L'équation de Bachet

Daniel PERRIN

Marne-la-Vallée, 15 janvier 2019

Pour des précisions sur ce sujet, voir, sur ma page web, à la rubrique *Conférences* :

https ://www.math.u-psud.fr/ perrin/Conferences/Bachet.pdf

https ://www.math.u-psud.fr/ perrin/Conferences/OlympiadeDP.pdf

Carrés et cubes d'entiers

- Voici la liste des premiers carrés d'entiers :

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169,$$

$$196, 225, 256, 289, 324, 361, 400, ...$$

Carrés et cubes d'entiers

- Voici la liste des premiers carrés d'entiers :

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169,$$

$$196, 225, 256, 289, 324, 361, 400, ...$$

- et celle des premiers cubes :

$$1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331,$$

$$1728, 2197, 2744, 3375, 4096, ...$$

Carrés et cubes d'entiers

- Voici la liste des premiers carrés d'entiers :

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169,$$

$$196, 225, 256, 289, 324, 361, 400, ...$$

- et celle des premiers cubes :

$$1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331,$$

$$1728, 2197, 2744, 3375, 4096, ...$$

- La question (ancienne et encore largement ouverte) est de trouver un cube x^3 et un carré y^2 qui diffèrent d'un entier d **donné** : $x^3 - y^2 = d$. Exemple : $d = 2$?

Bachet

- L'équation $x^3 = y^2 + d$ a été étudiée pour la première fois en 1621, dans le cas $d = 2$, par Bachet qui, à partir de la solution évidente $x = 3, y = 5$, a donné une méthode pour construire d'autres solutions **rationnelles**.

Bachet

- L'équation $x^3 = y^2 + d$ a été étudiée pour la première fois en 1621, dans le cas $d = 2$, par Bachet qui, à partir de la solution évidente $x = 3, y = 5$, a donné une méthode pour construire d'autres solutions **rationnelles**.
- La méthode algébrique : $x^3 = y^2 + d$, (a, b) solution, on cherche une solution $x = a + h$, $y = b + k$.

Bachet

- L'équation $x^3 = y^2 + d$ a été étudiée pour la première fois en 1621, dans le cas $d = 2$, par Bachet qui, à partir de la solution évidente $x = 3, y = 5$, a donné une méthode pour construire d'autres solutions **rationnelles**.
- La méthode algébrique : $x^3 = y^2 + d$, (a, b) solution, on cherche une solution $x = a + h$, $y = b + k$.
- $$x = \frac{9a^4 - 8ab^2}{4b^2} \quad y = \frac{8b^4 + 27a^6 - 36a^3b^2}{8b^3}.$$

  Exemple pour Bachet $\frac{129}{100}$, $\frac{383}{1000}$.

Bachet

- L'équation $x^3 = y^2 + d$ a été étudiée pour la première fois en 1621, dans le cas $d = 2$, par Bachet qui, à partir de la solution évidente $x = 3, y = 5$, a donné une méthode pour construire d'autres solutions **rationnelles**.
- La méthode algébrique : $x^3 = y^2 + d$, (a, b) solution, on cherche une solution $x = a + h$, $y = b + k$.
- $$x = \frac{9a^4 - 8ab^2}{4b^2} \quad y = \frac{8b^4 + 27a^6 - 36a^3b^2}{8b^3}.$$
  Exemple pour Bachet $\frac{129}{100}$, $\frac{383}{1000}$.
- La courbe* et l'explication géométrique.

Bachet

- L'équation $x^3 = y^2 + d$ a été étudiée pour la première fois en 1621, dans le cas $d = 2$, par Bachet qui, à partir de la solution évidente $x = 3, y = 5$, a donné une méthode pour construire d'autres solutions **rationnelles**.
- La méthode algébrique : $x^3 = y^2 + d$, (a, b) solution, on cherche une solution $x = a + h$, $y = b + k$.
- $$x = \frac{9a^4 - 8ab^2}{4b^2} \quad y = \frac{8b^4 + 27a^6 - 36a^3b^2}{8b^3}.$$
  Exemple pour Bachet $\frac{129}{100}$, $\frac{383}{1000}$.
- La courbe* et l'explication géométrique.
- Un mot sur les courbes elliptiques.

Fermat et les entiers, $d = 2$

Peut-on trouver en nombres entiers un carré autre que 25 qui, augmenté de 2, fasse un cube ? À la première vue cela paraît d'une recherche difficile ; en fractions une infinité de nombres se déduisent de la méthode de Bachet ; mais la doctrine des nombres entiers, qui est assurément très belle et très subtile, n'a été cultivée ni par Bachet, ni par aucun autre dans les écrits venus jusqu'à moi.

