Quelques grands problèmes de la théorie des nombres

Alexandre Bailleul

Lycée Val de Garonne - Marmande

2 mai 2019

La théorie des nombres, c'est quoi ?

- Le but de la théorie des nombres est d'étudier les nombres entiers. Ceux-ci recèlent, malgré leur simplicité, de nombreux mystères, et sont sources de nombreux problèmes.

La théorie des nombres, c'est quoi ?

- Le but de la théorie des nombres est d'étudier les nombres entiers. Ceux-ci recèlent, malgré leur simplicité, de nombreux mystères, et sont sources de nombreux problèmes.
- C'est un domaine mathématique très varié : algèbre, analyse, géométrie, probabilités, topologie, logique, etc.

La théorie des nombres, c'est quoi ?

- Le but de la théorie des nombres est d'étudier les nombres entiers. Ceux-ci recèlent, malgré leur simplicité, de nombreux mystères, et sont sources de nombreux problèmes.

- C'est un domaine mathématique très varié : algèbre, analyse, géométrie, probabilités, topologie, logique, etc.

Problèmes simples à énoncer, mais difficiles à résoudre !

Sommaire

Plan

Nombres premiers

Définition.

Un nombre premier est un entier qui admet exactement deux diviseurs positifs, 1 et lui-même.

Nombres premiers

Définition.

Un nombre premier est un entier qui admet exactement deux diviseurs positifs, 1 et lui-même.

- Exemples : 2, 3, 5, 7, 11, 13, 17, etc.
- $1, 6 = 2 \times 3$ et $100 = 10 \times 10$ ne sont pas premiers.

Une infinité de nombres premiers

Théorème (Euclide).

Il existe une infinité de nombres premiers.

Une infinité de nombres premiers

Théorème (Euclide).

Il existe une infinité de nombres premiers.

Démonstration. Si $p_1, \ldots, p_r$ sont des nombres premiers alors les facteurs premiers de

$$p_1 \times \cdots \times p_r + 1$$

ne peuvent pas être parmi les p_i. □

Pourquoi les nombres premiers ?

Théorème (fondamental de l'arithmétique).

Tout entier supérieur à 2 s'écrit de manière unique (à l'ordre près des facteurs) comme produit de nombres premiers.

Pourquoi les nombres premiers ?

Théorème (fondamental de l'arithmétique).

Tout entier supérieur à 2 s'écrit de manière unique (à l'ordre près des facteurs) comme produit de nombres premiers.

- Exemples :
  $18 = 2 \times 3^2, 11319 = 3 \times 7^3 \times 11, 4294967297 = 641 \times 6700417.$

Pourquoi les nombres premiers ?

Théorème (fondamental de l'arithmétique).

Tout entier supérieur à 2 s'écrit de manière unique (à l'ordre près des facteurs) comme produit de nombres premiers.

- Exemples :
  $18 = 2 \times 3^2, 11319 = 3 \times 7^3 \times 11, 4294967297 = 641 \times 6700417.$
- Les nombres premiers sont les briques de base de la structure multiplicative des entiers (la structure additive repose uniquement sur 1).

Pourquoi les nombres premiers ?

Théorème (fondamental de l'arithmétique).

Tout entier supérieur à 2 s'écrit de manière unique (à l'ordre près des facteurs) comme produit de nombres premiers.

- Exemples :
  $18 = 2 \times 3^2, 11319 = 3 \times 7^3 \times 11, 4294967297 = 641 \times 6700417.$
- Les nombres premiers sont les briques de base de la structure multiplicative des entiers (la structure additive repose uniquement sur 1).
- Applications théoriques (démonstrations) et pratiques (cryptographie).

Trouver les nombres premiers

Comment trouver les nombres premiers ?

- Méthode naïve : on teste si $d \mid n$ pour $2 \leq d \leq n-1$.

Trouver les nombres premiers

Comment trouver les nombres premiers ?

- Méthode naïve : on teste si $d \mid n$ pour $2 \leq d \leq n-1$.
- Méthode à peine moins naïve : on teste si $d \mid n$ pour $2 \leq d \leq \sqrt{n}$.

Trouver les nombres premiers

Comment trouver les nombres premiers ?

- Méthode naïve : on teste si $d \mid n$ pour $2 \leq d \leq n-1$.
- Méthode à peine moins naïve : on teste si $d \mid n$ pour $2 \leq d \leq \sqrt{n}$.
- Le crible d'Ératosthène : on écrit tous les entiers de 2 à N, on garde 2 et on raye ses multiples, puis on garde le prochain entier non rayé (3) et on raye ses multiples, etc.

Trouver les nombres premiers

Comment trouver les nombres premiers ?

- Méthode naïve : on teste si $d \mid n$ pour $2 \leq d \leq n-1$.
- Méthode à peine moins naïve : on teste si $d \mid n$ pour $2 \leq d \leq \sqrt{n}$.
- Le crible d'Ératosthène : on écrit tous les entiers de 2 à N, on garde 2 et on raye ses multiples, puis on garde le prochain entier non rayé (3) et on raye ses multiples, etc.
- Tout ça est peu efficace en pratique, et quasiment inutile en théorie. Cherchons une autre manière de produire des nombres premiers !

Nombres premiers de Mersenne

- Les nombres de la forme

$$M_n = 2^n - 1$$

sont de bons candidats pour être de grands nombres premiers.

Nombres premiers de Mersenne

- Les nombres de la forme

$$M_n = 2^n - 1$$

sont de bons candidats pour être de grands nombres premiers.

Théorème (Mersenne).

Si $2^n - 1$ est premier alors n est premier.

Nombres premiers de Mersenne

- Les nombres de la forme

$$M_n = 2^n - 1$$

sont de bons candidats pour être de grands nombres premiers.

Théorème (Mersenne).

Si $2^n - 1$ est premier alors n est premier.

n	2	3	5	7	11	13	17	19
M_n	3	7	31	127	**2047**	8191	131071	524287

Nombres premiers de Mersenne

- On a

$$M_{11} = 2047 = 23 \times 89,$$

et

$$M_{23} = 8388607 = 47 \times 178481.$$

Nombres premiers de Mersenne

- On a

$$M_{11} = 2047 = 23 \times 89,$$

et

$$M_{23} = 8388607 = 47 \times 178481.$$

Problème ouvert.

Existe-t-il une infinité de nombres de la forme $2^n - 1$ premiers ?
Existe-t-il une infinité de nombres de la forme $2^n - 1$ composés (non premiers) ?

Nombres premiers de Mersenne

- Même si tous les M_p ne sont pas premiers, les nombres de Mersenne permettent quand même de générer de grands nombres premiers (test de Lucas-Lehmer).

Nombres premiers de Mersenne

- Même si tous les M_p ne sont pas premiers, les nombres de Mersenne permettent quand même de générer de grands nombres premiers (test de Lucas-Lehmer).

- En 1903, Frank Cole donne une conférence durant laquelle il calcule au tableau en silence $M_{67} = 2^{67} - 1$ puis $193707721 \times 761838257287$ (qui vaut effectivement M_{67}). La recherche des facteurs premiers de M_{67} lui a pris trois ans !

Nombres premiers de Mersenne

- Même si tous les M_p ne sont pas premiers, les nombres de Mersenne permettent quand même de générer de grands nombres premiers (test de Lucas-Lehmer).
- En 1903, Frank Cole donne une conférence durant laquelle il calcule au tableau en silence $M_{67} = 2^{67} - 1$ puis $193707721 \times 761838257287$ (qui vaut effectivement M_{67}). La recherche des facteurs premiers de M_{67} lui a pris trois ans !
- $M_{82589933}$, qui s'écrit avec 24862048 chiffres, est le plus grand nombre premier connu.

