 1$ est $(x, y) = (1, 0)$.

Exercice (nettement plus difficile, résolu dans les années 1950) : les seules solutions de $y^2 = x^p + 1$ sont $(x, y) = (0, \pm 1)$, et $(x, y) = (2, \pm 3)$ quand $p = 3$.

L'équation générale a été résolue par P. Mihailescu en 2002 par des méthodes assez sophistiquées, mais loin du niveau de celle de Wiles. C'est un vrai tour de force et un miracle. Commentaire :

Equations de type Catalan (1)

L'équation de Catalan est $y^n - x^m = \pm 1$ avec $xy \neq 0$, qui a la solution évidente $3^2 - 2^3 = 1$.

Exercice (pas trop difficile, résolu par V.-A. Lebesgue au 19ème siècle) : la seule solution de $y^2 = x^p - 1$ est $(x, y) = (1, 0)$.

Exercice (nettement plus difficile, résolu dans les années 1950) : les seules solutions de $y^2 = x^p + 1$ sont $(x, y) = (0, \pm 1)$, et $(x, y) = (2, \pm 3)$ quand $p = 3$.

L'équation générale a été résolue par P. Mihailescu en 2002 par des méthodes assez sophistiquées, mais loin du niveau de celle de Wiles. C'est un vrai tour de force et un miracle. Commentaire :

Equations de type Catalan (1)

L'équation de Catalan est $y^n - x^m = \pm 1$ avec $xy \neq 0$, qui a la solution évidente $3^2 - 2^3 = 1$.

Exercice (pas trop difficile, résolu par V.-A. Lebesgue au 19ème siècle) : la seule solution de $y^2 = x^p - 1$ est $(x, y) = (1, 0)$.

Exercice (nettement plus difficile, résolu dans les années 1950) : les seules solutions de $y^2 = x^p + 1$ sont $(x, y) = (0, \pm 1)$, et $(x, y) = (2, \pm 3)$ quand $p = 3$.

L'équation générale a été résolue par P. Mihailescu en 2002 par des méthodes assez sophistiquées, mais loin du niveau de celle de Wiles. C'est un vrai tour de force et un miracle. Commentaire :

Equations de type Catalan (1)

L'équation de Catalan est $y^n - x^m = \pm 1$ avec $xy \neq 0$, qui a la solution évidente $3^2 - 2^3 = 1$.

Exercice (pas trop difficile, résolu par V.-A. Lebesgue au 19ème siècle) : la seule solution de $y^2 = x^p - 1$ est $(x, y) = (1, 0)$.

Exercice (nettement plus difficile, résolu dans les années 1950) : les seules solutions de $y^2 = x^p + 1$ sont $(x, y) = (0, \pm 1)$, et $(x, y) = (2, \pm 3)$ quand $p = 3$.

L'équation générale a été résolue par P. Mihailescu en 2002 par des méthodes assez sophistiquées, mais loin du niveau de celle de Wiles. C'est un vrai tour de force et un miracle. Commentaire :

Equations de type Catalan (2)

On peut généraliser et considérer par exemple $y^n - x^m = \pm 2$.
Exercice (pas difficile) Montrer que les seules solutions de $y^2 = x^p - 2$ sont $(x, y) = (3, \pm 5)$ pour $p = 3$.
Donc par analogie :
Exercice (nettement plus difficile) Montrer que les seules solutions de $y^2 = x^p + 2$ sont $(x, y) = (-1, \pm 1)$ quand p est impair.
Non, c'est une blague : l'exercice ci-dessus, pourtant d'énoncé très simple, est en fait une conjecture.

Equations de type Catalan (2)

On peut généraliser et considérer par exemple $y^n - x^m = \pm 2$.
Exercice (pas difficile) Montrer que les seules solutions de $y^2 = x^p - 2$ sont $(x, y) = (3, \pm 5)$ pour $p = 3$.
Donc par analogie :
Exercice (nettement plus difficile) Montrer que les seules solutions de $y^2 = x^p + 2$ sont $(x, y) = (-1, \pm 1)$ quand p est impair.
Non, c'est une blague : l'exercice ci-dessus, pourtant d'énoncé très simple, est en fait une conjecture.