Fermat et les entiers, $d = 4$

- *Je lui avais écrit* (à Frénicle) *qu'il n'y a qu'un nombre carré entier qui, joint au binaire, fasse un cube, et que ledit carré est 25, auquel, si vous ajoutez 2, il se fait 27, qui est un cube. Il a peine à croire cette proposition négative, et la trouve trop hardie et trop générale. Mais, pour augmenter son étonnement, je dis que, si l'on cherche un carré qui, ajouté à 4 fasse un cube, il ne s'en trouvera jamais que deux en nombres entiers, ...*

Fermat et les entiers, $d = 4$

- *Je lui avais écrit* (à Frénicle) *qu'il n'y a qu'un nombre carré entier qui, joint au binaire, fasse un cube, et que ledit carré est 25, auquel, si vous ajoutez 2, il se fait 27, qui est un cube. Il a peine à croire cette proposition négative, et la trouve trop hardie et trop générale. Mais, pour augmenter son étonnement, je dis que, si l'on cherche un carré qui, ajouté à 4 fasse un cube, il ne s'en trouvera jamais que deux en nombres entiers, ...*
- *... savoir 4 et 121, car 4 ajouté à 4 fait 8 qui est un cube et 121 ajouté à 4 fait 125 qui est aussi un cube ; mais, après cela, toute l'infinité des nombres n'en saurait fournir un troisième qui ait la propriété.* (lettre à Digby, 1657)

Comment aborder le problème ?

Arithmétique et factorisation

- Les équations en arithmétique (ou diophantiennes) : autant d'équations que d'inconnues ?

Arithmétique et factorisation

- Les équations en arithmétique (ou diophantiennes) : autant d'équations que d'inconnues ?
- Exemple 1 : $x + y = a$, a entier donné, par exemple $a = 105$.

Arithmétique et factorisation

- Les équations en arithmétique (ou diophantiennes) : autant d'équations que d'inconnues ?
- Exemple 1 : $x + y = a$, a entier donné, par exemple $a = 105$.
- Exemple 2 : $xy = a$, exemple $a = 105$.

Arithmétique et factorisation

- Les équations en arithmétique (ou diophantiennes) : autant d'équations que d'inconnues ?
- Exemple 1 : $x + y = a$, a entier donné, par exemple $a = 105$.
- Exemple 2 : $xy = a$, exemple $a = 105$.
- On voit ici deux choses : l'intérêt d'écrire les expressions sous formes de produits et l'importance de la décomposition (unique) en produit de facteurs premiers.

Arithmétique et factorisation

- Les équations en arithmétique (ou diophantiennes) : autant d'équations que d'inconnues ?
- Exemple 1 : $x + y = a$, a entier donné, par exemple $a = 105$.
- Exemple 2 : $xy = a$, exemple $a = 105$.
- On voit ici deux choses : l'intérêt d'écrire les expressions sous formes de produits et l'importance de la décomposition (unique) en produit de facteurs premiers.
- Un exemple facile : l'équation $x^2 = y^2 + d$.

Arithmétique et factorisation

- Les équations en arithmétique (ou diophantiennes) : autant d'équations que d'inconnues ?
- Exemple 1 : $x + y = a$, a entier donné, par exemple $a = 105$.
- Exemple 2 : $xy = a$, exemple $a = 105$.
- On voit ici deux choses : l'intérêt d'écrire les expressions sous formes de produits et l'importance de la décomposition (unique) en produit de facteurs premiers.
- Un exemple facile : l'équation $x^2 = y^2 + d$.
- Exemples : $d = 3, 2, 105$. La décomposition toujours.

Un exemple facile pour Bachet ?

- On regarde $x^3 = y^2 + d$ avec $d = -1$ (voire $d = -k^2$). On a :

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

Un exemple facile pour Bachet ?

- On regarde $x^3 = y^2 + d$ avec $d = -1$ (voire $d = -k^2$). On a :

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

- Un lemme important :
  Soient x, a, b des entiers > 0. On suppose qu'on a $x^3 = ab$ et que a et b sont premiers entre eux. Alors a et b sont des cubes (d'entiers).

Un exemple facile pour Bachet ?

- On regarde $x^3 = y^2 + d$ avec $d = -1$ (voire $d = -k^2$). On a :

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

- Un lemme important :
  Soient x, a, b des entiers > 0. On suppose qu'on a $x^3 = ab$ et que a et b sont premiers entre eux. Alors a et b sont des cubes (d'entiers).
- Conclure ? Oui pour y pair, pas si simple si y est impair ...

Revenons au cas de Bachet avec $d > 0$

- On a $x^3 = y^2 + d$. Si d est un entier positif, on ne peut pas factoriser $y^2 + d$ dans les entiers mais l'idée géniale (Euler, Lagrange, Gauss, Kümmer, ...) c'est qu'on peut le faire **dans les complexes** :

$$y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}).$$

Revenons au cas de Bachet avec $d > 0$

- On a $x^3 = y^2 + d$. Si d est un entier positif, on ne peut pas factoriser $y^2 + d$ dans les entiers mais l'idée géniale (Euler, Lagrange, Gauss, Kümmer, ...) c'est qu'on peut le faire **dans les complexes** :

$$y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}).$$

- Attention, pour faire de la divisibilité, il faut rester dans un anneau. Ici, l'anneau naturel est :

$$\mathbf{Z}[i\sqrt{d}] = \{a + bi\sqrt{d} \mid a, b \in \mathbf{Z}\}$$

Revenons au cas de Bachet avec $d > 0$

- On a $x^3 = y^2 + d$. Si d est un entier positif, on ne peut pas factoriser $y^2 + d$ dans les entiers mais l'idée géniale (Euler, Lagrange, Gauss, Kümmer, ...) c'est qu'on peut le faire **dans les complexes** :

$$y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}).$$

- Attention, pour faire de la divisibilité, il faut rester dans un anneau. Ici, l'anneau naturel est :

$$\mathbf{Z}[i\sqrt{d}] = \{a + bi\sqrt{d} \mid a, b \in \mathbf{Z}\}$$

- Comme les anciens, faisons comme si l'arithmétique fonctionnait dans ce cadre comme dans les entiers, on discutera ensuite ...

