# Conjecture de Goldbach (7 juin 1742)

- 271 ans
- **Énoncé** : Tout nombre pair ($n$) supérieur à 2 est la somme de deux nombres premiers.
- $\Longleftrightarrow$ Tout entier supérieur à 1 est la moyenne de deux nombres premiers $(\frac{1}{2}p_1 + \frac{1}{2}p_2)$.
- $98 = 19 + 79$
  $= 31 + 67$
  $= 37 + 61$

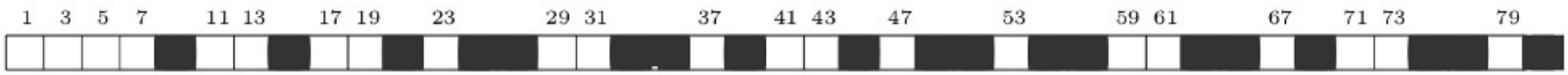
# Les tirettes de Laisant

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

- *"Ce fameux théorème empirique : Tout nombre pair est la somme de deux nombres premiers, dont la démonstration semble dépasser les possibilités scientifiques actuelles, a fait l'objet de nombreux travaux et de certaines contestations. Lionnet a tenté d'établir que la proposition devait probablement être inexacte. M. Georg Cantor l'a vérifiée numériquement jusqu'à 1000, en donnant pour chaque nombre pair toutes les décompositions en deux nombres premiers, et il a remarqué que le nombre de ces décompositions ne cesse de croître en moyenne, tout en présentant de grandes irrégularités."*

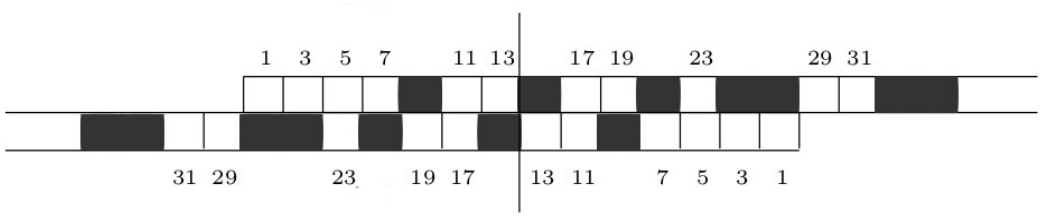
# Les tirettes de Laisant

- *"Voici un procédé qui permettrait de faire sans calculs la vérification expérimentale dont il s'agit, et d'avoir pour chaque nombre pair, à la seule inspection d'une figure, toutes les décompositions. Supposons que sur une bande formée de carrés accolés, représentant les nombres impairs successifs, on ait construit le crible d'Erathostène, en ombrant les nombres composés, jusqu'à une limite quelconque 2n."*