Nombres premiers de Mersenne

- Même si tous les M_p ne sont pas premiers, les nombres de Mersenne permettent quand même de générer de grands nombres premiers (test de Lucas-Lehmer).
- En 1903, Frank Cole donne une conférence durant laquelle il calcule au tableau en silence $M_{67} = 2^{67} - 1$ puis $193707721 \times 761838257287$ (qui vaut effectivement M_{67}). La recherche des facteurs premiers de M_{67} lui a pris trois ans !
- $M_{82589933}$, qui s'écrit avec 24862048 chiffres, est le plus grand nombre premier connu. Il a été découvert en décembre 2018 par le projet GIMPS (*Great Internet Mersenne Prime Search*).

Nombres premiers de Fermat

- Les nombres de la forme $2^k + 1$ sont également de bons candidats.

Nombres premiers de Fermat

- Les nombres de la forme $2^k + 1$ sont également de bons candidats.

Théorème (Euclide).

Si $2^k + 1$ est premier alors k est une puissance de 2.

Nombres premiers de Fermat

- Les nombres de la forme $2^k + 1$ sont également de bons candidats.

Théorème (Euclide).

Si $2^k + 1$ est premier alors k est une puissance de 2.

- On pose

$$F_n = 2^{2^n} + 1.$$

Conjecture (Fermat, 1640).

Pour tout entier $n \geq 0$, $2^{2^n} + 1$ est premier.

n	0	1	2	3	4	5
F_n	3	5	17	257	65537	**4294967297**

Nombres premiers de Fermat

- Leonhard Euler montre en 1732 que

  $F_5 = 4294967297 = 641 \times 6700417.$

  La conjecture de Fermat est fausse !

Nombres premiers de Fermat

- Leonhard Euler montre en 1732 que

  $F_5 = 4294967297 = 641 \times 6700417.$

  La conjecture de Fermat est fausse !

- En 1855, Thomas Clausen montre que F_6 est composé. Aujourd'hui, on sait que $F_6, F_7, \ldots, F_{32}$ sont composés.

Nombres premiers de Fermat

Conjecture (Folklore, XXème siècle).

Les seuls entiers $n \geq 0$ tels que $2^{2^n} + 1$ est premier sont $0, 1, 2, 3$ et 4.

Nombres premiers de Fermat

Conjecture (Folklore, XXème siècle).

Les seuls entiers $n \geq 0$ tels que $2^{2^n} + 1$ est premier sont $0, 1, 2, 3$ et 4.

Problème ouvert.

Existe-t-il une infinité de nombres de la forme $2^{2^n} + 1$ composés ?

Nombres premiers de Fermat

Conjecture (Folklore, XXème siècle).

Les seuls entiers $n \geq 0$ tels que $2^{2^n} + 1$ est premier sont $0, 1, 2, 3$ et 4.

Problème ouvert.

Existe-t-il une infinité de nombres de la forme $2^{2^n} + 1$ composés ?

- Les nombres de Fermat croissent extrêmement vite, ce qui rend les tests de primalité rapidement difficiles à réaliser. On ne connaît la factorisation que de $F_6, \ldots, F_{11}$. La nature de F_{33} est inconnue, mais on sait que certains très grands nombres de Fermat sont composés, par exemple $F_{2747497}$.

Une formule ?

- On ne connaît pas à ce jour de formule **exploitable** donnant tous les, ou au moins une infinité de nombres premiers.

Une formule ?

- On ne connaît pas à ce jour de formule **exploitable** donnant tous les, ou au moins une infinité de nombres premiers.

Exemples de tentatives :

- $n^2 + n + 41$ est premier pour $n = 0, 1, \ldots, 39$ mais $40^2 + 40 + 41$ est divisible par 41. Il n'existe pas de polynôme à coefficients entiers ne prenant que des valeurs premières à partir d'un certain rang.

Une formule ?

- On ne connaît pas à ce jour de formule **exploitable** donnant tous les, ou au moins une infinité de nombres premiers.

Exemples de tentatives :

- $n^2 + n + 41$ est premier pour $n = 0, 1, \ldots, 39$ mais $40^2 + 40 + 41$ est divisible par 41. Il n'existe pas de polynôme à coefficients entiers ne prenant que des valeurs premières à partir d'un certain rang.

- Avec le théorème de Wilson (n est premier si et seulement si $(n-1)! \equiv -1 \bmod n$), on montre que la fonction

$$f : n \mapsto 2 + (2(n!) \bmod (n+1))$$

ne prend que des valeurs premières, et produit tous les nombres premiers.

Une formule ?

- Suite aux travaux de Yuri Matyiasevich dans les années 70, on sait que les valeurs strictement positives de

$$
\begin{aligned}
&(k+2)(1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2\\
&-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2\\
&-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)\\
&+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2\\
&-[n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2\\
&-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\\
&-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2\\
&-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2)
\end{aligned}
$$

pour $a, b, \ldots, z \in \mathbb{N}^*$ sont exactement les nombres premiers.

Une formule ?

- Suite aux travaux de Yuri Matyiasevich dans les années 70, on sait que les valeurs strictement positives de

$$(k+2)(1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2$$
$$-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2$$
$$-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)$$
$$+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2$$
$$-[n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2$$
$$-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2$$
$$-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2)$$

pour $a, b, \ldots, z \in \mathbb{N}^*$ sont exactement les nombres premiers.

- On n'a su produire que 2 pour l'instant !

Répartition des nombres premiers

- On sait qu'il existe une infinité de nombres premiers, mais ceux-ci sont-ils « abondants » parmi les entiers ?

Répartition des nombres premiers

- On sait qu'il existe une infinité de nombres premiers, mais ceux-ci sont-ils « abondants » parmi les entiers ?

Définition.

Pour tout $x \geq 2$, on pose

$$\pi(x) = \#\{p \leq x \mid p \text{ premier}\}.$$

Répartition des nombres premiers

- On sait qu'il existe une infinité de nombres premiers, mais ceux-ci sont-ils « abondants » parmi les entiers ?

Définition.

Pour tout $x \geq 2$, on pose

$$\pi(x) = \#\{p \leq x \mid p \text{ premier}\}.$$

- Le théorème d'Euclide se réécrit

$$\pi(x) \underset{x \to +\infty}{\longrightarrow} +\infty.$$

La question est « à quelle vitesse » cette fonction tend-elle vers l'infini ?

Répartition des nombres premiers

- À la fin du XVIIIème siècle, Karl Friedrich Gauss (à l'âge de 15 ans !) et Adrien-Marie Legendre observent indépendamment que $\pi(x)$ est « proche » de $\frac{x}{\log x}$.

Répartition des nombres premiers

- À la fin du XVIIIème siècle, Karl Friedrich Gauss (à l'âge de 15 ans !) et Adrien-Marie Legendre observent indépendamment que $\pi(x)$ est « proche » de $\frac{x}{\log x}$.

Plus précisément

Conjecture (Gauss).

On a

$$\pi(x) \underset{x\to+\infty}{\sim} \mathrm{li}(x) = \int_0^x \frac{dt}{\log t} \quad \left(\underset{x\to+\infty}{\sim} \frac{x}{\log x}\right).$$

Répartition des nombres premiers

- À la fin du XVIIIème siècle, Karl Friedrich Gauss (à l'âge de 15 ans !) et Adrien-Marie Legendre observent indépendamment que $\pi(x)$ est « proche » de $\frac{x}{\log x}$.

Plus précisément

Conjecture (Gauss).

On a

$$\pi(x) \underset{x\to+\infty}{\sim} \mathrm{li}(x) = \int_0^x \frac{dt}{\log t} \quad \left(\underset{x\to+\infty}{\sim} \frac{x}{\log x}\right).$$

- Autrement dit, la « probabilité » qu'un nombre entier $\leq x$ est premier est proche de $\frac{1}{\log x}$.

