Equations Diophantiennes

Henri Cohen

Institut de Mathématiques de Bordeaux

16 novembre 2010, Caen

Première partie : équations diophantiennes

Système d'équations polynomiales dont on cherche les solutions en nombres entiers ou rationnels.

- Les polynômes sont à coefficients rationnels.
- On peut soit vouloir seulement connaître l'existence de solutions, soit demander une description complète de l'ensemble des solutions.

Chaque équation ou famille d'équations peut nécessiter l'introduction de nouvelles méthodes, ou même le développement de nouvelles branches des mathématiques. Exemple célèbre : le développement de la théorie algébrique des nombres par Kummer, Dirichlet, Dedekind,... en vue de résoudre l'équation de Fermat

$$x^n + y^n = z^n \, .$$

C'est un exemple d'équation avec paramètre, la variable n nétant pas considérée comme inconnue.

Première partie : équations diophantiennes

Système d'équations polynomiales dont on cherche les solutions en nombres entiers ou rationnels.

• Les polynômes sont à coefficients rationnels.

• On peut soit vouloir seulement connaître l'existence de solutions, soit demander une description complète de l'ensemble des solutions.

Chaque équation ou famille d'équations peut nécessiter l'introduction de nouvelles méthodes, ou même le développement de nouvelles branches des mathématiques. Exemple célèbre : le développement de la théorie algébrique des nombres par Kummer, Dirichlet, Dedekind,... en vue de résoudre l'équation de Fermat

$$x^n + y^n = z^n \, .$$

C'est un exemple d'équation avec paramètre, la variable n nétant pas considérée comme inconnue.

Exemples de problèmes résolus mais très difficiles I

Le problème de Fermat (FLT) ci-dessus est le plus célèbre :

- Le cas $n = 2$ résolu par les anciens Grecs (triangles pythagoriciens).

- Les cas $n = 3$ et $n = 4$ résolus par Fermat (méthode de descente infinie).

- Méthodes de théorie algébrique des nombres introduites par Kummer traitent $n \leq 10^8$ par exemple, mais pas tout n.

- Un théorème profond de Ribet ramène FLT à la conjecture de Taniyama–Weil, initiant ainsi les méthodes modulaires pour les équations diophantiennes.

- Finalement, en 1994-1995, Wiles et Taylor–Wiles démontrent la conjecture de TW semistable, ce qui est suffisant pour FLT.

Exemples de problèmes résolus mais très difficiles I

Le problème de Fermat (FLT) ci-dessus est le plus célèbre :

• Le cas $n = 2$ résolu par les anciens Grecs (triangles pythagoriciens).

• Les cas $n = 3$ et $n = 4$ résolus par Fermat (méthode de descente infinie).

• Méthodes de théorie algébrique des nombres introduites par Kummer traitent $n \leq 10^8$ par exemple, mais pas tout n.

• Un théorème profond de Ribet ramène FLT à la conjecture de Taniyama–Weil, initiant ainsi les méthodes modulaires pour les équations diophantiennes.

• Finalement, en 1994-1995, Wiles et Taylor–Wiles démontrent la conjecture de TW semistable, ce qui est suffisant pour FLT.

Exemples de problèmes résolus mais très difficiles II

Un deuxième exemple est la conjecture de Catalan : pour $m \geq 2$, $n \geq 2$, la seule solution de l'équation

$$x^m - y^n = 1$$

avec $xy \neq 0$ provient de l'égalité $3^2 - 2^3 = 1$ (donc pour $(m, n) = (2, 3)$ on a $(x, y) = (\pm 3, 2)$). L'historique est un peu différent :

• En 1850, V. A. Lebesgue résout le case $n = 2$ (pas de solution). Exercice, pas difficile mais pas si facile que ça ! ! !

• En 1950-60, Nagell, Chein et Ko Chao résolvent le cas beaucoup plus difficile $m = 2$ (solution $(\pm 3, 2)$ pour $n = 3$).

La morale (pas toujours vraie mais fréquente), est qu'il est souvent plus facile de montrer qu'une ED n'a pas du tout de solutions que de montrer qu'elle n'a que les solutions connues (FLT a des solutions nontriviales où l'une des variables est nulle).

Exemples de problèmes résolus mais très difficiles II

Un deuxième exemple est la conjecture de Catalan : pour $m \geq 2$, $n \geq 2$, la seule solution de l'équation

$$x^m - y^n = 1$$

avec $xy \neq 0$ provient de l'égalité $3^2 - 2^3 = 1$ (donc pour $(m, n) = (2, 3)$ on a $(x, y) = (\pm 3, 2)$). L'historique est un peu différent :

• En 1850, V. A. Lebesgue résout le case $n = 2$ (pas de solution). Exercice, pas difficile mais pas si facile que ça ! ! !

• En 1950-60, Nagell, Chein et Ko Chao résolvent le cas beaucoup plus difficile $m = 2$ (solution $(\pm 3, 2)$ pour $n = 3$).
La morale (pas toujours vraie mais fréquente), est qu'il est souvent plus facile de montrer qu'une ED n'a pas du tout de solutions que de montrer qu'elle n'a que les solutions connues (FLT a des solutions nontriviales où l'une des variables est nulle).

Exemples de problèmes résolus mais très difficiles II

Un deuxième exemple est la conjecture de Catalan : pour $m \geq 2$, $n \geq 2$, la seule solution de l'équation

$$x^m - y^n = 1$$

avec $xy \neq 0$ provient de l'égalité $3^2 - 2^3 = 1$ (donc pour $(m, n) = (2, 3)$ on a $(x, y) = (\pm 3, 2)$). L'historique est un peu différent :

• En 1850, V. A. Lebesgue résout le case $n = 2$ (pas de solution). Exercice, pas difficile mais pas si facile que ça ! ! !

• En 1950-60, Nagell, Chein et Ko Chao résolvent le cas beaucoup plus difficile $m = 2$ (solution $(\pm 3, 2)$ pour $n = 3$).

La morale (pas toujours vraie mais fréquente), est qu'il est souvent plus facile de montrer qu'une ED n'a pas du tout de solutions que de montrer qu'elle n'a que les solutions connues (FLT a des solutions nontriviales où l'une des variables est nulle).

Exemples de problèmes résolus mais très difficiles II

Un deuxième exemple est la conjecture de Catalan : pour $m \geq 2$, $n \geq 2$, la seule solution de l'équation

$$x^m - y^n = 1$$

avec $xy \neq 0$ provient de l'égalité $3^2 - 2^3 = 1$ (donc pour $(m, n) = (2, 3)$ on a $(x, y) = (\pm 3, 2)$). L'historique est un peu différent :

• En 1850, V. A. Lebesgue résout le case $n = 2$ (pas de solution). Exercice, pas difficile mais pas si facile que ça ! ! !

• En 1950-60, Nagell, Chein et Ko Chao résolvent le cas beaucoup plus difficile $m = 2$ (solution $(\pm 3, 2)$ pour $n = 3$).
La morale (pas toujours vraie mais fréquente), est qu'il est souvent plus facile de montrer qu'une ED n'a pas du tout de solutions que de montrer qu'elle n'a que les solutions connues (FLT a des solutions nontriviales où l'une des variables est nulle).

Exemples de problèmes résolus mais très difficiles III

On peut donc supposer $(m, n) = (p, q)$ avec p, q premiers impairs.

• En 1960, Cassels démontre le résultat fondamental que $x^p - y^q = 1$ implique $p \mid y$ et $q \mid p$. Démonstration tout a fait non triviale, mais classique, utilisant une méthode analytique appelée méthode de Runge.

• Dans les années suivantes, plusieurs auteurs trouvent des conditions analogues à celles pour FLT, et Tijdeman prouve la finitude du nombre total de solutions grâce aux techniques de formes linéaires en logarithmes initiées par Baker.

