Conjecture de Goldbach et systèmes de congruences du second degré

Denise Vella-Chemla

14/8/11

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Cette conjecture est trivialement vérifiée par les nombres pairs doubles de nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru[1] à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\, n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\, q \leq \sqrt{n},\quad p \not\equiv n\ (q)$$

Posons $n\ =\ x^2 b$ avec x^2 le plus grand carré divisant n.

b est le produit des nombres premiers de valuation p-adique impaire (i.e. élevés à une puissance impaire) dans la factorisation de n (ce faisant, on obéit en quelque sorte à la préconisation de Gauss dans l'article 146 page 109 point III de la section Quatrième des Recherches Arithmétiques : *"Au reste, on voit facilement que si parmi les facteurs p, p′, p″, etc., il y en a un nombre pair d'égaux entre eux, on peut les rejeter, puisqu'ils n'influent en rien sur la relation de p à n."*).

Résoudre un système d'incongruences quadratiques de la forme $\frac{1}{b}.p \not\equiv x^2\ (q)$ selon tous les modules premiers q inférieurs à $\sqrt{n}$ en utilisant la loi de réciprocité quadratique, le théorème d'or selon Gauss, permet-il de trouver un décomposant de Goldbach de n au moins ?

2 Méthode inductive à la recherche de *la raison qui fait que...*

Si l'on parvient à démontrer qu'un nombre premier p au moins vérifie les incongruences $\frac{1}{b}.p \not\equiv x^2\ (q)$ selon tous les modules premiers q inférieurs à $\sqrt{n}$, notre problème sera résolu. Si l'on appelle A le produit $\frac{1}{b}.p$, p est un diviseur de A. Il s'agit alors de résoudre l'incongruence $x^2 - A \not\equiv 0\ (q)$. Nous verrons que dans les articles 147 à 149 des Recherches Arithmétiques, Gauss fournit les formules qui contiennent tous les nombres premiers à A dont A est résidu, ou tous ceux qui sont diviseurs des nombres de la forme $x^2 - A$, x^2 étant un carré indéterminé.

2.1 Exemples 1 et 2

Commençons par le nombre pair $98\ =\ 2.7^2$.
Les 3 modules premiers impairs à considérer inférieurs à la racine de 98 sont 3, 5 et 7.
L'incongruence $p \not\equiv 2.7^2 (mod\ 3,\ 5\ et\ 7)$ devient $\frac{1}{2}.p \not\equiv 7^2 (mod\ 3,\ 5\ et\ 7)$.
L'écriture de 3 modules entre parenthèses est non-conventionnelle mais nous permet de gagner de la place,

[1] On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

elle indique une conjonction de faits[2].
L'inverse de 2 est 2 (mod 3), l'inverse de 2 est 3 (mod 5) et l'inverse de 2 est 4 (mod 7). 2 est non-résidu de 3. 3 est non-résidu de 5. 4 est résidu de 7.
Ici, on rappelle que tout nombre premier p est résidu de lui-même. D'autre part, bien qu'un nombre premier p ne soit pas inversible dans $(\mathbb{Z}/p\mathbb{Z}, \times)$, Gauss fournit à l'article 109, section Quatrième des Recherches Arithmétiques la convention selon laquelle si r est résidu de p, l'inverse de r noté $\frac{1}{r}$ est lui-aussi résidu de p pour p un nombre premier (ceci est en particulier vrai de p un nombre premier qui est toujours résidu de lui-même).
Le nombre premier recherché doit donc être :

- résidu de 3 pour que, en le multipliant par l'inverse de 2, on n'obtienne pas un carré ;
- résidu de 5 (pour la même raison) ;
- non-résidu de 7 (pour la raison opposée).

19 et 31 vérifient les 3 conditions exigées et sont des décomposants de Goldbach de 98. Si on dresse une petite table "est résidu de" des nombres premiers inférieurs à 49, la moitié de 98, selon les modules 3, 5 et 7, voici ce que l'on obtient :

	3	5	7
19	×	×	
31	×	×	
37	×		×
3	×		
5		×	
7	×		×
11		×	×
13	×		
17			
23			×
29		×	×
41		×	
43	×		×
47			

Les deux solutions que sont 19 et 31 sont "semblables du point de vue de leur relation quadratique" aux modules 3, 5 et 7.

19 est aussi décomposant de Goldbach de $242 = 2.11^2$ mais ne l'est plus de $238 = 2.13^2$. Le raisonnement est similaire mais il faut alors tenir compte de toute une série d'autres modules qui se sont ajoutés à l'ensemble des modules inférieurs à la racine du nombre pair que l'on considère.

2.2 Exemple 3

$100 = 2^2.5^2$ est un carré. En appliquant le même raisonnement que précédem-ment, on cherche un nombre qui soit à la fois non-résidu de 3, 5 et 7. C'est le cas de 17 et de 47 qui sont tous deux des décomposants de Goldbach de 100.

2.3 Autres exemples

A partir de là, on décide de suivre l'exemple d'Euler : dans l'article *"Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs"*, il fournit des résultats exhaustifs jusqu'à 100.

[2]Elle correspond à l'écriture suivante utilisée par Gauss dans l'article 105 de la section Quatrième des Recherches Arithmétiques *"selon les modules a, b, c, etc."*.

Peut-être que l'étude des nombres pairs factorisés jusqu'à 100 (on laisse de côté les doubles de premiers qui vérifient trivialement la conjecture) va petit à petit nous faire comprendre comment il faut généraliser...

$8 = 2^3$.
Le raisonnement habituel amène à chercher un résidu de 3 or 3 est bien un décomposant de Goldbach de 8.

$12 = 2^2.3$.
L'inverse de 3 est résidu de 3. 5, qui est non résidu du seul diviseur impair de 12 de valuation p-adique impaire, est un décomposant de Goldbach de 12.

$16 = 2^4$.
5 non résidu de 3 est décomposant de Goldbach de 16.

$18 = 2.3^2$.
On cherche un résidu de 3 (selon le raisonnement habituel uniquement selon le module 3) et 7 fournit bien une décomposition de Goldbach de 18.

$20 = 2^2.5$.
On cherche un résidu de 3. 3 ou bien 7 fournissent tous deux des décompositions de Godlbach de 20.

$24 = 2^3.3$.
3 apparaît avec une valuation p-adique impaire dans la factorisation de 24. L'inverse de 3 est résidu de 3. Il s'avère que 5 et 11, tous deux non-résidus de 3, fournissent des décompositions de Goldbach de 24 ainsi que 7 qui quant à lui est non-résidu de 5.

$28 = 2^2.7$.
Modulo 3, l'inverse de 7 est 1 qui est résidu de 3. Modulo 5, l'inverse de 7 est 3 qui est non-résidu de 5. On cherche donc un nombre qui soit non-résidu de 3 et résidu de 5. 5 et 11 sont dans ce cas et fournissent tous les deux des décompositions de Goldbach de 28.

$30 = 2.3.5$.
Ici, faisons un petit aparté : 30 a "beaucoup" de petits décomposants, de même que 60, 90, 120, 150 ou 900, par exemple. L'étude des points de la comète de Goldbach, en février 2011, nous a montré que ces nombres pairs ont un nombre de décompositions de Goldbach "bien supérieurs" à leurs voisins. On le constate en utilisant l'article de Cantor qui avait vérifié la conjecture jusqu'à 1000 et qui avait émis quelques conjectures que l'on retrouve notamment dans le chapitre *Cantor et la Conjecture de Goldbach* de l'excellent livre d'Anne-Marie Décaillot *"Cantor et la France"*.
L'inverse de 3 est résidu de 3, l'inverse de 5 l'est de 5. On constate que *tous* les premiers autres que 2, 3 et 5 (les diviseurs de 30) fournissent des décompositions de Goldbach : 7, 11 et 13.
Pour le nombre pair $60 = 2^2.3.5$, même chose : *tous* les nombres premiers de 7 à 29 sans exception fournissent des décompositions de Goldbach de 60.
Pour $120 = 2^3.3.5$, tous les premiers compris entre 7 et 59 fournissent une décomposition de Goldbach de 120 sauf 29 et 43 (ce qui représente 12 décomposi-tions et 2 "ratages").
Pour $150 = 2.3.5^2$, les résidus de 19 que sont 11, 19 et 23 fournissent 3 décompo-sants, tandis que les résidus de 17 que sont 43, 47, 53 et 67 en fournissent 4 autres.
Pour $90 = 2.3^3.5$, 48 nombres premiers sur les 81 nombres premiers compris entre 13 et 443 permettent d'obtenir une décomposition de Goldbach [3].
Parmi ces nombres, $270 = 2.3^3.5$ a un nombre de décomposants de Goldbach (il en a 20) qui vaut environ le double de celui de ses voisins immédiats (268 et 272 en ont respectivement 9 et 8). On s'est intéressé à lui car la conjecture de Goldbach aura 270 ans en 2012...

L'étude de ces nombres qui ont beaucoup de petits facteurs premiers nous amène à croire qu'il suffit peut-être parfois que la relation "non-résidu de" soit vérifiée pour l'un des diviseurs seulement pour permettre

[3] On peut carrément (!) parler de rentabilité...

l'obtention d'un décomposant de Goldbach. Cela nous fait vivement souhaiter comprendre la page 112 des Recherches Arithmétiques dans laquelle Gauss utilise un raisonnement combinatoire[4].

Poursuivons notre liste des nombres pairs inférieurs à 100 non doubles de premiers.

$32 = 2^5$
On cherche un résidu de 3 et 5 à la fois. 19 fournit une décomposition de 32.

$36 = 2^2.3^2$
C'est un carré. 5 qui est non-résidu de 3 fournit une décomposition mais 7 résidu de 3 en fournit une également.

$40 = 2^3.5$
Les résidus de 11 que sont 3 et 11 fournissent chacun une décomposition. 17 non-résidu de 3 en fournit une également.

$42 = 2.3.7$
Les résidus de 5 que sont 5, 11, 19, 29 et 31 fournissent chacun une décomposition.

$44 = 2^2.11$
Les résidus de 3 que sont 3, 7 et 13 fournissent chacun une décomposition.

$48 = 2^4.3$
Les résidus de 5 que sont 5, 11, 19, 29, 31 et 41 fournissent une décomposition.

$50 = 2.5^2$
Les résidus de 3 que sont 3, 7, 13 et 19 fournissent chacun une décomposition.

$52 = 2^2.13$
Les non-résidus de 3 que sont 5, 11 et 23 fournissent chacun une décomposition.

$54 = 2.3^3$
Les non-résidus de 3 que sont 7 et 13 fournissent une décomposition.

$56 = 2^3.7$
Les résidus de 3 que sont 3, 13 et 19 (7 étant un diviseur de 56 ne peut fournir de décomposition) fournissent chacun une décomposition.

$64 = 2^6$
Les non-résidus de 3 que sont 5, 11, 17 et 23 fournissent une décomposition.

$66 = 2.3.11$
Les résidus de 29 que sont 5, 7, 13, 23 et 29 fournissent chacun une décomposition.

$68 = 2^2.17$
Observons la table : pour ne conserver que 7 et 31, il faut qu'il y ait une croix en colonne 3 et que les colonnes 5 et 7 soient l'inverse l'une de l'autre. Cependant alors 19 et 43 vérifient cette condition bien que ne fournissant pas de décompositions de Goldbach. On constate que leur complémentaire à n est à chaque fois un carré (49 et 25).

[4]Malheureusement, on trouve à la fin de cette page un *"Mais pour abréger, nous sommes forcés de ne pas donner plus de développement à la démonstration."* qui rappelle furieusement le *"La marge est trop petite."* de Fermat...

$70 = 2.5.7$
Les non-résidus de 3 que sont 11, 17, 23 et 29 fournissent une décomposition.

$72 = 2^3.3^2$
Les résidus de 5 que sont 5, 11, 19, 29 et 31 fournissent chacun une décomposition.

$76 = 2^2.19$
Les non-résidus de 3 que sont 5, 17, 23 et 29 fournissent chacun une décomposition.

$78 = 2.3.13$
Les résidus de 19 que sont 5, 7, 11, 17 et 19 fournissent chacun une décomposition.

$80 = 2^4.5$
Les résidus de 3 que sont 7, 13, 19 et 37 fournissent chacun une décomposition.

