An elementary study of Goldbach Conjecture

Denise Chemla

26/5/2012

Goldbach Conjecture (7^{th}, june 1742) states that every even natural integer greater than 4 is the sum of two odd prime numbers. If we note $\mathbb{P}^*$ the set of odd prime numbers*, we can write Goldbach Conjecture as following :

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

We will call *Goldbach decomposition* of n such a sum $p+q$. p and q are called *Goldbach decomponents* of n.
Goldbach Conjecture was verified by computer until 4.10^{18}†.

In the following, n being a given naturel integer, we note :

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

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

We can reformulate Goldbach Conjecture by 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,

$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}_1^*(n),\ \forall\, m \in \mathbb{P}_2^*(n),$

$$\begin{aligned} & p \not\equiv n\ (mod\ m) \\ \Leftrightarrow\ & n-p \not\equiv 0\ (mod\ m) \\ \Leftrightarrow\ & n-p\ is\ prime. \end{aligned}$$

1 Examples study

1.1 Example 1 : Why 19 is the smallest 98's Goldbach decomponent ?

$$\begin{array}{ll} 98 \equiv 3\ (mod\ 5) & (98-3=95\ and\ 5|95) \\ 98 \equiv 5\ (mod\ 3) & (98-5=93\ and\ 3|93) \\ 98 \equiv 7\ (mod\ 7) & (98-7=91\ and\ 7|91) \\ 98 \equiv 11\ (mod\ 3) & (98-11=87\ and\ 3|87) \\ 98 \equiv 13\ (mod\ 5) & (98-13=85\ and\ 5|85) \\ 98 \equiv 17\ (mod\ 3) & (98-17=81\ and\ 3|81) \end{array}$$

$$\begin{array}{ll} 98 \not\equiv 19\ (mod\ 3) & (98-19=79\ and\ 3 \not| 79) \\ 98 \not\equiv 19\ (mod\ 5) & (98-19=79\ and\ 5 \not| 79) \\ 98 \not\equiv 19\ (mod\ 7) & (98-19=79\ and\ 7 \not| 79) \end{array}$$

All of the odd prime natural integers between 3 and 17 are congruent to 98 modulo an element of $\mathbb{P}_2^*(98)$ so none of those numbers can be a 98's Goldbach decomponent.

On the contrary, as requested : $\forall\, m \in \mathbb{P}_2^*(98),\ 19 \not\equiv 98\ (mod\ m)$.
So 19 is a 98's Goldbach decomponent. Effectively, $98 = 19 + 79$ with 19 and 79 two odd prime numbers.

*$\mathbb{P}^* = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\}$
†by Oliveira e Silva on 4.4.2012

1.2 Example 2 : Why 3 is a 40's Goldbach decomponent ?

In the following table are presented the equivalence classes of finite fields $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/11\mathbb{Z}$.

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

In each finite field, we colored in light pink 3's equivalence class, and we colored in light blue 40's equivalence class, the even natural integer to be Goldbach decomposed.

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

1.3 Example 3 : let us look for Goldbach decomponents for even natural integers that are $\equiv 2\ (mod\ 3)$ and $\equiv 3\ (mod\ 5)$ and $\equiv 3\ (mod\ 7)$.

Those numbers for which we are looking for Goldbach decomponents are natural integers of the form *210k+38* (consequently to Chinese Remainders Theorem that will be presented in the following).

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. the case where there is a congruence to 0 for one and only one module),

– *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* $6\ (mod\ 7)$.

Combining all possibilities, we obtain :

$$
\begin{array}{llllll}
1 & (mod\ 3) & 1 & (mod\ 5) & 1 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+1 \\
1 & (mod\ 3) & 1 & (mod\ 5) & 2 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+121 \\
1 & (mod\ 3) & 1 & (mod\ 5) & 4 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+151 \\
1 & (mod\ 3) & 1 & (mod\ 5) & 5 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+61 \\
1 & (mod\ 3) & 1 & (mod\ 5) & 6 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+181 \\
1 & (mod\ 3) & 2 & (mod\ 5) & 1 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+127 \\
1 & (mod\ 3) & 2 & (mod\ 5) & 2 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+37 \\
1 & (mod\ 3) & 2 & (mod\ 5) & 4 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+67 \\
1 & (mod\ 3) & 2 & (mod\ 5) & 5 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+187 \\
1 & (mod\ 3) & 2 & (mod\ 5) & 6 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+97 \\
1 & (mod\ 3) & 4 & (mod\ 5) & 1 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+169 \\
1 & (mod\ 3) & 4 & (mod\ 5) & 2 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+79 \\
1 & (mod\ 3) & 4 & (mod\ 5) & 4 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+109 \\
1 & (mod\ 3) & 4 & (mod\ 5) & 5 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+19 \\
1 & (mod\ 3) & 4 & (mod\ 5) & 6 & (mod\ 7) \quad \rightarrow \quad 210\mathrm{k}+139
\end{array}
$$

Here are some examples of Goldbach decomponent belonging to arithmetic progressions founded for some numbers of the arithmetic progression *210k+38*.

