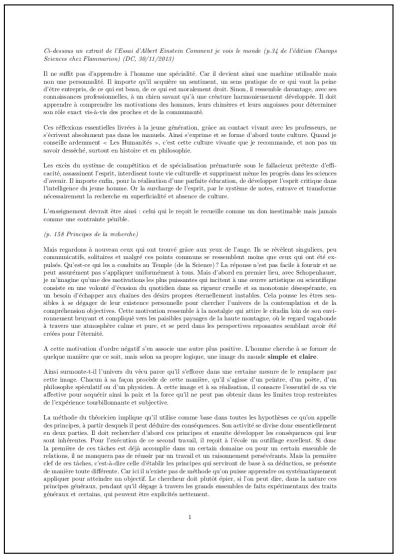
Le texte ci-dessous est le fichier https://denisevellachemla.eu/notesnp.html au format pdf
Denise Vella-Chemla, août 2025

J'étudie la conjecture depuis septembre 2005. Ci-dessous, les pistes suivies de septembre 2005 à septembre 2011 [1].

- Physique et philosophie (3.10.2011)



Ci-dessous un extrait de l'Essai d'Albert Einstein Comment je vois le monde (p.24 de l'édition Champs Sciences chez Flammarion) (DC, 30/11/2011)

Il ne suffit pas d'apprendre à l'homme une spécialité. Car il devient ainsi une machine utilisable mais non une personnalité. Il importe qu'il acquière un sentiment, un sens pratique de ce qui vaut la peine d'être entrepris, de ce qui est beau, de ce qui est moralement droit. Sinon, il ressemble davantage, avec ses connaissances professionnelles, à un chien savant qu'à une créature harmonieusement développée. Il doit apprendre à comprendre les motivations des hommes, leurs chimères et leurs angoisses pour déterminer son rôle exact vis-à-vis des proches et de la communauté.

Ces réflexions essentielles livrées à la jeune génération, grâce au contact vivant avec les professeurs, ne s'écrivent absolument pas dans les manuels. Ainsi s'exprime et se forme d'abord toute culture. Quand je conseille ardemment « Les Humanités », c'est cette culture vivante que je recommande, et non pas un savoir desséché, surtout en histoire et en philosophie.

Les excès du système de compétition et de spécialisation prématurée sous le fallacieux prétexte d'efficacité, assassinent l'esprit, interdisent toute vie culturelle et suppriment même les progrès dans les sciences d'avenir. Il importe enfin, pour la réalisation d'une parfaite éducation, de développer l'esprit critique dans l'intelligence du jeune homme. Or la surcharge de l'esprit, par le système de notes, entrave et transforme nécessairement la recherche en superficialité et absence de culture.

L'enseignement devrait être ainsi : celui qui le reçoit le recueille comme un don inestimable mais jamais comme une contrainte pénible.

(p. 158 Principes de la recherche)

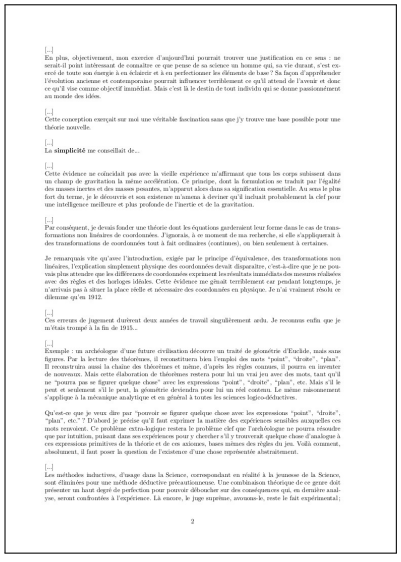
Mais regardons à nouveau ceux qui ont trouvé grâce aux yeux de l'ange. Ils se révèlent singuliers, peu communicatifs, solitaires et malgré ces points communs se ressemblent moins que ceux qui ont été exclus. Qu'est-ce qui les a conduits au Temple (de la Science) ? La réponse n'est pas facile à fournir et ne peut assurément pas s'appliquer uniformément à tous. Mais d'abord en premier lieu, avec Schopenhauer, je m'imagine qu'une des motivations les plus puissantes qui incitent à une oeuvre artistique ou scientifique consiste en une volonté d'évasion du quotidien dans sa rigueur cruelle et sa monotonie désespérante, en un besoin d'échapper aux chaînes des désirs propres éternellement instables. Cela pousse les êtres sensibles à se dégager de leur existence personnelle pour chercher l'univers de la contemplation et de la compréhension objectives. Cette motivation ressemble à la nostalgie qui attire le citadin loin de son environnement bruyant et compliqué vers les paisibles paysages de la haute montagne, où le regard vagabonde à travers une atmosphère calme et pure, et se perd dans les perspectives reposantes semblant avoir été créées pour l'éternité.

A cette motivation d'ordre négatif s'en associe une autre plus positive. L'homme cherche à se former de quelque manière que ce soit, mais selon sa propre logique, une image du monde **simple et claire**.

Ainsi surmonte-t-il l'univers du vécu parce qu'il s'efforce dans une certaine mesure de le remplacer par cette image. Chacun à sa façon procède de cette manière, qu'il s'agisse d'un peintre, d'un poète, d'un philosophe spéculatif ou d'un physicien. A cette image et à sa réalisation, il consacre l'essentiel de sa vie affective pour acquérir ainsi la paix et la force qu'il ne peut pas obtenir dans les limites trop restreintes de l'expérience tourbillonnante et subjective.

La méthode du théoricien implique qu'il utilise comme base dans toutes les hypothèses ce qu'on appelle des principes, à partir desquels il peut déduire des conséquences. Son activité se divise donc essentiellement en deux parties. Il doit rechercher d'abord ces principes et ensuite développer les conséquences qui leur sont inhérentes. Pour l'exécution de ce second travail, il reçoit à l'école un outillage excellent. Si donc la première de ces tâches est déjà accomplie dans un certain domaine ou pour un certain ensemble de relations, il ne manquera pas de réussir par un travail et un raisonnement persévérants. Mais la première clef de ces tâches, c'est-à-dire celle d'établir les principes qui serviront de base à sa déduction, se présente de manière toute différente. Car ici il n'existe pas de méthode qu'on puisse apprendre ou systématiquement appliquer pour atteindre un objectif. Le chercheur doit plutôt épier, si l'on peut dire, dans la nature ces principes généraux, pendant qu'il dégage à travers les grands ensembles de faits expérimentaux des traits généraux et certains, qui peuvent être explicités nettement.

1



[...]
En plus, objectivement, mon exercice d'aujourd'hui pourrait trouver une justification en ce sens : ne serait-il point intéressant de connaître ce que pense de sa science un homme qui, sa vie durant, s'est exercé de toute son énergie à en éclaircir et à en perfectionner les éléments de base ? Sa façon d'appréhender l'évolution ancienne et contemporaine pourrait influencer terriblement ce qu'il attend de l'avenir et donc ce qu'il vise comme objectif immédiat. Mais c'est là le destin de tout individu qui se donne passionnément au monde des idées.

[...]
Cette conception exerçait sur moi une véritable fascination sans que j'y trouve une base possible pour une théorie nouvelle.

[...]
La **simplicité** me conseillait de...

[...]
Cette évidence ne coïncidait pas avec la vieille expérience m'affirmant que tous les corps subissent dans un champ de gravitation la même accélération. Ce principe, dont la formulation se traduit par l'égalité des masses inertes et des masses pesantes, m'apparut alors dans sa signification essentielle. Au sens le plus fort du terme, je le découvris et son existence m'amena à devenir qu'il incitait probablement la clef pour une intelligence meilleure et plus profonde de l'inertie et de la gravitation.

[...]
Par *conséquent*, je devais fonder une théorie dont les équations garderaient leur forme dans le cas de transformations non linéaires de coordonnées. J'ignorais, à ce moment de ma recherche, si elle s'appliquerait à des transformations de coordonnées tout à fait ordinaires (continues), ou bien seulement à certaines.

Je remarquais vite qu'avec l'introduction, exigée par le principe d'équivalence, des transformations non linéaires, l'explication simplement physique des coordonnées devait disparaître, c'est-à-dire que je ne pouvais plus attendre que les différences de coordonnées expriment les résultats immédiats des mesures réalisées avec des règles et des horloges idéales. Cette évidence me gênait terriblement car pendant longtemps, je n'arrivais pas à situer la place réelle et nécessaire des coordonnées en physique. Je n'ai vraiment résolu ce dilemme qu'en 1912.

[...]
Ces erreurs de jugement durèrent deux années de travail singulièrement arduˆ. Je reconnus enfin que je m'étais trompé à la fin de 1915...

[...]
Exemple : un archéologue d'une future civilisation découvre un traité de géométrie d'Euclide, mais sans figures. Par la lecture des théorèmes, il reconstituera bien l'emploi des mots "point", "droite", "plan". Il reconnaîtra aussi la chaîne des théorèmes et même, d'après les règles connues, il pourra en inventer de nouveaux. Mais cette élaboration de théorèmes restera pour lui un vrai jeu avec des mots, tant qu'il ne "pourra pas se figurer quelque chose" avec les expressions "point", "droite", "plan", etc. Mais s'il le peut et seulement s'il le peut, la géométrie deviendra pour lui un réel contenu. Le même raisonnement s'applique à la mécanique analytique et en général à toutes les sciences logico-déductives.

Qu'est-ce que je veux dire par "pouvoir se figurer quelque chose avec les expressions "point", "droite", "plan", etc."? D'abord je pense qu'il faut exprimer la matière des expériences sensibles auxquelles ces mots renvoient. Ce problème extra-logique restera le problème clef que l'archéologue ne pourra résoudre que par intuition, puisant dans ses expériences pour y chercher s'il y trouverait quelque chose d'analogue à ces expressions primitives de la théorie et de ces axiomes, bases mêmes des règles du jeu. Voilà comment, absolument, il faut poser la question de l'existence d'une chose représentable abstraitement.

[...]
Les méthodes inductives, d'usage dans la Science, correspondant en réalité à la jeunesse de la Science, sont éliminées pour une méthode déductive préconitionneuse. Une combinaison théorique de ce genre doit présenter un haut degré de perfection pour pouvoir déboucher sur des conséquences qui, en dernière analyse, seront confrontées à l'expérience. Là encore, le juge suprême, avouons-le, reste le fait expérimental;

2

[1] On peut cliquer sur les images pour les agrandir, et sur les liens pour lire les notes correspondantes

mais la reconnaissance par le fait expérimental évalue aussi le travail terriblement long et complexe et souligne les ponts établis entre les immenses conséquences vérifiables et les axiomes qui les ont permis. Le théoricien doit entendre ce travail de Titan avec la claire certitude qu'il n'a d'autre ambition de préparer peut-être l'assommoir de sa propre théorie. On ne doit jamais critiquer le théoricien quand il entreprend un tel travail et le taxer de fantaisiste. Il faut estimer cette fantaisie. Car elle représente pour lui le seul itinéraire qui mène au but. Assurément il ne s'agit pas d'une plaisanterie, mais d'une patiente recherche en vue des possibilités **logiquement les plus simples**, et en vue de leurs conséquences.

[...]
Aussi Kepler devait-il avoir une singulière conviction en ces lois pour qu'il puisse, des dizaines d'années durant, y consacrer toutes ses forces par un travail obstiné et supérieurement compliqué.

[...]
Il est seul. Nul ne le soutient ni ne le comprend.

[...]
Mais Newton veut répondre à la question précise : existe-t-il **une règle simple** ?

[...]
Ces lois concernent le mouvement en tant qu'ensemble. Elles ne répondent pas à la question : "Comment de l'état de mouvement d'un système découle le mouvement qui lui succède immédiatement dans la durée ?".

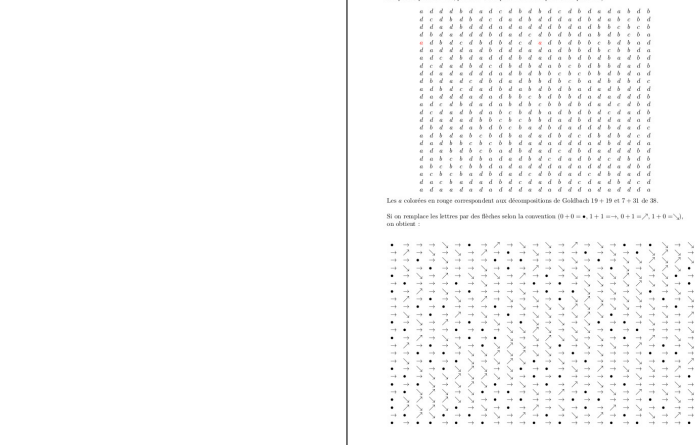
[...]
L'effort vers la connaissance, par sa nature propre, nous pousse en même temps à l'intelligence de l'extrême variété de l'expérience et à la maîtrise de la **simplicité** économique des hypothèses fondamentales. L'accord final de ces objectifs représente dans le premier moment de nos recherches un acte de foi. Sans cette foi, la conviction de la valeur indépendante de la connaissance n'existerait pas, collectée et indestructible.

Cette attitude profondément religieuse de l'homme scientifique face à la vérité rejaillit sur toute sa personnalité. En effet, en deux domaines les résultats de l'expérience et les lois de la pensée commandent par eux-mêmes. Et donc le chercheur, en principe, ne se fonde sur aucune autorité dont les décisions ou les communications pourraient prétendre à la vérité. D'où le violent paradoxe suivant : un homme livre toute son énergie à des expériences objectives et il se transforme, dès qu'on l'envisage en sa fonction sociale, en un individualiste extrême qui, théoriquement du moins, ne se fierait qu'à son propre jugement. On pourrait presque dire que l'individualisme intellectuel et la recherche scientifique naissent ensemble historiquement, et que depuis ils ne se séparent plus.

Or l'homme scientifique présenté ainsi, qu'est-il d'autre qu'une simple abstraction, invisible dans le monde réel, mais comparable à l'*homme économique* de l'économie classique ? Or, dans la réalité, la science concrète, celle de notre quotidien, ne se serait jamais créée et maintenue vivace si cet homme de science n'était apparu, au moins dans ses grandes lignes, dans un grand nombre d'individus et pendant de longs siècles.

Évidemment, je ne considère pas automatiquement comme un homme scientifique celui qui sait se servir d'instruments et de méthodes jugés scientifiques. Je ne pense qu'à ceux dont l'esprit se révèle vraiment scientifique.

On fournit ici une représentation de ce que l'on pourrait appeler l'" espace de Goldbach" qui représente les décompositions des nombres en sommes de deux entiers selon la convention choisie (*premier+premier = a, composé + premier = b, premier + composé = c* et *composé + composé = d*).



Les *a* colorés en rouge correspondent aux décompositions de Goldbach 19 = 19 et 7 = 31 de 38.

Si on remplace les lettres par des flèches selon la convention ($0+0=$●, $1+1=\searrow$, $0+1=\nearrow$, $1+0=\searrow$), on obtient :

Extraits de *Et si le temps n'existait pas ?* de Carlo Rovelli (DC 24/11/13)

(p. 13) Enfant, je lisais les fables d'un écrivain italien pour enfants, Gianni Rodari. L'une d'elles raconte l'histoire de Giovannino et de la route qui ne mène nulle part. Giovannino vivait dans un village où il y avait une route qui, d'après tout le monde, ne menait nulle part. Mais Giovannino était curieux et têtu et, malgré ce que tout le monde disait, il voulait aller voir. Il y alla, et bien sûr il trouva un château et une princesse, qui le couvrit de pierres précieuses. Quand il rentra au village, ainsi naanti, tout le monde se précipita sur la route, mais personne n'y trouva plus le matudre trésor.

J'ai lu cet extrait jeudi soir ; le matin-même, avec les élèves de CE1 que j'ai en classe, nous avions lu dans leur manuel de lecture une autre histoire de Gianni Rodari, celle de l'enfant qui posait ses questions à l'envers "Pourquoi les tiroirs ont-ils des tables ?".

(p. 67 et 68) La vieille idée aristotélicienne et cartésienne voit l'espace comme relation.

Une théorie complète de la gravitation quantique ne sera probablement construite qu'en abandonnant complètement l'idée nectonienne de l'espace comme entité. L'espace n'est pas une entité dans laquelle les objets sont localisés : l'entité "espace" n'existe pas. [...] Ce sont les relations qui constituent l'espace.

La base même de la science est donc la pensée critique : la conscience forte que nos visions du monde sont toujours partielles, subjectives, imprécises, provisoires et simplistes. Il faut sans cesse chercher à comprendre mieux. À ouvrir des horizons. À trouver un point de vue plus large. Cela n'est ni ecommode ni naturel car, d'une certaine façon, nous sommes prisonniers de nos pensées. Il est par définition impossible de sortir de notre propre pensée. On ne peut pas la regarder du dehors et la modifier. C'est de l'intérieur de nos erreurs qu'il faut travailler pour découvrir où nous sommes en train de nous tromper. Cela revient, pour utiliser une belle et célèbre image, à reconstruire son bateau tout en naviguant. La science, c'est cela : un effort continu pour reconstruire et restructurer notre propre pensée alors même que nous sommes en train de penser.

(p. 81 et 82) Dès mon arrivée, Wheeler est venu me voir dans le Bed and breakfast où j'avais trouvé à me loger. Nous avons pris le petit-déjeuner ensemble et puis il m'a accompagné dans une longue promenade à travers le campus. Je lui ai expliqué les résultats de nos calculs, tandis que lui me racontait ses histoires extraordinaires : Bohr, la bombe atomique... "Tu vois, Carlo, me disait-il, quand Einstein est arrivé ici la première fois, fuyant l'Allemagne nazie, je suis allé le chercher au petit matin, comme je viens de le faire avec toi, et nous nous sommes promenés le long du même parcours..." Pourquoi le vieillissage, même indirect, des hommes qui ont laissé le plus de traces dans notre pensée nous donne-t-il tant d'émotion ? Ce sont des hommes comme les autres, bien sûr, avec leurs faiblesses et leur humanité comme tout le monde, mais la fascination que nous avons éprouvée pour leurs idées leur confère une aura qui nous enchante. Ils nous ont ouvert des chemins que nous avons le privilège de pouvoir suivre, et de ce fait éveillent admiration, gratitude et affection.

(p. 94 et 95) Revenons-en aux principes. Ce qu'il faut comprendre pour commencer, c'est que lorsque deux *événements* se découlent en des endroits suffisamment éloignés, il n'y a pas de sens, en général, à dire lequel des deux arrive *le premier*. Et il n'y a pas de sens non plus à demander ce qui arrive en *ce moment précis* dans la galaxie d'Andromède, par exemple. La raison en est que le temps ne s'écoule pas partout de la même manière. Nous avons notre temps, et la galaxie d'Andromède a le sien, et de manière générale ces deux temps ne peuvent pas être mis en relation.

La seule chose qu'on puisse faire, c'est échanger des signaux, mais ceux-ci vont prendre des millions d'années pour faire l'aller-retour entre ici et Andromède. Imaginez un extra-terrestre qui nous envoie un signal depuis Andromède. Nous recevons ce message *aujourd'hui* et nous y répondons immédiatement. Nous pouvons dire que le moment où l'extra-terrestre a envoyé le signal se place *avant* aujourd'hui, et que le moment où il recevra la réponse viendra *après* aujourd'hui. Mais pendant les millions d'années qui s'écoulent entre l'envoi du signal par l'extra-terrestre et sa réception de notre réponse, il n'existe pas de moment particulier sur Andromède qui corresponde à cet "aujourd'hui" sur la Terre.

Tout cela pour dire que nous ne devons pas penser au temps comme s'il existait une horloge cosmique rythmant la vie de l'univers. Nous devons y penser comme à quelque chose de local : chaque objet dans l'univers possède son propre temps. La façon dont les temps de chacun s'articulent lorsque des objets se


rencontrent ou échangent des signaux peut être décrite précisément. Mais pour le faire, dans la description mathématique du monde, on ne parle pas de "temps" et d'"espace", mais d'une union des deux appelée "espace-temps".

(p. 106) Quand un scientifique formule une idée, il tend généralement à croire qu'elle est correcte. Si personne d'autre n'approuve, il continuera souvent à croire qu'il a raison et que les autres ont tort... mais il aura quelques doutes. S'il découvre que quelqu'un d'autre a trouvé la même idée indépendamment de lui, la tentation de croire que "nous" avons raison et que les autres "ne comprennent rien" devient irrésistible...

2

Ci-dessous un extrait d'une conférence de Serge Haroche "La physique quantique" à l'Université de tous les savoirs en 2000 (DV, 16/2/2014)

Lien vers la conférence :
http ://www.canal-u.tv/video/universite$_d$e$_t$ous$_l$es$_s$avoirs/la$_p$hysique$_q$uantique$_s$erge$_h$aroche.1065

En raison des imperfections de la cavité, d'une certaine rugosité du miroir, de temps en temps, un photon va s'échapper, et partir dans l'environnement. Dès que le photon est parti, c'en est fini de la cohérence quantique. Le premier photon qui s'échappe sert d'espion pour vous dire que vous êtes dans un chemin et pas dans l'autre. Le temps que le premier photon va mettre à disparaître est extrêmement court. Si vous avez un milliard de photons et un temps de relaxation d'une milliseconde, il vous faudra un milliardième de millisecondes pour que le premier photon s'échappe et la cohérence quantique aura disparu. On comprend que les cohérences macroscopiques disparaissent très très vite pour des champs macroscopiques et on ne peut faire des expériences que si n n'est pas trop grand. On a fait une telle expérience qui "saisit la décohérence au vol". Les cohérences quantiques sont extrêmement fragiles, elles s'évanouissent dès qu'un quantum s'est perdu dans l'environnement.

A relier à ceci, paru le 27 janvier 2014 :
http ://www2.cnrs.fr/presse/communique/3415.htm

Il a pris de mes nouvelles à distance depuis Helsinki et Vordingborg. A chaque fois qu'il le fait, mon cerveau se met en mouvement, c'est un bon catalyseur. Il a bien compris que je suis une sorte de particule quantique : mon état est complètement modifié quand on m'observe, je ne suis bien que là où je ne suis pas et je lui sais gré d'essayer de me perturber le moins possible.

En ce moment, c'est très difficile d'avancer, j'aimerais pouvoir m'isoler mais il y a trop de sollicitations. J'ai décidé que moi aussi, j'aurai une exigence : je chercherai une idée qui appartienne à mon domaine : bits, données, instructions, programmes, invariant, preuve. C'était nul d'aller fouiller leurs plates-bandes, elles sont si foisonnantes, si compliquées, je ne vois pas leur lumière, j'ai besoin de simplicité.

J'aimerais tant bénéficier de l'effet tunnel : en tant que particule quantique, je suis coincée dans une sorte de bol depuis 8 ans, je n'arrête pas de me cogner contre les parois, vraiment comme une mouche frappe bêtement contre une vitre une journée durant sous prétexte qu'elle voit la lumière derrière. Mon énergie est très inférieure à l'énergie minimum qu'il faudrait pour sauter par-dessus les parois du bol : je n'ai aucun bagage, c'est comme si j'escaladais les parois à mains nues, et nombreux sont ceux qui se sont moqués de moi. Il y a une probabilité infime que je passe de l'autre côté, que je trouve l'explication.

(DV, 4/1/14)

L'Homme magnétique. — L'Homme non magnétique.

L'homme robuste, gai, bien équilibré, conscient de sa force et du rôle important qu'il joue dans l'humanité ne ressemble en rien au pauvre mélancolique constamment en proie à la plus sombre tristesse et redoutant sans cesse des malheurs qui n'auront peut-être pas le temps de lui arriver. C'est que notre état physique et notre état moral sont solidaires l'un de l'autre et que, si l'un est sérieusement affecté, l'autre souffre toujours plus ou moins. La force silencieuse de la pensée agissant constamment dans le même sens, façonne notre corps, burine nos traits, dirige nos manières, assure nos gestes et règle notre démarche. En imprimant à tout notre être physique une série de mouvements correspondant à ceux de notre état mental, elle nous rend agréables, attractifs et sympathiques ou désagréables, répulsifs et antipathiques ; et les empreintes de ces qualités et de ces défauts se voient constamment sur notre physionomie, dans nos manières, dans notre attitude, dans notre allure, tout autant que ces qualités elles-mêmes se sentent, car elles sont directement perçues par un sens de l'esprit dont nous ne faisons que soupçonner l'existence.

S'il en est ainsi, on peut donc définir à l'avance le type de l'homme attractif dont la personnalité magnétique, est développée à un certain degré, et l'urnbull nous trace ainsi qu'il suit dans son Cours de Magnétisme personnel les traits caractéristiques de chacun d'eux ; voyons, d'abord, l'homme magnétique :

l'homme magnétique. — Quand vous vous trouvez en compagnie de l'homme consciemment magnétique, le premier effet qu'il vous fait est celui d'être au repos : il n'est point nerveux, il ne s'agite pas. Vous éprouvez, ensuite, le sentiment qu'il a en lui, une force en réserve quelque part, une force dont vous ne pouvez pas fixer l'endroit. Elle ne se trouve pas précisément dans son regard, ni dans ses manières, ni dans son parler, ni dans ses actions ; mais elle est là, elle existe et semble faire partie de lui. Voilà exactement le fait : c'est une partie de lui, et quelques minutes auparavant, tout singulier que cela vous paraisse, c'était dans une petite mesure une partie de vous ! Un peu de cette force d'attraction qu'il montre et dont vous êtes conscient est allé de vous à lui sans que vous le sachiez...

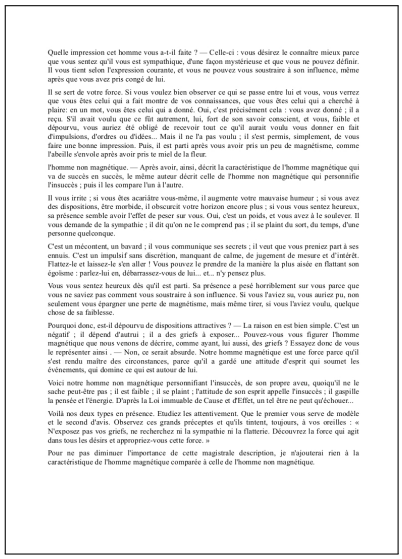
Examinons l'homme d'un peu plus près afin de connaître le secret de la fascination qu'il exerce sur vous. Observez, d'abord, son regard. Ses yeux vous dominant quoiqu'il ne vous regarde pas fixement. Il ne regarde pas dans vos yeux ni dans l'un plutôt que dans l'autre : il regarde juste entre les deux, là où votre nez prend racine. Son regard semble vous percer avec intention — un regard fixe et pénétrant, mais dans lequel il n'y a rien de désagréable. Vous sentez qu'il n'est pas, qu'il ne peut pas être impertinent. Remarquez également qu'il ne vous regarde pas ainsi quand vous parlez : il attend votre communication puis il vous envoie la sienne. Quand il parle, il vous regarde de cette manière déterminée, dominatrice et, cependant, bienveillante, mais il ne se fait, pas valoir...

