Etude de la Conjecture de Goldbach

Denise Vella-Chemla

24/4/2012

- **Conjecture de Goldbach** (7 juin 1742) : tout nombre pair supérieur ou égal à 4 est somme de deux nombres premiers.
- Vinogradov (1937)
- Chen Jingrun (1966)
- vérifiée par ordinateur jusqu'à 4.10^{18}
  (Oliveira e Silva, 4.4.2012)
- 270 ans

- $\forall\, n \geq 6, \exists\, p \leq n/2, \exists\, q \geq n/2,\ p \text{ et } q \text{ premiers impairs},$
  $n = p + q$
- $\forall\, n \geq 6,$
  $\exists\, p \leq n/2,\ p \text{ premier impair},$
  $\forall\, q \leq \sqrt{n},\ q \text{ premier impair},$
  $p \not\equiv n \,(mod\ q)$
- $p \not\equiv n \,(mod\ q) \iff n - p \not\equiv 0 \,(mod\ q) \iff n - p \text{ premier}$

Exemple :

$98 \equiv 3 \pmod 5$ (98-3=95 et 5 | 95)

$98 \equiv 5 \pmod 3$ (98-5=93 et 3 | 93)

$98 \equiv 7 \pmod 7$ (98-7=91 et 7 | 91)

$98 \equiv 11 \pmod 3$ (98-11=87 et 3 | 87)

$98 \equiv 13 \pmod 5$ (98-13=85 et 5 | 85)

$98 \equiv 17 \pmod 3$ (98-17=81 et 3 | 81)

$98 \not\equiv 19 \pmod 3$ (98-19=79 et $3 \nmid 79$)

$98 \not\equiv 19 \pmod 5$ (98-19=79 et $5 \nmid 79$)

$98 \not\equiv 19 \pmod 7$ (98-19=79 et $7 \nmid 79$)

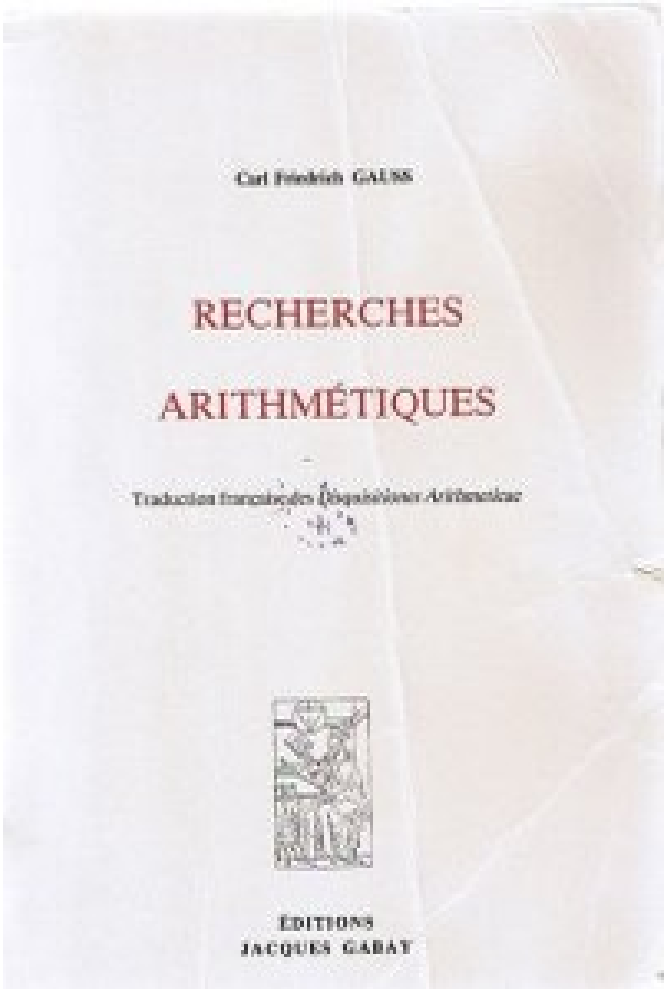
- $(\exists\, n \geq 6, \forall\, p \leq n/2, \exists\, q \leq \sqrt{n},\ p \text{ et } q \text{ premiers impairs},\ n \equiv p\ (mod\ q))$

