Goldbach Conjecture (7^{th} june 1742)

- We note $\mathbb{P}^*$ the odd prime numbers set.
  $\mathbb{P}^* = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\}$

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

- We call *n's Goldbach decomposition* such a sum $p + q$.

- p and q are said *n's Goldbach decomponents*.

- verified by computer until 4.10^{18}
  (Oliveira e Silva, 4.4.2012)

Notations

- In the following, *C.G.* signifies Goldbach Conjecture,
- *s.c.* signifies congruences system,
- *p.a.* signifies arithmetic progression,
- *T.r.c.* signifies Chinese Remainders Theorem.
- For a given n, we note :

$$\mathbb{P}_1^*(n) = \{x \in \mathbb{P}^* / x \leq \frac{n}{2}\}$$

$$\mathbb{P}_2^*(n) = \{x \in \mathbb{P}^* / x \leq \sqrt{n}\}$$

Reformulation

- Goldbach Conjecture is equivalent to the following statement :
  $\forall\ n\ \in\ 2\mathbb{N}\backslash\{0,2,4\},\ \exists\ p\ \in\ \mathbb{P}_1^*(n),\ \forall\ m\ \in\ \mathbb{P}_2^*(n),$
  $p\ \not\equiv\ n\ (mod\ m)$

- Indeed,
  $\forall\ n\ \in\ 2\mathbb{N}\backslash\{0,2,4\},\ \exists\ p\ \in\ \mathbb{P}_1^*(n),\ \forall\ m\ \in\ \mathbb{P}_2^*(n),$
  $p \not\equiv n\ (mod\ m) \Leftrightarrow n-p \not\equiv 0\ (mod\ m) \Leftrightarrow n-p\ is\ prime$

Examples study : Example 1

- *Why* 19 *is the smallest 98's Goldbach decomponent ?*

$98 \equiv 3 \pmod 5$ (98-3=95 and $5 \mid 95$)
$98 \equiv 5 \pmod 3$ (98-5=93 and $3 \mid 93$)
$98 \equiv 7 \pmod 7$ (98-7=91 and $7 \mid 91$)
$98 \equiv 11 \pmod 3$ (98-11=87 and $3 \mid 87$)
$98 \equiv 13 \pmod 5$ (98-13=85 and $5 \mid 85$)
$98 \equiv 17 \pmod 3$ (98-17=81 and $3 \mid 81$)

$98 \not\equiv 19 \pmod 3$ (98-19=79 and $3 \not\mid 79$)
$98 \not\equiv 19 \pmod 5$ (98-19=79 and $5 \not\mid 79$)
$98 \not\equiv 19 \pmod 7$ (98-19=79 and $7 \not\mid 79$)

- *Conclusion* : $\forall\ m \in \mathbb{P}_2^*(98),\ 19 \not\equiv 98\ (mod\ m)$
  19 is a 98's Goldbach decomponent.
  Indeed, $98 = 19 + 79$ with 19 and 79 both primes.

Examples study : Example 2

- *Why* 3 *is a* 40*'s Goldbach decomponent ?*

$\mathbb{Z}/3\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$								
$\mathbb{Z}/5\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$						
$\mathbb{Z}/7\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$				
$\mathbb{Z}/11\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$

3's equivalence class in each finite field,

40's equivalence class in each finite field.

- *Conclusion* : $\forall\ m \in \mathbb{P}_2^*(40),\ 3 \not\equiv 40\ (mod\ m)$
  3 is a 40's Goldbach decomponent.
  Indeed, $40 = 3 + 37$ with 3 and 37 primes.

Examples study : Example 3

- *We are looking for Goldbach decomponents of natural integers that are*

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

- Those numbers we are looking Goldbach decomponents for, are natural integers of the form $210k + 38$ (result provided by Chinese Remainders Theorem as we will see it sooner).

- We saw that odd prime natural integers p that are

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

  can be Goldbach decomponents of those numbers.