Equations de type Catalan (2)

On peut généraliser et considérer par exemple $y^n - x^m = \pm 2$.
Exercice (pas difficile) Montrer que les seules solutions de $y^2 = x^p - 2$ sont $(x, y) = (3, \pm 5)$ pour $p = 3$.
Donc par analogie :
Exercice (nettement plus difficile) Montrer que les seules solutions de $y^2 = x^p + 2$ sont $(x, y) = (-1, \pm 1)$ quand p est impair.
Non, c'est une blague : l'exercice ci-dessus, pourtant d'énoncé très simple, est en fait une conjecture.

Problèmes liés à la conjecture BSD (1)

La conjecture de Birch et Swinnerton-Dyer (BSD) est à mon avis l'une des plus élégantes et des plus importantes conjectures de toutes les mathématiques (en plus il y a 1 million de dollars à la clé). Je ne vais pas l'énoncer ici, mais donner un certain nombre de conséquences diophantiennes. J'insiste sur le fait que les conséquences sont probablement aussi difficiles que BSD elle-même, donc si vous trouvez la solution à l'un de ces problèmes, vous avez probablement aussi résolu BSD.

- Si n est un entier sans facteur carré et congru à 4, 6, 7, ou 8 modulo 9, alors n est somme de deux cubes de nombres rationnels. Exemple :

$$15 = (397/294)^3 + (683/294)^3 \ .$$

Noter que la plupart des autres entiers sans facteurs carrés (ceux congrus à 1, 2, 3, ou 5 modulo 9) ne sont pas somme de deux cubes, mais certains le sont :

Exercice Trouver x et y rationnels tels que $91 = x^3 + y^3$.

Problèmes liés à la conjecture BSD (1)

La conjecture de Birch et Swinnerton-Dyer (BSD) est à mon avis l'une des plus élégantes et des plus importantes conjectures de toutes les mathématiques (en plus il y a 1 million de dollars à la clé). Je ne vais pas l'énoncer ici, mais donner un certain nombre de conséquences diophantiennes. J'insiste sur le fait que les conséquences sont probablement aussi difficiles que BSD elle-même, donc si vous trouvez la solution à l'un de ces problèmes, vous avez probablement aussi résolu BSD.

- Si n est un entier sans facteur carré et congru à 4, 6, 7, ou 8 modulo 9, alors n est somme de deux cubes de nombres rationnels. Exemple :

$$15 = (397/294)^3 + (683/294)^3 \ .$$

Noter que la plupart des autres entiers sans facteurs carrés (ceux congrus à 1, 2, 3, ou 5 modulo 9) ne sont pas somme de deux cubes, mais certains le sont :

Exercice Trouver x et y rationnels tels que $91 = x^3 + y^3$.

Problèmes liés à la conjecture BSD (2)

- Le problème des nombres congruents. C'est le dernier problème hérité de l'antiquité qui n'est pas complètement résolu. Un nombre congruent est un entier S qui est la surface d'un triangle pythagoricien, c'est-à-dire un triangle rectangle à cotés rationnels. Par exemple le célèbre triangle de cotés $(3, 4, 5)$ a comme surface 6, donc 6 est congruent.

Exercice. Montrer que 5 et 7 sont aussi congruents (attention les cotés ne sont plus entiers).

Démontrer qu'un nombre n'est pas congruent est nettement plus difficile.

Exercice (Difficile ; si vous y arrivez sans connaitre la solution, envoyez moi un mail) : montrer que le nombre 1 n'est pas congruent.

Problèmes liés à la conjecture BSD (2)

- Le problème des nombres congruents. C'est le dernier problème hérité de l'antiquité qui n'est pas complètement résolu. Un nombre congruent est un entier S qui est la surface d'un triangle pythagoricien, c'est-à-dire un triangle rectangle à cotés rationnels. Par exemple le célèbre triangle de cotés $(3, 4, 5)$ a comme surface 6, donc 6 est congruent.

Exercice. Montrer que 5 et 7 sont aussi congruents (attention les cotés ne sont plus entiers).

