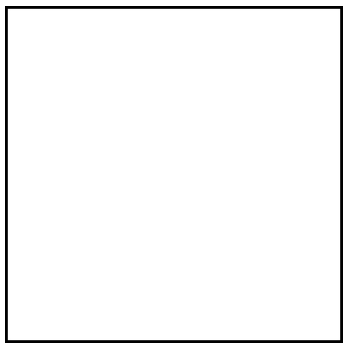
La Grange Mathématique

ou de l'envie de compter des carrés



Ceci n'est pas un carré.
Magritte.

Adieu donc, puisqu'en vain je tâche à vous résoudre.
Avec tous vos lauriers, craignez encor le foudre.
Le Cid, Corneille.

Du carré du carreau au carreau du carré
Le carme en son quartier s'en est accaparé
Car est-il plus centré sur un fil de carret
Qu'un racque qu'a rêvé un carrier préparé

À l'entour du théorème de Lagrange

Travail encadré de recherche
Master 1

Marguerite Flammarion
Elio Joseph

Résumé

Dans ce dossier, après avoir introduit les notions d'arithmétique modulaire nécessaires, on comptera le nombre de décompositions d'un entier comme somme de quatre carrés d'entiers.

Université Paris-Saclay

Sous la direction d'Olivier Fouquet

Novembre 2015 - Juin 2016

Contacts :
marguerite@flammarion.eu
josephelio@gmail.com

Préface

Lorsque M. et É. m'ont demandé si j'étais en mesure de rédiger la préface de leur grange aux mathématiques, je me suis empressé d'accepter. Non seulement, j'étais follement amusé par l'idée même d'accomplir cela, mais en plus, j'avais vu grandir et suivi chaque étape de la croissance de leur travail et bien que j'ose me targuer d'avoir participé à l'éclaircissement de certains de ses passages, je dois avouer que le fait d'apporter une pierre véritable à ce bel édifice me hantait plus que de raison.

Je ne suis pas un grand arithméticien. Bien sûr, j'ai appris lorsque j'avais deux ans que deux et deux font quatre - effort intellectuel plutôt impressionnant, me sens-je obligé d'ajouter : comment ai-je réussi à appréhender de manière si complète un nombre deux fois plus grand que moi en matière d'existence, je ne peux toujours pas l'expliquer aujourd'hui - mais un grand et long vide a suivi cela et c'est seulement à vingt-deux ans et pratiquement six mois que j'ai découvert l'existence de la borne dite de Minkowski. J'ai donc peiné à essayer de lire et surtout de comprendre l'ensemble des raisonnements à venir qui constituent l'essentiel de ce mémoire. Je pense pourtant, après avoir redoublé d'efforts incommensurables, avoir atteint à ce jour le stade d'une compréhension globale guère trop erronée des phénomènes sous-jacents au sujet présenté dans ces pages. Pour résumer brièvement, afin de satisfaire les étudiants impatients et sans aucun sens du suspense qui souhaiteraient afin d'obtenir une bonne note à leur prochain devoir-maison connaître immédiatement la fin de l'histoire, disons que si vous dessinez quatre carrés identiques sur une feuille de papier de telle sorte que chacun d'entre eux ait un coin qui touche un coin de chacun des trois autres, vous obtenez, en gommant toutes les lignes internes à la figure obtenue, un carre ? plus grand, d'aire égale à quatre fois celle des carrés de départ et de périmètre doublé par rapport aux mêmes. Me sentant d'âme plus géomètre qu'arithméticienne - c'est d'ailleurs plus facile à prononcer - j'ai préféré aborder l'ensemble du sujet avec cette approche, plus visuelle que celle suggérée par ses auteurs, qui utilise le concept de forme modulaire.

Il ne faut pas voir dans le paragraphe précédent une critique, quelle qu'elle soit, de la méthode utilisée par M. et É pour parvenir à leurs fins. Il est bien évident que la diversité des points de vue est un atout majeur qu'il ne faut sous aucun prétexte négliger en mathématiques, afin d'obtenir un rendement maximal dans leur développement. Parvenir à raccrocher ensemble des pans des mathématiques qui paraissaient jusqu'alors ne rien avoir en commun, c'est bien souvent donner naissance à toute une théorie riche et fructueuse et parfois même, résoudre des problèmes restés sans solution. Je m'emballe peut-être un peu vite, mais je sais pourquoi je dis cela. Il me semble que les travaux contenus dans les pages suivantes vont me mener bien rapidement à une démonstration de l'hypothèse de Riemann d'une simplicité surprenante. Il suffisait de tracer le bon pont, de relier les points d'amarrage exacts. Il n'est pas plus grand que les autres, ce n'est pas une merveille de technologie, mais il passe au-dessus de flots tumultueux et les deux berges réunies sont différentes à un point rare : cet édifice fait preuve d'audace et d'imagination et c'est là toute la force de son caractère. Faire des mathématiques, c'est exactement cela : joindre

des points entre eux sans posséder de règle, ni même de crayon. C'est inventer un système nouveau qui permette de le faire. Le lecteur va apprendre rapidement à s'habituer à construire de tels ouvrages.

Ce mémoire de projet est un original. Il ne fait rien comme tout le monde. Il ne faut pas s'arrêter à son écorce superficielle et s'imaginer qu'il est le fruit d'un délire psychédélique - ou assimilé comme tel - destiné à rassasier la soif de rire permanente habitant ses auteurs, s'effrayer face à toutes les surprises qu'il abrite et se mettre à douter du sérieux de son contenu scientifique. Il faut simplement y voir le vrai plaisir des mathématiques. Tous les deux jouent aux maths. Et ils gagnent.

À cet instant de l'écriture des présentes lignes - j'ai tenu à écrire tout au long de l'élaboration de ce mémoire, afin de ne pas apposer dessus d'ici quelques semaines un regard venant d'en haut, espérant chapeauter le tout de quelques aphorismes pseudo-intelligents que ne renierait pas M. Houellebecq, mais plutôt de rentrer en lui jusqu'à ce que nous fassions corps (de cardinal strictement inférieur à 2) et de m'en imprégner jusqu'à la moelle - je ne connais pas encore tout le contenu mathématique que suis censé être en train de commenter, d'introduire, de louer. Je parcours régulièrement l'avancée du chantier pour ne pas être totalement dépassé, mais celui-ci a mené au creusement d'excavation trop profondes et tortueuses pour que je puisse me plonger complètement dedans trois fois par semaine. Ce que je peux raconter pour l'instant, ce sont les anecdotes qui ont mené à la production de nombreuses pages partiellement recouvertes d'encre noire, parfois bleue ou rouge, mais plus rarement. Mais nullement je ne suis en mesure d'expliquer les dessins mystérieux que cette version technologique de la sépia a tracés lors du passage du papier au sein de l'imprimante. Pour cela, merci de patienter quelques semaines (pour moi), où quelques lignes (pour les autres - je n'écris pas "pour vous" par ignorance, tout simplement : je ne sais pas qui seront mes lecteurs (je n'écris pas "je ne sais pas qui vous êtes", car compte tenu de la phrase précédente, ce serait stupide)).

Le début du début. Si j'étais narcissique, je dirais que c'est grâce à moi ; si j'étais dépressif, je dirais que c'est entièrement ma faute ; si j'étais pessimiste, je dirais que je n'aurais pas dû initier cela et si j'étais vaniteux, je dirais que j'avais, sans le savoir, commencé, à l'instar de Cléopâtre, à ébranler la face du monde, mais comme je ne suis étymologiquement parlant qu'égocentrique, j'affirme haut et fort que l'origine c'est moi. Gaïa émerge de Chaos, j'arrive fièrement sur mon destrier de rayons du Soleil et je sauve le Monde. Ma première tâche sera de faire naître ce projet, d'en rassembler les protagonistes, de les encourager à poursuivre, de les convaincre, après moult discussions, que c'est la seule solution pour sauver leurs semblables. Même si l'histoire ne retiendra qu'eux, je tiens à rappeler que c'est ma main qui a guidé chacun de leurs gestes, ma parole qui a conduit chacune de leurs pensées et mon argent qui leur a permis de subsister pendant chacun des longs mois de dur labeur encore infructueux. Dans les grands endroits, les grands esprits se rencontrent, j'ai donc choisi la sortie des toilettes du restaurant universitaire Les Cèdres d'Orsay pour leur tapoter d'un geste bienveillant le sommet du crâne du bout de ma baguette magique - merisier premier choix, un euro quarante-neuf chez Decathlon. La magie a opéré

immédiatement et nous avons été transporté dans le vortex spatio-temporel dans lequel nous nous trouvons toujours et que je ne présenterai donc pas puisque nous le connaissons bien.

La carte postale de Strasbourg. M. et É. ont assisté en janvier dernier à un séminaire se tenant à Strasbourg (France, ex-Allemagne et encore un peu aujourd'hui, mais pas tout-à-fait) autour de la géométrie. Ils ont souhaité envoyer une carte à O.F. afin de le tenir au courant de leurs pérégrinations, afin qu'il ne s'inquiète pas de ne pas les avoir à portée de main pour les surveiller. Cela n'a pas eu l'effet escompté, puisque je crois savoir de source sûre que le pauvre homme, recevant la missive complètement déjantée de ses protégés, a craint pour l'intégrité de leurs capacités mentales. Affolé, il a tenté de les raisonner habilement afin qu'ils n'entrent pas complètement dans une phase déliro-schyzophrénique sévère. Il faut croire qu'il y est parvenu, puisque les deux ont réussi à mener à terme leur aventure et qu'ils vont soutenir leur oral dans quelques jours. Cette carte marque toutefois le début de ce que j'ai appelé plus tôt le jeu mathématique auquel s'adonnent les auteurs du présent mémoire.

Les boucles d'oreilles. Après les donuts toresques de l'année passée, M. ne pouvait faire autrement que de se trouver des boucles d'oreilles adaptées aux circonstances. Il fallait quelque chose de carré. Ou plutôt de carrés. Car un seul carré, c'est un objet mathématiquement pauvre. Seuls (mais tous) les carrés sont des carrés, au sens où les nombres se décomposant en somme d'un carré sont exactement les carrés. On tourne en rond. Il a été difficile de trouver. Alors ce fut la panique. La débandade générale. Et puis, alors que plus personne ne s'y attendait, elles sont apparues devant elle, comme une évidence. Comme quoi, c'est probablement vrai. Il ne faut pas chercher, ça vous tombe dessus comme ça, pouf. Depuis, tout le monde admire les boucles lagrangiennes pour appareils auditifs qui ont déambulé dans une bonne partie de l'université, et particulièrement aux abords du légendaire bâtiment 425 et son Lucky Luke phosphorescent. On peut en effet lire une intervention de J.M. dans les pages de ce mémoire.

Le ciné-thé(âtre). Le vendredi vingt mai deux-mille seize, M. et É ont débarqué de force chez O.F. et F.J. - nous disons en effet entre nous, étudiants, "nous allons chez...", les trois petits points étant remplacés à l'oral par le nom du chargé de projet de l'étudiant qui a la parole - armés d'une théière remplie d'une mixture dont je ne peux décrire la qualité (j'ai essayé de m'introduire dans la pièce subrepticement, mais j'ai malheureusement été refoulé par le chien de garde à l'entrée. O.F. et F.J. sont des paranoïaques notoires.), de quatre tasses provisoirement vides et de petits gâteaux originaires de contrées nordiques. Ils ont imposé la tenue d'un goûter dans ce bureau. Les chaises et les tables à qui cette mascarade a été sauvagement infligée sont encore aujourd'hui complètement scandalisées. Et nos quatre compères de siroter tranquillement en grignotant par-ci par-là, de grignoter joyeusement en sirotant avec parciparlàmonie, devisant gaiment. Le pire était pourtant encore à venir. Tous ensemble, ils ont osé visionner un film hautement subversif et délétère portant atteinte à l'intégrité de l'image des mathématiciens eux-mêmes. Ce sera mon seul reproche, mais je tiens à la faire figurer ici, car il faut être juste : ces personnes ont si

peu de considération pour elles-mêmes que, si elles n'avaient pas accompli ce qu'elles ont accompli, nous ne pourrions pas les prendre au sérieux. Un peu d'amour-propre, que diable !