Calculons sans crainte

- On a $x^3 = y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}) = z\overline{z}$.

Calculons sans crainte

- On a $x^3 = y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}) = z\overline{z}$.
- Le lemme vu ci-dessus montre que, si l'on a encore la factorisation unique dans $\mathbf{Z}[i\sqrt{d}]$ et si z et $\overline{z}$ sont premiers entre eux, ce sont des cubes dans $\mathbf{Z}[i\sqrt{d}]$.

Calculons sans crainte

- On a $x^3 = y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}) = z\overline{z}$.
- Le lemme vu ci-dessus montre que, si l'on a encore la factorisation unique dans $\mathbf{Z}[i\sqrt{d}]$ et si z et $\overline{z}$ sont premiers entre eux, ce sont des cubes dans $\mathbf{Z}[i\sqrt{d}]$.
- On a alors :
  $y + i\sqrt{d} = (a + ib\sqrt{d})^3 = a^3 + 3a^2bi\sqrt{d} - 3ab^2d - ib^3d\sqrt{d}$.

Calculons sans crainte

- On a $x^3 = y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}) = z\overline{z}$.
- Le lemme vu ci-dessus montre que, si l'on a encore la factorisation unique dans $\mathbf{Z}[i\sqrt{d}]$ et si z et $\overline{z}$ sont premiers entre eux, ce sont des cubes dans $\mathbf{Z}[i\sqrt{d}]$.
- On a alors :
  $y + i\sqrt{d} = (a + ib\sqrt{d})^3 = a^3 + 3a^2bi\sqrt{d} - 3ab^2d - ib^3d\sqrt{d}$.
- On en déduit, dans $\mathbf{Z}$, $y = a^3 - 3ab^2d$ et $1 = 3a^2b - b^3d$.

Calculons sans crainte

- On a $x^3 = y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}) = z\overline{z}$.
- Le lemme vu ci-dessus montre que, si l'on a encore la factorisation unique dans $\mathbf{Z}[i\sqrt{d}]$ et si z et $\overline{z}$ sont premiers entre eux, ce sont des cubes dans $\mathbf{Z}[i\sqrt{d}]$.
- On a alors :
  $y + i\sqrt{d} = (a + ib\sqrt{d})^3 = a^3 + 3a^2bi\sqrt{d} - 3ab^2d - ib^3d\sqrt{d}$.
- On en déduit, dans $\mathbf{Z}$, $y = a^3 - 3ab^2d$ et $1 = 3a^2b - b^3d$.
- Comme b divise 1, on a $b = \pm 1$ d'où $d = 3a^2 \pm 1$ (condition nécessaire) et les solutions $y = 3ad - a^3$ et $x = a^2 + d$! (On vérifie.)

Des solutions !

- $d = 3a^2 + 1$, $x = a^2 + d$, $y = 3ad - a^3$.

a	0	1	2	3	4	5
d	1	4	13	28	49	76
x	1	5	17	37	65	101
y	0	11	70	225	524	1015

Des solutions !

- $d = 3a^2 + 1$, $x = a^2 + d$, $y = 3ad - a^3$.

a	0	1	2	3	4	5
d	1	4	13	28	49	76
x	1	5	17	37	65	101
y	0	11	70	225	524	1015

- $d = 3a^2 - 1$, $x = a^2 + d$, $y = 3ad - a^3$.

a	1	2	3	4	5
d	2	11	26	47	74
x	3	15	35	63	99
y	5	58	207	500	985

Des solutions !

- $d = 3a^2 + 1$, $x = a^2 + d$, $y = 3ad - a^3$.

a	0	1	2	3	4	5
d	1	4	13	28	49	76
x	1	5	17	37	65	101
y	0	11	70	225	524	1015

- $d = 3a^2 - 1$, $x = a^2 + d$, $y = 3ad - a^3$.

a	1	2	3	4	5
d	2	11	26	47	74
x	3	15	35	63	99
y	5	58	207	500	985

- Pour $d = 74$ par exemple on a la solution $99^3 = 985^2 + 74$.

Discussion

Les problèmes

- On a trouvé des solutions de l'équation $x^3 = y^2 + d$ lorsque $d = 3a^2 \pm 1 := 3a^2 + \epsilon$, mais les a-t-on toutes ?

Les problèmes

- On a trouvé des solutions de l'équation $x^3 = y^2 + d$ lorsque $d = 3a^2 \pm 1 := 3a^2 + \epsilon$, mais les a-t-on toutes ?
- Évidemment non puisque pour $d = 4$ $(a = 1, \epsilon = 1)$ on a trouvé la solution $x = 5$, $y = 11$, mais pas $x = y = 2$.

Les problèmes

- On a trouvé des solutions de l'équation $x^3 = y^2 + d$ lorsque $d = 3a^2 \pm 1 := 3a^2 + \epsilon$, mais les a-t-on toutes ?
- Évidemment non puisque pour $d = 4$ $(a = 1, \epsilon = 1)$ on a trouvé la solution $x = 5$, $y = 11$, mais pas $x = y = 2$.
- Dans ce cas, on comprend pourquoi : dans l'écriture $2^3 = 2^2 + 4 = (2 + 2i)(2 - 2i)$, les éléments $2 + 2i$ et $2 - 2i$ ne sont évidemment pas premiers entre eux.

