Conjecture de Goldbach (7 juin 1742)

- On note $\mathbb{P}^*$ l'ensemble des nombres premiers impairs.
  $\mathbb{P}^* = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\}$

Énoncé :

$$\begin{gathered}\forall n \in 2\mathbb{N}\backslash\{0,2,4\},\\ \exists p \in \mathbb{P}^*,\ p \leq n/2,\\ \exists q \in \mathbb{P}^*,\ q \geq n/2,\\ n = p + q\end{gathered}$$

- 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 :

$$\forall n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists p \in \mathbb{P}^*(n/2),\ \forall m \in \mathbb{P}^*(\sqrt{n}),\\ p \not\equiv n\ (mod\ m)$$

- En effet,

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

Étude d'exemples : exemple 1

- *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 voir l'exemple 1

- *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.

Étude d'exemples : exemple 2

- *On cherche les décomposants de Goldbach d'entiers naturels pairs qui sont*

  $\equiv 2\ (mod\ 3)$ *et* $\equiv 3\ (mod\ 5)$ *et* $\equiv 3\ (mod\ 7)$.

- Ces nombres dont on cherche des décomposants de Goldbach sont des entiers naturels de la forme $210k + 38$ (établi par le théorème des restes chinois comme on le verra plus loin).

- On a vu que des nombres premiers impairs p qui sont

  $\not\equiv 2\ (mod\ 3)$ et $\not\equiv 3\ (mod\ 5)$ et $\not\equiv 3\ (mod\ 7)$

  peuvent être des décomposants de Goldbach de ces nombres.

- Si on omet le cas des "petits nombres premiers"

  (i.e. les cas de congruence à 0 selon un module et un seul),

  - p doit être $\equiv 1\ (mod\ 3)$.
  - p doit être $\equiv 1$ *ou* 2 *ou* $4\ (mod\ 5)$.
  - p doit être $\equiv 1$ *ou* 2 *ou* 4 *ou* 5 *ou* $6\ (mod\ 7)$.

Étude d'exemples : exemple 2

- *On cherche les décomposants de Goldbach de certains entiers naturels pairs*

$$\equiv 2\ (mod\ 3)\ \textit{et} \equiv 3\ (mod\ 5)\ \textit{et} \equiv 3\ (mod\ 7)$$

($\Leftrightarrow$ de la forme $210k + 38$)

- En combinant les différentes possibilités, on obtient :

$1\ (\text{mod}\ 3)$ et $1\ (\text{mod}\ 5)$ et $1\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $1\ (\text{mod}\ 5)$ et $2\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $1\ (\text{mod}\ 5)$ et $4\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $1\ (\text{mod}\ 5)$ et $5\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $1\ (\text{mod}\ 5)$ et $6\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $2\ (\text{mod}\ 5)$ et $1\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $2\ (\text{mod}\ 5)$ et $2\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $2\ (\text{mod}\ 5)$ et $4\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $2\ (\text{mod}\ 5)$ et $5\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $2\ (\text{mod}\ 5)$ et $6\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $4\ (\text{mod}\ 5)$ et $1\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $4\ (\text{mod}\ 5)$ et $2\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $4\ (\text{mod}\ 5)$ et $4\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $4\ (\text{mod}\ 5)$ et $5\ (\text{mod}\ 7)$
$1\ (\text{mod}\ 3)$ et $4\ (\text{mod}\ 5)$ et $6\ (\text{mod}\ 7)$

Étude d'exemples : exemple 2

- *On cherche les décomposants de Goldbach de certains entiers naturels pairs*

$$\equiv 2\ (mod\ 3)\ et \equiv 3\ (mod\ 5)\ et \equiv 3\ (mod\ 7)$$

($\Leftrightarrow$ de la forme $210k + 38$)

- En combinant les différentes possibilités, on obtient :