Lecture d'un texte éclairant. Je savais que pour comprendre ce projet, il fallait que je remonte jusqu'à ses origines profondes. Je devais impérativement me plonger dans l'univers d'O.F., saisir ses idées, appréhender son esprit, percevoir sa conscience. Aujourd'hui tout cela est facile, nous avons Internet et les moteurs de recherche. Sans difficulté, j'ai trouvé l'article qui selon moi est fondateur de toutes les pages qui suivent. La traduction de son titre anglais donne "La équivariante Tamagawa nombre conjecture pour modulaires motifs avec coefficients dans Hecke algèbres" mais je trouve cela maladroit et préfère soumettre ma propre version de celui-ci : "La conjecture équivariante sur les nombres de Tamagawa pour des motifs modulaires à coefficients dans des algèbres de Hecke". Pour résumer, sous des hypothèses faibles sur la représentation résiduelle, O.F. prouve dans ce papier la conjecture équivariante sur les nombres de Tamagawa pour les motifs modulaires à coefficients dans les anneaux de déformations universelles et les algèbres de Hecke en utilisant une combinaison nouvelle de la méthode des systèmes d'Euler et de celle des systèmes de Taylor-Wiles. Il prouve aussi la compatibilité de cette conjecture par spécialisation. On comprend sans que besoin de plus de détails se fasse sentir que c'est là la naissance de ce qui nous intéresse.

Le lecteur constatera à cette ligne précise que sa lecture a avancé depuis la dernière fois et qu'il est pratiquement apte à présent à se lancer dans le grand récit qui lui tend les bras. Il sait d'où celui-ci vient, les présentations sont faites, il se trouve en présence d'un ami qu'il a réussi à apprivoiser et qu'il peut donc approcher sans crainte aucune. Par ailleurs, nous sommes précisément quelques semaines plus tard - *id est* le temps lui aussi a fait un bond - et moi-même me sens capable d'aller plus avant. Il s'agit donc pour moi d'expliquer au lecteur ce qu'il va trouver dans la suite de cet ouvrage, et par la même, de rendre la lecture de celle-ci parfaitement inutile. Récit d'une promenade dans le monde des mathématiques. Dans une partie préliminatoire (nous sommes en pleine période de championnats d'Europe de football), le lecteur découvrira avec plaisir le démantèlement du réseau des "One-Sentence proofs", dont l'existence est indubitablement l'un des plus grands scandales mathématiques des X^{e} av.J.C ; IX^{e} av.J.C. ; VIII^{e} av.J.C ; VII^{e} av.J.C ; VI^{e} av.J.C. ; V^{e} av.J.C ; IV^{e} av.J.C ; III^{e} av.J.C ; II^{e} av J.C, I^{er} av.J.C ; I^{er} ; II^{e} ; III^{e} ; IV^{e} ; V^{e} ; VI^{e} ; VII^{e} ; VIII^{e} ; IX^{e} ; X^{e} ; XI^{e} ; XII^{e} ; XIII^{e} ; XIV^{e} ; XV^{e}, XVI^{e} ; XVII^{e} ; XVIII^{e} ; XIX^{e} et XX^{e} siècles confondus (autrement dit, de l'ensemble de l'histoire des mathématiques). Il lui sera montré de manière claire, nette et précise à quel point ces preuves-là sont traîtresses et n'ont de One-Sentence que le nom dont elles se targuent. Il est facile d'énoncer une phrase plus ou moins aléatoire et d'affirmer haut et fort que celle-ci démontre l'assertion voulue ; moi-même puis le faire. Mais ce ne sont pas là des mathématiques.

La première partie réelle (mais pas trop, comme on va le voir immédiatement) du travail que le lecteur a entre les mains s'attachera à démontrer le théorème des quatre carrés de Lagrange (il est nécessaire de préciser, afin de ne pas le confondre

avec le théorème de l'ordre d'un élément d'un groupe fini de Lagrange, ou encore - mais uniquement à l'oral - avec le théorème de la grange (hésiodienne), selon lequel "Ce n'est pas en remettant au lendemain que l'on remplit sa grange.") au moyen de l'outil formidable que sont les quaternions. D'un point de vue culturel, cette partie est donc fort intéressante puisque les quaternions sont trop rarement enseignés dans le premier cycle universitaire et que les concepts de base en sont fortement accessibles à n'importe qui que l'on croise dans la rue.

Une fois ces premiers résultats bien digérés, on arrive à une partie éclectique dans les faits qu'elle énonce. Le conseil que je puis faire au lecteur est d'observer les jolis dessins - j'imagine que l'âge moyen du lecteur de ce mémoire aura pour conséquence le fait qu'il n'aura pas lu de livre avec images depuis fort longtemps et que cela devrait lui rappeler quelques souvenirs émouvants de sa tendre enfance - sans trop réfléchir à l'obscur algorithme sous-jacent (cela lui épargnera bien des maux de tete) puis de se ruer sur le prochainement fameux théorème 5, qui constitue selon moi le cœur exact du sujet : celui-ci fournit une caractérisation des entiers s'écrivant uniquement comme une somme d'un, deux ou trois carrés. La preuve en est longue mais guère ardue et je suis prêt à parier que, motivé par la perspective de comprendre un résultat aussi frappant, le lecteur s'en délectera.

J'ai toujours été fasciné par J.M.. Pour moi, il s'agit d'un grand pédagogue. Pourtant je ne suis pas systématiquement d'accord avec ses opinions philosophiques (j'ai lu une bonne partie de ses articles qui traînent ci et là sur l'Internet) mais les trouve toujours au moins intéressantes et amenant la réflexion. Or, que peut-on demander de plus à un philosophe ? Même les plus célèbres ne font pas l'unanimité. Les différences de perception, de sensibilité savent être des barrières infranchissables. Alors, parvenu à la page intitulée "Métamathématiques", j'ai savouré avec plaisir une nouvelle fois la pensée de mon professeur d'intégration de l'an passé.

Passé cet exaltant moment arrivent, selon les dires des auteurs, les choses sérieuses. C'est malheureusement ici que tout se gâte. Il va falloir, donc, prendre ledit tout avec précaution. Des calculs immondes remplissent des pages entières. J'ai répertorié pas moins de deux-cent trente et une lignes de calcul, réparties sur vingt-six pages. Beaucoup trop, donc. Quitte à m'attirer les foudres de J.M., je conseille au lecteur de ne pas s'y attarder. Lire attentivement les énoncés, les comprendre, en saisir les conséquences me paraît être une activité bien plus saine. Il faut de temps en temps avoir un soupçon de confiance envers le reste de l'humanité, surtout quand cela est arrangeant pour soi, et je pense que c'est là un des moments parfaits pour l'utiliser. D'ailleurs, en comptant toutes ces lignes, j'ai eu lesdits calculs sous les yeux. Je déclare donc haut et fort que pas un ne m'a écorché l'œil ni n'a attiré mon attention en raison d'une faute grossière. C'est bien la preuve qu'ils doivent être justes. Et puis, ils permettent de démontrer ce qu'on cherche (qui est vrai, puisqu'on le démontre). Ils doivent donc être encore plus justes. Or, des calculs encore plus justes sont toujours justes [1326], ce qu'il fallait démontrer.

Une fois ce douloureux cap passé, le lecteur est au bout de ses peines. Il ne lui

reste plus qu'à déguster les quelques délicieuses trouvailles qui closent l'ensemble. Celles-ci ont pour moi une connotation toute particulière et, je dois bien le dire, fortement émouvante. En effet, j'y retrouve des idées, des théorèmes, des pages que j'ai vu naître, auxquelles j'ai peut-être parfois apporté un contribution et que j'ai été le premier à lire. Nous retrouvons là l'esprit premier de ce mémoire, qui a malheureusement été perdu dans l'abominable partie que j'évoquais il y a quelques lignes : celui du jeu (09-74-75-13-13). Du jeu mathématique, celui où nous deux apprentis mathématiciens, selon mes propres mots, gagnent (et ne perdent pas), mais aussi du véritable jeu de société, puisque ces deux-là ont trouvé le moyen d'en inventer un qui ait un rapport fort grand avec leur sujet. J'y ai joué, seul contre moi-même (je n'avais personne sous la main) et je dois dire que je me suis bien amusé. Tous les gamers trouveront du plaisir à pratiquer ce genre nouveau, qui ne nécessite même pas de connexion Internet valable pour fonctionner. Ce jeu, c'est l'avenir, en somme. Encore une fois, le lecteur pourra admirer de belles images très divertissantes et je lui conseille aimablement d'y consacrer suffisamment de temps pour être bien détendu. Surtout s'il a essayé de lire et de comprendre l'algorithme qui les accompagne (il faut croire que c'est une maladie chez ces gens-là d'être incapable de pondre des images sans les affubler de lignes capito-douloureuses gâchant tout le plaisir... à moins que cela ne soit qu'une forme de sadisme aigu). Il sera enfin possible de se désaltérer et de se restaurer avant d'attaquer la fin annexe du périple.

Je passerai rapidement sur la première, qui n'a pas d'autre but que de définir une division euclidienne sur l'ensemble des entiers relatifs et revêt donc un caractère fortement utilitariste, au sens où sa seule raison d'exister est de permettre certaines considérations la précédant dans le recueil. Je n'aime guère cet état d'esprit. Quant trois suivantes, voilà des pages qui méritent d'être sans arrêt encensées avec une ardeur sans cesse renouvelée ! Elles font partie de ce que j'estime être la naissance du CRCG et à ce titre, sont à qualifier de cœur des mathématiques. Jouer en s'amusant, s'amuser en travaillant, travailler sérieusement mais pas trop, produire pour faire rire, instruire en riant, pro du rire sans férir et ça m'use et entrave le vaillant : que peut-on vouloir faire de plus ?

La boucle est bouclée, à la manière anglo-saxonne, je suis revenu au point de départ. Les Français penseront que j'ai tourné en rond, mais Outre-Manche, on m'en remerciera. Ma soif insatiable de grandeur et de gloire m'imposent donc ce choix. Je serai lu jusqu'aux Amériques et au-delà ! Alors je m'adapte, victime de mon propre succès. Nul doute que ce mémoire fera date.

Calculus is not dead.

G.C.
13/06/2016.
Quelque part ailleurs.

Nos premiers remerciements vont sans suspens à l'encadrant qui aura su supporter sans sourciller toutes nos sottises. Un merci sincère à ce grand esprit. Merci Olivier Fouquet.

Rien ne se serait fait sans le voisin de bureau de notre encadrant, Florent Jouve, l'homme qui nous a enseigné l'arithmétique. Toujours accueillant, espérons qu'il lui reste une place pour un doctorant d'ici un ou deux ans.

Nous ne pourrions pas ne pas citer Etienne Fouvry, le doyen de l'arithmétique, ou celui qui nous a transmis sa soif. Il nous enseigna avec passion ce que nous avions toujours rêvé d'apprendre. Il nous présenta son épouse, un mercredi.

Invoquons alors Samuel Lelièvre dans cette litanie des remerciements car il nous conta des histoires joyeuses dans les moments difficiles.

Lorsque l'insatisfaction métaphysique nous a étreints, Joël Merker nous a apporté ses lumières. Pour lui, nous garderons précieusement cette insatisfaction.

Ensuite, remercions nos camarades qui ont porté ce projet dans leur cœur à tout instant du jour, de la nuit, en vacances ou en période d'examens. Ils furent, au quotidien, une présence attentive et un solide soutien. Pour leur ferveur et leur confiance, nous citons Gédéon Chevallier et Cyril Falcon.

Nous remercions très chaleureusement Bruno Arsac, l'homme qui sait enseigner, professeur émérite à la Martinière Monplaisir. Un entretien des plus enrichissants nous donna la clé d'une démonstration qui nous résistait.

Nous sommes conscients de tout ce que nous devons au jeune et talentueux Guillaume Matheron qui nous a permis de croire en notre conjecture en la vérifiant sur les $100\,000$ *premiers entiers.*

Nous remercions Patrick Gérard pour nous avoir donné un devoir en licence dont le résultat nous fut bien utile ici. Cotangente par-ci, cotangente par-là.

Nous voudrions exprimer notre reconnaissance à Nathalie Carrière qui, malgré ses matinées bien trop remplies, nous fit don de son temps précieux pour nous permettre d'imprimer des documents de la plus haute importance.

Nos pensées vont vers Sandrine Gauthier et Cyril Falcon, nos binômes de l'an passé. Ils nous firent grandir, ils nous firent faire des choses sérieuses, ils étaient l'équilibre qui nous poussa à nous dépasser cette année. Merci à eux.

Nous nous inclinons devant Joël Merker qui, malgré son jeudi après-midi bien occupé, a eu le courage d'assister à notre soutenance en compagnie d'Olivier Fouquet.

Un merci infini à ceux, nombreux, qui ont subi notre atroce enthousiasme pour ce

projet. Quand à de multiples reprises nous avons sombré dans la folie, ils ont eu la gentillesse de nous sourire tendrement.