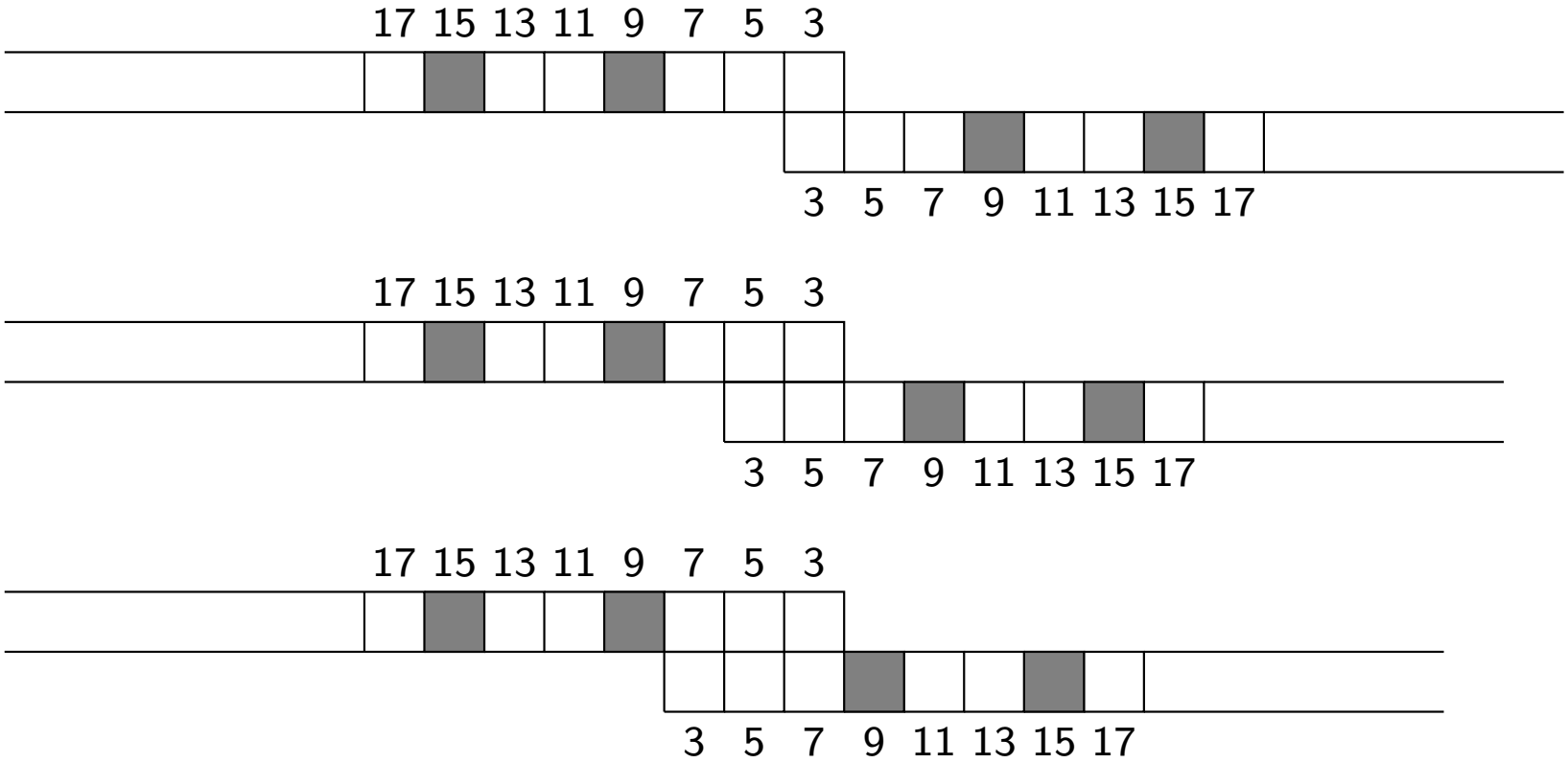
# Les tirettes de Laisant

- *"Si l'on a construit deux réglettes pareilles, et si l'on place la seconde au-dessous de la première en la retournant et en faisant correspondre la case* 1 *à* $2n$*, il est évident que si le théorème de Goldbach est vrai pour* $2n$*, il y aura quelque part deux cases blanches en correspondance ; et tous les couples de cases blanches donneront les diverses décompositions. On les aura même en lisant la moitié de la figure, à cause de la symétrie par rapport au milieu. Ainsi la vérification relative au nombre* 28 *donnera la figure 2 et montrera qu'on a les décompositions* $28 = 5 + 23 = 11 + 17$*."*



# Les tirettes de Laisant

- *"On comprend que les réglettes étant construites à l'avance, et un simple glissement permettant de passer d'un nombre à un autre, les vérifications sont très rapides."*



# Booléens

- On représente la primalité par des booléens.
- 0 signifie *est premier*, 1 signifie *est composé*.
- $23 \rightarrow 0$
- $25 \rightarrow 1$
- 

| 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 | ... |

# Copie de l'espace : matrices à 2 booléens

- On représente les décompositions de $n$ en sommes de deux nombres impairs par des matrices à 2 booléens (le booléen du nombre le plus petit en bas).
- $28 = \underset{p}{5} + \underset{p}{23} \rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} = a$
- $28 = \underset{c}{9} + \underset{p}{19} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} = b$
- $28 = \underset{p}{3} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = c$
- $40 = \underset{c}{15} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix} = d$

# Mots de 40, 42 et 44

| 40 | 37 | 35 | 33 | 31 | 29 | 27 | 25 | 23 | 21 |
|---|---|---|---|---|---|---|---|---|---|
| | 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* |

| 42 | 39 | 37 | 35 | 33 | 31 | 29 | 27 | 25 | 23 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 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* |

| 44 | 41 | 39 | 37 | 35 | 33 | 31 | 29 | 27 | 25 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 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* |

# Opérations sur les matrices

- Règle générale :