Répartition des nombres premiers

- À la fin du XVIIIème siècle, Karl Friedrich Gauss (à l'âge de 15 ans !) et Adrien-Marie Legendre observent indépendamment que $\pi(x)$ est « proche » de $\frac{x}{\log x}$.

Plus précisément

Conjecture (Gauss).

On a

$$\pi(x) \underset{x\to+\infty}{\sim} \mathrm{li}(x) = \int_0^x \frac{dt}{\log t} \quad \left(\underset{x\to+\infty}{\sim} \frac{x}{\log x}\right).$$

- Autrement dit, la « probabilité » qu'un nombre entier $\leq x$ est premier est proche de $\frac{1}{\log x}$.

- Exemple : $\pi(10^9) = 50847534$ et $|\pi(10^9) - \mathrm{li}(10^9)| = 1701$.

L'apport de Riemann

- En 1859, Bernhard Riemann publie un mémoire qui révolutionne la théorie des nombres. Il étudie la fonction

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \quad \left(= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots \right)$$

$$= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \quad \left(= \frac{1}{1-\frac{1}{2^s}} \times \frac{1}{1-\frac{1}{3^s}} \times \frac{1}{1-\frac{1}{5^s}} \times \dots \right)$$

pour tous les nombres complexes s tels que $\mathrm{Re}(s) > 1$.

L'apport de Riemann

- En 1859, Bernhard Riemann publie un mémoire qui révolutionne la théorie des nombres. Il étudie la fonction

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \quad \left(= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots \right)$$

$$= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \quad \left(= \frac{1}{1-\frac{1}{2^s}} \times \frac{1}{1-\frac{1}{3^s}} \times \frac{1}{1-\frac{1}{5^s}} \times \dots \right)$$

pour tous les nombres complexes s tels que $\mathrm{Re}(s) > 1$.

- Il découvre des propriétés remarquables de cette fonction, notamment une sorte de symétrie par rapport à la droite des nombres complexes de partie réelle $\frac{1}{2}$.

L'apport de Riemann

- Avec le produit eulérien, et les propriétés précédentes, Riemann obtient une formule **exacte** pour $\pi(x)$.

Théorème (Riemann, 1859).

Pour $x \geq 2$, on a

$$\pi(x) = \sum_{n=1}^{+\infty} \frac{\mu(n) f(x^{1/n})}{n},$$

où

$$\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \text{ a un facteur carré} \\ (-1)^k \text{ si } n = p_1 \times \cdots \times p_k \end{cases},$$

$$f(x) = \mathrm{li}(x) - \sum_{\rho} \mathrm{li}(x^{\rho}) + \int_x^{+\infty} \frac{1}{u^2 - 1} \frac{du}{u \log u} - \log 2,$$

où la somme porte sur tous les zéros de ζ.

Le théorème des nombres premiers

Théorème (Hadamard, de la Vallée-Poussin, 1896).

Pour tout réel $t \neq 0$,

$$\zeta(1+it) \neq 0.$$

Le théorème des nombres premiers

Théorème (Hadamard, de la Vallée-Poussin, 1896).

Pour tout réel $t \neq 0$,

$$\zeta(1+it) \neq 0.$$

Corollaire (Théorème des nombres premiers).

On a

$$\pi(x) \underset{x \to +\infty}{\sim} \mathrm{li}(x).$$

L'hypothèse de Riemann

Conjecture (Hypothèse de Riemann).

Si $\zeta(s) = 0$ et $0 \leq \mathrm{Re}(s) \leq 1$ alors $\mathrm{Re}(s) = \frac{1}{2}$.

L'hypothèse de Riemann

Conjecture (Hypothèse de Riemann).

Si $\zeta(s) = 0$ et $0 \leq \mathrm{Re}(s) \leq 1$ alors $\mathrm{Re}(s) = \frac{1}{2}$.

Théorème (Von Koch, 1901).

L'hypothèse de Riemann est équivalente à l'estimation

$$\pi(x) = \mathrm{li}(x) + R(x),$$

où

$$|R(x)| \leq Cx^{1/2} \log x$$

et $C > 0$ est une constante.

Ce que l'on sait

- Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

Ce que l'on sait

- Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.
- Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.

Ce que l'on sait

- Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.
- Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.
- Korobov, Vinogradov (1958) : $\zeta(s) \neq 0$ pour $\mathrm{Re}(s) \geq 1 - \frac{c}{(\log(|\mathrm{Im}(s)|+2))^{2/3}(\log\log(|\mathrm{Im}(s)|+2))^{1/3}}$

Ce que l'on sait

- Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.
- Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.
- Korobov, Vinogradov (1958) : $\zeta(s) \neq 0$ pour $\mathrm{Re}(s) \geq 1 - \frac{c}{(\log(|\mathrm{Im}(s)|+2))^{2/3}(\log\log(|\mathrm{Im}(s)|+2))^{1/3}}$

$$\Rightarrow |\pi(x) - \mathrm{li}(x)| \leq C_1 x \exp\left(-C_2 \frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}\right).$$

- Conrey (1989) : Au moins 40% des zéros de ζ ont pour partie réelle $\frac{1}{2}$.

Ce que l'on sait

- Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.
- Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.
- Korobov, Vinogradov (1958) : $\zeta(s) \neq 0$ pour $\mathrm{Re}(s) \geq 1 - \frac{c}{(\log(|\mathrm{Im}(s)|+2))^{2/3}(\log\log(|\mathrm{Im}(s)|+2))^{1/3}}$

$$\Rightarrow |\pi(x) - \mathrm{li}(x)| \leq C_1 x \exp\left(-C_2 \frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}\right).$$

- Conrey (1989) : Au moins 40% des zéros de ζ ont pour partie réelle $\frac{1}{2}$.
- Gourdon, Demichel (2004) : Les 10^{13} premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

La différence $\pi(x) - \mathrm{li}(x)$

- Gauss observa numériquement (jusqu'à $x = 3000000$) que $\mathrm{li}(x) > \pi(x)$.

La différence $\pi(x) - \mathrm{li}(x)$

- Gauss observa numériquement (jusqu'à $x = 3000000$) que $\mathrm{li}(x) > \pi(x)$.

Théorème (Littlewood, 1914).

La quantité $\pi(x) - \mathrm{li}(x)$ change de signe une infinité de fois.

La différence $\pi(x) - \mathrm{li}(x)$

- Gauss observa numériquement (jusqu'à $x = 3000000$) que $\mathrm{li}(x) > \pi(x)$.

Théorème (Littlewood, 1914).

La quantité $\pi(x) - \mathrm{li}(x)$ change de signe une infinité de fois.

- Stanley Skewes, étudiant de John Littlewood, détermine que le premier changement de signe se produit en un $x_S < 10^{10^{10^{963}}}$. Aujourd'hui on sait seulement que

$$10^{19} < x_S < 7 \times 10^{370}.$$

La différence $\pi(x) - \mathrm{li}(x)$

- Gauss observa numériquement (jusqu'à $x = 3000000$) que $\mathrm{li}(x) > \pi(x)$.

Théorème (Littlewood, 1914).

La quantité $\pi(x) - \mathrm{li}(x)$ change de signe une infinité de fois.

- Stanley Skewes, étudiant de John Littlewood, détermine que le premier changement de signe se produit en un $x_S < 10^{10^{10^{963}}}$. Aujourd'hui on sait seulement que

$$10^{19} < x_S < 7 \times 10^{370}.$$

Problème ouvert.

Déterminer x_S.

La conjecture de Goldbach

- La somme de deux nombres premiers (différents de 2) est paire.

La conjecture de Goldbach

- La somme de deux nombres premiers (différents de 2) est paire. Réciproquement on peut s'attendre à

Conjecture (Goldbach, 1742).