Enfin, nous tenons à exprimer de nouveau toute notre gratitude à celui qui fut tout pour nous. Merci du fond du cœur à notre maitre flamboyant dont nous ne sommes, finalement, que les humbles disciples. Car Olivier Fouquet fut, est et sera.

Prélude

Exorde. Nous voudrions commencer ce prodrome (projet de palindrome) par une approche téléologique. Rien que ça. Nous sommes donc deux ($1^2 + 1^2$) étudiants de l'admirable Université d'Orsay, et plus précisément du prestigieux M1 Voie Jacques Hadamard [1]. Un matin, alors que nous dînions au coquet restaurant universitaire d'Orsay, nous aperçûmes un meuble [2]. Nous décidâmes alors, d'un commun accord, de manger d'abord. En effet, nous avions grand faim. Puis nous nous regardâmes, les yeux luisants : nous avions pensé exactement la même chose.

Lagrange (Joseph, de son beau prénom), est né. Puis il décide, de sa propro volonté, de se consacrer aux mathématiques vers 17 ($4^2 + 1^2$) ans, après avoir brillamment étudié à l'université de sa ville natale et à la lecture d'un mémoire de Halley sur l'utilisation de l'optique. Il s'abîme alors aussitôt, seul et sans aide, dans la poignante étude des mathématiques. Puis il passe 20 ($4^2 + 2^2$) années de sa belle vie à l'Académie des Sciences à Berlin, qui sont considérablement plantureuses et prolifiques. Hormis quelques arrêts dus à une santé fragile, il publie avec une régularité monstrueuse des mémoires qui touchent tous les domaines des mathématiques et de la mécanique. Lagrange se distingue particulièrement en arithmétique, en résolvant plusieurs conjectures difficiles dues au grand Fermat et en prouvant que tout entier naturel est somme de 4 (2^2) carrés. Situé entre Euler et Gauss, Cauchy et Weierstrass, dans une période transitoire, Lagrange travaille un peu rigoureusement mais pas trop.

Nous avions compris que la grande, belle, mystérieuse et sauvage arithmétique était une terre arable, qui ne demandait qu'à perdre sa virginité et à être cultivée, en nous. Animés d'un feu augural, nous nous jetâmes dans l'aventure qui allait nous mener loin. Nous sombrâmes dans la langoureuse passion du compte, des carrés d'entiers. Et c'est bien là que Lagrange est intervenu, lui qui avait démontré le théorème qui porte son nom. Eclairés par ce mathématicien et par un phare breton, nous quêtâmes alors un guide, que nous trouvâmes en la personne de notre grand et vénéré maître, notre *sensei* comme nous nous plaisons à l'appeler, l'arbre de la connaissance et la berge folle de la compréhension [2]. Nous pûmes alors avancer tout droit sur les lignes courbes du théorème de Jacobi (dont nous épargnons la biographie au lecteur, pour l'instant) et prendre le chemin lumineux de la Sagesse arithmétique.

Pourquoi compter les carrés ? Pour plusieurs raisons, que le lecteur réfléchi dénichera

1. S'il existe un jésuite matois, ce n'est pas le mathématicien Jacques Hadamard. En effet, Jacques Hadamard est né en décembre 1865 ($29^2 + 32^2$) à Versailles. Il suit des études secondaires peu brillantes en mathématiques ; heureusement, il est reçu premier à l'École Polytechnique et à l'École Normale Supérieure. Il est nommé professeur à Paris, mais il a des difficultés pour se mettre au niveau de son public lycéen, qui compte pourtant en son sein Maurice Fréchet. Cette charge ne l'empêche pas de rédiger une très brillante thèse où il n'étudie pas les repères de Fréchet. C'est dans cette thèse notamment qu'apparait pour la première fois la formule dite de Hadamard, aussi appelée *règle d'Hadamard*. Hadamard épouse Louise Trénel, avec qui il aura 5 ($1^2 + 2^2$) enfants. Il meurt au coin du feu, un beau matin d'été.

2. Voir page 42 ($5^2 + 4^2 + 1^2$).

au fil de sa lecture attentive de notre écrit. Mais nous pouvons d'ores et déjà en donner quelques pistes. Les carrés. Ce n'est sans doute pas un hasard si l'on étudie les puissances en classe de $4^{\text{ème}}$, lorsque 4 est précisément le carré de 2. Les carrés sont omniprésents : ils déterminent les longueurs (Ô Pythagore [3]), ils déterminent les surfaces (Ô Maître [4]), ils déterminent les volumes (Ô Révolution [5]). Le dénombrement. Quand on est jeune, on compte les moutons pour s'endormir. Quand on est un peu plus âgé, on lit Bergson qui explique comment compter lesdits moutons : "*Pour que le nombre en aille croissant à mesure que j'avance, il faut bien que je retienne les images successives et que je les juxtapose à chacune des unités nouvelles dont j'évoque l'idée*" [6]. Le dénombrement est donc, avec les carrés, le fondement même de la mathématique. Une fois que cette réalité eut éclos à nos yeux, faire des mathématiques sans compter les carrés n'était plus concevable.

Sur ces entrefaites, comptons tous les carrés, jusqu'au dernier.

Olivier
Au lit vit et
Fou qu'est
Fouquet

3. Le théorème de Pythagore.
4. Le Maître carré.
5. Le cylindre ou le cône de Révolution.
6. Essai sur les données immédiates de la conscience.

Table des matières

1 Les formes modulaires, ou comment trouver un titre

Bien que le titre de cette section semble très prometteur, nous ne ferons que déflorer la surface d'un domaine qui nous dépasse et nous transcende, nous, pauvres étudiants, car la recherche et lui ne Fouquin.

En arithmétique, un et un font deux.
En amour, un et un devraient faire un,
et ça fait deux tout de même.
Guy de Maupassant.

1.1 Définitions

Définition 1 On définit G le *groupe modulaire* comme

$$G := \mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{id}\},$$

où $\mathrm{SL}_2(\mathbb{Z})$ est l'ensemble des matrices carrées de taille 2×2 à coefficients dans $\mathbb{Z}$ de déterminant 1.

Définition 2 Une fonction *faiblement modulaire de poids* $2k$ est une fonction f méromorphe sur $\mathbb{H}$ qui satisfait la relation

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad f(\gamma \cdot z) = (cz + d)^k f(z).$$

Avec des choix particuliers pour γ, cela nous donne

$$\forall z \in \mathbb{H} \quad \begin{cases} f(z+1) = f(z) \\ f\left(-\dfrac{1}{z}\right) = z^k f(z). \end{cases}$$

Définition 3 Une fonction faiblement modulaire est dite *modulaire* si elle est méromorphe aux pointes (*i.e.* les points envoyés à l'infini par un $\gamma \in \mathrm{SL}_2(\mathbb{Z})$).

Définition 4 On appelle *forme modulaire* une fonction modulaire qui est holomorphe partout.

Définition 5 On appelle *forme parabolique* une forme modulaire qui s'annule aux pointes.

Définition 6 Pour tout $k \geqslant 2$, on définit la *série d'Eisenstein de poids* $2k$ comme la fonction holomorphe

$$\forall z \in \mathbb{H} \quad G_{2k} := \sum_{(m,n) \in\ \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(mz+n)^{2k}}.$$

Définition 7 On définit $\Gamma_0(N)$ comme

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ N \mid c \right\}.$$

Montrons que $\Gamma_0(4)$ est engendré par γ_1 et γ_2.
Cette preuve se révèlera cruciale par la suite.

Définition 8 On définit le groupe $G =< \gamma_1, \gamma_2 >$ engendré par :

$$\gamma_1 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \text{ et } \gamma_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Théorème 1

$$\Gamma_0(4)/\{\pm 1\} = G$$

Preuve.
Tout d'abord, on calcule ${\gamma_1}^n$ et ${\gamma_2}^n$ par récurrence

$$\forall n \in \mathbb{Z} \quad {\gamma_1}^n = \begin{pmatrix} 1 & 0 \\ 4n & 1 \end{pmatrix} \text{ et } {\gamma_2}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Soit $\gamma = \begin{pmatrix} a & b \\ 4c & d \end{pmatrix} \in \Gamma_0(4)$.
Tout ce que nous faisons par la suite marche dès que ce par quoi nous quotientons est non nul. Dans le cas contraire, il n'y a généralement rien à démontrer.

- Posons q et r respectivement le quotient et le reste de la division euclidienne de a par $4c$.
  On a $a = 4cq + r$, donc $r = a - 4cq$.
  Alors on a

$$ {\gamma_2}^{-q}\gamma = \begin{pmatrix} a - 4cq & b - dq \\ 4c & d \end{pmatrix} = \begin{pmatrix} r & b' \\ 4c & d \end{pmatrix}. $$

- Posons q' et r' respectivement le quotient et le reste de la division euclidienne de c par a.
  On a $c = aq' + r'$, donc $4r' = 4c - 4aq'$.
  Alors on a

$$ {\gamma_1}^{-q'}\gamma = \begin{pmatrix} a & b \\ 4c - 4aq' & d - 4bq' \end{pmatrix} = \begin{pmatrix} a & b \\ 4r' & d' \end{pmatrix}. $$

On applique à présent l'algorithme d'Euclide prime qui se trouve dans une des annexes [7] à a et $4c$.
On obtient alors une suite de matrices de la forme :

$$\begin{pmatrix} a & b \\ 4c & d \end{pmatrix} \to \begin{pmatrix} r & \star \\ 4c & \star \end{pmatrix} \to \begin{pmatrix} r & \star \\ 4r' & \star \end{pmatrix} \to \cdots \to \begin{pmatrix} \pm 1 & \star \\ 0 & \star \end{pmatrix}.$$

En effet, $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$, donc $ad - 4bc = 1$.
Donc d'après le théorème de Bézout, $a \wedge c = 1$.

On travaille dans un quotient par $\{\pm 1\}$, ce qui nous permet de ne considérer que le cas positif.
Ainsi,

$$\exists \delta \in G \quad \delta\gamma = \begin{pmatrix} 1 & b' \\ 0 & d' \end{pmatrix}.$$

De plus, $\delta\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ donc $\det(\delta\gamma) = 1$, d'où $d' = 1$.
Donc,

$$\delta\gamma = \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix}.$$

Puis,

$$\gamma_2{}^{-b'}\delta\gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Donc $\gamma \in G$.
D'où $\Gamma_0(4) \subset G$.

Finalement,

$$\Gamma_0(4)/\{\pm 1\} = G. \qquad \square$$

Remarque 1 Cette preuve repose sur l'algorithme d'Euclide prime, en annexe, et sur des divisions euclidiennes sur $\mathbb{Z}$. Les idées sont cachées par les notations, et c'est pourquoi nous donnons un exemple, possiblement plus éclairant que la preuve elle-même.

Exemple 1 Soit $\gamma = \begin{pmatrix} 27 & 10 \\ 8 & 3 \end{pmatrix} \in \Gamma_0(4)$.

$$27 = 8 \times 3 + 3$$

7. Reste à savoir laquelle...

$$\gamma_2^{-3}\gamma = \begin{pmatrix} 3 & 1 \\ 8 & 3 \end{pmatrix}$$

$$2 = 3 \times 0 + 2$$

On comprend alors l'intérêt d'effectuer des divisions euclidiennes primes, en autorisant des restes négatifs afin de pouvoir imposer un quotient non nul.

$$2 = 3 \times 1 - 1$$

$$8 = 3 \times 4 - 4$$

$$\gamma_1^{-1}\gamma_2^{-3}\gamma = \begin{pmatrix} 3 & 1 \\ -4 & -1 \end{pmatrix}$$

$$3 = -4 \times -1 - 1$$

$$\gamma_2^{+1}\gamma_1^{-1}\gamma_2^{-3}\gamma = \begin{pmatrix} -1 & 0 \\ -4 & -1 \end{pmatrix}$$

$$-1 = -1 \times 1 + 0$$

$$-4 = -1 \times 4 + 0$$

$$\gamma_1^{-1}\gamma_2^{+1}\gamma_1^{-1}\gamma_2^{-3}\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Définition 9 On définit le *demi-plan de Poincaré* $\mathbb{H}$ comme

$$\mathbb{H} := \{z \in \mathbb{C},\ \mathfrak{I}(z) > 0\}.$$

Définition 10 On définit $\mathscr{D}_{\Gamma_0(4)}$ par :

$$\mathscr{D}_{\Gamma_0(4)} = \left\{ z \in \mathbb{H} : |\mathrm{Re}(z)| \leq \frac{1}{2} \text{ et } \left| z \pm \frac{1}{4} \right| \geq \frac{1}{4} \right\}.$$

Définition 11 Pour tout $z \in \mathscr{D}_{\Gamma_0(4)}$, on définit $I(z)$ le stabilisateur de z dans $\Gamma_0(4)/\{\pm 1\}$ par :

$$I(z) = \{\gamma \in \Gamma_0(4)/\{\pm 1\} :\ \gamma \cdot z = z\}.$$

Théorème 2 L'ensemble $\mathscr{D}_{\Gamma_0(4)}$ vérifie les propriétés suivantes :

- $\forall z \in \mathbb{H} \quad \exists \gamma \in \Gamma_0(4) \quad \gamma \cdot z \in \mathscr{D}_{\Gamma_0(4)}$.
- Pour tout $(z_1,z_2) \in {\mathscr{D}_{\Gamma_0(4)}}^2$ tel que $z_1 \sim z_2$, où $\sim$ désigne la congruence modulo $\Gamma_0(4)$, on a :
  - ou bien $\mathrm{Re}(z_1) = \pm\frac{1}{2}$ et $z_2 = z_1 \pm 1$
  - ou bien $\left|z_1 \pm \frac{1}{4}\right| = \frac{1}{4}$ et $z_2 = \frac{1}{\mp 4 z_1 + 1}$.
- $\forall z \in \mathscr{D}_{\Gamma_0(4)} \quad I(z) = 1$.

