Conjecture de Goldbach (7 juin 1742)

- On note $\mathbb{P}$ l'ensemble des nombres premiers.
  $\mathbb{P} = \{p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots\}$
- *remarque* : $1 \notin \mathbb{P}$
- **Énoncé :**
  Tout entier pair supérieur à 2 est la somme de deux nombres premiers.
  $\forall n \in 2\mathbb{N}, n > 2, \exists p, q \in \mathbb{P}, n = p + q$
- La conjecture de Goldbach a été vérifiée par ordinateur jusqu'à 4.10^{18}
  (Oliveira e Silva, 4.4.2012)
- On appelle *décomposition de Goldbach* de n une telle somme $p + q$.
  p et q sont dits *décomposants de Goldbach* de n.

Reformulation

- Notons $\mathbb{P}(y) = \{x \in \mathbb{P} / x \leq y\}$

- La conjecture de Goldbach est équivalente à l'énoncé suivant :

$$\forall n \in 2\mathbb{N}, n > 4, \exists p \in \mathbb{P}(n/2), \forall m \in \mathbb{P}(\sqrt{n}), \\ p \not\equiv n \,(mod\ m)$$

- En effet,

$$\forall n \in 2\mathbb{N}, n > 4, \exists p \in \mathbb{P}(n/2), \forall m \in \mathbb{P}(\sqrt{n}), \\ p \not\equiv n \,(mod\ m) \Leftrightarrow n - p \not\equiv 0 \,(mod\ m) \Leftrightarrow n - p \text{ premier}$$

Étude d'un exemple

- *Pourquoi 19 est-il le plus petit décomposant de Goldbach de 98 ?*

$$
\begin{aligned}
98 &\equiv 3 \pmod 5\\
98 &\equiv 5 \pmod 3\\
98 &\equiv 7 \pmod 7\\
98 &\equiv 11 \pmod 3\\
98 &\equiv 13 \pmod 5\\
98 &\equiv 17 \pmod 3
\end{aligned}
$$

$$
\begin{aligned}
98 &\not\equiv 19 \pmod 3\\
98 &\not\equiv 19 \pmod 5\\
98 &\not\equiv 19 \pmod 7
\end{aligned}
$$

- *Conclusion* : $\forall m \in \mathbb{P}(\sqrt{98}),\ 19 \not\equiv 98\ (mod\ m)$
  19 est un décomposant de Goldbach de 98.
  En effet, $98 = 19 + 79$ avec 19 et 79 premiers.

Une seconde façon de représenter l'exemple proposé

- *Pourquoi 19 est-il un décomposant de Goldbach de 98 ?*

$\mathbb{Z}/3\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$			
$\mathbb{Z}/5\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	
$\mathbb{Z}/7\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$

Classe d'appartenance de 19,

Classe d'appartenance de 98.

- *Conclusion* : $\forall m \in \mathbb{P}(\sqrt{98}),\ 19 \not\equiv 98\ (mod\ m)$
  19 est un décomposant de Goldbach de 98.
  En effet, $98 = 19 + 79$ avec 19 et 79 premiers.

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la conjecture de Goldbach

$(\exists x \in 2\mathbb{N},\ x \geq 20, x$ *ne vérifie pas la conjecture de Goldbach*$)$
$\Rightarrow$ *false*

mais
$\exists x \in 2\mathbb{N},\ x \geq 20, x$ *ne vérifie pas la conjecture de Goldbach*

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),$
x-p composé

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),$
$x\text{-}p \equiv 0\ (mod\ m)$

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),$
$x \equiv p\ (mod\ m)$

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la conjecture de Goldbach.

- Un nombre pair x ne vérifie pas la conjecture de Goldbach si et seulement si tout nombre premier impair p inférieur à sa moitié lui est congru selon un module premier impair m inférieur à sa racine.

- $$\exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),\ x \equiv p\ (mod\ m)$$

Descente infinie de Fermat

- Elle consiste à démontrer que si un nombre ne vérifiait pas la conjecture de Goldbach, il y en aurait un plus petit qui ne la vérifierait pas non plus

  (et ainsi de proche en proche, jusqu'à atteindre des nombres si petits qu'on sait qu'ils vérifient la conjecture).

- La descente infinie repose sur le fait qu'il n'existe pas de suite infinie strictement décroissante d'entiers naturels.

- Raisonnement par l'absurde :
  - on suppose que x est le plus petit entier tel que $P(x)$.
  - on montre qu'alors $P(x')$ avec $x' < x$.
  - on a abouti à une contradiction.

  (Si $P(n)$ pour un entier naturel n donné, il existe une partie non vide de $\mathbb{N}$ contenant un élément qui vérifie la propriété P. Cette partie admet un plus petit élément. En l'occurrence, la propriété P consiste à ne pas vérifier la conjecture de Goldbach)

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la conjecture de Goldbach.

- x est le nombre pair dont on considère au début de la démonstration qu'il est le plus entier naturel ne vérifiant pas la conjecture de Goldbach ;

- $\exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),$
  $x \equiv p\ (mod\ m)$

- x ne peut de toute façon être congru à aucun nombre premier selon tout module qui divise x donc $m \nmid x$.

- x est congru à un certain nombre (éventuellement nul) de nombres premiers selon le module 3, à un certain nombre (éventuellement nul) de nombres premiers selon le module 5, etc.

Descente infinie de Fermat

- x est congru à chaque nombre premier impair inférieur à sa moitié selon un certain module premier impair inférieur à sa racine.
- On partage l'ensemble des nombres premiers impairs $\mathbb{P}(x/2)$ en sous-ensembles disjoints dont l'union est l'ensemble total et tels que chaque sous-ensemble contient des nombres premiers impairs congrus à x selon un même module premier impair.
- $\mathbb{P}(x/2) = E_{x,m_1} \cup E_{x,m_2} \cup \ldots \cup E_{x,m_i}$
- où $E_{i,j} = \{p \text{ premier impair}, \ p \leq i/2 \text{ et } p \equiv i \ (mod\ j)\}$

Descente infinie de Fermat

- Considérons maintenant un nombre pair $x' = x - 2.\prod m_i$ inférieur strictement à x et congru à x selon tous les modules premiers impairs m_i inférieurs à $\sqrt{x}$.

- Il faudrait être capable de démontrer que par soustraction d'une primorielle, si x ne vérifiait pas Goldbach, x' ne la vérifierait pas non plus.

Conclusion

- On a utilisé un *Système de NUmération par les Restes dans les Parties Finies de* $\mathbb{N}$.

- On se situe dans le cadre d'une *théorie lexicale des nombres*, qui associe à un nombre un mot dont les lettres sont certains de ses restes modulaires selon des modules premiers.