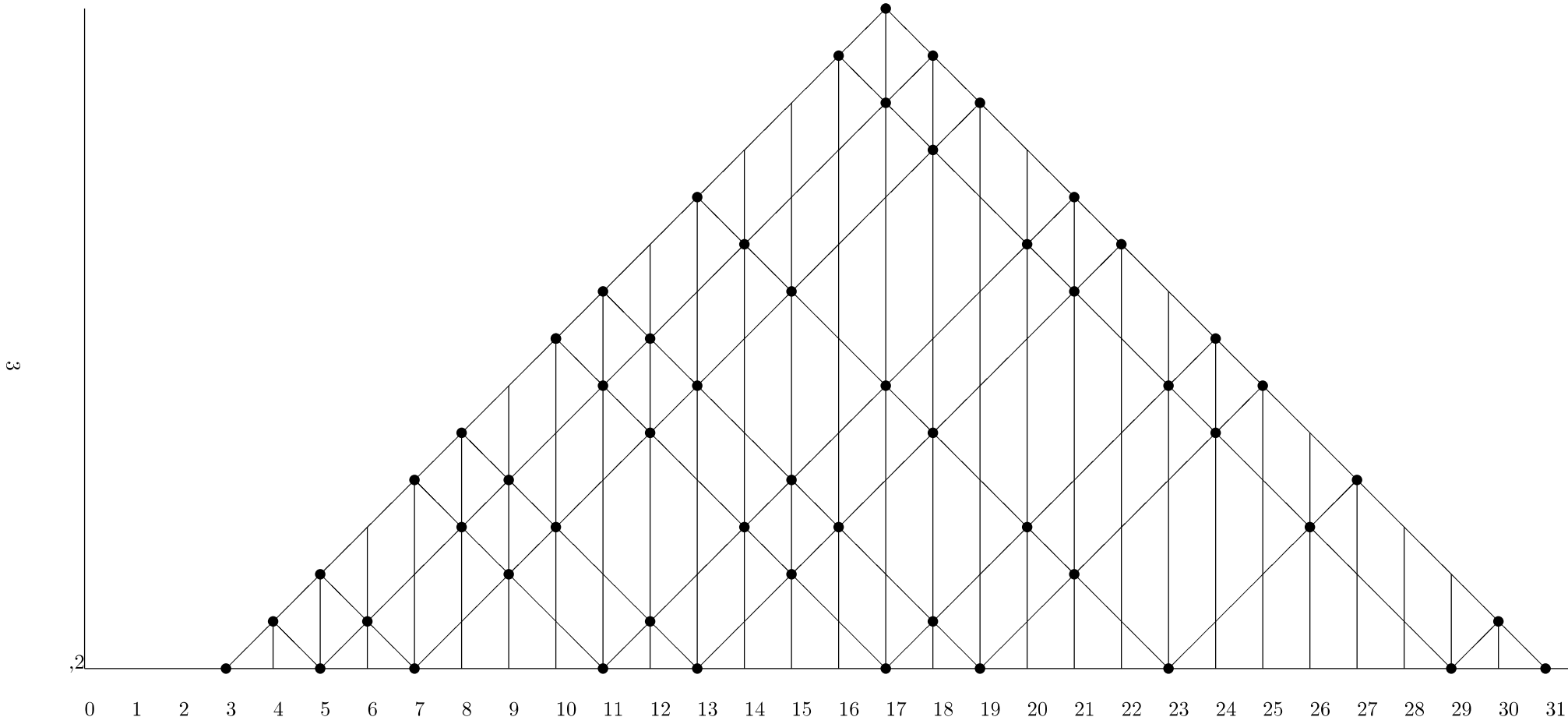


Figure 1: Le treillis Goldbach