Exemples de problèmes résolus mais très difficiles III

On peut donc supposer $(m, n) = (p, q)$ avec p, q premiers impairs.

- En 1960, Cassels démontre le résultat fondamental que $x^p - y^q = 1$ implique $p \mid y$ et $q \mid p$. Démonstration tout a fait non triviale, mais classique, utilisant une méthode analytique appelée méthode de Runge.

- Dans les années suivantes, plusieurs auteurs trouvent des conditions analogues à celles pour FLT, et Tijdeman prouve la finitude du nombre total de solutions grâce aux techniques de formes linéaires en logarithmes initiées par Baker.

Exemples de problèmes résolus mais très difficiles IV

- En 1999, Mihailescu réalise une percée en montrant que $q^{p-1} \equiv 1 \pmod{p^2}$ et $p^{q-1} \equiv 1 \pmod{q^2}$ (double condition Wieferich). Etonnant car 1 page de démonstration classique à partir de Cassels. On ne connait que 7 paires de Wieferich, mais on conjecture qu'il y en a une infinité.

- En 2000-2002, en utilisant les résultats classiques de théorie algébrique des nombres (nombres de classes, théorème de Stickelberger), il donne des critères supplémentaires pour Catalan.

- Enfin en 2002, en utilisant un profond théorème de Thaine toujours en TAN, mais beaucoup plus récent, il finit la démonstration de Catalan. Donc pas de méthodes modulaires ici.

Exemples de problèmes résolus mais très difficiles IV

• En 1999, Mihailescu réalise une percée en montrant que $q^{p-1} \equiv 1 \pmod{p^2}$ et $p^{q-1} \equiv 1 \pmod{q^2}$ (double condition Wieferich). Etonnant car 1 page de démonstration classique à partir de Cassels. On ne connait que 7 paires de Wieferich, mais on conjecture qu'il y en a une infinité.

• En 2000-2002, en utilisant les résultats classiques de théorie algébrique des nombres (nombres de classes, théorème de Stickelberger), il donne des critères supplémentaires pour Catalan.

• Enfin en 2002, en utilisant un profond théorème de Thaine toujours en TAN, mais beaucoup plus récent, il finit la démonstration de Catalan. Donc pas de méthodes modulaires ici.

Exemples de problèmes non résolus I

Chaque ED donne lieu à un nouveau challenge : en fait, dixième problème de Hilbert, résolu par une suite d'auteurs culminant avec Matyasevitch, dit qu'il ne peut pas y avoir d'algorithme de résolution. Voici une liste commentée :

- L'équation

$$y^2 = x^p + t\ .$$

Si p est fixé, ou bien si t est fixé et $t < 0$, on a des techniques, pas totalement générales, mais qui marchent bien. Par contre si t est fixé et $t > 0$, on ne sait pas grand chose.

Exemples de problèmes non résolus I

Chaque ED donne lieu à un nouveau challenge : en fait, dixième problème de Hilbert, résolu par une suite d'auteurs culminant avec Matyasevitch, dit qu'il ne peut pas y avoir d'algorithme de résolution. Voici une liste commentée :

- L'équation

$$y^2 = x^p + t \ .$$

Si p est fixé, ou bien si t est fixé et $t < 0$, on a des techniques, pas totalement générales, mais qui marchent bien. Par contre si t est fixé et $t > 0$, on ne sait pas grand chose.

Exemples de problèmes non résolus II

Exemples

$t = 1$: l'équation

$$y^2 = x^p + 1$$

résolue seulement en 1960 (ci-dessus).

$t = 2$: l'équation

$$y^2 = x^p + 2$$

est toujours non résolue !

$t = -2$: par contre l'équation

$$y^2 = x^p - 2$$

est facile à résoudre, bien qu'elle ait la solution $(x, y) = (3, \pm 5)$ pour $p = 3$; exercice ! ! (résolu plus loin pour $p = 3$, mais démonstration générale identique).

Exemples de problèmes non résolus II

Exemples

$t = 1$: l'équation

$$y^2 = x^p + 1$$

résolue seulement en 1960 (ci-dessus).

$t = 2$: l'équation

$$y^2 = x^p + 2$$

est toujours non résolue !

$t = -2$: par contre l'équation

$$y^2 = x^p - 2$$

est facile à résoudre, bien qu'elle ait la solution $(x, y) = (3, \pm 5)$ pour $p = 3$; exercice ! ! (résolu plus loin pour $p = 3$, mais démonstration générale identique).

Exemples de problèmes non résolus II

Exemples

$t = 1$: l'équation

$$y^2 = x^p + 1$$

résolue seulement en 1960 (ci-dessus).

$t = 2$: l'équation

$$y^2 = x^p + 2$$

est toujours non résolue !

$t = -2$: par contre l'équation

$$y^2 = x^p - 2$$

est facile à résoudre, bien qu'elle ait la solution $(x, y) = (3, \pm 5)$ pour $p = 3$; exercice ! ! (résolu plus loin pour $p = 3$, mais démonstration générale identique).

Exemples de problèmes non résolus II

- L'équation
$$x^3 + y^5 = z^7 .$$

Ici même pas de paramètre ! On doit demander x, y, z premiers entre eux, sinon solutions "triviales", exemple :

$$5526847993018333947494 4^3 + 507799783342085^5 = 6530347008^7 .$$

Exercice : retrouver cette solution ! On sait résoudre (avec difficulté) des équations telles que $x^2 + y^3 = z^7$, mais la présente semble beaucoup plus difficile.

- Plus généralement, équation superfermat
$$x^p + y^q = z^r$$

avec x, y, z premiers entre eux, p, q, $r \geq 2$ et $1/p + 1/q + 1/r < 1$ (sinon on sait faire). On connait exactement 10 solutions (aux signes et permutations près), telle que

$$43^8 + 96222^3 = 30042907^2 .$$

Y en a-t-il d'autres ?

Exemples de problèmes non résolus II

- L'équation
$$x^3 + y^5 = z^7 \ .$$

Ici même pas de paramètre ! On doit demander x, y, z premiers entre eux, sinon solutions "triviales", exemple :

$$5526847993018333947494 4^3 + 507799783342085^5 = 6530347008^7 \ .$$

Exercice : retrouver cette solution ! On sait résoudre (avec difficulté) des équations telles que $x^2 + y^3 = z^7$, mais la présente semble beaucoup plus difficile.

- Plus généralement, équation superfermat
$$x^p + y^q = z^r$$

avec x, y, z premiers entre eux, p, q, $r \geq 2$ et $1/p + 1/q + 1/r < 1$ (sinon on sait faire). On connait exactement 10 solutions (aux signes et permutations près), telle que

$$43^8 + 96222^3 = 30042907^2 \ .$$

Y en a-t-il d'autres ?

Exemples de problèmes non résolus III

• Le problème des nombres congruents, posé depuis les anciens Grecs : caractériser les entiers (nombres congruents) surfaces de triangles rectangles à cotés rationnels.
On sait (Fermat, Mordell) que s'il existe un tel triangle rectangle, il en existe une infinité.
Exemples : 6 est congruent (triangle $(3, 4, 5)$), 5 est congruent (triangle $(3/2, 20/3, 41/6)$), mais 1 n'est pas congruent (Fermat). Pas si facile à démontrer ! ! !

Se ramène à savoir si l'équation

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

a une solution rationnelle avec $y \neq 0$. “Presque” résolu par Tunnell, modulo la conjecture de Birch–Swinnerton Dyer BSD, voir ci-après.
Exemple (non résolu) : tout entier n (sans facteur carré) tel que $n \equiv 5, 6, 7 \pmod 8$ est congruent.