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

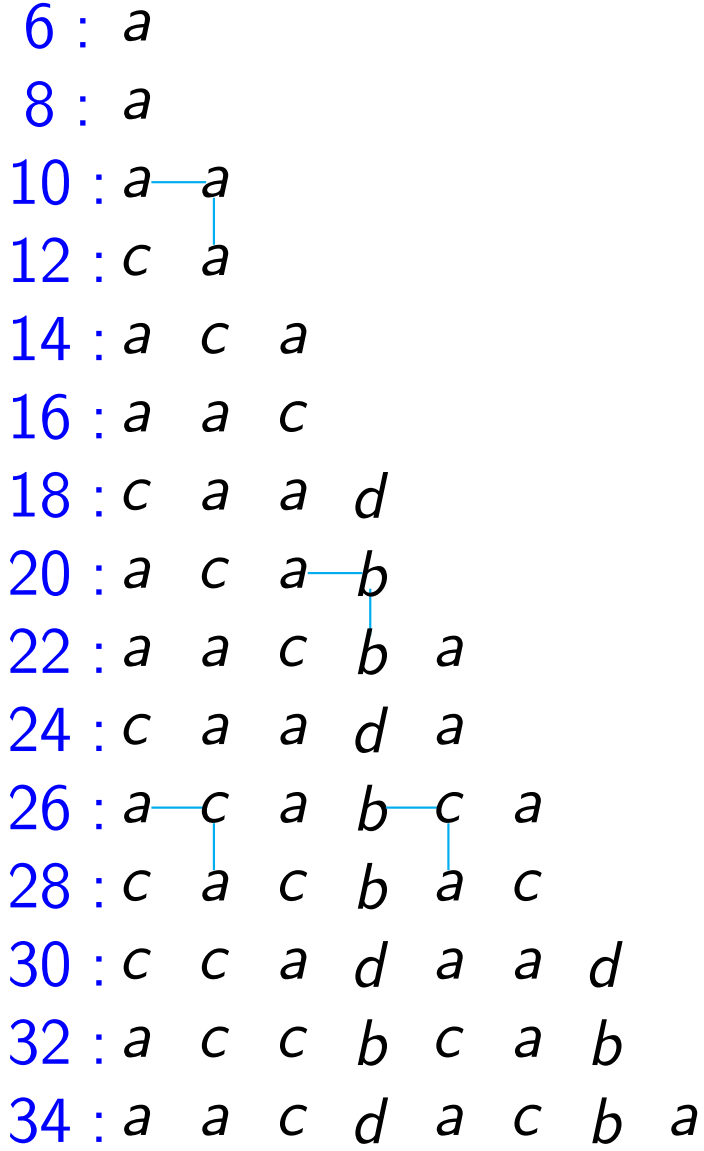
- Exemple :

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

- Règles particulières :

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

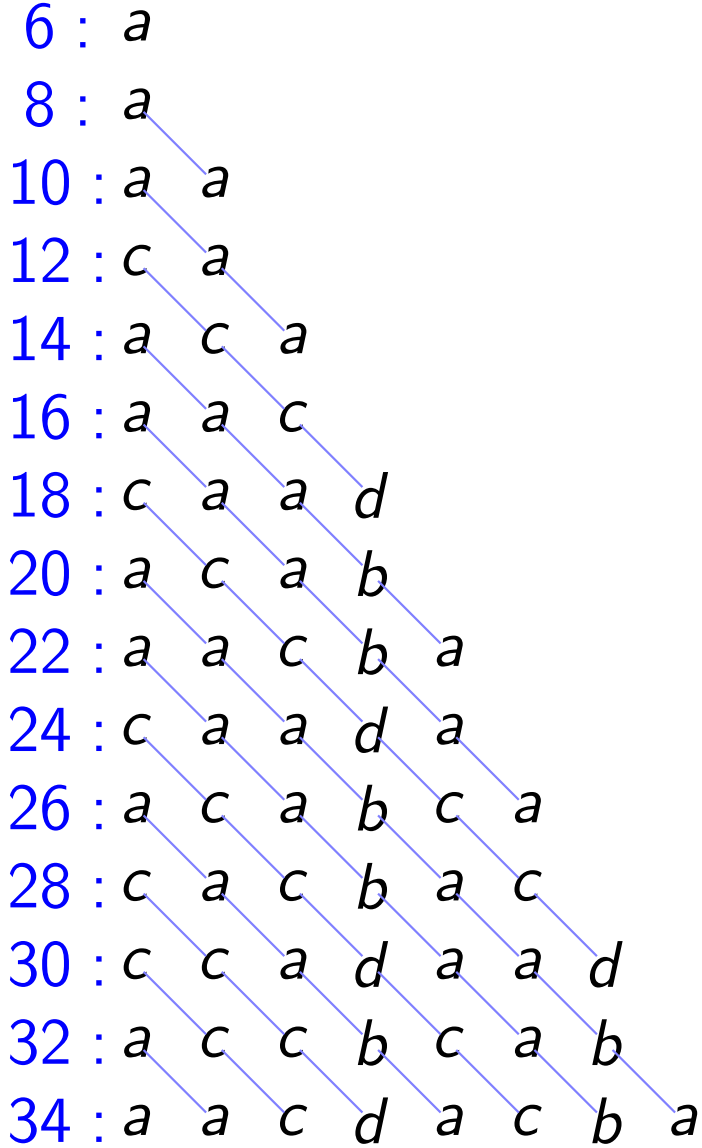
# Observer les mots : 16 règles de réécriture