- If we omit the case of "little prime numbers"
  (i.e. congruences cases to 0 modulo one odd prime and only one),
  - p must be $\equiv 1\ (mod\ 3)$.
  - p must be $\equiv 1$ *or* 2 *or* $4\ (mod\ 5)$.
  - p must be $\equiv 1$ *or* 2 *or* 4 *or* 5 *or* $6\ (mod\ 7)$.

Examples study : Example 3

- *We are looking for Goldbach decomponents of some even natural integers*

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

  ($\Leftrightarrow$ of the form $210k + 38$)

- Combining all differents possibilities, we obtain :

  $1 \pmod 3 \; 1 \pmod 5 \; 1 \pmod 7$

  $1 \pmod 3 \; 1 \pmod 5 \; 2 \pmod 7$

  $1 \pmod 3 \; 1 \pmod 5 \; 4 \pmod 7$

  $1 \pmod 3 \; 1 \pmod 5 \; 5 \pmod 7$

  $1 \pmod 3 \; 1 \pmod 5 \; 6 \pmod 7$

  $1 \pmod 3 \; 2 \pmod 5 \; 1 \pmod 7$

  $1 \pmod 3 \; 2 \pmod 5 \; 2 \pmod 7$

  $1 \pmod 3 \; 2 \pmod 5 \; 4 \pmod 7$

  $1 \pmod 3 \; 2 \pmod 5 \; 5 \pmod 7$

  $1 \pmod 3 \; 2 \pmod 5 \; 6 \pmod 7$

  $1 \pmod 3 \; 4 \pmod 5 \; 1 \pmod 7$

  $1 \pmod 3 \; 4 \pmod 5 \; 2 \pmod 7$

  $1 \pmod 3 \; 4 \pmod 5 \; 4 \pmod 7$

  $1 \pmod 3 \; 4 \pmod 5 \; 5 \pmod 7$

  $1 \pmod 3 \; 4 \pmod 5 \; 6 \pmod 7$

Examples : Example 3

- *We are looking for Goldbach decomponents of some even natural integers*

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

  (⇔ of the form $210k + 38$*)*

- Combining all differents possibilities, we obtain :

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

Examples study : Example 3

- *Here are some examples of Goldbach decomponents belonging to arithmetic progressions found for some even numbers of the arithmetic progression* $210k + 38$

- 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

- *Conclusion* : It works, of course, it is studied for.

We try to demonstrate the impossibility that exists an even natural integer that doesn't verify *C.G.*

- $(\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ x\ doesn't\ verify\ C.G.) \Rightarrow\ false$
- but

$$\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ x\ doesn't\ verify\ C.G.$$

$$\Leftrightarrow\ \exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ x - p\ is\ compound$$

$$\Leftrightarrow\ \exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ \exists\, m \in \mathbb{P}_2^*(x),\ x - p \equiv 0\ (mod\ m)$$

$$\Leftrightarrow\ \exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ \exists\, m \in \mathbb{P}_2^*(x),\ x \equiv p\ (mod\ m)$$

We try to demonstrate the impossibility that exists an even natural integer that doesn't verify *C.G.*

- $\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ \exists\, m \in \mathbb{P}_2^*(x),$
  $\mathrm{x} \equiv p\ (mod\ m)$

- Quantificators expansion

- $p_1, \ldots, p_k \in \mathbb{P}_1^*(x),\ \ m_1, \ldots, m_l \in \mathbb{P}_2^*(x).$
  $\exists\ \ x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},$
  $\forall\, i \in [1,k],\ \exists\, j \in [1,l]$
  $x \equiv p_i\ (mod\ m_j)$

We try to demonstrate the impossibility that exists an even natural integer that doesn't verify *C.G.*

- Let us write all of the congruences :

- $p_1, \ldots, p_k \in \mathbb{P}_1^*(x), \;\; m_{j_1}, \ldots, m_{j_k} \in \mathbb{P}_2^*(x).$
  $\exists \quad x \in 2\mathbb{N}\backslash\{0, 2, 4\}, \; x \geq 4.10^{18},$

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

- **Note** : m_i moduli are odd prime natural integers that are not mandatory all differents.

Interlude : Chinese Remainders Theorem

- We call arithmetic progression a set containing natural integers of the form $ax + b$ with $a \in \mathbb{N}^*$, $b \in \mathbb{N}$ and $x \in \mathbb{N}$.

