Goldbach conjecture (June 7, 1742)

- 271 years old.

- **Statement** : Every even number (n) greater than 2
  is the sum of two primes.

- $\iff$ Every integer greater than 1 is the average of two primes $(\frac{1}{2}p_1 + \frac{1}{2}p_2)$.

- $$\begin{aligned} 98 &= 19 + 79 \\ &= 31 + 67 \\ &= 37 + 61 \end{aligned}$$

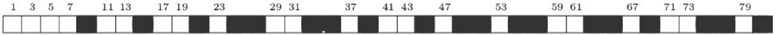
Laisant's strip

- **Charles-Ange Laisant** : Sur un procédé expérimental de vérification de la conjecture de Goldbach, Bulletin de la SMF, 25, 1897.

- *"This famous empirical theorem : every even number is the sum of two primes, whose demonstration seems to overpass actual possibilities, has generated a certain amount of works and contestations. Lionnet tried to establish the proposition should probably be false. M. Georg Cantor verified it numerically until 1000, giving for each even number all decompositions in two primes, and he noticed that this decompositions number is always growing in average, even if it presents big irregularities."*

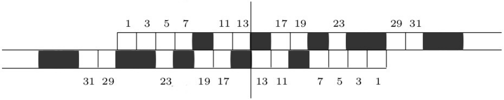
Laisant's strips

- *"Let us show a process that would permit to make without computing the experimental verification we mentioned, and to have, for each even number, only inspecting a figure, all the decompositions. Let us suppose that on a strip constituted by pasted squares, representing odd successive numbers, we had constructed the Erathosthene's sieve, shading compound numbers, until any limit 2n."*



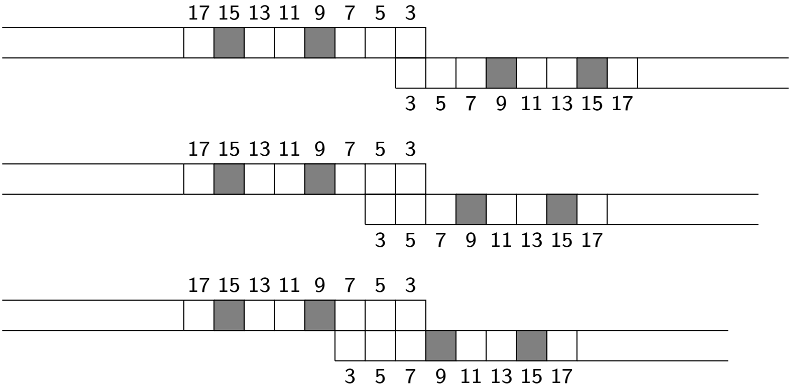
Laisant's strips

- *"If we constructed two similar strips, and if we put the second one behind the first one returning it and making correspond* 1 *cell with* $2n$ *cell, it is evident that if Goldbach theorem was true for* $2n$*, there would be somewhere two white cells corresponding to each other ; and all the couples of white cells will give diverse decompositions. We will even have them reading only the half of the figure, because of the symmetry around the middle. In this way, verification concerning* 28 *even number will give figure above and will show that we have* $28 = 5 + 23 = 11 + 17$*."*



Laisant's strips

- *"We understand that, strips being constructed in advance, a single shift permits to pass from one number to another, verifications are very rapid."*



Boolean algebra

- We represent primality by booleans.
- 0 signifies *is prime*, while 1 signifies *is compound*.
- $23 \rightarrow 0$
- $25 \rightarrow 1$
-

3	5	7	9	11	13	15	17	19	21	23	25	27	29	...
0	0	0	1	0	0	1	0	0	1	0	1	1	0	...