# Rappels de théorie des langages

- Un alphabet est un ensemble fini de symboles.
- Les alphabets utilisés ci-après sont :
  $A = \{a, b, c, d\}, A_{ab} = \{a, b\}, A_{cd} = \{c, d\}, A_{ac} = \{a, c\}$ et $A_{bd} = \{b, d\}$.
- Un mot sur l'alphabet $X$ est une séquence finie et ordonnée, éventuellement vide, d'éléments de l'alphabet. C'est une concaténation de lettres. On note $X^*$ l'ensemble des mots sur l'alphabet $X$.
- Un mot est préfixe d'un autre s'il contient, sur toute sa longueur, les mêmes lettres aux mêmes positions (Soient un alphabet $X$ et $w, u \in X^*$. $u$ est préfixe de $w$ si et seulement si $\exists v \in X^*$ tel que $w = u.v$).

# Observer les mots diagonaux



# Propriétés des mots diagonaux

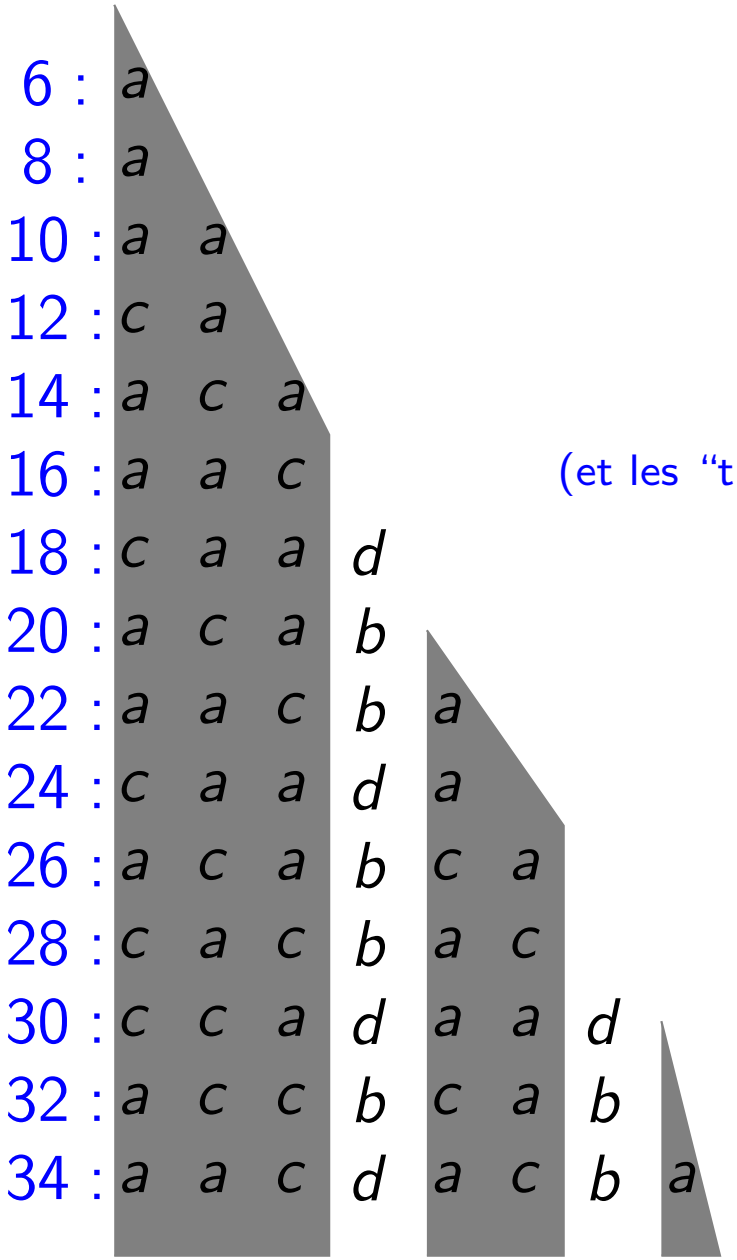
- Les mots diagonaux (diagonales) ont leurs lettres soit dans l'alphabet $A_{ab}$ soit dans l'alphabet $A_{cd}$.
- Toute diagonale est préfixe de la diagonale suivante définie sur le même alphabet.
- Une diagonale code en effet des décompositions de même second sommant et de premier sommant un nombre impair de la liste des impairs successifs à partir de 3.
- Par exemple, la diagonale *aaaba*, qui commence au *a* première lettre du mot de 26 sur la figure 1 code les décompositions $3+23, 5+23, 7+23; 9+23, 11+23$ et $13+23$.