Démontrer qu'un nombre n'est pas congruent est nettement plus difficile.

Exercice (Difficile ; si vous y arrivez sans connaitre la solution, envoyez moi un mail) : montrer que le nombre 1 n'est pas congruent.

Problèmes liés à la conjecture BSD (2)

• Le problème des nombres congruents. C'est le dernier problème hérité de l'antiquité qui n'est pas complètement résolu. Un nombre congruent est un entier S qui est la surface d'un triangle pythagoricien, c'est-à-dire un triangle rectangle à cotés rationnels. Par exemple le célèbre triangle de cotés $(3, 4, 5)$ a comme surface 6, donc 6 est congruent.

Exercice. Montrer que 5 et 7 sont aussi congruents (attention les cotés ne sont plus entiers).

Démontrer qu'un nombre n'est pas congruent est nettement plus difficile.

Exercice (Difficile ; si vous y arrivez sans connaitre la solution, envoyez moi un mail) : montrer que le nombre 1 n'est pas congruent.

Problèmes liés à la conjecture BSD (3)

BSD nous donne le résultat positif suivant (comme pour les sommes de 2 cubes) : si n est un entier sans facteur carré congru à 5, 6, ou 7 modulo 8 alors n est un nombre congruent.

En fait, aussi bien dans le cas des sommes de 2 cubes qu'ici, BSD nous donne une réponse conjecturale pour **tout** entier n. L'utilisation pratique pour la recherche d'une solution de ces équations est donc la suivante : si BSD nous dit qu'il ne doit pas y avoir de solution, on s'arrête là. Evidemment BSD pourrait être fausse et il pourrait y avoir une solution, mais c'est peu probable. Par contre si BSD nous dit qu'il doit y avoir une solution, on peut maintenant s'acharner avec des méthodes plus ou moins sophistiquées pour la trouver.

Problèmes liés à la conjecture BSD (3)

BSD nous donne le résultat positif suivant (comme pour les sommes de 2 cubes) : si n est un entier sans facteur carré congru à 5, 6, ou 7 modulo 8 alors n est un nombre congruent.
En fait, aussi bien dans le cas des sommes de 2 cubes qu'ici, BSD nous donne une réponse conjecturale pour **tout** entier n. L'utilisation pratique pour la recherche d'une solution de ces équations est donc la suivante : si BSD nous dit qu'il ne doit pas y avoir de solution, on s'arrête là. Evidemment BSD pourrait être fausse et il pourrait y avoir une solution, mais c'est peu probable. Par contre si BSD nous dit qu'il doit y avoir une solution, on peut maintenant s'acharner avec des méthodes plus ou moins sophistiquées pour la trouver.

Problèmes divers (1)

• Formes quadratiques ternaires. Un célèbre résultat de Gauss dit que tout entier (disons à nouveau sans facteur carré) est une somme de trois carrés (d'entiers ou de rationnels, ici contrairement aux cubes c'est la même chose) à l'exception de ceux congrus à 7 modulo 8 qui ne le sont pas (cette dernière assertion est un exercice immédiat). En d'autres termes l'équation $n = x^2 + y^2 + z^2$ est soluble pour tout $n \not\equiv 7 \pmod 8$. Philosophiquement c'est raisonnable, tout problème de ce type doit être facile.

Vraiment ?

Conjecture Si n est un nombre impair l'équation

$$n = x^2 + 2y^2 + 5z^2 + xz$$

a une solution. Commentaire :

Problèmes divers (1)

• Formes quadratiques ternaires. Un célèbre résultat de Gauss dit que tout entier (disons à nouveau sans facteur carré) est une somme de trois carrés (d'entiers ou de rationnels, ici contrairement aux cubes c'est la même chose) à l'exception de ceux congrus à 7 modulo 8 qui ne le sont pas (cette dernière assertion est un exercice immédiat). En d'autres termes l'équation $n = x^2 + y^2 + z^2$ est soluble pour tout $n \not\equiv 7 \pmod 8$. Philosophiquement c'est raisonnable, tout problème de ce type doit être facile.
Vraiment ?
Conjecture Si n est un nombre impair l'équation

$$n = x^2 + 2y^2 + 5z^2 + xz$$

a une solution. Commentaire :