Tout nombre pair supérieur à 4 s'écrit comme la somme de deux nombres premiers.

La conjecture de Goldbach

- La somme de deux nombres premiers (différents de 2) est paire. Réciproquement on peut s'attendre à

Conjecture (Goldbach, 1742).

Tout nombre pair supérieur à 4 s'écrit comme la somme de deux nombres premiers.

- Vérification numérique jusqu'à 4×10^{18}.

La conjecture de Goldbach

- La somme de deux nombres premiers (différents de 2) est paire. Réciproquement on peut s'attendre à

Conjecture (Goldbach, 1742).

Tout nombre pair supérieur à 4 s'écrit comme la somme de deux nombres premiers.

- Vérification numérique jusqu'à 4×10^{18}.

Théorème (Chen, 1966).

Tout nombre pair suffisamment grand s'écrit comme la somme d'un nombre premier et d'un produit d'au plus deux nombres premiers.

La conjecture de Goldbach

- La somme de deux nombres premiers (différents de 2) est paire. Réciproquement on peut s'attendre à

Conjecture (Goldbach, 1742).

Tout nombre pair supérieur à 4 s'écrit comme la somme de deux nombres premiers.

- Vérification numérique jusqu'à 4×10^{18}.

Théorème (Chen, 1966).

Tout nombre pair suffisamment grand s'écrit comme la somme d'un nombre premier et d'un produit d'au plus deux nombres premiers.

- « Suffisamment grand » veut dire $\geq 1,7 \times 10^{1872344071119348}$ (Yamada, 2015).

La conjecture de Goldbach

Conjecture (Goldbach faible).

Tout nombre impair supérieur à 7 s'écrit comme la somme de trois nombres premiers.

La conjecture de Goldbach

Conjecture (Goldbach faible).

Tout nombre impair supérieur à 7 s'écrit comme la somme de trois nombres premiers.

- Goldbach ⇒ Goldbach faible (si n est impair, $n-3$ est pair).

La conjecture de Goldbach

Conjecture (Goldbach faible).

Tout nombre impair supérieur à 7 s'écrit comme la somme de trois nombres premiers.

- Goldbach ⇒ Goldbach faible (si n est impair, $n-3$ est pair).

Théorème (Vinogradov, 1937).

Tout nombre impair suffisamment grand s'écrit comme la somme de trois nombres premiers.

- « Suffisamment grand » veut dire $\geq 10^{7000000}$ (Borozdkin, 1956). En 2002, la borne était baissée à 2×10^{1346}.

La conjecture de Goldbach

Conjecture (Goldbach faible).

Tout nombre impair supérieur à 7 s'écrit comme la somme de trois nombres premiers.

- Goldbach ⇒ Goldbach faible (si n est impair, $n-3$ est pair).

Théorème (Vinogradov, 1937).

Tout nombre impair suffisamment grand s'écrit comme la somme de trois nombres premiers.

- « Suffisamment grand » veut dire $\geq 10^{7000000}$ (Borozdkin, 1956). En 2002, la borne était baissée à 2×10^{1346}.

Théorème (Helfgott, 2013).

La conjecture de Goldbach faible est vraie.

Écarts entre nombres premiers

- Il est facile de voir qu'on peut toujours trouver des nombres premiers consécutifs p et p' tels que $p' - p$ soit aussi grand que l'on veut (tous les nombres de $n! + 2$ à $n! + n$ sont composés).

Écarts entre nombres premiers

- Il est facile de voir qu'on peut toujours trouver des nombres premiers consécutifs p et p' tels que $p' - p$ soit aussi grand que l'on veut (tous les nombres de $n! + 2$ à $n! + n$ sont composés).

Problème.

Peut-on trouver un entier n tel qu'il existe une infinité de nombres premiers différant d'au plus n ?

Écarts entre nombres premiers

- Le plus petit écart possible est 2. Il se produit pour $(3, 5), (5, 7), (11, 13), (17, 19)$, etc.

Écarts entre nombres premiers

- Le plus petit écart possible est 2. Il se produit pour $(3, 5), (5, 7), (11, 13), (17, 19)$, etc.

Conjecture (des nombres premiers jumeaux).

Il existe une infinité de nombres premiers p tels que $p+2$ soit premier.

Écarts entre nombres premiers

- Le plus petit écart possible est 2. Il se produit pour $(3, 5), (5, 7), (11, 13), (17, 19)$, etc.

Conjecture (des nombres premiers jumeaux).

Il existe une infinité de nombres premiers p tels que $p+2$ soit premier.

- Il y a également une conjecture pour les nombres premiers différant de 4 (premiers cousins), de 6 (premiers sexys) etc.

Écarts entre nombres premiers

Théorème (Zhang, 2013).

Il existe une infinité de nombres premiers p et p' tels que $p' - p \leq 70000000$.

Écarts entre nombres premiers

Théorème (Zhang, 2013).

Il existe une infinité de nombres premiers p et p' tels que $p' - p \leq 70000000$.

- Avant ça, on ne savait même pas qu'il existait une infinité de nombres premiers consécutifs dont la différence est **bornée** !

Écarts entre nombres premiers

Théorème (Zhang, 2013).

Il existe une infinité de nombres premiers p et p' tels que $p' - p \leq 70000000$.

- Avant ça, on ne savait même pas qu'il existait une infinité de nombres premiers consécutifs dont la différence est **bornée** !

Théorème (Maynard, Polymath, 2014).

Il existe une infinité de nombres premiers p et p' tels que $p' - p \leq 246$.

Plan

Équations diophantiennes

Définition.

Une équation diophantienne est une équation de la forme $P(x_1, \ldots, x_n) = 0$, où P est un polynôme à coefficients entiers, dont on cherche les solutions entières (voire rationnelles).