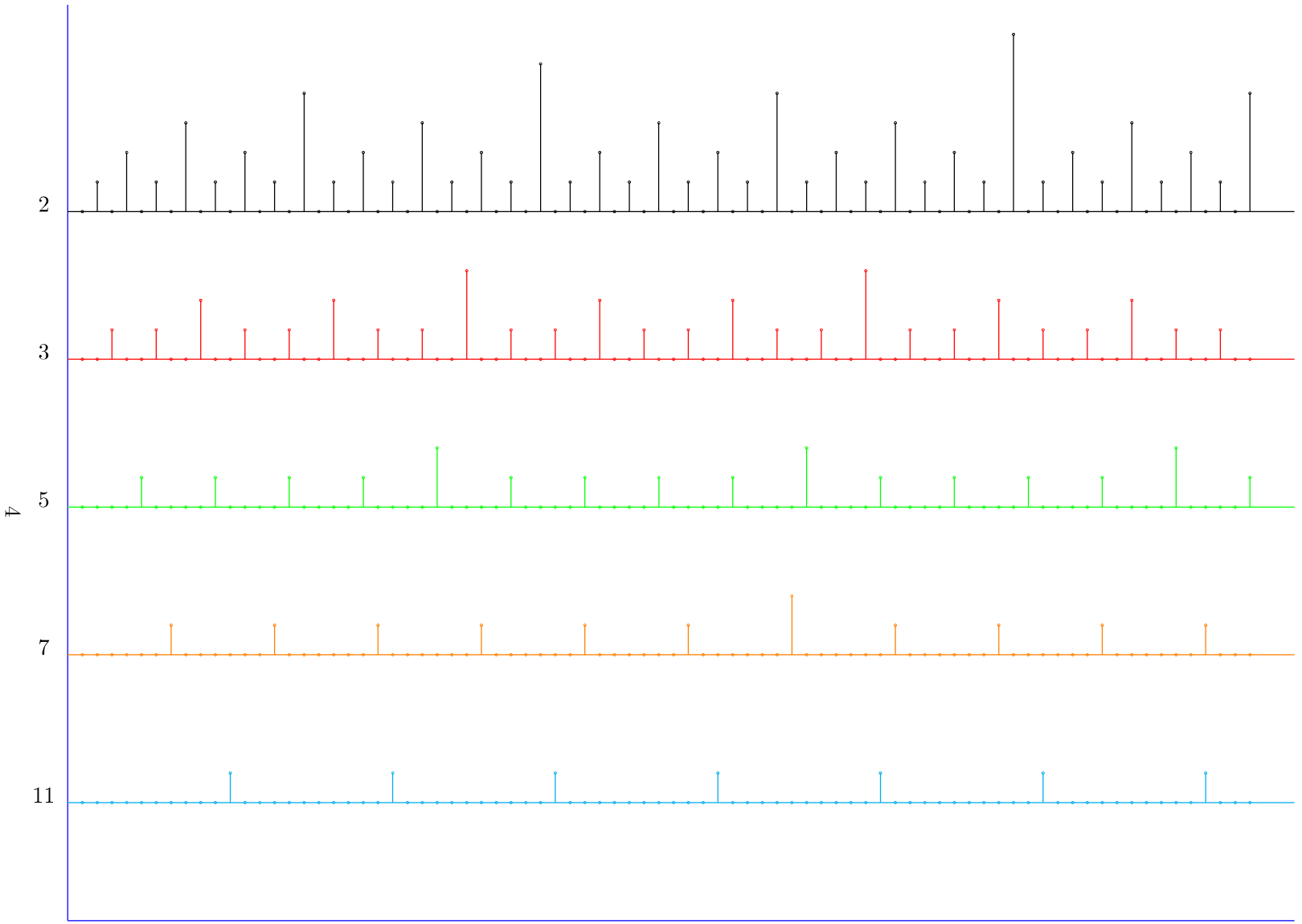
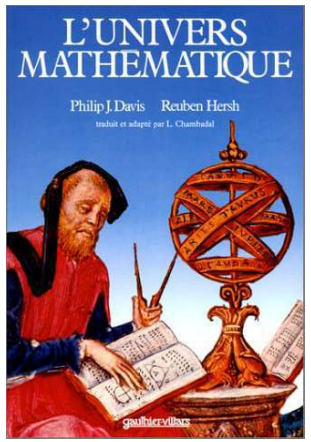