- A congruences system not containing contradiction can be solved by the Chinese Remainders Theorem.

- The Chinese Remainders Theorem establishes an isomorphism between $\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ and $\mathbb{Z}/\prod_{i=1}^{k} m_i\mathbb{Z}$ if and only if the modules m_i are two by two coprime.

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

- The Chinese Remainders Theorem establishes a bijection between the set of non-contradictory congruences systems and the set of arithmetic progressions.

Interlude : Recall of Chinese Remainders Theorem

- We are looking for the set of solutions of the following congruences system S :

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

- We set $M = \prod_{i=1}^{k} m_i$.
- Let us calculate $M_1 = M/m_1, M_2 = M/m_2, \ldots, M_k = M/m_k$.
- Let us calculate $d_1, d_2, \ldots, d_k$ such that

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

- S's solution is $\boxed{\mathrm{x} \equiv \Sigma_{i=1}^{k} r_i.d_i.M_i \ (mod \ M)}$

Interlude : Chinese Remainders Theorem

- Let us try to solve :

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

- We set $M = 3.5.7 = 105$.

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

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

that are the natural integers of the sequence : $103, 208, 313, \ldots$

i.e. from the arithmetic progression : $105k + 103$

- Ambiguity, Galois theory, invariant function by a roots permutation

Interlude : Chinese Remainders Theorem

- If we had to solve nearly the same congruences system, but with one congruence less :

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

- We set $M' = 5.7 = 35$.

$$\begin{array}{lll} M'_1 = M'/5 = 7 & 7.y'_1 \equiv 1 \ (mod\ 5) & y'_1 = 3 \\ M'_2 = M'/7 = 5 & 5.y'_2 \equiv 1 \ (mod\ 7) & y'_2 = 3 \end{array}$$

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

that are natural integers from the sequence :

$$33, 68, \underline{103}, 138, 173, \underline{208}, 243, \ldots$$

i.e. from the arithmetic progression : 35k+33

Interlude : Congruence relation powerfulness

- $\equiv$ is an equivalence relation.
- $$\frac{\begin{array}{c} a \equiv b \\ c \equiv d \end{array}}{\begin{array}{c} a+c \equiv b+d \\ ac \equiv bd \end{array}}$$
- Let us compare the resolution of the two following systems :

$$A : \left\{ \begin{array}{l} x \equiv 3 \; (mod \; 5) \\ x \equiv 5 \; (mod \; 7) \end{array} \right. \qquad B : \left\{ \begin{array}{l} x \equiv 13 \; (mod \; 5) \\ x \equiv 5 \; (mod \; 7) \end{array} \right.$$

- $A : x \equiv 3.3.7 + 5.3.5 = 63 + 75 = 138 = 33 \; (mod \; 35)$
- $B : x \equiv 13.3.7 + 5.3.5 = 273 + 75 = 348 = 33 \; (mod \; 35)$

Interlude : What does the Chinese Remainders Theorem bijection ?

- Chinese Remainders Theorem associates to every prime modules non-contradictory congruences system an arithemtic progression.

- Let us call E the set of prime modules congruences systems. Let us call E' the set of arithmetic progressions.

$$\begin{array}{ll} E & \to E' \\ sc_1 & \mapsto pa_1 \\ sc_2 & \mapsto pa_2 \\ sc_1 \wedge sc_2 & \mapsto pa_1 \cap pa_2 \end{array}$$

- Moreover,

$$(sc_1 \Rightarrow sc_2) \quad \Leftrightarrow (pa_1 \subset pa_2)$$

.

Interlude : Recalls

- An arithmetic progression being a part of $\mathbb{N}$, it admits a smallest element. We will choose in the following to represent an arithmetic progression by its smallest element.

- E and E' are two given arithmetic progressions, $E \subset E' \Rightarrow n' \leq n$

- A set E provided with a partial order relation is a *lattice* $\Leftrightarrow\ \forall a \in E, \forall b \in E, \{a, b\}$ admits a least upper bound and a greatest lower bound.