$84 = 2^2.3.7$
Les résidus de 5 que sont 5, 11, 31 et 41 fournissent chacun une décomposition, ainsi que les résidus de 13 que sont 13, 17 et 23 et enfin le résidu de 7 qu'est 37.

$88 = 2^3.11$
Les résidus de 5 que sont 5 et 41 fournissent chacun une décomposition, ainsi que les résidus de 13 que sont 17 et 29.

$90 = 2.3^2.5$
Les résidus de 19 que sont 7, 11, 17, 19 et 23 fournissent chacun une décomposition ainsi que les résidus de 7 que sont 29, 37 et 43.

$92 = 2^2.23$
Tous les résidus de 3 inférieurs à 36 que sont 3, 13, 19 et 31 fournissent chacun une décomposition.

$96 = 2^5.3$
Les résidus de 29 que sont 7, 13, 23 et 29 fournissent chacun une décomposition ainsi que les résidus de 3 que sont 37 et 43.

2.4 Pour résumer et tenter d'aller plus avant

Dans les listes de nombres suivantes, on fournit entre parenthèses après chaque nombre les modules p dont les résidus (R *suivi de* p) ou non-résidu (N *suivi de* p)[5] permettent d'en trouver le plus de décompositions de Goldbach.
On a trouvé des décomposants de Goldbach de n :

- qui étaient non-résidus du plus petit non-résidu de n pour les nombres pairs suivants : 16 ($N3$), 24 ($N5$), 28 ($N3$), 40 ($N3$), 52 ($N3$), 54 ($N3$), 64 ($N3$), 70 ($N3$), 76 ($N3$), 100 ($N3N5N7$), 242 ($N7$) ;
- qui étaient résidus d'un non-diviseur de n pour les nombres pairs suivants : 8 ($R3$), 20 ($R3$), 28 ($R5$), 30 ($R7$), 32 ($R3$), 40 ($R11$), 42 ($R5$), 44 ($R3$), 48 ($R5$), 50 ($R3$), 56 ($R3$), 60 ($R7$), 66 ($R29$), 68 ($R3$), 72 ($R5$), 78 ($R19$), 80 ($R3$), 84 ($R5$), 88 ($R5$), 90 ($R7$), 92 ($R3$), 96 ($R3$), 98 ($R3$), 120 ($R7$), 150 ($R17$), 242 ($R3$), 270 ($R7$), 900 ($R7$) ;
- qui étaient non-résidus d'un diviseur de valuation p-adique impaire pour les nombres pairs suivants : 12 ($N3$), 24 ($N3$) ;

[5] On reprend la notation de Gauss.

- qui étaient non-résidus d'un diviseur de valuation p-adique paire pour le nombre pair suivant : 36 ($N3$) ;
- qui étaient résidus d'un diviseur de valuation p-adique paire pour les nombres pairs suivants : 18 ($R3$), 36 ($R3$).

Les nombres des trois dernières catégories peuvent aisément être intégrés aux deux premières catégories. On a bien en tête la règle *"moins par moins donne plus, moins par plus donne moins"* pour les caractères résidu/non-résidu démontrée par Gauss dans l'article 98 de la section Quatrième des Recherches Arithmétiques.

Concernant la première catégorie, on fournit pour mémoire en annexe 1 les résidus quadratiques des nombres inférieurs à 100 pour vérification de ce que l'on a constaté.

Concernant la deuxième catégorie, même si la condition *résidu d'un non-diviseur* semble toujours permettre l'obtention d'un décomposant de Goldbach, on remarque également qu'on peut toujours trouver un nombre premier décomposant de Goldbach de n parmi les nombres premiers qui sont non-résidus de tous les diviseurs impairs de n et cette condition semble plus satisfaisante dans la mesure où Gauss fournit dans les articles 129 et 130 de la section Quatrième des Recherches Arithmétiques la démonstration d'un théorème selon lequel tout nombre premier de la forme $4n+1$ est toujours non-résidu d'un nombre premier au moins plus petit que lui. L'annexe 4 donne le détail de ce constat pour les nombres de la deuxième catégorie.

On a cependant beau essayer d'induire certaines formes des résultats ci-dessus, on ne trouve pas grand chose : il semblerait que les nombres pairs qui sont des puissances paires de 2 appartiennent toujours à la première classe identifiée alors que les nombres pairs puissances impaires de 2 appartiennent à la seconde, ou bien que les nombres premiers de la forme $4n+3$ apparaissent à une puissance impaire dans les nombres de la première classe mais on peut difficilement envisager de généraliser à partir de quelques nombres par ci, par là.

Il y a cependant une phrase de Gauss qui attire particulièrement notre attention : dans l'article 105, le module est composé, produit de premiers ou de puissances de premiers (ça pourrait être n dans notre cas) et Gauss écrit dans le deuxième paragraphe de cet article *que les différentes combinaisons donneront des valeurs différentes, et* ***qu'elles les donneront toutes***. Est-ce à dire qu'on peut toujours trouver un nombre premier satisfaisant les relations *"non-résidu"* qu'on cherche à satisfaire quel que soit n ?

On a vu qu'on doit étudier si les nombres premiers de valuation p-adique impaire sont résidus ou pas des modules premiers inférieurs à la racine du nombre pair considéré. Gauss conseille d'affecter les nombres premiers de la forme $4n+1$ du signe $+$ et les nombres premiers de la forme $4n+3$ du signe $-$[6] et compter s'ils se présentent en nombre pair ou pas. Il faudrait peut-être mettre en oeuvre un raisonnement combinatoire tel que celui de l'article 148 page 111 pour montrer qu'un tel nombre premier existe toujours, qui fournit une décomposition de Goldbach de n. Dans l'article 148 en question, Gauss établit un classement des nombres plus petits que n et premiers à n selon qu'ils sont dans le premier cas non-résidus d'aucun diviseur de n ou bien non-résidu d'un nombre pair de diviseurs de n et dans le second cas non-résidus d'un nombre impair de diviseurs de n. Un tel classement serait-il pertinent pour le problème qui nous intéresse ?

3 *"Est résidu quadratique de"*, une relation *"presque-symétrique"*

3.1 Illustration de la loi de réciprocité quadratique pour les modules premiers

On rappelle que p est résidu quadratique de q s'il existe un carré auquel p est congru selon le module q. Par exemple, 3 est résidu quadratique de 37 et réciproquement car $3 \equiv 15^2 (mod\ 37)$ et $37 \equiv 1^2 (mod\ 3)$.

[6] Gauss les appelle les $4n-1$.

Selon un module premier, il y a autant de résidus que de non-résidus. Deux nombres complémentaires à p sont soit tous deux résidus ou bien tous deux non-résidus lorsque p est un $4n+1$, soit l'un résidu et l'autre non-résidu lorsque p est un $4n+3$.

Illustrons cela dans deux tableaux, l'un pour le module 13 de la forme $4n+1$, l'autre pour le module 19, de la forme $4n+3$: comme q et $n-q$ ont même carré selon le module p, on va les mettre dans une même colonne du tableau (les plus grands dans la première ligne, les plus petits dans la deuxième). On va indiquer pour mémoire le résidu minimum absolu de leur carré selon le module considéré dans la troisième ligne. On va utiliser la couleur bleue pour les résidus seulement et constater la relation de symétrie ou d'anti-symétrie du caractère *"résidu de"* qui lie les deux nombres d'une même colonne.

Selon le module 13, de la forme $4n+1$:

13	12	11	10	9	8	7
0	1	2	3	4	5	6
0	1	4	9	3	12	10

Selon le module 19, de la forme $4n+3$:

19	18	17	16	15	14	13	12	11	10
0	1	2	3	4	5	6	7	8	9
0	1	4	9	16	6	17	11	7	5

Gauss fournit une application simple de la loi de réciprocité quadratique aux nombres premiers selon leur forme à la page 116 des Recherches Arithmétiques, article 151 : *"il s'ensuit que la relation de p à q est la même que celle de q à p, quand p ou q est de la forme $4n+1$, et qu'elle est inverse quand p et q sont de la forme $4n+3$"*.

Rappelons la table de la relation qui en découle (c'est la table II des annexes des Recherches Arithmétiques). Cette table présente une *"presque-symétrie"* selon sa diagonale. On a noté par une croix noire la relation lorsqu'elle est symétrique (entre deux nombres premiers impairs dont l'un au moins est un $4n+1$) et par une croix bleue la relation lorsqu'elle est anti-symétrique (lorsque les deux nombres premiers impairs sont des $4n+3$).

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
2	×			×			×		×		×		×		×
3	×	×			×	×			×			×			×
5	×		×		×			×		×	×		×		
7	×	×		×				×		×	×	×			×
11	×		×	×	×			×				×		×	
13	×	×				×	×		×	×				×	
17	×					×	×	×						×	×
19	×	×	×				×	×			×				
23	×			×	×	×		×	×	×			×	×	
29	×		×	×		×			×	×					
31	×	×	×		×			×	×		×		×	×	
37	×	×		×	×							×	×		×
41	×		×						×		×	×	×	×	
43	×	×		×		×	×		×				×	×	
47	×				×		×	×	×		×	×		×	×

En annexe 5, on illustre par les tables que les symétrie ou anti-symétrie du caractère résidu sont bien moins évidentes selon les modules impairs mais elles existent.

3.2 Illustrations du théorème fondamental dans le cas des modules pairs[7]

Au tout début de ces recherches, j'avais la conviction que la section Quatrième des Recherches Arithmétiques fournirait la solution au problème de Goldbach. J'avais étudié les résidus quadratiques mais mon problème était que, pour aller plus vite, je ne considérais dans mes tables que les seuls nombres impairs, et je perdais ainsi des informations précieuses qui permettent de faire apparaître une propriété de symétrie ou anti-symétrie verticale qui va être présentée maintenant.

3.2.1 Nombres pairs doubles de nombres premiers

On va maintenant s'intéresser aux nombres pairs $2p$ qui sont doubles de nombres premiers. Bien que vérifiant trivialement la conjecture, ils vont s'avérer présenter la propriété qu'on a découverte, et qui lie le caractère résidu de x à celui de $x+p$ parce qu'ils sont tous de la forme $4n+2$[8].
On s'intéresse notamment à ces nombres car l'étude des points de la comète de Goldbach en février 2011 nous a montré que ces nombres semblent *"minimiser"* la comète (avoir peu de décompositions de Goldbach comparativement à tous les autres). On a une explication heuristique de ce phénomène (ils n'ont pas de diviseurs autres qu'eux-mêmes et par ce que j'ai appelé la méthode du *"pliage de tissu"*, leurs colonnes s'éliminent systématiquement deux par deux au lieu de s'éliminer une par une comme elles le font dans le cas des diviseurs, ce qui minimisent le nombre de décompositions).

Si le nombre premier est un $4n+1$, on voit selon $2p$ une symétrie verticale qui fait que $x \ R \ 2p \iff x+p \ R \ 2p.$;
Si c'est un $4n+3$, on voit selon $2p$ une anti-symétrie verticale qui fait également que $x \ R \ 2p \iff x+p \ R \ 2p.$
La différence entre les deux sortes de nombres premiers est que dans un cas, les colonnes (qui contiennent un nombre x et son complémentaire à $2p$ qui est $2p-x$) soit contiennent deux résidus, soit contiennent deux non-résidus, alors que dans l'autre cas, ces deux cas peuvent se produire mais existent également des colonnes dans lesquelles l'un des nombres est un résidu et l'autre un non-résidu.

On omet dorénavant la ligne des restes des carrés dans les tables. On la remplace par une ligne de croix qui indique les décompositions de Goldbach (on suit la convention de Cantor qui consiste à considérer que 1 est un décomposant de Goldbach de $2p$ si $2p-1$ est premier).