Exemples de problèmes non résolus III

• Le problème des nombres congruents, posé depuis les anciens Grecs : caractériser les entiers (nombres congruents) surfaces de triangles rectangles à cotés rationnels.
On sait (Fermat, Mordell) que s'il existe un tel triangle rectangle, il en existe une infinité.
Exemples : 6 est congruent (triangle $(3, 4, 5)$), 5 est congruent (triangle $(3/2, 20/3, 41/6)$), mais 1 n'est pas congruent (Fermat). Pas si facile à démontrer ! ! !

Se ramène à savoir si l'équation

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

a une solution rationnelle avec $y \neq 0$. "Presque" résolu par Tunnell, modulo la conjecture de Birch–Swinnerton Dyer BSD, voir ci-après.
Exemple (non résolu) : tout entier n (sans facteur carré) tel que $n \equiv 5, 6, 7 \pmod 8$ est congruent.

Exemples de problèmes non résolus III

• Le problème des nombres congruents, posé depuis les anciens Grecs : caractériser les entiers (nombres congruents) surfaces de triangles rectangles à cotés rationnels.
On sait (Fermat, Mordell) que s'il existe un tel triangle rectangle, il en existe une infinité.
Exemples : 6 est congruent (triangle $(3, 4, 5)$), 5 est congruent (triangle $(3/2, 20/3, 41/6)$), mais 1 n'est pas congruent (Fermat). Pas si facile à démontrer ! ! !

Se ramène à savoir si l'équation

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

a une solution rationnelle avec $y \neq 0$. “Presque” résolu par Tunnell, modulo la conjecture de Birch–Swinnerton Dyer BSD, voir ci-après.
Exemple (non résolu) : tout entier n (sans facteur carré) tel que $n \equiv 5, 6, 7 \pmod 8$ est congruent.

Exemples de problèmes non résolus IV

- Si $n \equiv 4$, 6, 7 ou 8 modulo 9, existe-t-il x, y rationnels tels que

$$n = x^3 + y^3 \qquad ?$$

Ceci résulte aussi de BSD. Elkies a montré (mais jamais écrit, même sous forme de preprint) que c'est vrai si n est un nombre premier $n \equiv 4, 7 \pmod 9$.

- Dans un genre un peu différent : étant donné un entier impair n, existe-t-il x, y tels que

$$x^2 + 2y^2 + 5z^2 + xz = n \qquad ?$$

Invraisemblable que ce ne soit pas connu, car ce n'est qu'une forme quadratique à trois variables et petits coefficients ! ! ! On sait que c'est vrai pour n assez grand, mais borne non effective.

Exemples de problèmes non résolus IV

• Si $n \equiv 4$, 6, 7 ou 8 modulo 9, existe-t-il x, y rationnels tels que

$$n = x^3 + y^3 \qquad ?$$

Ceci résulte aussi de BSD. Elkies a montré (mais jamais écrit, même sous forme de preprint) que c'est vrai si n est un nombre premier $n \equiv 4, 7 \pmod 9$.

• Dans un genre un peu différent : étant donné un entier impair n, existe-t-il x, y tels que

$$x^2 + 2y^2 + 5z^2 + xz = n \qquad ?$$

Invraisemblable que ce ne soit pas connu, car ce n'est qu'une forme quadratique à trois variables et petits coefficients ! ! ! On sait que c'est vrai pour n assez grand, mais borne non effective.

Exemples de problèmes non résolus V

Les problèmes de résolution en entiers et non en rationnels sont souvent beaucoup plus difficiles. Exemples :

• Tout entier n tel que $n \not\equiv \pm 4 \pmod 9$ est-il somme de trois cubes d'entiers (relatifs) ? Et même d'une infinité de manières ? Il est évident que $n \equiv \pm 4 \pmod 9$ ne peut pas l'être. En d'autres termes, résoudre $x^3 + y^3 + z^3 = n$.

Exemple : il a fallu attendre 2007 pour qu'on puisse trouver la décomposition

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

et on ne sait toujours pas si les nombres 33, 42, 52 ou 74 sont sommes de trois cubes.

• Tout entier n est-il somme de quatre cubes d'entiers ? En d'autres termes, résoudre $x^3 + y^3 + z^3 + t^3 = n$. Un très joli théorème de Demjanenko, démonstration très astucieuse mais simple, montre que c'est vrai si $n \not\equiv \pm 4 \pmod 9$. Et les autres ? Et peut-on toujours avoir $t = z$?

Exemples de problèmes non résolus V

Les problèmes de résolution en entiers et non en rationnels sont souvent beaucoup plus difficiles. Exemples :

• Tout entier n tel que $n \not\equiv \pm 4 \pmod 9$ est-il somme de trois cubes d'entiers (relatifs) ? Et même d'une infinité de manières ? Il est évident que $n \equiv \pm 4 \pmod 9$ ne peut pas l'être. En d'autres termes, résoudre $x^3 + y^3 + z^3 = n$.

Exemple : il a fallu attendre 2007 pour qu'on puisse trouver la décomposition

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

et on ne sait toujours pas si les nombres 33, 42, 52 ou 74 sont sommes de trois cubes.

• Tout entier n est-il somme de quatre cubes d'entiers ? En d'autres termes, résoudre $x^3 + y^3 + z^3 + t^3 = n$. Un très joli théorème de Demjanenko, démonstration très astucieuse mais simple, montre que c'est vrai si $n \not\equiv \pm 4 \pmod 9$. Et les autres ? Et peut-on toujours avoir $t = z$?

Exemples de problèmes non résolus V

Les problèmes de résolution en entiers et non en rationnels sont souvent beaucoup plus difficiles. Exemples :

• Tout entier n tel que $n \not\equiv \pm 4 \pmod 9$ est-il somme de trois cubes d'entiers (relatifs) ? Et même d'une infinité de manières ? Il est évident que $n \equiv \pm 4 \pmod 9$ ne peut pas l'être. En d'autres termes, résoudre $x^3 + y^3 + z^3 = n$.

Exemple : il a fallu attendre 2007 pour qu'on puisse trouver la décomposition

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

et on ne sait toujours pas si les nombres 33, 42, 52 ou 74 sont sommes de trois cubes.

• Tout entier n est-il somme de quatre cubes d'entiers ? En d'autres termes, résoudre $x^3 + y^3 + z^3 + t^3 = n$. Un très joli théorème de Demjanenko, démonstration très astucieuse mais simple, montre que c'est vrai si $n \not\equiv \pm 4 \pmod 9$. Et les autres ? Et peut-on toujours avoir $t = z$?

Exemples de problèmes non résolus VI

Deux derniers exemples dans un genre encore un peu différent :

• Le problème du cuboïde rationnel : existe-t-il un parallelipipède rectangle dont tous les cotés, diagonales des faces, et diagonales principales, soient rationnels ? En d'autres termes, existe-t-il des rationnels a, b, c tels que a^2+b^2, a^2+c^2, b^2+c^2 et $a^2+b^2+c^2$ soient des carrés de rationnels ?
Possible en enlevant une condition, mais problème non résolu.

• Le problème des fractions égyptiennes : étant donné un entier $n>1$, existe-t-il des entiers positifs a, b, c tels que $4/n=1/a+1/b+1/c$? Vrai avec densité 1, mais pas démontré pour tout n. Ce n'est pas une équation diophantienne à cause de la condition a, b, c positifs.

Exemples de problèmes non résolus VI

Deux derniers exemples dans un genre encore un peu différent :

• Le problème du cuboïde rationnel : existe-t-il un parallelipipède rectangle dont tous les cotés, diagonales des faces, et diagonales principales, soient rationnels ? En d'autres termes, existe-t-il des rationnels a, b, c tels que $a^2 + b^2$, $a^2 + c^2$, $b^2 + c^2$ et $a^2 + b^2 + c^2$ soient des carrés de rationnels ?
Possible en enlevant une condition, mais problème non résolu.