Figure 1 : Séquences fractales de valuations p-adiques

Le partage de *dg*

- $20902 = 3 + 20899$ $20962 = 3 + 20959$
  $20904 = 5 + 20899$ $20964 = 5 + 20959$
  $20906 = 3 + 20903$ $20966 = 3 + 20963$
  $20908 = 5 + 20903$ $20968 = 5 + 20963$
  $20910 = 7 + 20903$ $20970 = 7 + 20963$
  $20912 = 13 + 20899$ $20972 = 13 + 20959$
  $20914 = 11 + 20903$ $20974 = 11 + 20963$
  $20916 = 13 + 20903$ $20976 = 13 + 20963$
  $20918 = 19 + 20899$ $20978 = 19 + 20959$
  $20920 = 17 + 20903$ $20980 = 17 + 20963$
  $20922 = 19 + 20903$ $20982 = 19 + 20963$
  $20924 = 3 + 20921$ $20984 = 3 + 20981$



- Des causes différentes produisent les mêmes effets (écart de 60, congrus mod 3 et 5).

Permutations des racines

- $$\begin{array}{ccc} 2p_i & \xrightarrow{f} & 2c \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ p_i & \xrightarrow{f} & p_j \end{array}$$

- $$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ \mathbb{Z}/3\mathbb{Z} \setminus \{0,1\} \times \mathbb{Z}/5\mathbb{Z} \setminus \{0,4\} \times \mathbb{Z}/7\mathbb{Z} \setminus \{0,3\} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z} \setminus \{0,1\} \times \mathbb{Z}/5\mathbb{Z} \setminus \{0,3\} \times \mathbb{Z}/7\mathbb{Z} \setminus \{0,4\} \end{array}$$

Permutations des racines

- $$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

- $\mathbb{Z}/3\mathbb{Z} \to Id$,
  $\mathbb{Z}/5\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 3 \end{pmatrix}$,
  $\mathbb{Z}/7\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$

Conclusion

- On a utilisé un SNURPF : un Système de NUmération par les Restes dans les Parties Finies de $\mathbb{N}$.

- On se situe dans une théorie lexicale des nombres, selon laquelle les nombres sont des mots.

Continuer de suivre Galois (DV - 21/12/2013)

On cherche une équation polynomiale qui aurait ses racines qui se verraient permutées par une certaine fonction et dont les solutions seraient les décomposants de Goldbach de n, un nombre pair, i.e. les nombres premiers dont les complémentaires à n seraient premiers également.

On "sent bien" que le générateur doit sûrement être la fonction $f : x \mapsto n - x$ car cette fonction envoie chaque nombre entier sur son complémentaire à n, la somme de ces deux nombres permettant d'obtenir n.

On trouve donc l'inéquation polynomiale $x^2 - nx \neq 0$ qui est invariante par la fonction f. En effet, $(n-x)^2 - n(n-x) = x^2 + n^2 - 2nx - n^2 + nx = x^2 - nx$. On est conforté dans cette idée par le fait que le polynôme proposé est égal à $x(n-x)$:

- d'une part, ce polynôme s'annule lorsque x est nul et la congruence $x \not\equiv 0 \ (mod\ p_i)$ dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ pour p_i un nombre premier quelconque inférieur à $\sqrt{n}$ correspond au fait que x est un nombre premier supérieur à $\sqrt{n}$;

- d'autre part, ce polynôme s'annule lorsque $x = n$ et la congruence $x \not\equiv n \ (mod\ p_i)$ dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ pour p_i un nombre premier quelconque inférieur à $\sqrt{n}$ correspond au fait que le complémentaire de x à n est premier.

Il faudrait pour prouver la conjecture de Goldbach être assuré que cette inéquation polynomiale $x^2 - nx \neq 0$ a une solution commune inférieure à $n/2$ dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ avec p_i un nombre premier quelconque inférieur à $\sqrt{n}$.

Traitons l'exemple de la recherche des décompositions de Goldbach de 98.
Le polynôme $x^2 - 98x$ est égal à $x^2 - 2x$ dans $\mathbb{Z}/3\mathbb{Z}$ tandis qu'il est égal à $x^2 - 3x$ dans $\mathbb{Z}/5\mathbb{Z}$, ou encore égal à x^2 tout simplement dans $\mathbb{Z}/7\mathbb{Z}$ puisque 7 divise 98.