# Propriétés des mots diagonaux

- Ainsi, les diagonales sur l'alphabet $A_{ab}$ "codent" les décompositions dont le second sommant est premier ; les lettres de telles diagonales codent soit par des $a$ correspondant aux nombres premiers, soit par des $b$ correspondant aux nombres composés la séquence des caractères de primalité des entiers impairs, à partir de 3.

- Les diagonales sur l'alphabet $A_{cd}$ "codent" quant à elles des décompositions dont le second sommant est composé ; les lettres de telles diagonales codent soit par des $c$ correspondant aux nombres premiers, soit par des $d$ correspondant aux nombres composés la séquence des caractères de primalité des entiers impairs, à partir de 3.

# Observer les mots verticaux

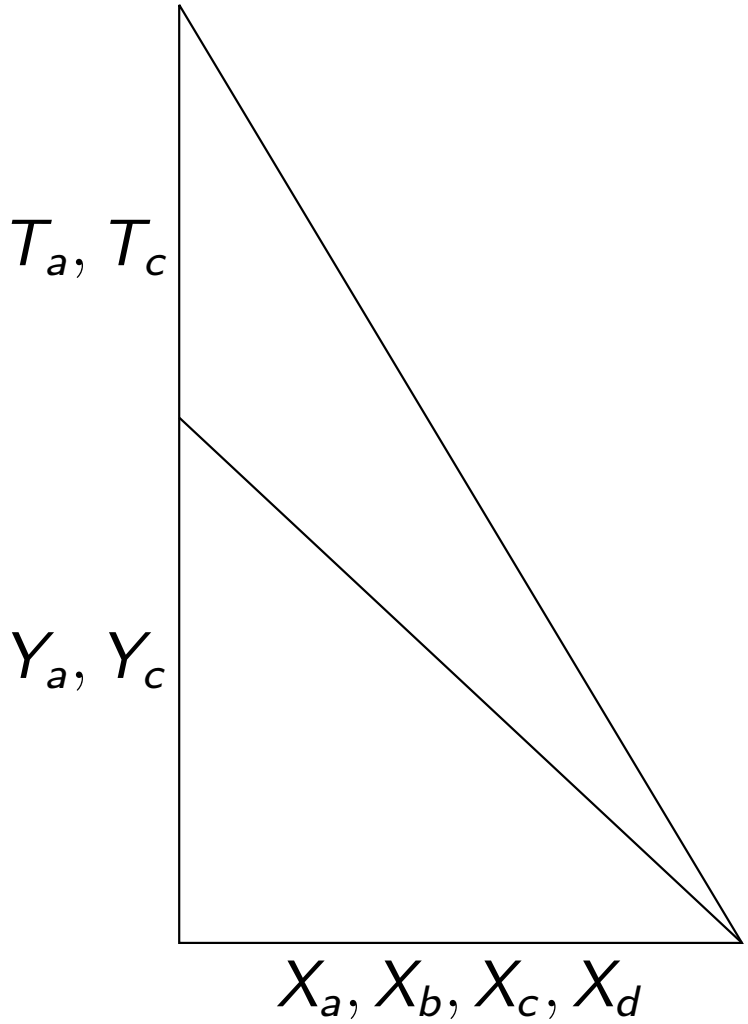



(et les “tranches” verticales)