• Le problème des fractions égyptiennes : étant donné un entier $n > 1$, existe-t-il des entiers positifs a, b, c tels que $4/n = 1/a + 1/b + 1/c$? Vrai avec densité 1, mais pas démontré pour tout n. Ce n'est pas une équation diophantienne à cause de la condition a, b, c positifs.

Deuxième partie. Méthodes classiques : congruences I

D'innombrables méthodes. Je vais donner des exemples typiques.

• Congruences. Souvent, en regardant une équation modulo n pour un n convenable, on montre qu'elle n'a pas de solution. Exemple : $x^3 + y^3 = 3z^3$, il suffit de raisonner modulo 3, après réduction à x, y, z premiers entre eux. Exemple semblable $x^3 + y^3 = z^3$ avec $3 \nmid xyz$. Ici il suffit de raisonner modulo 9.

• Plus généralement, on peut raisonner modulo p^n pour p premier et $n \geq 1$: si l'équation a une solution pour tout p^n, on dit qu'elle est localement soluble en p. Ceci est équivalent à la solubilité dans le corps $\mathbb{Q}_p$ des nombres p-adiques. On dit bien sûr qu'elle est partout localement soluble (PLS) si elle est localement soluble pour tout p.

Il n'est malheureusement pas vrai qu'une équation PLS est soluble, voir ci-dessous.

Deuxième partie. Méthodes classiques : congruences I

D'innombrables méthodes. Je vais donner des exemples typiques.

• Congruences. Souvent, en regardant une équation modulo n pour un n convenable, on montre qu'elle n'a pas de solution. Exemple : $x^3 + y^3 = 3z^3$, il suffit de raisonner modulo 3, après réduction à x, y, z premiers entre eux. Exemple semblable $x^3 + y^3 = z^3$ avec $3 \nmid xyz$. Ici il suffit de raisonner modulo 9.

• Plus généralement, on peut raisonner modulo p^n pour p premier et $n \geq 1$: si l'équation a une solution pour tout p^n, on dit qu'elle est localement soluble en p. Ceci est équivalent à la solubilité dans le corps $\mathbb{Q}_p$ des nombres p-adiques. On dit bien sûr qu'elle est partout localement soluble (PLS) si elle est localement soluble pour tout p.

Il n'est malheureusement pas vrai qu'une équation PLS est soluble, voir ci-dessous.

Deuxième partie. Méthodes classiques : congruences I

D'innombrables méthodes. Je vais donner des exemples typiques.

• Congruences. Souvent, en regardant une équation modulo n pour un n convenable, on montre qu'elle n'a pas de solution. Exemple : $x^3 + y^3 = 3z^3$, il suffit de raisonner modulo 3, après réduction à x, y, z premiers entre eux. Exemple semblable $x^3 + y^3 = z^3$ avec $3 \nmid xyz$. Ici il suffit de raisonner modulo 9.

• Plus généralement, on peut raisonner modulo p^n pour p premier et $n \geq 1$: si l'équation a une solution pour tout p^n, on dit qu'elle est localement soluble en p. Ceci est équivalent à la solubilité dans le corps $\mathbb{Q}_p$ des nombres p-adiques. On dit bien sûr qu'elle est partout localement soluble (PLS) si elle est localement soluble pour tout p.

Il n'est malheureusement pas vrai qu'une équation PLS est soluble, voir ci-dessous.

Méthodes classiques : congruences II

Exemple 1 :

$$C_c : \qquad x^4 + y^4 = cz^4 ,$$

avec $xyz \neq 0$, où on peut supposer $c > 0$ entier et non divisible par une puissance quatrième autre que 1. On montre assez facilement que C_c est PLS si et seulement si $c \equiv 1$ ou 2 modulo 16, $p \mid c$ premier impair implique $p \equiv 1 \pmod 8$, $c \not\equiv 3, 4 \pmod 5$, $c \not\equiv 7, 8, 11 \pmod{13}$, et $c \not\equiv 4, 5, 6, 9, 13, 22, 28 \pmod{29}$.

Conséquence interessante, notons que l'impossibilité de l'équation de Fermat $x^4 + y^4 = Z^2$ (prouvée par Fermat) entraîne que si p est un nombre premier tel que $p \equiv 1 \pmod{1160}$, l'équation C_{p^2} est PLS mais n'est pas soluble. C'est ce qu'on appelle une violation du principe de Hasse, donc pour une famille infinie puisqu'il existe une infinité de tels p.

Méthodes classiques : congruences II

Exemple 1 :

$$C_c : \qquad x^4 + y^4 = cz^4 \ ,$$

avec $xyz \neq 0$, où on peut supposer $c > 0$ entier et non divisible par une puissance quatrième autre que 1. On montre assez facilement que C_c est PLS si et seulement si $c \equiv 1$ ou 2 modulo 16, $p \mid c$ premier impair implique $p \equiv 1 \pmod 8$, $c \not\equiv 3, 4 \pmod 5$, $c \not\equiv 7, 8, 11 \pmod{13}$, et $c \not\equiv 4, 5, 6, 9, 13, 22, 28 \pmod{29}$.

Conséquence interessante, notons que l'impossibilité de l'équation de Fermat $x^4 + y^4 = Z^2$ (prouvée par Fermat) entraîne que si p est un nombre premier tel que $p \equiv 1 \pmod{1160}$, l'équation C_{p^2} est PLS mais n'est pas soluble. C'est ce qu'on appelle une violation du principe de Hasse, donc pour une famille infinie puisqu'il existe une infinité de tels p.

Méthodes classiques : congruences III

Exemple 2 :

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

(l'équation de Fermat), où on suppose $p \nmid xyz$ (le premier cas). En raisonnant simplement modulo p^2 (comme ci-dessus pour $p = 3$), on montre que l'équation n'a pas de solution si pour tout a tel que $1 \leq a \leq (p-1)/2$ on a

$$(a+1)^p - a^p - 1 \not\equiv 0 \pmod{p^2}\ .$$

Marche pour $p = 3$, 5, 11, 17, 23, etc...

Méthodes classiques : factorisation sur $\mathbb{Z}$

Ici on factorise sur $\mathbb{Z}$ certains polynômes liés à notre équation.
Exemple 1 dû à Fermat :

$$y^2 = x^3 + 7 \; .$$

On écrit

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4) = (x+2)((x-1)^2 + 3) \; .$$

En utilisant simplement des raisonnements modulo 2, 4 et 8, on montre successivement que x est impair, que le membre de droite est divisible par $p \equiv 3 \pmod 4$ à une puissance impaire, ce qui est impossible pour un nombre de la forme $y^2 + 1$.

Exemple 2 : FLT I, où on écrit $x^p + y^p = (x+y)(x^{p-1} - yx^{p-2} + \cdots + y^{p-1})$. On peut démontrer ainsi le théorème de Sophie Germain, si $2p+1$ est premier FLT I n'a pas de solution, et plus généralement le critère de Wendt.

Méthodes classiques : factorisation sur $\mathbb{Z}$

Ici on factorise sur $\mathbb{Z}$ certains polynômes liés à notre équation.
Exemple 1 dû à Fermat :

$$y^2 = x^3 + 7 \ .$$

On écrit

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4) = (x+2)((x-1)^2 + 3) \ .$$

En utilisant simplement des raisonnements modulo 2, 4 et 8, on montre successivement que x est impair, que le membre de droite est divisible par $p \equiv 3 \pmod 4$ à une puissance impaire, ce qui est impossible pour un nombre de la forme $y^2 + 1$.

Exemple 2 : FLT I, où on écrit $x^p + y^p = (x+y)(x^{p-1} - yx^{p-2} + \cdots + y^{p-1})$. On peut démontrer ainsi le théorème de Sophie Germain, si $2p+1$ est premier FLT I n'a pas de solution, et plus généralement le critère de Wendt.