Il vous écoute avec politesse ; mais vous recevez l'impression d'une volonté inflexible, vous percevez une puissance dans lui. C'est l'homme qui doit être obéi ; en un mot, l'impression qu'il vous laisse est celle de quelqu'un qui sait exactement ce qu'il veut et qui n'est pas pressé parce qu'il est certain de l'obtenir... Voilà, donc, pourquoi il est si calme, si assuré ! Le savoir est une Force et il sait que son état dépend des Lois de Cause, et d'Effet.

Analysons sa conversation. Vous a-t-il appris quelque chose ? Très peu, et rien qu'on puisse considérer comme vain ou prétentieux. Ce qu'il donne n'est généralement point important, quoique vous semblez croire cela tandis que vous l'écoutez.

Il n'est pas empressé. Il vous fait plutôt sentir que, s'il le voulait, il pourrait en dire long. Ainsi, il pique un peu votre curiosité..., mais il ne vous tend pas un piège pour chercher à se faire admirer...

Quand cet homme a attiré vers lui la popularité, l'influence, le succès, il a accepté ces dons : il les a considérés comme son dû..., puis il a continué son chemin... Il a acquis la richesse de la même façon qu'il a acquis la popularité : par la domination. Il a dominé par le magnétisme ; il a attiré les hommes à lui...



Quelle impression cet homme vous a-t-il faite ? — Celle-ci : vous désirez le connaître mieux parce que vous sentez qu'il vous est sympathique, d'une façon mystérieuse et que vous ne pouvez définir. Il vous tient selon l'expression courante, et vous ne pouvez vous soustraire à son influence, même après que vous avez pris congé de lui.

Il se sert de votre force. Si vous voulez bien observer ce qui se passe entre lui et vous, vous verrez que vous êtes celui qui a fait montre de vos connaissances, que vous êtes celui qui a cherché à plaire: en un mot, vous êtes celui qui a donné. Oui, c'est précisément cela : vous avez donné ; il a reçu. S'il avait voulu que ce fût autrement, lui, fort de son savoir conscient, et vous, faible et dépourvu, vous auriez été obligé de recevoir tout ce qu'il aurait voulu vous donner en fait d'impulsions, d'ordres ou d'idées... Mais il ne l'a pas voulu ; il s'est permis, simplement, de vous faire une bonne impression. Puis, il est parti après vous avoir pris un peu de magnétisme, comme l'abeille s'envole après avoir pris te miel de la fleur.

l'homme non magnétique. — Après avoir, ainsi, décrit la caractéristique de l'homme magnétique qui va de succès en succès, le même auteur décrit celle de l'homme non magnétique qui personnifie l'insuccès ; puis il les compare l'un à l'autre.

Il vous irrite ; si vous êtes acariâtre vous-même, il augmente votre mauvaise humeur ; si vous avez des dispositions, être morbide, il obscurcit votre horizon encore plus ; si vous vous sentez heureux, sa présence semble avoir l'effet de peser sur vous. Oui, c'est un poids, et vous avez à le soulever. Il vous demande de la sympathie ; il dit qu'on ne le comprend pas ; il se plaint du sort, du temps, d'une personne quelconque.

C'est un mécontent, un bavard ; il vous communique ses secrets ; il veut que vous preniez part à ses ennuis. C'est un impulsif sans discrétion, manquant de calme, de jugement de mesure et d'intérêt. Flattez-le et laissez-le s'en aller ! Vous pouvez le prendre de la manière la plus aisée en flattant son égoïsme : parlez-lui en, débarrassez-vous de lui... et... n'y pensez plus.

Vous vous sentez heureux dès qu'il est parti. Sa présence a pesé horriblement sur vous parce que vous ne saviez pas comment vous soustraire à son influence. Si vous l'aviez su, vous auriez pu, non seulement vous épargner une perte de magnétisme, mais même tirer, si vous l'aviez voulu, quelque chose de sa faiblesse.

Pourquoi donc, est-il dépourvu de dispositions attractives ? — La raison en est bien simple. C'est un négatif ; il dépend d'autrui ; il a des griefs à exposer... Pouvez-vous vous figurer l'homme magnétique que nous venons de décrire, comme ayant, lui aussi, des griefs ? Essayez donc de vous le représenter ainsi. — Non, ce serait absurde. Notre homme magnétique est une force parce qu'il s'est rendu maître des circonstances, parce qu'il a gardé une attitude d'esprit qui soumet les événements, qui domine ce qui est autour de lui.

Voici notre homme non magnétique personnifiant l'insuccès, de son propre aveu, quoiqu'il ne le sache peut-être pas ; il est faible ; il se plaint ; l'attitude de son esprit appelle l'insuccès ; il gaspille la pensée et l'énergie. D'après la Loi immuable de Cause et d'Effet, un tel être ne peut qu'échouer...

Voilà nos deux types en présence. Etudiez les attentivement. Que le premier vous serve de modèle et le second d'avis. Observez ces grands préceptes et qu'ils tintent, toujours, à vos oreilles : « N'exposez pas vos griefs, ne recherchez ni la sympathie ni la flatterie. Découvrez la force qui agit dans tous les désirs et appropriez-vous cette force. »

Pour ne pas diminuer l'importance de cette magistrale description, je n'ajouterai rien à la caractéristique de l'homme magnétique comparée à celle de l'homme non magnétique.

4 Loi de composition de Ritz-Rydberg

On teste ici sur deux exemples la loi de composition de Ritz-Rydberg, qui a pour conséquence que la composition des règles de réécriture (α, β) et (β, γ) a le même effet que la règle de réécriture (α, γ).

$ab/bc \to bba \to ba \to a$ permet d'obtenir le même résultat que $ac \to a$.

$cd/da \to ddc \to dc \to c$ permet d'obtenir le même résultat que $ca \to c$.

En annexe 2, sont fournies les 64 règles de composition qui vérifient le principe de Ritz-Rydberg.

Annexe 2 : Application de la loi de composition de Ritz-Rydberg aux règles de réécriture

$aa/aa \to aaa \to aa \to a$ permet d'obtenir le même résultat que $aa \to a$.
$aa/ab \to aab \to ab \to b$ permet d'obtenir le même résultat que $ab \to b$.
$aa/ac \to aaa \to aa \to a$ permet d'obtenir le même résultat que $ac \to a$.
$aa/ad \to aab \to ab \to b$ permet d'obtenir le même résultat que $ad \to b$.
$ab/ba \to bba \to ba \to a$ permet d'obtenir le même résultat que $aa \to a$.
$ab/bb \to bbb \to bb \to b$ permet d'obtenir le même résultat que $ab \to b$.
$ab/bc \to bba \to ba \to a$ permet d'obtenir le même résultat que $ac \to a$.
$ab/bd \to bbb \to bb \to b$ permet d'obtenir le même résultat que $ad \to b$.
$ac/ca \to acc \to ac \to a$ permet d'obtenir le même résultat que $ac \to a$.
$ac/cb \to acd \to ad \to b$ permet d'obtenir le même résultat que $ab \to b$.
$ac/cc \to acc \to ac \to a$ permet d'obtenir le même résultat que $ac \to a$.
$ac/cd \to acd \to ad \to b$ permet d'obtenir le même résultat que $ad \to b$.
$ad/da \to bdc \to bc \to a$ permet d'obtenir le même résultat que $aa \to a$.
$ad/db \to bdd \to bd \to b$ permet d'obtenir le même résultat que $ab \to b$.
$ad/dc \to bdc \to bc \to a$ permet d'obtenir le même résultat que $ac \to a$.
$ad/dd \to bdd \to bd \to b$ permet d'obtenir le même résultat que $ad \to b$.

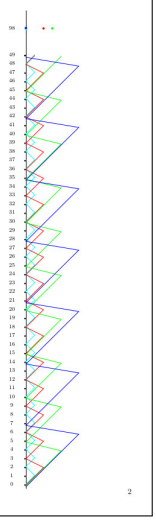
$ba/aa \to aaa \to aa \to a$ permet d'obtenir le même résultat que $ba \to a$.
$ba/ab \to aab \to ab \to b$ permet d'obtenir le même résultat que $bb \to b$.
$ba/ac \to aaa \to aa \to a$ permet d'obtenir le même résultat que $bc \to a$.
$ba/ad \to aab \to ab \to b$ permet d'obtenir le même résultat que $bd \to b$.
$bb/ba \to bba \to ba \to a$ permet d'obtenir le même résultat que $ba \to a$.
$bb/bb \to bbb \to bb \to b$ permet d'obtenir le même résultat que $bb \to b$.
$bb/bc \to bba \to ba \to a$ permet d'obtenir le même résultat que $bc \to a$.
$bb/bd \to bbb \to bb \to b$ permet d'obtenir le même résultat que $bd \to b$.
$bc/ca \to acc \to ac \to a$ permet d'obtenir le même résultat que $ba \to a$.
$bc/cb \to acd \to ad \to b$ permet d'obtenir le même résultat que $bb \to b$.
$bc/cc \to acc \to ac \to a$ permet d'obtenir le même résultat que $bc \to a$.
$bc/cd \to acd \to ad \to b$ permet d'obtenir le même résultat que $bd \to b$.
$bd/da \to bdc \to bc \to a$ permet d'obtenir le même résultat que $ba \to a$.
$bd/db \to bdd \to bd \to b$ permet d'obtenir le même résultat que $bb \to b$.
$bd/dc \to bdc \to bc \to a$ permet d'obtenir le même résultat que $bc \to a$.
$bd/dd \to bdd \to bd \to b$ permet d'obtenir le même résultat que $bd \to b$.

$ca/aa \to caa \to ca \to c$ permet d'obtenir le même résultat que $ca \to c$.
$ca/ab \to cab \to cb \to d$ permet d'obtenir le même résultat que $cb \to d$.
$ca/ac \to caa \to ca \to c$ permet d'obtenir le même résultat que $cc \to c$.
$ca/ad \to cab \to cb \to d$ permet d'obtenir le même résultat que $cd \to d$.
$cb/ba \to dba \to da \to c$ permet d'obtenir le même résultat que $ca \to c$.
$cb/bb \to dbb \to db \to d$ permet d'obtenir le même résultat que $cb \to d$.
$cb/bc \to dba \to da \to c$ permet d'obtenir le même résultat que $cc \to c$.
$cb/bd \to dbb \to db \to d$ permet d'obtenir le même résultat que $cd \to d$.
$cc/ca \to ccc \to cc \to c$ permet d'obtenir le même résultat que $ca \to c$.
$cc/cb \to ccd \to cd \to d$ permet d'obtenir le même résultat que $cb \to d$.
$cc/cc \to ccc \to cc \to c$ permet d'obtenir le même résultat que $cc \to c$.
$cc/cd \to ccd \to cd \to d$ permet d'obtenir le même résultat que $cd \to d$.

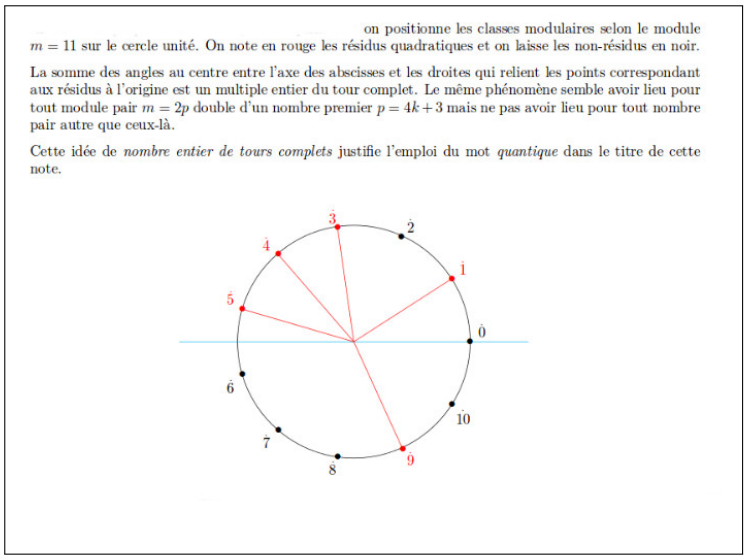
9

$cd/da \to ddc \to dc \to c$ permet d'obtenir le même résultat que $ca \to c$.
$cd/db \to ddd \to dd \to d$ permet d'obtenir le même résultat que $cb \to d$.
$cd/dc \to ddc \to dc \to c$ permet d'obtenir le même résultat que $cc \to c$.
$cd/dd \to ddd \to dd \to d$ permet d'obtenir le même résultat que $cd \to d$.

$da/aa \to caa \to ca \to c$ permet d'obtenir le même résultat que $da \to c$.
$da/ab \to cab \to cb \to d$ permet d'obtenir le même résultat que $db \to d$.
$da/ac \to caa \to ca \to c$ permet d'obtenir le même résultat que $dc \to c$.
$da/ad \to cab \to cb \to d$ permet d'obtenir le même résultat que $dd \to d$.
$db/aa \to dba \to da \to c$ permet d'obtenir le même résultat que $da \to c$.
$db/ab \to dbb \to db \to d$ permet d'obtenir le même résultat que $db \to d$.
$db/ac \to dba \to da \to c$ permet d'obtenir le même résultat que $dc \to c$.
$db/ad \to dbb \to db \to d$ permet d'obtenir le même résultat que $dd \to d$.
$dc/aa \to ccc \to cc \to c$ permet d'obtenir le même résultat que $da \to c$.
$dc/ab \to ccd \to cd \to d$ permet d'obtenir le même résultat que $db \to d$.
$dc/ac \to ccc \to cc \to c$ permet d'obtenir le même résultat que $dc \to c$.
$dc/ad \to ccd \to cd \to d$ permet d'obtenir le même résultat que $dd \to d$.
$dd/aa \to ddc \to dc \to c$ permet d'obtenir le même résultat que $da \to c$.
$dd/ab \to ddd \to dd \to d$ permet d'obtenir le même résultat que $db \to d$.
$dd/ac \to ddc \to dc \to c$ permet d'obtenir le même résultat que $dc \to c$.
$dd/ad \to ddd \to dd \to d$ permet d'obtenir le même résultat que $dd \to d$.



2



on positionne les classes modulaires selon le module $m = 11$ sur le cercle unité. On note en rouge les résidus quadratiques et on laisse les non-résidus en noir.

La somme des angles au centre entre l'axe des abscisses et les droites qui relient les points correspondant aux résidus à l'origine est un multiple entier du tour complet. Le même phénomène semble avoir lieu pour tout module pair $m = 2p$ double d'un nombre premier $p = 4k+3$ mais ne pas avoir lieu pour tout nombre pair autre que ceux-là.

Cette idée de *nombre entier de tours complets* justifie l'emploi du mot *quantique* dans le titre de cette note.

Notes sur En cherchant Majorana d'Etienne Klein
(Denise Chemla - 26/12/2013)

(p.54) Mais le mécanisme de cette radioactivité est incompréhensible dans le cadre de la physique classique. Et c'est là que Gamow et Majorana franchissent un seuil. Selon les lois classiques, il est impossible qu'une particule alpha sorte d'un noyau atomique, qui représente pour elle une cuvette aux parois infranchissables, autrement dit une "barrière de potentiel". Ce que Gamow comprend et que Majorana démontre formellement, c'est qu'une telle interdiction peut être déjouée par les lois quantiques. Appliquées à une particule alpha prétendument prisonnière d'un noyau, elles lui permettent d'apparaître... à l'extérieur du noyau! Elles lui offrent en effet une probabilité non nulle de traverser la barrière de potentiel. Initialement confinée, la particule alpha se déplace très vite, ne cesse d'aborder de se cogner et de rebondir sur la paroi intérieure du noyau ; puis, après de multiples tentatives infructueuses, profitant du jeu des probabilités et de la multiplicité des occasions, elle finit par passer au travers - d'où le terme d'"effet tunnel" inventé par Gamow.

Mon interprétation : je suis une particule alpha et j'ai une probabilité infime d'échapper à ma condition, à force de m'être cognée à CG, et de réussir peut-être à la désastrer, par "effet tunnel" !!!

(p.109) Majorana dans son dernier article émet l'hypothèse que certaines particules dépourvues de charge électrique pourraient être leur propre antiparticule - une hypothèse à l'origine de recherches menées aujourd'hui sur des particules fascinantes et fantomatiques, les neutrinos.

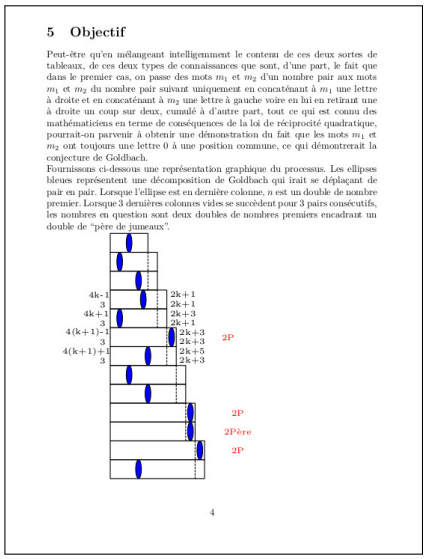
(P.110) L'équation de Dirac recèle quelque chose d'étrange : certaines des solutions de son équation correspondent à des particules d'énergie... négative! Or toutes les particules connues sont dotées d'une énergie positive, y compris lorsqu'elles sont immobiles, puisque leur énergie est alors égale à leur énergie de masse mc^2. Si ces particules d'énergie négative existaient, elles auraient donc une masse négative. Cela impliquerait que, sous l'action d'une force, elles se déplaceraient dans le sens contraire à celui des particules ordinaires, toutes dotées d'une masse positive.[...] Or nouvel objet microscopique est l'"antiparticule de l'électron", qui sera bientôt baptisée le "positron". Dirac démontre en outre qu'un électron et un positron ne peuvent apparaître qu'ensemble, c'est à dire par paire, un peu comme des frères jumeaux.

(p.112) Majorana montre d'abord, de façon très élégante, qu'on peut déduire l'équation de Dirac d'un principe plus fondamental, en fait plus symétrique, que celui dont est parti le théoricien anglais. Il montre ensuite qu'on peut donner une autre forme à cette équation et qu'alors certaines de ses solutions correspondent à des particules qui sont... leur propre antiparticule! Majorana pour cela identifie d'autres matrices que celles de Dirac satisfaisant aux règles de la même algèbre (de Clifford), les "matrices de Majorana" dont toutes les composantes sont des nombres imaginaires purs (de partie réelle nulle), ce qui permet à la nouvelle équation ainsi obtenue d'avoir des solutions réelles (au sens où elles ne sont pas complexes). Ces solutions réelles correspondent à des particules qui sont leur propre antiparticule.

Mon interprétation : Les particules qui sont leur propre antiparticule sont les nombres premiers. Les électrons et les positrons qui vont par deux correspondent à mes caractères de divisibilité dans les grilles. On n'aura qu'à affecter aux nombres jusqu'à $n/2$ des électrons seulement et aux nombres de $n/2$ à n les positrons correspondants.

1

- 21.10.2014 : Pour ceux qui aiment bien s'abaisser les dioptries et les dixièmes, un programme et son résultat (261) pgmcg.pdf rescg.pdf en `Python` pgmcg.py
- 20.10.2014 : Résumé de l'observation des relations invariantes entre nombres de décompositions de Goldbach codées dans un langage à 4 lettres (260) resume.pdf
- 14.09.2014 : dans la note du 17 mai, j'ai commis une grossière erreur page 8 ;

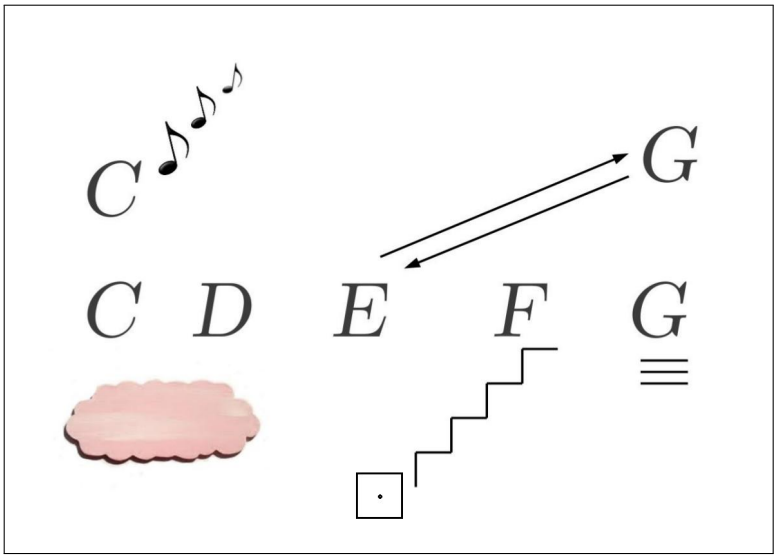


5 Objectif

Peut-être qu'en mélangeant intelligemment le contenu de ces deux sortes de tableaux, de ces deux types de connaissances que sont, d'une part, le fait que dans le premier cas, on passe des mots m_1 et m_2 d'un nombre pair aux mots m_1 et m_2 du nombre pair suivant uniquement en concaténant à m_1 une lettre à droite et en concaténant à m_2 une lettre à gauche voire en lui en retirant une à droite un coup sur deux, cumulé à d'autre part, tout ce qui est connu des mathématiciens en terme de conséquences de la loi de réciprocité quadratique, pourrait-on parvenir à obtenir une démonstration du fait que les mots m_1 et m_2 ont toujours une lettre 0 à une position commune, ce qui démontrerait la conjecture de Goldbach.
Fournissons ci-dessous une représentation graphique du processus. Les ellipses bleues représentent une décomposition de Goldbach qui irait se déplaçant de pair en pair. Lorsque l'ellipse est en dernière colonne, n est un double de nombre premier. Lorsque 3 dernières colonnes vides se succèdent pour 3 pairs consécutifs, les nombres en question sont deux doubles de nombres premiers encadrant un double de "père de jumeaux".

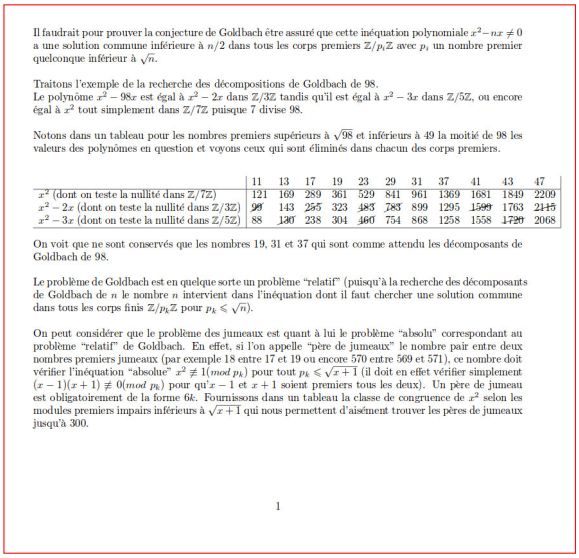
4

- je vais essayer de la corriger en utilisant uniquement des démonstrations par récurrence (pages 6, 7 et 8) ; remerciements à D.Perrin qui a lu ma note et signalé l'erreur. (259)
- 05.08.2014 : Nuage rose le soir, de beau temps, l'espoir...



- 10.07.2014 : Primalité et zéros de sommes de cosinus (258) primesommecos.pdf
- 19.06.2014 : Calcul simplifié de la somme des diviseurs (257) somme-div-cos.pdf
- 23.05.2014 : Gauss a écrit : "Le problème de distinguer les nombres premiers des nombres composés et de décomposer ceux-ci en leurs facteurs premiers est connu comme un des plus importants et des plus utiles de toute l'Arithmétique. [...] En outre, la dignité de la Science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre."

- 17.05.2014 : Conjecture de Goldbach, langage à 4 lettres, variables et invariants (256) cg-mots-autom.pdf annexes.pdf e-cg-mots-autom.pdf transp-mots.pdf e-transp-mots.pdf
- ♥ 17.05.2014 : continuer de suivre Galois (ajout du problème des nombres premiers d'écart 2) (255) invariante.pdf



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

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

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

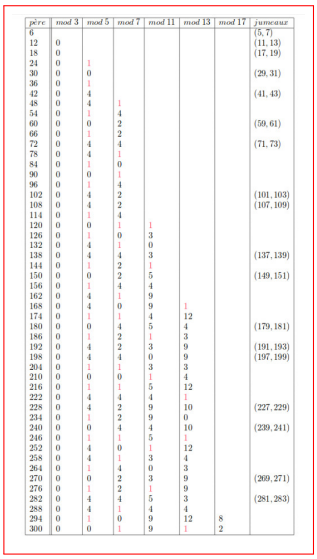
	11	13	17	19	23	29	31	37	41	43	47
x^2 (dont on teste la nullité dans $\mathbb{Z}/7\mathbb{Z}$)	121	169	289	361	529	841	961	1369	1681	1849	2209
$x^2 - 2x$ (dont on teste la nullité dans $\mathbb{Z}/3\mathbb{Z}$)	~~99~~	143	~~255~~	323	~~483~~	~~783~~	899	1295	~~1599~~	1763	~~2115~~
$x^2 - 3x$ (dont on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

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

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

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

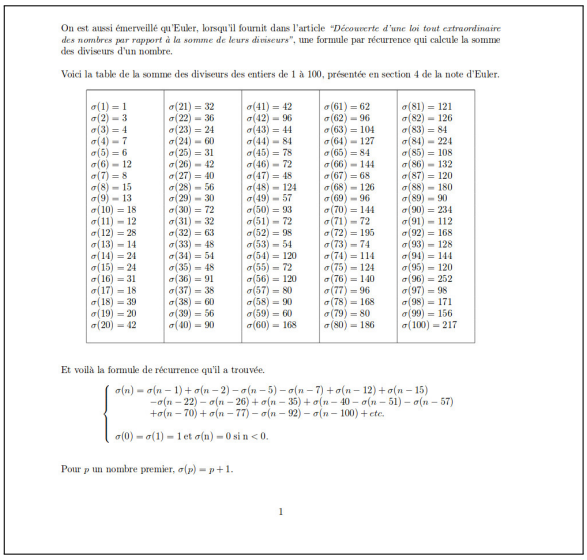
1



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

- ♥ 11.05.2014 : Un beau souvenir de 2005 : empilement de valuations p-adiques, en continuant de suivre Laisant (254) Laisant-empilement.pdf

- 26.04.2014 : Essayer de remonter à la source des idées (253) origine-idees.pdf
- 26.04.2014 : La leçon de mathématiques absurdes d'Eugène Ionesco (252) Ionesco.pdf
- 23.04.2014 : Conjecture de Goldbach, langage à 4 lettres, variables et invariants (251) cg-info.pdf annexes.pdf e-cg-info.pdf
- 18.04.2014 : Conjecture de Goldbach et langage à 4 lettres, grâce à l'aide de Claude que je remercie (250) cgtempo.pdf
- 16.04.2014 : Les nombres sont des mots (249) protos.pdf
- 12.04.2014 : Diaporama Les nombres sont des mots (248) transp-l4.pdf e-transp-l4.pdf
- 12.04.2014 : Observer les mots (247) contradiction.pdf e-contradiction.pdf
- 12.04.2014 : Positionner les décompositions triviales de Goldbach sur la droite du plan complexe de partie réelle 1/2 (246) complexe.pdf
- 28.03.2014 : Les points du maillage commutent-ils ? (245) maillage.pdf
- ...27.03.2014 : On peut oublier l'indéterminisme sur la première lettre des mots en utilisant des mots infinis des deux côtés... (244)
- 27.03.2014 : Mots bouclés (243) boucles.pdf
- 26.03.2014 : Programmer la note Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs (242) pgm-Euler.pdf Euler-decouv.pdf 6.4.2025 : programme `Python` Euler-sumdiv-en-python.pdf
- Euler et sa loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs (241) calculer les sommes de diviseurs par un calcul matriciel matdivmodif.pdf



On est aussi émerveillé qu'Euler, lorsqu'il fournit dans l'article *"Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs"*, une formule par récurrence qui calcule la somme des diviseurs d'un nombre.