Notons dans un tableau pour les nombres premiers supérieurs à $\sqrt{98}$ et inférieurs à 49 la moitié de 98 les valeurs des polynômes en question et voyons ceux qui sont éliminés dans chacun des corps premiers.

	11	13	17	19	23	29	31	37	41	43	47
x^2 (dont on teste la nullité dans $\mathbb{Z}/7\mathbb{Z}$)	121	169	289	361	529	841	961	1369	1681	1849	2209
$x^2 - 2x$ (dont on teste la nullité dans $\mathbb{Z}/3\mathbb{Z}$)	~~99~~	143	~~255~~	323	~~483~~	~~783~~	899	1295	~~1599~~	1763	~~2115~~
$x^2 - 3x$ (dont on teste la nullité dans $\mathbb{Z}/5\mathbb{Z}$)	88	~~130~~	238	304	~~460~~	754	868	1258	1558	~~1720~~	2068

On voit que ne sont conservés que les nombres 19, 31 et 37 qui sont comme attendu les décomposants de Goldbach de 98.

Le problème de Goldbach est en quelque sorte un problème "relatif" (puisqu'à la recherche des décomposants de Goldbach de n le nombre n intervient dans l'inéquation dont il faut chercher une solution commune dans tous les corps finis $\mathbb{Z}/p_k\mathbb{Z}$ pour $p_k \leqslant \sqrt{n}$).

On peut considérer que le problème des jumeaux est quant à lui le problème "absolu" correspondant au problème "relatif" de Goldbach. En effet, si l'on appelle "père de jumeaux" le nombre pair entre deux nombres premiers jumeaux (par exemple 18 entre 17 et 19 ou encore 570 entre 569 et 571), ce nombre doit vérifier l'inéquation "absolue" $x^2 \not\equiv 1 (mod\ p_k)$ pour tout $p_k \leqslant \sqrt{x+1}$ (il doit en effet vérifier simplement $(x-1)(x+1) \not\equiv 0 (mod\ p_k)$ pour qu'$x-1$ et $x+1$ soient premiers tous les deux). Un père de jumeau est obligatoirement de la forme $6k$. Fournissons dans un tableau la classe de congruence de x^2 selon les modules premiers impairs inférieurs à $\sqrt{x+1}$ qui nous permettent d'aisément trouver les pères de jumeaux jusqu'à 300.

père	*mod* 3	*mod* 5	*mod* 7	*mod* 11	*mod* 13	*mod* 17	*jumeaux*
6							$(5,7)$
12	0						$(11,13)$
18	0						$(17,19)$
24	0	1					
30	0	0					$(29,31)$
36	0	1					
42	0	4					$(41,43)$
48	0	4	1				
54	0	1	4				
60	0	0	2				$(59,61)$
66	0	1	2				
72	0	4	4				$(71,73)$
78	0	4	1				
84	0	1	0				
90	0	0	1				
96	0	1	4				
102	0	4	2				$(101,103)$
108	0	4	2				$(107,109)$
114	0	1	4				
120	0	0	1	1			
126	0	1	0	3			
132	0	4	1	0			
138	0	4	4	3			$(137,139)$
144	0	1	2	1			
150	0	0	2	5			$(149,151)$
156	0	1	4	4			
162	0	4	1	9			
168	0	4	0	9	1		
174	0	1	1	4	12		
180	0	0	4	5	4		$(179,181)$
186	0	1	2	1	3		
192	0	4	2	3	9		$(191,193)$
198	0	4	4	0	9		$(197,199)$
204	0	1	1	3	3		
210	0	0	0	1	4		
216	0	1	1	5	12		
222	0	4	4	4	1		
228	0	4	2	9	10		$(227,229)$
234	0	1	2	9	0		
240	0	0	4	4	10		$(239,241)$
246	0	1	1	5	1		
252	0	4	0	1	12		
258	0	4	1	3	4		
264	0	1	4	0	3		
270	0	0	2	3	9		$(269,271)$
276	0	1	2	1	9		
282	0	4	4	5	3		$(281,283)$
288	0	4	1	4	4		
294	0	1	0	9	12	8	
300	0	0	1	9	1	2	