On constate selon les modules $10, 26, 34, 58, 74, 82$ une symétrie verticale qui fait que $x \ R \ 2p \iff x+p \ R \ 2p.$

Selon le module 10, de la forme $2(4n+1)$:

10	9	8	7	6	5
0	1	2	3	4	5
			×		×

Selon le module 26, de la forme $2(4n+1)$:

26	25	24	23	22	21	20	19	18	17	16	15	14	13
0	1	2	3	4	5	6	7	8	9	10	11	12	13
			×				×						×

Selon le module 34, de la forme $2(4n+1)$:

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			×		×						×						×

[7] Ou encore pour paraphraser le titre de l'article d'Euler *"Découverte d'une loi tout extraordinaire des résidus/non-résidus des modules pairs* $4n+2$ *:* $x \ R \ p \iff x+p \ R \ 2p$

[8] Si $2a$ est de la forme $2(4n+1)$, $2a = 8n+2 = 2(4n)+2 = 4(2n)+2 = 4b+2$ tandis que si $2a$ est de la forme $2(4n+3)$, $2a = 2(4n+3) = 8n+6 = 8n+4+2 = 4(2n)+4+2 = 4(2n+1)+2 = 4b+2$.

Selon le module 58, de la forme $2(4n+1)$:

58	57	56	55	54	53	52	51	50	49	48	47	46	45	44
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
					×						×			

43	42	41	40	39	38	37	36	35	34	33	32	31	30	29
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
		×												×

Selon le module 74, de la forme $2(4n+1)$:

74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	×		×				×						×					

55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
												×						×

Selon le module 82, de la forme $2(4n+1)$:

82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
			×								×									

61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
		×						×												×

Voyons maintenant les modules doubles de premiers selon lesquels la symétrie devient une anti-symétrie. Selon ces modules $6, 14, 22, 38, 46, 62, 86, 94$, on constate une anti-symétrie verticale qui fait que $x \; R \; 2p \iff x+p \; R \; 2p$.

Selon le module 6, de la forme $2(4n+3)$:

6	5	4	3
0	1	2	3
	×		×

Selon le module 14, de la forme $2(4n+3)$:

14	13	12	11	10	9	8	7
0	1	2	3	4	5	6	7
	×		×				×

Selon le module 22, de la forme $2(4n+3)$:

22	21	20	19	18	17	16	15	14	13	12	11
0	1	2	3	4	5	6	7	8	9	10	11
			×		×						×

Selon le module 38, de la forme $2(4n+3)$:

38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	×						×												×

Selon le module 46, de la forme $2(4n+3)$:

46	45	44	4	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
			×		×												×						×

Selon le module 62, de la forme $2(4n+3)$:

62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	×		×												

46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
			×												×

Selon le module 86, de la forme $2(4n+3)$:

86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
			×				×						×						×		

64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
																					×

Selon le module 94, de la forme $2(4n+3)$:

94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
					×						×												×

70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
																	×						

3.2.2 Nombres pairs doubles d'impairs-non premiers

Selon les modules qui sont des nombres pairs doubles d'impairs non-premiers (les $4n+2$ qui ne sont pas doubles d'un nombre premier impair), $x \ R \ 2p \iff x+p \ R \ 2p$.

Selon le module $18 = 2.3^2$, de la forme $2(4n+3)^2$:

18	17	16	15	14	13	12	11	10	9
0	1	2	3	4	5	6	7	8	9
0	1	4	9	16	7	0	13	10	9

Selon le module $30 = 2p = 2.3.5$, de la forme $2(4n+3)(4n+1)$:

30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	4	9	16	25	6	19	4	21	13	1	24	19	16	15

Selon le module 30, en ne conservant que les colonnes des nombres premiers à 30, les relations verticales disparaissent :

29	23	19	17
1	7	11	13
1	19	1	19

Selon le module $42 = 2.3.7$, de la forme $2(4n+3)(4n'+3)$:

42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
	×				×						×		×						×		

Selon le module $50 = 2.5^2$, de la forme $2(4n+1)^2$:

50	49	48	47	46	45	44	43	42	41	40	39	38
0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	4	9	16	25	36	49	14	31	0	21	44

37	36	35	34	33	32	31	30	29	28	27	26	25
13	14	15	16	17	18	19	20	21	22	23	24	25
19	46	25	6	39	24	11	0	41	34	29	26	25

Selon le module $54 = 2.3^3$, de la forme $2(4n+3)^3$:

54	53	52	51	50	49	48	47	46	45	44	43	42	41
0	1	2	3	4	5	6	7	8	9	10	11	12	13
	×						×				×		×

40	39	38	37	36	35	34	33	32	31	30	29	28	27
14	15	16	17	18	19	20	21	22	23	24	25	26	27
			×						×				

Selon le module $66 = 2.3.11$, de la forme $2(4n+3)(4n'+3)$:

66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
					×		×						×			

49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
		×				×						×				

Selon le module $70 = 2.5.7$, de la forme $2(4n+1)(4n'+3)$:

70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			×								×						×

52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
					×						×						

Selon le module $78 = 2.3.13$, de la forme $2(4n+3)(4n'+1)$:

78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
					×		×				×						×		×

58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
											×						×		

Selon le module $90 = 2.3^2.5$, de la forme $2(4n+3)^2(4n'+1)$:

90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	×						×				×						×		×			

67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45
23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
×						×		×						×						×		

Selon le module $98 = 2.7^2$, de la forme $2(4n+3)^2$:

98	97	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	×																		×					

73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
						×						×												

Il semblerait que si la factorisation de n ne contient aucun nombre premier impair de la forme $4n+3$, on constate une symétrie verticale qui fait que

$$x \; R \; 2p \iff x+p \; R \; 2p.$$

Tandis que si la factorisation de n contient un nombre premier de la forme $4n+3$ au moins, on constate une anti-symétrie verticale qui fait également que

$$x \; R \; 2p \iff x+p \; R \; 2p.$$

.
Cette propriété découle vraisemblablement de la loi de réciprocité quadratique.

3.2.3 Nombres pairs doubles de pairs

Pour les nombres pairs doubles de pairs, on ne constate pas de symétrie ou d'anti-symétrie verticale par rapport à la ligne médiane du tableau symbolisée par deux doubles barres verticales autour de la colonne médiane. On essaiera cependant de comprendre les relations existant entre les caractères *résidu/non-résidu de* $2p$ de x et $x+p$.

Selon le module 8, de la forme 2^3 :

8	7	6	5	4
0	1	2	3	4
	×		×	

Selon le module $12 = 2^2.3$, de la forme $4(4n+3)$:

12	11	10	9	8	7	6
0	1	2	3	4	5	6
	×				×	

Selon le module 16, de la forme 2^4 :

16	15	14	13	12	11	10	9	8
0	1	2	3	4	5	6	7	8
			×		×			

Selon le module $20 = 2^2.5$, de la forme $4(4n+1)$:

20	19	18	17	16	15	14	13	12	11	10
0	1	2	3	4	5	6	7	8	9	10
	×		×				×			

Selon le module $24 = 2^3.3$, de la forme $2^3(4n+3)$:

24	23	22	21	20	19	18	17	16	15	14	13	12
0	1	2	3	4	5	6	7	8	9	10	11	12
	×				×		×				×	

Selon le module $28 = 2^2.7$, de la forme $4(4n+3)$:

28	27	26	25	24	23	22	21	20	19	18	17	16	15	14
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
					×						×			

Selon le module 32, de la forme 2^5 :

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	×		×										×			

Selon le module $36 = 2^2.3^2$, de la forme $4(4n+3)^2$:

36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	2	20	19	18
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
					×		×						×				×	

Selon le module $40 = 2^4.5$, de la forme $2^4(4n+1)$:

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
			×								×						×			

Selon le module $44 = 2^2.11$, de la forme $4(4n+3)$:

44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	×		×				×						×									

Selon le module $48 = 2^4.3$, de la forme $2^4(4n+3)$:

48	47	46	45	44	4	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
					×		×				×						×		×					

Selon le module $52 = 2^2.13$, de la forme $4(4n+1)$:

52	51	50	49	48	47	46	45	44	4	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
					×						×												×			

Selon le module $56 = 2^3.7$, de la forme $2^3(4n+3)$:

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
			×										×	

41	40	39	38	37	36	35	34	33	32	31	30	29	28
15	16	17	18	19	20	21	22	23	24	25	26	27	28
				×									

Selon le module $60 = 2^2.3.5$, de la forme $4(4n+3)(4n'+1)$:

60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	×						×						×		

44	43	42	41	40	39	38	37	36	35	34	33	32	31	30
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	×		×				×						×	

Selon le module 64, de la forme 2^6 :

64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
			×		×						×					

47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
×						×									

Selon le module $68 = 2^2.17$, de la forme $4(4n + 1)$:

68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	×						×										

50	49	48	47	46	45	44	4	42	41	40	39	38	37	36	35	34
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
													×			

Selon le module $72 = 2^3.3^2$, de la forme $2^3(4n + 3)^2$:

72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18
	×				×						×		×					

53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
×										×		×					

Selon le module $76 = 2^2.19$, de la forme $4(4n + 3)$:

76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18	19
			×		×												×		

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
			×						×									

Selon le module $80 = 2^4.5$, de la forme $2^4(4n+1)$:

80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18	19	20
	×						×						×						×	

59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40
2	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
																×			

Selon le module $84 = 2^2.3.7$, de la forme $4(4n+3)(4n'+3)$:

84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18	19	20	21
	×				×						×		×				×				

62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
	×								×						×				×	

Selon le module $88 = 2^3.11$, de la forme $2^3(4n+3)$:

88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
					×												×					

65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44
23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
						×												×			

Selon le module $92 = 2^2.23$, de la forme $4(4n+3)$:

92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	2	22	23
			×										×						×				

68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
							×															

Selon le module $96 = 2^5.3$, de la forme $2^5(4n+3)$:

96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	2	22	23	24
							×						×				×						×	

71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
				×								×						×					

Selon le module $100 = 2^2.5^2$, de la forme $4(4n+1)^2$:

100	99	98	97	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
			×								×						×								

74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
			×												×						×			

3.3 Progressions arithmétiques

Gauss fait mention de nombres appartenant à des progressions arithmétiques dans les articles 104, 147, 148 et 149 de la section Quatrième des Recherches Arithmétiques.

Voyons si les cas étudiés permettent d'obtenir des généralisations.
La première catégorie, pour laquelle un non-résidu du plus petit non-résidu de n fournit systématiquement une décomposition de Goldbach, les nombres sont $16, 24, 28, 40, 52, 54, 64, 70, 100$: à part 3 d'entre eux, (24, 54 et 70), ils sont tous de la forme $12k+4$. Cette notion de *non-résidu d'un non-résidu* est cependant problématique car la relation *résidu* ou la relation *non-résidu* ne sont pas transitives.

Dans la deuxième catégorie, pour lesquels on trouve toujours un non-résidu de tous les diviseurs impairs de n fournissant une décomposition de Goldbach, ils sont tous des formes suivantes : $12k$, $12k+2$, $12k+6$, $12k+8$ ou $12k+10$.

Mais en unifiant les deux catégories en une, dans la mesure où l'on peut toujours pour les nombres de la première catégorie trouver un décomposant de Goldbach qui soit non-résidu de tous les diviseurs de n, il semblerait qu'on puisse pour tous les nombres pairs n trouver un nombre premier non-résidu de tous les diviseurs impairs de n qui fournit une décomposition de Godlbach de n.

Essayons sur un nombre plus grand : $1182666 = 2.3.439.449$. Le nombre premier 157 est non-résidu à la fois de 3, 49 et 449 et il fournit une décomposition de Goldbach de 1182666.

4 Rêves d'un prince

On peut trouver sur la toile le journal mathématique de Gauss. On y lit que Gauss a étudié la conjecture de Goldbach le 14 mai 1796. On peut imaginer que les deux premières lettres mystérieuses du mot GEGAN qui apparaît dans la citation "Vicimus GEGAN" du 11 octobre 1796 sont les initiales respectives de Goldbach et Euler...