Méthodes classiques : factorisation sur $\mathbb{Z}$

Ici on factorise sur $\mathbb{Z}$ certains polynômes liés à notre équation.
Exemple 1 dû à Fermat :

$$y^2 = x^3 + 7 \, .$$

On écrit

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4) = (x+2)((x-1)^2 + 3) \, .$$

En utilisant simplement des raisonnements modulo 2, 4 et 8, on montre successivement que x est impair, que le membre de droite est divisible par $p \equiv 3 \pmod 4$ à une puissance impaire, ce qui est impossible pour un nombre de la forme $y^2 + 1$.

Exemple 2 : FLT I, où on écrit
$x^p + y^p = (x+y)(x^{p-1} - yx^{p-2} + \cdots + y^{p-1})$. On peut démontrer ainsi le théorème de Sophie Germain, si $2p+1$ est premier FLT I n'a pas de solution, et plus généralement le critère de Wendt.

Méthodes classiques : factorisation sur $\mathbb{Z}_K$ I

Méthode beaucoup plus puissante, essentiellement due à Kummer : factorisation dans les corps de nombres.

Exemple 1 dû à Fermat :

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

Ici on écrit $y^2 + 2 = x^3$, qu'on factorise comme

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3 \; .$$

On travaille dans $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2},\ a, b \in \mathbb{Z}\}$. On a de la chance : c'est un anneau principal, dont les seuls éléments inversibles (appelés unités) sont ± 1. On en déduit que

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 \; ,$$

et de là il est facile d'obtenir une contradiction.

Méthodes classiques : factorisation sur $\mathbb{Z}_K$ II

Exemple 2 dû à Kummer : FLT $x^p + y^p = z^p$, qu'on écrit

$$(x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1}y) = z^p \ ,$$

où ζ_p est une racine primitive p-ième de 1. Ici on travaille dans $\mathbb{Z}[\zeta_p]$, mais beaucoup plus compliqué, même quand $\mathbb{Z}[\zeta_p]$ est principal.

Inutile d'entrer dans les définitions détaillées : trois points importants toutefois :

- C'est agréable quand $\mathbb{Z}_K$ est un anneau principal, puisqu'on peut le traiter (en partie) comme $\mathbb{Z}$. Mais, invention géniale de Kummer, Dirichlet, et Dedekind, même si non principal, toujours factorisation unique en idéaux, donc notion d'idéal. Pour se ramener aux éléments, il faut faire une hypothèse sur la non divisibilité du nombre de classes (inutile de définir) par certains premiers (3 pour l'exemple 1, p pour l'exemple 2).

Méthodes classiques : factorisation sur $\mathbb{Z}_K$ II

Exemple 2 dû à Kummer : FLT $x^p + y^p = z^p$, qu'on écrit

$$(x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1}y) = z^p \;,$$

où ζ_p est une racine primitive p-ième de 1. Ici on travaille dans $\mathbb{Z}[\zeta_p]$, mais beaucoup plus compliqué, même quand $\mathbb{Z}[\zeta_p]$ est principal.

Inutile d'entrer dans les définitions détaillées : trois points importants toutefois :

• C'est agréable quand $\mathbb{Z}_K$ est un anneau principal, puisqu'on peut le traiter (en partie) comme $\mathbb{Z}$. Mais, invention géniale de Kummer, Dirichlet, et Dedekind, même si non principal, toujours factorisation unique en idéaux, donc notion d'idéal. Pour se ramener aux éléments, il faut faire une hypothèse sur la non divisibilité du nombre de classes (inutile de définir) par certains premiers (3 pour l'exemple 1, p pour l'exemple 2).

Méthodes classiques : factorisation sur $\mathbb{Z}_K$ III

• Il est essentiel de s'occuper des unités (éléments inversibles) de $\mathbb{Z}_K$. Quand il y en a une infinité, ça pose problème. Exemples :

$$y^2 = x^p - 2$$

"facile" car on écrit $y^2 + 2 = x^p$ donc

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^p$$

et $\mathbb{Z}[\sqrt{-2}]$ n'a que ± 1 comme unités.

Par contre

$$y^2 = x^p + 2$$

très difficile (et non résolu) car

$$(y + \sqrt{2})(y - \sqrt{2}) = x^p$$

mais $\mathbb{Z}[\sqrt{2}]$, bien que principal, a une infinité d'unités

$$u = \pm(1 + \sqrt{2})^k$$

pour tout $k \in \mathbb{Z}$.

Méthodes classiques : factorisation sur $\mathbb{Z}_K$ III

• Il est essentiel de s'occuper des unités (éléments inversibles) de $\mathbb{Z}_K$. Quand il y en a une infinité, ça pose problème. Exemples :

$$y^2 = x^p - 2$$

"facile" car on écrit $y^2 + 2 = x^p$ donc

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^p$$

et $\mathbb{Z}[\sqrt{-2}]$ n'a que ± 1 comme unités.

Par contre

$$y^2 = x^p + 2$$

très difficile (et non résolu) car

$$(y + \sqrt{2})(y - \sqrt{2}) = x^p$$

mais $\mathbb{Z}[\sqrt{2}]$, bien que principal, a une infinité d'unités

$$u = \pm(1 + \sqrt{2})^k$$

pour tout $k \in \mathbb{Z}$.

Méthodes classiques : factorisation sur $\mathbb{Z}_K$ IV

• Dans le cas de FLT, il y a bien une infinité d'unités u dans $\mathbb{Z}[\zeta]$ (pour $p \geq 5$). On se sort de ce problème grâce à un résultat (facile) affirmant que $\overline{u}/u = \zeta_p^r$, donc ne peut prendre qu'un nombre fini de valeurs.

Méthodes classiques : courbes elliptiques I

J'introduirai ci-dessous les courbes elliptiques (CE). Quatre utilisations (au moins) dans le domaine des équations diophantiennes :

- Utilisation “classique”, ayant son origine chez Fermat.

- Utilisation “moderne” grâce aux méthodes modulaires de Ribet–Wiles.

- Première utilisation “magique” utilisant la conjecture de Birch–Swinnerton-Dyer (BSD).

- Deuxième utilisation “magique” utilisant les points de Heegner.

Méthodes classiques : courbes elliptiques I

J'introduirai ci-dessous les courbes elliptiques (CE). Quatre utilisations (au moins) dans le domaine des équations diophantiennes :

- Utilisation "classique", ayant son origine chez Fermat.

- Utilisation "moderne" grâce aux méthodes modulaires de Ribet–Wiles.

- Première utilisation "magique" utilisant la conjecture de Birch–Swinnerton-Dyer (BSD).

- Deuxième utilisation "magique" utilisant les points de Heegner.

Méthodes classiques : courbes elliptiques I

J'introduirai ci-dessous les courbes elliptiques (CE). Quatre utilisations (au moins) dans le domaine des équations diophantiennes :

- Utilisation "classique", ayant son origine chez Fermat.

- Utilisation "moderne" grâce aux méthodes modulaires de Ribet–Wiles.

- Première utilisation "magique" utilisant la conjecture de Birch–Swinnerton-Dyer (BSD).

- Deuxième utilisation "magique" utilisant les points de Heegner.

Méthodes classiques : courbes elliptiques I

J’introduirai ci-dessous les courbes elliptiques (CE). Quatre utilisations (au moins) dans le domaine des équations diophantiennes :

• Utilisation “classique”, ayant son origine chez Fermat.

• Utilisation “moderne” grâce aux méthodes modulaires de Ribet–Wiles.

• Première utilisation “magique” utilisant la conjecture de Birch–Swinnerton-Dyer (BSD).

• Deuxième utilisation “magique” utilisant les points de Heegner.