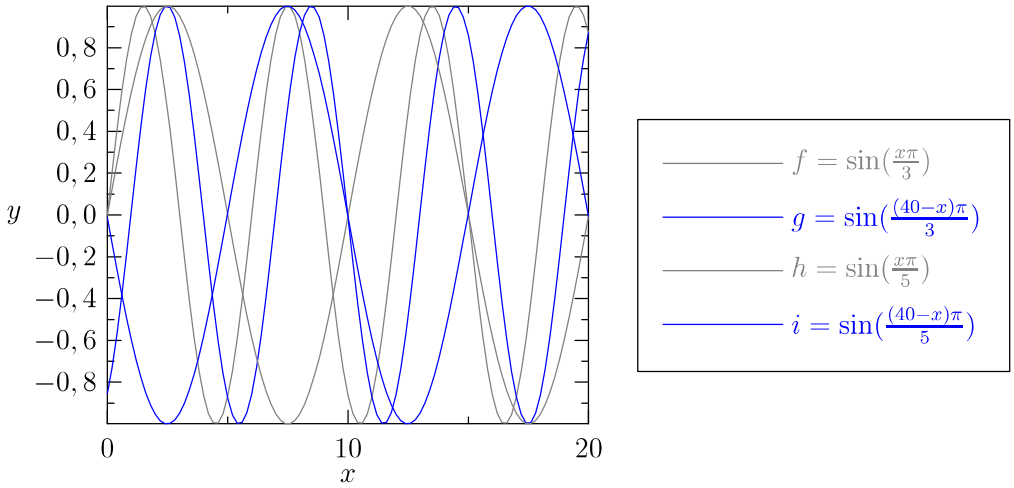
On ne réexplique pas ici la représentation par les grilles de divisibilité qui nous a permis de mieux comprendre la conjecture de Goldbach et dont l'exemple du nombre pair 40 est représenté ci-dessus. 11 et 17, qui ne sont divisibles ni par 3 ni par 5 et qui ne partagent avec 40 aucun de leur reste dans des divisions euclidiennes par 3 ou 5 (i.e. dont la colonne ne contient pas de case colorée) sont des décomposants de Goldbach de 40.

On a proposé à partir de ces grilles la possibilité de trouver les décomposants de Goldbach en calculant des produits de sinusoïdes.

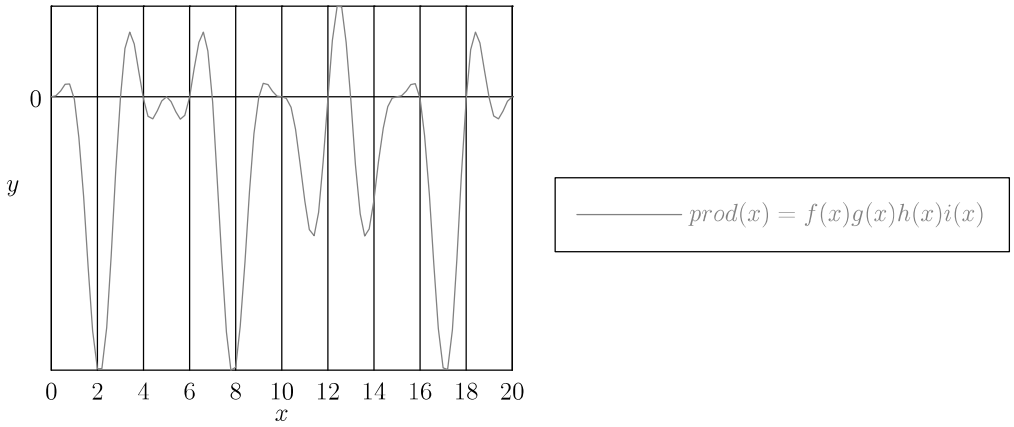
Les décomposants de Goldbach de n sont en effet les seuls nombres entiers impairs inférieurs à $n/2$ qui n'annulent pas le produit suivant :

$$\prod_{3 \leqslant p \ un \ nb \ 1^{er} \leqslant \sqrt{n}} sin\left(\frac{x\pi}{p}\right).sin\left(\frac{(n-x)\pi}{p}\right)$$

Les sinusoïdes correspondant au cas du nombre pair 40 (se reporter à la grille de divisibilité ci-dessus) sont :



Leur produit ne s'annule effectivement pas pour les nombres entiers impairs 11 et 17.