# Propriétés des mots verticaux

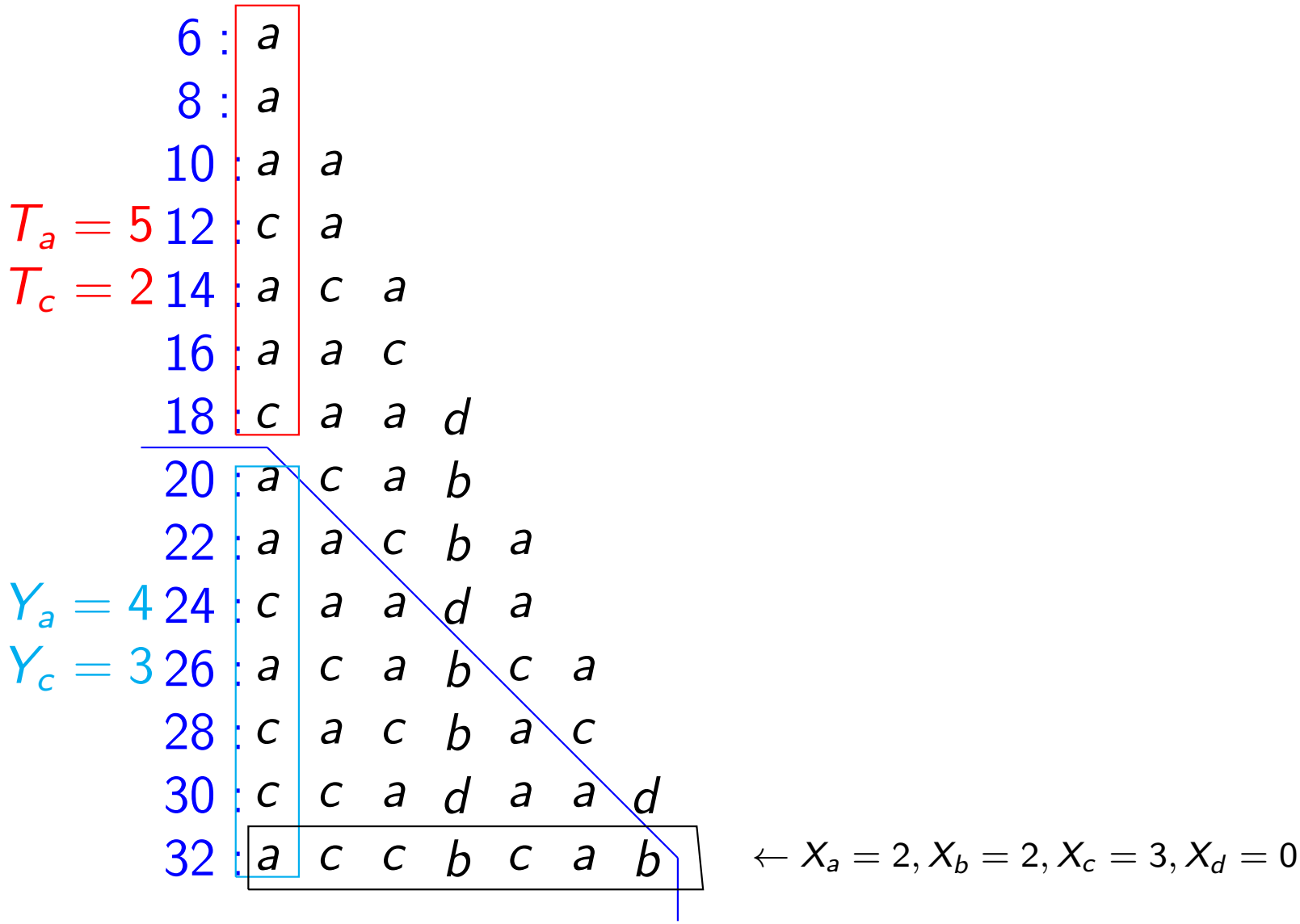
- Les mots verticaux ont leurs lettres soit dans l'alphabet $A_{ac}$ soit dans l'alphabet $A_{bd}$.
- Un mot vertical code des décompositions successives en somme de deux impairs de même premier sommant.
- Tout mot vertical est contenu dans un mot vertical qui se trouve à sa gauche et qui est défini sur le même alphabet.