Annexe 1 : Résidus quadratiques des nombres inférieurs à 100

2 : 1
3 : 1
4 : 1
5 : 1 4
6 : 1 3 4
7 : 1 2 4
8 : 1 4
9 : 1 4 7
10 : 1 4 5 6 9
11 : 1 3 4 5 9
12 : 1 4 9
13 : 1 3 4 9 10 12
14 : 1 2 4 7 8 9 11
15 : 1 4 6 9 10
16 : 1 4 9
17 : 1 2 4 8 9 13 15 16
18 : 1 4 7 9 10 13 16
19 : 1 4 5 6 7 9 11 16 17
20 : 1 4 5 9 16
21 : 1 4 7 9 15 16 18
22 : 1 3 4 5 9 11 12 14 15 16 20
23 : 1 2 3 4 6 8 9 12 13 16 18
24 : 1 4 9 12 16
25 : 1 4 6 9 11 14 16 19 21 24
26 : 1 3 4 9 10 12 13 14 16 17 22 23 25
27 : 1 4 7 9 10 13 16 19 22 25
28 : 1 4 8 9 16 21 25
29 : 1 4 5 6 7 9 13 16 20 22 23 24 25 28
30 : 1 4 6 9 10 15 16 19 21 24 25
31 : 1 2 4 5 7 8 9 10 14 16 18 19 20 25 28
32 : 1 4 9 16 17 25
33 : 1 3 4 9 12 15 16 22 25 27 31
34 : 1 2 4 8 9 13 15 16 17 18 19 21 25 26 30 32 33
35 : 1 4 9 11 14 15 16 21 25 29 30
36 : 1 4 9 13 16 25 28
37 : 1 3 4 7 9 10 11 12 16 21 25 26 27 28 30 33 34 36
38 : 1 4 5 6 7 9 11 16 17 19 20 23 24 25 26 28 30 35 36
39 : 1 3 4 9 10 12 13 16 22 25 27 30 36
40 : 1 4 9 16 20 24 25 36
41 : 1 2 4 5 8 9 10 16 18 20 21 23 25 31 32 33 36 37 39 40
42 : 1 4 7 9 15 16 18 21 22 25 28 30 36 37 39
43 : 1 4 6 9 10 11 13 14 15 16 17 21 23 24 25 31 35 36 38 40 41
44 : 1 4 5 9 12 16 20 25 33 36 37
45 : 1 4 9 10 16 19 25 31 34 36 40
46 : 1 2 3 4 6 8 9 12 13 16 18 23 24 25 26 27 29 31 32 35 36 39 41
47 : 1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42
48 : 1 4 9 16 25 33 36
49 : 1 2 4 8 9 11 15 16 18 22 23 25 29 30 32 36 37 39 43 44 46
50 : 1 4 6 9 11 14 16 19 21 24 25 26 29 31 34 36 39 41 44 46 49
51 : 1 4 9 13 15 16 18 19 21 25 30 33 34 36 42 43 49
52 : 1 4 9 12 13 16 17 25 29 36 40 48 49
53 : 1 4 6 7 9 10 11 13 15 16 17 24 25 28 29 36 37 38 40 42 43 44 46 47 49 52
54 : 1 4 7 9 10 13 16 19 22 25 27 28 31 34 36 37 40 43 46 49 52
55 : 1 4 5 9 11 14 15 16 20 25 26 31 34 36 44 45 49
56 : 1 4 8 9 16 25 28 32 36 44 49
57 : 1 4 6 7 9 16 19 24 25 28 30 36 39 42 43 45 49 54 55
58 : 1 4 5 6 7 9 13 16 20 22 23 24 25 28 29 30 33 34 35 36 38 42 45 49 51 52 53 54 57

59 : 1 3 4 5 7 9 12 15 16 17 19 20 21 22 25 26 27 28 29 35 36 41 45 46 48 49 51 54 53 57
60 : 1 4 9 16 21 24 25 36 40 45 49
61 : 1 3 4 5 9 12 13 14 15 16 19 20 22 25 27 34 36 39 41 42 45 46 47 48 49 52 54 56 57 58 60
62 : 1 2 4 5 7 8 9 10 14 16 18 19 20 25 28 31 32 33 35 36 38 39 40 41 45 47 49 54 50 51 56 59
63 : 1 4 7 9 16 18 22 25 28 36 37 43 46 49 58
64 : 1 4 9 16 17 25 33 36 41 49 57
65 : 1 4 9 10 14 16 25 26 29 30 35 36 39 40 49 51 55 56 61 64
66 : 1 3 4 9 12 15 16 22 25 27 31 33 34 36 37 42 45 48 49 55 58 60 64
67 : 1 4 6 9 10 14 15 16 17 19 21 22 23 24 25 26 29 33 35 36 37 39 40 47 49 54 55 56 59 60 62 64 65
68 : 1 4 8 9 13 16 17 21 25 32 33 36 49 52 53 60 64
69 : 1 3 4 6 9 12 13 16 18 24 25 27 31 36 39 46 48 49 52 54 55 58 64
70 : 1 4 9 11 14 15 16 21 25 29 30 35 36 39 44 46 49 50 51 56 60 64 65
71 : 1 2 3 4 5 6 8 9 10 12 15 16 18 19 20 24 25 27 29 30 32 36 37 38 40 43 45 48 49 50 54 57 58 60 64
72 : 1 4 9 16 25 28 36 40 49 52 64
73 : 1 2 3 4 6 8 9 12 16 18 19 23 24 25 27 32 35 36 37 38 41 46 48 49 50 54 55 57 61 64 65 67 69 70 71 72
74 : 1 3 4 7 9 10 11 12 16 21 25 26 27 28 30 33 34 36 37 38 40 41 44 46 47 48 49 53 58 62 63 64 65 67 70 71 73
75 : 1 4 6 9 16 19 21 24 25 31 34 36 39 46 49 51 54 61 64 66 69
76 : 1 4 5 9 16 17 20 24 25 28 36 44 45 49 57 61 64 68 73
77 : 1 4 9 11 14 15 16 22 23 25 36 37 42 44 49 53 56 58 60 64 67 70 71
78 : 1 3 4 9 10 12 13 16 22 25 27 30 36 39 40 42 43 48 49 51 52 55 61 64 66 69 75
79 : 1 2 4 5 8 9 10 11 13 16 18 19 20 21 22 23 25 26 31 32 36 38 40 42 44 45 46 49 50 51 52 55 62 64 65 67 72 73 76
80 : 1 4 9 16 20 25 36 41 49 64 65
81 : 1 4 7 9 10 13 16 19 22 25 28 31 34 36 37 40 43 46 49 52 55 58 61 63 64 67 70 73 76 79
82 : 1 2 4 5 8 9 10 16 18 20 21 23 25 31 32 33 36 37 39 40 41 42 43 45 46 49 50 51 57 59 61 62 64 66 72 73 74 77 78 80 81
83 : 1 3 4 7 9 10 11 12 16 17 21 23 25 26 27 28 29 30 31 33 36 37 38 40 41 44 48 49 51 59 61 63 64 65 68 69 70 75 77 78 81
84 : 1 4 9 16 21 25 28 36 37 49 57 60 64 72 81
85 : 1 4 9 15 16 19 21 25 26 30 34 35 36 49 50 51 55 59 60 64 66 69 70 76 81 84
86 : 1 4 6 9 10 11 13 14 15 16 17 21 23 24 25 31 35 36 38 40 41 43 44 47 49 52 53 54 56 57 58 59 60 64 66 67 68 74 78 79 81 83 84
87 : 1 4 6 7 9 13 16 22 24 25 28 30 33 34 36 42 45 49 51 52 54 57 58 63 64 67 78 81 82
88 : 1 4 9 12 16 20 25 33 36 44 48 49 56 60 64 80 81
89 : 1 2 4 5 8 9 10 11 16 17 18 20 21 22 25 32 34 36 39 40 42 44 45 47 49 50 53 55 57 64 67 68 69 71 72 73 78 79 80 81 84 85 87 88
90 : 1 4 9 10 16 19 25 31 34 36 40 45 46 49 54 55 61 64 70 76 79 81 85
91 : 1 4 9 14 16 22 23 25 29 30 35 36 39 42 43 49 51 53 56 64 65 74 77 78 79 81 88
92 : 1 4 8 9 12 13 16 24 25 29 32 36 41 48 49 52 64 69 72 73 77 81 85
93 : 1 4 7 9 10 16 18 19 25 28 31 33 36 39 40 45 49 51 63 64 66 67 69 70 72 76 78 81 82 87 90
94 : 1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42 47 48 49 50 51 53 54 55 56 59 61 63 64 65 68 71 72 74 75 79 81 83 84 89
95 : 1 4 5 6 9 11 16 19 20 24 25 26 30 35 36 39 44 45 49 54 55 61 64 66 74 76 80 81 85
96 : 1 4 9 16 25 33 36 48 49 57 64 73 81
97 : 1 2 3 4 6 8 9 11 12 16 18 22 24 25 27 31 32 33 35 36 43 44 47 48 49 50 53 54 61 62 64 65 66 70 72 73 75 79 81 85 86 88 89 91 93 94 95 96
98 : 1 2 4 8 9 11 15 16 18 22 23 25 29 30 32 36 37 39 43 44 46 49 50 51 53 57 58 60 64 65 67 71 72 74 78 79 81 85 86 88 92 93 95
99 : 1 4 9 16 22 25 27 31 34 36 37 45 49 55 58 64 67 70 81 82 88 91 97
100 : 1 4 9 16 21 24 25 29 36 41 44 49 56 61 64 69 76 81 84 89 96

Annexe 2 : Extraits de la section Quatrième *"Des Congruences du second degré"* des Recherches Arithmétiques

On ne fait ici que recopier des extraits de la section Quatrième des Recherches Arithmétiques qu'il faudrait bien maîtriser pour pouvoir démontrer que l'existence d'un décomposant de Goldbach pour chaque nombre pair découle de l'existence d'au moins une solution pour un certain système de congruences (ou incongruences, c'est quasiment l'opposé) quadratiques, cette dernière existence découlant quant à elle du théorème d'or appliqué aux nombres adéquats. Les articles les plus difficiles, mais peut-être les plus utiles pour notre problème sont **les articles** 104 **et** 105 puis 147**,** 148 **et** 149.

page 69, article 94 : THÉORÈME. Un nombre quelconque m étant pris pour module, il ne peut y avoir dans la suite $1, 2, 3 \ldots m-1$, plus de $\frac{1}{2}m+1$ nombres, quand m est pair, et plus de $\frac{1}{2}m+\frac{1}{2}$, quand m est impair, qui soient congrus à un carré.

page 70, article 96 : Le nombre premier p étant pris pour module, la moitié des nombres $1, 2, 3 \ldots p-1$, sera composée de résidus quadratiques, et l'autre moitié de non-résidus, c'est-à-dire qu'il y aura $\dfrac{1}{2}(p-1)$ résidus, et autant de non-résidus.

page 72, article 98 : THÉORÈME. Le produit de deux résidus quadratiques d'un nombre premier p est un résidu ; le produit d'un résidu et d'un non-résidu est non-résidu ; enfin le produit de deux non-résidus est résidu.
1°. Soient A et B les résidus qui proviennent des carrés a^2, b^2, ou soient $A \equiv a^2 \ (mod\ p)$ et $B \equiv b^2$, on aura $AB \equiv a^2b^2$, c'est-à-dire qu'il sera un résidu.
2°. Quand A est résidu, ou que $A \equiv a^2$, mais que B est non-résidu, AB est non-résidu. Soit en effet, s'il se peut $AB \equiv k^2$ et $\frac{k}{a} \ (mod\ p) \equiv b$, on aura $a^2B \equiv a^2b^2$ et partant $B \equiv b^2$, contre l'hypothèse.
Autrement. Si l'on multiplie par A les $\frac{p-1}{2}$ nombres de la suite $1, 2, 3 \ldots p-1$, qui sont résidus, tous les produits seront des résidus quadratiques, et ils seront tous incongrus. Or si l'on multiplie par A un nombre B non-résidu, le produit ne sera congru à aucun des précédents : donc, s'il était résidu, il y aurait $\frac{1}{2}(p+1)$ résidus incongrus, parmi lesquels ne serait pas 0, ce qui est impossible (n^o 96).
3°. Soient A et B deux nombres non-résidus, en multipliant par A tous les nombres qui sont résidus dans la suite $1, 2, 3, \ldots p-1$, on aura $\frac{p-1}{2}$ non-résidus, incongrus entr'eux (2°). Or le produit AB ne peut être congru à aucun de ceux-là ; donc s'il était non-résidu, on aurait $\frac{p+1}{2}$ non-résidus incongrus entr'eux ; ce qui est impossible (n^o 96).
Ces théorèmes se déduisent encore plus facilement des principes de la section précédente. En effet, puisque l'indice d'un résidu est toujours pair, et celui d'un non-résidu toujours impair, l'indice du produit de deux résidus ou non-résidus sera pair, et partant, le produit sera lui-même un résidu. Au contraire, si l'un des facteurs est non-résidu, et l'autre résidu, l'indice sera impair, et le produit non-résidu.
On peut aussi faire usage des deux méthodes pour démontrer ce THÉORÈME[9] : *la valeur de l'expression* $\frac{a}{b} \ (mod\ p)$*, sera un résidu, quand les nombres a et b seront tous les deux résidus ou non-résidus. Elle sera un non-résidu, quand l'un des nombres a et b sera résidu et l'autre non-résidu.* On le démontrerait encore en renversant les théorèmes précédents.