Les problèmes

- On a trouvé des solutions de l'équation $x^3 = y^2 + d$ lorsque $d = 3a^2 \pm 1 := 3a^2 + \epsilon$, mais les a-t-on toutes ?
- Évidemment non puisque pour $d = 4$ $(a = 1, \epsilon = 1)$ on a trouvé la solution $x = 5$, $y = 11$, mais pas $x = y = 2$.
- Dans ce cas, on comprend pourquoi : dans l'écriture $2^3 = 2^2 + 4 = (2 + 2i)(2 - 2i)$, les éléments $2 + 2i$ et $2 - 2i$ ne sont évidemment pas premiers entre eux.
- À côté de ce point un peu anecdotique il y en a un autre bien plus sérieux : a-t-on toujours factorisation unique dans l'anneau $\mathbf{Z}[i\sqrt{d}]$?

Quelques rappels techniques

Soit A un anneau commutatif.

- a **divise** b : il existe $c \in A$ tel que $b = ac$.

Quelques rappels techniques

Soit A un anneau commutatif.

- a **divise** b : il existe $c \in A$ tel que $b = ac$.
- a est **inversible** : il existe $b \in A$ avec $ab = 1$.

Quelques rappels techniques

Soit A un anneau commutatif.

- a **divise** b : il existe $c \in A$ tel que $b = ac$.
- a est **inversible** : il existe $b \in A$ avec $ab = 1$.
- a est **irréductible** : les seuls diviseurs de a sont les inversibles et les éléments associés à a.

Quelques rappels techniques

Soit A un anneau commutatif.

- a **divise** b : il existe $c \in A$ tel que $b = ac$.
- a est **inversible** : il existe $b \in A$ avec $ab = 1$.
- a est **irréductible** : les seuls diviseurs de a sont les inversibles et les éléments associés à a.
- a, b sont **premiers entre eux** s'ils n'ont pas de diviseurs communs autres que les inversibles.

Quelques rappels techniques

Soit A un anneau commutatif.

- a **divise** b : il existe $c \in A$ tel que $b = ac$.
- a est **inversible** : il existe $b \in A$ avec $ab = 1$.
- a est **irréductible** : les seuls diviseurs de a sont les inversibles et les éléments associés à a.
- a, b sont **premiers entre eux** s'ils n'ont pas de diviseurs communs autres que les inversibles.
- A est **factoriel** si tout élément s'écrit, de manière unique, comme produit fini d'irréductibles.

Quelques rappels techniques

Soit A un anneau commutatif.

- a **divise** b : il existe $c \in A$ tel que $b = ac$.
- a est **inversible** : il existe $b \in A$ avec $ab = 1$.
- a est **irréductible** : les seuls diviseurs de a sont les inversibles et les éléments associés à a.
- a, b sont **premiers entre eux** s'ils n'ont pas de diviseurs communs autres que les inversibles.
- A est **factoriel** si tout élément s'écrit, de manière unique, comme produit fini d'irréductibles.
- L'unicité est équivalente au **lemme d'Euclide** : si p irréductible divise ab, il divise a ou b.

Un premier théorème : $(*)$

- On suppose que d est un entier sans facteur carré et congru à 1 ou 2 modulo 4 et qu'on a décomposition unique dans l'anneau $\mathbf{Z}[i\sqrt{d}]$. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$, $\overline{z} = y - i\sqrt{d}$.

Un premier théorème : $(*)$

- On suppose que d est un entier sans facteur carré et congru à 1 ou 2 modulo 4 et qu'on a décomposition unique dans l'anneau $\mathbf{Z}[i\sqrt{d}]$. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$, $\overline{z} = y - i\sqrt{d}$.
- Alors les nombres z et $\overline{z}$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{d}]$ et sont des cubes de $\mathbf{Z}[i\sqrt{d}]$.

Un premier théorème : $(*)$

- On suppose que d est un entier sans facteur carré et congru à 1 ou 2 modulo 4 et qu'on a décomposition unique dans l'anneau $\mathbf{Z}[i\sqrt{d}]$. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$, $\overline{z} = y - i\sqrt{d}$.
- Alors les nombres z et $\overline{z}$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{d}]$ et sont des cubes de $\mathbf{Z}[i\sqrt{d}]$.
- Sous les hypothèses ci-dessus :
  1) Si d n'est pas de la forme $3a^2 \pm 1$ l'équation de Bachet $x^3 = y^2 + d$ n'a pas de solutions dans $\mathbf{Z}$.
  2) Si $d = 3a^2 \pm 1$, les solutions positives de l'équation de Bachet sont $x = a^2 + d, \quad y = a(3d - a^2)$.

Factorialité ? Hélas !

- (#) L'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est factoriel que pour $d = 1$ ou $d = 2$.

Factorialité ? Hélas !

- $(\#)$ L'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est factoriel que pour $d = 1$ ou $d = 2$.
- Pour le voir, encore un peu de technique : la norme, $N(a + ib\sqrt{d}) = N(z) = z\overline{z} = a^2 + db^2$.

Factorialité ? Hélas !

- $(\#)$ L'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est factoriel que pour $d = 1$ ou $d = 2$.
- Pour le voir, encore un peu de technique : la norme, $N(a + ib\sqrt{d}) = N(z) = z\overline{z} = a^2 + db^2$.
- La norme est à valeurs dans $\mathbf{N}$ et multiplicative.