Voici la table de la somme des diviseurs des entiers de 1 à 100, présentée en section 4 de la note d'Euler.

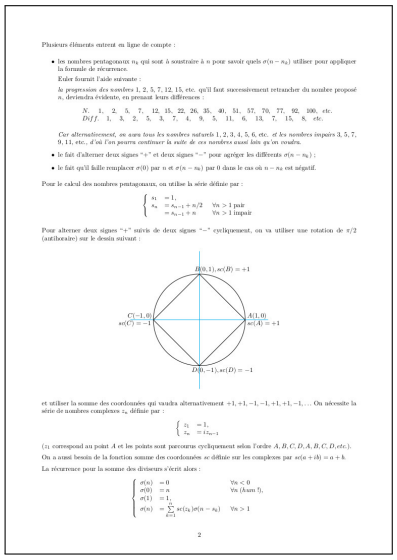
$\sigma(1) = 1$	$\sigma(21) = 32$	$\sigma(41) = 42$	$\sigma(61) = 62$	$\sigma(81) = 121$
$\sigma(2) = 3$	$\sigma(22) = 36$	$\sigma(42) = 96$	$\sigma(62) = 96$	$\sigma(82) = 126$
$\sigma(3) = 4$	$\sigma(23) = 24$	$\sigma(43) = 44$	$\sigma(63) = 104$	$\sigma(83) = 84$
$\sigma(4) = 7$	$\sigma(24) = 60$	$\sigma(44) = 84$	$\sigma(64) = 127$	$\sigma(84) = 224$
$\sigma(5) = 6$	$\sigma(25) = 31$	$\sigma(45) = 78$	$\sigma(65) = 84$	$\sigma(85) = 108$
$\sigma(6) = 12$	$\sigma(26) = 42$	$\sigma(46) = 72$	$\sigma(66) = 144$	$\sigma(86) = 132$
$\sigma(7) = 8$	$\sigma(27) = 40$	$\sigma(47) = 48$	$\sigma(67) = 68$	$\sigma(87) = 120$
$\sigma(8) = 15$	$\sigma(28) = 56$	$\sigma(48) = 124$	$\sigma(68) = 126$	$\sigma(88) = 180$
$\sigma(9) = 13$	$\sigma(29) = 30$	$\sigma(49) = 57$	$\sigma(69) = 96$	$\sigma(89) = 90$
$\sigma(10) = 18$	$\sigma(30) = 72$	$\sigma(50) = 93$	$\sigma(70) = 144$	$\sigma(90) = 234$
$\sigma(11) = 12$	$\sigma(31) = 32$	$\sigma(51) = 72$	$\sigma(71) = 72$	$\sigma(91) = 112$
$\sigma(12) = 28$	$\sigma(32) = 63$	$\sigma(52) = 98$	$\sigma(72) = 195$	$\sigma(92) = 168$
$\sigma(13) = 14$	$\sigma(33) = 48$	$\sigma(53) = 54$	$\sigma(73) = 74$	$\sigma(93) = 128$
$\sigma(14) = 24$	$\sigma(34) = 54$	$\sigma(54) = 120$	$\sigma(74) = 114$	$\sigma(94) = 144$
$\sigma(15) = 24$	$\sigma(35) = 48$	$\sigma(55) = 72$	$\sigma(75) = 124$	$\sigma(95) = 120$
$\sigma(16) = 31$	$\sigma(36) = 91$	$\sigma(56) = 120$	$\sigma(76) = 140$	$\sigma(96) = 252$
$\sigma(17) = 18$	$\sigma(37) = 38$	$\sigma(57) = 80$	$\sigma(77) = 96$	$\sigma(97) = 98$
$\sigma(18) = 39$	$\sigma(38) = 60$	$\sigma(58) = 90$	$\sigma(78) = 168$	$\sigma(98) = 171$
$\sigma(19) = 20$	$\sigma(39) = 56$	$\sigma(59) = 60$	$\sigma(79) = 80$	$\sigma(99) = 156$
$\sigma(20) = 42$	$\sigma(40) = 90$	$\sigma(60) = 168$	$\sigma(80) = 186$	$\sigma(100) = 217$

Et voilà la formule de récurrence qu'il a trouvée.

$$\begin{cases} \sigma(n) = \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \sigma(n-12) + \sigma(n-15) \\ \qquad -\sigma(n-22) - \sigma(n-26) + \sigma(n-35) + \sigma(n-40 - \sigma(n-51) - \sigma(n-57) \\ \qquad +\sigma(n-70) + \sigma(n-77) - \sigma(n-92) - \sigma(n-100) + etc. \\ \\ \sigma(0) = \sigma(1) = 1 \text{ et } \sigma(\text{n}) = 0 \text{ si n} < 0. \end{cases}$$

Pour p un nombre premier, $\sigma(p) = p + 1$.

1



Plusieurs éléments entrent en ligne de compte :

- les nombres pentagonaux n_k qui sont à soustraire à n pour savoir quels $\sigma(n - s_k)$ utiliser pour appliquer la formule de récurrence.
  Euler fournit l'aide suivante :
  la progression des nombres 1, 2, 5, 7, 12, 15, etc. qu'il faut successivement retrancher du nombre proposé n, deviendra évidente, en prenant leurs différences :

  $N.\ \ 1,\ \ 2,\ \ 5,\ \ 7,\ \ 12,\ \ 15,\ \ 22,\ \ 26,\ \ 35,\ \ 40,\ \ 51,\ \ 57,\ \ 70,\ \ 77,\ \ 92,\ \ 100,\ \ etc.$
  $Diff.\ \ 1,\ \ 3,\ \ 2,\ \ 5,\ \ 3,\ \ 7,\ \ 4,\ \ 9,\ \ 5,\ \ 11,\ \ 6,\ \ 13,\ \ 7,\ \ 15,\ \ 8,\ \ etc.$

  Car alternativement, on aura tous les nombres naturels 1, 2, 3, 4, 5, 6, etc. *et les nombres impairs* 3, 5, 7, 9, 11, etc., *d'où l'on pourra continuer la suite de ces nombres aussi loin qu'on voudra.*
- le fait d'alterner deux signes "+" et deux signes "−" pour agréger les différents $\sigma(n - s_k)$;
- le fait qu'il faille remplacer $\sigma(0)$ par n et $\sigma(n - s_k)$ par 0 dans le cas où $n - s_k$ est négatif.

Pour le calcul des nombres pentagonaux, on utilise la série définie par :

$$\begin{cases} s_1 &= 1, \\ s_n &= s_{n-1} + n/2 \quad \forall n > 1 \text{ pair} \\ &= s_{n-1} + n \quad \forall n > 1 \text{ impair} \end{cases}$$

Pour alterner deux signes "+" suivis de deux signes "−" cycliquement, on va utiliser une rotation de $\pi/2$ (antihoraire) sur le dessin suivant :

et utiliser la somme des coordonnées qui vaudra alternativement $+1, +1, -1, -1, +1, +1, -1, \ldots$ On nécessite la série de nombres complexes z_n définie par :

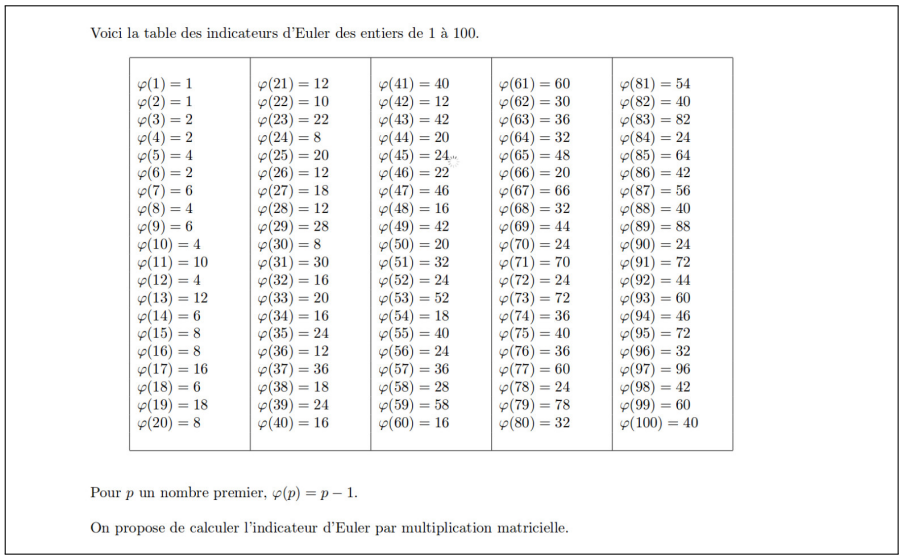
$$\begin{cases} z_1 &= 1, \\ z_n &= iz_{n-1} \end{cases}$$

(z_1 correspond au point A et les points sont parcourus cycliquement selon l'ordre $A, B, C, D, A, B, C, D, etc.$).
On a aussi besoin de la fonction somme des coordonnées ar définie sur les complexes par $ar(a + ib) = a + b$.
La récurrence pour la somme des diviseurs s'écrit alors :

$$\begin{cases} \sigma(n) &= 0 & \forall n < 0 \\ \sigma(0) &= n & \forall n \text{ (bam !)}, \\ \sigma(1) &= 1, \\ \sigma(n) &= \sum_{k=1} ar(z_k)\sigma(n - s_k) & \forall n > 1 \end{cases}$$

2

- 23.03.2014 : Conjecture de Goldbach et mouvement brownien, mais l'indéterminisme sur la première lettre des mots reste patent (on jette l'éponge) brownien.pdf (en) brownian.pdf)
- 22.03.2014 : Retrouver Euler et son indicatrice (239) indicatrice_d_Euler.pdf
- calculer les indicateurs d'Euler par un calcul matriciel (238) matindicEuler.pdf



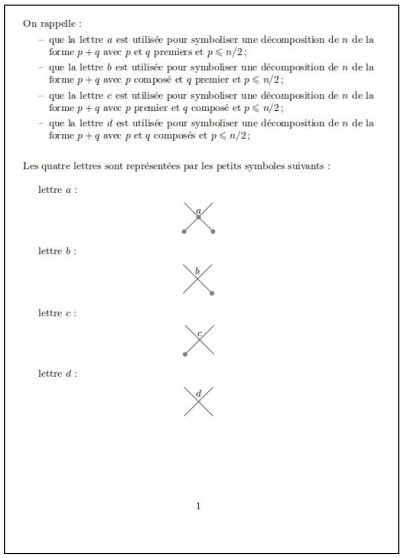
Voici la table des indicateurs d'Euler des entiers de 1 à 100.

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

Pour p un nombre premier, $\varphi(p) = p - 1$.

On propose de calculer l'indicateur d'Euler par multiplication matricielle.

- 22.03.2014 : Récurrence mystérieuse pour la somme des diviseurs (237) recurrence-mysterieuse.pdf
- 22.03.2014 : Des règles de réécriture et un indéterminisme patent complètement décourageants (236) reglessibizarres.pdf
- 20.03.2014 : 1 monoïde, 2 booléens, 4 lettres, 16 règles, 1 invariant et des changements de parité (a+c fonction en espalier qui compte les doubles de premiers) (235) transposition.pdf
- 21.02.2014 : Le petit baluchon (234) baluchon.pdf
- 16.02.2014 : Conjecture de Goldbach : écrire, réécrire, compter (233) ecrreecc.pdf
- 12.02.2014 : Conjecture de Goldbach, langage, réécriture (232) abcd.pdf
- 08.02.2014 : où l'on retrouve le maillage d'octobre 2005 (231) merveilleuxmaillage.pdf



On rappelle :

- que la lettre a est utilisée pour symboliser une décomposition de n de la forme $p + q$ avec p et q premiers et $p \leqslant n/2$;
- que la lettre b est utilisée pour symboliser une décomposition de n de la forme $p + q$ avec p composé et q premier et $p \leqslant n/2$;
- que la lettre c est utilisée pour symboliser une décomposition de n de la forme $p + q$ avec p premier et q composé et $p \leqslant n/2$;
- que la lettre d est utilisée pour symboliser une décomposition de n de la forme $p + q$ avec p et q composés et $p \leqslant n/2$;

Les quatre lettres sont représentées par les petits symboles suivants :

lettre a :

lettre b :

lettre c :

lettre d :

1

Les 16 règles de réécriture sont alors aisées à retrouver :

1) règle $aa \to a$:

2) règle $ab \to b$:

3) règle $ac \to a$:

4) règle $ad \to b$:

5) règle $ba \to a$:

6) règle $bb \to b$:

7) règle $bc \to a$:

8) règle $bd \to b$:

9) règle $ca \to c$:

10) règle $cb \to d$:

11) règle $cc \to c$:

12) règle $cd \to d$:

13) règle $da \to c$:

14) règle $db \to d$:

15) règle $dc \to c$:

16) règle $dd \to d$:

On peut ainsi "lire verticalement" les mots sur notre alphabet de 4 lettres associés aux nombres pairs successifs (les décompositions de Goldbach sont indiquées par les lettres a rouges).

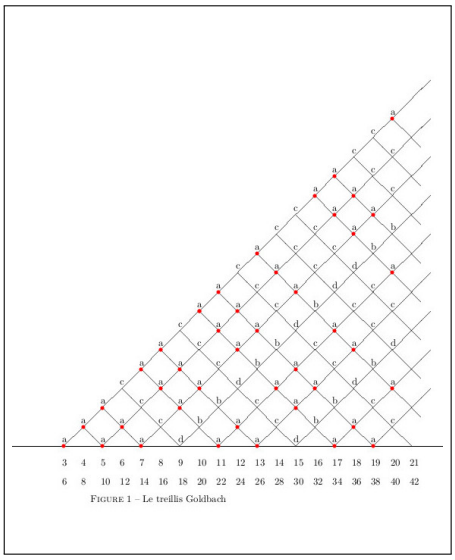
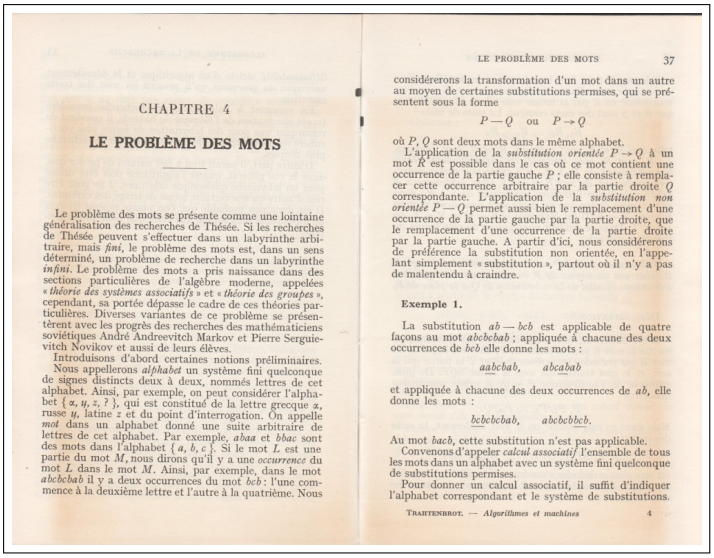


FIGURE 1 – Le treillis Goldbach

- 05.02.2014 : Le petit livre orange de Trahtenbrot du professeur Yves Césari (que je remercie, ainsi que Michel Chein, Olivier Cogis, Jean-Paul Bordat, Hervé Dicky, Eric Terouanne, Max Vincent, Pierre Dujols, et les autres) qui traite entre autres du problème du mot (230)



CHAPITRE 4

LE PROBLÈME DES MOTS

Le problème des mots se présente comme une lointaine généralisation des recherches de Thésée. Si les recherches de Thésée peuvent s'effectuer dans un labyrinthe arbitraire, mais *fini*, le problème des mots est, dans un sens déterminé, un problème de recherche dans un labyrinthe *infini*. Le problème des mots a pris naissance dans des sections particulières de l'algèbre moderne, appelées « *théorie des systèmes associatifs* » et « *théorie des groupes* », cependant, sa portée dépasse le cadre de ces théories particulières. Diverses variantes de ce problème se présentèrent avec les progrès des recherches des mathématiciens soviétiques André Andreevitch Markov et Pierre Serguievitch Novikov et aussi de leurs élèves.

Introduisons d'abord certaines notions préliminaires.

Nous appellerons *alphabet* un système fini quelconque de signes distincts deux à deux, nommés lettres de cet alphabet. Ainsi, par exemple, on peut considérer l'alphabet $\{\alpha, u, z, ?\}$, qui est constitué de la lettre grecque α, russe u, latine z et du point d'interrogation. On appelle *mot* dans un alphabet donné une suite arbitraire de lettres de cet alphabet. Par exemple, *abaa* et *bbac* sont des mots dans l'alphabet $\{a, b, c\}$. Si le mot L est une partie du mot M, nous dirons qu'il y a une *occurrence* du mot L dans le mot M. Ainsi, par exemple, dans le mot *abcbcbab* il y a deux occurrences du mot *bcb* : l'une commence à la deuxième lettre et l'autre à la quatrième. Nous

considérerons la transformation d'un mot dans un autre au moyen de certaines substitutions permises, qui se présentent sous la forme

$$P - Q \quad \text{ou} \quad P \to Q$$

où P, Q sont deux mots dans le même alphabet.

L'application de la *substitution orientée* $P \to Q$ à un mot R est possible dans le cas où ce mot contient une occurrence de la partie gauche P ; elle consiste à remplacer cette occurrence arbitraire par la partie droite Q correspondante. L'application de la *substitution non orientée* $P - Q$ permet aussi bien le remplacement d'une occurrence de la partie gauche par la partie droite, que le remplacement d'une occurrence de la partie droite par la partie gauche. A partir d'ici, nous considérerons de préférence la substitution non orientée, en l'appelant simplement « substitution », partout où il n'y a pas de malentendu à craindre.

Exemple 1.

La substitution $ab - bcb$ est applicable de quatre façons au mot *abcbcbab* ; appliquée à chacune des deux occurrences de *bcb* elle donne les mots :

$$a\underline{abcbab}, \qquad \underline{abcbab}$$

et appliquée à chacune des deux occurrences de *ab*, elle donne les mots :

$$\underline{bcbcbcbab}, \qquad abcbc\underline{bcb}.$$

Au mot *bacb*, cette substitution n'est pas applicable.

Convenons d'appeler *calcul associatif* l'ensemble de tous les mots dans un alphabet avec un système fini quelconque de substitutions permises.

Pour donner un calcul associatif, il suffit d'indiquer l'alphabet correspondant et le système de substitutions.

Si le mot R peut être transformé en le mot S par une seule application d'une substitution permise, S peut être transformé en R par la même voie ; dans ce cas, on dira que R et S sont des mots *contigus*. La suite de mots :

$$R_1, R_2, \ldots, R_{n-1}, R_n$$

telle que R_1 et R_2 sont contigus, R_2 et R_3 sont contigus, ..., R_{n-1} et R_n sont contigus, sera appelée *chaîne déductive* conduisant de R_1 à R_n. S'il existe une chaîne déductive conduisant du mot R au mot S, alors, évidemment, il existe une chaîne déductive conduisant de S à R ; dans ce cas, nous dirons que ces mots sont *équivalents* et nous écrirons $R \sim S$. Il est clair que si $S \sim R$ et $R \sim T$, on a $S \sim T$. Dans ce qui suit nous aurons de plus besoin du théorème suivant :

Théorème. — *Soit $P \sim Q$; si dans un mot quelconque R il existe une occurrence de P on obtient un mot équivalent à R comme résultat de la substitution de Q à la place de P.*

DÉMONSTRATION.

Il est commode, sous les conditions du théorème, de mettre le mot R sous la forme SPT, où S est la partie du mot R qui précède l'occurrence de P et T la partie qui la suit, et le mot transformé sous la forme SQT. De plus, en vertu de l'équivalence $P \sim Q$, il existe une chaîne déductive

$$P, P_1, P_2, \ldots, P_m, Q.$$

Mais dans ce cas, comme on le voit facilement, la suite des mots :

$$SPT,\ SP_1T,\ SP_2T,\ \ldots,\ SP_mT,\ SQT$$

est une chaîne déductive conduisant de SPT (c'est-à-dire R) à SQT (c'est-à-dire au mot transformé). Le théorème est démontré.

Exemple 2.

Considérons le calcul associatif qui a été étudié par G. S. Tseitin.

Alphabet :

$$\{ a, b, c, d, e \}.$$

Système de substitutions permises

$$\begin{array}{c} ac \to ca \\ ad \to da \\ bc \to cb \\ bd \to db \\ abac \to abacc \\ eca \to ae \\ edb \to be. \end{array}$$

Dans ce calcul, au mot *abcde* s'applique seulement la troisième substitution et il a seulement un mot contigu *acbde*. Puis on a l'équivalence $abcde \sim cadedb$, comme on le voit à partir de la chaîne déductive suivante :

$$\underline{abcde},\ \underline{acbde},\ \underline{cabde},\ \underline{cadbe},\ cadedb$$

Si on prend le mot *aaabb*, aucune des substitutions ne lui est applicable et donc il n'a aucun mot contigu ; à fortiori, il n'existe pas de mot différent de *aaabb* qui lui serait équivalent.

Chaque calcul associatif a son propre *problème d'équivalence des mots*. Il s'exprime ainsi :

Pour deux mots arbitraires dans un calcul donné, on veut savoir s'ils sont équivalents ou non.

Puisqu'il existe un ensemble infini de mots différents dans un calcul arbitraire, on a en fait une série infinie de problèmes du même type et leur solution se présente sous forme d'un algorithme discernant l'équivalence ou la non-équivalence de deux mots arbitraires.

On peut avoir l'impression que le problème des mots n'est qu'un casse-tête artificiellement tiré par les cheveux

et par conséquent que la découverte d'un tel algorithme ne présente pas d'intérêt théorique ou pratique particulier. En réalité, il en est loin d'être ainsi ; on peut montrer que ce problème est très naturel, a une grande valeur théorique et pratique et que l'effort dirigé vers la construction de l'algorithme correspondant est pleinement justifié. Toutefois, au présent stade de notre exposé, nous nous en abstiendrons, en attendant d'étudier cette question à fond et nous passerons à la considération de certains faits concrets.

D'abord, indiquons le lien du problème de l'équivalence des mots avec le problème de Thésée. Si on construit pour chaque mot sa « place » et pour chaque paire de mots contigus un corridor joignant les places correspondantes, le calcul associatif nous apparaît sous la forme d'un labyrinthe, avec un nombre infini de places et de corridors, de chaque place duquel rayonne seulement un nombre fini de corridors (à vrai dire, on peut trouver ici des places dont ne sort aucun corridor : par exemple le mot *aaabb* de l'exemple 2). De plus la chaîne déductive conduisant de chaque mot R au mot Q se présente comme un chemin du labyrinthe conduisant d'une place à une autre et l'équivalence des mots correspond à l'accessibilité mutuelle d'une place à partir d'une autre. Enfin, avec cette interprétation, le problème des mots revient lui-même à des problèmes de recherche de chemins dans un labyrinthe infini.

Afin de mieux élucider les aspects spécifiques des difficultés qui surgissent ici, considérons d'abord le *problème restreint des mots* qui s'énonce de la façon suivante :

Pour deux mots arbitraires R et T dans un calcul associatif donné, on veut savoir si on peut transformer l'un en l'autre à l'aide de k applications successives au plus des substitutions permises (le nombre naturel k est choisi arbitrairement, mais fixe).

Pour le problème ainsi posé, on construit aisément un algorithme : en effet, on peut utiliser l'algorithme du triage, qui nous est déjà connu, suivant lequel on examine

la liste de tous les mots, en commençant par le mot R, puis l'on passe à tout mot qui lui est contigu, puis de mots contigus en mots contigus et ainsi de suite k fois. La réponse à la question posée sera affirmative ou négative suivant que le mot T sera ou non découvert dans cette liste.

Cependant, si on retourne au problème non limité des mots, la situation est essentiellement différente. Quelle que soit la longueur de la chaîne déductive, conduisant de R à T (s'il existe une telle chaîne), il peut arriver, généralement parlant, que l'on ne sache pas quand il convient de tenir pour terminé le processus de triage. Supposons, par exemple, que nous ayons déjà poursuivi le processus de triage jusqu'au

$$10^{20} = 100\,000\,000\,000\,000\,000\,000$$

triage et que nous disposons déjà d'une liste de tous les mots que l'on peut obtenir à partir de R à l'aide des applications réitérées des substitutions dont le nombre total ne dépasse pas 10^{20}, et supposons que le mot T ne se trouve pas dans cette liste. Est-ce que cela nous donne une raison quelconque de conclure à la non-équivalence des mots R et T ? Certainement pas, car n'est pas exclue la possibilité que R et T soient équivalents, mais que la chaîne déductive qui les relie est plus longue encore.

