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 3

- *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 :

$1\ (\text{mod}\ 3)$ 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 3

- *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 3

- *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.

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

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

$$\mathcal{S}_0 \begin{cases} x \equiv p_1\ (mod\ m_{j_1}) \\ x \equiv p_2\ (mod\ m_{j_2}) \\ \ldots \\ x \equiv p_k\ (mod\ m_{j_k}) \end{cases}$$

- **Note** : les modules m_{j_i} sont des modules premiers impairs qui ne sont pas forcément tous différents.

Intermède : le théorème des restes chinois

- On appelle progression arithmétique un ensemble d'entiers naturels de la forme $ax + b$ avec $a \in \mathbb{N}^*$, $b \in \mathbb{N}$ et $x \in \mathbb{N}$.

- Un système de congruences de modules premiers entre eux 2 à 2 se résout par le théorème des restes chinois.

- Le théorème des restes chinois établit un isomorphisme entre $\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ et $\mathbb{Z}/\prod_{i=1}^{k} m_i\mathbb{Z}$
si et seulement les m_i sont deux à deux premiers entre eux.

  $(\forall m_i \in \mathbb{N}^*, \forall m_j \in \mathbb{N}^*, (m_i, m_j) = 1)$

- Le théorème des restes chinois établit une surjection
entre l'ensemble des systèmes de congruences de modules premiers entre eux 2 à 2
et l'ensemble des progressions arithmétiques.

Intermède : application du théorème des restes chinois

- On cherche l'ensemble des solutions du systèmes de congruences S suivant :

$$\begin{cases} x \equiv r_1 \ (mod \ m_1) \\ x \equiv r_2 \ (mod \ m_2) \\ \dots \\ x \equiv r_k \ (mod \ m_k) \end{cases}$$

- Les modules sont premiers entre eux 2 à 2.
- Posons $M = \prod_{i=1}^{k} m_i$.
- Calculons $M_1 = M/m_1, M_2 = M/m_2, \dots, M_k = M/m_k$.
- Soient $d_1, d_2, \dots, d_k$ tels que

$$\begin{cases} d_1.M_1 \equiv 1 \ (mod \ m_1) \\ d_2.M_2 \equiv 1 \ (mod \ m_2) \\ \dots \\ d_k.M_k \equiv 1 \ (mod \ m_k) \end{cases}$$

- La solution de S est $\boxed{x \equiv \Sigma_{i=1}^{k} r_i.d_i.M_i \ (mod \ M)}$

Intermède : le théorème des restes chinois

- Cherchons à résoudre le système de congruences :

$$\begin{cases} x \equiv 1 \ (mod\ 3) \\ x \equiv 3 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \end{cases}$$

- On pose $M = 3.5.7 = 105$.

$$\begin{array}{lll} M_1 = M/3 = 105/3 = 35 & 35.y_1 \equiv 1 \ (mod\ 3) & y_1 = 2 \\ M_2 = M/5 = 105/5 = 21 & 21.y_2 \equiv 1 \ (mod\ 5) & y_2 = 1 \\ M_3 = M/7 = 105/7 = 15 & 15.y_3 \equiv 1 \ (mod\ 7) & y_3 = 1 \end{array}$$

$$\begin{aligned} x &\equiv r_1.M_1.y_1 + r_2.M_2.y_2 + r_3.M_3.y_3 \\ &\equiv 1.35.2 + 3.21.1 + 5.15.1 = 70 + 63 + 75 = 208 = 103 \ (mod\ 105) \end{aligned}$$

qui sont les nombres de la suite : $103, 208, 313, \ldots$
i.e. de la progression arithmétique : $105k + 103$

Intermède : le théorème des restes chinois

- Si on avait eu à résoudre presque le même système, mais avec une congruence en moins :

$$\begin{cases} x \equiv 3 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \end{cases}$$

- On pose $M' = 5.7 = 35$.

$$M'_1 = M'/5 = 7 \qquad 7.y'_1 \equiv 1 \ (mod\ 5) \qquad y'_1 = 3$$
$$M'_2 = M'/7 = 5 \qquad 5.y'_2 \equiv 1 \ (mod\ 7) \qquad y'_2 = 3$$

$$\begin{aligned} x &\equiv r'_1.M'_1.y'_1 + r'_2.M'_2.y'_2 \\ &\equiv 3.3.7 + 5.3.5 = 63 + 75 = 138 = 33 \ (mod\ 35) \end{aligned}$$

qui sont les nombres de la suite :

33, 68, 103, 138, 173, 208, 243, ...

i.e. de la progression arithmétique : 35k+33

- *Conclusion :* la progression arithmétique obtenue contient la progression arithmétique trouvée par le système de congruences impliquant de la page précédente.