On dit que $\mathscr{D}_{\Gamma_0(4)}$ est un *domaine fondamental* de l'action de $\Gamma_0(4)$ sur $\mathbb{H}$.

Remarque 2 A propos de $\mathscr{D}_{\Gamma_0(4)}$.
Nous avions initialement commencé à prouver le théorème 2, avant de revenir à la raison. Tout l'intérêt de ceci était de montrer que le groupe $\Gamma_0(4)$ est engendré par γ_1 et γ_2, preuve que nous avons déjà faite (théorème 1). Nous avons décidé de procéder de la sorte, car toute la théorie des domaines fondamentaux et des actions de groupes nous semblait bien trop importante pour un énoncé aussi élémentaire sur les matrices. Dans la mesure du possible, il nous semblait plus honnête d'essayer d'abord sans cette conséquente théorie.
La chance nous a souri et notre approche fut couronnée de succès pour cette fois-ci, ce qui ne serait pas perpétuellement le cas.

1.2 Préliminaires

Commençons par divers travaux, ne trouvant malheureusement pas de place attitrée ailleurs dans cet écrit. Leurs contributions, qui peut sembler maigre, est néanmoins à considérer avec respect. Chaque résultat, aussi petit soit-il, a sa place dans l'édifice mathématique.

Tout est nombre[8]
Pythagore.

1.2.1 Premier résultat

Nous étudions la preuve *"A One-Sentence Proof That Every Prime* $p \equiv 1 \pmod 4$ *Is a Sum of Two Squares"* [9].

Le théorème qui nous intéresse, et dont nous nous servirons par la suite, est le suivant.

Théorème 3 Pour tout nombre premier p tel que $p \equiv 1 \pmod 4$,

$$\exists (a,b) \in \mathbb{Z}^2 \quad p = a^2 + b^2.$$

Un article clame haut et fort avoir prouvé ce théorème en une phrase. Sa preuve est la suivante.

8. *Tout est forme.* Cyril Falcon

Preuve.
L'application

$$s: \quad \begin{array}{ccc} S & \longrightarrow & S \\ (x,y,z) & \longmapsto & \begin{cases} (x+2z,z,y-x-z) & \text{si } x < y-z \\ (2y-x,y,x-y+z) & \text{si } y-z < x < 2y \\ (x-2y,x-y+z,y) & \text{si } x > 2y \end{cases} \end{array}$$ □

où l'ensemble $S := \{(x,y,z) \in \mathbb{N}^3,\ x^2+4yz = p\}$ est fini, est une involution et a exactement un point fixe, donc $|S|$ est impair et l'involution $(x,y,z) \mapsto (x,z,y)$ a aussi un point fixe.

Cette preuve demande néanmoins moult vérifications techniques laissées en exercice au lecteur. Nous sommes le lecteur, nous faisons ces vérifications.

L'ensemble S est clairement fini car les points choisis sont à coordonnées positives.

Pour montrer que l'involution est bien définie, montrons que $2y \geqslant y-z$, et que $x \neq y-z$ et $x \neq 2y$, le tout avec $(x,y,z) \in S$ bien sûr.
Si $2y < y-z$, alors $y < -z$, donc $y < 0$ car $z \geqslant 0$, ce qui est absurde car $y \in \mathbb{N}$.
Si $x = y-z$, alors

$$\begin{aligned} x^2-4yz = p &\iff (y-z)^2-4yz = p \\ &\iff y^2+z^2+2yz = p \\ &\iff (y+z)^2 = p. \end{aligned}$$

Or p est un nombre premier congru à 1 modulo 4, donc $p \geqslant 5$, donc $y \geqslant 1$ ou $z \geqslant 1$, donc p se factorise, donc p n'est pas premier, ce qui est absurde.
Si $x = 2y$, alors

$$\begin{aligned} x^2-4yz = p &\iff (2y)^2-4yz = p \\ &\iff 4y(y-z) = p. \end{aligned}$$

Donc p est congru à 0 modulo 4, ce qui est absurde.

Montrons que cette involution... est une involution. On l'appellera désormais s.
Soit $(x,y,z) \in S$.

- Si $x < y-z$.
  Alors $s(x,y,z) = (x+2z,z,y-x-z) =: (X,Y,Z)$.
  Or $X > 2Y$ car $x+2z > 2z$ car $x > 0$ car $(x,y,z) \in S$ et p est congru à 1 modulo 4.
  Donc

$$\begin{aligned} s^2(x,y,z) &= s(X,Y,Z) \\ &= (X-2Y,X-Y+Z,Y) \\ &= (x+2z-2z,x+2z-z+y-x-z,z) \\ &= (x,y,z), \end{aligned}$$

donc s est bien une involution dans ce cas.

- Si $y-z<x<2y$.
  Alors $s(x,y,z)=(2y-x,y,x-y+z)=:(X,Y,Z)$.
  Or $X<2Y$ car $2y-x<2y$ car $x>0$ car $(x,y,z)\in S$ et p est congru à 1 modulo 4.
  Et $X>Y-Z$ car $Y-Z=y-x+y-z=2y-x-z=X-z$ et car $z>0$ car $(x,y,z)\in S$ et p est premier.
  Donc $Y-Z<X<2y$.
  Donc

$$\begin{aligned} s^2(x,y,z) &= s(X,Y,Z) \\ &= (2Y-X,Y,X-Y+Z) \\ &= (2y-2y+x,y,2y-x-y+x-y+z) \\ &= (x,y,z), \end{aligned}$$

  donc s est bien une involution dans ce cas.

- Si $x>2y$.
  Alors $s(x,y,z)=(x-2y,x-y+z,y)=:(X,Y,Z)$.
  Or $X<Y-Z$ car $x-2y<x-y+z-y=X+z$ car $x>0$ car $z>0$ car $(x,y,z)\in S$ et p est premier.
  Donc

$$\begin{aligned} s^2(x,y,z) &= s(X,Y,Z) \\ &= (X+2Z,Z,Y-X-Z) \\ &= (x-2y+2y,y,x-y+z-x+2y-y) \\ &= (x,y,z), \end{aligned}$$

  donc s est bien une involution dans ce cas.

Finalement, dans tous les cas, s est bien une involution.

Montrons que s a exactement un point fixe.
Soit p un nombre premier de la forme $4k+1$.
On a $(1,1,k)\in S$ car $1^2+4\times 1\times k=1+4k=p$.
On a $1-1<1<2\times 1$, donc $s(1,1,k)=(2\times 1,1,1-1+k)=(1,1,k)$.

Donc (1,1,k) est un point fixe de s.
C'est le seul car s est une involution (différente de l'identité) donc s est bijective.

Montrons que $|S|$ est impair.
Notons M l'ensemble des points bougés par s.
Alors si $m \in M$, $s(m) \neq m$, et $m = s^2(m) \neq s(m) \in M$, donc les points de M vont tous par deux.
Donc $|M|$ est pair.
Comme s a un unique point fixe d'après précédemment, $|S \setminus M| = 1$.
Donc $|S|$ est impair.

L'application $(x,y,z) \mapsto (x,z,y)$ est clairement une involution sur S.
De plus comme le cardinal de S est impair d'après précédemment, cette application a au moins un moins fixe sur S, notons le (α,β,γ).
On a donc $(\alpha,\beta,\gamma) = (\alpha,\gamma,\beta)$, donc $\beta = \gamma$.
De plus ce triplet est dans S, donc $\alpha^2 + 4\beta\beta = p$, donc

$$\alpha^2 + (2\beta)^2 = p.$$

Finalement, p peut s'écrire comme somme de deux carrés.

1.2.2 Quelques propositions utiles

Proposition 1 Soit p un nombre premier.

$$(-1) \text{ est un carré modulo } p \iff (p = 2 \text{ ou } p \equiv 1 \pmod 4).$$

Preuve.
Supposons dans un premier temps que -1 est un carré modulo p, *i.e.* il existe $\alpha \in \mathbb{Z}$ tel que

$$\alpha^2 = -1 \pmod p.$$

Alors ou bien $p = 2$, ou bien p est impair.
On suppose $p \geqslant 3$.
Dans $(\mathbb{Z}/p\mathbb{Z})^*$, -1 est d'ordre 2.
Or on a

$$1 = (-1)^2 = (\alpha^2)^2 = \alpha^4,$$

donc l'ordre de α dans $(\mathbb{Z}/p\mathbb{Z})^*$ divise 4.
On a clairement $\alpha \neq 1$, donc l'ordre de α vaut 2 ou 4.
Or si l'ordre de α était 2, alors

$$\alpha^2 = 1$$

donc

$$(\alpha - 1)(\alpha + 1) = 0.$$

Donc α serait égal à 1 ou à -1 car $(\mathbb{Z}/p\mathbb{Z})^*$ est intègre car p est premier, et c'est impossible car $p \geqslant 3$.
L'ordre de α est donc 4, or d'après le théorème de Lagrange [9] pour les groupes finis,

9. Encore lui !

l'ordre de α divise le cardinal du groupe.
Donc

$$4 \mid p-1$$

donc

$$p \equiv 1 \pmod 4.$$

Réciproquement, supposons que $p \equiv 1 \pmod 4$ et notons g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$, qui est un groupe cyclique car p est premier.
Alors

$$-1 = g^k,$$

donc

$$g^{2k} = 1.$$

Ainsi,

$$p-1 \mid 2k$$ □

Et $4 \mid p-1$ donc k est pair.
Finalement, $-1 = \left(g^{\frac{k}{2}}\right)^2$ est bien un carré modulo p.

Proposition 2 Soit p un nombre premier, alors

$$\exists (a,b) \in \mathbb{N}^2 \quad p = a^2 + b^2 \iff (p = 2 \text{ ou } p \equiv 1 \pmod 4).$$

Preuve.
Le sens direct de l'équivalence est clair. En effet, une somme de deux carrés est toujours égale à 0, 1 ou 2 dans $\mathbb{Z}/4\mathbb{Z}$.
Réciproquement, si $p = 2$, alors $p = 1^2 + 1^2$.
Sinon, $p \equiv 1 \pmod 4$.
Alors, d'après la proposition 1, (-1) est un carré modulo p.
Soit $m \in \mathbb{N}$ tel que $m^2 \equiv -1 \pmod p$.
Alors il existe $k \in \mathbb{Z}$ tel que $m^2 = -1 + kp$.
Ainsi $m^2 + 1 = kp$, donc

$$(m+i)(m-i) = kp.$$

Donc

$$p \mid (m+i)(m-i).$$

On raisonne à présent par l'absurde.
Supposons que p est premier dans $\mathbb{Z}[i]$.
Alors

$$p \mid (m+i) \text{ ou } p \mid (m-i)$$

ce qui est clairement faux.
On en déduit que p n'est pas premier dans $\mathbb{Z}[i]$.
Il existe donc $(z_1,z_2) \in \mathbb{Z}[i]^2$ tel que $p = z_1 z_2$.
On calcule la norme de cette égalité :

$$N(z_1)N(z_2) = N(p) = p^2.$$

Or p n'est pas premier, donc $N(z_1) \neq 1$.
Ainsi,

$$N(z_1) = p = a^2 + b^2.$$

□

2 Trouver un autre titre (différent du premier)

2.1 Théorème de Lagrange

Théorème 4 Tout entier positif peut s'exprimer comme la somme de quatre carrés d'entiers.