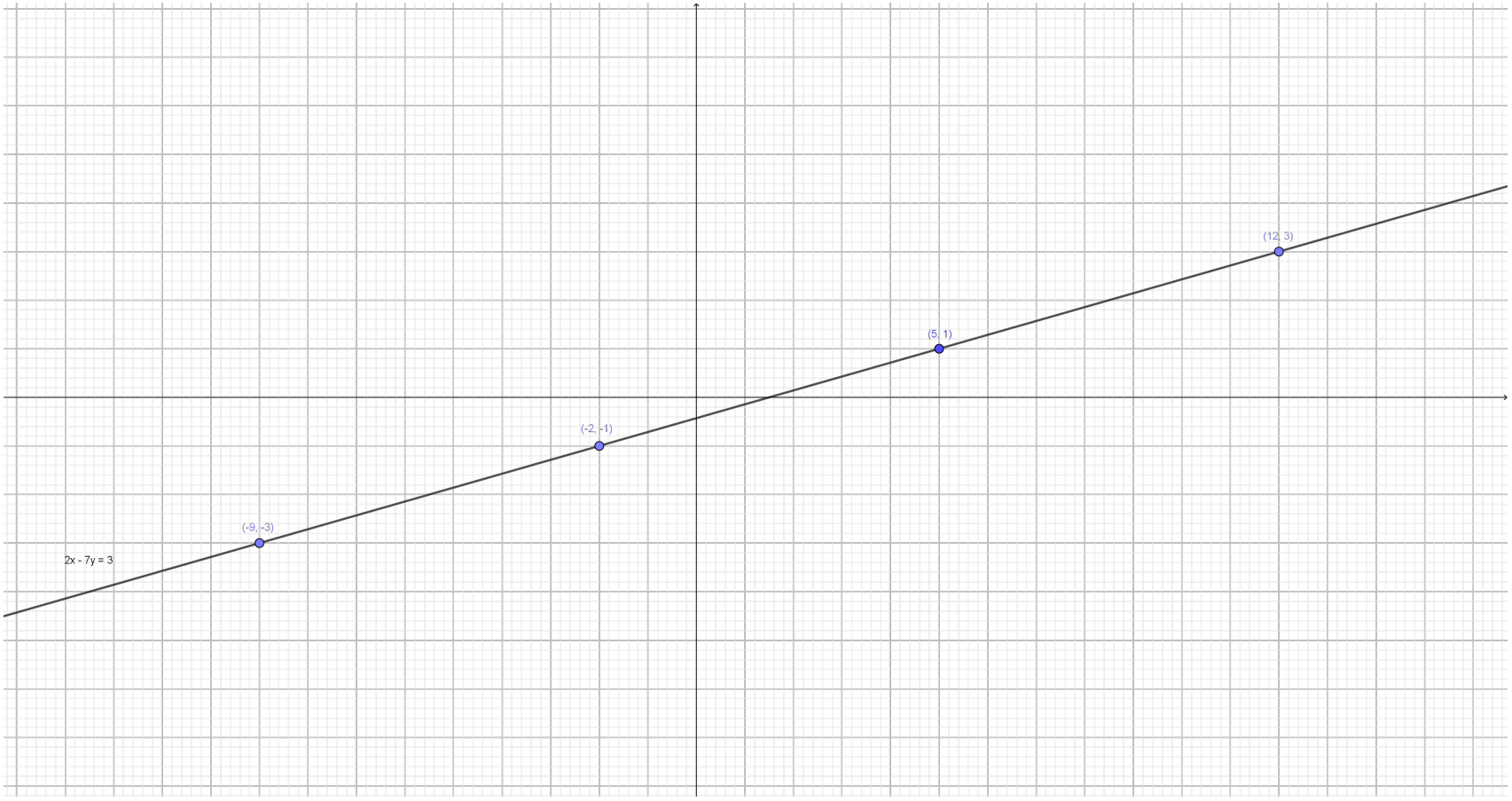
Équations diophantiennes

Définition.

Une équation diophantienne est une équation de la forme $P(x_1, \ldots, x_n) = 0$, où P est un polynôme à coefficients entiers, dont on cherche les solutions entières (voire rationnelles).

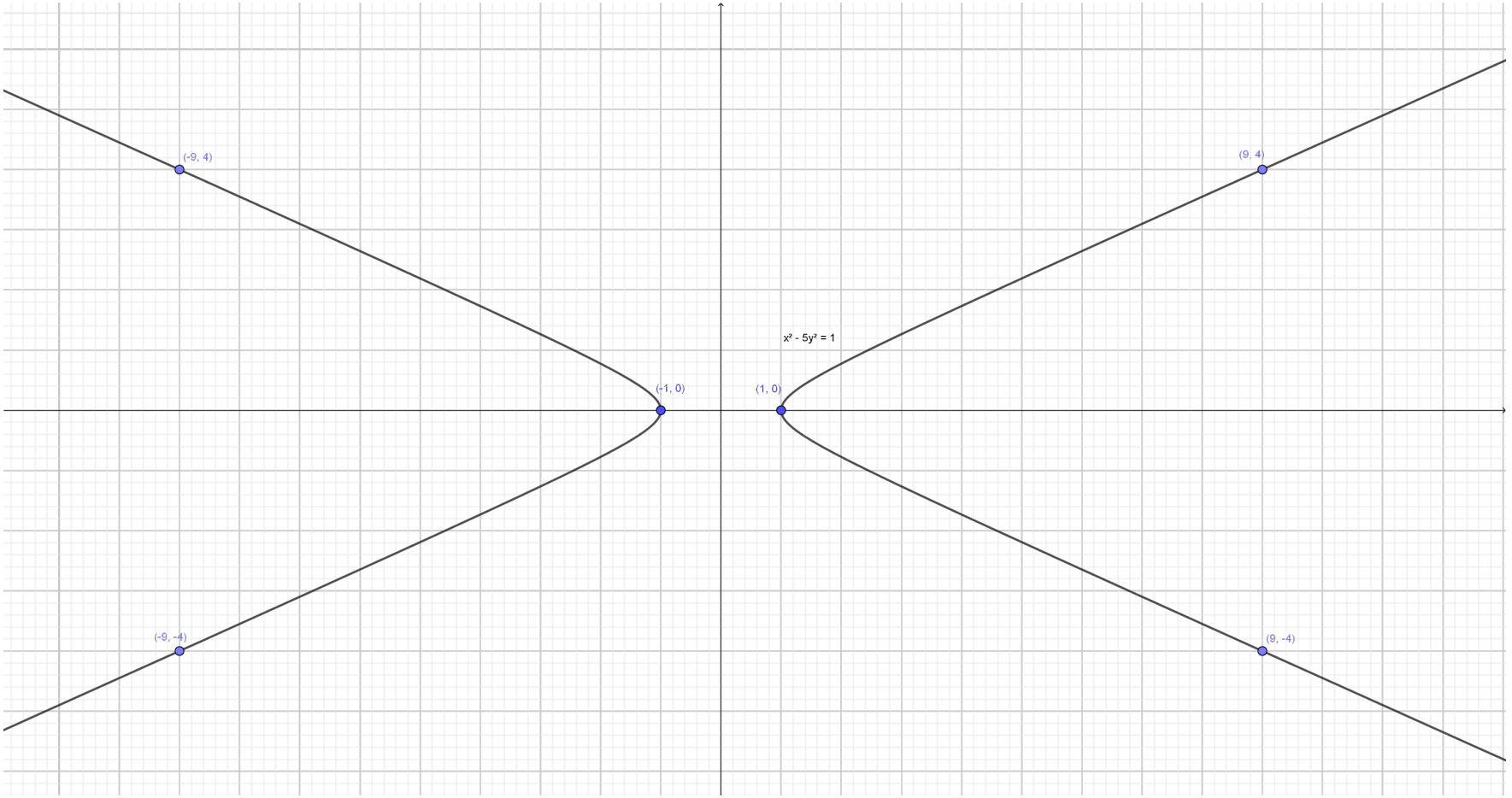
- Si $n = 2$, une équation de la forme $P(x, y) = 0$ définit une courbe dans le plan. Résoudre l'équation diophantienne $\Leftrightarrow$ trouver les points à coordonnées entières sur la courbe.