Intermède : rappels

- Une progression arithmétique étant une partie de $\mathbb{N}$ admet un plus petit élément. On choisira dans la suite d'associer à une progression arithmétique son plus petit entier naturel.

- Quelles sont les solutions obtenues par le théorème des restes chinois ?

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$$

$(0,0) \mapsto 0$	
$(0,1) \mapsto 6$	
$(0,2) \mapsto 12$	
$(0,3) \mapsto 3$	
$(0,4) \mapsto 9$	
$(1,0) \mapsto 10$	
$(1,1) \mapsto 1$	
$(1,2) \mapsto 7$	
$(1,3) \mapsto 13$	
$(1,4) \mapsto 4$	
$(2,0) \mapsto 5$	
$(2,1) \mapsto 11$	
$(2,2) \mapsto 2$	
$(2,3) \mapsto 8$	
$(2,4) \mapsto 14$	

Intermède : observons plus finement la bijection *trc* intervenant dans le théorème des restes chinois

- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/105\mathbb{Z}$

$(0,0,0) \mapsto 0$	$(0,1,0) \mapsto 21$	$(0,2,0) \mapsto 42$	$(0,3,0) \mapsto 63$	$(0,4,0) \mapsto 84$
$(0,0,1) \mapsto 15$	$(0,1,1) \mapsto 36$	$(0,2,1) \mapsto 57$	$(0,3,1) \mapsto 78$	$(0,4,1) \mapsto 99$
$(0,0,2) \mapsto 30$	$(0,1,2) \mapsto 51$	$(0,2,2) \mapsto 72$	$(0,3,2) \mapsto 93$	$(0,4,2) \mapsto 9$
$(0,0,3) \mapsto 45$	$(0,1,3) \mapsto 66$	$(0,2,3) \mapsto 87$	$(0,3,3) \mapsto 3$	$(0,4,3) \mapsto 24$
$(0,0,4) \mapsto 60$	$(0,1,4) \mapsto 81$	$(0,2,4) \mapsto 102$	$(0,3,4) \mapsto 18$	$(0,4,4) \mapsto 39$
$(0,0,5) \mapsto 75$	$(0,1,5) \mapsto 96$	$(0,2,5) \mapsto 12$	$(0,3,5) \mapsto 33$	$(0,4,5) \mapsto 54$
$(0,0,6) \mapsto 90$	$(0,1,6) \mapsto 6$	$(0,2,6) \mapsto 27$	$(0,3,6) \mapsto 48$	$(0,4,6) \mapsto 69$
$(1,0,0) \mapsto 70$	$(1,1,0) \mapsto 91$	$(1,2,0) \mapsto 7$	$(1,3,0) \mapsto 28$	$(1,4,0) \mapsto 49$
$(1,0,1) \mapsto 85$	$(1,1,1) \mapsto 1$	$(1,2,1) \mapsto 22$	$(1,3,1) \mapsto 43$	$(1,4,1) \mapsto 64$
$(1,0,2) \mapsto 100$	$(1,1,2) \mapsto 16$	$(1,2,2) \mapsto 37$	$(1,3,2) \mapsto 58$	$(1,4,2) \mapsto 79$
$(1,0,3) \mapsto 10$	$(1,1,3) \mapsto 31$	$(1,2,3) \mapsto 52$	$(1,3,3) \mapsto 73$	$(1,4,3) \mapsto 94$
$(1,0,4) \mapsto 25$	$(1,1,4) \mapsto 46$	$(1,2,4) \mapsto 67$	$(1,3,4) \mapsto 88$	$(1,4,4) \mapsto 4$
$(1,0,5) \mapsto 40$	$(1,1,5) \mapsto 61$	$(1,2,5) \mapsto 82$	$(1,3,5) \mapsto 103$	$(1,4,5) \mapsto 19$
$(1,0,6) \mapsto 55$	$(1,1,6) \mapsto 76$	$(1,2,6) \mapsto 97$	$(1,3,6) \mapsto 13$	$(1,4,6) \mapsto 34$
$(2,0,0) \mapsto 35$	$(2,1,0) \mapsto 56$	$(2,2,0) \mapsto 77$	$(2,3,0) \mapsto 98$	$(2,4,0) \mapsto 14$
$(2,0,1) \mapsto 50$	$(2,1,1) \mapsto 71$	$(2,2,1) \mapsto 92$	$(2,3,1) \mapsto 8$	$(2,4,1) \mapsto 29$
$(2,0,2) \mapsto 65$	$(2,1,2) \mapsto 86$	$(2,2,2) \mapsto 2$	$(2,3,2) \mapsto 23$	$(2,4,2) \mapsto 44$
$(2,0,3) \mapsto 80$	$(2,1,3) \mapsto 101$	$(2,2,3) \mapsto 17$	$(2,3,3) \mapsto 38$	$(2,4,3) \mapsto 59$
$(2,0,4) \mapsto 95$	$(2,1,4) \mapsto 11$	$(2,2,4) \mapsto 32$	$(2,3,4) \mapsto 53$	$(2,4,4) \mapsto 74$
$(2,0,5) \mapsto 5$	$(2,1,5) \mapsto 26$	$(2,2,5) \mapsto 47$	$(2,3,5) \mapsto 68$	$(2,4,5) \mapsto 89$
$(2,0,6) \mapsto 20$	$(2,1,6) \mapsto 41$	$(2,2,6) \mapsto 62$	$(2,3,6) \mapsto 83$	$(2,4,6) \mapsto 104$