page 73, article 99 : Généralement, le produit de tant de facteurs qu'on voudra est un résidu, soit lorsque tous les facteurs en sont eux-mêmes, soit lorsque le nombre de facteurs non-résidus est pair ; mais quand le nombre des facteurs non-résidus est impair, le produit est non-résidu. On peut donc juger facilement si un nombre composé est résidu ou non ; pourvu qu'on sache ce que sont ses différents facteurs. Aussi dans la Table II, nous n'avons admis que les nombres premiers. Quant à sa disposition, les modules sont en marge[10], en tête les nombres premiers successifs ; quand l'un de ces derniers est résidu, on a placé un trait dans l'espace qui correspond au module et à ce nombre ; quand il est non-résidu, on a laissé l'espace vide.

page 73, article 100 : Si l'on prend pour module la puissance p^n d'un nombre premier, p étant > 2, une moitié des nombres non-divisibles par p et $< p^n$ seront des résidus, et l'autre des non-résidus ; c'est-à-dire

[9] Ici, je mets les petites capitales à ce mot bien qu'elles ne soient pas présentes dans les Recherches Arithmétiques dans la mesure où la démonstration de ce théorème n'est pas fournie.
[10] On verra bientôt comment on peut se passer des modules composés.

qu'il y en aura $\frac{p-1}{2}.p^{n-1}$ de chaque espèce.
En effet, si r est un résidu, il sera congru à un carré dont la racine ne surpasse pas la moitié du module (n^o 94) ; et l'on voit facilement qu'il y a $\frac{1}{2}p^{n-1}(p-1)$ nombres $< \frac{p^n}{2}$ et non-divisibles par p. Ainsi il reste à démontrer que les carrés de tous ces nombres sont incongrus, ou qu'ils donnent des résidus différents. Or si deux nombres a et b non-divisibles par p et plus petits que la moitié du module, avaient leurs carrés congrus, on aurait $a^2 - b^2$ ou $(a+b)(a-b)$ divisible par p^n, en supposant $a > b$, ce qui est permis. Mais cette condition ne peut avoir lieu, à moins que l'un des deux nombres $(a-b)$, $(a+b)$ ne soit divisible par p^n, ce qui est impossible, puisque chacun d'eux est plus petit que p^n, ou bien que l'un étant divisible par p^μ, l'autre le soit par $p^{\nu-\mu}$ ou chacun d'eux par p ; ce qui est encore impossible, puisqu'il s'ensuivrait que la somme $2a$ et la différence $2b$, et partant a et b eux-mêmes seraient divisibles par p, contre l'hypothèse. Donc enfin parmi les nombres non-divisibles par p et moindres que le module, il y a $\frac{p-1}{2}p^{n-1}$ résidus, et les autres, en même nombre, sont non-résidus.

page 74, article 101 : Tout nombre non-divisible par p, qui est résidu de p, sera aussi résidu de p^n ; celui qui ne sera pas résidu de p ne le sera pas non plus de p^n.
La seconde partie de cette proposition est évidente par elle-même ; ainsi si la première n'était pas vraie, parmi les nombres plus petits que p^n et non-divisibles par p, il y en aurait plus qui fussent résidus de p qu'il n'y en aurait qui le fussent de p^n, c'est-à-dire plus de $\frac{1}{2}p^{n-1}(p-1)$. Mais on peut voir sans peine que le nombre des résidus de p qui se trouvent entre 1 et p^n, est précisément $\frac{1}{2}p^{n-1}(p-1)$.
Il est tout aussi facile de trouver effectivement un carré qui soit congru à un résidu donné, suivant le module p^n, si l'on connaît un carré congru à ce résidu suivant le module p.
Soit en effet a^2 un carré congru au résidu donné A, suivant le module p^μ, on en déduira, de la manière suivante, un carré $\equiv A$, suivant le module p^ν, ν étant $> \mu$ et non plus grand que 2μ. Supposons que la racine du carré cherché soit $\pm a + xp^\mu$; et il est aisé de s'assurer que c'est là la forme qu'elle doit avoir. Il faut donc qu'on ait $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv A \ (mod\ p^\nu)$, ou comme $2\mu > \nu$, on aura $\pm 2axp^\mu \equiv A - a^2 \ (mod\ p^\nu)$. Soit $A - a^2 = p^\mu.d$, on aura $\pm 2ax \equiv d \ (mod\ p^{\nu-\mu})$; donc x sera la valeur de l'expression $\pm\frac{d}{2a} \ (mod\ p^{\nu-\mu})$. Ainsi étant donné un carré congru à A, suivant le module p, on en déduira un carré congru à A, suivant le module p^2 ; de là au module p^4, au module p^8, etc.
Exemple. Etant proposé le résidu 6 congru au carré 1, suivant le module 5, on trouve le carré 9^2 auquel il est congru suivant le module 25, 16^2 auquel il est congru suivant le module 125, etc.

page 75, article 102 : Quant à ce qui regarde les nombres divisibles par p, il est clair que leurs carrés seront divisibles par p^2, et que partant tous les nombres qui seront divisibles par p et non par p^2, seront non-résidus de p^n. Et en général, si l'on propose le nombre p^kA, A n'étant pas divisible par p, il y aura trois cas à distinguer :
1°. Si $k \geq n$, on aura $p^kA \equiv 0 \ (mod\ p^n)$, c'est-à-dire qu'il sera résidu.
2°. Si $k < n$ et impair, p^kA sera non-résidu.
3°. Si $k < n$ et pair, p^kA sera résidu ou non-résidu de p^n suivant que A sera résidu ou non-résidu de p.

page 76, article 103 : Comme nous avons commencé (n^o 100) par exclure le cas où $p = 2$, il faut ajouter quelque chose à ce sujet. Quand 2 est module, tous les nombres sont résidus, et il n'y en a point de non-résidus. Quand le module est 4, tous les nombres impairs de la forme $4k+1$ sont résidus, et tous ceux de la forme $4k+3$ sont non-résidus. Enfin, quand le module est 8 ou une plus haute puissance de 2, tous les nombres impairs de la forme $8k+1$ sont résidus, et les autres, ou ceux de la forme $8k+3$, $8k+5$, $8k+7$ sont non-résidus ;

page 77, article 104 : Pour ce qui regarde le nombre de valeurs différentes, c'est-à-dire incongrues suivant le module, que peut admettre l'expression $V = \sqrt{A} \ (mod\ p^n)$, pourvu que A soit un résidu de p^n, on déduit facilement de ce qui précède, les conclusions suivantes. Nous supposons toujours que p est un nombre premier et, pour abréger, nous considérons en même temps le cas où $n = 1$.
1^o. Si A n'est pas divisible par p, V n'a qu'une seule valeur pour $p = 2$ et $n = 1$; ce sera $V \equiv 1$; il en a deux quand p est impair, ou bien quand on a $p = 2$ et $n = 2$; et, si l'une est $\equiv \nu$, l'autre sera $\equiv -\nu$; il en a quatre pour $p = 2$ et $n > 2$; et si l'une est $\equiv \nu$, les autres seront $\equiv \nu + 2^{n-1}, -\nu + 2^{n-1}, -\nu$.
2^o. Si A est divisible par p, mais non par p^n, soit $p^{2\mu}$ la plus haute puissance de p qui divise A, car

cette puissance doit être paire (n^o 102), et $A = ap^{2\mu}$; il est clair que toutes les valeurs de V doivent être divisibles par p^μ, et que tous les quotients donnés par ces divisions seront les valeurs de l'expression $V' = \sqrt{a}\ (mod\ p^{n-2\mu})$; on aura donc toutes les valeurs différentes de V, en multipliant par p^μ, toutes celles de V' contenues entre 0 et $p^{n-\mu}$. Elles seront, par conséquent,
$\nu p^\mu, \nu p^\mu + p^{n-\mu}, \nu p^\mu + 2p^{n-\mu}, \ldots \nu p^\mu + (p^\mu - 1)p^{n-\mu}$,
ν étant une valeur quelconque de V : suivant donc que V' aura 1, ou 2, ou [11] valeurs, V en aura p^μ, ou $2p^\mu$ ou $4p^\mu$ (1^o).
3^o. Si A est divisible par p^n, on voit facilement, en posant $n = 2m$ ou $= 2m - 1$, suivant que n est pair ou impair, que tous les nombres divisibles par p^m sont des valeurs de V, et qu'il n'y en a pas d'autres ; mais les nombres divisibles par p^m sont $0, p^m, 2p^m \ldots (p^{n-m} - 1)p^m$, dont le nombre est p^{n-m}.

page 78, article 105 : Il reste à examiner le cas où le module m est composé de plusieurs modules premiers. Soit $m = abc\ etc.$, a, b, c, *etc.* étant des nombres premiers différents. Il est clair d'abord que si n est résidu de m, il le sera aussi des différents nombres, a, b, c, *etc.*, et que partant il sera non-résidu de m, s'il est non-résidu de quelqu'un de ces nombres. Réciproquement, si n est résidu des différents nombres a, b, c, *etc.*, il le sera de leur produit m ; en effet, si l'on a $n \equiv A^2, B^2, C^2, etc.$, suivant les modules a, b, c, *etc.*, respectivement (n^o 32), on aura $n \equiv N^2$, suivant tous ces modules, et conséquemment suivant leur produit.
Comme on voit facilement que la valeur de N résulte de la combinaison d'une valeur quelconque de A, ou de l'expression $\sqrt{n}\ (mod\ a)$, avec une valeur quelconque de B, avec une valeur quelconque de C, *etc*, que les différentes combinaisons donneront des valeurs différentes, et qu'elles les donneront toutes ; le nombre des valeurs de N sera égal au produit des nombres de valeurs de A, B, C, *etc.* que nous avons appris à déterminer dans l'article précédent.

page 78, article 106 : On voit par ce qui précède, qu'il suffit de reconnaître si un nombre donné est résidu ou non-résidu d'un nombre premier donné, et que tous les cas reviennent à celui-là.
Un nombre quelconque A, non divisible par un nombre premier $2m + 1$, est résidu ou non-résidu de ce nombre premier suivant que $A^m \equiv +1 ou \equiv -1\ (mod\ 2m + 1)$.

page 80, article 109 : en effet, il est évident que si r est un résidu, $\dfrac{1}{r}\ (mod\ p)$ en sera un aussi.