Pour obtenir les résultats désirés, il convient ici de renoncer à un simple triage ; il est nécessaire d'adopter une autre voie, reposant sur l'analyse du mécanisme même de la transformation d'un mot en un autre à l'aide des substitutions permises. Nous essaierons, par exemple, d'élucider si les mots *abaacd* et *acbdad* sont équivalents dans le calcul de Tseitin (cf. exemple 2). Une réponse négative à cette question provient des considérations suivantes. Dans chacune des substitutions permises de ce calcul, la partie gauche et la partie droite contiennent le même nombre d'occurrences de la lettre *a* (ou ne contiennent pas du tout cette lettre) ; donc, dans une chaîne déductive quelconque, tous les mots doivent contenir

le même nombre d'occurrrences de la lettre *a*. Comme dans les deux mots proposés le nombre d'occurrences de la lettre *a* n'est pas le même, ces mots ne sont pas équivalents.

La découverte de semblables *invariants déductifs* c'est-à-dire de propriétés qui restent invariables pour tous les mots d'une chaîne déductive, permet, dans certains cas, de trouver des algorithmes pour la solution cherchée.

Exemple 3.

Alphabet :

$$\{ a, b, c, d, e \}.$$

Système de substitutions permises

$$\begin{array}{llll} ab \to ba\,; & ae \to ea\,; & be \to eb\,; & de \to ed\,; \\ ac \to ca\,; & bc \to cb\,; & cd \to dc\,; & \\ ad \to da\,; & bd \to db\,; & ce \to ec. & \end{array}$$

Ces substitutions permises ne changent pas la quantité des occurrences de chaque lettre dans un mot, et changent seulement l'ordre des lettres dans un mot. On voit immédiatement que deux mots sont équivalents si et seulement s'ils renferment le même nombre d'occurrences de chaque lettre. D'après cela, il y a un algorithme très simple qui permet de discerner l'équivalence et qui se ramène à compter le nombre des occurrences des lettres dans chacun de ces mots et à comparer ces nombres.

Nous verrons plus bas, d'une manière détaillée, un exemple plus complexe ; mais d'abord nous conviendrons dans ce qui suit d'une généralisation des notions de « mot » et de « substitution permise ». De façon précise, nous considérerons, outre les mots usuels, dans l'alphabet considéré, le *mot vide*, qui ne contient aucune lettre, et nous le symboliserons par Λ. En outre, nous admettrons une substitution de la forme

$$P \to \Lambda.$$

De plus le remplacement de la partie gauche par le mot vide signifie simplement que l'on retranche l'occurrence du mot P dans le mot à transformer. Le remplacement de la partie droite par la partie gauche signifie qu'entre deux lettres quelconques du mot à transformer ; ou devant lui, ou derrière lui, on met le mot P.

Exemple 4.

Soit donné le calcul associatif dans l'alphabet $\{ a, b, c \}$ avec le système de substitutions :

$$\begin{array}{c} b \to acc \\ ca \to accc \\ aa \to \Lambda \\ bb \to \Lambda \\ cccc \to \Lambda. \end{array}$$

On demande de trouver un algorithme de résolution pour le problème de l'équivalence des mots dans ce calcul.

Construisons un algorithme auxiliaire, l'algorithme de réduction, qui pour un mot arbitraire indique un mot d'une forme particulière qui lui est équivalent — le mot réduit. Pour cela, considérons le système mis sous forme de substitutions orientées

$$\begin{array}{c} b \to acc \\ ca \to accc \\ aa \to \Lambda \\ cccc \to \Lambda \end{array}$$

et convenons que dans l'application à un mot quelconque R, l'algorithme fonctionne ainsi : on prend la première des substitutions (orientées), dans l'ordre où elles se présentent sur cette liste, qui soit applicable au mot R et, parmi les occurrences de sa partie gauche dans le mot R, cette substitution s'applique à la première, c'est-à-dire la plus à gauche ; si, après un nombre fini de tels pas, on obtient le mot S, auquel aucune des substitutions précédentes

n'est plus applicable, on dit que l'algorithme appliqué au mot R le transforme en le mot S (1).

Nous montrerons que, quel que soit le mot R, l'algorithme de réduction s'applique et le transforme en un des huit mots suivants (mots réduits) :

$$\Lambda,\ c,\ cc,\ ccc,\ a,\ ac,\ acc,\ accc.$$

En effet, si dans le mot R il existe une occurrence de la lettre b, on appliquera d'abord la première substitution qui élimine b et la remplace par acc, jusqu'à ce qu'il ne reste plus de b. Puis fonctionne la deuxième substitution, qui transfère la lettre a à gauche de la lettre c, jusqu'à ce qu'il ne reste plus de a suivant immédiatement à droite une lettre c, en d'autres termes, jusqu'à ce que tous les a se trouvent avant tous les c. Enfin commence le processus de suppression des paires de a voisins et des quadruples de c voisins, jusqu'à ce que n'apparaissent plus que des mots qui ne contiennent pas plus d'un a et pas plus de trois c ; il ne peut donc y avoir que huit de ces mots et ils viennent d'être énumérés plus haut.

Il est évident que chaque mot est équivalent à son mot réduit, donc que deux mots sont équivalents si et seulement s'il leur correspond le même mot réduit, ou deux mots réduits équivalents. Nous montrerons plus bas que les huit mots réduits sont deux à deux non équivalents. Il en résultera que deux mots sont équivalents si et seulement s'il leur correspond le même mot réduit. Ainsi on aura construit un algorithme pour la décision du problème des mots. Il consistera de l'application de l'algo-

(1) Les algorithmes pour le traitement des mots dans un alphabet, qui sont ainsi formés d'un système quelconque de substitutions orientées, écrites dans un ordre déterminé, sont dits « normaux ». La théorie des algorithmes normaux, qui présente le plus grand intérêt théorique et pratique, a été fondée par A. A. Markov, membre correspondant de l'Académie des sciences d'U. R. S. S. et exposée dans son livre *Théorie des Algorithmes*.

rithme de la réduction à chacun des deux mots considérés, puis, ensuite, de la comparaison des mots réduits obtenus.

Soient, par exemple, les mots donnés $cacb$ et bb. Cherchons les mots réduits :

1) $cacb$, $cacacc$, $acccacc$, $accacccc$, $accaccccccc$, $acaccccccccc$, $aaccccccccccc$, $ccccccccccccc$, $cccccccccc$, $ccccc$, cc ;

2) bb, $accb$, $accacc$, $acaccccc$, $aacccccccc$, $ccccccc$, $cccc$, Λ.

Conclusion : les mots $caccb$ et bb ne sont pas équivalents car on obtient deux mots réduits différents cc et Λ.

Démonstration de la non-équivalence mutuelle des huit mots réduits.

D'abord, remarquons que si une chaîne déductive donnée conduit d'un mot quelconque R, ne contenant pas la lettre b, au mot S, ne contenant pas non plus cette lettre, on peut en extraire une chaîne déductive, conduisant de R à S, mais telle que dans les mots intermédiaires de la chaîne on ne rencontre pas la lettre b. En effet, si dans tous les mots d'une chaîne déductive donnée on remplace chaque occurrence de la lettre b par le mot acc, on obtient une suite de mots dans laquelle deux mots côte à côte sont contigus (1) (au sens du calcul) ou simplement identiques. Si on enlève maintenant les mots qui se répètent inutilement (parmi ceux qui sont côte à côte),

(1) Ceci n'est pas exact. Voici un contre-exemple

$$\Lambda \text{ — } bb \text{ — } accb \text{ — } accacc.$$

Cette chaîne déductive devient par l'opération indiquée :

$$\Lambda \text{ — } accacc \text{ — } accacc \text{ — } accacc$$

et les deux premiers mots ne sont ni contigus ni identiques mais équivalents. Il faut dire que d'une chaîne déductive où le mot initial et le mot terminal ne contiennent pas la lettre b, on peut *déduire* une chaîne déductive qui ne contient pas cette lettre (*N. d. T.*).

on obtient la chaîne déductive cherchée. Dans les chaînes déductives de ce type, la substitution b — acc n'intervient à aucun moment.

Puis, dans chacune des substitutions permises qui subsistent, le nombre des occurrences de la lettre a dans la partie gauche et le nombre des occurrences dans la partie droite sont en même temps pairs ou en même temps impairs. On a une proposition analogue pour la lettre c. C'est-à-dire que la parité du nombre des occurrences de la lettre a (ou de la lettre c) est un invariant déductif pour les chaînes déductives de la forme indiquée plus haut. Il résulte immédiatement de là qu'aucun des quatre mots réduits, contenant une seule occurrence de la lettre a, n'est équivalent à un des quatre mots réduits qui ne contiennent aucune occurrence de cette lettre. De même, aucun des mots réduits, qui contiennent une ou trois occurrences de la lettre c, n'est équivalent à un mot quelconque qui contient deux ou ne contient aucune occurrence de cette lettre. Il reste donc encore à se convaincre de la non-équivalence des paires suivantes de mots :

$$\Lambda,\ cc\ ;\ c,\ ccc\ ;\ a,\ acc\ ;\ ac,\ accc.$$

Si on avait l'équivalence pour une des trois premières paires, comme conséquence du théorème de ce paragraphe, on aurait l'équivalence de la quatrième. Il suffit donc d'établir la non-équivalence de la paire, ac, $accc$, et c'est ce que nous allons faire tout de suite.

Convenons de la terminologie suivante :

On appelle *indice* d'une *occurrence* quelconque *de la lettre* a dans le mot R le nombre de toutes les occurrences de la lettre c que l'on rencontre à droite de cette occurrence de la lettre a. *L'indice du mot* R est, par définition la somme des indices de toutes les occurrences de la lettre a (1). Cha-

(1) Par exemple, dans le mot $acbca$, la première occurrence à gauche de la lettre a a l'indice 2 ; la deuxième occurrence à gauche de la lettre a a l'indice 0 (à droite il n'y a pas d'occurrence de la lettre c). L'indice du mot est 2.

cune des substitutions aa — Λ et ccc — Λ ne change pas la parité de l'indice d'un mot. En effet, pour la substitution de aa à la place du mot vide, l'indice du mot considéré croît de la somme des indices, égaux entre eux, de ces deux occurrences de la lettre a, c'est-à-dire d'un nombre pair ; pour le remplacement d'une occurrence de aa par le mot vide, l'indice du mot considéré diminue d'un nombre pair.

Quand on substitue $cccc$ à Λ, les indices de certaines occurrences de a augmentent de quatre, les indices des autres occurrences ne changent pas ; au total, l'indice du mot considéré croît d'un nombre pair. Même chose pour l'élimination de $cccc$. La substitution b — acc, de façon évidente, ne change pas la parité de l'indice du mot (1).

Enfin, montrons que la substitution ca — $accc$ change la parité de l'indice du mot. Pour cela, comparons les mots

$$PcaQ \quad \text{et} \quad PacccQ\ ;$$

l'indice de chaque occurrence de a dans la partie P du mot R change juste de 2, et l'indice de l'occurrence de a dans Q ne change pas. Quant à l'indice de l'unique occurrence de a entre P et Q, il change exactement de 3. Au total, l'indice du mot change d'un nombre impair.

Les mots ac et $accc$ ont tous deux des indices de même parité. Donc, s'ils sont équivalents, dans la chaîne déductive correspondante (on peut dire que l'on n'y rencontre pas la lettre b, voir plus haut) il peut y avoir seulement un nombre pair de substitutions ca — $accc$.

Cependant, une telle hypothèse conduit à une contradiction, comme on le voit par le raisonnement suivant. Chaque application de la substitution ca — $accc$ change le nombre des occurrences de la lettre c de 2, donc un nombre pair d'applications de cette substitution change

(1) Il est d'ailleurs inutile de considérer cette substitution, d'après la remarque faite au début de la démonstration (*N. d. T.*).

le nombre des occurrences de la lettre c d'un nombre qui est multiple de 4. Il est clair que la substitution ccc — Λ change le nombre des occurrences de la lettre c juste de 4 et que la substitution aa — Λ ne change pas du tout ce nombre. D'après tout ce que nous venons de dire, nous devons conclure que si $ac \sim accc$, les nombres d'occurrences de la lettre c qui s'y trouvent diffèrent d'un multiple de 4, ce qui, en fait, n'est pas. Ainsi, les mots ac et $accc$ ne sont pas équivalents. Ceci termine l'exposé de l'algorithme proposé.

La résolution détaillée du problème des mots pour un calcul associatif concret, que nous avons effectuée dans l'exemple 4, caractérise en gros les notions et méthodes qui surgissent pour les problèmes de mots cherchés pour d'autres calculs. Il nous reste encore à expliquer le sens interne du problème des mots et sa signification en algèbre moderne. Il est commode de le faire sur un exemple concret.

Prenons un carré quelconque (fig. 9, I). Considérons ses trois *automorphismes*, c'est-à-dire les transformations qui transforment le carré en lui-même :

1) symétrie (image dans un miroir) relativement à un axe vertical passant par le centre O du carré ;

2) symétrie relativement à un axe horizontal passant par le centre O du carré ;

3) rotation dans le sens des aiguilles d'une montre de 90° autour du centre O.

Nous appellerons élémentaires ces transformations et les désignerons par les lettres respectives a, b, c. Sur la figure 9 (III-IV-V) on voit comment change la disposition des sommets du carré (II) pour chacune des transformations élémentaires.

Remarquons que le résultat des exécutions successives de n'importe lequel de deux ou plusieurs automorphismes du carré est encore un automorphisme du carré. Nous nous en tiendrons à la définition, généralement admise, d'après laquelle multiplier deux transformations données (en particulier deux automorphismes du carré) veut dire

exécuter successivement, l'une après l'autre, les deux transformations. Convenons encore de conserver, pour l'opération du produit de transformations, le système usuel d'écriture et aussi le terme de *produit* pour la transformation résultante. Ainsi, par exemple, le produit cc est le résultat de deux rotations successives de 90°, c'est-à-dire une rotation de 180° ; le produit ac, résultat d'une symétrie par rapport à l'axe vertical et d'une rotation postérieure de 90°, est équivalent à une symétrie par rapport à la diagonale gauche (voir fig. 9, I).

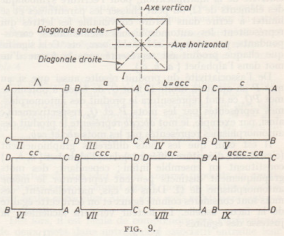


FIG. 9.

Notre multiplication n'est pas commutative : figure 9 (VIII-IX) sont représentées les deux dispositions distinctes des sommets du carré qui prennent naissance par les automorphismes ac, ca, du carré primitif (II). Cependant, elle se rapproche de la multiplication arithmétique par la propriété d'associativité (combinativité) : quelles que

soient les transformations p, q, r, on a l'égalité $(pq)r = p(qr)$. Grâce à cela, dans les produits on peut négliger les parenthèses car, par exemple, $(ac)\,(c)$ et $((ac)c)c)$ donnent le même automorphisme du carré, à savoir la symétrie par rapport à la diagonale gauche.

L'objet de notre étude ultérieure sera l'ensemble Ω constitué des transformations élémentaires a, b, c, et de tous les automorphismes du carré qui peuvent être considérés comme des produits d'un nombre fini (mais arbitraire) de transformations élémentaires. Grâce à l'associativité de la multiplication, pour l'écriture symbolique des éléments de Ω, on peut chasser les parenthèses et se limiter à écrire dans l'ordre convenable les lettres qui représentent les automorphismes élémentaires correspondants, par exemple *abb*, *cabb*, *accc*, etc. Cela signifie que chaque produit est représenté sous la forme d'un mot dans l'alphabet $\{ a, b, c \}$.

De l'associativité du produit résulte aussi que si au mot P on ajoute à droite le mot Q, de façon à obtenir le mot PQ, ce mot représentera le produit des automorphismes représentés par les mots P et Q, respectivement ; ainsi, par exemple, le mot *abccab* représente le produit des automorphismes représentés par les mots *abc* et *cab*.

Il est clair que les mots différents graphiquement (c'est-à-dire d'écriture différente) dans l'alphabet $\{ a, b, c \}$ constituent un ensemble infini ; cependant, des mots graphiquement distincts peuvent représenter le même automorphisme de Ω. Dans ce cas, naturellement, ces mots sont considérés comme égaux et on écrit cette égalité de la façon usuelle. Le lecteur vérifiera facilement la justesse des égalités :

$$b = acc \qquad (1)$$
$$ca = accc \qquad (2)$$

Pour cela, il suffit de comparer les dispositions des sommets du carré qui résultent des transformations représentées par les parties droites et gauches de ces égalités. De plus, on voit facilement que chacun des mots : *aa*, *bb*, *cccc* donne le même automorphisme, à savoir la transformation appelée « transformation identique », pour laquelle tous les sommets restent à leur place antérieure. Puisque cette transformation ne change rien, on la représente aussi rationnellement par le mot vide Λ. Ainsi, on a les égalités :

$$aa = \Lambda \qquad (3)$$
$$bb = \Lambda \qquad (4)$$
$$cccc = \Lambda \qquad (5)$$

La comparaison des égalités (1)-(5) avec les substitutions permises du calcul associatif de l'exemple 4 suggère la proposition suivante, qui constitue le lien entre ce calcul et le système considéré de transformations du carré:

Deux produits d'automorphismes élémentaires du carré donnent la même transformation si, et seulement si les mots qui les représentent sont équivalents dans le calcul de l'exemple 4.

En effet, des égalités (1)-(5) résulte que pour chaque application arbitraire des substitutions permises à un mot arbitraire S, ce mot est transformé en un mot égal. Par exemple, si on applique la substitution $ca \to accc$ au mot *bcac*, on obtient le mot *bacccc* ; mais en vertu de l'associativité du produit, nous pouvons écrire :

$$bcac = b(ca)c \quad \text{et} \quad bacccc = b(accc)c\,;$$

les parties droites sont égales, comme produits de multiplicateurs respectivement égaux, donc les parties gauches sont égales entre elles. Ainsi, *deux mots arbitraires contigus sont égaux.*

Dès lors, il est facile de comprendre que l'équivalence de deux mots dans notre calcul associatif entraîne leur égalité (c'est-à-dire l'identité des automorphismes correspondants). Par conséquent si $S \sim T$, dans la chaîne correspondante deux éléments contigus quelconques sont égaux et donc $S = T$.

La réciproque est vraie : *si deux mots sont égaux, ils sont équivalents.* En effet, si deux mots sont égaux, les mots réduits correspondants sont égaux (cela résulte de

la proposition directe). De plus, on peut vérifier immédiatement que tous les mots réduits donnent des automorphismes mutuellement distincts (voir fig. 9, II-IX, où sont représentées les dispositions des sommets du carré (fig. 9, II) pour les automorphismes correspondants aux huit mots réduits). Donc, si deux mots sont égaux, il leur correspond le même mot réduit et donc ils sont équivalents d'après ce qui a été précédemment démontré. Ainsi, l'équivalence formelle de deux mots dans notre calcul reçoit un sens géométrique concret et la reconnaissance de l'équivalence de deux mots acquiert la valeur de la solution d'un problème géométrique concret. De plus, l'algorithme décrit nous présente une méthode générale de résolution de problèmes géométriques arbitraires d'un type donné.

On se trouve devant une situation analogue avec d'autres calculs, dans lesquels l'équivalence formelle permet aussi une interprétation concrète, géométrique, algébrique ou autre. Sans exagération, on peut dire que dans chaque domaine des mathématiques il existe des théorèmes qui peuvent être formulés, après une certaine élaboration, sous la forme d'affirmations d'équivalence de deux mots dans un certain calcul. Dans ce petit livre, il n'est pas possible de faire le tour de ces questions : certaines explications seront encore données dans la suite de l'exposé (*cf.* chap. 7).

Remarquons qu'à partir de cette interprétation géométrique, qui nous a fourni le problème des mots dans le calcul considéré, on peut maintenant construire un algorithme direct et même quelque peu plus simple. Notamment, il suffit pour chacun de deux produits proposés de réaliser effectivement la suite d'automorphismes correspondants (au moins sur le dessin) et de comparer les résultats.

Exercice

Résoudre le problème des mots pour le calcul associatif dans l'alphabet $\{ a, b \}$ avec les substitutions permises

$$aaa = bb$$
$$bbbb = \Lambda.$$

CHAPITRE 5

MACHINES A CALCULER A CONDUITE AUTOMATIQUE

La production d'un algorithme pour les problèmes d'un type donné (et en particulier d'un algorithme « *bon* », commode) dans les cas où on y a réussi, a dépendu en général de raisonnements subtils et complexes, et demandé un niveau élevé et une grande ingéniosité. Cependant, dès le moment où un tel algorithme est formé, le processus de résolution des problèmes correspondants devient tel qu'il peut être appliqué correctement par un homme qui n'a pas la plus petite notion de l'essence même du problème. On demande seulement que cet homme soit capable d'effectuer les opérations, simples et peu nombreuses, dont est formé le processus et, outre cela, qu'il se laisse guider, consciencieusement et sans murmurer, par la prescription (l'algorithme) qu'on lui donne. Un tel homme agit, comme on dit quelquefois, purement machinalement, en résolvant avec succès un problème arbitraire du type considéré. L'expression « action machinale » n'est employée ici que pour exprimer la définissabilité de l'algorithme ; cependant, grâce aux développements modernes de la science et de la technique, elle a déjà acquis un sens précis. En effet, à la place de l'homme hypothétique qui résout un problème dont il ne comprend pas (ou ne veut pas connaître) le sens, on peut en réalité substituer une machine qui exécute le processus. Une telle machine est une machine à calculer moderne à conduite automatique.

CHAPITRE 13

IMPOSSIBILITÉ D'UN ALGORITHME POUR LE PROBLÈME D'ÉQUIVALENCE DES MOTS

Dans ce paragraphe, on démontre *l'impossibilité d'un algorithme pour décider de l'équivalence des mots dans un calcul quelconque.*

Cette démonstration se fait en deux étapes :

A la première étape (1er point de ce chapitre), on considère les calculs associatifs Π avec substitutions orientées de la forme $P \to Q$ (voir chap. 4). Pour ces calculs, que l'on peut appeler calculs « à un côté », on considère le problème de la traductibilité des mots. On dit que le mot R est traduisible en le mot S, s'il existe une chaîne déductive

$$R_1 \to R_2 \to R_3 \to \ldots \to R_k$$

où R_1 est R, R_k est S, et où la flèche indique que l'on passe d'un mot au suivant en appliquant une seule fois une substitution orientée. On démontrera qu'il n'existe pas d'algorithme pour décider de la traductibilité des mots dans un calcul à un côté arbitraire. De pair avec les calculs Π, nous considérons les calculs Π'. On obtient un calcul Π' à partir du calcul Π correspondant, en remplaçant chacune des substitutions orientées de la forme $P \to Q$ par une substitution non orientée de la forme $P — Q$.

Il est clair que si chacun des deux mots R, S est traductible en l'autre dans Π, ces mots sont équivalents dans Π'. La réciproque n'est pas vraie, en général, car pour établir l'équivalence, on admet aussi des chaînes déductives, dans lesquelles, avec les substitutions données de la forme $P \to Q$, sont permises aussi les substitutions de la forme $Q \to P$. Donc, le résultat obtenu pour les calculs à un côté ne s'étend pas automatiquement à des calculs arbitraires.

A la deuxième étape (2e point de ce chapitre) de la démonstration cette difficulté est précisément surmontée et on établit le théorème de l'insolubilité pour le problème de l'équivalence.

1. — Impossibilité d'un algorithme pour décider de la traductibilité des mots.

Théorème 1. — *Il n'existe pas d'algorithme qui permette de déterminer, pour une paire arbitraire de mots, R, S, dans un calcul arbitraire, si R est ou non traductible dans S.*

DÉMONSTRATION

La démonstration du théorème 1 consiste à réduire le problème de la traductibilité pour les machines de Turing au problème de la traductibilité pour les calculs à un côté. Puisque le premier est algorithmiquement insoluble il en est ainsi du second. Les notions et constructions, que nous introduisons plus bas, sont précisément destinées à la réduction du premier problème au second.

Considérons une configuration d'une machine de Turing. Convenons d'appeler *actives* dans la configuration considérée les cases suivantes :

a) la case vue ;

b) les cases qui contiennent des lettres (différentes du signe vide Λ) ;

c) chaque case à gauche et à droite de laquelle il y a des cases du type *a*) ou *b*).

L'ensemble de toutes les cases actives forme une partie ininterrompue du ruban — sa *partie active*. On a représenté figure 26 quelques configurations et marqué les parties actives correspondantes du ruban. Dans la configuration de la figure 26 *a*, la case vue n'est pas extrême, c'est-à-dire qu'à sa droite et à sa gauche on trouve encore des cases de la partie active du ruban. Nous appellerons une telle configuration, configuration *profonde*, à la différence des configurations du type de la figure 26 *b*, de la figure 26 *c*, de la figure 26 *d*, que nous appellerons respectivement configuration *gauche*, *droite*, *isolée*.

Supposons que l'alphabet extérieur de la machine soit :

$$s_1,\ s_2,\ \ldots,\ s_m$$

et l'alphabet intérieur :

$$q_1,\ q_2,\ \ldots,\ q_k.$$

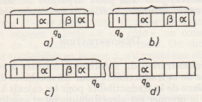


FIG. 26.

On utilisera aussi la lettre h (qui n'appartient pas à ces alphabets) et qui sert à marquer les extrémités de la partie active du ruban.

On peut représenter chaque configuration par un mot hRh, où R est un mot formé comme on l'a fait au chap. 11.