# $n$ ne vérifie pas la conjecture de Goldbach.

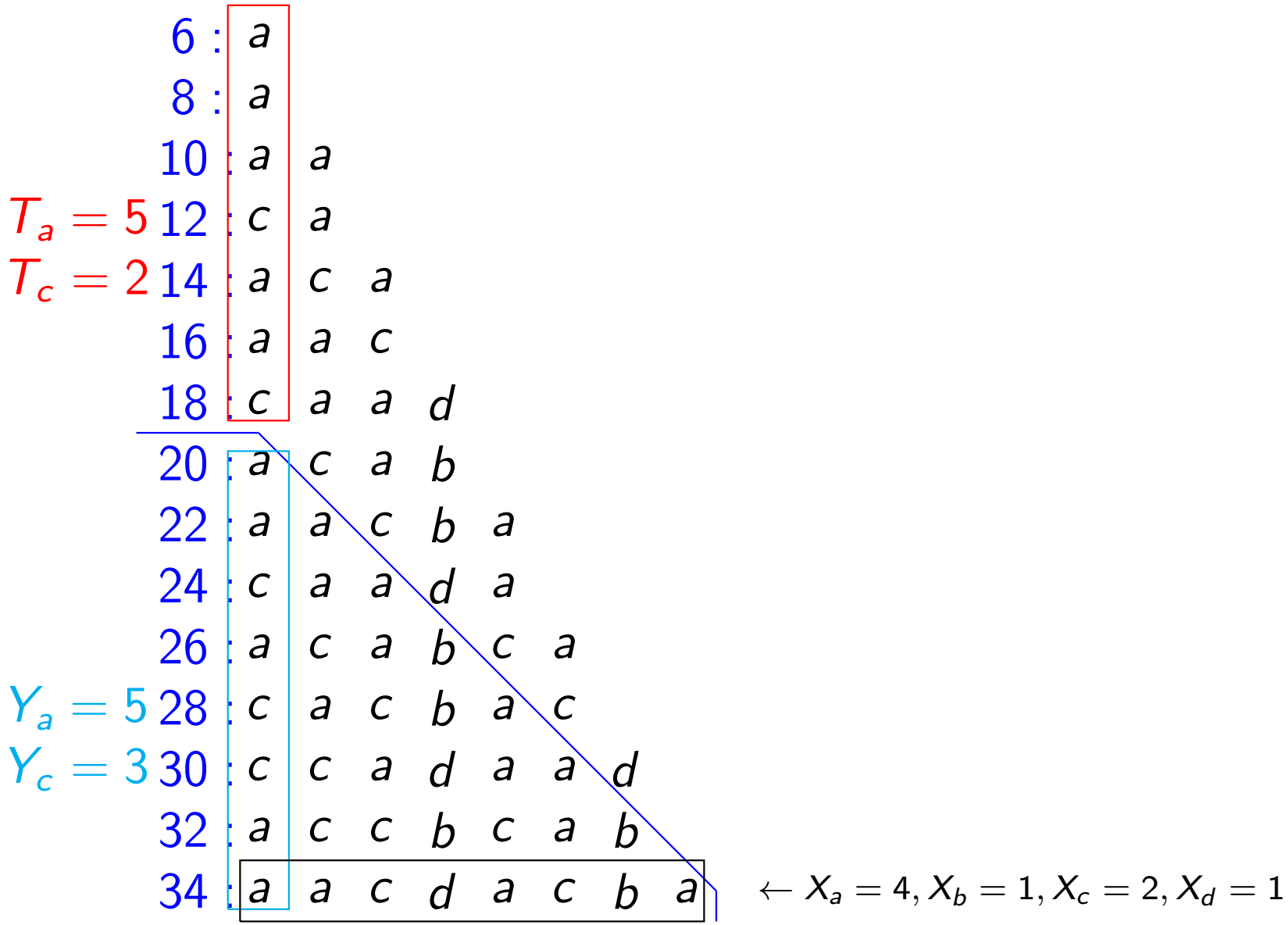



- Les variables sont liées.