A space copy : 2 booleans matrices

- We represent n decompositions in sums of two odd numbers by 2 booleans matrices (the boolean in the bottom corresponding to the smaller number).
- $28 = \underset{p}{5} + \underset{p}{23} \rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} = a$
- $28 = \underset{c}{9} + \underset{p}{19} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} = b$
- $28 = \underset{p}{3} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = c$
- $40 = \underset{c}{15} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix} = d$

40, 42 and 44 words

	37	35	33	31	29	27	25	23	21
40	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
	a	*c*	*c*	*b*	*a*	*c*	*d*	*a*	*c*

	39	37	35	33	31	29	27	25	23	21
42	1	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	c	*a*	*c*	*d*	*a*	*a*	*d*	*c*	*a*	*d*

	41	39	37	35	33	31	29	27	25	23
44	0	1	0	1	1	0	0	1	1	0
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	a	*c*	*a*	*d*	*c*	*a*	*b*	*c*	*c*	*b*

Operations on matrices

- General rule :

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} . \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ y_2 \end{pmatrix}$$

- Example :

$$\underset{c}{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} . \underset{b}{\begin{pmatrix} 0 \\ 1 \end{pmatrix}} = \underset{d}{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}$$

- Particular rules :

$aa \to a$	$ba \to a$	$ca \to c$	$da \to c$
$ab \to b$	$bb \to b$	$cb \to d$	$db \to d$
$ac \to a$	$bc \to a$	$cc \to c$	$dc \to c$
$ad \to b$	$bd \to b$	$cd \to d$	$dd \to d$

Let us observe words : 16 rewriting rules.

6 : *a*

8 : *a*

10 : *a a*

12 : *c a*

14 : *a c a*

16 : *a a c*

18 : *c a a d*

20 : *a c a b*

22 : *a a c b a*

24 : *c a a d a*

26 : *a c a b c a*

28 : *c a c b a c*

30 : *c c a d a a d*

32 : *a c c b c a b*

34 : *a a c d a c b a*

Language theory reminders

- An alphabet is a finite set of symbols.
- Alphabets used in the following are : $A = \{a, b, c, d\}, A_{ab} = \{a, b\}, A_{cd} = \{c, d\}, A_{ac} = \{a, c\}$ and $A_{bd} = \{b, d\}$.
- A word on X alphabet is a finite and ordered sequence, eventually empty, of alphabet elements. It's a letters concatenation. We note X^* set of words on X alphabet.
- A word is a prefix of another one if it contains, on all its length, the same letters at the same positions (X being an alphabet and $w, u \in X^*$. u is a prefix of w if and only if $\exists v \in X^*$ such that $w = u.v$)

Let us observe diagonal words.

6 :	*a*							
8 :	*a*							
10 :	*a*	*a*						
12 :	*c*	*a*						
14 :	*a*	*c*	*a*					
16 :	*a*	*a*	*c*					
18 :	*c*	*a*	*a*	*d*				
20 :	*a*	*c*	*a*	*b*				
22 :	*a*	*a*	*c*	*b*	*a*			
24 :	*c*	*a*	*a*	*d*	*a*			
26 :	*a*	*c*	*a*	*b*	*c*	*a*		
28 :	*c*	*a*	*c*	*b*	*a*	*c*		
30 :	*c*	*c*	*a*	*d*	*a*	*a*	*d*	
32 :	*a*	*c*	*c*	*b*	*c*	*a*	*b*	
34 :	*a*	*a*	*c*	*d*	*a*	*c*	*b*	*a*

Diagonal words properties

- Diagonal words (diagonals) have their letters either in A_{ab} alphabet or in A_{cd} alphabet.
- Each diagonal is a prefix of the following diagonal using same alphabet.
- Indeed, a diagonal codes decompositions that have the same second term and that have as first term an odd number from sequence of odd numbers beginning with 3.
- For instance, diagonal *aaaba*, that begins with an *a* letter, first letter of 26's word on figure 1 codes following decompositions : $3+23, 5+23, 7+23; 9+23, 11+23$ and $13+23$.

Diagonal word properties

- Thus, diagonals on A_{ab} alphabet "code" decompositions that have a second term that is prime ; letters of such diagonals code either by a letters corresponding to prime numbers, or by b letters corresponding to compound numbers, the sequence of primality characters of odd numbers, beginning by 3.

- On the other side, diagonals on A_{cd} alphabet "code" decompositions that have a second term that is compound ; letters of such diagonals code either by c letters corresponding to prime numbers, or by d letters corresponding to compound numbers, the sequence of primality characters of odd numbers, beginning by 3.

Let us observe vertical words.