Ces mots seront appelés K-mots (de configuration). Par exemple, aux configurations de la figure 26 correspondent les mots

$$h \mid \Lambda\, \alpha\, \Lambda\, q_0\, \beta\alpha h \qquad h \mid q_0\, \Lambda\, \alpha\, \Lambda\, \beta\alpha h$$
$$h \mid \Lambda\, \alpha\, \Lambda\, \beta\alpha\, \Lambda\, q_0\, h \qquad h\alpha q_0\, h.$$

Confrontons maintenant la machine M au calcul Π_M ainsi formé :

1. — L'alphabet de Π_M est formé de la lettre h et de toutes les lettres de l'alphabet de la machine M. Remarquons qu'alors que chaque K-mot est un mot dans le calcul Π_M, tous les mots dans Π_M ne sont pas des mots de configuration. Ainsi, par exemple, dans le mot $hs_1q_1s_1q_1h$, on rencontre deux fois la lettre de l'alphabet intérieur q_1, ce que ne peut être le fait d'un K-mot.

2. — Les substitutions (orientées) dans Π_M sont construites précisément de façon à assurer les transformations des K-mots qui correspondent aux transformations de configurations dans la machine suivant les commandements de cette machine. Expliquons en détail comment cela se réalise.

Considérons un commandement de la forme

$$sq \to s'\, Nq' \qquad (1)$$

lequel ne change pas la case vue. Il est facile de voir que ce commandement ne change pas la partie active du ruban. Si on compare les K-mots avant et après l'exécution du commandement, on voit que la paire de lettres sq est simplement changée en la paire de lettres $s'\,q'$. Nous ferons correspondre à ce commandement (1) de la machine de Turing la substitution orientée

$$sq \to s'\, q'.$$

Si le commandement prescrit un mouvement, il peut, selon le caractère de la configuration (profonde,

gauche, etc.) et du mouvement (à gauche, à droite), se produire un changement de la partie active du ruban.

Pour cette raison on ne peut indiquer une substitution unique qui serait, dans le calcul, l'équivalent du commandement (au sens où cela se réalisait pour le commandement (1)). Cependant, comme on le verra plus bas, on peut indiquer un système fini de substitutions qui, dans son ensemble, est équivalent au commandement donné.

Exemple.

Conformément au commandement

$$\mid q_0 \to \Lambda\, Dq_2$$

du schème fonctionnel pour l'addition, on effectue les transformations de configurations indiquées, figure 27.

Figure 27 *a*, la partie active du ruban n'a pas changé. Figure 27 *b*, et figure 27 *c*, elle a subi une réduction (à gauche) et un allongement (à droite) respectivement. Figure 27 *d*, on a représenté une partie active de ruban variable sans changement de grandeur.

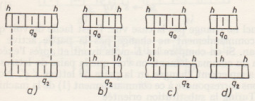


FIG. 27.

Pour les K-mots correspondants, nous avons la transformation donnée par le tableau 3.

TABLEAU 3

K-mot de départ	K-mot transformé
$h \mid\mid q_0 \mid h$	$h \mid \Lambda \mid q_2 h$
$h \mid q_0 \mid h$	$h \mid q_2 h$
$h \mid\mid q_0 h$	$h \mid \Lambda\Lambda\, q_2 h$
$h \mid q_0 h$	$h\, \Lambda\, q_2 h$

Il est facile de voir que les mots de la colonne de droite ne proviennent pas de l'application d'une seule et même substitution orientée aux mots correspondants de la colonne de gauche.

Montrons maintenant comment construire un système de substitutions orientées correspondant aux commandements de la forme

$$sq \to s'\, Dq' \qquad (2)$$

(on étudiera de façon analogue le cas des commandements de la forme $sq \to s'\, Gq'$).

Introduisons les notations suivantes : si une case, contiguë à gauche à la case vue, est active, nous désignerons par σ la lettre qui s'y trouve ; de même on désigne par τ la lettre qui se trouve dans la case voisine de droite, si elle est active ; de plus il n'est pas exclu que σ ou τ ou tous les deux en même temps soient le signe vide.

Les substitutions qui correspondent aux commandements (2) peuvent être classées commodément suivant les types de configurations :

1. — Configuration profonde. On a dans le K-mot une occurrence de la forme $\sigma sq\tau$. A chacune de ces occurrences (σ, τ étant des lettres arbitraires de l'alphabet extérieur de la machine) correspond la substitution

$$\sigma sq\tau \to \sigma s'\tau q'.$$

2. — Configuration gauche. Dans les K-mots on a des occurrences de la forme $hsq\tau$. Il leur correspond des substitutions de la forme

$$hsq\tau \to hs'\,\tau q' \quad , \quad \text{si } s' \neq \Lambda,$$
$$hsq\tau \to h\tau q' \quad , \quad \text{si } s' = \Lambda.$$

La dernière substitution reflète le fait que la case qui contient s cesse d'être active (voir fig. 28).

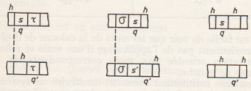


FIG. 28.

FIG. 29.

FIG. 30.

3. — Configuration droite. Dans les K-mots on a des occurrences de la forme σsqh, auxquelles correspondent des substitutions

$$\sigma sqh \to \sigma s'\, \Lambda\, q'\, h$$

qui reflètent l'allongement vers la droite de la partie active du ruban (voir fig. 29).

4. — Configuration isolée. Dans les K-mots on a des occurrences $hsqh$, auxquelles correspondent les substitutions :

$$hsqh \to hs'\, \Lambda\, q'\, h \quad , \quad \text{si } s' \neq \Lambda,$$
$$hsqh \to h\, \Lambda\, q'\, h \quad , \quad \text{si } s' = \Lambda.$$

La dernière substitution reflète le changement de l'unique case active (voir fig. 30).

Ainsi s'achève la liste des substitutions orientées qui correspondent dans le calcul Π_M au commandement de la machine de la forme (2).

Exemple.

Construire, pour la machine de Turing Σ, qui réalise l'addition (cf. chap. 9), le calcul correspondant Π_Σ.

Alphabet de Π_Σ :

$$\mid,\ \Lambda,\ *,\ h.$$

Au commandement $\Lambda\, q_2 \to \mid Nq_1$ correspond la substitution

$$\Lambda\, q_2 \to \mid q_1.$$

Au commandement $\mid q_0 \to \Lambda\, Dq_2$ correspondent les substitutions :

Profondes :

$$\begin{array}{ll} \mid\mid q_0 \mid & \to \mid \Lambda \mid q_2 \\ \mid q_0\, \Lambda & \to \mid \Lambda\, \Lambda\, q_2 \\ \mid q_0\, * & \to \mid \Lambda * q_2 \\ \Lambda \mid q_0 \mid & \to \Lambda\Lambda \mid q_2 \\ \Lambda \mid q_0\, * & \to \Lambda\Lambda * q_2 \\ \Lambda \mid q_0\, \Lambda & \to \Lambda\Lambda\Lambda\, q_2 \\ * \mid q_0 \mid & \to * \Lambda \mid q_2 \\ * \mid q_0\, \Lambda & \to * \Lambda\Lambda\, q_2 \\ * \mid q_0\, * & \to * \Lambda * q_2 \end{array}$$

Gauches :

$$\begin{array}{ll} h \mid q_0 \mid & \to h \mid q_2 \\ h \mid q_0\, \Lambda & \to h\, \Lambda\, q_2 \\ h \mid q_0\, * & \to h * q_2 \end{array}$$

Droites :

$$\begin{array}{ll} \mid\mid q_0\, h & \to \mid \Lambda\Lambda\, q_2\, h \\ \Lambda \mid q_0\, h & \to \Lambda\Lambda\, q_2\, h \\ * \mid q_0\, h & \to * \Lambda\Lambda\, q_2\, h \end{array}$$

Isolée :

$$h \mid q_0\, h \to h\, \Lambda\, q_2\, h.$$

On peut indiquer de la même façon les substitutions qui correspondent aux autres commandements.

Remarquons maintenant les propriétés suivantes du calcul Π_M, construit pour la machine M considérée.

Proposition 1. — *Chaque K-mot pour la machine M est un mot dans* Π_M.

Proposition 2. — *Si* $\widetilde{\mathfrak{A}}$ *est un K-mot, décrivant la configuration* $\mathfrak{A}$, *il ne lui est applicable dans* Π_M *qu'une substitution au plus. Cette substitution transforme* $\mathfrak{A}$ *en un mot* $\widetilde{\mathfrak{B}}$ *qui décrit la configuration* $\mathfrak{B}$, *en laquelle la machine transforme* $\mathfrak{A}$.

Proposition 3. — *Si* $\mathfrak{A}$ *est une configuration terminale de la machine M, aucune substitution n'est applicable à* $\widetilde{\mathfrak{A}}$.

De ces propositions résulte immédiatement que la question de la traductibilité d'une configuration $\mathfrak{A}$ en une autre configuration $\mathfrak{B}$ de la machine M est équivalente à la question de la traductibilité du K-mot $\widetilde{\mathfrak{A}}$ en le K-mot $\widetilde{\mathfrak{B}}$ dans le calcul Π_M. En d'autres termes, le problème de décider de la traductibilité pour les machines de Turing se réduit au problème de décider de la traductibilité pour les calculs à substitutions orientées. *Ainsi se termine la démonstration du théorème* 1.

Si pour $\mathfrak{B}$ on ne prend que des configurations terminales de la machine M, il résulte de la réductibilité mentionnée plus haut le :

Théorème 2. — *Il n'existe pas d'algorithme qui permette de déterminer, pour un calcul arbitraire à substitutions orientées et pour une paire arbitraire de mots* $\widetilde{\mathfrak{A}}$ *et* $\widetilde{\mathfrak{B}}$, *dont le deuxième est terminal, si* $\widetilde{\mathfrak{A}}$ *est traductible en* $\widetilde{\mathfrak{B}}$ *ou non.*

2. Insolubilité du problème de l'équivalence.

Soient R et S deux K-mots dans un calcul Π_M. Si R est traductible en S avec des substitutions orientées, à plus forte raison R et S sont équivalents dans Π_M. De nouvelles équivalences apparaissent-elles s'il y a dans Π_M des substitutions non orientées ? La réponse à cette question est donnée par le lemme suivant :

Lemme. — *Si S est un K-mot terminal et R est équivalent à S dans* Π_M' *(on permet les substitutions non orientées), R est traductible en S par des substitutions orientées seulement.*

De ce lemme résulte immédiatement l'impossibilité d'un algorithme pour résoudre les problèmes d'équivalence des mots dans les calculs associatifs. En effet, cet algorithme résoudrait en même temps aussi le problème de la traductibilité des mots, en mots terminaux, au moyen de substitutions orientées. Le théorème 2 affirme l'impossibilité d'un tel algorithme.

Démonstration du lemme

Si $R \sim S$, il existe une chaîne déductive allant de R à S :

$$R = R_1 — R_2 — R_3 — \cdots — R_{k-1} — R_k = S. \quad (3)$$

Soient R_j, R_{j+1} deux mots contigus de cette chaîne. Si le passage de R_j à R_{j+1} se fait par application d'une substitution orientée de la forme $P \to Q$, nous écrirons $R_j \to R_{j+1}$; si ce passage se fait en remplaçant dans R_j les occurrences de la partie droite d'une substitution permise par la partie gauche correspondante de cette substitution (ou, ce qui revient au même, si R_{j+1} devient R_j par application d'une substitution orientée) nous écrirons $R_j \leftarrow R_{j+1}$. Considérons maintenant les cas suivants possibles pour un triple de mots dans la chaîne (3) :

$$R_{j-1} \leftarrow R_j \to R_{j+1} \quad (4)$$

$$R_{j-1} \to R_j \leftarrow R_{j+1}. \quad (5)$$

En vertu de la proposition 2, les mots R_{j-1} et R_{j+1} dans le cas (4) coïncident, car au mot R_j n'est applicable qu'une seule substitution. Donc, quand on trouve un tel triple dans la chaîne déductive, on peut la réduire en enlevant deux mots (par exemple R_{j-1} et R_j). Dans le cas (5) les

mots R_{j-1} et R_{j+1} peuvent être en effet différents ; en termes de machines de Turing, ceci correspond au fait qu'une configuration donnée de la machine peut provenir de plusieurs configurations différentes.

Revenons maintenant à la chaîne (3). Puisque R_k est une configuration terminale, on ne peut avoir que $R_{k-1} \to R_k$ (voir proposition 3). Si, dans la chaîne considérée, toutes les flèches sont dirigées vers la droite, le lemme est déjà démontré. S'il existe des flèches dirigées vers la gauche, supposons que la dernière qui se rencontre soit devant le $j^{\text{ième}}$ mot. On a alors le triple

$$R_{j-1} \leftarrow R_j \to R_{j+1}$$

qui peut être réduit à deux mots, et nous obtenons une chaîne déductive plus courte qui conduit de R à S. En continuant ce procédé de raccourcissement des chaînes, nous arrivons à une chaîne qu'il n'est plus possible de raccourcir, puisque toutes les flèches qui s'y trouvent sont orientées vers la droite. Ainsi, R est réduit à S par des substitutions orientées.

REMARQUES FINALES

Faisons, en conclusion, quelques remarques générales.

1. — D'abord, les théorèmes d'insolubilité algorithmique de telle ou telle classe de problèmes ne fournissent pas prétexte à tomber dans l'agnosticisme. En effet, chaque théorème semblable concerne une classe entière de problèmes et établit l'insolubilité de tous les problèmes de cette classe par une méthode effective — un algorithme — unique.

Ceci ne veut pas du tout dire que parmi les problèmes isolés réunis dans cette classe, il y en a qui sont insolubles. Par exemple, il ne faut pas comprendre le théorème démontré plus haut comme exprimant qu'il existe un chiffre dont on ne peut, en principe, établir qu'il est autoapplicable ou non.

Cela veut dire seulement que le type considéré de problèmes est si général et si large qu'il n'existe pas un algorithme unique pour la résolution de tous les problèmes du type considéré. Dans ce cas, le but des recherches mathématiques est la création continuelle d'algorithmes de plus en plus larges, permettant de réduire à un calcul automatique des sous-classes de plus en plus vastes de problèmes du type considéré.

2. — Deuxièmement, les théorèmes sur l'insolubilité algorithmique montrent que les mathématiques ne se réduisent pas à la construction d'algorithmes, que le processus de connaissance en Mathématiques ne peut être

finalement automatisé. Déjà, dans divers domaines, relativement étroits, des mathématiques (comme la théorie des groupes à un nombre fini de générateurs, etc.) apparaissent des séries de problèmes qu'aucun automate (c'est-à-dire aucune machine de Turing avec un nombre fini de positions et une mémoire finie) n'est capable de résoudre. Bien plus absurde encore serait l'affirmation qu'une machine puisse remplacer le travail créateur du savant.

3. — Il faut, en outre, reconnaître que le domaine d'application des processus algorithmiques est très large et qu'il ne concerne pas seulement les processus de calcul qu'on rencontre en mathématiques. De plus, pour de nombreux processus, que l'on considère habituellement comme très pénibles et très complexes, on peut théoriquement construire des algorithmes dont l'idée est assez simple ; pratiquement donc, les difficultés que l'on rencontre pour la réalisation de ces processus sont liées à ce que les règles de l'algorithme sont très longues et demandent un nombre extrêmement grand d'opérations (bien que ces opérations, en elles-mêmes, soient simples). Cette remarque s'applique en particulier aux processus des jeux (et en particulier au jeu d'échecs), où le succès, dans beaucoup de cas, dépend de l'habileté à passer en revue un plus grand nombre de variantes pour le choix de la variante optimale.

Avec la création des machines à calculer à fonctionnement rapide nous avons considérablement agrandi le nombre des algorithmes pratiquement réalisables.

4. — Enfin, reportons encore une fois notre attention sur le fait que chaque machine à calculer, physiquement réalisable, ne peut être considérée que comme un modèle approché de machine de Turing. En effet, dans les machines réelles, l'étendue de la mémoire extérieure est limitée, alors que dans le schème d'une machine de Turing figure un ruban sans fin. Bien entendu, la réalisation technique d'une mémoire illimitée est impossible, mais un agrandissement considérable de l'étendue de la mémoire dans les machines, par rapport au niveau déjà atteint, est

non seulement désirable mais encore tout à fait possible. En fait, dans cette direction de l'allongement de l'étendue de la mémoire extérieure et de la vitesse du calcul, on peut s'attendre à de grands progrès ultérieurs dans l'évolution des automates calculateurs.

Dépôt légal N° 4302, 3e trimestre 1963
Imprimé en France
Imp. Jouve, 15, rue Racine, PARIS VIe.

TRAHTENBROT B. A. **Algorithmes et machines à calculer**
Paris, *Dunod,* 1963, 17 cm., 149 p. Tabl. (Coll. *Monographies Dunod*)

Excellente introduction, la théorie des algorithmes, qui, sans nécessiter de grandes connaissances, demande une solide aptitude à suivre jusqu'au bout un raisonnement simple mais très abstrait.

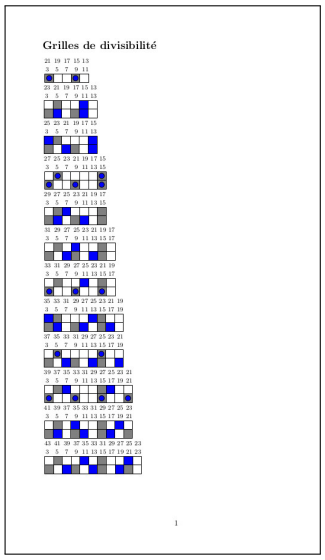
Intuitivement un algorithme est une notion vague qui se définit comme un problème arbitraire d'une classe déterminée de problèmes. Une machine à calculer réelle peut résoudre les problèmes d'une certaine classe, en suivant le processus donné par l'algorithme de cette classe.

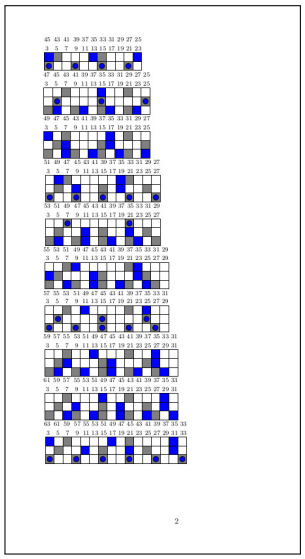
Le biais de la machine de Turing permet de donner une définition mathématique de la notion d'algorithme.

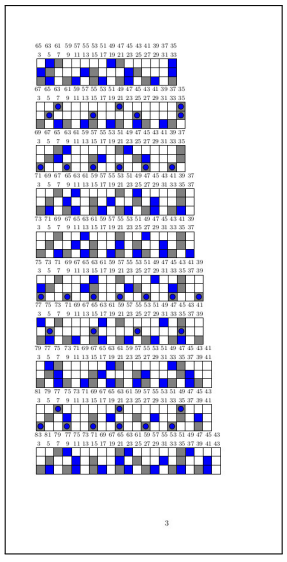
Il existe des classes de problèmes algorithmiquement insolubles. Ce qui montre que les machines ne remplacent pas l'homme et ne le remplaceront pas aussi longtemps qu'elles seront fondées sur les principes actuels.

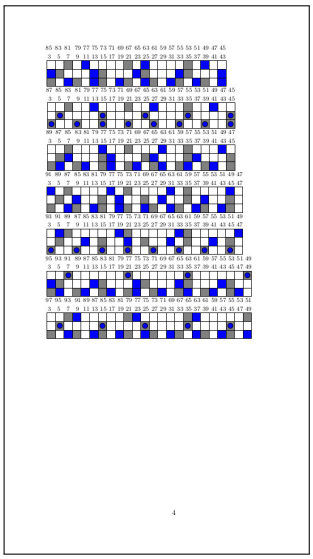
R. N.

- 04.02.2014 : conjecture de Goldbach, mots booléens, parité, imparité, invariant (229) imparite.pdf
- 30.01.2014 : Conjecture de Goldbach, mots booléens, invariant (228) moBoolInv.pdf
- 18.01.2014 : Leçons de solfège et de piano (227) Quignard.pdf
- 18.01.2014 : Conjecture de Goldbach, mots booléens et LRQ (226) moBoolelrq.pdf
- 13.01.2014 : Une drôle de relation (225) relation.pdf
- 12.01.2014 : Tirettes de Charles-Ange Laisant (224) Laisant.pdf tirettes-de-Laisant.pdf
- 11.01.2014 : Mots cycliques (mots gris, mots bleus) conservant une lettre 0 par permutations (223) mocycliques.pdf
- 04.01.2014 : Anagrammes de mots de restes (222) anamoreste.pdf
- 30.12.2013 : Pierre Boulez : rechercher des formes (221) Boulez.pdf (221) Grilles grilles24-100.pdf

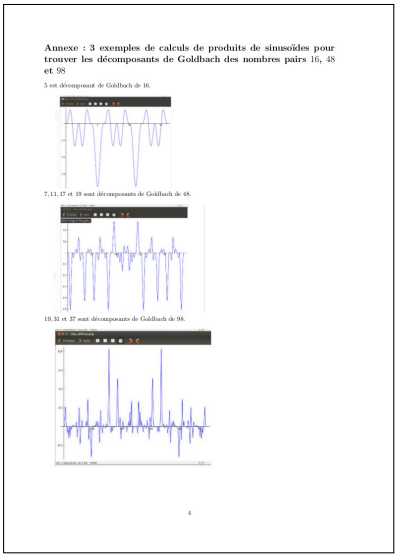

Grilles de divisibilité
1

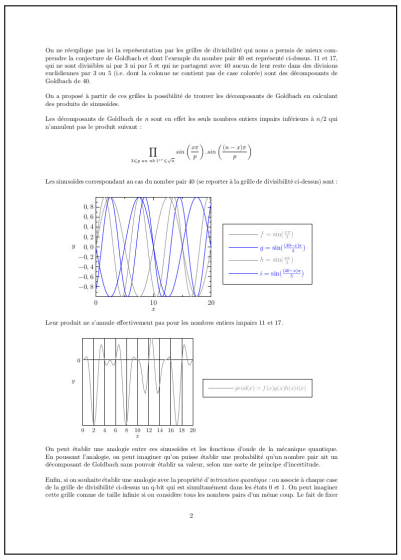

2


3



- 23.12.2013 : Analogie (220) analogie.pdf
- 21.12.2013 : Continuer de suivre Galois (219) invariante.pdf retrouve-galois.pdf
- 18.12.2013 : Yves Meyer (que je remercie) présentera la preuve d'Harald Helfgott le 30 janvier, lors d'une conférence intitulée "Preuve de la conjecture de Goldbach", aux lycéens du Lycée Lakanal de Sceaux Yves Meyer a reçu le Prix Abel en 2017. (218)
- Sinusoïdes (217)
- 18.12.2013 : Résumé de l'approche par le produit des sinusoïdes (traitement d'un signal) (216) mai2009.pdf sinusoides.pdf





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

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

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

$$\prod_{3\leq p \text{ et } 3<^{p}\leq\sqrt{n}} \sin\left(\frac{px}{p}\right).\sin\left(\frac{(n-x)\pi}{p}\right)$$

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

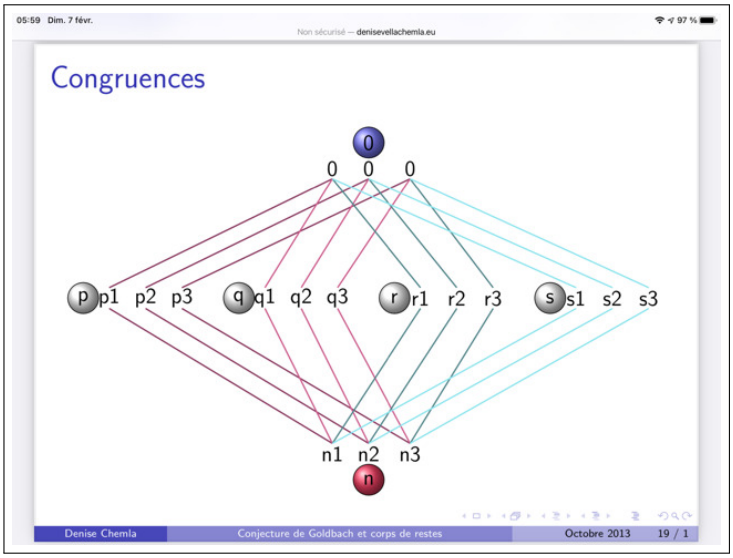
Leur produit ne s'annule effectivement pas pour les nombres entiers impairs 11 et 17.

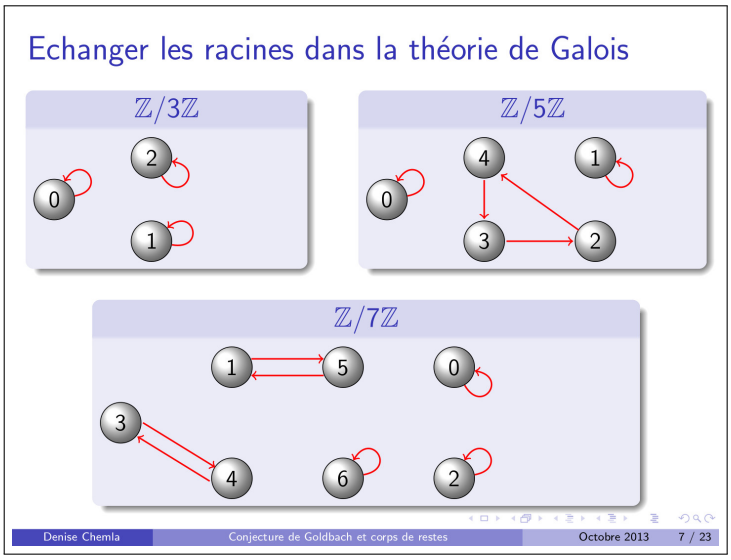
On peut établir une analogie entre ces sinusoïdes et les fonctions d'onde de la mécanique quantique. En poussant l'analogie, on peut imaginer qu'on puisse établir une probabilité qu'un nombre pair ait un décomposant de Goldbach sans pouvoir établir sa valeur, selon une sorte de principe d'incertitude.