  $\Longrightarrow\ false$

- $n \equiv p\ (mod\ q) \iff n - p \equiv 0\ (mod\ q) \iff n - p$ composé

- **Théorème des restes chinois**
- $$\begin{cases} n \equiv 1 \ (mod\ 3) \\ n \equiv 3 \ (mod\ 5) \\ n \equiv 5 \ (mod\ 7) \end{cases}$$
- $5 \times 7 = 35,\ 3 \times 7 = 21,\ 3 \times 5 = 15, 3 \times 5 \times 7 = 105.$
- $2 \times 35 \equiv 1 \ (mod\ 3),\ 21 \equiv 1 \ (mod\ 5),\ 15 \equiv 1 \ (mod\ 7)$
- $1 \times 70 + 3 \times 21 + 5 \times 15 = 70 + 63 + 75 = 208 = 103 \ (mod\ 105)$ qui sont les nombres de la suite $103, 208, 313, \ldots$
- $$\begin{cases} n \equiv 3 \ (mod\ 5) \\ n \equiv 5 \ (mod\ 7) \end{cases}$$
- $3 \times 21 + 5 \times 15 = 63 + 75 = 138 = 33 \ (mod\ 35)$ qui sont les nombres de la suite $33, 68, 103, 138, 173, 208, 243, 278, 313, \ldots$

- **Gauss, 1801, Recherches Arithmétiques**
- Articles 33 à 36 de la Section 2 : Des congruences du premier degré



33. Quand tous les nombres A, B, C, etc. sont premiers entre eux, leur produit est le plus petit nombre divisible par chacun d'eux; et dans ce cas il est évident que toutes les congruences $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, etc. se ramèneront à une seule $z \equiv r \pmod{R}$ qui leur équivaudra, R étant le produit des nombres A, B, C, etc.: il sort de là réciproquement qu'une seule condition $z \equiv r \pmod{R}$ peut être décomposée en plusieurs $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$; $z \equiv r \pmod{C}$, etc. si A, B, C, etc. sont les différens facteurs premiers entr'eux qui composent R. Cette observation nous donne non-seulement le moyen de découvrir l'impossibilité lorsqu'elle existe, mais encore une méthode plus commode et plus élégante pour déterminer les racines.

34. Soient comme ci-dessus les conditions $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$, etc. On résoudra tous les modules en facteurs premiers entr'eux; A en $A' A'' A'''$ etc.; B en $B' B'' B'''$ etc.; de manière que les nombres A', A'', etc., B', B'', etc. soient premiers ou puissances de nombres premiers; si l'un des nombres A, B, C, etc. était premier lui-même ou puissance d'un nombre premier, il n'y aurait, pour lui, aucune décomposition à faire. Alors ce qui précède fait voir que l'on peut, aux conditions données, substituer les suivantes $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$, etc.; $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$, etc., etc.; Or, à moins que tous les nombres A, B, C, etc. ne fussent premiers entr'eux; par exemple, si A n'est pas premier avec B, il est évident que tous les diviseurs premiers ne peuvent être différens dans A et dans B, mais qu'il doit y avoir quelqu'un des diviseurs A', A'', etc., qui trouve son égal, son multiple, ou son sous-multiple parmi les diviseurs B', B'', etc. Soit d'abord $A' = B'$, les conditions $z \equiv a \pmod{A'}$, $z \equiv b \pmod{B'}$, doivent être identiques, et l'on doit avoir $a \equiv b \pmod{A'}$ ou $\pmod{B'}$; ainsi l'une ou l'autre de ces deux conditions peut être rejetée; mais si l'on n'a pas $a \equiv b \pmod{A'}$, le problème est impossible. Soit ensuite B' un multiple de A', la condition $z \equiv a \pmod{A'}$ doit être contenue dans celle-ci, $z \equiv b \pmod{B'}$, ou bien celle-ci, $z \equiv b \pmod{A'}$, qui se déduit de la dernière, doit être équivalente à la première; d'où il suit que la condition $z \equiv a \pmod{A'}$, peut être rejetée, si elle ne contrarie pas l'autre, auquel cas le problème serait im-

C

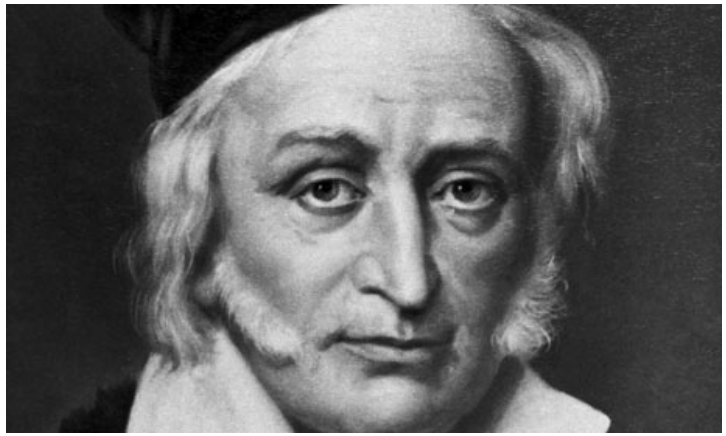
possible. Quand toutes les conditions superflues sont ainsi rejetées, il est évident que tous les modules qui restent sont premiers entr'eux ; on est sûr alors de la possibilité du problème, et on peut procéder d'après la manière enseignée plus haut.