# $n$ ne vérifie pas la conjecture de Goldbach.



# $n$ ne vérifie pas la conjecture de Goldbach.



# Bijections à la Cantor

- $T_a$ compte les décompositions de la forme $n' = 3 + p_i$, $p_i$ premier, $n' \leqslant 2\left\lceil \frac{n+2}{4} \right\rceil$.
- Par exemple, pour $n = 34$,
  $T_a = \#\{3+3, 3+5, 3+7, 3+11, 3+13\}$.
- $T_c$, quant à elle, compte les décompositions de la forme $n' = 3 + c_i$, $c_i$ composé $n' \leqslant 2\left\lceil \frac{n+2}{4} \right\rceil$.
- Par exemple, pour $n = 34$, $T_c = \#\{3+9, 3+15\}$.

# Bijections à la Cantor

- Cette bijection triviale sur le deuxième sommant permet d'expliquer aisément pourquoi $Y_a = X_a + X_b$ ou bien pourquoi $Y_c = X_c + X_d$. La simple présentation des ensembles en extension suffit à s'en convaincre.

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

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

# Bijections à la Cantor

- La bijection $f$ qui permet de passer de la ligne 2 du tableau la ligne 1 est telle que $f(a) = f(c) = a$ et $f(b) = f(d) = c$.
- La bijection $g$ qui permet de passer de la ligne 2 du tableau la ligne 3 est telle que $g(a) = g(b) = a$ et $g(c) = g(d) = c$.
- C'est la duplication de la dcomposition $3 + n/2$ dans le cas des doubles d'impairs qui ncessite l'introduction de la variable $\epsilon$ qui vaut alors 1 et 0 sinon.

# Bijections à la Cantor

- 

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

- 

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

# $n$ ne vérifie pas la conjecture de Goldbach.

- Les contraintes suivantes sont toujours vérifiées :

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

- $\epsilon = 1$ si $n$ est un double d'impair, $\epsilon = 0$ sinon.
- $m_n$ ne contenant aucune lettre $a$, on a $X_a = 0$.
- Mais puisque $Y_a = X_a + X_b$, on a alors $Y_a = X_b$.

# $n$ ne vérifie pas la conjecture de Goldbach.

- En identifiant $Y_a$ à $X_b$ et $Y_c$ à $X_c + X_d$ dans la dernière contrainte toujours respectée, on obtient la suite d'égalités suivante :

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

- Rappel du sens des variables :
  - $T_a + T_c = \left\lfloor \frac{n-4}{4} \right\rfloor$ ;
  - $X_b$ compte le nombre de décompositions de $n$ sous la forme d'une somme de deux nombres impairs $p + q$ avec $p \leqslant n/2$ composé et $q$ premier ;
  - $Y_c$ compte le nombre de nombres composés impairs compris entre $n/2$ et $n - 3$.

# $n$ ne vérifie pas la conjecture de Goldbach.

- Le nombre $X_b$ de décompositions de $n$ sous la forme d'une somme de deux nombres impairs $p+q$ avec $p \leqslant n/2$ composé et $q$ premier étant forcément inférieur au nombre de nombres premiers compris entre $n/2$ et $n-3$, on a $X_b < Y_a$ (on a utilisé ici une sorte de "principe des tiroirs" inversé : si on met 0 ou 1 objet dans $k$ tiroirs, on ne peut avoir plus d'objets que de tiroirs, i.e. plus de $k$ objets). Mais le nombre de nombres premiers contenus dans un intervalle est toujours inférieur au nombre de nombres composés contenus dans cet intervalle (pour $n > 100$). Donc $Y_a < Y_c$. Donc $X_b + Y_c < Y_a + Y_c < 2Y_c$.

- $\left\lfloor \frac{n-4}{4} \right\rfloor$ est pour tout entier supérieur à un certain entier assez petit (comme 100) supérieur à $2Y_c$. Cela assure qu'on a jamais l'égalité $T_a + T_c + \epsilon = X_b + Y_c$ qui découlerait de l'absence de lettre $a$ dans un mot.

# Conclusion

- On a utilisé un langage à 4 lettres pour représenter les décompositions de $n$ comme somme de deux impairs.
- Les règles de réécriture préservent la largeur des “tranches de lettres”.
- On se situe dans une théorie lexicale des nombres, selon laquelle les nombres sont des mots.
- Il faut toujours bien observer l'ordre des lettres dans les mots.