1	(mod	3)	et	1	(mod	5)	et	1	(mod	7)	→	210k+1
1	(mod	3)	et	1	(mod	5)	et	2	(mod	7)	→	210k+121
1	(mod	3)	et	1	(mod	5)	et	4	(mod	7)	→	210k+151
1	(mod	3)	et	1	(mod	5)	et	5	(mod	7)	→	210k+61
1	(mod	3)	et	1	(mod	5)	et	6	(mod	7)	→	210k+181
1	(mod	3)	et	2	(mod	5)	et	1	(mod	7)	→	210k+127
1	(mod	3)	et	2	(mod	5)	et	2	(mod	7)	→	210k+37
1	(mod	3)	et	2	(mod	5)	et	4	(mod	7)	→	210k+67
1	(mod	3)	et	2	(mod	5)	et	5	(mod	7)	→	210k+187
1	(mod	3)	et	2	(mod	5)	et	6	(mod	7)	→	210k+97
1	(mod	3)	et	4	(mod	5)	et	1	(mod	7)	→	210k+169
1	(mod	3)	et	4	(mod	5)	et	2	(mod	7)	→	210k+79
1	(mod	3)	et	4	(mod	5)	et	4	(mod	7)	→	210k+109
1	(mod	3)	et	4	(mod	5)	et	5	(mod	7)	→	210k+19
1	(mod	3)	et	4	(mod	5)	et	6	(mod	7)	→	210k+139

Étude d'exemples : exemple 2

- *Voici quelques exemples de décomposants de Goldbach appartenant aux progressions arithmétiques trouvées pour quelques nombres de la progression arithmétique* $210k + 38$

- 248 : 7 19 37 67 97 109
  458 : 19 37 61 79 109 127 151 181 229 (2p)
  668 : 7 37 61 67 97 127 181 211 229 271 331
  878 : 19 67 109 127 139 151 271 277 307 331 337 379 421 439 (2p)
  1088 : 19 37 67 79 97 151 181 211 229 277 331 337 349 379 397 457 487 541
  1298 : 7 19 61 67 97 127 181 211 229 277 307 331 379 421 439 487 541 547 571 607

- Pas de surprise pour $n = 248,\ 458,\ 668,\ 878,\ 1088$ et 1298 : tout nombre premier inférieur à $n/2$ et non congru à n selon tout module premier impair inférieur à $\sqrt{n}$ est un décomposant de Goldbach de n.

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.

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

- $\exists x \in 2\mathbb{N},\ x \geq 20,$
  $\forall p_1, \ldots, p_k \in \mathbb{P}^*(x/2), \exists m_{j_1}, \ldots, m_{j_k} \in \mathbb{P}^*(\sqrt{x}).$

$$\mathcal{S} \begin{cases} x \equiv p_1\ (mod\ m_{j_1}) \\ x \equiv p_2\ (mod\ m_{j_2}) \\ \ldots \\ x \equiv p_k\ (mod\ m_{j_k}) \end{cases}$$

- **Note** : les modules m_{j_i} sont des modules premiers impairs qui peuvent être égaux.

Rappel : descente infinie de Fermat

- 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.

- 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)

Rappel : on cherche à aboutir à une contradiction à partir de l'hypothèse :

$\exists x \in 2\mathbb{N}$, $x \geq 20$, *tel que*
$\forall p_1, \ldots, p_k \in \mathbb{P}^*(x/2)$, $\exists m_{j_1}, \ldots, m_{j_k} \in \mathbb{P}^*(\sqrt{x})$.

- $$\mathcal{S} \begin{cases} x \equiv p_1 \ (mod \ m_{j_1}) \\ x \equiv p_2 \ (mod \ m_{j_2}) \\ \ldots \\ x \equiv p_k \ (mod \ m_{j_k}) \end{cases}$$

- x n'est congru à aucun nombre premier selon tout module qui divise 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.
- Il faut démontrer qu'il existe forcément deux modules selon lesquels x est congru à un entier naturel différent.

Rappels

- On appelle congruence canonique une congruence de la forme $x \equiv a\ (mod\ m)$ avec $a < m$ (par exemple, $x \equiv 3\ (mod\ 5)$ est une congruence canonique alors que $x \equiv 8\ (mod\ 5)$ n'en est pas une).

- Le plus petit entier naturel vérifiant une congruence canonique de la forme $x \equiv a\ (mod\ m)$ est a.

- Deux congruences $x \equiv a\ (mod\ m)$ et $x \equiv b\ (mod\ n)$ ont un même plus petit entier naturel les vérifiant si et seulement si $a = b$.