Remarque 3 Subjugué par la beauté de ce théorème, la première réaction du mathématicien sera certainement de partager ce délice arithmétique au monde qui l'entoure. Cependant, poster sur tous les réseau sociaux : "Tout entier est somme de quatre carrés ! ! ! #Lagrange #funnymoment #goyave" ne satisfera sûrement pas son besoin de communication. La mathématicien se pose alors la question ontologique suivante : comment expliquer ce pimpant théorème à quelqu'un qui ignore tout de l'arithmétique ?

Vous pouvez réaliser l'expérience suivante chez vous (attention, ce protocole peut présenter un danger si vous vivez seul !).

1. Munissez-vous d'un individu étranger aux divins astres mathématiques qui vous habitent. Présentez-lui un ensemble de pièces carrées identiques (une boite de briques emboitables d'une célèbre société danoise fera l'affaire).
2. Demandez-lui d'en saisir un certain nombre. Puis demandez-lui de constituer quatre carrés (ou moins) à l'aide de ces objets.
3. Une fois qu'il y sera parvenu plus ou moins rapidement en fonction du nombre d'objets initialement choisi, dites-lui qu'une telle reconstitution est possible quel que soit le nombre d'objets. Devant son air dubitatif, proposez-lui de recommencer avec quelques objets en plus ou en moins.
4. Par récurrence immédiate, lorsqu'il sera courbatu de former tout ces carrés, il acceptera le théorème avec certitude.

Recommencez ensuite l'expérience autant de fois que cela vous appète. Pensez juste à changer votre cobaye entre chaque utilisation.

2.2 Démonstration du théorème de Lagrange

Nous démontrerons ici le théorème de Lagrange grâce au corps gauche des quaternions $\mathbb{H}$.

Bien qu'une démonstration plus élémentaire puisse être faite, les quaternions nous semblent un objet suffisamment intéressant en soi pour que l'excuse de la démonstration du théorème de Lagrange soit une raison valable pour les étudier un peu.

Définition 12 On appelle *quaternion* un élément de $\mathbb{R}[i,j,k]$ où i,j et k vérifient les relations

$$i^2 = j^2 = k^2 = ijk = -1.$$

Remarque 4 L'ensemble des quaternions est un corps gauche.

Définition 13 Soit $\alpha \in \mathbb{H}$ un quaternion, on appelle (a_0,a_1,a_2,a_3) ses *coordonnées* si

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k.$$

On dira que α est *entier* si ses coordonnées sont soient toutes entières, soient toutes demi-entières.
On note $\mathbb{Z}_{\frac{1}{2}} := \left\{ \frac{n}{2},\ n \text{ entier impair} \right\}$ l'ensemble des *demi-entiers*.

Si $\alpha \in \mathbb{H} \setminus \{0\}$ est un quaternion entier tel que α^{-1} soit aussi un entier, on dira que α est une *unité*.

On dira que $\alpha,\beta \in \mathbb{H}$ sont *associés* s'il existe $\varepsilon \in \mathbb{H}$ une unité telle que

$$\alpha = \beta\varepsilon \text{ ou } \alpha = \varepsilon\beta.$$

On définit la norme N d'un quaternion $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ comme

$$N(\alpha) = \sum_{i=1}^{4} a_i^2.$$

On défini le conjugué d'un quaternion $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ comme

$$\overline{\alpha} = a_0 - a_1 i - a_2 j - a_3 k.$$

On définit la *parité* d'un quaternion comme la parité de sa norme.

On dit que β *divise* α *à gauche* (resp. *à droite*) si $\alpha = \beta\gamma$ (resp. $\alpha = \gamma\beta$).

On dit que δ est le *plus grand diviseur commun à droite* (resp. *à gauche*) si

(i) δ est un diviseur à droite (resp. à gauche) de α et β,

(ii) tout diviseur à droite (resp. à gauche) de α et β est un diviseur à droite (resp. à gauche) de δ.

Proposition 3 La norme est multiplicative sur $\mathbb{H}$.

Preuve.
Soient $q_1 = a + bi + cj + dk$ et $q_2 = e + fi + gj + hk$ dans $\mathbb{H}$.
Tout d'abord, on rappelle que :

$$\|q_1\| = a^2 + b^2 + c^2 + d^2,$$

et

$$\|q_2\| = e^2 + f^2 + g^2 + h^2.$$

Ensuite, on cherche à exprimer le produit de q_1 et q_2 :

$$\begin{aligned} q_1 q_2 &= (a + bi + cj + dk)(e + fi + gj + hk) \\ &= (ae - bf - cg - dh) + (af + be + ch - dg)i + (ag - bh + ce + df)j + (ah + bg - cf + de)k. \end{aligned}$$

Ainsi, on a

$$\|q_1q_2\| = (ae-bf-cg-dh)^2+(af+be+ch-dg)^2+(ag-bh+ce+df)^2+(ah+bg-cf+de)^2.$$

En développant, les termes vont se simplifier deux à deux, et il reste :

$$\begin{aligned}\|q_1q_2\| &= a^2\underbrace{(e^2+f^2+g^2+h^2)}_{\|q_2\|}+b^2\|q_2\|+c^2\|q_2\|+d^2\|q_2\| \\ &= (a^2+b^2+c^2+d^2)\|q_2\| \\ &= \|q_1\|\|q_2\|, \end{aligned}$$ □

ce qui prouve bien que la norme N est multiplicative.

Lemme 1 Les unités sont les quaternions de norme 1.

Preuve.
Si ε est une unité, alors $\varepsilon\varepsilon^{-1} = 1$, donc par multiplicativité de la norme des quaternions, $N(\varepsilon)N(\varepsilon^{-1}) = N(1) = 1$. Donc car la norme d'un quaternion entier est à valeurs dans $\mathbb{N}$, on a $N(\varepsilon) = 1$.
Réciproquement, si α est un quaternion entier tel que $N(\alpha) = 1$. Alors car $\alpha\overline{\alpha} = N(\alpha) = 1$, on a $\alpha^{-1} = \overline{\alpha}$ qui est bien un quaternion entier. Donc α est une unité. □

Lemme 2 • Si α est un quaternion entier, alors il existe β associé à α tel que β soit à coordonnées entières.

• Si α est impair, alors il existe β associé à α tel que β soit à coordonnées non entières.

Preuve.
Prouvons chacun des • séparément [10].

• Si α est à coordonnées entières, alors notre travail s'arrête ici, sinon α a des coordonnées toutes demi-entières. On peut donc choisir des signes $\pm$ tels que

$$\alpha = \underbrace{b_0+b_1i+b_2j+b_3k}_{\beta}+\underbrace{\frac{1}{2}(\pm1\pm i\pm j\pm k)}_{\gamma}.$$

avec les b_i pairs.
Comme $N(\gamma) = 1$, d'après le lemme 1, γ est une unité, donc $\overline{\gamma}$ est aussi une unité.
On a

$$\alpha\overline{\gamma} = \beta\overline{\gamma}+\gamma\overline{\gamma} = \beta\overline{\gamma}+N(\gamma) = \beta\overline{\gamma}+1,$$

Comme β a ses coordonnées paires, $\beta\overline{\gamma}$ est à coordonnées entières.
Finalement, $\alpha\overline{\gamma}$ est à coordonnées entières.

10. Cicéron c'est Poincaré.

- Si α est impair, alors il existe $(\delta_i)_{0\leqslant i\leqslant 3} \in \{0,1\}^4$ tel que

$$\alpha = \underbrace{b_0 + b_1 i + b_2 j + b_3 k}_{\beta} + \underbrace{\delta_0 + \delta_1 i + \delta_2 j + \delta_3 k}_{\gamma},$$

avec les b_i pairs.
Comme $N(\alpha)$ est impaire, soit un unique δ_i vaut 1, soit exactement trois d'entre eux valent 1.
De même que précédemment, tout associé de β a des coordonnées entières, il faut donc vérifier qu'un associé de γ a quant à lui des coordonnées non entières.
Pour cela il faut distinguer les cas, *i.e.* vérifier que chacun des huit quaternions suivants a un associé qui a des coordonnées non entières : 1, i, j, k, $1+i+j$, $1+j+k$, $1+i+k$ et $i+j+k$.
On remarque que

$$\rho := \frac{1}{2}(1+i+j+k) \tag{1}$$

est une unité car $N(\rho) = 1$.
Si $\gamma \in \{1,i,j,k\}$, alors $\gamma\rho$ a des coordonnées non entières.
Si $\gamma = 1+i+j$, alors

$$\gamma = 1+i+j = \underbrace{(1+i+j+k)}_{\lambda} - k.$$

Or

$$\lambda\overline{\rho} = (1+i+j+k)\frac{1}{2}(1-i-j-k) = 2\rho\overline{\rho} = 2 \qquad \square$$

qui est à coordonnées entières, mais $k\overline{\rho}$ n'est pas à coordonnées entières.
Donc $\gamma\overline{\rho}$ est un associé de γ à coordonnées non entières.
On traite les trois derniers cas par symétries.

Lemme 3 Tout quaternion entier s'écrit sous la forme

$$k_0\rho + k_1 i + k_2 j + k_3 k \tag{2}$$

où ρ est défini en (1), et $(k_i)_{0\leqslant i\leqslant 3} \in \mathbb{Z}^4$.

Preuve.
Selon la parité de k_0, tout quaternion sous la forme (2) a toutes ses coordonnées demi-entières, ou toutes ses coordonnées entières, c'est donc bien un quaternion entier.
Réciproquement, si $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ est un quaternion entier.
Posons

$$\begin{cases} k_0 := 2a_0 \\ \forall i \in \{1,2,3\} \quad k_i := a_i - a_0. \end{cases}$$

On remarque alors que $\alpha = k_0 + k_1 i + k_2 j + k_3 k$ est bien de la forme (2). $\square$

Lemme 4 (Pseudo-Hurwitz) Si κ est un quaternion entier et $m \in \mathbb{N}$, alors il existe λ un quaternion entier tel que

$$N(\kappa - m\lambda) < m^2.$$

Preuve.
Si $m = 1$, il suffit de choisir $\lambda := \kappa$ qui est un quaternion entier car κ l'est et nous avons terminé.
Sinon, $m \geqslant 2$.
On écrit alors κ et gamma sous la forme (2) ce qui est possible d'après le lemme 3. Ainsi,

$$\begin{cases} \kappa = k_0\rho + k_1 i + k_2 j + k_3 k \\ \lambda = \ell_0\rho + \ell_1 i + \ell_2 j + \ell_3 k \end{cases}$$

avec $(k_0,k_1,k_2,k_3,\ell_0,\ell_1,\ell_2,\ell_3) \in \mathbb{Z}^8$.
On a alors

$$\begin{aligned} \kappa - m\lambda = &\frac{1}{2}(k_0 - m\ell_0) \\ &+ \frac{1}{2}(k_0 + 2k_1 - m(\ell_0 + 2\ell_1))i \\ &+ \frac{1}{2}(k_0 + 2k_2 - m(\ell_0 + 2\ell_2))j \\ &+ \frac{1}{2}(k_0 + 2k_3 - m(\ell_0 + 2\ell_3))k. \end{aligned}$$

On va maintenant choisir correctement les ℓ_i pour finir de démontrer le lemme.
On effectue la division euclidienne de k_0 par m, ainsi il existe ℓ_0 tel que

$$k_0 = m\ell_0 + r_0 \quad \text{avec } 0 \leqslant r_0 < m.$$

Si $r_0 \geqslant \frac{m}{2}$, alors on remplace ℓ_0 par $\ell_0 + 1$ de sorte à ce qu'on ait toujours

$$|r_0| \leqslant \frac{m}{2}.$$

Ainsi,

$$\left(\frac{1}{2}(k_0 - m\ell_0)\right)^2 \leqslant \frac{m^2}{16}.$$

On effectue ensuite de façon similaire la division euclidienne de $k_0 + 2k_1 - m\ell_0$ par $2m$ pour trouver ℓ_1 de sorte à ce que

$$\left(\frac{1}{2}(k_0 + 2k_1 - m(\ell_0 + 2\ell_1))\right)^2 \leqslant \frac{m^2}{4}.$$

On fait de même pour trouver ℓ_1 et ℓ_2.
Ainsi,

$$N(\kappa - m\lambda) \leqslant \frac{m^2}{16} + 3\frac{m^2}{4} = \frac{13}{16}m^2 < m^2,$$

ce qui démontre le lemme. □

Lemme 5 (Division euclidienne) Soient α et $\beta \neq 0$ des quaternions entiers, alors il existe des quaternions entiers λ et γ tels que

$$\alpha = \lambda\beta + \gamma, \text{ avec } N(\gamma) < N(\beta).$$

Preuve.
Posons $\kappa := \alpha\overline{\beta}$ et $m = \beta\overline{\beta} = N(\beta)$.
On applique le lemme 4 à κ et m, ce qui nous donne donc l'existence d'un quaternion entier λ tel que

$$N(\kappa - m\lambda) < m^2.$$

Posons

$$\gamma := \alpha - \lambda\beta.$$

On a alors car $\beta \neq 0$ donc $N(\overline{\beta}) = \frac{1}{m}$

$$\begin{aligned} N(\gamma) &= N(\alpha - \lambda\beta) \\ &\leqslant N(\alpha - \lambda\beta)N(\overline{\beta})\frac{1}{m} \\ &= \frac{1}{m}N(\alpha\overline{\beta} - \lambda\beta\overline{\beta}) \\ &= \frac{1}{m}N(\kappa - \lambda m) \\ &< \frac{1}{m}m^2 \\ &= m \\ &= N(\beta). \end{aligned}$$

□

Définition 14 Soit $\mathfrak{I}$ un ensemble de quaternions entiers, on dit que $\mathfrak{I}$ est un *idéal à droite* (resp. *à gauche*) si

(i) $\mathfrak{I}$ est un sous-groupe additif de $\mathbb{H}$,

(ii) pour tout $\alpha \in \mathfrak{I}$ et pour tout quaternion entier λ, $\lambda\alpha \in \mathfrak{I}$ (resp. $\alpha\lambda \in \mathfrak{I}$).