55. Si nous supposons comme au n° 32 $z \equiv 17 \pmod{504}$, $\equiv -4 \pmod{35}$, $\equiv 33 \pmod{16}$; ces conditions peuvent se décomposer en celles qui suivent : $z \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$; $z \equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$; $z \equiv 33 \pmod{16}$. De ces conditions on peut rejeter $z \equiv 17 \pmod{8}$ et $z \equiv 17 \pmod{7}$, car la première est renfermée dans la condition $z \equiv 33 \pmod{16}$, et la seconde est équivalente à $z \equiv -4 \pmod{7}$: il reste ainsi

$$z \equiv \left\{ \begin{array}{l} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16} \end{array} \right\} \text{ d'où l'on tire } z \equiv 3041 \pmod{5040}.$$

Au reste il est clair qu'il sera souvent plus commode de ramener à une seule les conditions qui restent et qui proviennent de la même, ce qui se fera sans peine. Par exemple, quand on a rejeté quelques-unes des conditions $z \equiv a \pmod{A}$, $z \equiv a \pmod{A'}$, etc. celle qui se composera des conditions restantes sera $z \equiv a$, suivant le module formé par le produit de tous les modules qui restent. Ainsi dans notre exemple des conditions $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$; on tire sur-le-champ la condition $z \equiv -4 \pmod{35}$, d'où elles dérivent; il s'ensuit qu'il n'est pas indifférent, quant à la briéveté du calcul, de rejeter l'une ou l'autre des conditions équivalentes ; mais il n'entre pas dans notre plan de parler de ces détails ni d'autres artifices pratiques que l'usage apprend mieux que les préceptes.

56. Quand tous les modules A, B, C, etc. sont premiers entr'eux, il est préférable le plus souvent d'employer la méthode suivante. On déterminera un nombre α congru à l'unité suivant A, et à 0 suivant le produit des autres modules; c'est-à-dire, que α sera une valeur quelconque de l'expression $\frac{1}{BCD \text{ etc.}} \pmod{A}$, multipliée par BCD etc. (n° 32) ; mais il vaut mieux prendre la plus petite de ces valeurs. Soit de même $\beta \equiv 1 \pmod{B}$, et $\equiv 0 \pmod{ACD \text{ etc.}}$;



$\gamma \equiv 1 \pmod{C}$, et $\equiv 0 \pmod{ABD}$ etc.). Alors si l'on cherche un nombre z qui soit congru aux nombres a, b, c, etc. suivant les modules A, B, C, etc. respectivement, on pourra poser..... $z \equiv \alpha a + \beta b + \gamma c +$ etc. $\pmod{ABCD}$ etc.); en effet on a évidemment $\alpha a \equiv a \pmod{A}$, et les autres termes sont $\equiv 0 \pmod{A}$; donc $z \equiv a \pmod{A}$. La démonstration est la même pour les autres modules. Cette solution est préférable à la première; quand on a à résoudre plusieurs problèmes du même genre, pour lesquels les valeurs de A, B, C, etc. sont les mêmes; car alors on trouve pour α, β, etc. des valeurs constantes. Ceci s'applique au problème de chronologie dans lequel on cherche le quantième de l'année pour laquelle l'indiction, le nombre d'or et le cycle solaire sont donnés. Ici $A = 15$, $B = 19$, $C = 28$; ainsi comme la valeur de l'expression $\frac{1}{19.28} \pmod{15}$, ou $\frac{1}{532} \pmod{15}$ est 13, on aura $\alpha = 6916$; on trouvera de même $\beta = 4200$, $\gamma = 4845$. Donc le nombre cherché sera le résidu *minimum* du nombre $6916a + 4200b + 4845c$, a représentant l'indiction, b le nombre d'or, et c le cycle solaire.

37. Nous n'en dirons pas davantage sur les congruences du premier degré, qui ne renferment qu'une seule inconnue; il nous reste à parler des congruences qui renferment plusieurs inconnues; mais, comme il faudrait donner trop d'extension à ce chapitre, si nous voulions exposer chaque chose en toute rigueur, et notre projet n'étant pas d'épuiser ici la matière, mais seulement de présenter ce qui est le plus digne d'attention; nous bornerons notre recherche à un petit nombre d'observations, réservant l'exposition complète pour une autre occasion.