Exemples

- $$\begin{cases} x \equiv 2\ (mod\ 3) & \rightarrow 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38 \\ x \equiv 3\ (mod\ 5) & \rightarrow 3, 8, 13, 18, 23, 28, 33, 38, 43, 48 \end{cases}$$
  $$\overline{\qquad\qquad\qquad\qquad}$$
  $$x \equiv 8\ (mod\ 15)$$

$$\begin{cases} x \equiv 2\ (mod\ 3) & \rightarrow 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38 \\ x \equiv 2\ (mod\ 5) & \rightarrow 2, 7, 12, 17, 22, 27, 32, 37, 42, 47 \end{cases}$$
$$\overline{\qquad\qquad\qquad\qquad}$$
$$x \equiv 2\ (mod\ 15)$$

Utilitaire : solutions minimales de systèmes de congruences

$$\mathcal{S}\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 1\ (mod\ 3) \\ x \equiv 4\ (mod\ 5) \\ x \equiv 5\ (mod\ 7) \\ x \equiv 6\ (mod\ 11) \\ x \equiv 3\ (mod\ 13) \end{cases}$$

sol.min.	2	3	5	7	11	13
21544	0	1	4	5	6	3
754	0	1	4	5	6	×
2434	0	1	4	5	×	3
124	0	1	4	5	×	×
94	0	1	4	×	6	3
94	0	1	4	×	6	×
94	0	1	4	×	×	3
4	0	1	4	×	×	×
3526	0	1	×	5	6	3
292	0	1	×	5	6	×
250	0	1	×	5	×	3
40	0	1	×	5	×	×
94	0	1	×	×	6	3
28	0	1	×	×	6	×
16	0	1	×	×	×	3
4	0	1	×	×	×	×

sol.min.	2	3	5	7	11	13
1524	0	×	4	5	6	3
754	0	×	4	5	6	×
614	0	×	4	5	×	3
54	0	×	4	5	×	×
94	0	×	4	×	6	3
94	0	×	4	×	6	×
94	0	×	4	×	×	3
4	0	×	4	×	×	×
1524	0	×	×	5	6	3
138	0	×	×	5	6	×
68	0	×	×	5	×	3
12	0	×	×	5	×	×
94	0	×	×	×	6	3
6	0	×	×	×	6	×
16	0	×	×	×	×	3
×	0	×	×	×	×	×

Utilitaire : solutions minimales de systèmes de congruences

- On passe de la solution n du système contenant toutes les congruences à une solution n' d'un système inclus en soustrayant un multiple le plus grand possible d'un produit de nombres premiers.
- Par exemple, $21544 - 3526 = 18018 = 2.3^2.7.11.13$.
- Il faudrait être capable de démontrer que, par une telle soustraction d'un multiple de primorielle, si un nombre ne vérifiait pas Goldbach, un nombre plus petit ne la vérifierait pas non plus.

Descente infinie de Fermat

	m_1	m_2	$\dots$	m_i	$\dots$	m_k	
p_1	r_1						
p_2		r_2					
$\vdots$							
p_i				r_i			
$\vdots$							
p_k						r_k	
$\vdots$							
$x - \prod m_i$	r_1	r_2	$\dots$	r_i			*ne vérifie pas CG*
$\vdots$							
x	r_1	r_2	$\dots$	r_i	$\dots$	r_k	*ne vérifie pas CG*

Descente infinie de Fermat

- 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 ;
- les $p_1, p_2, \ldots, p_k$ sont les nombres premiers impairs inférieurs à la moitié de x ;
- s'en déduisent les modules $m_1, m_2, \ldots, m_k$ selon lesquels x est congru aux différents p_i ; même si plusieurs colonnes peuvent avoir le même entête, on les a distinguées pour faciliter l'écriture du tableau de restes ;
- $x - \prod m_i$ est l'entier naturel strictement plus petit que x dont il faut s'assurer qu'il ne vérifie pas non-plus la conjecture de Goldbach de façon à "descendre" une marche de Fermat.
- $x - \prod m_i$ a les mêmes restes que x selon chacun des m_i intervenant dans le produit.

Étude d'exemples : exemple 3

- Recherche de décomposants de Goldbach de $n = 38$.

- *Première étape* : élimination :

  1) des "petits" nombres premiers qui sont inférieurs à $\sqrt{n}$ (qui pourraient parfois être des décomposants de Goldbach de n mais on cherche à démontrer qu'il existe toujours des décomposants de Goldbach de n non-compris ceux-là)

  2) des nombres composés dont un diviseur est un nombre premier inférieur à $\sqrt{n}$

- Pour cela, on élimine tout nombre qui a un reste égal à 0 selon l'un des modules inférieurs à $\sqrt{n}$).