(Les **articles** 108 **à** 124 **des pages** 79 **à** 91 traitent des cas particuliers 1, -1, 2, -2, 3, -3, 5, -5, 7 et -7.)

page 81, article 111 : Si donc r est résidu d'un nombre premier de la forme $4n + 1$, $-r$ le sera aussi, et tous les non-résidus seront encore non-résidus en changeant les signes[12]. Le contraire arrive pour les nombres premiers de la forme $4n + 3$, dont les résidus deviennent non-résidus, et réciproquement quand on change le signe (n^o 98).
Au reste on déduit facilement de ce qui précède cette règle générale : -1 est résidu de tous les nombres qui ne sont divisibles ni par 4, ni par aucun nombre de la forme $4n + 3$. Il est non-résidu de tous les autres.(N^{os} 103 *et* 105).

page 81, article 112 : Passons maintenant aux résidus $+2$ et -2.
Si dans la table II on prend tous les nombres premiers dont le module est $+2$, on trouvera $7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97$. Or on remarque facilement qu'aucun d'eux n'est de la forme $8n + 3$ ou $8n + 5$.
Voyons donc si cette induction peut devenir une certitude.
Observons d'abord que tout nombre composé de la forme $8n + 3$ ou $8n + 5$ renferme nécessairement un facteur premier de l'une ou l'autre forme ; en effet les nombres premiers de la forme $8n + 1$ et $8n + 7$ ne peuvent former que des nombres de la forme $8n + 1$ ou $8n + 7$. Si donc notre induction est généralement vraie, il n'y aura aucun nombre de la forme $8n + 3$, $8n + 5$, dont le résidu soit $+2$. Or il est bien certain qu'il n'existe aucun nombre de cette forme et au-dessous de 100, dont le résidu soit $+2$; mais s'il y en avait au-dessus de cette limite, supposons que t soit le plus petit de tous ; t sera de la forme $8n + 3$ ou $8n + 5$, et $+2$ sera son résidu ; mais il sera non-résidu de tous les nombres semblables plus petits. Soit $a^2 \equiv 2\ (mod\ t)$, on pourra toujours prendre a impair et $< t$, car a a au moins deux valeurs positives plus

[11] ici, je crois qu'il manque un mot, le chiffre 4 ?
[12] Ainsi quand nous parlerons d'un nombre, en tant qu'il sera résidu ou non-résidu d'un nombre de la forme $4n + 1$, nous pouvons ne faire aucune attention à son signe, ou lui donner le signe $\pm$.

petites que t, dont la somme $= t$, et dont par conséquent l'une est paire et l'autre impaire (N^{os} 104, 105). Cela posé, soit $a^2 = 2 + ut$ ou $ut = a^2 - 2$, a^2 sera de la forme $8n + 1$, et par-conséquent ut de la forme $8n - 1$; donc u sera de la forme $8n + 3$ ou $8n + 5$ suivant que t sera de la forme $8n + 5$ ou $8n + 3$; mais de l'équation $a^2 = 2 + tu$, on tire la congruence $a^2 \equiv 2(mod\ u)$, c'est-à-dire que $+2$ serait aussi résidu de u. Il est aisé de voir qu'on a $u < t$; il s'ensuivrait que t ne serait pas le plus petit nombre qui eût $+2$ pour résidu, ce qui est contre l'hypothèse ; d'où suit enfin une démonstration rigoureuse de cette proposition que nous avions déduite de l'induction.
En combinant cette proposition avec celles du n^o 111, on en déduit les théorèmes suivants :
I. $+2$ est non-résidu, et -2 est résidu de tous les nombres premiers de la forme $8n + 3$.
II. $+2$ et -2 sont non-résidus de tous les nombres premiers de la forme $8n + 5$.

page 82, article 113 : Par une semblable induction on tirera de la Table II, pour les nombres premiers dont le résidu est -2, ceux-ci : $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$[13]. Parmi ces nombres il ne s'en trouve aucun de la forme $8n + 5$ ou $8n + 7$; cherchons donc si de cette induction nous pouvons tirer un théorème général. On fera voir de la même manière que dans l'article précédent, qu'un nombre composé de la forme $8n + 5$ ou $8n + 7$, doit renfermer un facteur premier de la forme $8n + 5$ ou de la forme $8n + 7$; de sorte que si notre induction est généralement vraie, -2 ne peut être résidu d'aucun nombre de la forme $8n + 5$ ou $8n + 7$; or s'il peut y en avoir de tels, soit t le plus petit de tous, et qu'on ait $-2 = a^2 - tu$. Si l'on prend, comme plus haut, a impair et $< t$, u sera de la forme $8n + 5$ ou $8n + 7$ suivant que t sera de la forme $8n + 7$ ou $8n + 5$; mais de ce qu'on a $a < t$ et $ut = a^2 + 2$, il est facile de déduire que u est $< t$; et comme -2 serait aussi résidu de u, il s'ensuivrait que t ne serait pas le plus petit nombre dont -2 est le résidu, ce qui est contre l'hypothèse. Donc -2 sera nécessairement non-résidu de tous les nombres de la forme $8n + 5$ ou $8n + 7$.
En combinant cette proposition avec celles du n^o 111, on en déduit les théorèmes suivants :
I. -2 et $+2$ sont non-résidus de tous les nombres premiers de la forme $8n + 5$; comme nous l'avons déjà trouvé.
II.-2 est non-résidu et $+2$ résidu de tous les nombres premiers de la forme $8n + 7$.
Au reste, nous aurions pu prendre a pair dans les deux démonstrations ; mais alors il eût fallu distinguer le cas où a est de la forme $4n + 2$, de celui où il est de la forme $4n$; d'ailleurs la marche est absolument la même et n'est sujette à aucune difficulté.

page 83, article 114 : Il nous reste encore à traiter le cas où le nombre premier est de la forme $8n + 1$; mais il échappe à la méthode précédente et demande des artifices tout-à-fait particuliers.
Soit, pour le module premier $8n+1$, une racine primitive quelconque a, on aura (n^o 62) $a^{4n} \equiv -1\ (mod\ 8n+1)$; cette congruence peut se mettre sous la forme $(a^{2n} + 1)^2 \equiv 2a^{2n}\ (mod\ 8n + 1)$, ou $(a^{2n} - 1)^2 \equiv -2a^{2n}$; d'où il suit que $2a^{2n}$ et $-2a^{2n}$ sont résidus de $8n + 1$; mais comme a^{2n} est un carré non-divisible par le module, $+2$ et -2 seront aussi résidus (n^o 98).

page 84, article 116 : Au reste on tire facilement de ce qui précède la règle générale suivante : $+2$ est résidu de tout nombre qui n'est divisible ni par 4 ni par aucun nombre premier de la forme $8n + 3$ ou $8n+5$, et non-résidu de tous les autres, par exemple, de tous ceux de la forme $8n+3$, $8n+5$, tant premiers que composés.

page 91, article 125 : Tout nombre premier de la forme $4n + 1$ soit positif, soit négatif, est non-résidu de quelques nombres premiers, et même de nombres premiers plus petits que lui (il est évident qu'il faut éviter $+1$).

page 95, article 129 : Théorème. Si a est un nombre premier de la forme $8n+1$, il y aura nécessairement au-dessous de $2\sqrt{a}$ un nombre premier dont a est non-résidu.

page 95, article 130 : Maintenant que nous avons démontré que tout nombre premier de la forme $4n+1$ positif ou négatif, est toujours non-résidu d'un nombre premier au moins plus petit que lui...

page 98, au milieu du article 132 : mais, avant tout, il faut observer que tout nombre de la forme $4n + 1$ ne renfermera aucun facteur de la forme $4n + 3$, ou en renfermera un nombre pair parmi lesquels

[13]En considérant -2 comme le produit de $+2$ par -1 ; voyez n^o 111.

il pourra y en avoir d'égaux ; tandis que tout nombre de la forme $4n+3$ doit en renfermer un nombre impair. Le nombre des facteurs de la forme $4n+1$ reste indéterminé.

pages 108 et suiv., articles 146 à 150 : Au moyen du théorème fondamental [14] et des propositions relatives à -1, ± 2, on peut toujours déterminer si un nombre donné quelconque est résidu ou non-résidu d'un nombre premier donné.

Ensuite, dans l'**article 146**, Gauss généralise et explique la méthode permettant, étant donnés deux nombres quelconques P et Q, de trouver si l'un d'eux est résidu ou non-résidu de l'autre. Pour cela, il étudie la relation qui lie Q à chaque puissance de premier qui intervient dans la factorisation de P. Ce qui retient l'attention, c'est le début du point III de cet article 146, qui explique comment s'effectue le passage du second degré au premier degré :
On cherchera de la manière suivante la relation d'un nombre quelconque Q à un nombre premier a impair : quand $Q > a$, on substituera à Q son *résidu minimum positif* suivant le module a, ou, ce qui est quelquefois avantageux, son *résidu minimum absolu*, qui aura avec a la même relation que Q.
Or si l'on résoud Q, ou le nombre pris à sa place, en facteurs premiers p, p', p'', *etc.*, auxquels il faut joindre le facteur -1, quand Q est négatif, il est évident que la relation de Q à a dépendra de la relation des facteurs p, p', p'', *etc.* à a : de sorte que, si parmi eux il y en a $2m$ non-résidus de a, on aura QRa[15] ; mais s'il y en a $2m+1$, on aura QNa. Au reste, on voit facilement que si parmi les facteurs p, p', p'', *etc.*, il y en a un nombre pair d'égaux entre eux, on peut les rejeter, puisqu'ils n'influent en rien sur la relation de Q à a.

Dans les **articles** 147**,** 148 **et** 149, Gauss résoud le problème suivant : Etant proposé un nombre quelconque A, on peut trouver certaines formules qui contiennent tous les nombres premiers à A dont A est résidu, ou tous ceux qui sont diviseurs des nombres de la forme $x^2 - A$, x^2 étant un carré indéterminé. Nous appellerons simplement ces nombres *diviseurs* de $x^2 - A$; l'on voit facilement ce que sont les *non-diviseurs*. Mais pour abréger nous ne considérerons que les diviseurs qui sont impairs et premiers à A, les autres cas se ramenant sans peine à celui-là.

On recopie intégralement ces trois articles qui nous semblent très liés à l'idée que l'on cherche à développer.

Suite de l'article 147, page 110 : Soit d'abord A un nombre premier positif de la forme $4n+1$, ou négatif de la forme $4n-1$. Suivant le théorème fondamental, tous les nombres premiers qui, pris positivement, sont résidus de A, seront diviseurs de $x^2 - A$; mais tous les nombres premiers non-résidus de A seront non-diviseurs de $x^2 - A$, si pourtant on en excepte 2, qui est toujours diviseur. Soient r, r', r'', *etc.*, tous les résidus de A qui sont plus petits que lui, et n, n', n'', *etc.*, tous les non-résidus ; alors tout nombre premier contenu dans une des formes $Ak+r$, $Ak+r'$, $Ak+r''$, *etc.*, sera diviseur de $x^2 - A$; mais tout nombre premier contenu dans une des formes $Ak+n$, $Ak+n'$, *etc.*, sera non-diviseur de $x^2 - A$, k étant un nombre entier indéterminé. Nous appellerons les premières *formes des diviseurs* de $x^2 - A$ et les dernières *formes des non-diviseurs*. Le nombre de chacune d'elles sera égal au nombre de résidus r, r', *etc.* ou de non-résidus n, n', *etc.*, et partant, $(n^o\ 96) = \frac{1}{2}(A-1)$. Or si B est un nombre composé impair et que l'on ait ARB, tous les facteurs premiers de B seront contenus dans une des premières formes, et par conséquent, B lui-même ; donc tout nombre composé impair qui sera contenu dans la forme des non-diviseurs sera non-diviseur de $x^2 - A$; mais on ne peut pas dire que les non-diviseurs de $x^2 - A$ sont tous compris dans la forme des non-diviseurs, car en supposant B non-diviseur de $x^2 - A$, et si le nombre de ces facteurs est pair, B sera compris dans quelque forme de diviseurs (n^o 93).
Ainsi, soit $A = -11$; on trouvera que les formes des diviseurs de $x^2 + 11$ sont $11k+1$, 2, 3, 4, 5, 9, et que celles des non-diviseurs sont $11k+2$, 6, 7, 8, 10. Ainsi -11 sera résidu de tous les nombres premiers contenus dans une des premières formes et non-résidu de ceux qui sont contenus dans une des dernières.
On peut trouver des formes semblables pour les diviseurs et les non-diviseurs de $x^2 - A$, quel que soit A ; mais on voit aisément qu'on n'a à considérer que les valeurs de A qui ne sont divisibles par aucun carré ; car si $A = a^2A'$, tous les diviseurs de $x^2 - A$ premiers avec A, seront diviseurs de $x^2 - A'$, et de même pour les non-diviseurs. Or nous distinguerons trois cas : 1°. quand A est de la forme $4n+1$ ou $-(4n-1)$; 2°. quand A est de la forme $4n-1$ ou $-(4n+1)$; 3°. quand A est pair ou de la forme $\pm(4n+2)$.