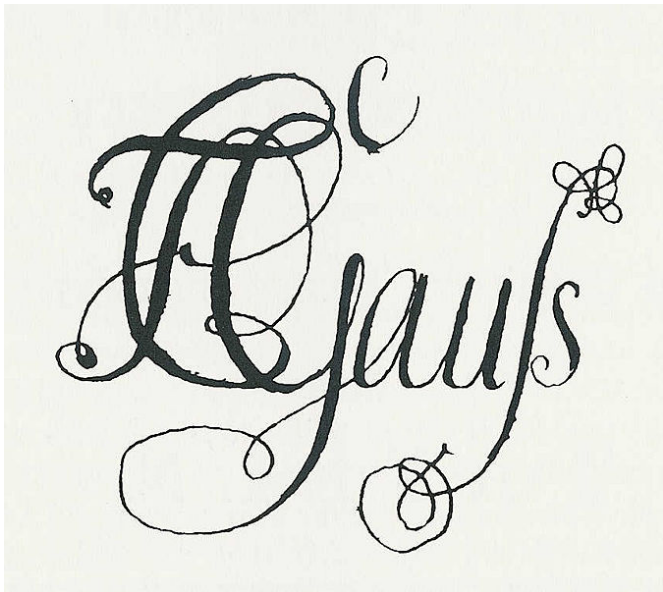
1°. De même que dans les équations, on voit qu'il faut avoir autant de congruences qu'il y a d'inconnues à déterminer.

2°. Soient donc proposées les congruences

$$ax + by + cz \ldots \equiv f \pmod{m} \ldots (A)$$
$$a'x + b'y + c'z \ldots \equiv f' \ldots\ldots\ldots (A')$$
$$a''x + b''y + c''z \ldots \equiv f'' \ldots\ldots\ldots (A'')$$
etc.

en même nombre que les inconnues x, y, z, etc.

2



- **Journal mathématique de Gauss**
- 14 mai 1796 (Göttingen) :
  écrit la conjecture de Goldbach
  (Numeri cuiusvis divisibilitas varia in binos primos.)
- 21 octobre 1796 (Brunswick) :
  Vicimus Gegan.
- Préface à la traduction du journal (Eymard et Lafon) :
  A plusieurs reprises, nous voyons Gauss découvrir d'importants théorèmes par des essais numériques et provoquer l'heureuse rencontre des chiffres, forçant ensuite la démonstration rigoureuse par une recherche de plusieurs mois.

- **Gauss** (Recherches Arithmétiques, p.416)

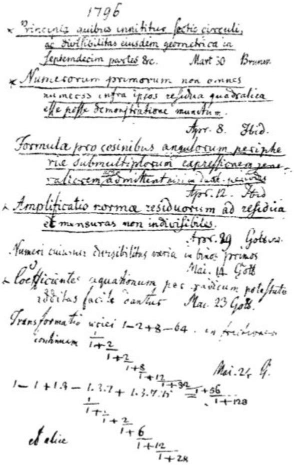
  Le problème où l'on se propose de distinguer les nombres premiers des nombres composés, [...], est connu comme un des plus importants et des plus utiles de toute l'Arithmétique ; [...] En outre, la dignité de la science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre.

- **Gauss** (9 juillet 1814)

  Dedekind a de cette manière vérifié la proposition pour tous les nombres premiers inférieurs à 100.

- **Poincaré** (La Science et l'Hypothèse)

  Une accumulation de faits n'est pas plus une science qu'un tas de pierres n'est une maison.


1796

Principia quibus innititur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes &c. Mart 30 Brunsv.

Numerorum primorum non omnes numeros infra ipsos residua quadratica esse posse demonstratione munitum. Apr. 8. Ibid.

Formula pro cosinibus angulorum peripheriae submultiplorum expressionem generaliorem non admittentium [illegible] Apr. 12. Ibid

Amplificatio normae residuorum ad residua et mensuras non indivisibiles. Apr. 29 Gottingae.

Numeri cuiusvis divisibilitas varia in binos primos Mai. 14 Gott

Coefficientes aequationum per radicum potestatum summas facile dantur Mai. 23 Gott.

Transformatio seriei 1−2+8−64 . in fractionem continuam Mai. 24 G.