Degré 1



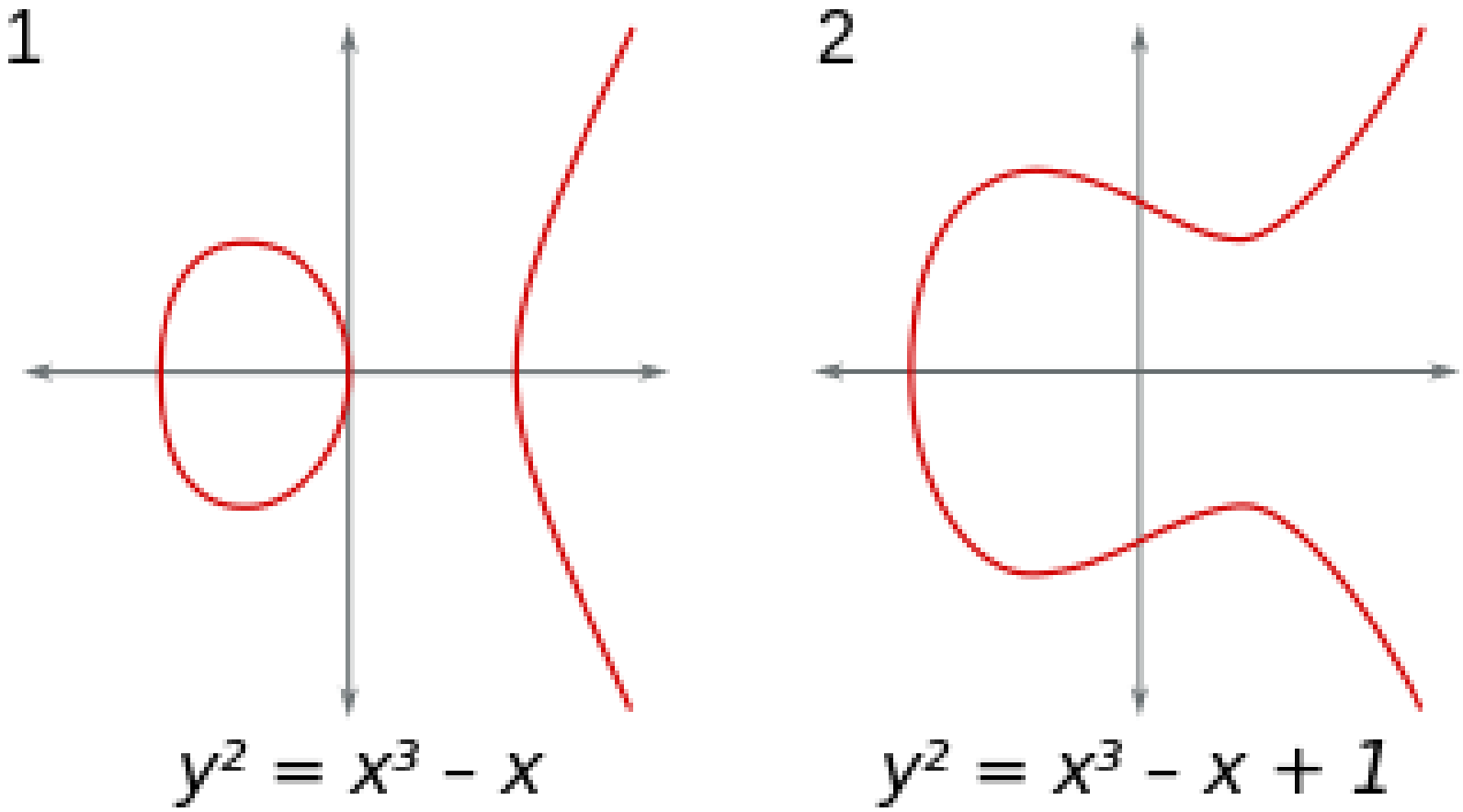
- $ax + by = c \longrightarrow$ équation de droite. Soit pas de solution, soit une infinité.

Degré 2



- (Après changement de repère) $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ (ellipse) ou $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ (hyperbole) ou $y^2 = 2px$ (parabole).

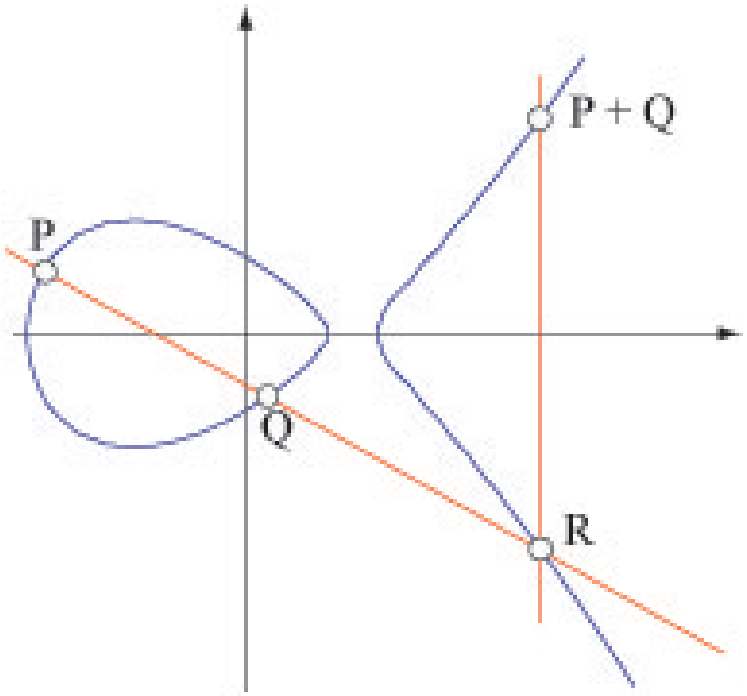
Degré 3



- (Après changement de repère) $y^2 = x^3 + ax + b \longrightarrow$ courbe elliptique.

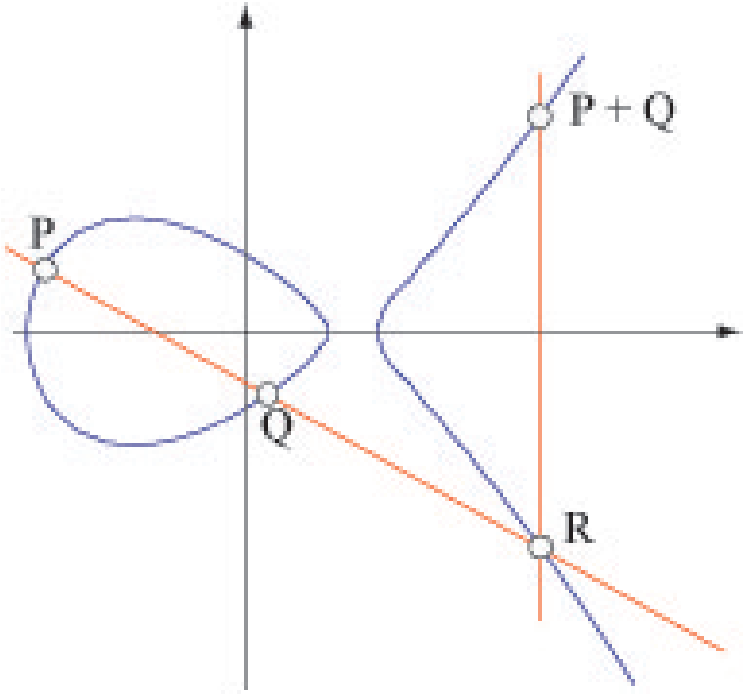
Addition sur les courbes elliptiques

- Soient $P, Q \in E$. La droite (PQ) coupe E en un troisième point R (éventuellement P, Q ou à l'infini). Si $P = Q$ on considère que (PQ) est la tangente à E en P. On définit $P + Q$ comme le symétrique de R par rapport à l'axe des abscisses.



Addition sur les courbes elliptiques

- Soient $P, Q \in E$. La droite (PQ) coupe E en un troisième point R (éventuellement P, Q ou à l'infini). Si $P = Q$ on considère que (PQ) est la tangente à E en P. On définit $P + Q$ comme le symétrique de R par rapport à l'axe des abscisses.



Théorème (Mordell, 1922).

Le groupe $E(\mathbb{Q})$ des points rationnels de E est de type fini, *i.e.* il existe un nombre fini de points rationnels $P_1, \ldots, P_r$ tels que tout point rationnel $P \in E$ peut être obtenu par le procédé de cordes et tangentes à partir de $P_1, \ldots, P_r$.

Rang des courbes elliptiques

Problème ouvert.

Existe-t-il des courbes elliptiques de rang arbitrairement grands ?

Rang des courbes elliptiques

Problème ouvert.

Existe-t-il des courbes elliptiques de rang arbitrairement grands ?

- Le plus grand rang connu est 28.

Rang des courbes elliptiques

Problème ouvert.

Existe-t-il des courbes elliptiques de rang arbitrairement grands ?

- Le plus grand rang connu est 28.
- Il est conjecturé que « la moitié » des courbes elliptiques ont rang 0, et l'autre moitié 1.

Finitude sur les courbes elliptiques

Théorème (Siegel, 1929).

Il n'existe qu'un nombre fini de points entiers sur une courbe elliptique.

Finitude sur les courbes elliptiques

Théorème (Siegel, 1929).