Factorialité ? Hélas !

- $(\#)$ L'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est factoriel que pour $d = 1$ ou $d = 2$.
- Pour le voir, encore un peu de technique : la norme, $N(a + ib\sqrt{d}) = N(z) = z\overline{z} = a^2 + db^2$.
- La norme est à valeurs dans $\mathbf{N}$ et multiplicative.
- Un élément $z \in \mathbf{Z}[i\sqrt{d}]$ est inversible si et seulement si $N(z) = 1$.

Factorialité ? Hélas !

- $(\#)$ L'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est factoriel que pour $d = 1$ ou $d = 2$.
- Pour le voir, encore un peu de technique : la norme, $N(a + ib\sqrt{d}) = N(z) = z\overline{z} = a^2 + db^2$.
- La norme est à valeurs dans $\mathbf{N}$ et multiplicative.
- Un élément $z \in \mathbf{Z}[i\sqrt{d}]$ est inversible si et seulement si $N(z) = 1$.
- Un nombre premier $p \in \mathbf{Z}$ est irréductible dans $\mathbf{Z}[i\sqrt{d}]$ si et seulement si ce n'est pas une norme. Retour à $(\#)$.

Factorialité ? Hélas !

- $(\#)$ L'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est factoriel que pour $d = 1$ ou $d = 2$.
- Pour le voir, encore un peu de technique : la norme, $N(a + ib\sqrt{d}) = N(z) = z\overline{z} = a^2 + db^2$.
- La norme est à valeurs dans $\mathbf{N}$ et multiplicative.
- Un élément $z \in \mathbf{Z}[i\sqrt{d}]$ est inversible si et seulement si $N(z) = 1$.
- Un nombre premier $p \in \mathbf{Z}$ est irréductible dans $\mathbf{Z}[i\sqrt{d}]$ si et seulement si ce n'est pas une norme. Retour à $(\#)$.
- Exemple d'un nombre avec deux décompositions : $d = 5$, $21 = 3 \times 7 = (4 + i\sqrt{5})(4 - i\sqrt{5})$.

Les nombres idéaux

Il ne faut pas jeter le bébé avec l'eau du bain

- La démonstration du théorème $(*)$ est trop séduisante pour être vraiment fausse, même dans le cas $d > 2$.

Il ne faut pas jeter le bébé avec l'eau du bain

- La démonstration du théorème $(*)$ est trop séduisante pour être vraiment fausse, même dans le cas $d > 2$.
- C'est ce sentiment qui a conduit Kümmer* à inventer les idéaux pour surmonter cette difficulté (dans le cas du grand théorème de Fermat).

Un exemple dans $\mathbf{Z}$ pour comprendre

- Considérons la décomposition banale, dans $\mathbf{Z}$:

$$210 = 14 \times 15 = 10 \times 21.$$

Un exemple dans $\mathbf{Z}$ pour comprendre

- Considérons la décomposition banale, dans $\mathbf{Z}$:

$$210 = 14 \times 15 = 10 \times 21.$$

- Bien sûr, les facteurs ne sont pas premiers :

$$210 = (2 \times 7) \times (5 \times 3) = (2 \times 5) \times (7 \times 3).$$

Un exemple dans $\mathbf{Z}$ pour comprendre

- Considérons la décomposition banale, dans $\mathbf{Z}$:

$$210 = 14 \times 15 = 10 \times 21.$$

- Bien sûr, les facteurs ne sont pas premiers :

$$210 = (2 \times 7) \times (5 \times 3) = (2 \times 5) \times (7 \times 3).$$

- Si on note (a, b) le pgcd de a et b dans $\mathbf{N}$, on a :

$$(14, 10)(14, 21)(15, 10)(15, 21) = (14, 10)(15, 10)(14, 21)(15, 21).$$

Un exemple dans $\mathbf{Z}$ pour comprendre

- Considérons la décomposition banale, dans $\mathbf{Z}$:

$$210 = 14 \times 15 = 10 \times 21.$$

- Bien sûr, les facteurs ne sont pas premiers :

$$210 = (2 \times 7) \times (5 \times 3) = (2 \times 5) \times (7 \times 3).$$

- Si on note (a, b) le pgcd de a et b dans $\mathbf{N}$, on a :

$$(14, 10)(14, 21)(15, 10)(15, 21) = (14, 10)(15, 10)(14, 21)(15, 21).$$

- On a les relations $14 = (14, 10)(14, 21)$, plus généralement $a = (a, u)(a, v)$ si a divise uv et si u, v sont premiers entre eux.

Et dans $\mathbf{Z}[i\sqrt{d}]$?

- Revenons à l'égalité $21 = 3 \times 7 = (4 + i\sqrt{5})(4 - i\sqrt{5})$.

Et dans $\mathbf{Z}[i\sqrt{d}]$?

- Revenons à l'égalité $21 = 3 \times 7 = (4 + i\sqrt{5})(4 - i\sqrt{5})$.
- L'explication précédente ne tient plus car les facteurs sont irréductibles donc premiers entre eux.

Et dans $\mathbf{Z}[i\sqrt{d}]$?