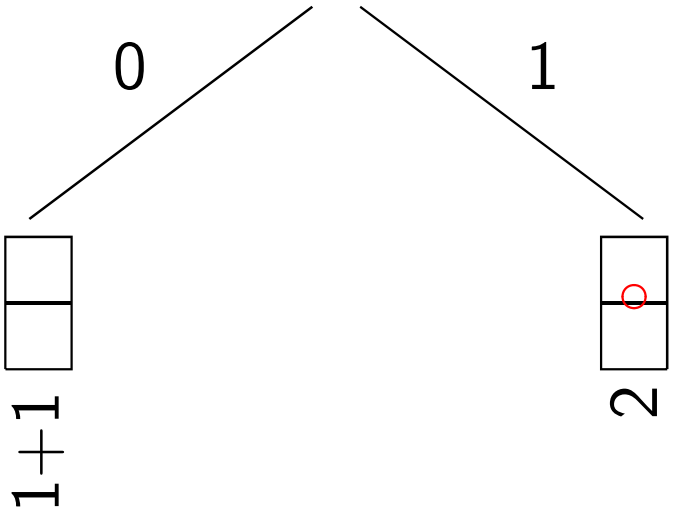


On peut établir une analogie entre ces sinusoïdes et les fonctions d'onde de la mécanique quantique. En poussant l'analogie, on peut imaginer qu'on puisse établir une probabilité qu'un nombre pair ait un décomposant de Goldbach sans pouvoir établir sa valeur, selon une sorte de principe d'incertitude.

Enfin, si on souhaite établir une analogie avec la propriété d'*intrication quantique* : on associe à chaque case de la grille de divisibilité ci-dessus un q-bit qui est simultanément dans les états 0 et 1. On peut imaginer cette grille comme de taille infinie si on considère tous les nombres pairs d'un même coup. Le fait de fixer