Il n'existe qu'un nombre fini de points entiers sur une courbe elliptique.

Théorème (Baker, ≈ 1970).

Si $y^2 = x^3 + ax + b$ avec $a, b, x, y \in \mathbb{Z}$ alors

$$\max(|x|, |y|) < e^{(10^6 H)^{10^6}},$$

où $H = \max(|a|, |b|)$.

Finitude sur les courbes elliptiques

Théorème (Siegel, 1929).

Il n'existe qu'un nombre fini de points entiers sur une courbe elliptique.

Théorème (Baker, ≈ 1970).

Si $y^2 = x^3 + ax + b$ avec $a, b, x, y \in \mathbb{Z}$ alors

$$\max(|x|, |y|) < e^{(10^6 H)^{10^6}},$$

où $H = \max(|a|, |b|)$.

Problème ouvert.

Trouver un algorithme efficace pour trouver les points entiers d'une courbe elliptique.

Courbes plus compliquées

Théorème (Faltings, 1984).

Soit $\mathcal{C}$ une courbe plane lisse de genre $g \geq 2$. Alors $\mathcal{C}$ n'a qu'un nombre fini de points **rationnels**.

Courbes plus compliquées

Théorème (Faltings, 1984).

Soit $\mathcal{C}$ une courbe plane lisse de genre $g \geq 2$. Alors $\mathcal{C}$ n'a qu'un nombre fini de points **rationnels**.

- Que se passe-t-il avec plus de variables ? !

Courbes plus compliquées

Théorème (Faltings, 1984).

Soit $\mathcal{C}$ une courbe plane lisse de genre $g \geq 2$. Alors $\mathcal{C}$ n'a qu'un nombre fini de points **rationnels**.

- Que se passe-t-il avec plus de variables ? ! La théorie des surfaces arithmétiques est loin d'être développée aujourd'hui.

Le dixième problème de Hilbert

- En 1900, David Hilbert pose 23 problèmes pour guider la recherche mathématique du XXème siècle. Le dixième problème est : « Existe-t-il un algorithme permettant de décider si une équation diophantienne admet une solution ou non ? »

Le dixième problème de Hilbert

- En 1900, David Hilbert pose 23 problèmes pour guider la recherche mathématique du XXème siècle. Le dixième problème est : « Existe-t-il un algorithme permettant de décider si une équation diophantienne admet une solution ou non ? »

Théorème (Matyiasevich, 1970).

Les ensembles diophantiens (ensembles de d'équations diophantiennes possédant une solution) sont exactement les ensembles récursivement énumérables. En particulier, le dixième problème de Hilbert n'admet pas de solution.

Le dixième problème de Hilbert

- En 1900, David Hilbert pose 23 problèmes pour guider la recherche mathématique du XXème siècle. Le dixième problème est : « Existe-t-il un algorithme permettant de décider si une équation diophantienne admet une solution ou non ? »

Théorème (Matyiasevich, 1970).

Les ensembles diophantiens (ensembles de d'équations diophantiennes possédant une solution) sont exactement les ensembles récursivement énumérables. En particulier, le dixième problème de Hilbert n'admet pas de solution.

- En particulier, l'hypothèse de Riemann est équivalente à la non existence de solutions d'une certaine équation diophantienne !

Un peu d'histoire

- Au XVIIème siècle, Pierre de Fermat lit et annote un livre de Diophante. Dans ce livre, on trouve des résultats sur les **triplets pythagoriciens** : des entiers x, y et z tels que $x^2 + y^2 = z^2$, *i.e.* des côtés entiers d'un triangle rectangle.

Un peu d'histoire

- Au XVIIème siècle, Pierre de Fermat lit et annote un livre de Diophante. Dans ce livre, on trouve des résultats sur les **triplets pythagoriciens** : des entiers x, y et z tels que $x^2 + y^2 = z^2$, *i.e.* des côtés entiers d'un triangle rectangle.

Théorème (Non daté).

Il existe une infinité de triplets d'entiers (x, y, z) tels que $x^2 + y^2 = z^2$. Les triplets solutions premiers entre eux sont, à l'ordre près de x et y, de la forme

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2.$$

Un peu d'histoire

- Fermat annote : « Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir. »

Un peu d'histoire

- Fermat annote : « Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir. »

- Personne n'a trouvé de trace de la démonstration de Fermat.

Un peu d'histoire

- Fermat annote : « Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir. »

- Personne n'a trouvé de trace de la démonstration de Fermat.

Conjecture (Grand (ou dernier) théorème de Fermat, 1637).

Soit $n \geq 3$ un entier. Il n'existe pas de triplet d'entiers non nuls (x, y, z) tel que $x^n + y^n = z^n$.

Un peu d'histoire

- Fermat annote : « Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir. »

- Personne n'a trouvé de trace de la démonstration de Fermat.

Conjecture (Grand (ou dernier) théorème de Fermat, 1637).

Soit $n \geq 3$ un entier. Il n'existe pas de triplet d'entiers non nuls (x, y, z) tel que $x^n + y^n = z^n$.

- Au début du XIXème siècle, c'est le seul résultat annoncé par Fermat dont on ne connaît pas de démonstration.

Petites valeurs de n

- Fermat prouve son théorème pour $n = 4$ à l'aide de sa méthode de « descente infinie ».

Petites valeurs de n

- Fermat prouve son théorème pour $n = 4$ à l'aide de sa méthode de « descente infinie ». Il montre que s'il existe $x, y, z > 0$ tels que $x^4 + y^4 = z^4$ alors il existe x', y', z' tels que $0 < x' < x, 0 < y' < y, 0 < z' < z$ et $(x')^4 + (y')^4 = (z')^4$.

Petites valeurs de n

- Fermat prouve son théorème pour $n = 4$ à l'aide de sa méthode de « descente infinie ». Il montre que s'il existe $x, y, z > 0$ tels que $x^4 + y^4 = z^4$ alors il existe x', y', z' tels que $0 < x' < x, 0 < y' < y, 0 < z' < z$ et $(x')^4 + (y')^4 = (z')^4$.

- Euler donne une démonstration du cas $n = 3$ en 1770. Le cas $n = 5$ est démontré par Dirichlet et Legendre vers 1825. Puis $n = 14$ (Dirichlet, 1832), $n = 7$ (Lamé, 1839), ...

Petites valeurs de n

- Fermat prouve son théorème pour $n = 4$ à l'aide de sa méthode de « descente infinie ». Il montre que s'il existe $x, y, z > 0$ tels que $x^4 + y^4 = z^4$ alors il existe x', y', z' tels que $0 < x' < x, 0 < y' < y, 0 < z' < z$ et $(x')^4 + (y')^4 = (z')^4$.

- Euler donne une démonstration du cas $n = 3$ en 1770. Le cas $n = 5$ est démontré par Dirichlet et Legendre vers 1825. Puis $n = 14$ (Dirichlet, 1832), $n = 7$ (Lamé, 1839), ...

- En fait, il suffit de démontrer le théorème pour $n = 4$ et $n = p$ premier puisque $x^{ab} = (x^a)^b$.

Quelques attaques

- Dans les années 1820, Sophie Germain trouve un critère pour montrer qu'il n'existe pas de x, y, z tels que $x^p + y^p = z^p$ et p ne divise ni x, ni y, ni z. Elle démontre que c'est le cas pour tous les nombres premiers $p < 270$.

Quelques attaques

- Dans les années 1820, Sophie Germain trouve un critère pour montrer qu'il n'existe pas de x, y, z tels que $x^p + y^p = z^p$ et p ne divise ni x, ni y, ni z. Elle démontre que c'est le cas pour tous les nombres premiers $p < 270$.