248 : 7 19 37 67 97 109
458 : 19 37 61 79 109 127 151 181 229 (*double of a prime*)
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 (*double of a prime*)
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

2 Our objective : to reach a contradiction from the hypothesis that an even natural integer doesn't verify Goldbach Conjecture

We are trying to demonstrate the impossibility that exists an even natural integer that doesn't verify Goldbach Conjecture. It corresponds to the fact that the hypothesis :

$$\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ x \text{ doesn}'\text{t verify Goldbach Conjecture}$$

permits to lead to a contradiction.

But :

$\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ x$ doesn't verify Goldbach Conjecture
$\Leftrightarrow$ $\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ x - p$ compound
$\Leftrightarrow$ $\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ \exists\, m \in \mathbb{P}_2^*(x),\ x - p \equiv 0\ (mod\ m)$
$\Leftrightarrow$ $\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ \exists\, m \in \mathbb{P}_2^*(x),\ x \equiv p\ (mod\ m)$

Expanding des quantificators, we obtain :

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

Let us write all the congruence relations :

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

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

It is important to notice that moduli are odd prime natural integers that are not necessarily differents (some of them can be equal).

3 Chinese Remainders Theorem

3.1 Recalls

We call arithmetic progression a set of natural integers of the form $ax+b$ with $a \in \mathbb{N}^*,\ b \in \mathbb{N}$ and $x \in \mathbb{N}$.
A congruences system that doesn't contain contradictions can be solved using 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 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 congruences systems and the

set of arithmetic progressions.
We are looking for solutions for the following congruences system S :

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

We set $M = \prod_{i=1}^{k} m_i$.

Let us calculate : • $M_1 = M/m_1, M_2 = M/m_2, \dots, M_k = M/m_k$.

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

The solution of S is $\boxed{\text{x} \equiv \Sigma_{i=1}^{k} r_i.d_i.M_i \ (mod\ M)}$.

3.2 Example 1

Let us try to solve the following congruences system :

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

We set $M = 3.5.7 = 105$.
$M_1 = M/3 = 105/3 = 35, \quad 35.y_1 \equiv 1 \ (mod\ 3), \quad y_1 = 2.$
$M_2 = M/5 = 105/5 = 21, \quad 21.y_2 \equiv 1 \ (mod\ 5), \quad y_2 = 1.$
$M_3 = M/7 = 105/7 = 15, \quad 15.y_3 \equiv 1 \ (mod\ 7), \quad y_3 = 1.$

$x \equiv r_1.M_1.y_1 + r_2.M_2.y_2 + r_3.M_3.y_3$
$\equiv 1.35.2 + 3.21.1 + 5.15.1 = 70 + 63 + 75 = 208 = 103 \ (mod\ 105)$
that are the natural integers of the sequence : $103, 208, 313, \dots,$
i.e. those of the arithmetic progression : *105k+103*.

3.3 Example 2

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 $M' = 5.7 = 35$.
$M'_1 = M'/5 = 7, \quad 7.y'_1 \equiv 1 \ (mod\ 5), \quad y'_1 = 3.$
$M'_2 = M'/7 = 5, \quad 5.y'_2 \equiv 1 \ (mod\ 7), \quad y'_2 = 3.$

$x \equiv r_1.M_1.y_1 + r_2.M_2.y_2$
$\equiv 3.3.7 + 5.3.5 = 63 + 75 = 138 = 33 \ (mod\ 35)$
that are the natural integers of the sequence : $33, 68, \underline{103}, 138, 173, \underline{208}, 243, \dots,$
i.e. those of the arithmetic progression : *35k+33*

3.4 Congruence relation powerfulness

The congruence relation (noted $\equiv$), that was invented by Gauss, is an equivalence relation.

$$\begin{array}{c} a \equiv b \\ c \equiv d \\ \hline a + c \equiv b + d \\ ac \equiv bd \end{array}$$

Let us compare two congruences systems resolutions :

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

$$\begin{array}{l} A : x \equiv 3.3.7 + 5.3.5 = 63 + 75 = 138 = 33 \ (mod\ 35) \\ B : x \equiv 13.3.7 + 5.3.5 = 273 + 75 = 348 = 33 \ (mod\ 35) \end{array}$$

Because 3 and 13 are congruent (mod 5), we found the same arithmetic progression by congruence ($modulo$ 35) ; it is the solution of both two systems.