[14] communément appelé actuellement la *"loi de réciprocité quadratique"*.
[15] Gauss utilise la lettre R pour signifier *"est résidu quadratique de"* et la lettre N pour signifier *"est non-résidu quadratique de"*.

page 111, article 148 : *Premier cas.* Quand A est de la forme $4n+1$ ou $-(4n-1)$. On résoudra A en facteurs premiers a, b, c, d, *etc.*, en affectant du signe + ceux de la forme $4n+1$, et du signe − ceux de la forme $4n-1$ qui seront en nombre pair ou impair, suivant que A sera de la forme $4n+1$ ou $-(4n-1)$ (n^o 132). On distribuera en deux classes les nombres plus petits que A et premiers avec lui ; en mettant dans la première ceux qui ne sont non-résidus d'aucun diviseur de A, ou qui sont non-résidus d'un nombre pair de ces diviseurs, et dans la seconde ceux qui sont non-résidus d'un nombre impair des mêmes diviseurs. Désignons les premiers par r, r', r'', *etc.* et les seconds par n, n', n'', *etc.* ; alors $Ak+r$, $Ak+r'$, *etc.* sont les formes des diviseurs de x^2-A, et $Ak+n$, $Ak+n'$, *etc.* celles des non-diviseurs. C'est-à-dire que tout nombre premier, excepté 2, sera diviseur ou non-diviseur de x^2-A, suivant qu'il sera contenu dans l'une des premières ou l'une des dernières formes.
En effet, si p est un nombre premier résidu ou non-résidu d'un des facteurs de A, ce facteur sera résidu ou non-résidu de p (théor. fond.) ; donc si parmi les facteurs de A, il y en a m dont p soit non-résidu, il y en aura autant qui seront non-résidus de p, et partant, lorsque p sera contenu dans l'une des premières formes, m sera pair et ARp, et lorsque p sera contenu dans une des dernières, p sera impair et ANp.
Exemple. Soit $A=+105=(-3)\times(+5)\times(-7)$[16] ;
les nombres r, r', r'', *etc.* sont :
1, 4, 16, 46, 64, 79, qui ne sont non-résidus d'aucun facteur. ;
2, 8, 23, 32, 53, 92, qui sont non-résidus de 3 et 5 ;
26, 41, 59, 89, 101, 104, ... 3 et 7 ;
23, 52, 73, 82, 97, 103, ... 5 et 7 ;
les nombres n, n', n'', *etc.* sont :
11, 29, 44, 71, 74, 86, non-résidus de 3 ;
22, 37, 43, 58, 67, 88, ... de 5 ;
19, 31, 34, 61, 76, 94, ... de 7 ;
17, 38, 47, 62, 68, 83, ... de 3, 5 et 7 ;
On déduit facilement de la théorie des combinaisons et des $n^{os}(32,96)$ que la multitude des nombres r, r', *etc.* sera

$$t\Big(1+\frac{l(l-1)}{1.2}+\frac{l(l-1)(l-2)(l-3)}{1.2.3.4}+etc.\Big)$$

et celle des nombres n, n', *etc.*

$$t\Big(l+\frac{l(l-1)(l-2)}{1.2.3}+\frac{l(l-1)(l-2)(l-3)(l-4)}{1.2.3.4.5}+etc.\Big)$$

l désignant le nombre des facteurs a, b, c, d, *etc.*, t étant
$=2^{-l}(a-1)(b-1)(c-1)etc.$, et chaque série devant être continuée jusqu'à ce qu'elle s'arrête d'elle-même. (En effet il y a t nombres résidus de a, b, c, d, *etc.*, $t.\frac{l.(l-1)}{1.2}$ non-résidus de deux de ces facteurs, etc. Mais pour abréger, nous sommes forcés de ne pas donner plus de développement à la démonstration). Or chacune des séries a pour somme $l.2^{l-1}$; car la première provient de
$1+\frac{l-1}{1}+\frac{(l-1)(l-2)}{1.2}+\frac{(l-1)(l-2)(l-3)}{1.2.3}+etc.$ en prenant le premier terme, puis la somme du second et du troisième, puis la somme du quatrième et du cinquième, etc. : la seconde provient aussi de la même série, en joignant le premier terme au second, le troisième au quatrième, etc. Il y a donc autant de formes de diviseurs de x^2-A, que de formes de non-diviseurs ; et ils sont en nombre $2^{l-1}.t$ de chaque espèce, ou $\frac{1}{2}(a-1)(b-1)(c-1)(d-1)etc.$

page 113, article 149 : Nous pouvons traiter ensemble le second et le troisième cas. En effet on pourra toujours poser $A=(-1)Q$, ou $=(+2)Q$, ou $=(-2)Q$, Q étant un nombre de la forme $4n+1$ ou $-(4n-1)$. Soit généralement $A=\alpha Q$, de sorte que α soit ou -1 ou ± 2. Alors A sera résidu de tout nombre dont α et Q seront tous deux résidus, ou tous deux non-résidus : au contraire il sera non-résidu de tout nombre dont l'un d'eux seulement sera non-résidu. De là on déduit sans peine les formes des diviseurs et des non-diviseurs de x^2-A. Si $\alpha=-1$; nous partagerons tous les nombres plus petits que $4A$ et premiers avec lui, en deux classes. La première renfermera ceux qui sont dans quelque forme des diviseurs de x^2-Q, et en même temps de la forme $4n+1$, et aussi ceux qui sont dans quelque forme des non-diviseurs de x^2-Q et en même temps de la forme $4n-1$: la seconde renfermera tous les autres. Soient r, r', r'', *etc.* les premiers et n, n', n'', *etc.* les derniers ; A sera résidu de tous les nombres premiers contenus dans une

[16] Cela peut surprendre d'utiliser ainsi des nombres négatifs dans la factorisation mais Gauss explique qu'il affecte systématiquement les nombres premiers de la forme $4n+3$ du signe − et ceux de la forme $4n+1$ du signe + à cause de leur comportement démontré par le théorème fondamental.

des formes $4Ak+r$, $4Ak+r'$, $4Ak+r''$, *etc.*, et non-résidu de tous les nombres premiers contenus dans une des formes $4Ak+n$, $4Ak+n'$, $4Ak+n''$, *etc.* Si $\alpha = \pm 2$, nous distribuerons tous les nombres plus petits que $8Q$ et premiers avec lui en deux classes : la première renfermera tous ceux qui sont contenus dans quelque forme des diviseurs de $x^2 - Q$, et qui sont de la forme $8n+1$ ou $8n+7$, pour le signe supérieur, et de la forme $8n+1$ ou $8n+3$ pour le signe inférieur ; cette classe comprendra aussi tous ceux qui sont contenus dans quelque forme de non-diviseurs de $x^2 - Q$ et qui sont, pour le signe supérieur, de la forme $8n+3$, $8n+5$, et pour le signe inférieur, de la forme $8n+5$, $8n+7$, et la seconde tous les autres. Alors désignant les nombres de la première classe par r, r', r'', *etc.*, ceux de la seconde par n, n', n'', *etc.*, $\pm 2Q$ sera résidu de tous les nombres premiers contenus dans les formes $8Qk+r$, $8Qk+r'$, $8Qk+r''$, *etc.* et non-résidu de tous ceux contenus dans les formes $8Qk+n$, $8Qk+n'$, $8Qk+n''$, *etc.* Au reste, on peut démontrer facilement qu'il y a autant de formes de diviseurs qu'il y en a de non-diviseurs.
Exemple. On trouve ainsi que 10 est résidu de tous les nombres premiers contenus dans les formes $40K+1$, $+3$, $+9$, $+13$, $+27$, $+31$, $+37$, $+39$, et non-résidu de tous les nombres premiers contenus dans les formes $40K+7$, $+11$, $+17$, $+19$, $+21$, $+23$, $+29$, $+33$.

page 114, article 150 : Ces formes ont plusieurs propriétés assez remarquables ; nous n'en citerons cependant qu'une seule. Si B est un nombre composé premier avec A, tel qu'un nombre $2m$ de ses facteurs premiers soient compris dans quelque forme de non-diviseurs de $x^2 - A$, B sera contenu dans quelque forme de diviseurs de $x^2 - A$; mais si le nombre de facteurs premiers de B contenus dans quelque forme de non-diviseurs de $x^2 - A$ est impair, B sera aussi contenu dans quelque forme de non-diviseurs. Nous omettons la démonstration, qui n'a rien de difficile[17]. Il suit de là que non-seulement tout nombre premier ; mais aussi tout nombre composé impair et premier avec A est non-diviseur dès qu'il est contenu dans une des formes de non-diviseur ; car nécessairement quelque facteur premier de ce nombre sera non-diviseur.

page 116, article 152 : Jusqu'à présent nous n'avons traité que la congruence simple $x^2 \equiv A (mod\ m)$, et nous avons appris à reconnaître les cas où elle est résoluble. Par le n^o 105, la recherche des racines elles-mêmes est ramenée au cas où m est un nombre premier, ou une puissance d'un nombre premier ; et par le n^o 101, ce dernier cas est ramené à celui où m est un nombre premier. Quant à celui-ci, en comparant ce que nous avons dit (n^{os} 61 et suiv.) avec ce que nous enseignerons sect. V et VIII, on aura presque tout ce qui peut se faire par les méthodes générales. Mais dans les cas où elles sont applicables, elles sont infiniment plus longues que les méthodes indirectes que nous exposerons dans la section VI, et partant elles sont moins remarquables par leur utilité dans la pratique que par leur beauté.

Annexe 3 : Deux extraits de la lettre de Carl Frédéric Gauss à Sophie Germain du 30 avril 1807 (extrait des Oeuvres philosophiques de Sophie Germain, 1879, p. 274-282)

Voici une autre proposition relative aux residus quarrés, dont la demonstration est moins cachée : je ne l'ajoute pas, pour ne pas vous derober le plaisir de la developper vous-même, si vous la trouverez digne d'occuper quelques moments de votre loisir.
Soit p un nombre premier. Soient les $p-1$ nombres inférieurs à p partagés en deux classes :
A.....$1, 2, 3, 4....\frac{1}{2}(p-1)$
B.....$\frac{1}{2}(p+1), \frac{1}{2}(p+3), \frac{1}{2}(p+5), ...p-1$ Soit a un nombre quelconque non divisible par p. Multipliés tous les nombres A par a; prenés-en les moindres residus selon le module p, soient, entre ces residus, α appartenants à A, et β appartenants à B, de sorte que $\alpha + \beta = \frac{1}{2}(p-1)$. Je dis que a è residu quarré de p lorsque β è pair, non residu lorsque β è impair.

Le second extrait est davantage *"connu"*

Le goût pour les sciences abstraites en général et surtoût pour les mysteres des nombres est fort rare : on ne s'en étonne pas ; les charmes enchanteurs de cette sublime science ne se decelent dans toute leur

[17] On suppose donc que Gauss l'a faite, dans une quelconque marge...

beauté qu'à ceux qui ont le courage de l'approfondir. Mais lorsqu'une personne de ce sexe, qui, par nos moeurs et par nos préjugés, doit rencontrer infiniment plus d'obstacles et de difficultés, que les hommes, à se familiariser avec ces recherches epineuses, sait neansmoins franchir ces entraves et penétrer ce qu'elles ont de plus caché, il faut sans doute, qu'elle ait le plus noble courage, des talens tout à fait extraordinaires, le génie supérieur. En effet, rien ne pourroit me prouver d'une manière plus flatteuse et moins équivoque, que les attraits de cette science, qui ont embelli ma vie de tant de jouissances, ne sont pas chimériques, que la predilection, dont vous l'avez honorée.