Lemme 6 (Principalité) Tout idéal à droite est principal.

Preuve.
Soit S un idéal à droite, alors tous les éléments de $S \setminus \{0\}$ sont des quaternions entiers, donc l'ensemble

$$\{N(s),\ s \in S \setminus \{0\}\}$$

est discret.
Il admet donc un minimum.
Soit $\delta \in S$ réalisant ce minimum.

Soit $\alpha \in S$, alors comme S est un idéal à droite, pour tout quaternion entier λ,

$$\alpha - \lambda\delta \in S.$$

Comme α et δ sont deux quaternions entiers et que $\delta \neq 0$, on peut d'après le lemme 5 effectuer la "division euclidienne" de α par δ.
Ainsi, il existe λ et γ deux quaternions entiers tels que

$$\begin{cases} \alpha = \lambda\delta + \gamma \\ N(\gamma) < N(\delta). \end{cases}$$

Donc

$$N(\gamma) = N(\underbrace{\alpha - \lambda\delta}_{\in S}) < N(\delta),$$

donc $\gamma = \alpha - \lambda\delta = 0$ car δ minimise la norme sur $S \setminus \{0\}$.
Donc $\alpha = \lambda = \delta$, donc

$$S = (\delta),$$

donc S est principal. □

Lemme 7 (Pseudo-Bézout) Soient α et $\beta \neq 0$ deux quaternions entiers, non tous deux nuls. Alors leur plus grand diviseur commun à droite δ existe et est unique à multiplication à gauche par une unité près.
De plus, il existe μ et ν quaternions entiers tels que

$$\delta = \mu\alpha + \nu\beta.$$

On note $\delta =: (\alpha,\beta)$.

Preuve.
Soient α et $\beta \neq 0$ deux quaternions entiers, non tous deux nuls.
Commençons par l'existence.
Posons

$$S := \{\mu\alpha + \nu\beta,\ \mu \text{ et } \nu \text{ quaternions entiers}\}.$$

Soient $(\mu\alpha + \nu\beta, \mu'\alpha + \nu'\beta) \in S^2$ et λ un quaternion entier.
Alors

(i) $\mu\alpha + \nu\beta \pm (\mu'\alpha + \nu'\beta) = (\mu \pm \mu')\alpha + (\nu \pm \nu')\beta \in S$,
(ii) $\lambda(\mu\alpha + \nu\beta) = (\lambda\mu)\alpha + (\lambda\nu)\beta \in S$,

donc S est un idéal à droite.
Donc d'après le lemme 6, S est principal.
Il existe donc $\delta \in S$ tel que $S = (\delta)$.
Comme $\delta \in S$, il existe μ et ν des quaternions entiers tels que

$$\delta = \mu\alpha + \nu\beta.$$

Comme $(\alpha,\beta) \in S^2$, il existe deux quaternions entiers λ et λ' tels que

$$\begin{cases} \alpha = \lambda\delta \\ \beta = \lambda'\delta. \end{cases}$$

Donc δ est un diviseur commun à droite à α et β.
Si δ' est aussi un diviseur commun à droite à α et β, alors

$$\delta' \mid \mu\alpha + \nu\beta = \delta,$$

ce qui montre que δ est le plus grand diviseur commun à droite à α et β.

Reste l'unicité à multiplication par une unité près.
Si δ et δ' vérifient tous deux cette propriété, alors

$$\begin{cases} \delta \mid \delta' \\ \delta' \mid \delta, \end{cases}$$

donc il existe λ et λ' deux quaternions entiers tels que

$$\begin{cases} \lambda\delta = \delta' \\ \lambda'\delta' = \delta. \end{cases}$$

Donc

$$\delta' = \lambda\delta = \lambda\lambda'\delta'$$

donc

$$\lambda\lambda' = 1$$

et donc λ et λ' sont des unités. □

Lemme 8 Soient α un quaternion entier et $m \in \mathbb{N}_{>0}$, alors

$$(\alpha,m) = 1 \iff (N(\alpha),m) = 1.$$

Preuve.
Soit α un quaternion entier $m \in \mathbb{N}_{>0}$.
Alors d'après le lemme 7, il existe deux quaternions entiers μ' et ν' tels que

$$\varepsilon \cdot 1 = \mu'\alpha + \nu' m,$$

où ε est une unité.
Donc en posant $\mu := \varepsilon^{-1}\mu'$ et $\nu := \varepsilon^{-1}\nu'$, on a

$$1 = \mu\alpha + \nu m.$$

On a

$$\begin{aligned} N(\mu)N(\alpha) &= N(\mu\alpha) \\ &= N(1-\nu m) \\ &= (1-\nu m)(1-\overline{\nu} m) \\ &= 1 - (\nu + \overline{\nu})m + m^2 N(\nu). \end{aligned}$$

Or

$$\left(N(\mu)N(\alpha) = 1 - (\nu+\overline{\nu})m + m^2 N(\nu)\right) \Longrightarrow \left(0 \equiv 1 \pmod{(N(\alpha),m)}\right),$$

donc

$$(N(\alpha),m) = 1.$$

Pour la réciproque, nous procédons par contraposée.
Si α et m sont tels que $(\alpha,m) = \delta$ avec δ qui n'est pas associé à 1, *i.e.* δ n'est pas une unité.
Alors par multiplicativité et additivité de la norme, et en choisissant μ et ν comme dans le lemme 7,

$$N(\delta) = N(\mu)N(\alpha) + N(\nu)N(m).$$

Ainsi, car μ,ν et m sont entiers, et car δ n'est pas une unité,

$$1 < N(\delta) = \mu^2 N(\alpha) + \nu^2 m^2.$$

Or si un quaternion est entier, alors ses coordonnées sont toutes entières ou toutes demi-entières, donc sa norme (qui rappelons est la somme du carré des coordonnées), est entière.
Nous avons donc obtenu un relation de Bézout dans $\mathbb{Z}$ avec $N(\delta) > 1$, donc

$$(N(\alpha),m) > 1,$$

ce qui conclut la démonstration. □

Définition 15 On dit qu'un quaternion π est *premier* si π n'est pas une unité et que ses seuls diviseurs sont ses associés et les unités.

Lemme 9 Un nombre premier n'est pas un quaternion premier. Jamais. Impossible.

Preuve.
Comme souvent en arithmétique, 2 est un nombre premier un peu à part. Nous lui procurons donc le traitement qu'il mérite.
On a

$$2 = (1+i)(1-i),$$

donc 2 n'est pas un quaternion premier car $(1+i)$ et $(1-i)$ (de norme 2) ne sont pas des unités (ni 2 d'ailleurs).
Soit maintenant p un nombre premier impair.
Considérons les ensembles

$$\begin{cases} A := \left\{ x^2,\, 0 \leqslant x \leqslant \dfrac{p-1}{2} \right\} \\ \\ B := \left\{ -1-y^2,\, 0 \leqslant y \leqslant \dfrac{p-1}{2} \right\}. \end{cases}$$

Le nombre p est premier, donc $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc l'équation $x^2 = y \pmod p$ a exactement deux solutions, qui sont x et $-x$.
Ainsi, pour tous x, x' tels que $0 \leqslant x, x' \leqslant \dfrac{p-1}{2}$, $x \neq x' \pmod p$ implique $x^2 \neq x'^2 \pmod p$.
Donc

$$\mathrm{Card}(A) = \mathrm{Card}\left(\left\{ 0 \leqslant x \leqslant \frac{p-1}{2} \right\} \right) = \frac{p+1}{2}.$$

De même,

$$\mathrm{Card}(B) = \frac{p+1}{2}.$$

De plus A et B sont disjoints car $A \subset \mathbb{Z}_{\geqslant 0}$ et $B \subset \mathbb{Z}_{<0}$.
Donc

$$\mathrm{Card}(A \cup B) = \frac{p+1}{2} + \frac{p+1}{2} = p+1.$$

Comme il n'existe que p classes de congruences modulo p, il existe $(\alpha,\beta) \in (A \cup B)^2$ tel que $\alpha \neq \beta$ et

$$\alpha \equiv \beta \pmod p.$$

Or $A \cap B = \varnothing$, donc $(\alpha,\beta) \in A \times B$ ou $(\alpha,\beta) \in B \times A$.
Donc il existe $(x^2, -1-y^2) \in A \times B$ tel que

$$x^2 \equiv -1 - y^2 \pmod{p},$$

donc finalement, il existe $(x,y) \in \{1,\dots,p-1\}^2$ tel que

$$1 + x^2 + y^2 \equiv 0 \pmod{p}.$$

Posons

$$\gamma := 1 + xi + yj.$$

Alors

$$N(\gamma) = 1 + x^2 + y^2 \equiv 0 \pmod{p}.$$

Donc $(N(\gamma),p) > 1$, donc d'après le lemme 8, $(\gamma,p) = \delta$ avec δ qui n'est pas associé à 1, *i.e.* δ n'est pas une unité.
Il existe donc λ_1 et λ_2 tels que

$$\begin{cases} \gamma = \lambda_1 \delta \\ p = \lambda_2 \delta. \end{cases}$$

Si par l'absurde λ_2 était une unité, alors alors on aurait

$$\gamma = \lambda_1 {\lambda_2}^{-1} p,$$

et p diviserait γ, donc chacune de ses coordonnées.
On rappelle que $\gamma = 1 + xi + yj$, donc $p \mid 1$, ce qui est absurde.
Donc λ_2 n'est pas une unité, comme on a montré que δ n'en était pas une non plus, on en déduit que

$$p = \lambda_2 \delta$$

n'est pas premier. □

Armés, nous pouvons finir la preuve quaternionienne du théorème de Lagrange.

Soit

$$n := \prod_{p \text{ premier}} p^{v_p(n)}.$$

Alors par multiplicativité de la norme

$$N(n) = \prod_{p \text{ premier}} N(p)^{v_p(n)}.$$

Or on a déjà montré qu'un produit de sommes de quatre carrés reste une somme de quatre carrés.

Il suffit donc de montrer que tout nombre premier s'écrit comme somme de quatre carrés.
Soit p un nombre premier.
Alors d'après le théorème 9, il existe α et β deux quaternions entiers tels que

$$p = \alpha\beta.$$

On a

$$p^2 = N(p) = N(\alpha\beta) = \underbrace{N(\alpha)}_{\in\,\mathbb{Z}}\underbrace{N(\beta)}_{\in\mathbb{Z}},$$

Donc $N(\alpha) = N(\beta) = p$.
Si α n'est pas à coordonnées entières, alors il existe d'après le lemme 2 $\tilde{\alpha}$ associé à α, donc de même norme que α tel que $\tilde{\alpha}$ est des coordonnées entières.
On peut donc supposer, quitte à considérer $\tilde{\alpha}$, que α a des coordonnées entières $(a_1,a_2,a_3,a_4) \in \mathbb{Z}^4$.
Finalement,

$$p = N(\alpha) = \sum_{i=1}^{4} {a_i}^2,$$

ce qui démontre le théorème de Lagrange.

□ □
□ □

Le lecteur informé aura peut être initialement maudit la longueur de cette démonstration sachant qu'une preuve élémentaire de quelques pages aurait suffi. L'indicible beauté du corps des quaternions lui aura rapidement fait oublier son amertume, et c'est le sourire aux lèvres qu'il continuera son chemin.