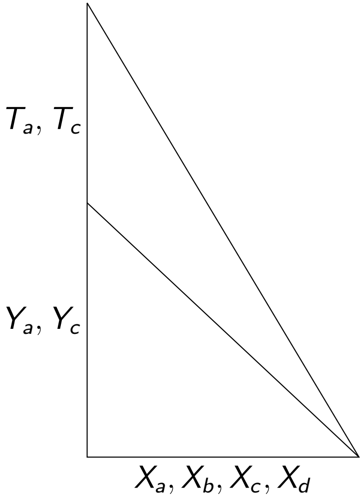
6 :	*a*							
8 :	*a*							
10 :	*a*	*a*						
12 :	*c*	*a*						
14 :	*a*	*c*	*a*					
16 :	*a*	*a*	*c*					
18 :	*c*	*a*	*a*	*d*				
20 :	*a*	*c*	*a*	*b*				
22 :	*a*	*a*	*c*	*b*	*a*			
24 :	*c*	*a*	*a*	*d*	*a*			
26 :	*a*	*c*	*a*	*b*	*c*	*a*		
28 :	*c*	*a*	*c*	*b*	*a*	*c*		
30 :	*c*	*c*	*a*	*d*	*a*	*a*	*d*	
32 :	*a*	*c*	*c*	*b*	*c*	*a*	*b*	
34 :	*a*	*a*	*c*	*d*	*a*	*c*	*b*	*a*

(and vertical “slices”)

Vertical words properties

- Vertical words have their letters either in A_{ac} alphabet or in A_{bd} alphabet.
- A vertical word codes successive decompositions that have the same first term.
- Every vertical word is contained in a vertical word that is on its left side and that is defined on the same alphabet.

n doesn't verify Goldbach conjecture.



n doesn't verify Goldbach conjecture.

	6 :	a							
	8 :	a							
	10 :	a	a						
$T_a = 5$	12 :	c	a						
$T_c = 2$	14 :	a	c	a					
	16 :	a	a	c					
	18 :	c	a	a	d				
	20 :	a	c	a	b				
	22 :	a	a	c	b	a			
$Y_a = 4$	24 :	c	a	a	d	a			
$Y_c = 3$	26 :	a	c	a	b	c	a		
	28 :	c	a	c	b	a	c		
	30 :	c	c	a	d	a	a	d	
	32 :	a	c	c	b	c	a	b	$\leftarrow X_a = 2, X_b = 2, X_c = 3, X_d = 0$

n doesn't verify Goldbach conjecture.

	6 :	a								
	8 :	a								
	10 :	a	a							
$T_a = 5$	12 :	c	a							
$T_c = 2$	14 :	a	c	a						
	16 :	a	a	c						
	18 :	c	a	a	d					
	20 :	a	c	a	b					
	22 :	a	a	c	b	a				
	24 :	c	a	a	d	a				
	26 :	a	c	a	b	c	a			
$Y_a = 5$	28 :	c	a	c	b	a	c			
$Y_c = 3$	30 :	c	c	a	d	a	a	d		
	32 :	a	c	c	b	c	a	b		
	34 :	a	a	c	d	a	c	b	a	$\leftarrow X_a = 4, X_b = 1, X_c = 2, X_d = 1$

Cantor-like one-to-one mappings

- T_a counts decompositions of the form $n' = 3 + p_i$, p_i prime, $n' \leqslant 2\left\lceil \dfrac{n+2}{4} \right\rceil$.
- For instance, if $n = 34$, $T_a = \#\{3+3, 3+5, 3+7, 3+11, 3+13\}$.
- T_c, on its side, counts decompositions of the form $n' = 3 + c_i$, c_i compound $n' \leqslant 2\left\lceil \dfrac{n+2}{4} \right\rceil$.
- For instance, if $n = 34$, $T_c = \#\{3+9, 3+15\}$.

Cantor-like one-to-one mappings

- The trivial one-to-one mapping on decompositions second term permits to easily explain why $Y_a = X_a + X_b$ or $Y_c = X_c + X_d$. The simple presentation of sets in extension suffices to convince oneself.