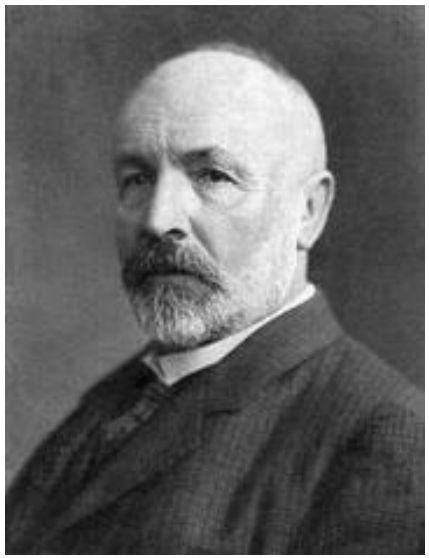
Et aliae

- $\exists$ n $\geq$ 6, $\forall$ p $\leq$ n/2, $\exists$ q $\leq \sqrt{n}$, p et q premiers impairs,

$$\mathcal{S} \begin{cases} n \equiv p_1 \ (mod \ q_1) \\ n \equiv p_2 \ (mod \ q_2) \\ \dots \\ n \equiv p_k \ (mod \ q_k) \end{cases}$$

- $\Longrightarrow$ false

- **Cantor** : Congrès de l'AFAS de Caen en 1894



M. George CANTOR

Professeur à l'Université de Halle.

VÉRIFICATION JUSQU'A 1000 DU THÉORÈME EMPIRIQUE DE GOLDBACH [I 9 c]

— Séance du 10 août 1894 —

Il y a environ dix ans, j'ai fait calculer pour tous les nombres pairs de 2 à 1000, une table qui contient toutes les partitions de ces nombres en deux nombres premiers.

On arrive par l'examen de cette table, donnant aussi le nombre des décompositions, à la conviction que non seulement la proposition est exacte, mais encore que le nombre des décompositions de 2 N croît indéfiniment avec N (sauf les oscillations qui se produisent toujours dans les fonctions relatives à la théorie des nombres).

TABLEAU DES DÉCOMPOSITIONS DES NOMBRES PAIRS 2 N, DE 2 A 1000, EN SOMMES DE DEUX NOMBRES PREMIERS

(Si $2N = x + y$, avec $x < y$, le tableau donne x, le plus petit des deux nombres premiers).
(La dernière colonne indique le nombre n des décompositions.)

2 N	x	n	2 N	x	n
2	1.	1	20	1, 3, 7.	3
4	1, 2.	2	22	3, 5, 11.	3
6	1, 3.	2	24	1, 5, 7, 11.	4
8	1, 3.	2	26	3, 7, 13.	3
10	3, 5.	2	28	5, 11.	2
12	1, 5.	2	30	1, 7, 11, 13.	4
14	1, 3, 7.	3	32	1, 3, 13.	3
16	3, 5.	2	34	3, 5, 11, 17.	4
18	1, 5, 7.	3	36	5, 7, 13, 17.	4

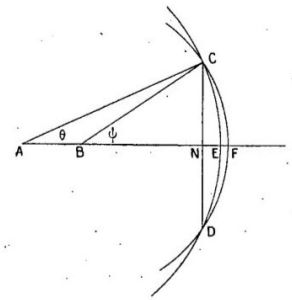
2 N	x	n
986	3, 19, 67, 79, 103, 109, 127, 157, 163, 199, 229, 277, 313, 367, 373, 379, 409, 439, 463, 487.	20
988	5, 11, 17, 41, 47, 59, 101, 107, 131, 149, 167, 179, 191, 227, 269, 311, 347, 389, 401, 419, 431, 467, 479.	23
990	7, 13, 19, 23, 37, 43, 53, 61, 71, 79, 83, 103, 107, 109, 113, 127, 131, 137, 151, 163, 167, 179, 181, 193, 229, 233, 239, 251, 257, 263, 271, 281, 307, 313, 317, 331, 337, 347, 349, 359, 373, 383, 389, 397, 419, 421, 433, 443, 449, 467, 487, 491.	32
992	1, 73, 109, 139, 163, 181, 223, 241, 283, 331, 349, 373, 379, 421.	14
994	3, 11, 17, 23, 41, 47, 53, 83, 107, 113, 131, 137, 167, 173, 197, 233, 251, 293, 311, 317, 347, 353, 401, 431, 491.	25
996	5, 13, 19, 29, 43, 59, 67, 89, 109, 113, 137, 139, 157, 167, 173, 199, 223, 227, 239, 257, 263, 269, 277, 313, 337, 349, 353, 379, 383, 389, 397, 409, 419, 433, 439, 449, 487.	36
998	1, 7, 31, 61, 79, 139, 211, 229, 241, 271, 307, 337, 367, 379, 397, 421, 457, 499.	18
1000	3, 17, 23, 29, 47, 53, 59, 71, 89, 113, 137, 173, 179, 191, 227, 239, 257, 281, 317, 347, 353, 359, 383, 401, 431, 443, 479, 491.	28

M. R.-W. GENESE

Professeur à l'University College of Wales, Aberystwyth (Angleterre).