- Axiomes de l'arithmétique de Peano : on ajoute (1,1,1) récursivement à partir de (0,0,0) *(fonction Succ)*

La bijection *trc_restreint*

- On définit la bijection *trc_restreint* comme la bijection qui à un système de congruences selon une base modulaire de nombres premiers associe **le plus petit entier naturel** de la progression arithmétique que lui associe le théorème des restes chinois.

- La bijection inverse associe à tout entier entre deux primorielles successives $\#p_i$ et $\#p_{i+1}$, le système de congruences qui fournit les restes de cet entier selon les modules premiers inférieurs ou égaux p_i.

- **Conséquence du fait que *trc* (et *trc_restreint*) sont des bijections**
  La bijection *trc_restreint* associant à chaque système de congruence de modules premiers impairs des m_i tous différents un nombre de la partie finie de $\mathbb{N}$ compris entre 0 et $\prod_{i=1}^{k} m_i$, si $sc_1 \Rightarrow sc_2$ et $sc_1 \neq sc_2$ alors la solution du système de congruences sc_1 (l'image de sc_1 par la bijection *trc_restreint*) est strictement supérieure à la solution du système de congruences sc_2.

Un exemple de l'image par la bijection *trc_restreint* d'un n-uplet et des n-uplets qui sont ses projetés selon certaines coordonnées

- Etudions les projections du triplet $(1, 4, 3)$.

$$\begin{array}{rl} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \to \mathbb{N} \\ (1,4,3) & \mapsto 94 \end{array}$$

$$\begin{array}{rl} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} & \to \mathbb{N} \\ (1,4) & \mapsto 4 \end{array}$$

$$\begin{array}{rl} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \to \mathbb{N} \\ (1,3) & \mapsto 10 \end{array}$$

$$\begin{array}{rl} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \to \mathbb{N} \\ (4,3) & \mapsto 24 \end{array}$$

- 94 a trois images qui lui sont strictement inférieures par la bijection *trc_restreint*.
- 94 se projette dans des nombres strictement plus petits que lui parce que $3.5 < 3.7 < 5.7 < 94 < 3.5.7$.

Intermède : 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 :

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

- $$\mathcal{S}_0 \begin{cases} x \equiv p_1 \ (mod\ m_{j_1}) \\ x \equiv p_2 \ (mod\ m_{j_2}) \\ \ldots \\ x \equiv p_k \ (mod\ m_{j_k}) \end{cases}$$

- **Note :** certains modules peuvent être égaux.

Première étape

- Transformation du système pour ordonner les modules selon un ordre croissant, éliminer les redondances, ne conserver que les modules de la plus grande primorielle inférieure ou égale à x.

$\exists x \in 2\mathbb{N},\ x \geq 20,\ \textit{tel que}$
$\forall p'_1, \ldots, p'_k \in \mathbb{P}^*(x/2),\ \#p'_k < x < \#p'_{k+1},$
$\exists n_{j_1}, \ldots, n_{j_k} \in \mathbb{P}^*(\sqrt{x}).$

- $$\mathcal{S} \begin{cases} x \equiv p'_1 \ (mod\ n_{j_1}) \\ x \equiv p'_2 \ (mod\ n_{j_2}) \\ \ldots \\ x \equiv p'_k \ (mod\ n_{j_k}) \end{cases}$$

- $\mathcal{S}$ a pour image d par la bijection *trc_restreint*.

D'où peut provenir la contradiction ?

- Elle peut provenir du principe de Descente infinie de Fermat.
- On sait que la bijection *trc_restreint* fournit comme solution de $\mathcal{S}$ l'entier naturel d qui est le plus petit entier de la progression arithmétique associée à $\mathcal{S}$ par le théorème des restes chinois.
- Le système $\mathcal{S}$ est tel que d ne vérifie pas la conjecture de Goldbach
- *Conclusion : On cherche un système de congruences $\mathcal{S}'$, impliqué par $\mathcal{S}$ et $\neq$ de $\mathcal{S}$, à qui soit associée par la bijection trc_restreint un entier naturel $d' < d$, avec d' ne vérifie pas la conjecture de Goldbach non plus.*

On cherche $\mathcal{S}' \Leftarrow \mathcal{S}$ qui a pour image $d' < d$ par la bijection *trc_restreint*.