Méthodes classiques : courbes elliptiques II

Pour faire bref, une courbe elliptique est une cubique projective plane non singulière ayant au moins un point rationnel (la définition est plus générale).

Ce qui est remarquable c'est qu'on peut munir cette courbe (avec son point à l'infini) d'une loi de groupe abélien naturelle : si P_1 et P_2 sont deux points sur la courbe, on trace la droite D passant par ces deux points (la tangente si $P_1 = P_2$), qui coupe la courbe en un troisième point Q, et on définit $P_1 + P_2$ comme le symétrique de Q par rapport à l'axe des x.

Méthodes classiques : courbes elliptiques III

A partir d'un point, on peut souvent ainsi construire une infinité de points sur la courbe, qui seront tous à coordonnées rationnelles si la courbe et le point initial le sont.
Exemple positif dû à Fermat : trouver x, y, z entiers positifs tels que

$$x^3 + y^3 = 9z^3 \ ,$$

autres que les points évidents provenant de $1^3 + 2^3 = 9$.

Plus petite solution ($6(1, 2)$) a 12 chiffres :

$$(x, y, z) = (676702467503, 415280564497, 348671682660) \ .$$

Méthodes classiques : courbes elliptiques III

A partir d'un point, on peut souvent ainsi construire une infinité de points sur la courbe, qui seront tous à coordonnées rationnelles si la courbe et le point initial le sont.
Exemple positif dû à Fermat : trouver x, y, z entiers positifs tels que

$$x^3 + y^3 = 9z^3 \ ,$$

autres que les points évidents provenant de $1^3 + 2^3 = 9$.

Plus petite solution ($6(1, 2)$) a 12 chiffres :

$$(x, y, z) = (676702467503, 415280564497, 348671682660) \ .$$

Méthodes classiques : courbes elliptiques IV

L'utilisation classique, essentiellement due à Fermat, est la méthode de descente. S'utilise principalement pour montrer qu'une équation n'a pas de solution.
L'idée naïve, pas toujours évidente à mettre en œuvre, est la suivante : on part d'une solution (x, y, z) à une équation diophantienne homogène de degré 3 ou 4 (en fait une courbe elliptique), où on suppose $m = \max(|x|, |y|, |z|)$ minimal et non nul, et on construit de manière plus ou moins astucieuse une nouvelle solution (x', y', z') avec $\max(|x'|, |y'|, |z'|) < m$ et non nul, contradiction. Il faut souvent modifier l'équation de départ, ce n'est pas toujours facile.

Idée plus moderne et qui marche plus souvent : d'après un théorème de Mordell, généralisé par Weil, le groupe $E(\mathbb{Q})$ des points rationnels d'une courbe elliptique est de type fini (groupe abélien fini somme directe avec $\mathbb{Z}^r$). Les méthodes modernes de descente (2-descente, 3-descente, n-descente) permettent presque toujours de déterminer $E(\mathbb{Q})$, donc de résoudre l'équation.

Méthodes classiques : courbes elliptiques IV

L'utilisation classique, essentiellement due à Fermat, est la méthode de descente. S'utilise principalement pour montrer qu'une équation n'a pas de solution.
L'idée naïve, pas toujours évidente à mettre en œuvre, est la suivante : on part d'une solution (x, y, z) à une équation diophantienne homogène de degré 3 ou 4 (en fait une courbe elliptique), où on suppose $m = \max(|x|, |y|, |z|)$ minimal et non nul, et on construit de manière plus ou moins astucieuse une nouvelle solution (x', y', z') avec $\max(|x'|, |y'|, |z'|) < m$ et non nul, contradiction. Il faut souvent modifier l'équation de départ, ce n'est pas toujours facile.

Idée plus moderne et qui marche plus souvent : d'après un théorème de Mordell, généralisé par Weil, le groupe $E(\mathbb{Q})$ des points rationnels d'une courbe elliptique est de type fini (groupe abélien fini somme directe avec $\mathbb{Z}^r$). Les méthodes modernes de descente (2-descente, 3-descente, n-descente) permettent presque toujours de déterminer $E(\mathbb{Q})$, donc de résoudre l'équation.

Méthodes magiques : utilisation de BSD I

J'en viens maintenant à deux méthodes “magiques” utilisant les courbes elliptiques. Considérons les trois équations suivantes (toutes des courbes elliptiques) :

$$y^2 = x^3 - 157^2 x\ , \quad y^2 = x^3 + 877x\ , \quad y^2 + y = x^3 - 3279211\ .$$

Dans les trois cas, la recherche de points rationnels est infructueuse, et les méthodes de descente (2-descente ou 3-descente) ne marchent pas.

La conjecture BSD permet de répondre rapidement au moins à la question de l'existence ou non d'une solution (et donc d'une infinité de solutions d'après le théorème de Mordell).

On associe à toute courbe elliptique rationnelle E une fonction de variable complexe $L(E, s)$, à priori définie pour $\Re(s) > 3/2$ mais qui d'après Wiles et al. peut se prolonger analytiquement à $\mathbb{C}$.

Méthodes magiques : utilisation de BSD I

J'en viens maintenant à deux méthodes “magiques” utilisant les courbes elliptiques. Considérons les trois équations suivantes (toutes des courbes elliptiques) :

$$y^2 = x^3 - 157^2 x \ , \quad y^2 = x^3 + 877x \ , \quad y^2 + y = x^3 - 3279211 \ .$$

Dans les trois cas, la recherche de points rationnels est infructueuse, et les méthodes de descente (2-descente ou 3-descente) ne marchent pas.

La conjecture BSD permet de répondre rapidement au moins à la question de l'existence ou non d'une solution (et donc d'une infinité de solutions d'après le théorème de Mordell).

On associe à toute courbe elliptique rationnelle E une fonction de variable complexe $L(E, s)$, à priori définie pour $\Re(s) > 3/2$ mais qui d'après Wiles et al. peut se prolonger analytiquement à $\mathbb{C}$.

Méthodes magiques : utilisation de BSD I

J'en viens maintenant à deux méthodes "magiques" utilisant les courbes elliptiques. Considérons les trois équations suivantes (toutes des courbes elliptiques) :

$$y^2 = x^3 - 157^2 x \;, \quad y^2 = x^3 + 877x \;, \quad y^2 + y = x^3 - 3279211 \;.$$

Dans les trois cas, la recherche de points rationnels est infructueuse, et les méthodes de descente (2-descente ou 3-descente) ne marchent pas.

La conjecture BSD permet de répondre rapidement au moins à la question de l'existence ou non d'une solution (et donc d'une infinité de solutions d'après le théorème de Mordell).

On associe à toute courbe elliptique rationnelle E une fonction de variable complexe $L(E,s)$, à priori définie pour $\Re(s) > 3/2$ mais qui d'après Wiles et al. peut se prolonger analytiquement à $\mathbb{C}$.

Méthodes magiques : utilisation de BSD II

Cette fonction est très rapide à calculer sur ordinateur. Une forme faible de BSD affirme que E a une infinité de points rationnels si et seulement si $L(E,1)=0$.

D'où la méthode évidente suivante : on calcule $L(E,1)$ a 15 décimales. Si $L(E,1)$ est loin de 0, inutile de continuer l'équation n'a qu'un nombre fini de solutions, qu'il est facile de trouver (c'est ce qu'on appelle les points de torsion).

Si par contre

$$L(E,1)=0.000000000000000$$

semble être nul, on n'a rien prouvé, mais il est moralement certain que l'équation a une infinité de solutions.

Toutefois, aucune indication sur ces solutions.

Méthodes magiques : utilisation de BSD II

Cette fonction est très rapide à calculer sur ordinateur. Une forme faible de BSD affirme que E a une infinité de points rationnels si et seulement si $L(E,1) = 0$.