- The set of prime modules congruences systems (all modules being differents) is a lattice provided with a partial order (based on logical implication relationship ($\Rightarrow$)).

- The set of arithmetic progressions is a lattice provided with a partial order (based on set inclusion relationship ($\subset$)).

Interlude : Let us observe more precisely the *trc* bijection intervening in Chinese Remainders Theorem

- What are the solutions obtained by Chinese Remainders Theorem ?

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

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

- In this array, line $(1, 3) \mapsto 13$ must be read "the set of numbers that are congruent to 1 (mod 3) and to 3 (mod 5) is equal to the set of numbers that are congruent to 13 (mod 15)". It is interesting to notice that the same line can be read "13 is congruent to 1 (mod 3) and to 3 (mod 5)" (fractality).

- Peano's arithmetic axioms : let us add (1,1) recursively from (0,0) *(Succ function)*.

Interlude : Let us observe more precisely *trc* bijection intervening in Chinese Remainders Theorem

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

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

- Same remark as for previous page concerning the two possible manners to read each line.

restricted_trc bijection

- Let us define *restricted_trc* bijection as the bijection that associates to a congruences system **the smallest natural integer** of the arithmetic progression the Chinese Remainders Theorem associates to it.

- **Consequence of the fact that *trc* (and *restricted_trc*) are bijections**
  restricted_trc bijection associating to each prime modules congruences system with modules some m_i all differents a natural integer from the finite part $\mathbb{N}$ that is between 0 and $\prod_{i=1}^{k} m_i$, if $sc_1 \Rightarrow sc_2$ and $sc_1 \neq sc_2$ then the $sc1$ congruences system solution (the natural integer paired with sc_1 by *restricted_trc* bijection) is strictly greater than the sc_2 congruences system solution.

Let us provide an example of paired integer by *restricted_trc* bijection of a t-uple and of the t-uples that are its projection according to some of its coordinates

- Let us study 3-uple $(1, 4, 3)$ projections.

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

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

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

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

- 94 has three integers paired with itself that are strictly lesser than it by *restricted_trc* bijection.
- 94 projects itself in natural integers strictly lesser than it because $3.5 < 3.7 < 5.7 < 94 < 3.5.7$.

Interlude : Fermat's Infinite Descent

- If an even integer should not verify Goldbach Conjecture, there should be another even integer lesser than the first one that should not verify Goldbach Conjecture neither and step by step, like this, we proceed until reaching so little integers that we know they verify Goldbach Conjecture.

- Exists no infinite strictly decreasing sequence of natural integers.

- Reductio ad absurdum :
  - we suppose that x is the smallest such that $P(x)$.
  - we show that then $P(x')$ with $x' < x$.
  - we reached a contradiction.

  (If $P(n)$ for a given natural integer n, there exists a non-empty part of $\mathbb{N}$ containing an element that verifies property P.

  This part admits a smallest element. In our case, property P consists in not verifying Goldbach Conjecture)

Recall : We try to reach a contradiction from the following hypothesis :

- $p_1, \ldots, p_k \in \mathbb{P}_1^*(x), \;\; m_{j_1}, \ldots, m_{j_k} \in \mathbb{P}_2^*(x)$.
  $\exists \;\; x \in 2\mathbb{N}\backslash\{0,2,4\},\; x \geq 4.10^{18}$,

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

- **Note :** some modules can be equal.

First step

- System transformation to order modules according to an increasing order and to eliminate redundancies.

- $p'_1, \ldots, p'_k \in \mathbb{P}^*_1(x), \quad n_{j_1}, \ldots, n_{j_k} \in \mathbb{P}^*_2(x)$.
  $\exists \quad x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18}$,

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

- $\mathcal{S}$ has d that is paired with itself by *restricted_trc* bijection.

Where can contradiction come from ?