Au cas où il resterait quelque sceptique doutant encore de l'intérêt des quaternions, fournissons à titre d'exemple un résultat bonus pouvant découler facilement de toute la théorie que nous avons commencé à élaborer.

Proposition 4 Si p est un nombre premier impair, alors $4p$ s'écrit comme somme de quatre carrés impairs.

Preuve.
Soit p un nombre premier impair, alors de même que dans la précédente démonstration on choisit α un quaternion tel que $p = N(\alpha)$.
On utilise de nouveau le lemme 2, mais cette fois-ci pour trouver $\tilde{\alpha}$ associé à α tel que les coordonnées de $\tilde{\alpha}$ soient demi-entières au cas où celles de α ne le seraient pas elles-mêmes.
Ainsi, quitte à remplacer α par $\tilde{\alpha}$ (tous deux de même norme), on peut supposer que les coordonnées de α sont demi-entières.
Il existe donc $(a_1,a_2,a_3,a_4) \in \mathbb{Z}^4$ tel que

$$\alpha = a_1 + \frac{1}{2} + \left(a_2 + \frac{1}{2}\right) i + \left(a_3 + \frac{1}{2}\right) j + \left(a_4 + \frac{1}{2}\right) k.$$

Donc

$$p = N(\alpha) = \sum_{i=1}^{4} \left(a_i + \frac{1}{2}\right)^2,$$

donc

$$4p = \sum_{i=1}^{4} (2a_i + 1)^2.$$

□

3 Randonnées sylvestres

3.1 Algogo à gogo

L'heure est maintenant venue, le glas a sonné. Quelques expérimentations heuristiques ne seraient pas de trop, n'est-il pas ? Comme toujours, les mathématiques se conçoivent avant de se formaliser. Il serait donc intéressant de voir ce qu'il se passe concrètement au travers du théorème de Lagrange.
Rappelons pour l'étourdi qui aura profité de cette belle matinée pour lire ce mémoire sur un banc public et par là même fut distrait par l'écureuil non loin : le théorème de Lagrange stipule que tout entier s'écrit comme somme d'au plus quatre carrés. Mais cela ne répond ni au nombre minimal d'entiers nécessaires pour représenter un entier donné, ni au nombre de façon de décomposer un entier comme somme de quatre carrés [11].

Définition 16 On appelle Lag [12] la fonction arithmétique qui à un entier n donné fait correspondre le nombre minimal k d'entiers positifs $(x_1,\ldots,x_k)$ nécessaires pour représenter n sous la forme

$$n = \sum_{l=1}^{k} {x_l}^2.$$

Autrement dit

$$\forall n \in \mathbb{N} \quad \mathrm{Lag}(n) = \min\left\{k,\, \exists (x_1,\ldots,x_k) \in \mathbb{N}^k \quad n = \sum_{l=1}^{k} {x_l}^2\right\}.$$

Le théorème de Lagrange dit exactement que

$$\forall n \in \mathbb{N} \quad \mathrm{Lag}(n) \leqslant 4.$$

Les *carrés parfaits* sont les nombres n vérifiant $\mathrm{Lag}(n) \leqslant 1$.
L'application Lag n'est pas multiplicative, bien qu'on puisse énoncer des résultats plus faibles, comme

$$\forall (m,n) \in \mathbb{N}^2 \quad (\mathrm{Lag}(m) \leqslant 2 \text{ et } \mathrm{Lag}(n) \leqslant 2) \Rightarrow \mathrm{Lag}(mn) \leqslant 2.$$

Définition 17 On appelle $\mathscr{N}$ la fonction arithmétique qui a un entier n donné fait correspondre le nombre total de décompositions de n comme somme de quatre carrés d'entiers positifs (éventuellement nuls).
Autrement dit

$$\forall n \in \mathbb{N} \quad \mathscr{N}(n) = \#\left\{(x_1,x_2,x_3,x_4) \in \mathbb{N}^4,\ \sum_{i=1}^{4} {x_i}^2 = n\right\}.$$

11. Certains carrés pouvant être égaux à 0, mais pas négatifs (dans cette partie uniquement, ils auront bientôt le loisir d'être aussi négatifs qu'ils le souhaitent).
12. Quel est le bruit de l'arithméticien quand il se noie ? Laglaglaglaglag...

Le théorème de Lagrange assure la non-annulation de cette application.

Nous allons maintenant donner quelques algorithmes qui calculent les valeurs de ces fonctions pour nous. Tous les algorithmes donnés seront écrits en Sage [13].
Commençons par donner un algorithme calculant trois choses distinctes, pour tous les entiers positifs inférieurs à l'argument n donné à l'algorithme. La première liste renvoyée correspond aux valeurs de $\mathscr{N}$. La deuxième liste donne une [14] décomposition en somme de quatre carrés telle que cette décomposition utilise le moins de nombre non nuls possible. La troisième liste correspond aux valeurs de Lag.

```
def decompojusk(n):
    N=[0 for x in [0..n]];
    D=[[-1,-1,-1,-1] for x in [0..n]];
    T=[5 for x in [0..n]]
    N[0]=1;
    D[0]=[0,0,0,0];
    T[0]=1;
    for i in [1..sqrt(n)]:
        I=i^2;
        for j in [0..min(sqrt(n-I),i)]:
            J=j^2
            for k in [0..min(sqrt(n-I-J),j)]:
                K=k^2;
                for l in [0..min(sqrt(n-I-J-K),k)]:
                    R=I+J+K+l^2;
                    if j==0:
                        taille=1;
                    elif k==0:
                        taille=2;
                    elif l==0:
                        taille=3;
                    else:
                        taille=4;
                    N[R]=N[R]+factorial(taille);
                    if D[R][0]==-1:
                        D[R][0]=i;
                        D[R][1]=j;
                        D[R][2]=k;
                        D[R][3]=l;
                        T[R]=taille;
                    elif taille<4:
                            if D[R][taille]>0:
                                D[R][0]=i;
                                D[R][1]=j;
                                D[R][2]=k;
```

13. Qu'est-ce qu'un S ? C'est un sage sans âge...
14. Et non la...

```
                D[R][3]=l;
                T[R]=taille;


    return [N,D,T]
```

À titre d'exemple que nous espérons éclairant, donnons le résultat de cet algorithme pour $n = 20$.

```
decompojusk(20):
        [[1, 1, 2, 6, 25, 2, 6, 24, 2, 7, 26, 6, 30, 26, 6, 24,\\
25, 8, 32, 30, 26], [[0, 0, 0, 0], [1, 0, 0, 0], [1, 1, 0, 0],\\
[1, 1, 1, 0], [2, 0, 0, 0], [2, 1, 0, 0], [2, 1, 1, 0], [2, 1,\\
1, 1], [2, 2, 0, 0], [3, 0, 0, 0], [3, 1, 0, 0], [3, 1, 1, 0],\\
[2, 2, 2, 0], [3, 2, 0, 0], [3, 2, 1, 0], [3, 2, 1, 1], [4, 0,\\
0, 0], [4, 1, 0, 0], [3, 3, 0, 0], [3, 3, 1, 0], [4, 2, 0, 0]],\\
[1, 1, 2, 3, 1, 2, 3, 4, 2, 1, 2, 3, 3, 2, 3, 4, 1, 2, 2, 3, 2]]
```

Ceci étant fait, l'envie qui nous vient est de nous servir de cet algorithme pour faire des choses. Plein de choses. Commençons par l'utiliser pour décomposer chaque entier entre 0 et 30 comme somme de carrés (avec le moins de nombres possibles dans la décomposition s'il vous plaît !).
Pour cela nous avons besoin d'un petit algorithme, dont l'unique but sera de présenter joliment le travail déjà effectué par `decompojusk`. Le voici.

```
def affichejoliment(L):
    i=-1
    for d in L:
        i=i+1;
        if d[0]==0:
            print "0=0"
        elif d[1]==0:
            print `i`+"="+`d[0]`+"^2"
        elif d[2]==0:
            `i`+"="+`d[0]`+"^2+"+`d[1]`+"^2"
        elif d[3]==0:
            `i`+"="+`d[0]`+"^2+"+`d[1]`+"^2+"+`d[2]`+"^2"
        else:
            print `i`+"="+`d[0]`+"^2+"+`d[1]`+"^2+"+`d[2]`\\
+"^2+"+`d[3]`+"^2"
```

Ce qui nous donne finalement (après remise en forme) :

Etagre cube Modulo 4 cases carré? Pin massif

34,90€

Voir l'offre

Ajouter aux favoris

- INFORMATIONS UTILES

Livraison : 2 jours

Frais de port : 20€

Vendu par la boutique : Meubles en pin pas cher

Référence : 352714

Catégories du produit : meubles , étagères & bibliothèques , meubles de rangement , étagères , naturel .

- DESCRIPTION

Etagre cube Modulo 4 cases carr pin massif Brut. Ce modulo de rangement ÊenÊpin massif Brut peut tre utilis seul, ou s'associer Êla gamme de meubles MODULO empiler et adapter de faon horizontale ou verticale au gr de vos besoins. Le + produit : de finition BRUT il est totalement personnalisable vous pouvez le peindre ou le customiser selon vos envies (voir rubrique accessoires) . Pour plus de rangement penser insrer notre caisse adaptable avec poignes.

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

Toujours grâce à l'algorithme `decompojusk`, nous pouvons sans effort tracer les valeurs de la fonction Lag pour $0 \leqslant n \leqslant 100$, ce qui est donné dans la figure 1. On peut remarquer que les entiers n vérifiant $\mathrm{Lag}(n) \in \{2,3\}$ sont plus nombreux que ceux vérifiant $\mathrm{Lag}(n) \in \{1,4\}$. Ce qui est tempéré existe-il toujours en majorité ? Ce qui sort de la norme est-il nécessairement rare ?

Nous ne tenterons pas ici de répondre à ces questions, pourtant captivantes. Nous nous contenterons seulement de rappeler le célèbre syllogisme paradoxal :

Tout ce qui est rare est cher.
Or un cheval bon marché est rare.
Donc un cheval bon marché est cher.

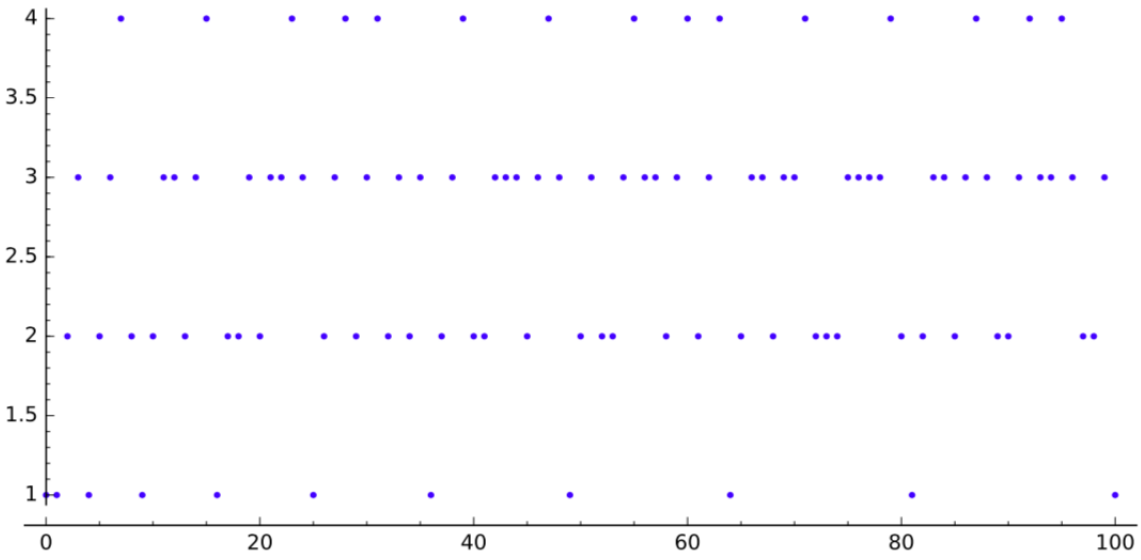


FIGURE 1 – Lag(n) pour $0 \leqslant n \leqslant 100$

Nous ne nous arrêtons pas en si bon chemin. On donne aussi les valeurs de $\mathscr{N}$ pour $0 \leqslant n \leqslant 100$ et $0 \leqslant n \leqslant 1000$ sur les figures 2 et 3 respectivement.