Problèmes divers (2)

• Sommes de cubes. On a vu ci-dessus une conjecture pour les sommes de 2 cubes. Pour plus de 2, on a les conjectures suivantes :
(1). Tout entier n qui n'est pas congru à 4 ou 5 modulo 9 est une somme de 3 cubes d'entiers. (exercice immédiat : la condition n non congru à 4 ou 5 modulo 9 est nécessaire). En plus, il devrait même y avoir une infinité de telles représentations. Assez récemment, on a trouvé la première solution pour $n = 30$:

$$30 = (-283059965)^3 + (-2218888517)^3 + (2220422932)^3$$

Pour $n \leq 100$ on ne connait aucune solution pour $n = 33$, 42, et 74. Des amateurs ?

Problèmes divers (3)

(2). Conjecture : tout entier est somme de 4 cubes d'entiers (on a besoin d'au moins 4 puisque 3 ne suffisent pas pour les $n \equiv 4$ ou 5 modulo 9).

Exercice (facile, utiliser des identités sur des polynômes du premier degré) : montrer que c'est vrai pour tout entier n divisible par 3.

Un très joli théorème de Demyanenko (complètement élementaire mais très astucieux) montre que c'est vrai justement pour tous les nombres non congrus à 4 ou 5 modulo 9. Commentaire :

Problèmes divers (3)

(2). Conjecture : tout entier est somme de 4 cubes d'entiers (on a besoin d'au moins 4 puisque 3 ne suffisent pas pour les $n \equiv 4$ ou 5 modulo 9).

Exercice (facile, utiliser des identités sur des polynômes du premier degré) : montrer que c'est vrai pour tout entier n divisible par 3.

Un très joli théorème de Demyanenko (complètement élementaire mais très astucieux) montre que c'est vrai justement pour tous les nombres non congrus à 4 ou 5 modulo 9. Commentaire :

Problèmes divers (3)

(2). Conjecture : tout entier est somme de 4 cubes d'entiers (on a besoin d'au moins 4 puisque 3 ne suffisent pas pour les $n \equiv 4$ ou 5 modulo 9).

Exercice (facile, utiliser des identités sur des polynômes du premier degré) : montrer que c'est vrai pour tout entier n divisible par 3.

Un très joli théorème de Demyanenko (complètement élementaire mais très astucieux) montre que c'est vrai justement pour tous les nombres non congrus à 4 ou 5 modulo 9. Commentaire :

Problèmes divers (4)

• Le problème du cuboide rationnel : existe-t-il un parallelipipède rectangle dont tous les cotés, diagonales des faces, et diagonales principales sont rationnels ? En d'autres termes, existe-t-il des entiers a, b et c tels que $a^2 + b^2$, $a^2 + c^2$, $b^2 + c^2$, et $a^2 + b^2 + c^2$ sont tous des carrés parfaits ?

Exercice. Trouver (par ordinateur) des cuboides satisfaisant aux trois premières conditions, et des cuboides satisfaisant à toutes sauf l'une des trois premières.

L'intuition philosophique mentionnée au début semble indiquer que la réponse devrait être négative.

Problèmes divers (4)

• Le problème du cuboide rationnel : existe-t-il un parallelipipède rectangle dont tous les cotés, diagonales des faces, et diagonales principales sont rationnels ? En d'autres termes, existe-t-il des entiers a, b et c tels que $a^2 + b^2$, $a^2 + c^2$, $b^2 + c^2$, et $a^2 + b^2 + c^2$ sont tous des carrés parfaits ?

Exercice. Trouver (par ordinateur) des cuboides satisfaisant aux trois premières conditions, et des cuboides satisfaisant à toutes sauf l'une des trois premières.

L'intuition philosophique mentionnée au début semble indiquer que la réponse devrait être négative.

Problèmes divers (5)

- Les fractions égyptiennes.