- Revenons à l'égalité $21 = 3 \times 7 = (4 + i\sqrt{5})(4 - i\sqrt{5})$.
- L'explication précédente ne tient plus car les facteurs sont irréductibles donc premiers entre eux.
- L'idée de Kümmer c'est que certains le sont plus que d'autres car ils vérifient une identité de Bézout par exemple 3 et 7 : $4 \times 7 - 9 \times 3 = 1$ et $(-4 + 3i\sqrt{5})(4 + i\sqrt{5}) + 8(4 - i\sqrt{5}) = 1$. En revanche ce n'est pas vrai pour 3 et $4 + i\sqrt{5}$ par exemple.

Et dans $\mathbf{Z}[i\sqrt{d}]$?

- Revenons à l'égalité $21 = 3 \times 7 = (4 + i\sqrt{5})(4 - i\sqrt{5})$.
- L'explication précédente ne tient plus car les facteurs sont irréductibles donc premiers entre eux.
- L'idée de Kümmer c'est que certains le sont plus que d'autres car ils vérifient une identité de Bézout par exemple 3 et 7 : $4 \times 7 - 9 \times 3 = 1$ et $(-4 + 3i\sqrt{5})(4 + i\sqrt{5}) + 8(4 - i\sqrt{5}) = 1$. En revanche ce n'est pas vrai pour 3 et $4 + i\sqrt{5}$ par exemple.
- Ce qu'imagine Kümmer c'est qu'il existe un pgcd "idéal" noté encore $(3, 4 + i\sqrt{5})$ et qu'on a la décomposition "idéale" :

$$21 = (3, 4 + i\sqrt{5})(3, 4 - i\sqrt{5})(7, 4 + i\sqrt{5})(7, 4 - i\sqrt{5})$$

$$= (3, 4 + i\sqrt{5})(7, 4 + i\sqrt{5})(3, 4 - i\sqrt{5})(7, 4 - i\sqrt{5}).$$

Ce que dit Kümmer

Lettre à Liouville (1847) :

"quant à la propriété qu'un nombre complexe ne peut être décomposé en facteurs premiers que d'une seule manière, je puis vous assurer qu'elle n'a pas lieu généralement tant qu'il s'agit des nombres de la forme : $a + ib\sqrt{d}$ mais qu'on peut la sauver en introduisant un nouveau genre de nombres complexes que j'ai nommé nombre complexe idéal.".

Le parallèle avec la chimie (1851)

"Qu'il me soit permis de signaler ici en peu de mots l'analogie de cette théorie de la composition des nombres idéaux avec les principes fondamentaux de la chimie. La composition des nombres complexes peut être envisagée comme l'analogue de la composition chimique ; les facteurs premiers correspondent aux éléments (...). Les nombres complexes idéaux sont comparables aux radicaux hypothétiques qui n'existent pas par eux-mêmes, mais seulement dans les combinaisons ; le fluor (...) peut être comparé à un facteur premier idéal. (...) Toutes ces analogies qu'on pourra poursuivre et augmenter à volonté, ne proviennent pas d'un jeu d'esprit oisif, mais elles sont bien fondées en ce que les mêmes idées fondamentales de la composition et de la décomposition des éléments règnent aussi bien dans la chimie des matières naturelles que dans celle des nombres complexes."

Formalisation

- Il s'agit de donner un sens à l'écriture (a, b) pour un pgcd idéal de a et b.

Formalisation

- Il s'agit de donner un sens à l'écriture (a, b) pour un pgcd idéal de a et b.
- Dans $\mathbf{Z}$, ce pgcd est un nombre d et on a l'égalité de Bézout $d = \alpha a + \beta b$, de plus les éléments de la forme $\alpha a + \beta b$ sont exactement les multiples de d.

Formalisation

- Il s'agit de donner un sens à l'écriture (a, b) pour un pgcd idéal de a et b.
- Dans $\mathbf{Z}$, ce pgcd est un nombre d et on a l'égalité de Bézout $d = \alpha a + \beta b$, de plus les éléments de la forme $\alpha a + \beta b$ sont exactement les multiples de d.
- Dans $\mathbf{Z}[i\sqrt{d}]$ il faut remplacer le **nombre** d par **l'ensemble** des $\alpha a + \beta b$: **l'idéal** engendré par a et b. On a le cas particulier d'un élément : d correspond à l'ensemble (d) des multiples de d (idéal principal).

Formalisation

- Il s'agit de donner un sens à l'écriture (a, b) pour un pgcd idéal de a et b.
- Dans $\mathbf{Z}$, ce pgcd est un nombre d et on a l'égalité de Bézout $d = \alpha a + \beta b$, de plus les éléments de la forme $\alpha a + \beta b$ sont exactement les multiples de d.
- Dans $\mathbf{Z}[i\sqrt{d}]$ il faut remplacer le **nombre** d par **l'ensemble** des $\alpha a + \beta b$: **l'idéal** engendré par a et b. On a le cas particulier d'un élément : d correspond à l'ensemble (d) des multiples de d (idéal principal).
- Cela permet d'interpréter la relation de divisibilité comme l'inclusion des idéaux (en sens inverse) et le pgcd comme la somme des idéaux.

Formalisation (suite)

- Somme et produit des idéaux.

Formalisation (suite)

- Somme et produit des idéaux.
- Idéaux premiers entre eux ou étrangers : $I + J = A$.