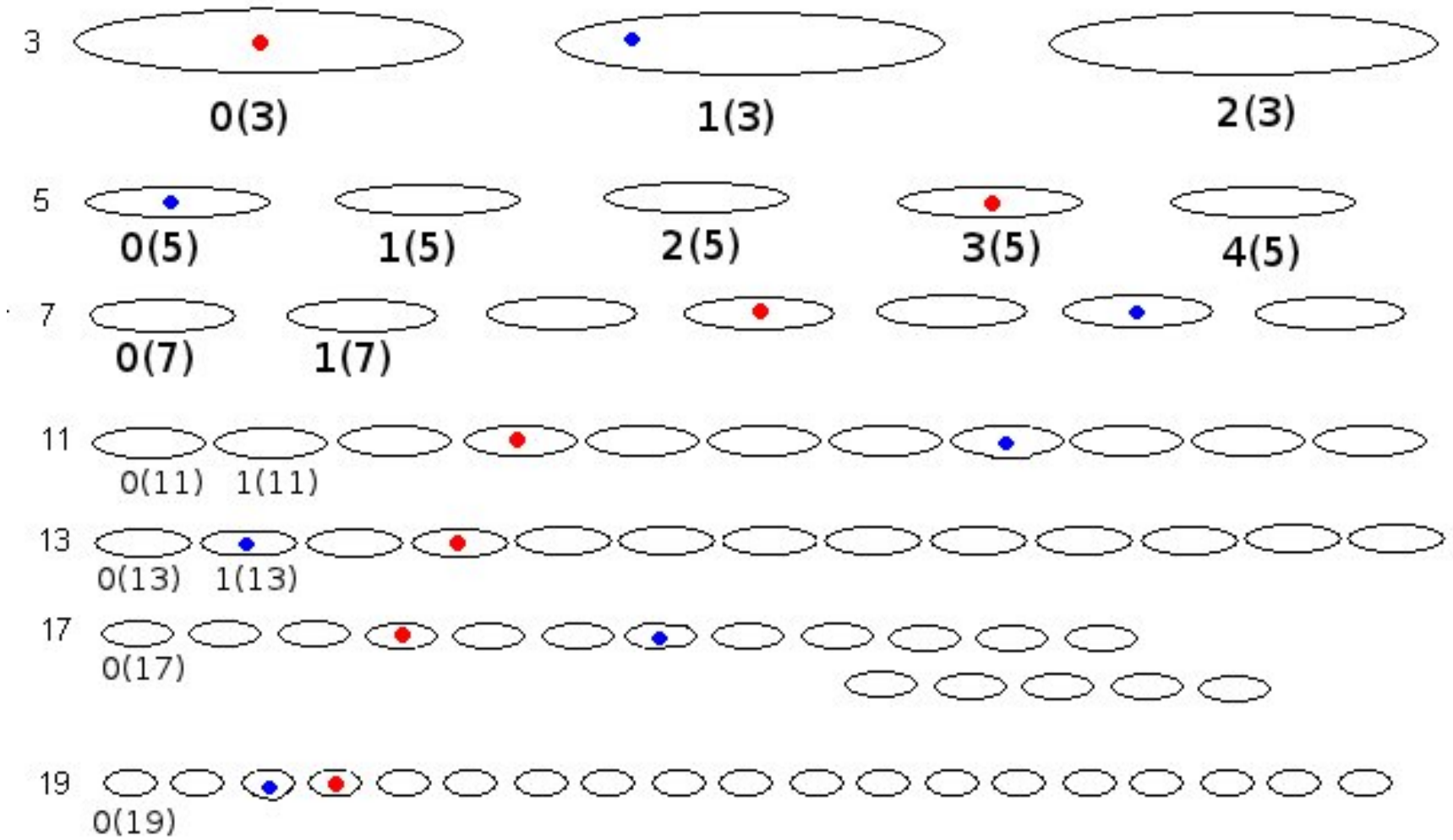
SUR UNE INÉGALITÉ TRIGONOMÉTRIQUE [K 20 e]