Annexe 4 : un nombre premier non-résidu de tous les diviseurs impairs des nombres pairs n de la deuxième catégorie fournit une décomposition de Goldbach

20, diviseur 5, 3N5, 3+17
28, diviseur 7, 5N7, 5+23
30, diviseurs 3 et 5, 17N3, 17N5, 17+13
40, diviseur 5, 3N5, 3+37
42, diviseurs 3 et 7, 5N3, 5N7, 5+37
44, diviseur 11, 7N11, 7+37
48, diviseur 3, 5N3, 5+43
50, diviseur 5, 3N5, 3+47
56, diviseur 7, 3N7, 3+47
60, diviseurs 3 et 5, 17N3, 17N5, 17+43
66, diviseurs 3 et 11, 29N3, 29N11, 29+47
68, diviseur 17, 7N17, 7+61
72, diviseur 3, 5N3, 5+67
78, diviseurs 3 et 13, 5N3, 5N13, 5+73
80, diviseur 5, 7N5, 7+73
84, diviseurs 3 et 7, 5N3, 5N7, 5+79
88, diviseur 11, 17N11, 17+71
90, diviseurs 3 et 5, 17N3, 17N5, 17+73
92, diviseur 23, 19N23, 19+73
96, diviseur 3, 17N3, 17+79
98, diviseur 7, 19N7, 19+79

Annexe 5 : Illlustrations du théorème fondamental pour les modules impairs

Pour les modules impairs, des relations existent entre le caractère résidu/non-résidu de x à m et de $x + \frac{p+1}{2}$ à m. Les tables ci-dessous illustrent le fait qu'elles sont assez difficiles à trouver. Par exemple, sur les tables associées aux modules 15 et 75, on voit qu'il y a anti-symétrie entre x et $x + \frac{p+1}{2}$ quand ce sont tous deux des $4n+2$ ou des $4n$ et symétrie quand ce sont tous deux des $4n+1$ ou des $4n+3$.

Comme on s'intéresse à la conjecture de Goldbach, on axera plutôt les recherches sur les modules pairs.

5.1 : Illustrations du théorème fondamental pour les modules impairs puissances de nombres premiers impairs

Selon le module 9, de la forme $(4n+3)^2$:

9	8	7	6	5
0	1	2	3	4
0	1	4	0	7

Selon le module 27, de la forme $(4n+3)^3$:

27	26	25	24	23	22	21	20	19	18	17	16	15	14
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	1	4	9	16	25	9	22	10	0	19	13	9	7

Selon le module 25, de la forme $(4n+1)^2$:

25	24	23	22	21	20	19	18	17	16	15	14	13
0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	4	9	16	0	11	24	14	6	0	2	19

5.2 : Illustrations du théorème fondamental pour les modules impairs produits de nombres premiers impairs

Selon le module 15, de la forme $(4n+3)(4n+1)$:

15	14	13	12	11	10	9	8
0	1	2	3	4	5	6	7
0	1	4	9	1	10	6	4

Selon le module 45, de la forme $(4n+3)^2(4n+1)$:

45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
0	1	4	9	16	25	36	4	19	36	10	31	9	34	16	0	31	19	9	1	40	36	34

Selon le module 75, de la forme $(4n+3)(4n+1)^2$:

75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	1	4	9	16	25	36	49	64	6	25	46	69	19	21	0	31	64	24

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
61	25	66	34	4	51	25	1	54	34	16	0	61	49	39	31	25	21	19

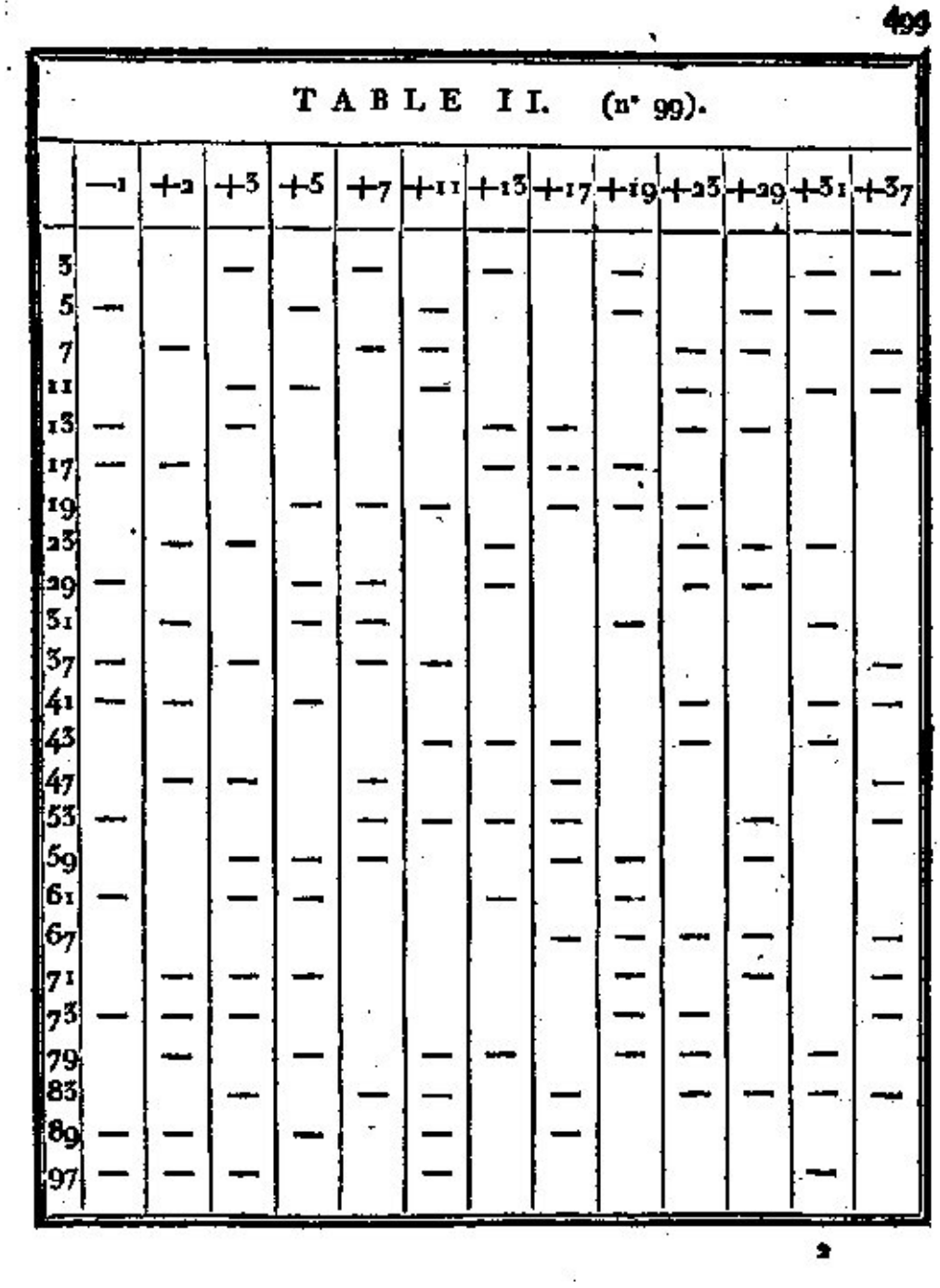
Annexe 6 : L'orthographe des Recherches Arithmétiques

Ici, on recense quelques différences orthographiques par rapport à l'orthographe actuelle :

- quarré, soumultiple, alongeraient
- différens, précédens, quotiens, coefficiens, suivans, élégans
- parceque, parconséquent, ensorte que
- entr'eux, long-temps

Annexe 7 : La table II des Recherches Arithmétiques

La table que nous avons fournie est une inversion lignes-colonnes de la table de Gauss.

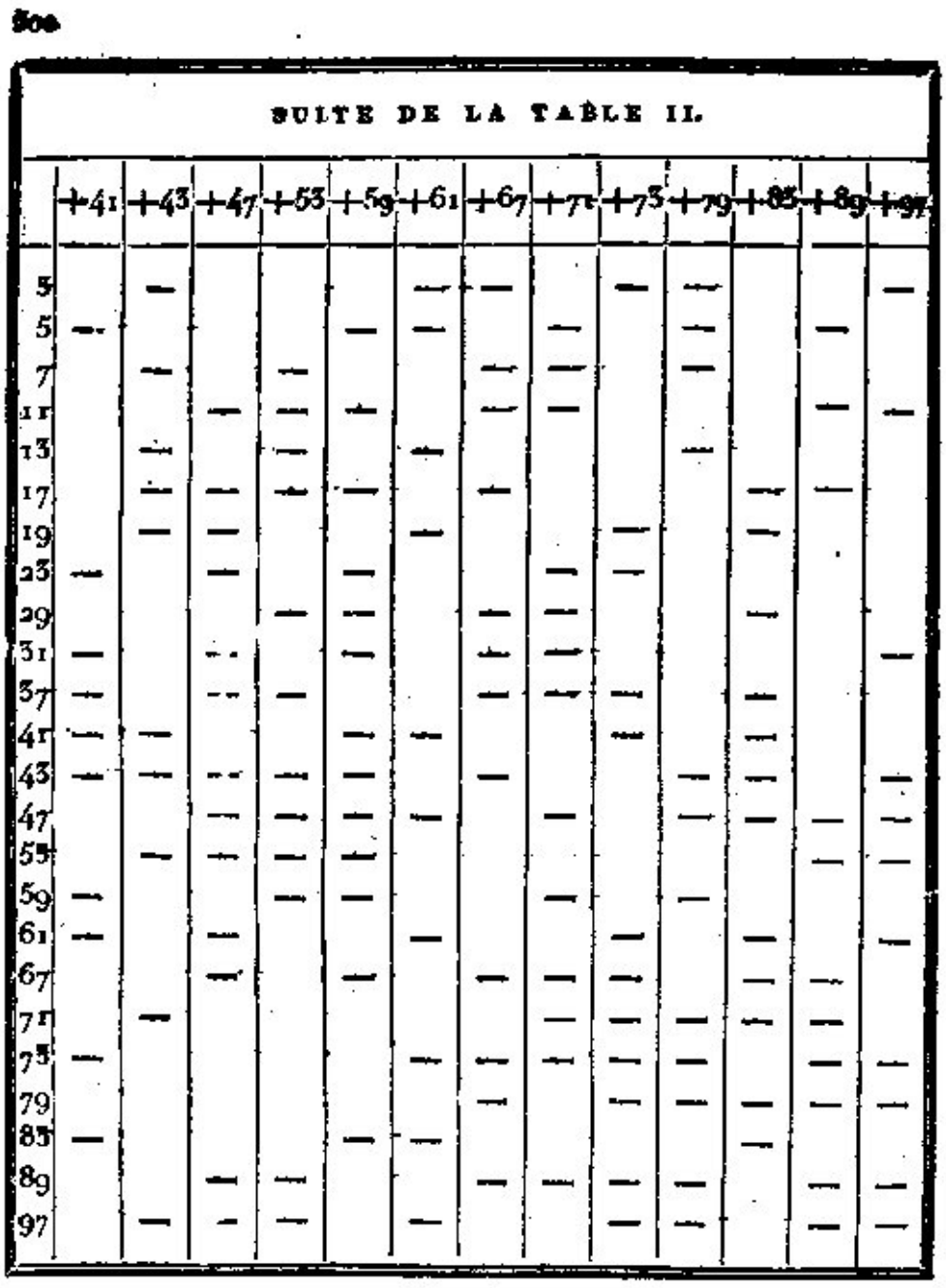


499

TABLE II. (n° 99).

	−1	+2	+3	+5	+7	+11	+13	+17	+19	+23	+29	+31	+37
3			−		−		−		−			−	−
5	−			−		−			−		−	−	
7		−			−	−				−	−		−
11			−	−		−				−		−	−
13	−		−				−	−		−	−		
17	−	−					−	−	−				
19				−	−	−		−	−	−			
23		−	−				−			−	−	−	
29	−			−	−		−			−	−		
31		−		−	−				−			−	
37	−		−		−	−							−
41	−	−		−						−		−	−
43						−	−	−		−		−	
47		−	−		−			−					−
53	−				−	−	−	−			−		−
59			−	−	−			−	−		−		
61	−		−	−			−		−				
67								−	−	−	−		−
71		−	−	−					−		−		−
73	−	−	−						−	−			−
79		−		−		−	−		−	−		−	
83			−		−	−		−		−	−	−	−
89	−	−		−		−		−					
97	−	−	−			−						−	

2



Annexe 8 : Initiale G

Goldbach, Gauss, Germain, Galois, Godel, Grothendieck...

Bibliographie

[1] **C. F. Gauss**, *Recherches Arithmétiques*, Editions Jacques Gabay, 1801.

[2] **G. Cantor**, *Vérification jusqu'à 1000 du théorème empirique de Goldbach*, Congrès de Caen de l'A.F.A.S. (Association Française pour l'Avancement des Sciences) du 10 août 1894, p.117 à 134.

[3] **A.-M. Décaillot**, *Cantor et la France*, Ed. Kimé, 2008.