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

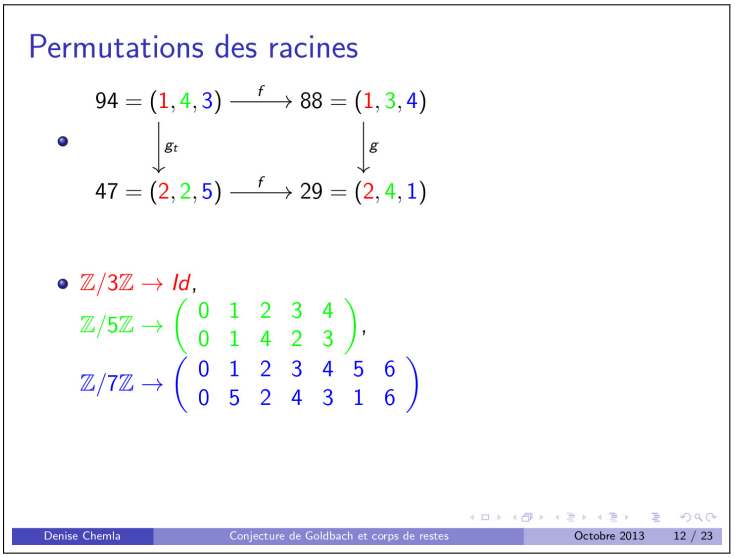
2

- 24.11.2013 : Modélisation spatiale (215) espace2.pdf
- 10.11.2013 : Minimiser / maximiser (214) minimax.pdf
- 06.11.2013 : Approche vectorielle (213) vecto.pdf
- 31.10.2013 : Echanger (212) transp-echanger.pdf



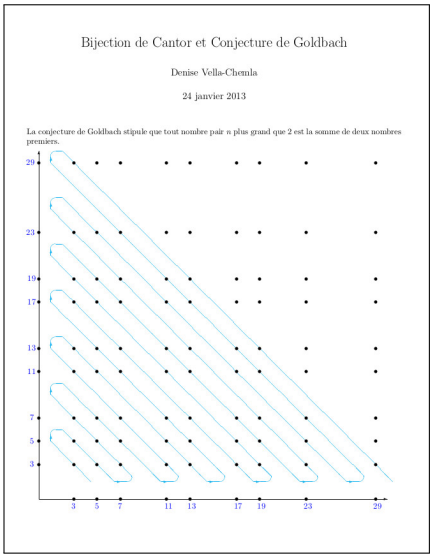


- 31.10.2013 : Note sur l'approche par le transfert d'une solution triviale (211) plonger.pdf



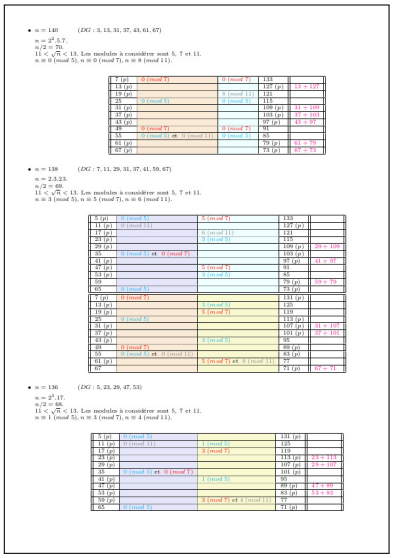
- 24.10.2013 : Localisation en prose (210) apres-visite.pdf
- 13.10.2013 : Dévisser des groupes (209) devissage.pdf
- 22.09.2013 : Combinatoire de congruences (208) combinatoire-de-congruences.pdf
- 13.09.2013 : Pistes à creuser (207) acreuser.pdf
- 24.08.2013 : Division euclidienne et conjecture de Goldbach (206) partage-de-restes.pdf
- 10.08.2013 : Division euclidienne et conjecture de Goldbach (205) diveuclidienne.pdf
- 09.08.2013 : Parité... (204) parite.pdf
- 02.08.2013 : Brisure de symétrie (203) brisure.pdf

- 15.07.2013 : Espace, distance, horloges (202) algebre-espace.pdf
- novembre 2013 à février 2014 : S'intéresser, un peu, à la physique, notamment quantique (201) phys-quant.pdf
- 02.06.2013 : Les livres délivrent. (200) deslivres.pdf
- 01.04.2013 : Minorer le nombre de décomposants de Goldbach (199) derminoDeniseChemla.pdf
- 16.03.2013 : Minorer le nombre de décomposants de Goldbach (198) hetbgp3.pdf
- 05.02.2013 : Equations polynomiales modulaires et conjecture de Goldbach (197) galgolfin.pdf
- 04.02.2013 : Théorie de Galois et conjecture de Goldbach (196) galgol.pdf
- 02.02.2013 : Expérimentations numériques à l'aide du logiciel Gap et du package associé Loops (195) gaploopsexperience.pdf
- 30.01.2013 : Théorie des groupes et Conjecture de Goldbach (remerciements à GreginGre et Archimède du forum Algèbre du site les-mathematiques.net) (194) dextrolevo.pdf
- 28.01.2013 : Où Galois cite la méthode de Libri pour trouver des solutions entières (p.405) (193) GaloisLibrip405.pdf
- 28.01.2013 : Extrait de Libri auquel Galois fait référence (192) Libri.pdf
- 25.01.2013 : Dessin de la bijection de Cantor (191) snake.pdf



- 16.01.2013 : Recherche de suites les plus longues de nombres respectant certaines contraintes, articles de Legendre et Desboves (190) legdebtranslation.pdf
- 11.01.2013 : Minorer par le nombre de décompositions de Goldbach des doubles de nombres premiers qui vérifient trivialement la conjecture. (189) comparatif.pdf

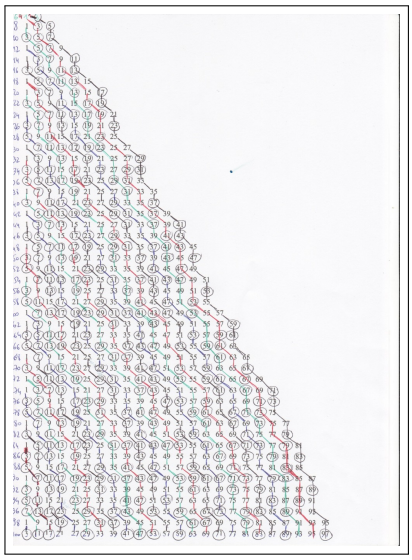
- 08.01.2013 : Idem mais en notant les divisibilités pour la seconde passe plutôt que les congruences à n (188) metdeszeros.pdf
- 08.01.2013 : Le double crible, Brun y a pensé en 1919. (187) Brun.pdf
- 05.01.2013 : Séparer les problèmes, selon Pólya : les 6m, les 6m+2, les 6m+4 (186) couleurpartout6m.pdf couleurpartout6m+2.pdf couleurpartout6m+4.pdf
- 30.12.2012 : Remettre les nombres dans l'ordre pour bien voir les récurrences, mais on ne sait toujours pas comment relier les deux colonnes... (185) couleurpartout.pdf



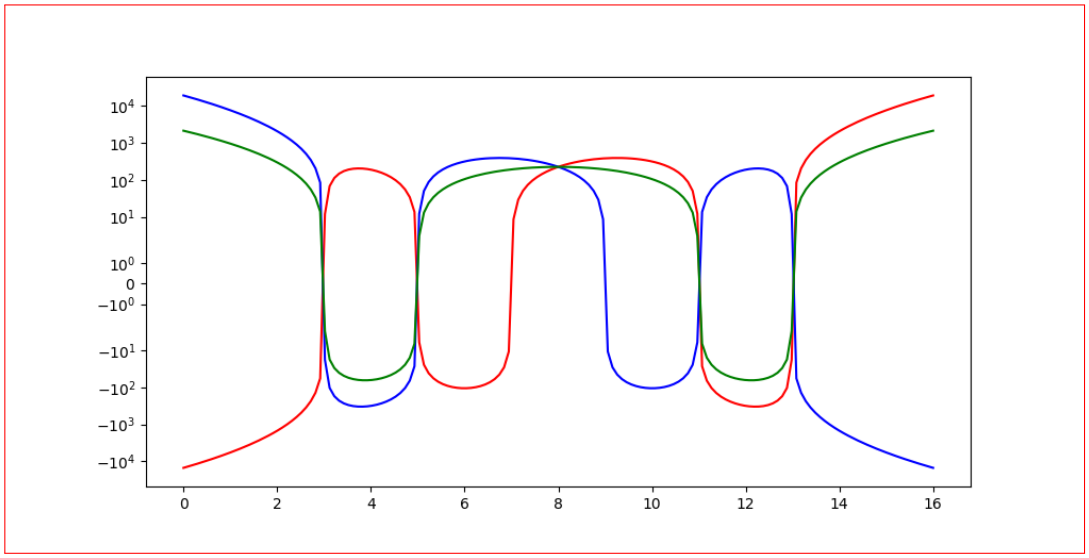
- 27.12.2012 : Desboves critique Legendre (1855) (184) legendrecritiquepardesboves.pdf
- Noël 2012 : Diaporama : Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair (183) CGtranspnoel2012.pdf
- Noël 2012 : Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair (182) CGnoel2012.pdf
- Christmas 2012 : Slides : An algorithm to obtain an even number's Goldbach components (181) GCtranspnoel2012$_e$*n.pdf*
- Christmas 2012 : An algorithm to obtain an even number's Goldbach components (180) GCtranspnoel2012$_e$*n.pdf*
- 24.12.2012 : Un extrait du tome II de la Théorie des nombres de Legendre (179) legendrepa.pdf
- 19.12.2012 : Etude de cas (178) fincas_144_26.pdf
- 19.12.2012 : Case study (177) fincases_144_26.pdf
- 19.12.2012 : Diaporama : Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair (176) CGAlgo.pdf

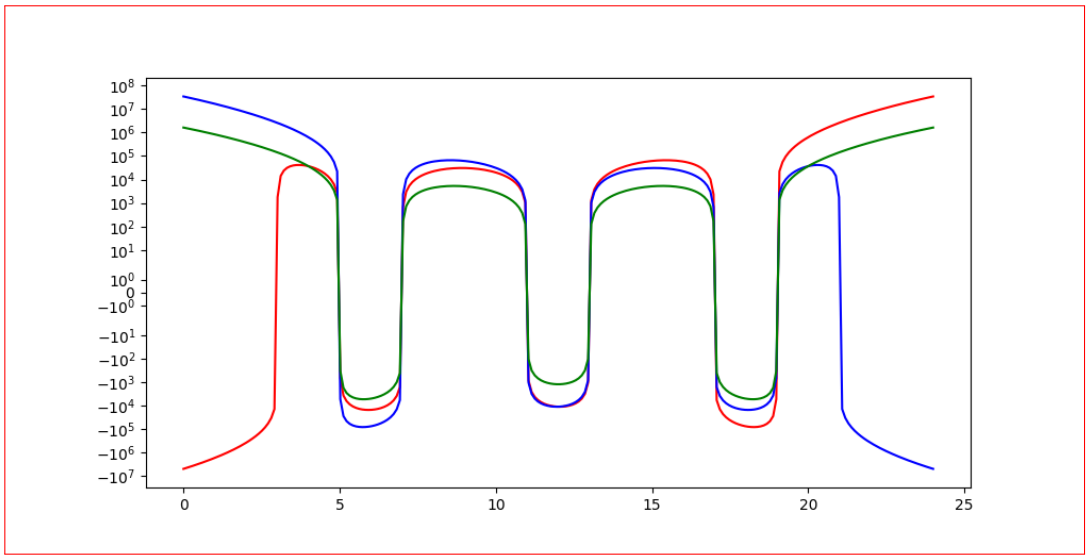
- 19.12.2012 : Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair (175) vfalgogcsansbij.pdf
- 19.12.2012 : Slides : An algorithm to obtain an even number's Goldbach components (174) CGAlgo$_e$*n.pdf*
- 19.12.2012 : An algorithm to obtain an even number's Goldbach components (173) algogcsansbij.pdf
- 04.12.2012 : Application double du crible d'Eratosthène pour trouver les décomposants de Goldbach d'un nombre pair (172) derdoublecrible.pdf
- 04.12.2012 : Etude de cas (171) casdoublecrible26_144.pdf
- 01.12.2012 : Les décomposants de Goldbach de x se trouvent par application double du crible d'Eratosthène (170) doublecrible.pdf
- 01.12.2012 : Chercher une démonstration par récurrence (169) recurrence.pdf
- 01.12.2012 : Les progressions arithmétiques, c'est extra ! (168) extra.pdf
- 10.11.2012 : (diaporama) Etude élémentaire de la conjecture de Goldbach (167) reecriture.pdf
- 07.10.2012 : Une méthode originale de David Angell pour calculer la résiduosité quadratique d'un nombre à un autre (166) s9.pdf
- 01.09.2012 : Méthode quasi-exhaustive (165) combilineaires.pdf
- 14.07.2012 : (diaporama) Etude élémentaire de la conjecture de Goldbach (remerciements à Cyril qui m'a bien aidée à les améliorer) (164) pistegoldbachgauss2.pdf
- 07.07.2012 : Découverte d'une loi tout extraordinaire par rapport à certaines sommes de restes des nombres premiers (163) decouvsommerestes.pdf
- 04.07.2012 : Tentative ratée de minoration probabiliste pour Goldbach (162) minoproba.pdf
- 02.07.2012 : (diaporama) Etude élémentaire de la conjecture des nombres premiers d'écart 2 (161) pistegemeauxgauss.pdf
- 30.06.2012 : Infinité de l'ensemble des nombres premiers d'écart 2, conjecture de Goldbach et un lemme de Gauss (article 127) (160) gemeauxgauss.pdf
- 24.06.2012 : (diaporama) Etude élémentaire de la conjecture de Goldbach (159) minipiste.pdf
- 15.06.2012 : Conjecture des nombres premiers d'écart 2, construction de nombres pairs juste entre deux nombres premiers compris entre deux primorielles successives (à revoir) (158) gigognegemeaux.pdf
- 14.06.2012 : Conjecture des nombres premiers d'écart 2 et argument d'Euclide (note reprise) (157) euclide2gemeaux.pdf

- 13.06.2012 : Conjecture des nombres premiers d'écart 2 et argument d'Euclide (note) (156) euclidegemeaux.pdf
- 12.06.2012 : Conjecture des nombres premiers d'écart 2 et diagonale de Cantor (note) (155) dergemeaux.pdf
- 07.06.2012 : Génération de nombres premiers d'écart 2 (154) generegemeaux.pdf
- 06.06.2012 : Infinitude de l'ensemble des nombres premiers d'écart 2 (une idée provenant de l'exercice consistant à démontrer l'infinitude de l'ensemble des nombres premiers de la forme 6k+1) (153) trianglePascal.pdf
- 06.06.2012 : Versions anglaises (152) may2012.pdf minenglish.pdf PascalTriangleEnglish.pdf
- 23.05.2012 : Infinitude de l'ensemble des nombres premiers d'écart 2 (reprise) (151) infgemeaux.pdf
- 30.04.2012 : (diaporama) La piste qui me semble la bonne, depuis longtemps (150) bonnepiste.pdf
- 30.04.2012 : (diaporama) Les autres pistes que j'ai suivies (149) autrespistes.pdf
- 30.04.2012 : (diaporama) La piste que je veux suivre (148) bonnepiste.pdf
- 24.04.2012 : Retour aux congruences (147) j2442012.pdf
- 20.04.2012 : Décompositions de Goldbach et transitivité (146) j2042012.pdf
- 16.04.2012 : Lier décomposants de Goldbach et non-résidus quadratiques (145) j16-4-2012.pdf
- 09.03.2012 : Début d'une récurrence (144) j932012.pdf
- ♥ 01.01.2012 : Bonne année 2012... (143) (nullité déterminant matrice de Sylvester) j112012.pdf
- 25.12.2011 : Nullité du déterminant d'une matrice de Sylvester (142) noel2011.pdf
- 11.12.2011 : Invariance de polynômes (141) resolubles.pdf
- 27.11.2011 : Algorithme combinatoire (140) d271111.pdf
- 25.11.2011 : Compter des nombres dans des lignes (139)



- ♥ 23.11.2011 : Une vision plus algorithmique de la conjecture de Goldbach (138) (récurrence sur une seule séquence de nombres) m231111.pdf
- ♥ 20.11.2011 : Rester éberluée face aux polynômes (137) d201111.pdf
- 16.11.2011 : La conjecture de Goldbach est peut-être vraie à cause de la Théorie de Galois (136) m161111.pdf
- ♥ 11.11.2011 : En attendant le 7 juin 2012 (les 270 ans de la conjecture de Goldbach), utiliser les équations algébriques pour trouver les décomposants de Goldbach... (135) j111111.pdf¡BR¿ réétudié en mai 2025 : mardi16mai-pgcd.pdf





- ♥ 06.11.2011 : Une dernière idée : utiliser la théorie de Galois pour trouver les décomposants de Goldbach... (134) j6112011.pdf
- ♥ 31.10.2011 : Une dernière idée : utiliser la théorie de Galois pour trouver les décomposants de Goldbach... (133) j31102011.pdf
- 30.10.2011 : Conjecture de Goldbach d'un point de vue analytique (132) analyse.pdf
- 28.10.2011 : On trouve toujours un non-résidu quadratique de n qui fournisse une décomposition de Goldbach de n (131) j28102011.pdf
- 25.10.2011 : Une nouvelle tentative pour prouver que tout nombre pair supérieur à 2 est la somme de deux nombres premiers
- (où l'on repart du côté des résidus et non-résidus quadratiques) qui n'aboutit toujours pas. (130) j25102011.pdf
- 22.10.2011 : Une nouvelle tentative, utilisant le produit des unités de n, de prouver que tout nombre pair supérieur à 2 est la somme de deux nombres premiers, mais qui n'aboutit pas non plus. (129) j22102011.pdf
- 05.10.2011 : La racine carrée d'un résidu quadratique inversible de n fournit une décomposition de Goldbach de n. (128) octobre5.pdf
- 03.10.2011 : Tables de visualisation des décompositions de Goldbach, des résidus et non-résidus quadratiques de n, tous premiers à n (127) tables-unites.pdf
- 03.10.2011 : Tables de visualisation des décompositions de Goldbach, des résidus et non-résidus quadratiques de n, tous premiers à n (126) tables-unites.pdf
- 01.10.2011 : Quel est le nombre de résidus quadratiques de n qui sont premiers à n ? (125) formule-nb-resid-quad-premiers-a-n.pdf

- 28.09.2011 : Il existe un non-résidu de n dont le carré modulo n est premier à n et qui fournit une décomposition de Goldbach de n. (124) non-resid-n.pdf

- 27.09.2011 : Bicentenaire de la naissance d'Evariste Galois, le 25.10.2011. (123)

La tête dans les nombres...

Accueil Notes Pages Autre

Je voudrais ici recopier un extrait d'une superbe biographie de Galois par Alexandre Astruc, publiée aux éditions Flammarion en 1994.

Astruc écrit (p.157) que "communiquer ses découvertes, être reconnu par ses pairs, telles sont les idées fixes de tout savant, et Galois ne fait pas exception à cette règle".

Un peu plus loin, il cite intégralement la préface de Galois à ses "deux mémoires d'analyse pure". Je voudrais seulement ici transmettre la fin de cette préface car elle préfigure le partage actuel de la connaissance et que cette notion de partage m'est chère.

extrait de la préface d'Evariste Galois à ses "deux mémoires d'Analyse Pure" :

[On doit prévoir que, traitant des sujets aussi nouveaux, hasardé dans une voie aussi insolite, bien souvent des difficultés se sont présentées que je n'ai su vaincre. Aussi, dans ces deux mémoires et surtout dans le second qui est plus récent, trouvera-t-on souvent la formule : "Je ne sais pas." La classe des lecteurs dont j'ai parlé au commencement* ne manquera pas d'y trouver à rire. C'est que malheureusement on ne se doute pas que le livre le plus précieux du plus savant serait celui où il dirait tout ce qu'il ne sait pas, c'est qu'on ne se doute pas qu'un auteur ne nuit jamais tant à ses lecteurs que quand il dissimule une difficulté. Quand la concurrence, c'est à dire l'égoïsme, ne régnera plus dans les sciences, quand on s'associera pour étudier, au lieu d'envoyer aux Académies des paquets cachetés**, on s'empressera de publier les moindres observations pour peu qu'elles soient nouvelles, et on ajoutera : "Je ne sais pas le reste."]

Dans la mesure où trouver les décomposants Goldbach d'un nombre pair 2x consiste à trouver les solutions entières de certains systèmes de congruences de restes chinois (complémentaires du système des restes chinois qui décrit 2x et sans congruences à 0 pour éviter les nombres composés), j'ai cru que l'extrait suivant de Galois suffisait à prouver la conjecture. J'aimerais beaucoup qu'un professeur de mathématiques prenne un jour le temps de m'expliquer cet autre extrait des écrits de Galois...

[Le principal avantage de la nouvelle théorie que nous venons d'exposer est de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant de racines qu'il y a d'unités dans l'ordre de leur degré. La méthode pour avoir toutes ces racines sera très simple. Premièrement, on pourra toujours préparer la congruence donnée Fx = 0, et le moyen de le faire est évidemment le même que pour les équations ordinaires.

Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à Fx = 0 et à $x^{p-1} = 1$. Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand facteur commun à Fx = 0 et à $x^{p^2-1} = 1$. C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée [...] Ainsi, pour chaque nombre de la forme p^n, on pourra former un groupe de permutations tel que toute fonction des racines invariable par ces permutations devra admettre une valeur rationnelle quand l'équation de degré p^n sera primitive et soluble par radicaux.]

* ici, Galois veut parler des mathématiciens qui ont dérigné son travail à l'époque.

- 27.09.2011 : Evariste Galois cite Guillaume Libri (Journal de Crelle, IX, se reporter à la page 19 du pdf - ou p. 186 du Journal - où sont présentées certaines équations ayant forcément des solutions entières). (122) libri.pdf

- 27.09.2011 : Evariste Galois cite Guillaume Libri (se reporter à la page 50 du pdf - ou p.44 du mémoire - pour voir ce que propose Libri pour trouver les solutions entières de certaines équations). (121) libri2.pdf

- 18.09.2011 : Un non-résidu de tous les diviseurs impairs de n fournit une décomposition de Goldbach de n (120) non-resid-diviseurs-impairs.pdf

- 07.09.2011 : Où ça devient carrément de plus en plus joli... (119) tempo-sept2011.pdf

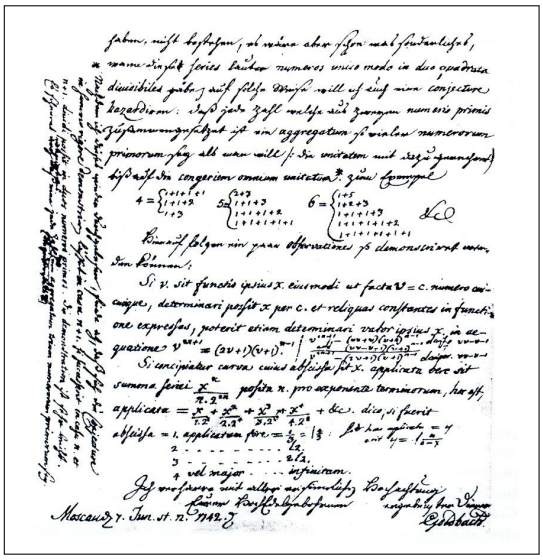
- 02.09.2011 : Pas de fourmi et méthode Coué... (118) septembre2011.pdf

- 31.08.2011 : Un article de Anne-Marie Décaillot qui présente une démonstration de la loi de réciprocité quadratique basée sur l'arithmétique des tissus de Lucas (117) decaillot.pdf

- 24.08.2011 : Conjecture de Goldbach et congruences du second degré (116) aout2011.pdf

- 22.08.2011 : La note de Cantor au Congrès de l'AFAS de Caen en 1894 (115) Cantor-Goldbach.pdf

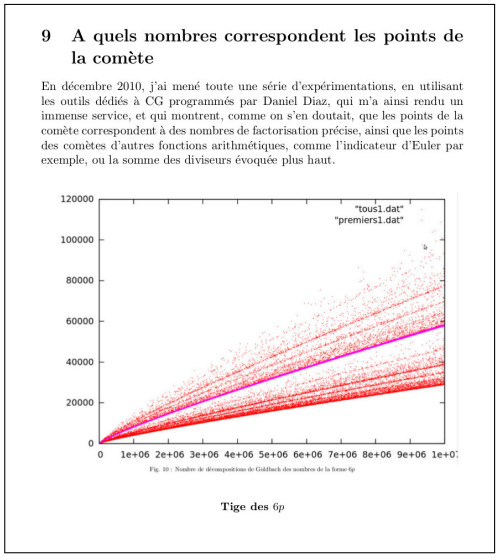
- 22.08.2011 : Lettre manuscrite de Goldbach à Euler du 7 juin 1742 (114)

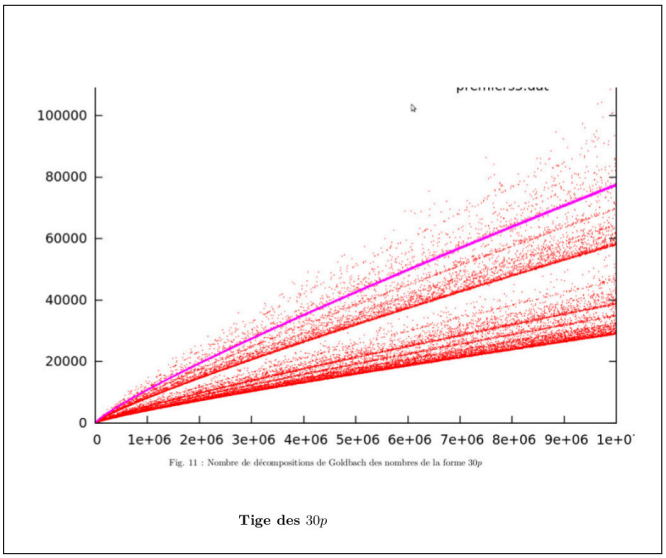


- 22.08.2011 : Version de Fuss de la Lettre de Goldbach à Euler (113) lettre-Goldbach-Euler-7juin1742.pdf
- 22.08.2011 : Version de Fuss de la réponse d'Euler à Goldbach du 30 juin 1742 (112) lettre-Euler-Goldbach-30juin1742.pdf
- 08.08.2011 : L'intellectuel de Beauval

- 20.02.2011 : Expérimentations autour des nombres de décompositions de Goldbach (partitions pour les $2^k.p$) (111) fevrier2011.pdf
- 14.01.2011 : Poursuite des expérimentations, à la recherche d'une récurrence fournissant le nombre de décompositions de Goldbach d'un nombre pair donné (110) lignes.pdf
- 08.01.2011 : Présentation du crible basé sur la symétrie (109) reflexion-dchemla.pdf

- 07.01.2011 : Grilles d'obtention de certaines décompositions de Goldbach de $2x$ par symétrie autour de x (108) grilles.pdf
- ♦♦ à Daniel Diaz, qui a écrit gnu-prolog (😉). (107) CGoldbach-en-gnu-prolog.pdf
- 01.01.2011 : Comète de Goldbach et autres comètes (suite) (106) CGoldbach-en-gnu-prolog.pdf





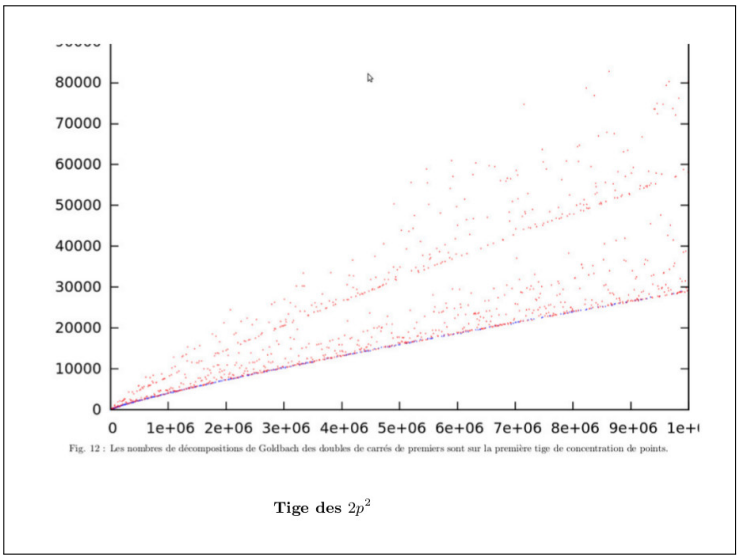


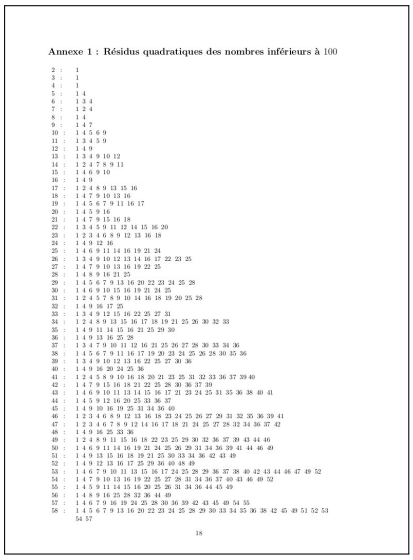
Fig. 12 : Les nombres de décompositions de Goldbach des doubles de carrés de premiers sont sur la première tige de concentration de points.