- It can come from Fermat's Infinite Descent.
- We know that *restricted_trc* bijection provides as solution for $\mathcal{S}$ the natural integer d that is the smallest natural integer of the arithmetic progression associated to $\mathcal{S}$ by the Chinese Remainders Theorem.
- $\mathcal{S}$ system is such that d doesn't verify Goldbach Conjecture.
- *Conclusion : We are looking for a $\mathcal{S}'$ congruences system, implied by $\mathcal{S}$ and $\neq$ to $\mathcal{S}$, to what restricted_trc bijection associates a natural integer $d' < d$, with d' doesn't verify Goldbach Conjecture neither.*

We look for $\mathcal{S}' \Leftarrow \mathcal{S}$ that has $d' < d$ paired with it by *restricted_trc* bijection.

- Let us consider a $\mathcal{S}'$ congruences system constituted by a certain number of congruences of $\mathcal{S}$ according to all differents odd prime natural integers m_i, i an integer between 1 and k, such that $d > \prod_{i=1}^{k} m_i$;

- *First problem* : To descend one Fermat's descent step, it is necessary that $d' < d$.

  But we saw that $d' < d$ comes from *restricted_trc* bijection.

- *Second problem* : How to be sure that d' doesn't verify Goldbach Conjecture neither ?

  For this aim, we need that congruences kept from initial $\mathcal{S}$ congruences system are such that d' is congruent to all $\mathbb{P}_1^*(d')$ elements according to a module that is an element of $\mathbb{P}_2^*(d')$.

- (Said in another way, we must be sure that removing congruences to make strictly decrease the congruences system solution, we won't "lose" congruences that ensured the Goldbach Conjecture non-verification.)

Second step

- We keep from the resulting congruences system a maximum of congruences in a new system $\mathcal{S}'$ in such a way that d, the initial system $\mathcal{S}$'s solution, is strictly greater than the moduli kept in the new system product and in such a way that every module intervening in a kept congruence of the system is lesser than $\sqrt{d'}$. .
- $p'_1, \dots, p'_{k'} \in \mathbb{P}_1^*(x), \;\; n_{j_1}, \dots, n_{j_{k'}} \in \mathbb{P}_2^*(x)$.
  $\exists \quad x \in 2\mathbb{N}\backslash\{0,2,4\},\, x \geq 4.10^{18}$,

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

- $d > \prod_{u=1}^{k'} n_{j_u}$
- p'_x are all differents odd prime natural integers and n_y are all differents odd prime natural integers ordered according to an increasing order.
- $\mathcal{S}'$ is paired with d' by *restricted_trc* bijection.

Why d' doesn't verify Goldbach Conjecture neither ?

- $d' < \prod_{u=1}^{k'} n_{j_u} < d$
- So $\dfrac{d'}{2} < \dfrac{d}{2} \Leftrightarrow \mathbb{P}_1^*(d') \subset \mathbb{P}_1^*(d).$
- But $\forall\ m_i \in \mathbb{P}_2^*(d),$ $d' \equiv d\ (mod\ m_i).$
- Then $\forall p_i \in \mathbb{P}_1^*(d),\ \exists m_i \in \mathbb{P}_2^*(d),$ $d \equiv p_i\ (mod\ m_i)$
- $\Leftrightarrow$ $\forall p_i \in \mathbb{P}_1^*(d),\ \exists m_i \in \mathbb{P}_2^*(d),$ $d' \equiv p_i\ (mod\ m_i)$
- $\Rightarrow$ $\forall p_i \in \mathbb{P}_1^*(d'),\ \exists m_i \in \mathbb{P}_2^*(d'),$ $d' \equiv p_i\ (mod\ m_i)$
- The implication is true because every kept module is an element of $\mathbb{P}_2^*(d')$.
- This last line expresses the fact that d' doesn't verify Goldbach

Conclusion

- If one natural even integer d doesn't verify Goldbach Conjecture $C.G.$, we are ensured to find another natural even integer $d' < d$ not verifying Goldbach Conjecture neither, we established a contradiction from the hypothesis that d was the smallest natural even integer not verifying Goldbach Conjecture

- We so established that we always reach a contradiction when we start from the hypothesis that some natural even integer doesn't verify Goldbach Conjecture.

- For this aim, we used what we could call a *"Residue Numeration System in Finite Parts of $\mathbb{N}$"*

- Congruence relationship makes of $\mathbb{N}$ the natural integers set a fractal set.