3.5 What makes the bijection provided by Chinese Remainders Theorem ?

The Chinese Remainders Theorem associates to each non-contradictory congruences system containing prime moduli an arithmetic progression.

Let us call E the congruences modulo prime natural integers systems set. Let us call E' the arithmetic progressions set.

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

Moreover,

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

An arithmetic progression being a part of the natural integers set admits a smallest element. In the following, we will choose to represent an arithmetic progression by its smallest natural integer.

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

We call *"lattice"* a set E provided with a partial order relation and such that :

$$\forall\ a \in E,\ \forall\ b \in E,\ \{a, b\} \text{ admits a least upper bound and a greatest lower bound.}$$

The congruences modulo prime natural integers systems set is a lattice provided with a partial order (based on the *logical implication* relation ($\Rightarrow$)).

The arithmetic progressions set is a lattice provided with a partial order (based on the *set inclusion* relation ($\subset$)).

3.6 Let us observe more precisely the bijection intervening in Chinese Remainders Theorem

Let us see the result of applying the bijection (that we will call trc) of Chinese Remainders Theorem to the cartesian product $A = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. The elements that are paired with A's elements are equivalence classes of $\mathbb{Z}/15\mathbb{Z}$.

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

In this table, the line $(1,3) \mapsto 13$ must be read "the set of natural integers that are congruent to 1 (*mod* 3) and to 3 (*mod* 5) is equal to the set of natural integers that are congruent to 13 (*mod* 15)". It can be noticed that the same line could be read "13 is congruent to 1 (*mod* 3) and to 3 (*mod* 5)"[‡].

Let us study now the bijection that pairs $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ with $\mathbb{Z}/105\mathbb{Z}$

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

In each cell, we colored the smallest number of the cell, on which we can imagine the other numbers of the cell "project" themselves when we suppress congruences in the system that correspond to them. We remark that applying Succ Peano Arithmetic function (adding recursively (1,1) from (0,0)), we pass across all the table cells one by one following descending diagonals (and going to the bottom of a column or to the extrem left of a line when the cell we reached is out of the table).

We easily understand that our observed results on the cartesian product of 3 finite fields are generalisable to cartesian products of as many finite fields as we want..

[‡]We can consider that this property corresponds to a kind of "fractality" of natural integers set, that can be called "auto-similarity", that is such that a same property is to be found at the elements level and at the element sets level for $\mathbb{N}$.

3.7 The bijection *restricted_trc* (or the smallest natural integer reached by *trc*)

We define bijection *restricted_trc* as the bijection that to a congruences system associates **the smallest natural integer** of the arithmetic progression that is associated to it by the Chinese Remainders.

There is an important consequence to the fact that *trc* (and *restricted_trc*) are bijections : bijection *restricted_trc* associating to each congruences system modulo prime natural integers that are all differents, a natural integer belonging to the finite part of $\mathbb{N}$ containing the natural integers from 0 to $\prod_{i=1}^{k} m_i$, if $sc_1 \Rightarrow sc_2$ and $sc_1 \neq sc_2$ then the solution of congruences system sc_1 (the element paired with sc_1 by the bijection *restricted_trc*) is strictly greater than the solution paired with the congruences system sc_2.

3.8 An application example of bijection *restricted_trc*

The natural integer 94 is between $3.5 = 15$ and $3.5.7 = 105$. Let us study the projections of 3-uple $(1, 4, 3)$ belonging to the cartesian product $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ on each one of its coordinates.

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

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

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

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

94 has three numbers paired with him by *restricted_trc*, one for each of its coordinates. 94 is projecting in natural integers strictly lesser than him because $3.5 < 3.7 < 5.7 < 94 < 3.5.7$.

4 Fermat's Infinite Descent

4.1 Recalls

Using Fermat's Infinite Descent method to prove Goldbach Conjecture consists in demonstrating that if there was a natural integer that would not verify Goldbach Conjecture, there would be another one, smaller than the first one, that would not verify Goldbach Conjecture neither, and like this, step by step, until reaching so little natural integers, than for them, we know they verify Goldbach Conjecture.