- 01.01.2011 : Comète de Goldbach et autres comètes (idem mais dessins au format paysage) (105) cometes1111landscape.pdf
- 25.12.2010 : Comète de Goldbach et autres comètes (104) decembre252010.pdf
- 05.12.2010 : Des fonctions qui semblent minorer le nombre de décompositions de Goldbach d'un nombre pair 2x donné (103) decembre42010.pdf
- 28.11.2010 : Note concernant une fonction qui semble minorer le nombre de décompositions de Goldbach d'un nombre pair 2x donné (102) nov282010.pdf
- 24.11.2010 : De surprise en surprise : floor$(\sqrt{x}/4)$ semble minorer le nombre de décompositions de Goldbach d'un nombre pair 2x donné (101)
- 23.11.2010 : Une fonction simple qui semble minorer le nombre de décompositions de Goldbach d'un nombre pair donné (100) nov232010.pdf
- 11.11.2010 : Petites notes dont une fonction qui semble minorer le nombre de décompositions de Goldbach d'un nombre pair donné (99) novembre2010.pdf
- 12.09.2010 : L'ensemble des nombres premiers d'écart 2 est infini (98) infgemeaux.pdf
- 01.05.2010 : Chercher un lien entre la conjecture de Goldbach et la Loi de réciprocité quadratique (97) avril2010.pdf

Annexe 2 : Table de la relation *"est un résidu quadratique de"*

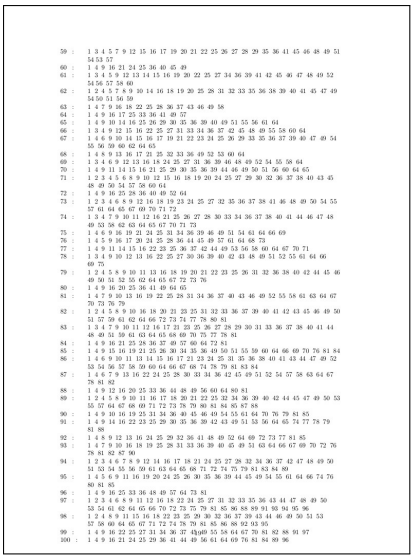
Une croix dans la case à l'intersection de la colonne de 19 et de la ligne de 31 signifie que 19 est un résidu quadratique de 31. En effet, $19 \equiv 9^2 \ (mod\ 31)$.
Cette relation est non-commutative.

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



Annexe 1 : Résidus quadratiques des nombres inférieurs à 100

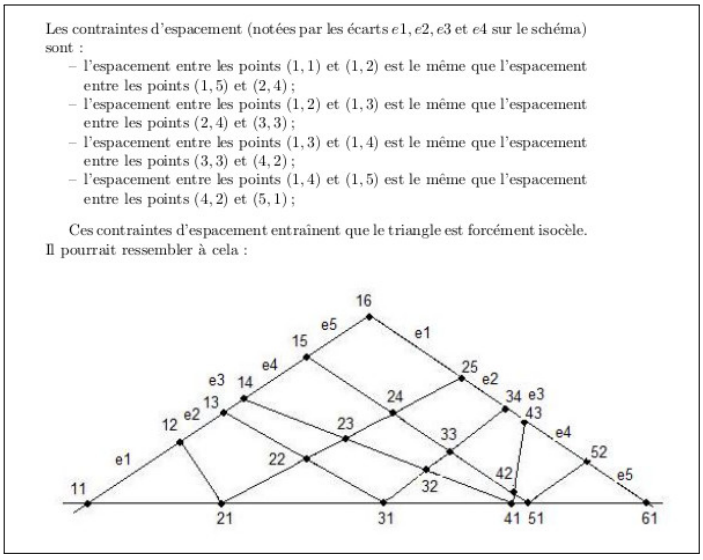
2 : 1
3 : 1
4 : 1
5 : 1 4
6 : 1 3 4
7 : 1 2 4
8 : 1 4
9 : 1 4 7
10 : 1 4 5 6 9
11 : 1 3 4 5 9
12 : 1 4 9
13 : 1 3 4 9 10 12
14 : 1 2 4 7 8 9 11
15 : 1 4 6 9 10
16 : 1 4 9
17 : 1 2 4 8 9 13 15 16
18 : 1 4 7 9 10 13 16
19 : 1 4 5 6 7 9 11 16 17
20 : 1 4 5 9 16
21 : 1 4 7 9 15 16 18
22 : 1 3 4 5 9 11 12 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 15 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 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 31 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 43q60 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

- 11.03.2010 : Conjecture de Goldbach, Jacquard et réécriture ; il faut conserver les deux dimensions des grilles et prouver que les substitutions horizontales ont une conséquence verticale... (96) mars2010v2.pdf
- 08.03.2010 : Conjecture de Goldbach, Jacquard et réécriture (95) mars2010.pdf
- 01.02.2010: La fonction récursive ne permet pas de progresser (94) vingtdix.pdf
- 07.08.2009 : Une fonction récursive de comptage liée à la conjecture de Goldbach (93) aout.pdf
- 17.06.2009 : Une fonction récursive de comptage liée à la conjecture de Goldbach (92) explique.pdf
- 15.06.2009 : Résumé de la méthode utilisant la fonction récursive f (91) langage.pdf
- Diapositives (14.06.2009) : Une fonction récursive de comptage liée à la conjecture de Goldbach (90) cgdvctransp.pdf
- 13.06.2009 : Introduction de la fonction récursive de comptage liée à la conjecture de Goldbach (89) cgdvc.pdf
- Diapositives (4.06.2009) : Conjecture de Goldbach et formule du crible de Poincaré (88) cgpctransp.pdf
- 03.06.2009 : Conjecture de Goldbach et formule du crible de Poincaré (87) cgpc.pdf
- 27.05.2009 : Conjecture de Goldbach, Conjecture des nombres premiers d'écart 2, test de primalité et sinusoïdes (86) notecgcjtp.pdf
- 24.05.2009 : Résumé de la méthode utilisant les matrices carrées de congruence (85) temporaire.pdf
- 20.05.2009 : Valeurs absolues des résidus minima absolus de Gauss et conjecture de Goldbach (84) varma.pdf
- 12.05.2009 : Tester autrement la primalité (83) primalite.pdf
- Diapositives (10.05.2009) : Une nouvelle caractérisation des nombres premiers (82) nouvelledef.pdf
- 10.05.2009 : Valeurs absolues des résidus minima absolus de Gauss et conjecture de Goldbach (81) decouverte.pdf
- 09.05.2009 : Méthode de recherche des décomposants de Goldbach par les ensembles d'entiers (80) vaucluse.pdf
- Diapositives (8.05.2009) : Conjecture de Goldbach et ensembles de restes modulaires (79) residus.pdf
- Diapositives (7.05.2009) : Conjecture de Goldbach et théorie des graphes (78) minigraphes.pdf

- Diapositives (3.05.2009) : Algorithme de calcul des décomposants de Goldbach utilisant des mots binaires (77) algo.pdf
- 01.05.2009 : Des formulations équivalentes de la conjecture de Goldbach (approche par la théorie des langages, la théorie des graphes, la théorie des ensembles) (76) formulations.pdf
- 27.04.2009 : Piste pour une démonstration de la conjecture de Goldbach (75) demon-cg.pdf
- 26.04.2009 : Conjecture de Goldbach et mots binaires (74) constr-exemples.pdf
- ♥♥ 26.04.2009 : Reformulation de la conjecture de Goldbach dans le domaine de la combinatoire des mots (73) combimots.pdf
- 25.04.2009 : Conjecture de Goldbach et affectation de mots binaires (72) constructif.pdf
- 25.04.2009 : Où l'on plie des tissus (71) pliage.pdf
- 22.04.2009 : Etude graphique de la conjecture de Goldbach (70) fingeom.pdf
- 18.04.2009 : Vision géométrique de la conjecture de Goldbach (69) geom.pdf


Les contraintes d'espacement (notées par les écarts $e1, e2, e3$ et $e4$ sur le schéma) sont :

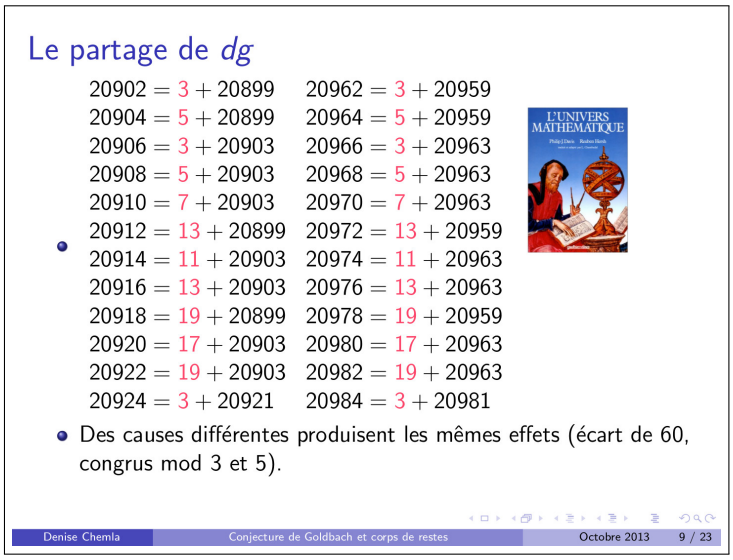
- l'espacement entre les points $(1,1)$ et $(1,2)$ est le même que l'espacement entre les points $(1,5)$ et $(2,4)$;
- l'espacement entre les points $(1,2)$ et $(1,3)$ est le même que l'espacement entre les points $(2,4)$ et $(3,3)$;
- l'espacement entre les points $(1,3)$ et $(1,4)$ est le même que l'espacement entre les points $(3,3)$ et $(4,2)$;
- l'espacement entre les points $(1,4)$ et $(1,5)$ est le même que l'espacement entre les points $(4,2)$ et $(5,1)$;

Ces contraintes d'espacement entraînent que le triangle est forcément isocèle. Il pourrait ressembler à cela :

- 16.04.2009 : Etude combinatoire de la conjecture de Goldbach (68) combinat.pdf
- 14.04.2009 : Arithmétique des tissus et conjecture de Goldbach (67) tissu.pdf
- 01.04.2009 : Conjecture de Goldbach et suite de mots binaires (66) boolseq.pdf
- Diapositives (24.03.2009) : Treillis d'ensembles de nombres (65) treillis.pdf
- 23.03.2009 : Polynômes caractéristiques de matrices de congruence (64) polycarac.pdf
- Diapositives (21.03.2009) : Etude de la conjecture de Goldbach utilisant les restes modulaires (63) cg-beamer.pdf

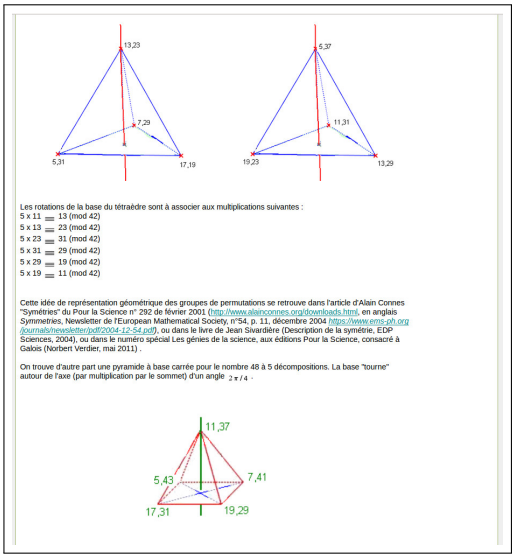
- Programmation de la méthode par les valeurs absolues des résidus modulaires minima de Gauss (62) preparationnp.html
- Idée enfantine de Gauss (61) niemenp.html
- Tout écrit est un appel. (60) desnotesnp.html
- Matrices carrées de booléens vues comme des matrices d'incidence de graphes (59) petits-graphesnp.html
- Programmation de la méthode de recherche des décomposants de Goldbach utilisant des mots binaires (un décomposant de Goldbach d'un entier lui permet de vérifier la conjecture de Goldbach) (58) expliquenp.html
- Programmation de l'algorithme de calcul des mots associés à un nombre pair (57) vendredinp.html
- Théorie des langages, combinatoire des mots (56) mercredinp.html
- Etudier la conjecture de Goldbach en utilisant les probabilités (55) probanp.html
- Galois (54) evaristenp.html
- Décompositions de Goldbach des premiers entiers (qui leur permet de vérifier la conjecture de Goldbach) (53) decomposnp.html

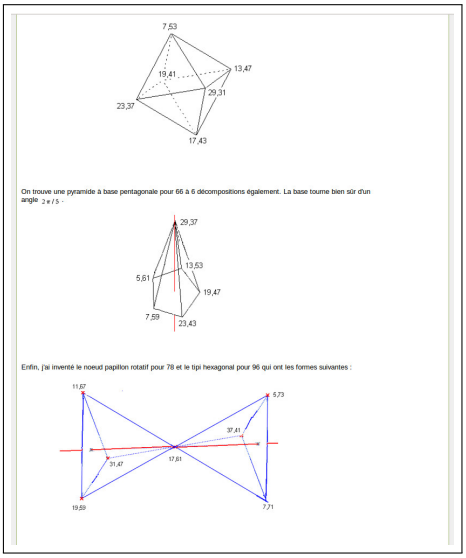
- Ma conjecture : $2x$ (supérieur à 12) partage toujours l'un de ses décomposants de Goldbach avec $2x - 6$ (et vérifie ainsi la conjecture de Goldbach) (52) arbres2np.html

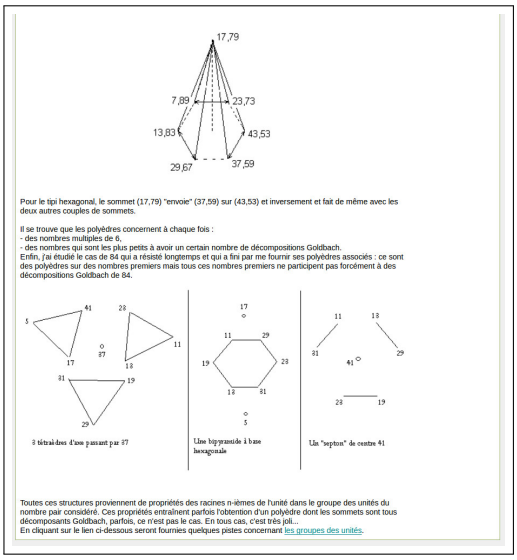


- Associer à chaque entier un ensemble de fractions rationnelles et caractériser autrement la primalité (51) beautenp.html
- Hilbert et Cantor (50) cantornp.html
- Revenir à la division euclidienne (49) division-euclidiennenp.html
- Empilement de valuations p-adiques et TNP (Théorème des Nombres Premiers) (48) empilementnp.html
- Enoncé de la conjecture de Goldbach (47) enoncenp.html
- Divisibilité des factorielles (Lucas) (46) factonp.html
- ♥ Fractales (45) fractalesnp.html
- Démonstration constructive ou non, fenêtre de recherche d'un décomposant de Goldbach d'un entier (lui permettant de vérifier la conjecture de Goldbach) (44) generiquenp.html
- Géométrie des nombres de Minkowski, équations de droites, théorème de Noël (43) goldonp.html
- Conjecture de Goldbach et Théorie des graphes (à arêtes colorées, cf Ramsey) (42) graphesnp.html
- Groupe cyclique des unités (41) groupescycliquesnp.html
- Incongruences (dessin des ensembles) (40) incongrusnp.html
- Indicateur d'Euler (39) indiceulernp.html
- Crible de Matiiassevitch (38) matiiassevitchnp.html
- Moyennes arithmétiques (densité du photon !) (37) moyennesnp.html
- Rencontre de la non-commutativité, à minuscule échelle (36) noncommutnp.html

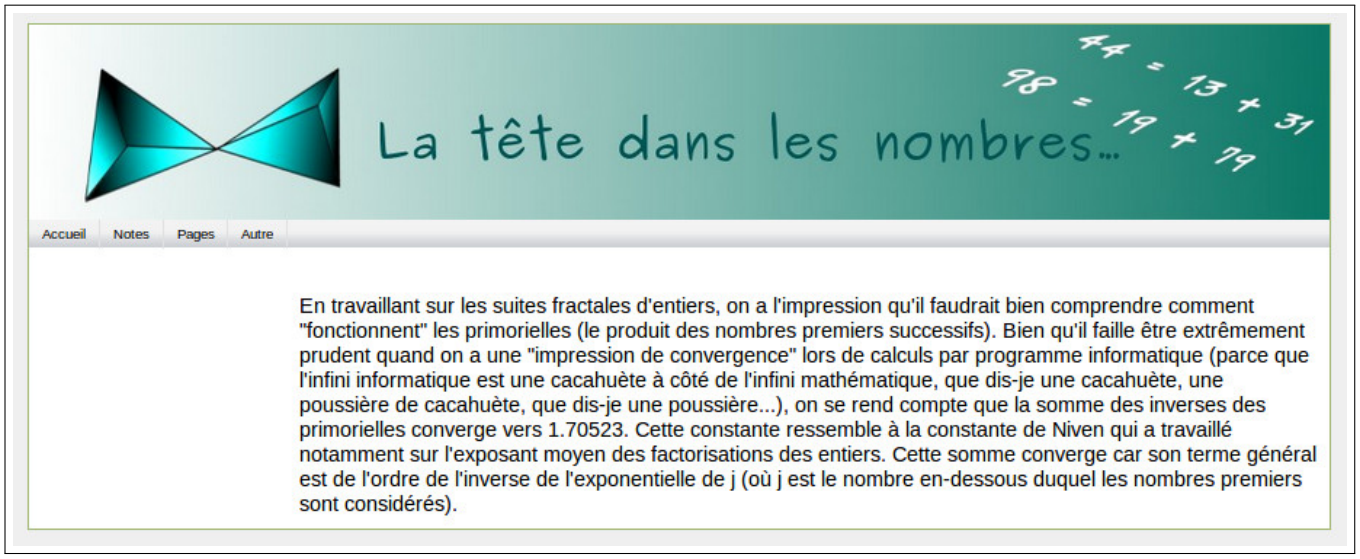
- Okounkov (35) okounkovnp.html
- Merveilleux polyèdres (34) polyedresnp.html



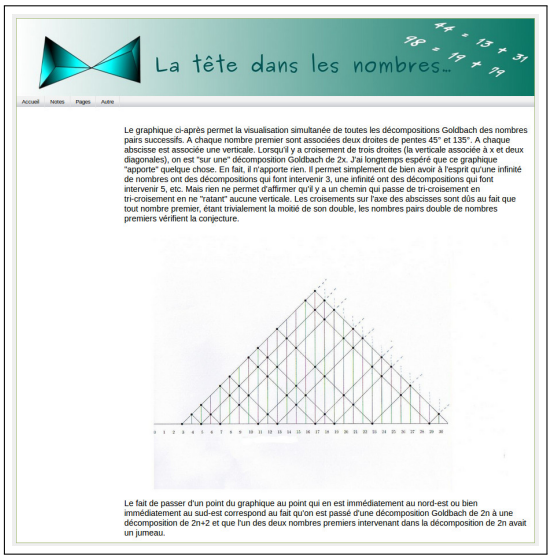




- Racines de polynomes, Congruence des sommes de racines (33) polynomesnp.html
- Primorielles (32) primonp.html

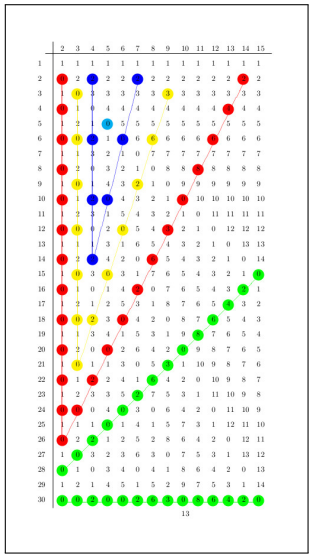


- Théorème des quatre carrés de Lagrange (31) quatrecarresnp.html
- La loi de réciprocité quadratique de Gauss (30) reciprocitenp.html
- Un beau maillage (29) treillisnp.html

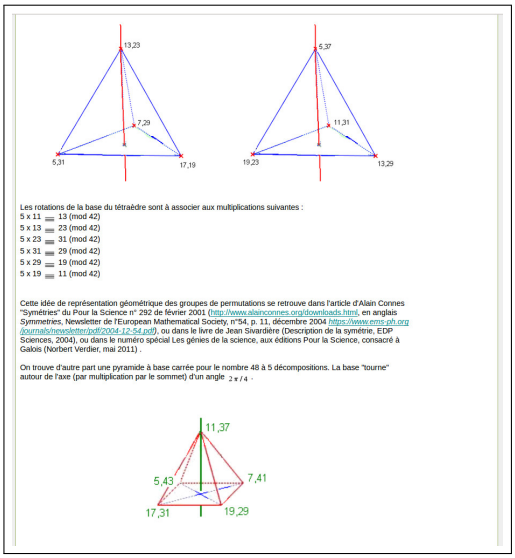


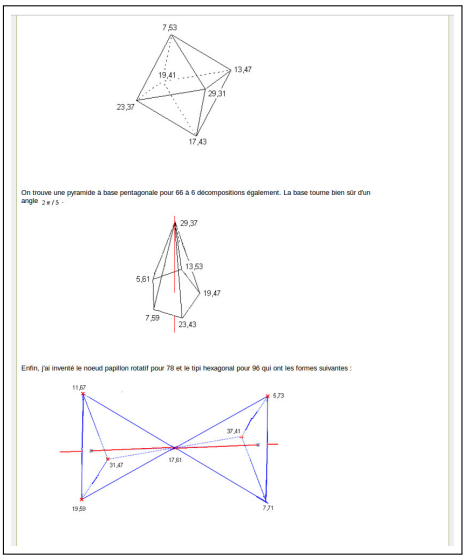
- Démonstration par récurrence, réglettes de Laisant (28) recunp.html
- 01.03.2009 : Matrices de congruence et descente infinie (27) codage-et-descente.pdf
- 27.02.2009 : Utiliser les probabilités pour étudier la conjecture de Goldbach (26) proba.pdf
- 22.11.2008 : Congruences, combinaisons linéaires (25) explic-a-x-plus-b.pdf
- 01.11.2008 : Approches algébrique et géométrique de la conjecture de Goldbach (24) CGoldAlgebreGeom.pdf
- 12.05.2008 : Partage des décomposants de Goldbach (ou bien pour ceux que ça transporte de voir 123321 sur le compteur kilométrique) (23) partager.pdf
- 31.03.2008 : Prendre la tangente (22) prendre-la-tangente.pdf
- 09.01.2008 : Petites notes (21) (Sharol Nau https://static1.bridgesmathart.org/art-exhibits/bridges06/na petites-notes-sans-legendre.pdf
- 01.11.2007 : Détermination des décomposants de Goldbach grâce au théorème des restes chinois (20) chine-vella.pdf
- 01.10.2007 : Changer l'ordre sur les entiers naturels pour comprendre le partage des décomposants de Goldbach (19) reordonner.pdf
- 01.07.2007 : Arbres de nombres et conjecture de Goldbach (18) arbres.pdf
- 01.01.2007 : Une nouvelle façon de voir les nombres premiers (17) premiers.pdf
- 01.01.2007 : Conjecture de Goldbach et propriétés de symétrie d'une table de congruence (16) preuve-math.pdf
- 01.01.2007 : Une approche enfantine des nombres premiers (15) nieme.pdf

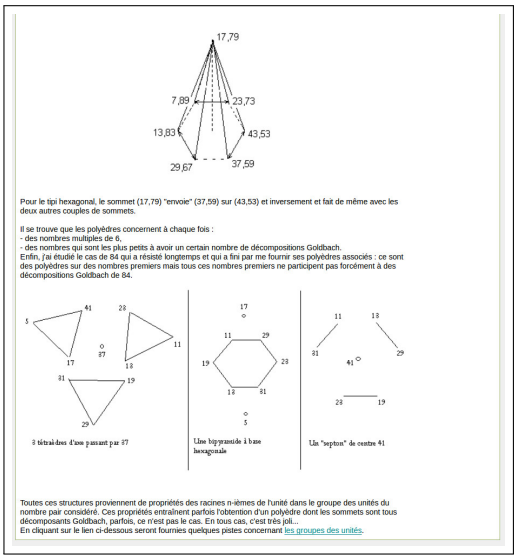
- 25.12.2006 : Conjecture de Goldbach et symétrie dans les tables de congruence (14) noel2006.pdf



- 01.11.2006 : Résultats trouvés sur différents groupes avec l'outil GAP (13) novembre2006.pdf
- 01.10.2006 : Conjecture de Goldbach et théorie des groupes (12) octobre2006.pdf
- 01.09.2006 : Esthétique des décompositions de Goldbach de certains nombres pairs (11) septembre2006.pdf



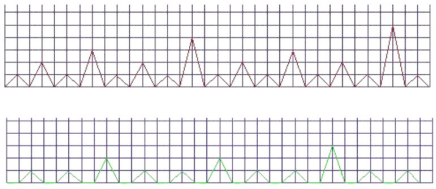




- 01.08.2006 : Conjecture de Goldbach et polynômes symétriques (10) aout2006.pdf
- 01.06.2006 : Sous-graphe d'ordre maximal d'un graphe coloré (9) juin2006.pdf
- 03.05.2006 : Factorisation des factorielles, ensembles et relations (8) mai2006-2.pdf
- 01.05.2006 : Représentation de la combinatoire associée à la conjecture de Goldbach par des graphes (7) mai2006-1.pdf
- ♥ 01.02.2006 : Fractales, symétrie et conjecture de Goldbach (6) fevrier2006.pdf

En février 2006, j'ai écrit une note *Fractales, symétries et conjecture de Goldbach* : elle présentait la suite des nombres premiers comme une séquence fractale d'entiers.