- Considérons un système de congruences $\mathcal{S}'$ constitué d'un certain nombre de congruences de $\mathcal{S}$ selon des modules m_i premiers impairs tous différents, i compris entre 1 et k, tels que $d > \prod_{i=1}^{k} m_i$;
- *Premier problème* :

  Pour pouvoir descendre une marche de Fermat, il faut que $d' < d$.
  Mais on a vu que $d' < d$ découle de la bijection *trc_restreint*.
- *Deuxième problème* :

  Comment être sûr que d' ne vérifie pas la conjecture de Goldbach non-plus ?
  Il faut pour cela que les congruences conservées du système $\mathcal{S}$ initial soient telles que d' soit congru
  à tous les nombres premiers impairs de $\mathbb{P}^*(d'/2)$
  selon un module premier impair de $\mathbb{P}^*(\sqrt{d'})$.
- (dit autrement, il faut être sûr qu'en enlevant des congruences pour faire diminuer strictement la solution du système, on ne va pas "perdre" des congruences qui assuraient la non-vérification de la conjecture de Goldbach).

Deuxième étape

- On conserve du système résultant un maximum de congruences dans un système $\mathcal{S}'$ de telle manière que d, la solution du système initial $\mathcal{S}$, soit strictement supérieur au produit des modules conservés dans le nouveau système et que chaque module intervenant dans une congruence conservée du système soit inférieur à $\sqrt{d'}$.

$\exists x \in 2\mathbb{N},\ x \geq 20,\ \textit{tel que}$
$\forall p'_1, \ldots, p'_{k'} \in \mathbb{P}^*(x/2),\ \#p'_{k'} < x < \#p'_{k'+1},$
$\exists n_{j_1}, \ldots, n_{j_{k'}} \in \mathbb{P}^*(\sqrt{d'}).$

- $$\mathcal{S}' \begin{cases} x \equiv p'_1 \ (mod\ n_{j_1}) \\ x \equiv p'_2 \ (mod\ n_{j_2}) \\ \ldots \\ x \equiv p'_{k'} \ (mod\ n_{j_{k'}}) \end{cases}$$

- $d > \prod_{u=1}^{k'} n_{j_u}$
- Les p'_x sont des nombres premiers impairs tous $\neq$ et les n_y sont des nombres premiers impairs tous $\neq$ et ordonnés selon un ordre croissant.

Pourquoi d' ne vérifie-t-il pas la conjecture de Goldbach non plus ?

- $d' < \prod_{u=1}^{k'} n_{j_u} < d$
- Donc $\frac{d'}{2} < \frac{d}{2} \Leftrightarrow \mathbb{P}^*(d'/2) \subset \mathbb{P}^*(d/2).$
- Mais $\forall m_i \in \mathbb{P}^*(\sqrt{d}), \quad d' \equiv d \ (mod\ m_i).$
- Donc $\forall p_i \in \mathbb{P}^*(d/2), \exists m_i \in \mathbb{P}^*(\sqrt{d}), \quad d \equiv p_i \ (mod\ m_i)$
- $\Leftrightarrow$ $\forall p_i \in \mathbb{P}^*(d/2), \exists m_i \in \mathbb{P}^*(\sqrt{d}), \quad d' \equiv p_i \ (mod\ m_i)$
- $\stackrel{?}{\Rightarrow}$ $\forall p_i \in \mathbb{P}^*(d'/2), \exists m_i \in \mathbb{P}^*(\sqrt{d'}), \quad d' \equiv p_i \ (mod\ m_i)$
- L'implication est vraie parce que chaque module conservé est un élément de $\mathbb{P}^*(\sqrt{d'})$.

Conclusion

- Si un nombre d ne vérifie pas la conjecture de Goldbach, on est assuré de toujours pouvoir obtenir un $d' < d$ ne vérifiant pas non-plus la conjecture de Goldbach, on a établi une contradiction à partir de l'hypothèse que d était le plus petit entier ne vérifiant pas la conjecture de Goldbach

- On a ainsi établi qu'on aboutit toujours à une contradiction si on part de l'hypothèse qu'un entier ne vérifie pas la conjecture de Goldbach.

- Pour cela, on a utilisé ce que l'on pourrait appeler un *"Système de NUmération par les Restes dans les Parties Finies de* $\mathbb{N}$*"* (un *SNURPF*)