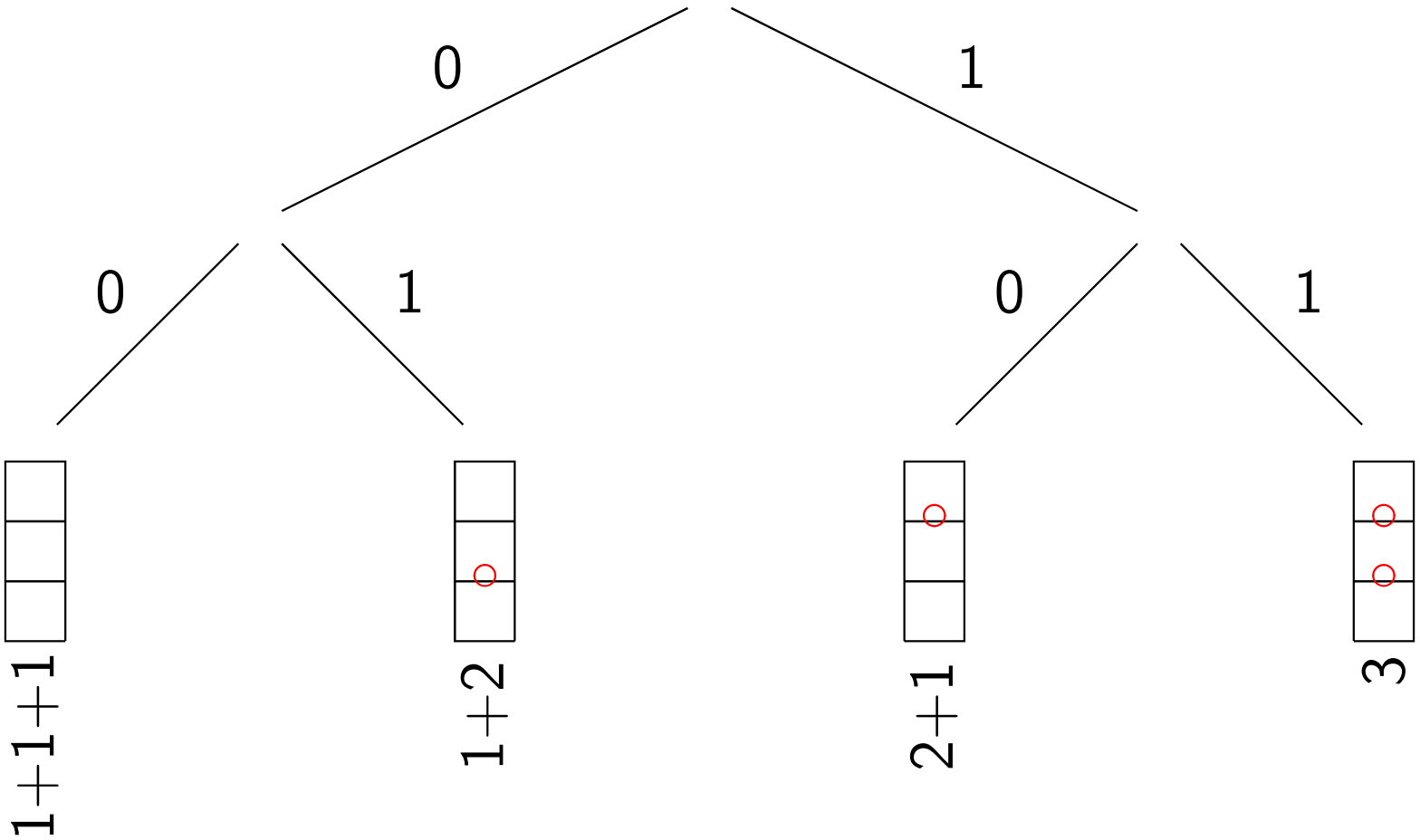
Compositions et mots booléens

- A chaque entier n, on associe ses 2^{n-1} compositions additives.
- *exemple* : arbre binaire des compositions de 2



Exemple

- *exemple* : arbre binaire des compositions de 3



- Noter que la composition $1+2$ est différente de la composition $2+1$.

Obtention des compositions de $n+1$ à partir de celles de n

- On concatène 0 ou 1 au début de chaque mot booléen de n.
- Cela correspond à deux actions syntaxiques : concaténer “1+” en début de composition ou bien remplacer le premier sommant par son successeur.

Nombre composé / nombre premier

- On appelle compositions triviales la composition correspondant au mot booléen ne contenant que des 0 (composition de la forme $1+1+\ldots+1$) ou bien la composition correspondant au mot booléen contenant $n-1$ lettres 1 (composition de la forme n).

- Un nombre composé admet au moins une décomposition non triviale de la forme $x+x+x+\ldots+x$ contenant 2 occurrences de x au moins.

- A chaque entier est associé un ensemble de mots booléens, i.e. un ensemble de parties de $\mathbb{N}$.

$$\mathbb{N} \longrightarrow \{0,1\}^{\{0,1\}^{\mathbb{N}}}$$
$$n \longmapsto \{s \in \{0,1\}^{\mathbb{N}} / \forall i \geqslant n, s[i] = 0\} \subset \mathcal{P}(\mathbb{N})$$

Formalisation

- Le passage de n à $n+1$ est codé par le diagramme suivant :

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{d_n} & \{0,1\}^{\{0,1\}^{\mathbb{N}}} \\ {\scriptstyle +1}\downarrow & & \downarrow{\scriptstyle d_{n+1}} \\ \mathbb{N} & \xrightarrow[d_n]{} & \{0,1\}^{\{0,1\}^{\mathbb{N}}} \end{array}$$

avec $d_n : \mathbb{N} \longrightarrow \{0,1\}$

et

$$d_{n+1} : \begin{array}{ccc} k & \longmapsto & d_n(k-1), \forall k \geqslant 1 \\ 0 & \longmapsto & 0 \end{array}$$

- faire l'union de cet ensemble de fonctions avec l'ensemble des fonctions d_{n+1} qui associent l'image 1 (plutôt que 0) à 0.

Nombre composé / nombre premier

- Un nombre est composé n si l'un de ces mots non triviaux (dont on considère les $n-1$ premières lettres, i.e. la partie des mots avant l'infinité de zéros) admet une période (c'est un motif qui se répète, en théorie des langages).

- Un nombre est premier si tous ses mots sont apériodiques.