En résumé, on s'intéresse à la séquence des valuations 2-adiques des nombres entiers successifs (l'exposant de la puissance de 2 dans leur décomposition). On la représente sur le graphique suivant :



Cette séquence peut s'obtenir récursivement de la façon suivante :
- la séquence initiale est "01".
- pour passer de la séquence d'un niveau n à la séquence du niveau n+1, concaténer deux séquences de niveau n et changer le dernier chiffre en son successeur.
On obtient 01 puis 0102 puis 01020103 puis 0102010301020104, etc...

De la même façon, on obtient la séquence des valuations 3-adiques, puis 5-adiques, puis 7-adiques, etc... La procédure récursive d'obtention de la séquence de niveau n+1 nécessite simplement alors de concaténer 3, ou 5, ou 7 séquences pour passer d'un niveau au niveau supérieur.

Ces séquences sont appelées séquences fractales d'entiers (cf Mandelbrot, Kimberling) parce qu'elles s'"auto-contiennent". Si on enlève tous les zéros de la séquence des valuations 2-adiques, et qu'on retranche 1 aux éléments restants, on retrouve la séquence initiale. Avant Mandelbrot, Peano, Sierpinski ou Hilbert avait inventé des courbes fractales, capables de recouvrir le plan (ça n'était d'ailleurs pas sans poser problème que le plan et la ligne se retrouve de même dimension en quelque sorte, ces courbes ont même été qualifiées de "monstruosités").

Considérons la séquence obtenue en additionnant les éléments des i séquences p-adiques associées à tous les nombres premiers p_i inférieurs à n. Cette séquence est fractale (si l'on ne conserve de cette séquence que les éléments d'indices multiples du produit des p_i - que j'appelle la primorielle- et qu'on leur retranche i, on retrouve la séquence initiale des sommes). Les log(n) premiers éléments de cette séquence qui ont pour valeur 1 sont d'indices premiers.

Maintenant, raisonnons plus simplement, en considérant des booléens au lieu des valuations p-adiques.
Je veux ajouter 01 à 001. J'ajoute (je fais un "ou" booléen) 010101 à 001001. J'obtiens la séquence 011101 de longueur 6 (=2x3). Dans cette séquence, on voit que 5 est premier (ni divisible par 2 ni par 3).
Je réitère le processus avec le nouveau nombre premier obtenu 5 : je dois ajouter 011101 à 00001. J'obtiens par addition de :
011101 011101 011101 011101 011101 à
00001 00001 00001 00001 00001 00001
la séquence de longueur 30 (=2x3x5)
011110110110101110110111101101

Dans cette séquence symétrique autour de 15, je vois simultanément que 7, 11, 13, 17, 19, 23 et 29 sont premiers. 13 et 17 sont symétriques autour de 15, 11 et 19 sont symétriques autour de 15, 7 et 23 sont symétriques autour de 15.
Dans ce cas, tous les nombres premiers apparaissent en même temps car on est dans le cas "chanceux" où la racine de 30 est inférieur ou égale à 6 qui est le nombre juste au-dessus du dernier nombre premier considéré 5. A la passe suivante, 2x3x5x7 = 210 mais la racine carrée de 210 est bien supérieure à 7+1, et donc les symétriques autour de 105 auront seulement les mêmes propriétés de divisibilité par 2,3,5 ou 7 mais ne seront pas forcément systématiquement premiers 2 par 2. C'est un peu comme si au fur et à mesure qu'une structure était en train de se construire, quelque chose venait la modifier pendant le cours de sa construction.

Ce qui peut être intéressant concernant la conjecture de Goldbach, c'est que les séquences de valuations p-adiques (comme les séquences de booléens ci-dessus) contiennent des sous-séquences "palindromes" (présentant une symétrie-miroir autour de leur élément médian) qui sont forcément centrées sur des éléments de valuation p-adique non nulle et que cette propriété semble se transférer aux sommes de séquences.
Les graphiques correspondant aux valuations p-adiques ci-dessus ressemblent un peu à des électrocardiogrammes. Il faudrait réussir à prouver que les $2x-p_i$ (à droite de x) ne peuvent pas tous se retrouver en haut des pics ; l'un d'entre eux doit forcément se retrouver dans des trous et ce, dans toutes les séquences des p_i .

Au début, je pensais que la conjecture "tout nombre pair est la somme de deux nombres premiers" était un cas restreint d'un énoncé plus général tel que "tout multiple de k (au lieu de tout nombre pair) est la somme de k (au lieu de 2) nombres premiers". Les éléments présentés ci-dessus concernant les valuations p-adiques semblent au contraire indiquer que la conjecture est la généralisation d'énoncés plus contraints, chaque énoncé concernant un nombre premier seulement.

Enfin, une anecdote : un jour, un enfant me proposa de me "montrer l'infini"... Il sortit un miroir de sa poche et le plaça face à un miroir accroché au mur. La suite de miroirs de plus en plus petits semblait ne jamais s'arrêter et l'enfant était émerveillé. La découverte de toutes ces symétries-miroir dans les séquences d'entiers est aussi fascinante. On pourra lire à ce propos les éléments de bibliographie concernant les "symétries dans la nature" et les "fractales dans la nature".

Une symétrie-miroir naturelle (village de La Roche en Rame)

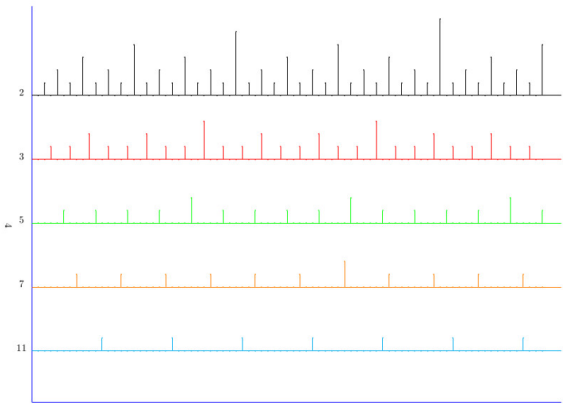
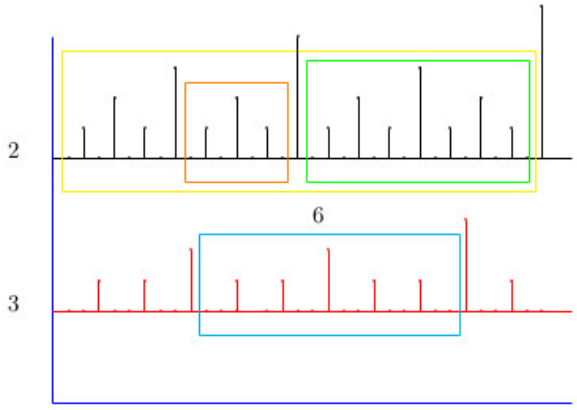
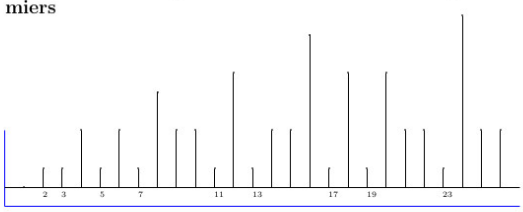


Figure 1 : Séquences fractales de valuations p-adiques

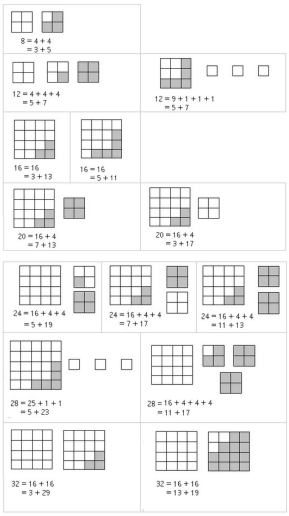
Figure 2 : Exemples de fenêtres centrées sur des multiples



Annexe 6 : la séquence fractale des nombres premiers



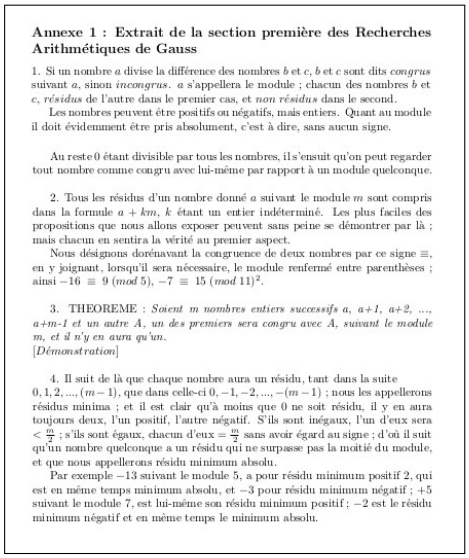
La séquence fractale des nombres premiers (de dimension fonction de la primorielle ?)



- 01.01.2006 : Lien conjecture de Goldbach / indicateur drsquo;Euler (5) janvier2006.pdf
- 01.12.2005 : Vers une preuve de la conjecture de Goldbach (4) decembre2005.pdf

quatrecarres.jpg

- 01.11.2005 : Vers une preuve de la conjecture de Goldbach (3) novembre2005.pdf
- 01.10.2005 : Extraits des Recherches arithmétiques de Gauss



Annexe 1 : Extrait de la section première des Recherches Arithmétiques de Gauss

1. Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est à dire, sans aucun signe.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque.

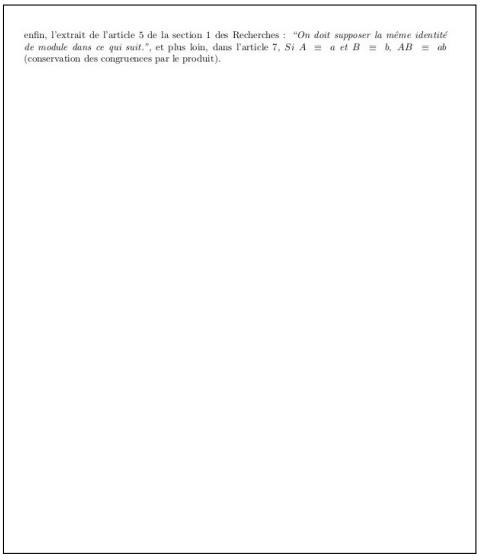
2. Tous les résidus d'un nombre donné a suivant le module m sont compris dans la formule $a + km$, k étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer peuvent sans peine se démontrer par là ; mais chacun en sentira la vérité au premier aspect.

Nous désignons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses ; ainsi $-16 \equiv 9 \ (mod\ 5)$, $-7 \equiv 15 \ (mod\ 11)^2$.

3. THEOREME : *Soient m nombres entiers successifs a, a+1, a+2, ..., a+m-1 et un autre A, un des premiers sera congru avec A, suivant le module m, et il n'y en aura qu'un.*
[*Démonstration*]

4. Il suit de là que chaque nombre aura un résidu, tant dans la suite $0, 1, 2, ..., (m-1)$, que dans celle-ci $0, -1, -2, ..., -(m-1)$; nous les appellerons résidus minima ; et il est clair qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. S'ils sont inégaux, l'un d'eux sera $< \frac{m}{2}$; s'ils sont égaux, chacun d'eux $= \frac{m}{2}$ sans avoir égard au signe ; d'où il suit qu'un nombre quelconque a un résidu qui ne surpasse pas la moitié du module, et que nous appellerons résidu minimum absolu.

Par exemple -13 suivant le module 5, a pour résidu minimum positif 2, qui est en même temps minimum absolu, et -3 pour résidu minimum négatif ; $+5$ suivant le module 7, est lui-même son résidu minimum positif ; -2 est le résidu minimum négatif et en même temps le minimum absolu.



enfin, l'extrait de l'article 5 de la section 1 des Recherches : *"On doit supposer la même identité de module dans ce qui suit."*, et plus loin, dans l'article 7, *Si* $A \equiv a$ *et* $B \equiv b$, $AB \equiv ab$ (conservation des congruences par le produit).

l'article 78 des Recherches Arithmétiques : Le théorème de *Wilson* peut être rendu plus général en l'énonçant comme il suit : *le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$, et positivement dans tous les autres cas. Le théorème de Wilson est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$ est $\equiv 1$ (*mod* 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de deux racines ; ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le $n°75$, si l'on y joint ce que nous dirons tout à l'heure des modules composés. ;

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'un 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 $\frac{1}{2}(p-1)$ 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, on 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 $\frac{k}{a} \equiv b$ (*mod* p) on a, ou 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 ($n°$ 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 ($n°$ 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[3] : *la valeur de l'expression* $\frac{k}{a}$ (*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[4], 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

[3] Ici, je note 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.
[4] 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 ($n°$ 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^n, l'autre le soit par p^{n-r} 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 α^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 $\pm\alpha + xp^\mu$; il est ainsi de s'assurer que c'est là la forme qu'elle doit avoir. Il faut donc qu'on ait $\alpha^2 \pm 2\alpha xp^\mu + x^2p^{2\mu} \equiv A \pmod{p^\nu}$, ou comme $2\mu > \nu$, on aura $\pm 2\alpha xp^\mu \equiv A - \alpha^2 \pmod{p^\nu}$.
Soit $A - \alpha^2 = p^\mu A$, on aura $\pm 2\alpha x \equiv A \pmod{p^{\nu-\mu}}$; donc x sera la valeur de l'expression $\pm\frac{A}{2\alpha} \pmod{p^{\nu-\mu}}$. 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^2. Et en général, si l'on propose le nombre $p^\mu A$, A n'étant pas divisible par p, il y aura trois cas à distinguer :
1°. Si $k \geq n$, on aura $p^\mu A \equiv 0 \pmod{p^n}$, c'est-à-dire qu'il sera résidu.
2°. Si $k < n$ et impair, $p^\mu A$ sera non-résidu.
3°. Si $k < n$ et pair, $p^\mu A$ 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 ($n°$ 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 3 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 on 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 $V = \sqrt{A} \pmod{p^n}$, 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°. 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 $\equiv v$, l'autre sera $\equiv -v$; il en a quatre pour $p = 2$ et $n > 2$; et si l'une est $\equiv v$, les autres seront $\equiv v + 2^{n-1}$, $-v + 2^{n-1}$, $-v$.
2°. Si A est divisible par p, mais non par p^n, soit $p^{2\mu}$ la plus haute puissance de p qui divise A, on

cette puissance doit être paire (n° 102), et $A = ap^{2\nu}$; il est clair que toutes les valeurs de V doivent être divisibles par p^{ν}, et que tous les quotients donnés par ces divisions seront les valeurs de l'expression $V' = \sqrt{n}\ (mod\ p^{\mu-2\nu})$; on aura donc toutes les valeurs différentes de V, en multipliant par p^{ν}, toutes celles de V' contenues entre 0 et $p^{\mu-\nu}$. Elles seront, par conséquent,

$$vp^{\nu}, vp^{\nu}+p^{\mu-\nu}, vp^{\nu}+2p^{\mu-\nu}, \ldots vp^{\nu}+(p^{\mu}-1)p^{\mu-\nu},$$

v étant une valeur quelconque de V : suivant donc que V' aura 1, ou 2, ou ^{11} valeurs, V en aura p^{ν}, ou $2p^{\nu}$ ou $4p^{\nu}$ (1°).

3°. Si A est divisible par p^{ν}, 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 $0, p^{m}, 2p^{m}, \ldots (p^{\mu-m}-1)p^{m}$, dont le nombre est $p^{\mu-m}$.

page 78, article 105 : Il reste à examiner le cas où le module m est composé de plusieurs modules premiers. Soit $m = a\delta c\ etc.$, $a, b, c, etc.$ 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° 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, $\frac{1}{r}\ (mod\ p)$ 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° 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. (X^{me} 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] Mais 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 (X^{me} 104, 105). Cela posé, soit $a^2 = 2 + at$ ou $at = a^2 - 2$, a^2 sera de la forme $8n+1$, et par-conséquent at 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° 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 $u < t$ et $ut = a^2+2$, il est facile de déduire que a 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° 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 ($n°$ 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 $(a^{2n}-1)^2 = -2a^{2n}$; 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° 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 écrire -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° 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 résout 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 $Q R a^{2k}$; mais a 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 résout 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 $Ak+r, Ak+r', etc.$, 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, ($n°$ 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 ($n°$ 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 lettr 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° 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 $A\mathfrak{D}p$, et lorsque p sera contenu dans une des dernières, p sera impair et $A\mathfrak{N}p$.
Exemple. Soit $A=+105=(-3)\times(+5)\times(-7)$[38] ;
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 $n^{mes}(32,96)$ 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 $l2^{l-1}$; 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

[38] 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 $\alpha=\pm2$, 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.*, $\pm2Q$ 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[37]. 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° 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° 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°s 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 notre proposition relative aux résidus quarrés, dont la démonstration est moins cachée : je ne l'ajoute pas, pour ne pas vous dérober 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 α un nombre quelconque non divisible par p. Multipliés tous les nombres A par α; 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 α 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 surtoit pour les mysteres des nombres est fort rare : on ne s'en étonne pas ; les charmes enchanteurs de cette sublime science ne se dovèlent dans toute leur

[37] On suppose donc que Gauss l'a fait, 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 épineuses, sait neanmoins 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.

4 Le lemme de l'article 127 des Recherches arithmétiques de Gauss

Gauss, dans l'article 127 des Recherches arithmétiques, fournit le lemme suivant :

"Dans la progression $a, a+1, a+2, \ldots, a+n-1$, il ne peut y avoir plus de termes divisibles par un nombre quelconque h que dans la progression $1, 2, 3, \ldots, n$ qui a le même nombre de termes."

Il en donne ensuite la démonstration suivante :

"En effet, on voit sans peine que
- si n est divisible par h, il y a dans chaque progression $\frac{n}{h}$ termes divisibles par h ;
- sinon soit $n = he + f$, f étant $< h$; il y aura dans la première série e termes, et dans la seconde e ou $e+1$ termes divisibles par h."

Il suit de là, comme corollaire, que $\frac{a(a+1)(a+2)(a+3)\ldots(a+n-1)}{1.2.3.\ldots n}$ est toujours un nombre entier : proposition connue par la théorie des nombres figurés mais qui, si je ne me trompe, n'a jamais été démontrée par personne.

Enfin, nous aurions pu présenter plus généralement ce lemme de la façon suivante :
"Dans la progression $a, a+1, a+2, \ldots, a+n-1$, il ne peut y avoir plus de termes divisibles par un nombre quelconque h que dans la progression $1, 2, 3, \ldots, n$ qui a le même nombre de termes."

Par exemple, dans l'article 131, *Tout nombre qui, pris positivement, est résidu ou non-résidu de p, aura pour résidu ou non-résidu, $+p$ ou $-p$, selon que p sera de la forme $4n+1$ ou $4n+3$.*

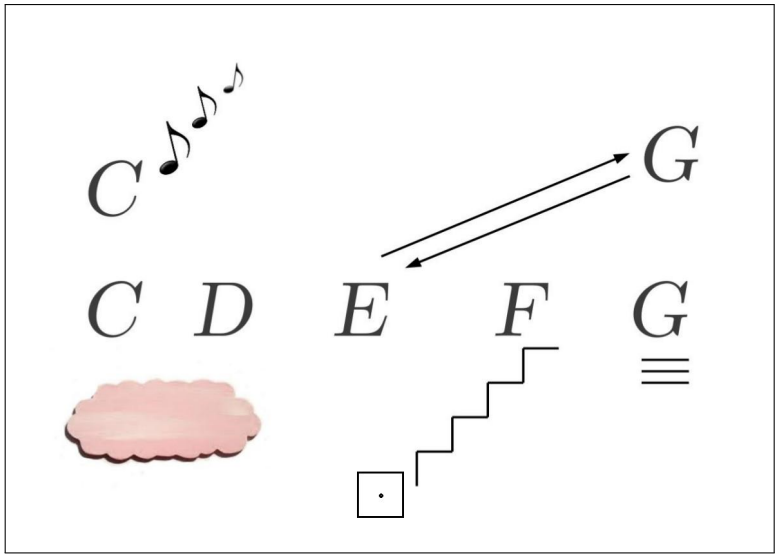
2. article 151 page 116 des Recherches arithmétiques : "il s'ensuit que la relation de p à q est la même que celle de q à p quand p ou q est de la forme $4k+1$, et qu'elle est inverse quand p et q sont de la forme $4k+3$.

un *"artifice technique"* que Gauss présente à la fin de la section 4 des Recherches Arithmétiques : $a \equiv b \,(mod\ m)$ est équivalent à $ca \equiv cb \,(mod\ cm)$[1].
Par exemple, $5 \equiv 17 \,(mod\ 3) \iff 35 \equiv 119 \,(mod\ 21)$;

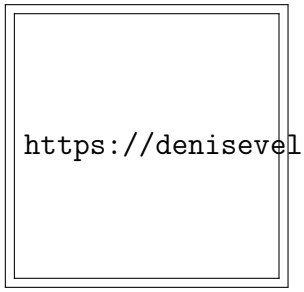
[1]L'extrait de l'article 152, page 117 est *Soit la congruence* $ax^2 + bx + c \equiv 0 \,(mod\ m)$ *; elle sera équivalente à celle-ci :* $4a^2x^2 + 4abx + 4ac \equiv 0 \,(mod\ 4am)$.

un *"artifice technique"* que Gauss présente à la fin de la section 4 des Recherches Arithmétiques : $a \equiv b \,(mod\ m)$ est équivalent à $ca \equiv cb \,(mod\ cm)$[1].
Par exemple, $5 \equiv 17 \,(mod\ 3) \iff 35 \equiv 119 \,(mod\ 21)$;


COME HERE RIGHT NOW!
NEVER!


C
G
C D E F G

- 01.10.2005 : Vers une preuve de la conjecture de Goldbach (2) octobre2005.pdf
- 1994 : un seul article publié, présenté à `ILPS'94` (International Logic Programming Symposium, Ithaca, New-York), coécrit avec Daniel Diaz, Serge Manchon, Philippe Kerlirzin, lors d'une mission `SYSECA` au `CENA` (Centre d'Etudes de la Navigation Aérienne) *Using `CLP(FD)` to solve Air Traffic Flow Management* (1) https://pdfs.semanticscholar.org/e4e2/a73a960f977c01b6cde302e
- **Compilations** : cliquer sur les titres de la (ou des) page(s) de garde pour aller directement sur les notes ;
- 2005 à 2008 table-des-matieres-compil1.pdf 2009 à 2010 table-des-matieres-compil2.pdf 2011 table-des-matieres-compil3.pdf 2012 (avant oct.) table-des-matieres-compil4.pdf nov. 2012 à juil. 2013 table-des-matieres-compil5.pdf juil. 2013 à avr. 2014 table-des-matieres-compil6.pdf avr. à oct. 2014 table-des-matieres-compil7.pdf 2015 table-des-matieres-compil8.pdf 2016 table-des-matieres-compil9.pdf 2017 table-des-matieres-compil10.pdf 2018 table-des-matieres-compil11.pdf 2019 table-des-matieres-compil12.pdf Chouettes souvenirs table-des-matieres-chous.pdf juin 2019-juin 2020 hrefhttps://denisevellachemla.eu/compil13.pdfcompil13.pdf 2020 transc-trad-LaTex compil2020-table-secr.pdf 2020 recherches compil2020.pdf 2021 compil2021.pdf 2022 compil2022.pdf 2023 compil2023etimages.pdf
- "Sourire, sourire, toujours sourire, même si l'on te traite de p'tit laid..." (Claude Nougaro)
- 02.04.2019 : bouts'd'vie https://milliardsdautres.blogspot.com/¡/a¿ carrousel1.html carrousel2.html carrousel3.html carrousel4.html
- 



`https://denisevellachemla.eu/dvmini.jpeg`

Contact : chemla point denise at orange point fr
Blog : https://milliardsdautres.blogspot.com

En haut de la page, les onglets :

Accueil	qui fournit les quelques pages qui me semblent les plus importantes du site ;
Notes	qui fournit l'intégralité des notes écrites depuis 2005 ;
Tamiser	qui fournit mes notes préférées (celles marquées d'un ou deux dans la page Notes ;
Vidéos	qui fournit des liens vers vidéos de mathématiciennes et mathématiciens (à noter : 8 petites vidéos pour donner, peut-être, le goût des mathématiques à des élèves de CM2) ;
Bibliographie	qui fournit une liste des livres et articles ainsi que de nombreuses transcriptions et/ou traductions de certains articles ou extraits ;
Transcriptions	qui fournit l'ensemble des transcriptions et traductions effectuées ;
Webio. d'A. Connes	qui est une page de liens vers des vidéos d'Alain Connes la page imagée est ici ; la page des transcriptions en lien avec la géométrie non-commutative est là ;
Webio. de P. Cartier	: page d'hommage au grand pédagogue qu'était Pierre Cartier.