D'où la méthode évidente suivante : on calcule $L(E,1)$ a 15 décimales. Si $L(E,1)$ est loin de 0, inutile de continuer l'équation n'a qu'un nombre fini de solutions, qu'il est facile de trouver (c'est ce qu'on appelle les points de torsion).

Si par contre

$$L(E,1) = 0.000000000000000$$

semble être nul, on n'a rien prouvé, mais il est moralement certain que l'équation a une infinité de solutions.

Toutefois, aucune indication sur ces solutions.

Méthodes magiques : utilisation de BSD II

Cette fonction est très rapide à calculer sur ordinateur. Une forme faible de BSD affirme que E a une infinité de points rationnels si et seulement si $L(E,1)=0$.

D'où la méthode évidente suivante : on calcule $L(E,1)$ a 15 décimales. Si $L(E,1)$ est loin de 0, inutile de continuer l'équation n'a qu'un nombre fini de solutions, qu'il est facile de trouver (c'est ce qu'on appelle les points de torsion).

Si par contre

$$L(E,1)=0.000000000000000$$

semble être nul, on n'a rien prouvé, mais il est moralement certain que l'équation a une infinité de solutions.

Toutefois, aucune indication sur ces solutions.

La conjecture BSD I

Quelques mots sur la conjecture elle-même : tout d'abord, à mon avis, la conjecture BSD est la conjecture la plus fascinante de toute la théorie des nombres, en particulier à cause du fait qu'en rang $r \geq 2$ (voir ci-dessous) on n'a aucune idée de comment aborder le problème, et du fait qu'elle est très concrète.

Exemple : pour tout p premier, on définit $a(p) = p - N(p)$, où $N(p)$ est le nombre de couples (x, y) modulo p vérifiant

$$y^2 + xy \equiv x^3 - x^2 - 79x + 289 \pmod{p} .$$

On définit $\chi(p) = 0$ si $p = 2$ ou $p = 117223$ (discriminant ci-dessus), $\chi(p) = 1$ sinon, puis par récurrence

$$a(p^k) = a(p)a(p^{k-1}) - \chi(p)pa(p^{k-2}) ,$$

et enfin $a(n)$ pour tout n par multiplicativité.

La conjecture BSD I

Quelques mots sur la conjecture elle-même : tout d'abord, à mon avis, la conjecture BSD est la conjecture la plus fascinante de toute la théorie des nombres, en particulier à cause du fait qu'en rang $r \geq 2$ (voir ci-dessous) on n'a aucune idée de comment aborder le problème, et du fait qu'elle est très concrète.

Exemple : pour tout p premier, on définit $a(p) = p - N(p)$, où $N(p)$ est le nombre de couples (x, y) modulo p vérifiant

$$y^2 + xy \equiv x^3 - x^2 - 79x + 289 \pmod{p} .$$

On définit $\chi(p) = 0$ si $p = 2$ ou $p = 117223$ (discriminant ci-dessus), $\chi(p) = 1$ sinon, puis par récurrence

$$a(p^k) = a(p)a(p^{k-1}) - \chi(p)pa(p^{k-2}) ,$$

et enfin $a(n)$ pour tout n par multiplicativité.

La conjecture BSD II

En quelques secondes on calcule 1 million de valeurs de $a(n)$, par exemple pour $n = 1, 2, \ldots$ on a

$$a(n) = 1, -1, -3, 1, -4, 3, -5, -1, 6, 4, -6, -3, -6, 5, 12, \ldots$$

D'autre part, pour $x > 0$ on pose

$$f(x) = \int_1^\infty e^{-xt} \log(t)^2 \, dt \,,$$

et enfin

$$S = \sum_{n=1}^{\infty} a(n) f\left(\frac{2\pi n}{\sqrt{234446}}\right) \,,$$

qui converge exponentiellement vite ($f(x) \sim 2e^{-x}/x^3$).

En quelques secondes, on trouve

$$S = 0.0000000000000000000000000000000000000000000 \cdots$$

à des milliers de décimales : même pour cet exemple précis, c'est conjectural !

La conjecture BSD II

En quelques secondes on calcule 1 million de valeurs de $a(n)$, par exemple pour $n = 1, 2, \ldots$ on a

$$a(n) = 1, -1, -3, 1, -4, 3, -5, -1, 6, 4, -6, -3, -6, 5, 12, \ldots$$

D'autre part, pour $x > 0$ on pose

$$f(x) = \int_1^\infty e^{-xt} \log(t)^2 \, dt \ ,$$

et enfin

$$S = \sum_{n=1}^{\infty} a(n) f\left(\frac{2\pi n}{\sqrt{234446}}\right) \ ,$$

qui converge exponentiellement vite ($f(x) \sim 2e^{-x}/x^3$).

En quelques secondes, on trouve

$$S = 0.000000000000000000000000000000000000000000000000\cdots$$

à des milliers de décimales : même pour cet exemple précis, c'est conjectural !

La conjecture BSD II

En quelques secondes on calcule 1 million de valeurs de $a(n)$, par exemple pour $n = 1, 2, \ldots$ on a

$$a(n) = 1, -1, -3, 1, -4, 3, -5, -1, 6, 4, -6, -3, -6, 5, 12, \ldots$$

D'autre part, pour $x > 0$ on pose

$$f(x) = \int_1^\infty e^{-xt} \log(t)^2 \, dt \ ,$$

et enfin

$$S = \sum_{n=1}^{\infty} a(n) f\left(\frac{2\pi n}{\sqrt{234446}}\right) \ ,$$

qui converge exponentiellement vite ($f(x) \sim 2e^{-x}/x^3$).

En quelques secondes, on trouve

$$S = 0.0000000000000000000000000000000000000000000 \cdots$$

à des milliers de décimales : même pour cet exemple précis, c'est conjectural !

Méthodes magiques : points de Heegner I

D'après Mordell, le groupe des points rationnels $E(\mathbb{Q})$ est isomorphe a la somme directe d'un groupe abélien fini (facile à déterminer) et de $\mathbb{Z}^r$, où r s'appelle le rang. Si $r = 0$, rien à faire. Heuristique très plausibles : asymptotiquement 50% de courbes de rang 0, 50% de courbes de rang 1. On se concentre donc sur les courbes de rang 1 :

- La méthode magique BSD permet de séparer rang 0 et rang 1.
- La méthode magique des points de Heegner permet de construire analytiquement et bien sûr explicitement un point rationnel non trivial quand le rang est 1.

Dans les trois exemples ci-dessus, cette méthode permet de trouver une solution explicite, bien que la plus petite ait 60 chiffres décimaux.

Méthodes magiques : points de Heegner I

D'après Mordell, le groupe des points rationnels $E(\mathbb{Q})$ est isomorphe a la somme directe d'un groupe abélien fini (facile à déterminer) et de $\mathbb{Z}^r$, où r s'appelle le rang. Si $r = 0$, rien à faire. Heuristique très plausibles : asymptotiquement 50% de courbes de rang 0, 50% de courbes de rang 1. On se concentre donc sur les courbes de rang 1 :

- La méthode magique BSD permet de séparer rang 0 et rang 1.

- La méthode magique des points de Heegner permet de construire analytiquement et bien sûr explicitement un point rationnel non trivial quand le rang est 1.

Dans les trois exemples ci-dessus, cette méthode permet de trouver une solution explicite, bien que la plus petite ait 60 chiffres décimaux.

Méthodes magiques : points de Heegner I

D'après Mordell, le groupe des points rationnels $E(\mathbb{Q})$ est isomorphe a la somme directe d'un groupe abélien fini (facile à déterminer) et de $\mathbb{Z}^r$, où r s'appelle le rang. Si $r = 0$, rien à faire. Heuristique très plausibles : asymptotiquement 50% de courbes de rang 0, 50% de courbes de rang 1. On se concentre donc sur les courbes de rang 1 :

• La méthode magique BSD permet de séparer rang 0 et rang 1.