Formalisation (suite)

- Somme et produit des idéaux.
- Idéaux premiers entre eux ou étrangers : $I + J = A$.
- Un résultat qui justifie l'écriture :
  Soient A un anneau intègre et $a, u, v \in A$. On suppose que a divise uv et que u et v sont étrangers, c'est-à-dire qu'on a, en termes d'idéaux, $(u, v) = (1)$. Alors on a la formule, sur les idéaux : $(a) = (a, u)(a, v)$.

Anneaux de Dedekind

- Définition des idéaux premiers, le lemme d'Euclide : I est premier si $ab \in I$ implique a ou $b \in I$.

Anneaux de Dedekind

- Définition des idéaux premiers, le lemme d'Euclide : I est premier si $ab \in I$ implique a ou $b \in I$.
- La décomposition unique dans le cadre des idéaux :
  On suppose $d \equiv 1, 2 \pmod 4$. *Tout idéal de* $\mathbf{Z}[i\sqrt{d}]$ *se décompose de manière unique en produits d'idéaux premiers.*

Retour à l'équation de Bachet

- On suppose toujours d sans facteur carré et $d \equiv 1, 2 \mod 4$.

Retour à l'équation de Bachet

- On suppose toujours d sans facteur carré et $d \equiv 1, 2 \mod 4$.
- *Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$. Alors les idéaux (z) et $(\overline{z})$ sont étrangers dans $\mathbf{Z}[i\sqrt{d}]$.*

Retour à l'équation de Bachet

- On suppose toujours d sans facteur carré et $d \equiv 1, 2 \mod 4$.
- *Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$. Alors les idéaux (z) et $(\overline{z})$ sont étrangers dans $\mathbf{Z}[i\sqrt{d}]$.*
- L'idéal (z) est un cube. **Attention**, encore une difficulté ...

Retour à l'équation de Bachet

- On suppose toujours d sans facteur carré et $d \equiv 1, 2 \mod 4$.
- *Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$. Alors les idéaux (z) et $(\overline{z})$ sont étrangers dans $\mathbf{Z}[i\sqrt{d}]$.*
- L'idéal (z) est un cube. **Attention**, encore une difficulté ...
- Si I est un idéal dont le cube est principal, I est-il principal ? (si oui on dira que 3 est régulier pour d).

Le théorème $(**)$

- On suppose que d est un entier sans facteur carré avec $d \equiv 1, 2 \mod 4$ et que 3 est régulier pour d. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$.

Le théorème $(**)$

- On suppose que d est un entier sans facteur carré avec $d \equiv 1, 2 \mod 4$ et que 3 est régulier pour d. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$.
- Alors les nombres z et $\overline{z}$ sont étrangers entre eux dans $\mathbf{Z}[i\sqrt{d}]$ et sont des cubes de $\mathbf{Z}[i\sqrt{d}]$.

Le théorème $(**)$

- On suppose que d est un entier sans facteur carré avec $d \equiv 1, 2 \mod 4$ et que 3 est régulier pour d. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$.
- Alors les nombres z et $\overline{z}$ sont étrangers entre eux dans $\mathbf{Z}[i\sqrt{d}]$ et sont des cubes de $\mathbf{Z}[i\sqrt{d}]$.
- 1) Si d n'est pas de la forme $3a^2 \pm 1$ l'équation de Bachet $x^3 = y^2 + d$ n'a pas de solutions dans $\mathbf{Z}$.
  2) Si $d = 3a^2 \pm 1$, les solutions positives de l'équation de Bachet sont $x = a^2 + d$, $y = a(3d - a^2)$.

Et le grand théorème de Fermat ?

- On cherche les solutions entières de $x^p + y^p = z^p$, avec p premier.

Et le grand théorème de Fermat ?

- On cherche les solutions entières de $x^p + y^p = z^p$, avec p premier.
- On décompose dans les complexes :

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

où ζ est une racine primitive p-ième de l'unité.

Et le grand théorème de Fermat ?

- On cherche les solutions entières de $x^p + y^p = z^p$, avec p premier.
- On décompose dans les complexes :

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

où ζ est une racine primitive p-ième de l'unité.

- On travaille dans l'anneau $\mathbf{Z}[\zeta]$ des nombres complexes de la forme $a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ avec $a_i \in \mathbf{Z}$.

Et le grand théorème de Fermat ?

- On cherche les solutions entières de $x^p + y^p = z^p$, avec p premier.
- On décompose dans les complexes :

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

où ζ est une racine primitive p-ième de l'unité.

- On travaille dans l'anneau $\mathbf{Z}[\zeta]$ des nombres complexes de la forme $a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ avec $a_i \in \mathbf{Z}$.
- On voudrait montrer que les $x + \zeta^i y$ sont des puissances p-ièmes dans cet anneau par des raisonnements de divisibilité.

Et le grand théorème de Fermat ?

- On cherche les solutions entières de $x^p + y^p = z^p$, avec p premier.
- On décompose dans les complexes :

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

où ζ est une racine primitive p-ième de l'unité.

- On travaille dans l'anneau $\mathbf{Z}[\zeta]$ des nombres complexes de la forme $a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ avec $a_i \in \mathbf{Z}$.
- On voudrait montrer que les $x + \zeta^i y$ sont des puissances p-ièmes dans cet anneau par des raisonnements de divisibilité.
- Comme le dit Kümmer l'anneau $\mathbf{Z}[\zeta]$n'est pas factoriel en général (c'est vrai seulement pour $p \leq 19$).

Et le grand théorème de Fermat (suite)

- Comme pour l'équation de Bachet on contourne cette difficulté en utilisant la décomposition en idéaux premiers.