Étude d'exemples : exemple 3

-

mod	3	5	
1	1	1	
3	⓪	3	*
5	2	⓪	*
7	1	2	
9	⓪	4	*
11	2	1	
13	1	3	
15	⓪	⓪	*
17	2	2	
19	1	4	
38	2	3	

Étude d'exemples : exemple 3

- *Deuxième étape* : élimination des nombres congrus à n selon un module premier inférieur à $\sqrt{n}$.
-

mod	3	5	
1	1	1	
3	0	③	*
5	②	0	*
7	1	2	
9	0	4	
11	②	1	*
13	1	③	*
15	0	0	
17	②	2	*
19	1	4	
38	2	3	

Étude d'exemples : exemple 3

- Une propriété découlant de la théorie des congruences : il y a autant de nombres congrus à n $(mod\ p_k)$ sur l'intervalle $(1, n/2)$ que de nombres divisibles par p_k sur cet intervalle.

- Note : le nombre 3, divisible par 3 d'une part, et partageant son reste dans la division par 5 avec 38 d'autre part, est éliminé lors des deux étapes. Le nombre 5, divisible par 5 d'une part, et partageant son reste dans la division par 3 avec 38 d'autre part, est également éliminé lors des deux étapes.

Minoration du nombre de décompositions de Goldbach

- On note x mod p le reste de la division de x par p.
- De 1 à x, il y a $\left\lfloor \frac{x}{p} \right\rfloor$ nombres congrus à 0 $(mod\ p)$.
- Et si $2x \not\equiv 0\ (mod\ p)$, de 1 à x,

  - il y a $\left\lfloor \frac{x}{p} \right\rfloor$ nombres congrus à $2x\ (mod\ p)$

  $$\Leftrightarrow\ x \bmod p < \tfrac{p-1}{2}\ ;$$

  - il y a $\left\lfloor \frac{x}{p} \right\rfloor + 1$ nombres congrus à $2x\ (mod\ p)$

  $$\Leftrightarrow\ x \bmod p > \tfrac{p-1}{2}.$$

- Problème : on ne sait pas comment combiner ces quantités de nombres déterminées selon chaque module.

Minoration du nombre de décomposants de Goldbach

- Il semblerait alors qu'on puisse minorer le nombre de décomposants de Goldbach d'un nombre pair donné en appliquant la fonction π de comptage des nombres premiers à $\pi(\frac{n+2}{4})$.

- La première application de la fonction π étant destinée à éliminer de l'intervalle $[1, n/2]$ les nombres composés (ainsi que les petits premiers)

- La deuxième application de la fonction π servant quant à elle à éliminer les nombres congrus à n parmi les nombres restants.

Minoration du nombre de décomposants de Goldbach

- Il semblerait que l'application réitérée de la fonction π qui compte le nombre de nombres premiers inférieurs à n permette de minorer le nombre de décomposants de Goldbach pour les nombres pairs doubles de nombres premiers

- Cas des nombres pairs doubles de nombres premiers :

n	$n/2$	$\frac{n+2}{4}$	$\pi(\frac{n+2}{4})$	$\pi(\pi(\frac{n+2}{4}))$	$NbDG(n)$
202	101	51	15	6	9
2 018	1 009	505	96	24	28
20 014	10 007	5 004	670	121	174
200 006	100 003	50 002	5 133	685	1 071
2 000 006	1 000 003	500 002	41 538	4 343	7 336
20 000 038	10 000 019	5 000 010	348 513	29 859	53 269

Minoration du nombre de décomposants de Goldbach

- Voyons maintenant le nombre de décomposants de Goldbach pour les nombres pairs doubles de nombres composés.
- Le double d'un nombre composé doit avoir plus de décomposants de Goldbach que tout double de nombre premier qui le divise.
- En ce qui concerne les doubles de nombres composés, le pair n ayant plusieurs restes nuls, davantage de nombres sont éliminés à la fois par les deux étapes, ce qui fait forcément éliminer moins de nombres que dans le cas des pairs doubles de nombres premiers.
- L'écart entre le nombre obtenu et le nombre de décomposants de Goldbach est encore plus grand que pour les doubles de nombres premiers.

Minoration du nombre de décomposants de Goldbach

- Cas des nombres pairs doubles de nombres composés :

n	$\pi(n/4)$	$\pi(\pi(n/4))$	$\pi(n/2)$	$\pi(\pi(n/2))$	$NbDG(n)$
10^2	9	4	15	6	6
10^3	53	16	95	24	28
10^4	367	73	669	121	127
10^5	2 762	402	5 133	685	810
10^6	22 044	2 470	41 538	4 343	5 402
10^7	183 072	16 589	348 513	29 859	38 807
10^8	1 565 927	118 784	3 001 134	216 890	291 400

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*, selon laquelle *"les nombres sont des mots"*.