— Séance du 10 août 1894 —

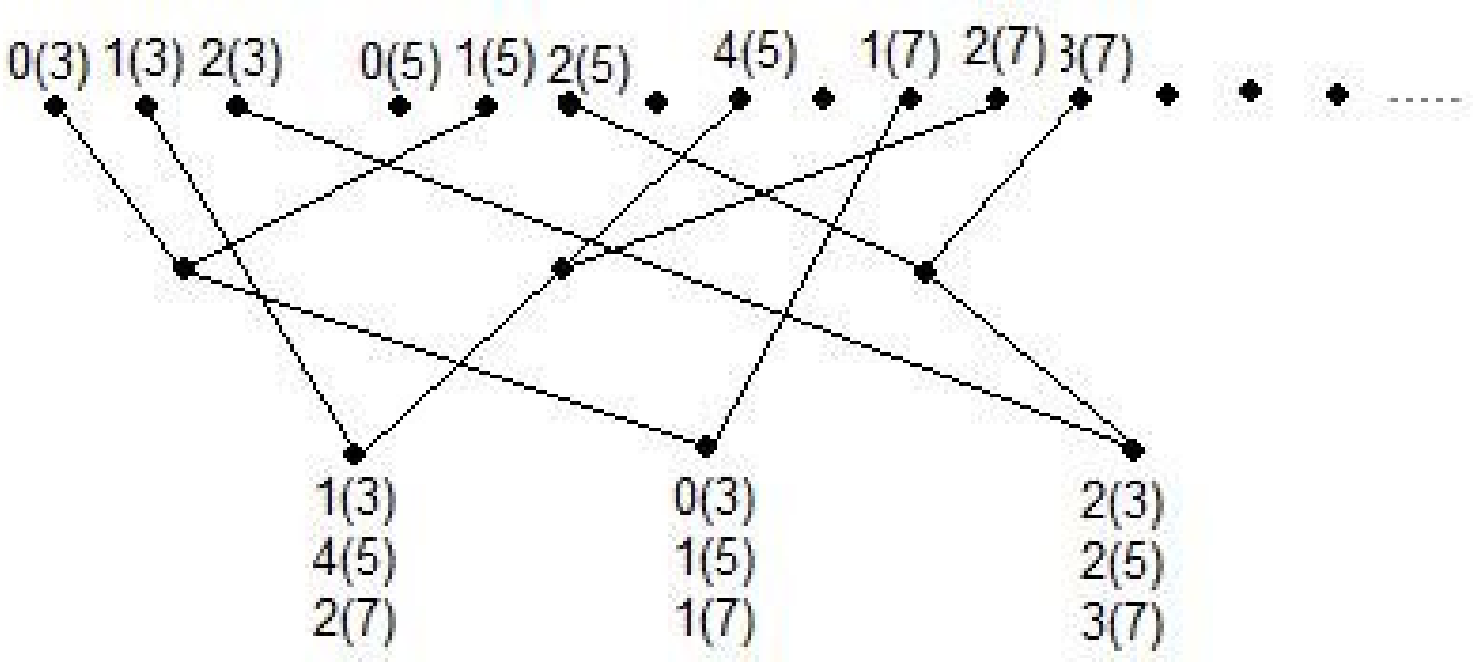


Soit CD la corde commune de deux cercles dont les centres A, B sont du même côté de CD, et soit AC > BC. L'arc mineur CED du cercle A sera donc dans l'intérieur du segment mineur CFD du cercle B. Donc, arc CED < arc CFD. De plus, on peut faire tourner le plan du cercle A autour de la droite CD. Donc, *si deux arcs mineurs de circonférence (pas nécessairement du même plan) ont mêmes extrémités, celui qui a le plus grand rayon est le plus petit*. Par exemple, un arc mineur de grand cercle

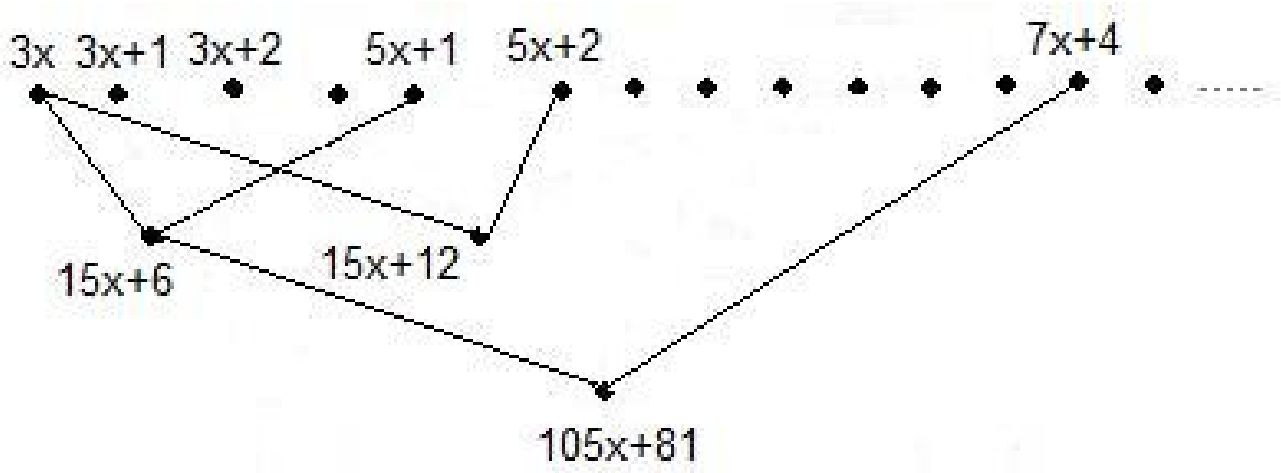
- **Ensembles de Cantor** (40=3+37)