- $$Y_a = \#\{3+17, 3+19, 3+23, 3+29, 3+31\}$$
  $$X_a = \#\{3+31, 5+29, 11+23, 17+17\}$$
  $$X_b = \#\{15+19\}$$

  $$Y_c = \#\{3+21, 3+25, 3+27\}$$
  $$X_c = \#\{7+27, 13+21\}$$
  $$X_d = \#\{9+25\}$$

Cantor-like one-to-one mappings

- One-to-one mapping f that permits to pass from line 2 to line 1 of the table above is such that $f(a) = f(c) = a$ and $f(b) = f(d) = c$.

- One-to-one mapping g that permits to pass from line 2 to line 3 is such that $g(a) = g(b) = a$ and $g(c) = g(d) = c$.

- It's the $3 + n/2$ decomposition duplication in cases of odd numbers doubles that necessitates the introduction of ϵ variable that equals 1 in those cases and 0 in others.

Cantor-like one-to-one mappings

	3	3	3	3	3	3	3
1	*a*	*a*	*a*	*c*	*a*	*a*	*c*
	3	5	7	9	11	13	15
	3	5	7	9	11	13	15
2	*a*	*c*	*c*	*b*	*c*	*a*	*b*
	29	27	25	23	21	19	17
	29	27	25	23	21	19	17
3	*a*	*c*	*c*	*a*	*c*	*a*	*a*
	3	3	3	3	3	3	3

	3	3	3	3	3	3	3	3
1	*a*	*a*	*a*	*c*	*a*	*a*	*c*	*a*
	3	5	7	9	11	13	15	17
	3	5	7	9	11	13	15	17
2	*a*	*a*	*c*	*d*	*a*	*c*	*b*	*a*
	31	29	27	25	23	21	19	17
	31	29	27	25	23	21	19	17
3	*a*	*a*	*c*	*c*	*a*	*c*	*a*	*a*
	3	3	3	3	3	3	3	3

n doesn't verify Goldbach conjecture.

- Following constraints are always satisfied :

$$Y_a = X_a + X_b$$
$$Y_c = X_c + X_d$$
$$T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d)$$

- $\epsilon = 1$ si n est un double d'impair, $\epsilon = 0$ sinon.

- m_n contains no a, we have $X_a = 0$.

- But since $Y_a = X_a + X_b$, we also have $Y_a = X_b$.

n doesn't verify Goldbach conjecture.

- Identifying Y_a with X_b and Y_c with $X_c + X_d$ in last constraint, one obtains the following equalities :

$$\begin{aligned} T_a + T_c + Y_a + Y_c + \epsilon &= 2(X_a + X_b + X_c + X_d) \\ T_a + T_c + X_b + X_c + X_d + \epsilon &= 2X_a + 2X_b + 2X_c + 2X_d \\ T_a + T_c + \epsilon &= X_b + X_c + X_d \\ T_a + T_c + \epsilon &= X_b + Y_c \end{aligned}$$

- We must now remind the variables meaning :
  - $T_a + T_c = \left\lfloor \frac{n-4}{4} \right\rfloor$;
  - X_b counts the number of n decompositions as a sum of two odd numbers $p + q$ with $p \leqslant n/2$ compound and q prime.
  - Y_c counts the number of odd compound numbers between $n/2$ and $n - 3$.

n doesn't verify Goldbach conjecture.

- The number X_b of n decompositions de n as a sum of two odd numbers $p+q$ with $p \leqslant n/2$ compound and q prime being necessarily lesser than the number of primes between $n/2$ and $n-3$, we have $X_b < Y_a$ (we used here a sort of inverted pigeonhole principle : if we put 0 or 1 object in k holes, there can be more objects than holes, i.e. more than k objects). But the number of prime numbers contained in an interval is always lesser than the number of odd compound numbers contained in the same interval (since $n > 100$). Thus $Y_a < Y_c$. Thus $X_b + Y_c < Y_a + Y_c < 2Y_c$.
- $\left\lfloor \dfrac{n-4}{4} \right\rfloor$ is greater than $2Y_c$ for all integer greater than a certain one that is small (such as 100). This ensures that we never have $T_a + T_c + \epsilon = X_b + Y_c$ which would result from the absence of a letter in a word.

Conclusion

- We used a 4 letters language to represent n decompositions as two odd numbers sums.
- Rewriting rules preserve "letters slices" width.
- We use a lexical theory of numbers, according to which numbers are words.
- We have always to well observe letters order in words.