La conjecture de Goldbach* stipule que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs.
Cela équivaut à: $\forall\, n \geq 6,\ \exists\, p \leq n/2,\ p\ premier\ impair,\ \forall\, q \leq \sqrt{n},\ q\ premier\ impair,\ p \not\equiv n\ (mod\ q)$

Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17, les plus petits nombres premiers impairs, sont tous congrus à 98 selon un module premier impair inférieur à $\sqrt{98}$ tandis que 19 n'est congru à 98 selon aucun d'entre eux.

$98 \equiv 3\ (mod\ 5)$.
$98 \equiv 5\ (mod\ 3)$.
$98 \equiv 7\ (mod\ 7)$.
$98 \equiv 11\ (mod\ 3)$.
$98 \equiv 13\ (mod\ 5)$.
$98 \equiv 17\ (mod\ 3)$.

$98 \not\equiv 19\ (mod\ 3)$.
$98 \not\equiv 19\ (mod\ 5)$.
$98 \not\equiv 19\ (mod\ 7)$.

On choisit de démontrer plutôt :

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

Notons $p_1, p_2, \ldots, p_k$ les nombres premiers impairs inférieurs ou égaux à $n/2$ et $q_1, q_2, \ldots, q_k$, les nombres premiers impairs inférieurs ou égaux à $\sqrt{n}$. Les q_i sont les modules selon lesquels n est congru aux différents p_i. Cherchons à établir d'où provient la contradiction. On a† :

$$\begin{aligned} &n \equiv p_1\ (mod\ q_1)\\ &n \equiv p_2\ (mod\ q_2)\\ &\ldots\\ &n \equiv p_k\ (mod\ q_k) \end{aligned}$$

D'après le théorème des restes chinois, les q_i étant soit égaux soit premiers entre eux 2 à 2, le système de congruences

$$\begin{aligned} &n \equiv p_1\ (mod\ q_1)\\ &n \equiv p_2\ (mod\ q_2)\\ &\ldots\\ &n \equiv p_k\ (mod\ q_k) \end{aligned}$$

aboutit à une contradiction de deux façons possibles.

Premier cas : Soit la contradiction provient du fait que le système contient des congruences contradictoires, telles que $n \equiv p_i\ (mod\ q), n \equiv p_j\ (mod\ q)$ avec $p_i \not\equiv p_j\ (mod\ q)$.

Second cas : Soit la contradiction provient du principe de *"descente infinie"* de Fermat : on ne conserve du système de congruences qu'un sous-ensemble de celui-ci, contenant des congruences selon des modules tous différents (les congruences omises étant non-contradictoires avec les congruences conservées sinon on se situerait dans le premier cas). Ce nouveau système S admet une solution unique n modulo M, le plus petit commun multiple des q_i. Le plus petit nombre vérifiant cette congruence unique ne satisfait pas la conjecture de Goldbach. Mais si l'on prend maintenant un sous-ensemble S' de congruences du nouveau système S, il admettra une solution unique également et le plus petit nombre n' vérifiant cette congruence

* $\forall\, n \geq 6,\ \exists\, p \leq n/2,\ \exists\, q \geq n/2,\ p\ et\ q\ premiers\ impairs,\ \ n = p + q,$

†Le problème consiste à "agréger" les différentes congruences concernant n : on ne peut pas par exemple déduire des différentes congruences sur n la congruence suivante :

$$n^k \equiv \textstyle\prod_{p_1}^{p_k} p_i\ (mod\ \prod_{q_1}^{q_k} q_i)$$

Illustrons cette impossibilité sur un exemple :

$n \equiv 2\ (mod\ 3)$ *a pour solutions entières* $2,\ 5,\ 8,\ 11,\ 14,\ 17,\ 20,\ 23,\ 26,\ 29,\ 32,\ 35,\ 38, \ldots$
$n \equiv 3\ (mod\ 5)$ *a pour solutions entières* $3,\ 8,\ 13,\ 18,\ 23,\ 28,\ 33,\ 38, \ldots$

Mais les solutions du système constitué des 2 congruences sont $8, 23, 38, \ldots$, i.e. les solutions de la congruence $n \equiv 8\ (mod\ 15)$ qui ne s'obtient pas par une simple "multiplication terme à terme" des deux congruences initiales, mais par l'application complexe du théorème des restes chinois.

unique sera plus petit que n et ne vérifiera pas la conjecture de Goldbach non plus. On aboutit donc à une contradiction dans tous les cas[‡].

(Denise Chemla, 26/4/2012)

[‡]Illustrons l'inclusion d'ensembles de nombres en terme d'inclusion inverse des systèmes de congruences : le système de congruences

$$n \equiv 3 \ (mod\ 5)$$
$$n \equiv 5 \ (mod\ 7)$$

est inclu dans le système de congruence

$$n \equiv 1 \ (mod\ 3)$$
$$n \equiv 3 \ (mod\ 5)$$
$$n \equiv 5 \ (mod\ 7)$$

$5 \times 7 = 35,\ 3 \times 7 = 21,\ 3 \times 5 = 15, 3 \times 5 \times 7 = 105.$
$2 \times 35 \equiv 1 \ (mod\ 3),\ 21 \equiv 1 \ (mod\ 5),\ 15 \equiv 1 \ (mod\ 7).$
Le deuxième système a pour solution unique les nombres congrus à $1 \times 70 + 3 \times 21 + 5 \times 15 = 70 + 63 + 75 = 208 = 103 \ (mod\ 105)$ qui sont les nombres de la suite $103, 208, 313, \ldots$
Le premier système a quant à lui pour solution unique les nombres congrus à $3 \times 21 + 5 \times 15 = 63 + 75 = 138 = 33 \ (mod\ 35)$ qui sont les nombres de la suite $33, 68, 103, 138, 173, 208, 243, 278, 313, \ldots$
Comme prévu, les nombres vérifiant le deuxième système de congruences (plus contraint, une congruence supplémentaire) vérifient également le premier système (moins contraint).

Annexe : articles 33 à 36 (théorème des restes chinois) des Recherches Arithmétiques de Gauss

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 suit 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 sousmultiple 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 $a \equiv b \pmod{A' \text{ ou } B'}$; 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-

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 problême, et on peut procéder d'après la manière enseignée plus haut.

35. 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

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

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.

36. 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 $\equiv 0 \pmod{ACD \text{ etc.}}$;

$\gamma \equiv 1$ (mod. C), et $\equiv 0$ (mod. 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. (mod. $ABCD$ etc.); en effet on a évidemment $\alpha a \equiv a$ (mod. A), et les autres termes sont $\equiv 0$ (mod. A); donc $z \equiv a$ (mod. 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 $\frac{1}{19.28}$ (mod. 15), ou $\frac{1}{532}$ (mod. 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

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

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

2