• La méthode magique des points de Heegner permet de construire analytiquement et bien sûr explicitement un point rationnel non trivial quand le rang est 1.
Dans les trois exemples ci-dessus, cette méthode permet de trouver une solution explicite, bien que la plus petite ait 60 chiffres décimaux.

Méthodes magiques : points de Heegner II

Pour illustrer l'incroyable simplicité et efficacité de la méthode, je donne le code GP pour $y^2 = x^3 - 157^2 x$. Le tout prend moins de 30 secondes de temps CPU (on peut faire mieux).

```
allocatemem(2*10^8); default(realprecision,70);
e=ellinit([0,0,0,-157^2,0]); ered=ellglobalred(e);
om1=e.omega[1]; om2=e.omega[2]; om=2*om1;
N=ered[1]; c=ered[3]; vole=e.area;
D=-39; b=lift(sqrt(Mod(D,4*N)));
v=ellan(e,10^7);
ph(tau)=local(s,q,q1);s=0.;q=exp(2*I*Pi*tau);q1=1;\
 for(n=1,10^7,q1*=q;s+=v[n]/n*q1);return(s);
z1=ph((-b+I*sqrt(39))/(2*N));
z2=ph((-b+I*sqrt(39))/(4*N));
z=2*real(z1+z2)+27*om1;
x1=ellwp(e,(2*z+2*om1)/8);
rx=contfrac(real(x1));
mx=contfracpnqn(vector(39,i,rx[i]));
x=mx[1,1]/mx[2,1];
y=ellordinate(e,x)[1];
```

Courbes de genre supérieur I

Sans vouloir définir le genre, les coniques sont de genre 0, les courbes elliptiques de genre 1, les courbes d'équation

$$y^2 = P(x)$$

avec P polynôme sans racines multiples de degré d sont de genre $\lfloor (d-1)/2 \rfloor$, les quartiques planes non singulières sont de genre 3, etc...

Vu ci-dessus genre 0 (facile) et 1 (gouverné par Mordell et BSD).

Le genre $g \geq 2$ est de nature différente : conjecture de Mordell démontrée par Faltings (très difficile) : il n'y a qu'un nombre fini de points rationnels sur une courbe de genre $g \geq 2$ définie sur $\mathbb{Q}$.

Malheureusement non effectif : ne donne aucune indication ni sur le nombre ni sur la taille des solutions.

Courbes de genre supérieur I

Sans vouloir définir le genre, les coniques sont de genre 0, les courbes elliptiques de genre 1, les courbes d'équation

$$y^2 = P(x)$$

avec P polynôme sans racines multiples de degré d sont de genre $\lfloor (d-1)/2 \rfloor$, les quartiques planes non singulières sont de genre 3, etc...

Vu ci-dessus genre 0 (facile) et 1 (gouverné par Mordell et BSD).

Le genre $g \geq 2$ est de nature différente : conjecture de Mordell démontrée par Faltings (très difficile) : il n'y a qu'un nombre fini de points rationnels sur une courbe de genre $g \geq 2$ définie sur $\mathbb{Q}$.

Malheureusement non effectif : ne donne aucune indication ni sur le nombre ni sur la taille des solutions.

Courbes de genre supérieur I

Sans vouloir définir le genre, les coniques sont de genre 0, les courbes elliptiques de genre 1, les courbes d'équation

$$y^2 = P(x)$$

avec P polynôme sans racines multiples de degré d sont de genre $\lfloor (d-1)/2 \rfloor$, les quartiques planes non singulières sont de genre 3, etc...

Vu ci-dessus genre 0 (facile) et 1 (gouverné par Mordell et BSD).

Le genre $g \geq 2$ est de nature différente : conjecture de Mordell démontrée par Faltings (très difficile) : il n'y a qu'un nombre fini de points rationnels sur une courbe de genre $g \geq 2$ définie sur $\mathbb{Q}$.

Malheureusement non effectif : ne donne aucune indication ni sur le nombre ni sur la taille des solutions.

Courbes de genre supérieur I

Sans vouloir définir le genre, les coniques sont de genre 0, les courbes elliptiques de genre 1, les courbes d'équation

$$y^2 = P(x)$$

avec P polynôme sans racines multiples de degré d sont de genre $\lfloor (d-1)/2 \rfloor$, les quartiques planes non singulières sont de genre 3, etc...

Vu ci-dessus genre 0 (facile) et 1 (gouverné par Mordell et BSD).

Le genre $g \geq 2$ est de nature différente : conjecture de Mordell démontrée par Faltings (très difficile) : il n'y a qu'un nombre fini de points rationnels sur une courbe de genre $g \geq 2$ définie sur $\mathbb{Q}$.

Malheureusement non effectif : ne donne aucune indication ni sur le nombre ni sur la taille des solutions.

Courbes de genre supérieur II

Toutefois, bien avant Faltings, Chabauty a inventé une méthode de résolution effective, mais qui ne marche que dans certains cas. Méthode généralisée et améliorée par Coleman, et plus récemment méthode de Chabauty elliptique.

Idée : une courbe C de genre $g \geq 2$ n'est pas naturellement un groupe. Mais sa Jacobienne (définition pas difficile) J est une variété de dimension g dont l'ensemble $J(\mathbb{Q})$ des points rationnels est un groupe abélien de type fini qu'on peut habituellement calculer explicitement comme pour les courbes elliptiques par des méthodes de descente. Appelons r son rang, $r = \dim_{\mathbb{Q}}(J(\mathbb{Q}) \otimes \mathbb{Q})$.

Courbes de genre supérieur II

Toutefois, bien avant Faltings, Chabauty a inventé une méthode de résolution effective, mais qui ne marche que dans certains cas. Méthode généralisée et améliorée par Coleman, et plus récemment méthode de Chabauty elliptique.

Idée : une courbe C de genre $g \geq 2$ n'est pas naturellement un groupe. Mais sa Jacobienne (définition pas difficile) J est une variété de dimension g dont l'ensemble $J(\mathbb{Q})$ des points rationnels est un groupe abélien de type fini qu'on peut habituellement calculer explicitement comme pour les courbes elliptiques par des méthodes de descente. Appelons r son rang, $r = \dim_{\mathbb{Q}}(J(\mathbb{Q}) \otimes \mathbb{Q})$.

Courbes de genre supérieur III

La courbe C peut être plongée dans sa jacobienne, et en identifiant avec son image on a donc

$$C(\mathbb{Q}) = J(\mathbb{Q}) \cap C \ .$$

Inclus dans l'intersection d'un sous-espace de dimension r et d'une courbe (donc de dimension 1) dans un espace de dimension $g = \dim(J)$: nombre fini de points en général, explicites, si $r + 1 \leq g$, c'est à dire

$$r \leq g - 1 \ :$$

C'est la condition de succès de la méthode de Chabauty.

Par exemple, pour les courbes de genre $g = 2$, il faut que $J(\mathbb{Q})$ soit de rang 0 ou 1.

Courbes de genre supérieur III

La courbe C peut être plongée dans sa jacobienne, et en identifiant avec son image on a donc

$$C(\mathbb{Q}) = J(\mathbb{Q}) \cap C \,.$$

Inclus dans l'intersection d'un sous-espace de dimension r et d'une courbe (donc de dimension 1) dans un espace de dimension $g = \dim(J)$: nombre fini de points en général, explicites, si $r + 1 \leq g$, c'est à dire

$$r \leq g - 1 \ :$$

C'est la condition de succès de la méthode de Chabauty.

Par exemple, pour les courbes de genre $g = 2$, il faut que $J(\mathbb{Q})$ soit de rang 0 ou 1.