Et le grand théorème de Fermat (suite)

- Comme pour l'équation de Bachet on contourne cette difficulté en utilisant la décomposition en idéaux premiers.
- On tombe ici encore sur la deuxième difficulté : un idéal I tel que I^p soit principal est-il principal (p régulier) ?

Et le grand théorème de Fermat (suite)

- Comme pour l'équation de Bachet on contourne cette difficulté en utilisant la décomposition en idéaux premiers.
- On tombe ici encore sur la deuxième difficulté : un idéal I tel que I^p soit principal est-il principal (p régulier) ?
- Sinon, on ne sait pas conclure par cette méthode. Or il y a beaucoup de nombres premiers irréguliers. Voir Bonus.

Et le grand théorème de Fermat (suite)

- Comme pour l'équation de Bachet on contourne cette difficulté en utilisant la décomposition en idéaux premiers.
- On tombe ici encore sur la deuxième difficulté : un idéal I tel que I^p soit principal est-il principal (p régulier) ?
- Sinon, on ne sait pas conclure par cette méthode. Or il y a beaucoup de nombres premiers irréguliers. Voir Bonus.
- Cette difficulté n'est toujours pas entièrement surmontée à l'heure actuelle et la démonstration du théorème de Fermat qu'Andrew Wiles a donnée en 1993-94 est fondée sur une approche radicalement différente.

Un exercice pour la route

- Le résultat est le suivant :
  On suppose que d est de la forme $4a^2+1$ avec $a \geq 1$ et a non multiple de 3. Alors l'équation $x^3 = y^2 + d$ n'a pas de solution.

Un exercice pour la route

- Le résultat est le suivant :
  On suppose que d est de la forme $4a^2+1$ avec $a \geq 1$ et a non multiple de 3. Alors l'équation $x^3 = y^2 + d$ n'a pas de solution.
- La recette est de travailler avec les congruences modulo 4 et d'utiliser le résultat classique suivant :
  Si p est un nombre premier congru à -1 modulo 4, -1 n'est pas un carré modulo p.

Un exercice pour la route

- Le résultat est le suivant :
  On suppose que d est de la forme $4a^2+1$ avec $a \geq 1$ et a non multiple de 3. Alors l'équation $x^3 = y^2 + d$ n'a pas de solution.
- La recette est de travailler avec les congruences modulo 4 et d'utiliser le résultat classique suivant :
  Si p est un nombre premier congru à -1 modulo 4, -1 n'est pas un carré modulo p.
- Je vous remercie de votre attention.

BONUS

Les autres cas

- Le cas où d a un facteur carré, en particulier $d = 4$.

Les autres cas

- Le cas où d a un facteur carré, en particulier $d = 4$.
- Le cas $d \equiv -1 \pmod 4$.

Les autres cas

- Le cas où d a un facteur carré, en particulier $d = 4$.
- Le cas $d \equiv -1 \pmod 4$.
- Le cas où 3 est irrégulier (pour $d \leq 100$, $d = 23, 26, 29, 31, 38, 53, 59, 61, 83, 87, 89$).

Les autres cas

- Le cas où d a un facteur carré, en particulier $d = 4$.
- Le cas $d \equiv -1 \pmod 4$.
- Le cas où 3 est irrégulier (pour $d \leq 100$, $d = 23, 26, 29, 31, 38, 53, 59, 61, 83, 87, 89$).
- Le point sur l'équation de Bachet*.

Une hypothèse sur une preuve de Fermat pour $d = 2$

- Source : le livre d'André Weil *From Hammourabi to Legendre, Number Theory, an approach through history*.

Une hypothèse sur une preuve de Fermat pour $d = 2$

- Source : le livre d'André Weil *From Hammourabi to Legendre, Number Theory, an approach through history*.
- L'hypothèse de Weil : elle repose sur l'étude des décompositions des entiers sous la forme $a^2 + 2b^2$.

Une hypothèse sur une preuve de Fermat pour $d = 2$

- Source : le livre d'André Weil *From Hammourabi to Legendre, Number Theory, an approach through history*.
- L'hypothèse de Weil : elle repose sur l'étude des décompositions des entiers sous la forme $a^2 + 2b^2$.
- Par exemple, si p est premier impair, il admet une telle décomposition, unique, si et seulement si p est congru à 1 ou 3 modulo 8.

Compléments sur le grand théorème de Fermat

- Les réguliers : on sait qu'il y a une infinité d'irréguliers alors qu'on ne le sait pas pour les réguliers. Cependant on conjecture (et on vérifie expérimentalement) que la densité des réguliers est environ égale à $0,6065$, donc plus grande que celle des irréguliers. Les plus petits irréguliers sont $37, 59$ et 67.

Compléments sur le grand théorème de Fermat

- Les réguliers : on sait qu'il y a une infinité d'irréguliers alors qu'on ne le sait pas pour les réguliers. Cependant on conjecture (et on vérifie expérimentalement) que la densité des réguliers est environ égale à $0,6065$, donc plus grande que celle des irréguliers. Les plus petits irréguliers sont $37, 59$ et 67.
- La méthode de Wiles utilise la courbe elliptique d'Hellegouarch : si $a^p + b^p = c^p$ est une solution de Fermat, il s'agit de la courbe $y^2 = x(x - a^p)(x - b^p)$.