Fermat's Infinite Descent Method results from the fact that there is no infinite and strictly decreasing sequence of natural integers. The reasoning on which Fermat's Infinite Descente is based is the well-known "reductio ad absurdum" :

- let us suppose that x is the smallest natural integer such that P(x) ;
- we show that then P(x') with x' <x ;
- we reached a contradiction.

If $P(n)$ for a natural integer n given, there exists a non-empty part of $\mathbb{N}$ that contains an element that verifies the property P. This part of $\mathbb{N}$ admits a smallest element. In our case, the property P consists in "not verifying Goldbach Conjecture".

We recall that we try to reach a contradiction from the hypothesis :

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

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

It is important to remember that some moduli can be equal.

4.2 First step

Let us transform our congruences system so that moduli are put in an increasing order and in the aim to eliminate redundancies.

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

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

$\mathcal{S}$ is paired with d by *restricted_trc* bijection.

4.3 From where can the contradiction come from ?

It can come from the Fermat's Infinite Descent principle.

We know that *restricted_trc* bijection provides as solution for $\mathcal{S}$ the natural integer d that is the smallest integer of the arithmetic progression associated to $\mathcal{S}$ by the Chinese Remainders Theorem.

$\mathcal{S}$ congruences system is such that d doesn't verify Goldbach Conjecture.

We are looking for a congruences system $\mathcal{S}'$, that is implied by $\mathcal{S}$ and $\neq$ from $\mathcal{S}$, to which is associated by *restricted_trc* bijection a natural integer $d' < d$, with d' doesn't verify Goldbach Conjecture neither.

Let us consider a congruences system $\mathcal{S}'$ constituted of a certain number of congruences from $\mathcal{S}$ modulo some moduli m_i that are prime odd natural integers all differents, i between 1 and k, such that $d > \prod_{i=1}^{k} m_i$.

To be able to descent one step of the Fermat's Descent steps, it is necessary that $d' < d$. But we saw that $d' < d$ comes from the fact that *restricted_trc* is a bijection.

How can we be sure that d' doesn't verify Goldbach Conjecture neither ?

For this, it is necessary that congruences kept from the initial system $\mathcal{S}$ are so that d' is congruent to all prime natural integers in $\mathbb{P}^*_1(d')$ modulo a prime natural integer in $\mathbb{P}^*_2(d')$.

Told in another way, we must be sure that removing some congruences to make the congruences system's solution strictly decrease, we are not going to "lose" congruences that ensured Goldbach Conjecture non-verification by d'.

4.4 Second step

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

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

We have $d > \prod_{u=1}^{k'} n_{j_u}$. The p'_x are odd prime natural integers all differents and the n_y are odd prime natural integers all differents and ordered in an increasing order.

$\mathcal{S}'$ is paired with d' by *restricted_trc* bijection.

4.5 Why d' doesn't verify Goldbach Conjecture neither ?

We have $d' < \prod_{u=1}^{k'} n_{j_u} < d.$

So $\frac{d'}{2} < \frac{d}{2} \Leftrightarrow \mathbb{P}_1^*(d') \subset \mathbb{P}_1^*(d).$

But $\forall\, m_i \in \mathbb{P}_2^*(d), \quad d' \equiv d\ (mod\ m_i).$

So $\forall p_i \in \mathbb{P}_1^*(d),\ \exists m_i \in \mathbb{P}_2^*(d), \quad d \equiv p_i\ (mod\ m_i).$

$\Leftrightarrow$ $\forall p_i \in \mathbb{P}_1^*(d),\ \exists m_i \in \mathbb{P}_2^*(d), \quad d' \equiv p_i\ (mod\ m_i)$

$\Rightarrow$ $\forall p_i \in \mathbb{P}_1^*(d'),\ \exists m_i \in \mathbb{P}_2^*(d'), \quad d' \equiv p_i\ (mod\ m_i)$

The implication is true because all the kept moduli are elements of $\mathbb{P}_2^*(d')$.

This last line asserts that d' doesn't verify Goldbach Conjecture neither.

5 Conclusion

If a natural integer d doesn't verify Goldbach Conjecture, we are ensured that we always can obtain a natural integer $d' < d$ not verifying Goldbach Conjecture neither, we reached a contradiction from the hypothesis that d was the smallest natural integer not verifying Goldbach Conjecture.

So doing, we established that we always lead to a contradiction from the hypothesis that a natural integer doesn't verify Goldbach Conjecture.

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

Congruence relation yields the set of natural integers $\mathbb{N}$ a fractal set.