- Treillis de Cantor



- Treillis de Cantor



- Cherchons les décomposants de Goldbach de nombres de la forme : 2(3) 3(5) 3(7) $\rightarrow$ 210k+38
- 1(3) 1(5) 1(7) $\rightarrow$ 210k+1
- 1(3) 1(5) 2(7) $\rightarrow$ 210k+121
- 1(3) 1(5) 4(7) $\rightarrow$ 210k+151
- 1(3) 1(5) 5(7) $\rightarrow$ 210k+61
- 1(3) 1(5) 6(7) $\rightarrow$ 210k+181
- 1(3) 2(5) 1(7) $\rightarrow$ 210k+127
- 1(3) 2(5) 2(7) $\rightarrow$ 210k+37
- 1(3) 2(5) 4(7) $\rightarrow$ 210k+67
- 1(3) 2(5) 5(7) $\rightarrow$ 210k+187
- 1(3) 2(5) 6(7) $\rightarrow$ 210k+97
- 1(3) 4(5) 1(7) $\rightarrow$ 210k+169
- 1(3) 4(5) 2(7) $\rightarrow$ 210k+79
- 1(3) 4(5) 4(7) $\rightarrow$ 210k+109
- 1(3) 4(5) 5(7) $\rightarrow$ 210k+19
- 1(3) 4(5) 6(7) $\rightarrow$ 210k+139

- Exemples de $210k + 38$
- 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

- Descente infinie de **Fermat**
- Si un nombre ne vérifiait pas la Conjecture de Goldbach, il y en aurait un plus petit qui ne la vérifierait pas non plus et ainsi de proche en proche, jusqu'à atteindre des nombres si petits qu'on sait qu'ils vérifient la Conjecture.
- Raisonnement par l'absurde

- $\exists$ n $\geq$ 6, $\forall$ p $\leq$ n/2, $\exists$ q $\leq \sqrt{n}$, p et q premiers impairs,

$$\mathcal{S} \begin{cases} n \equiv p_1 \ (mod \ q_1) \\ n \equiv p_2 \ (mod \ q_2) \\ \dots \\ n \equiv p_k \ (mod \ q_k) \end{cases}$$

- $\Longrightarrow$ false

- congruences contradictoires
  $(n \equiv p_i \ (mod\ q), n \equiv p_j \ (mod\ q)$ avec $p_i \not\equiv p_j \ (mod\ q))$
- sous-ensemble S de $\mathcal{S}$,
  modules tous $\neq$

  (congruences omises non-contradictoires avec les congruences conservées, sinon $\rightarrow$ premier cas).
- S admet une solution unique n modulo $M = PPCM(q_i)$.
  Le plus petit entier vérifiant cette congruence unique ne vérifie pas la conjecture de Goldbach.
- sous-ensemble S' de congruences de S admet une solution unique
  $n' < n$ et
  n' ne vérifie pas la conjecture de Goldbach non plus.
- On aboutit donc à une contradiction dans tous les cas.

- Ma conjecture, sous la forme d'une montée infinie.
- Tout nombre pair n partage avec $n+6$ au moins l'un de ses décomposants de Goldbach
- Vérifiée par ordinateur jusqu'à 16.10^8.

- L'Univers mathématique de Davis et Hersh

$20902 = 3 + 20899$ $20962 = 3 + 20959$
$20904 = 5 + 20890$ $20964 = 5 + 20959$
$20906 = 3 + 20903$ $20966 = 3 + 20963$
$20908 = 5 + 20903$ $20968 = 5 + 20963$
$20910 = 7 + 20903$ $20970 = 7 + 20963$
$20912 = 13 + 20899$ $20972 = 13 + 20959$
$20914 = 11 + 20903$ $20974 = 11 + 20963$
$20916 = 13 + 20903$ $20976 = 13 + 20963$
$20918 = 19 + 20899$ $20978 = 19 + 20959$
$20920 = 17 + 20903$ $20980 = 17 + 20963$
$20922 = 19 + 20903$ $20982 = 19 + 20963$
$20924 = 3 + 20921$ $20984 = 3 + 20981$

- des causes différentes peuvent produire les mêmes effets (congrus 2 à 2 modulo 3 et 5)...