Je termine par un problème (conjectural) sur lequel il est très facile de trouver des résultats partiels : le problème $4/n$. On dira que n est un nombre égyptien (ma terminologie) s'il existe des entiers positifs a, b, c tels que

$$\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}\,.$$

Une petite recherche sur ordinateur montre que tout entier semble être égyptien, et même que le nombre de solutions à l'équation ci-dessus croit très vite avec n. Et pourtant on ne sait pas démontrer que ce nombre est non nul pour tout n. Frustrant.

Problèmes divers (5)

- Les fractions égyptiennes.

Je termine par un problème (conjectural) sur lequel il est très facile de trouver des résultats partiels : le problème $4/n$. On dira que n est un nombre égyptien (ma terminologie) s'il existe des entiers positifs a, b, c tels que

$$\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}\,.$$

Une petite recherche sur ordinateur montre que tout entier semble être égyptien, et même que le nombre de solutions à l'équation ci-dessus croit très vite avec n. Et pourtant on ne sait pas démontrer que ce nombre est non nul pour tout n. Frustrant.

Problèmes divers (6)

Il est alors interessant de trouver des ensembles infinis d'entiers qui sont égyptiens, et essayer comme cela de recouvrir le plus d'entiers possibles. Suggestions d'exercices, aucun vraiment difficile. Il faut toutefois connaitre les CNS pour que -3 et -4 soient des carrés modulo un nombre premier p, et la conséquence sur la représentation de p sous la forme $p = x^2 - xy + y^2$ et $p = x^2 + y^2$ respectivement.

(1). Le plus petit entier non égyptien, s'il existe, est un nombre premier.

(2). Montrer que si il existe un diviseur de $n + 4$ qui est congru à 3 modulo 4 alors n est égyptien. En particulier si $n \equiv 0$ ou 2 modulo 3 (déja les $2/3$ de tous les entiers) n est égyptien.

(3). Déduire de (2) que si $n+4$ n'est pas une somme de 2 carrés, alors n est égytien. Ceci montre (grâce à des théorèmes sur les sommes de 2 carrés) que les entiers non égyptiens sont de densité nulle.

Problèmes divers (6)

Il est alors interessant de trouver des ensembles infinis d'entiers qui sont égyptiens, et essayer comme cela de recouvrir le plus d'entiers possibles. Suggestions d'exercices, aucun vraiment difficile. Il faut toutefois connaitre les CNS pour que -3 et -4 soient des carrés modulo un nombre premier p, et la conséquence sur la représentation de p sous la forme $p = x^2 - xy + y^2$ et $p = x^2 + y^2$ respectivement.

(1). Le plus petit entier non égyptien, s'il existe, est un nombre premier.

(2). Montrer que si il existe un diviseur de $n + 4$ qui est congru à 3 modulo 4 alors n est égyptien. En particulier si $n \equiv 0$ ou 2 modulo 3 (déja les $2/3$ de tous les entiers) n est égyptien.

(3). Déduire de (2) que si $n+4$ n'est pas une somme de 2 carrés, alors n est égytien. Ceci montre (grâce à des théorèmes sur les sommes de 2 carrés) que les entiers non égyptiens sont de densité nulle.

Problèmes divers (6)

Il est alors interessant de trouver des ensembles infinis d'entiers qui sont égyptiens, et essayer comme cela de recouvrir le plus d'entiers possibles. Suggestions d'exercices, aucun vraiment difficile. Il faut toutefois connaitre les CNS pour que -3 et -4 soient des carrés modulo un nombre premier p, et la conséquence sur la représentation de p sous la forme $p = x^2 - xy + y^2$ et $p = x^2 + y^2$ respectivement.
(1). Le plus petit entier non égyptien, s'il existe, est un nombre premier.
(2). Montrer que si il existe un diviseur de $n + 4$ qui est congru à 3 modulo 4 alors n est égyptien. En particulier si $n \equiv 0$ ou 2 modulo 3 (déja les $2/3$ de tous les entiers) n est égyptien.
(3). Déduire de (2) que si $n+4$ n'est pas une somme de 2 carrés, alors n est égytien. Ceci montre (grâce à des théorèmes sur les sommes de 2 carrés) que les entiers non égyptiens sont de densité nulle.