- En 1847, Gabriel Lamé prétend démontrer le théorème :

Quelques attaques

- Dans les années 1820, Sophie Germain trouve un critère pour montrer qu'il n'existe pas de x, y, z tels que $x^p + y^p = z^p$ et p ne divise ni x, ni y, ni z. Elle démontre que c'est le cas pour tous les nombres premiers $p < 270$.

- En 1847, Gabriel Lamé prétend démontrer le théorème : soit $\zeta_p = e^{\frac{2i\pi}{p}}$ une racine p-ième de l'unité (*i.e.* $\zeta_p^p = 1$).

Quelques attaques

- Dans les années 1820, Sophie Germain trouve un critère pour montrer qu'il n'existe pas de x, y, z tels que $x^p + y^p = z^p$ et p ne divise ni x, ni y, ni z. Elle démontre que c'est le cas pour tous les nombres premiers $p < 270$.

- En 1847, Gabriel Lamé prétend démontrer le théorème : soit $\zeta_p = e^{\frac{2i\pi}{p}}$ une racine p-ième de l'unité (*i.e.* $\zeta_p^p = 1$). On a

$$x^p + y^p = (x+y) \times (x+\zeta_p y) \times (x+\zeta_p^2 y) \times \cdots \times (x+\zeta_p^{p-1} y).$$

  Si tout se passe comme dans $\mathbb{Z}$, on déduit alors de l'égalité $x^p + y^p = z^p$ que chaque $x + \zeta_p^j y$ est une puissance p-ième dans

$$\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} \mid a_0, \ldots, a_{p-1} \in \mathbb{Z}\}.$$

Quelques attaques

- Joseph Liouville remarque que la démonstration de Lamé ne tient pas : dans $\mathbb{Z}[\zeta_{23}]$ il n'y a pas unicité dans la décomposition en facteurs premiers !

Quelques attaques

- Joseph Liouville remarque que la démonstration de Lamé ne tient pas : dans $\mathbb{Z}[\zeta_{23}]$ il n'y a pas unicité dans la décomposition en facteurs premiers !
- Ernst Kummer reprend la méthode de Lamé et développe la théorie algébrique des nombres.

Quelques attaques

- Joseph Liouville remarque que la démonstration de Lamé ne tient pas : dans $\mathbb{Z}[\zeta_{23}]$ il n'y a pas unicité dans la décomposition en facteurs premiers !

- Ernst Kummer reprend la méthode de Lamé et développe la théorie algébrique des nombres.

Théorème (Kummer, 1850).

Le théorème de Fermat est vrai pour les nombres premiers *réguliers*.

Quelques attaques

- Joseph Liouville remarque que la démonstration de Lamé ne tient pas : dans $\mathbb{Z}[\zeta_{23}]$ il n'y a pas unicité dans la décomposition en facteurs premiers !

- Ernst Kummer reprend la méthode de Lamé et développe la théorie algébrique des nombres.

Théorème (Kummer, 1850).

Le théorème de Fermat est vrai pour les nombres premiers *réguliers*.

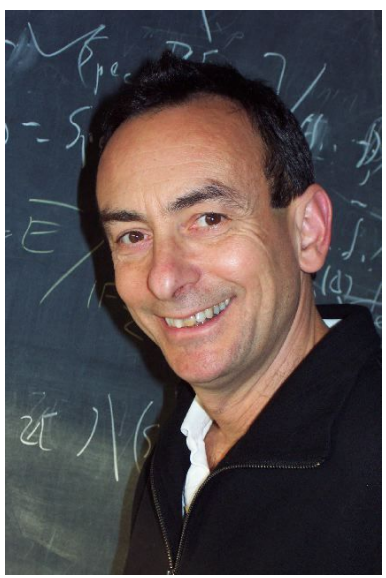
- Les seuls nombres premiers < 270 qui ne sont pas réguliers sont $37, 59, 67, 101, 103, 131, 149, 157, 233, 257$ et 263. On ne sait pas s'il existe une infinité de nombres premiers réguliers...

Fin de l'histoire

- Dans les années 80, Gerhrard Frey, Ken Ribet et Jean-Pierre Serre démontrent que si (a, b, c) est un contre-exemple au théorème de Fermat, alors la courbe elliptique d'équation

$$y^2 = x(x - a^p)(x + b^p)$$

possèderait des propriétés contredisant une conjecture profonde sur les courbes elliptiques : la conjecture de Taniyama-Shimura-Weil.

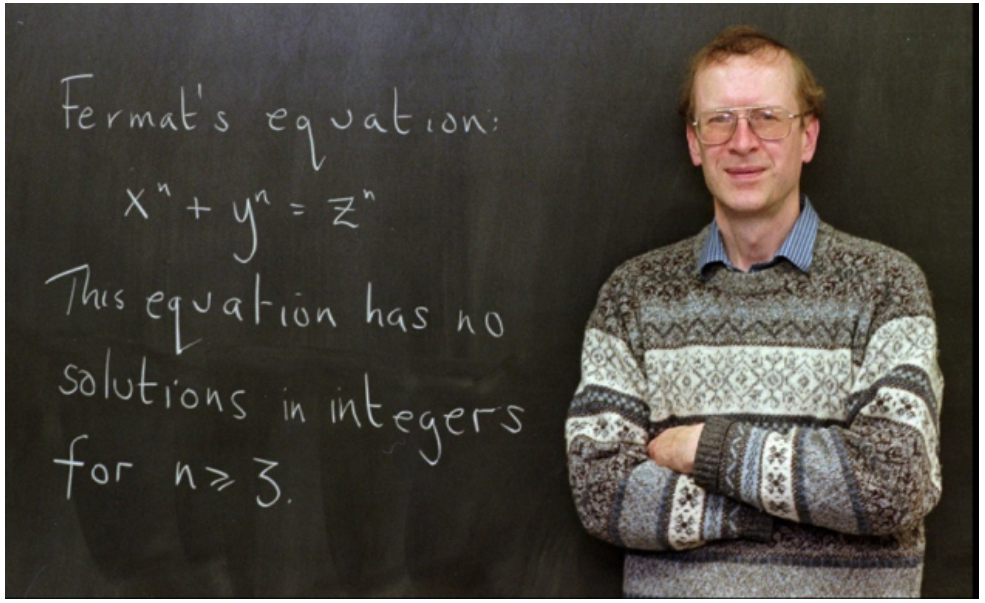




Andrew Wiles

- Le mathématicien anglais Andrew Wiles travaille dans le plus grand secret de 1987 à 1994 et annonce avoir résolu un partie de la conjecture de Taniyama-Shimura-Weil, suffisante pour impliquer le dernier théorème de Fermat.

Andrew Wiles

- Le mathématicien anglais Andrew Wiles travaille dans le plus grand secret de 1987 à 1994 et annonce avoir résolu un partie de la conjecture de Taniyama-Shimura-Weil, suffisante pour impliquer le dernier théorème de Fermat.



Théorème (Wiles, 1994*).

Le dernier théorème de Fermat est vrai !

Problèmes ouverts pour lycéens

- Il existe une infinité de nombres premiers de la forme $2^n - 1$.
- Il existe une infinité de nombres premiers de la forme $n^2 + 1$.
- Les seuls entiers $n \geq 0$ tels que $2^{2^n} + 1$ est premier sont $0, 1, 2, 3$ et 4.
- Tout nombre pair supérieur à 4 s'écrit comme la somme de deux nombres premiers.
- Il existe une infinité de nombres premiers p tels que $p + 2, p + 4, p + 6, \ldots$ soit premier.
- Il existe une infinité de nombres premiers p tels que $2p + 1$ soit premier.
- Il n'existe pas d'entier impair n tel que n soit la somme de ses diviseurs stricts.
- Trouver les solutions entières de $x^3 - 1 = (y^3 - 1)z^2$.

Merci de votre attention !