Problèmes divers (6)

Il est alors interessant de trouver des ensembles infinis d'entiers qui sont égyptiens, et essayer comme cela de recouvrir le plus d'entiers possibles. Suggestions d'exercices, aucun vraiment difficile. Il faut toutefois connaitre les CNS pour que -3 et -4 soient des carrés modulo un nombre premier p, et la conséquence sur la représentation de p sous la forme $p = x^2 - xy + y^2$ et $p = x^2 + y^2$ respectivement.
(1). Le plus petit entier non égyptien, s'il existe, est un nombre premier.
(2). Montrer que si il existe un diviseur de $n + 4$ qui est congru à 3 modulo 4 alors n est égyptien. En particulier si $n \equiv 0$ ou 2 modulo 3 (déja les $2/3$ de tous les entiers) n est égyptien.
(3). Déduire de (2) que si $n+4$ n'est pas une somme de 2 carrés, alors n est égytien. Ceci montre (grâce à des théorèmes sur les sommes de 2 carrés) que les entiers non égyptiens sont de densité nulle.

Problèmes divers (7)

(4). Supposons $4/n = 1/a+1/b+1/c$ où on peut supposer $a \leq b \leq c$. Donner des bornes sur a en fonction de n, puis sur b en fonction de a et n, et en déduire que le nombre de solutions à l'équation est fini, et trouver un majorant.

(5). Soit $n \geq 2$. Montrer qu'il existe des entiers positifs a et b tels que $3/n = 1/a + 1/b$ si et seulement si il existe un diviseur premier de n qui n'est pas congru à 1 modulo 3. En déduire que si n n'est pas de la forme $n = x^2 - xy + y^2$ alors n est égyptien. Comme dans l'exercice précédent, les entiers de la forme $n = x^2 - xy + y^2$ sont de densité nulle.

(6) Dans un genre un peu différent, montrer que tout nombre rationnel positif est somme d'un nombre fini de fractions de la forme $1/a_i$ avec les a_i entiers positifs distincts (sinon c'est trop facile !).

Problèmes divers (7)

(4). Supposons $4/n = 1/a+1/b+1/c$ où on peut supposer $a \leq b \leq c$. Donner des bornes sur a en fonction de n, puis sur b en fonction de a et n, et en déduire que le nombre de solutions à l'équation est fini, et trouver un majorant.

(5). Soit $n \geq 2$. Montrer qu'il existe des entiers positifs a et b tels que $3/n = 1/a + 1/b$ si et seulement si il existe un diviseur premier de n qui n'est pas congru à 1 modulo 3. En déduire que si n n'est pas de la forme $n = x^2 - xy + y^2$ alors n est égyptien. Comme dans l'exercice précédent, les entiers de la forme $n = x^2 - xy + y^2$ sont de densité nulle.

(6) Dans un genre un peu différent, montrer que tout nombre rationnel positif est somme d'un nombre fini de fractions de la forme $1/a_i$ avec les a_i entiers positifs distincts (sinon c'est trop facile !).

Problèmes divers (7)

(4). Supposons $4/n = 1/a+1/b+1/c$ où on peut supposer $a \leq b \leq c$. Donner des bornes sur a en fonction de n, puis sur b en fonction de a et n, et en déduire que le nombre de solutions à l'équation est fini, et trouver un majorant.
(5). Soit $n \geq 2$. Montrer qu'il existe des entiers positifs a et b tels que $3/n = 1/a + 1/b$ si et seulement si il existe un diviseur premier de n qui n'est pas congru à 1 modulo 3. En déduire que si n n'est pas de la forme $n = x^2 - xy + y^2$ alors n est égyptien. Comme dans l'exercice précédent, les entiers de la forme $n = x^2 - xy + y^2$ sont de densité nulle.
(6) Dans un genre un peu différent, montrer que tout nombre rationnel positif est somme d'un nombre fini de fractions de la forme $1/a_i$ avec les a_i entiers positifs distincts (sinon c'est trop facile !).

Mon site web

`http ://www.math.u-bordeaux1.fr/~cohen/`

Cet article, incluant le texte et les exercices :

irem.pdf