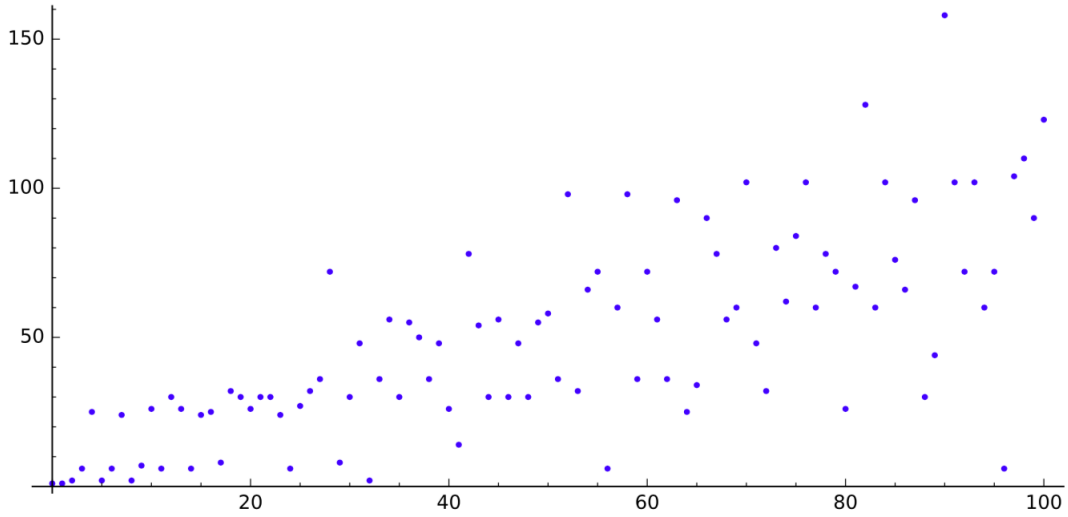


FIGURE 2 – $\mathscr{N}(n)$ pour $0 \leqslant n \leqslant 100$

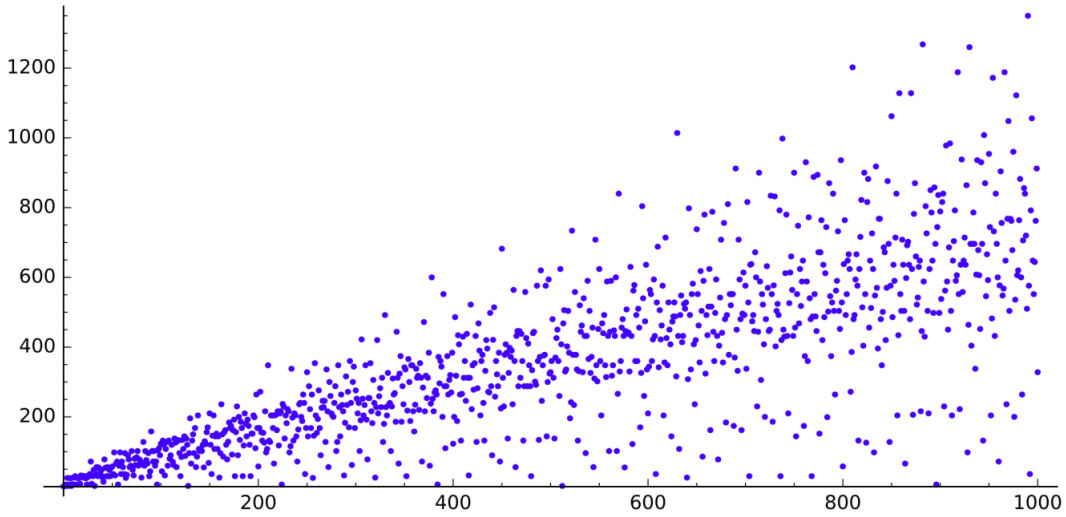


FIGURE 3 – $\mathscr{N}(n)$ pour $0 \leqslant n \leqslant 1000$

On observe alors de jolies comètes de points, avec une bien plus forte densité en points au centre de la comète.
Il nous vient alors une idée saugrenue. Nous allons regarder les entiers tels que $\mathscr{N}(n) = 1$.
Pour cela, créons un petit algorithme qui liste les entiers n tels que $\mathscr{N}(n) = k$ pour un k fixé.

```
def Negalk(k,liste):
    i=0;
    L=[];
    for n in liste[0]:
        if n==k:
            L.append(i)
        i=i+1;
    return L
```

On trouve seulement 0 et 1. On s'empresse alors de conjecturer que

$$\forall n \geqslant 2 \quad \mathscr{N}(n) \geqslant 2.$$

On lance alors l'algorithme `Negalk` pour $k = 2$, et ils nous renvoie trouve `[2, 5, 8, 32, 128, 512, 2048]`. Mis à part le "raté" du début avec 5, cela nous a tout l'air de lister une puissance de deux... sur deux. On s'empresse alors de conjecturer que

$$\forall n \geqslant 6 \quad (\mathscr{N}(n) = 2 \iff \exists k \in \mathbb{N} \quad n = 2^k \text{ et } k \equiv 1 \pmod 2).$$

Notre soif inextinguible de généralités nous enjoint d'écrire un algorithme qui nous permettra de tracer le graphe de l'application suivante

$$\begin{array}{rccl} N_n\colon & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & k & \longmapsto & \#\{0 \leqslant \ell \leqslant n, \mathscr{N}(\ell) = k\}, \end{array}$$

graphe qui est donné sur la figure 4 pour $n = 1000$. Pour k grand, on remarque que l'on a nécessairement $N_n(k) = 0$.
L'algorithme est celui-ci :

```
def nombredeNegalk(liste):
    L=[0];
    for n in liste[0]:
        tmp=n-len(L);
        if tmp>=0:
            L=L+[0 for x in [0..tmp]];
        L[n]=L[n]+1;
    return L
```

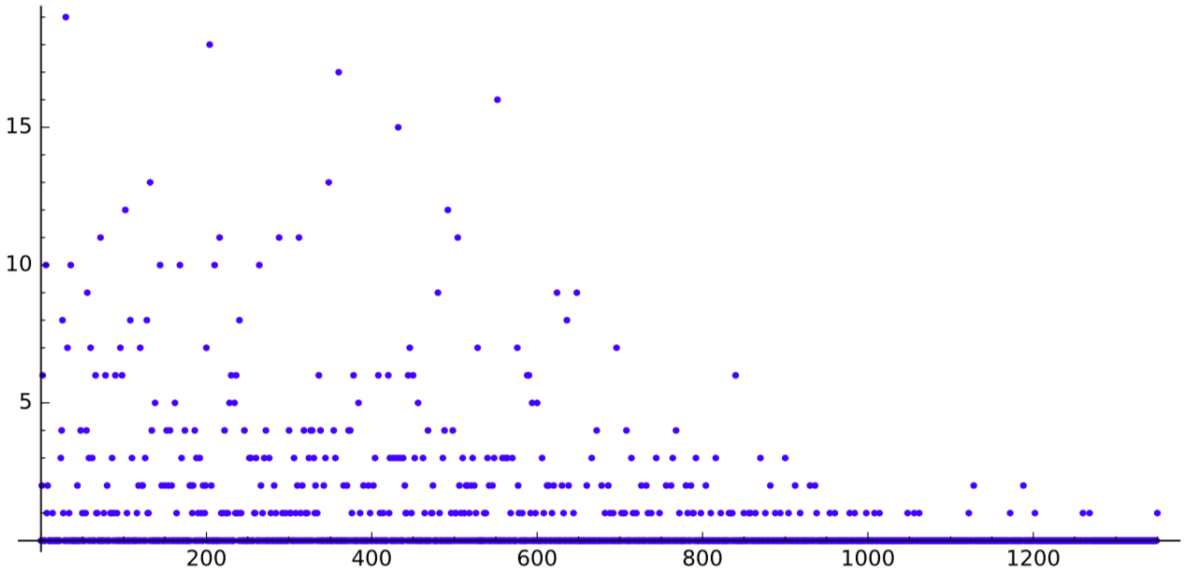


FIGURE 4 – Graphe de N_{1000}

Finalement, regroupons les différentes courbes dans un unique graphique (figure 5), et ce en utilisant un code couleur.
Pour cela commençons, comme à notre habitude, par donner un algorithme :

```
def trace_couleur(L):
    l=len(tmp[0]);
    un=[0 for x in [0..l]];
    de=[0 for x in [0..l]];
    tr=[0 for x in [0..l]];
    qa=[0 for x in [0..l]];
    i=0;
    for d in L[0]:
        if L[2][i]<=1:
            un[i]=d;
        elif L[2][i]==2:
            de[i]=d;
```

```
            elif L[2][i]==3:
                tr[i]=d;
            elif L[2][i]==4:
                qa[i]=d;
            i=i+1;
        return list_plot(un,color='yellow')+list_plot(de,color='blue')\\
+list_plot(tr,color='red')+list_plot(qa,color='black')
```

Ainsi, grâce à l'algorithme `trace_couleur`, nous traçons les valeurs de $\mathscr{N}(n)$ pour $0 \leqslant n \leqslant 1000$, avec le code couleur [15] suivant :

- On trace $\mathscr{N}(n)$ en **jaune** si $\text{Lag}(n) = 1$,
- On trace $\mathscr{N}(n)$ en **bleu** si $\text{Lag}(n) = 2$,
- On trace $\mathscr{N}(n)$ en **rouge** si $\text{Lag}(n) = 3$,
- On trace $\mathscr{N}(n)$ en **noir** si $\text{Lag}(n) = 4$.

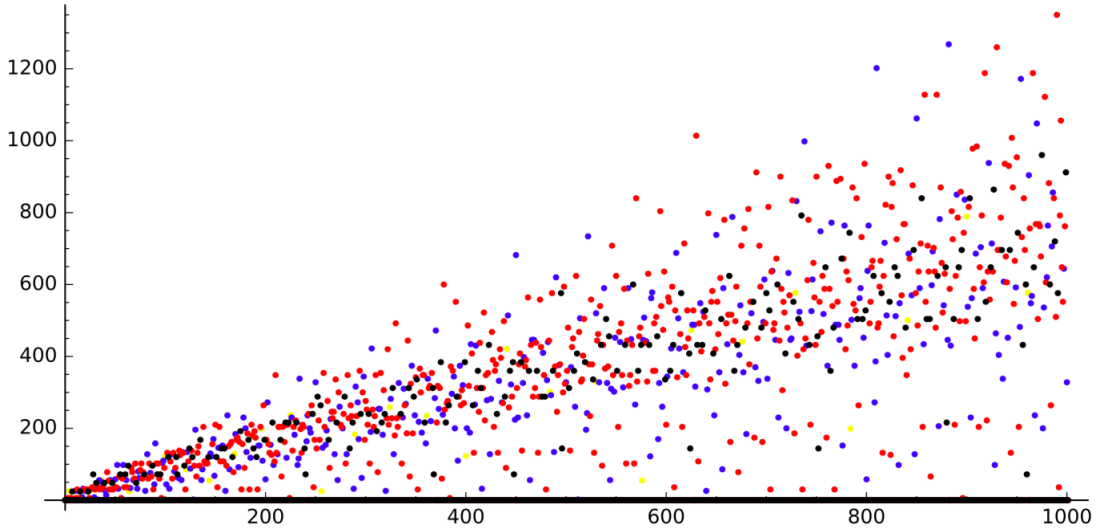


FIGURE 5 – Graphe de $\mathscr{N}(n)$ pour $0 \leqslant n \leqslant 1000$ avec des couleurs visualisant $\text{Lag}(n)$

Sous nos yeux ébahis s'affichent alors une myriade de couleurs, un bouquet de points naturellement colorés par le plus beau des désordres mathématiques.
Fort de notre curiosité, faisons la constatation suivante. Les points, tracés ici en noir, représentant les entiers n tels que $\text{Lag}(n) = 4$ sont les points les moins dispersés. Étrangement. Étrangement ? À suivre...

3.2 Quelques conséquences

Nous avons conjecturé précédemment un énoncé, que nous énonçons puis démontrons ici.

15. D'avance nous nous excusons pour ceux qui ne disposent que d'une version imprimée en noir et blanc. Le code couleur perd tout de suite de son intérêt, ce qui est fâcheux. Nous en profitons pour signaler qu'une jolie version en haute qualité et en couleur est disponible en ligne.

Théorème 5 On considère toutes les décompositions d'un entier comme somme de un, deux, trois ou quatre carrés.

(i) Un nombre s'écrit uniquement comme un carré si, et seulement s'il est de la forme 4^k ou s'il est nul.

(ii) Un nombre s'écrit uniquement comme somme de deux carrés et ce d'une seule façon

- si, et seulement s'il est de la forme 2^{2k+1} si les carrés sont identiques,
- seulement s'il est de la forme $5 \cdot 4^k$ ou $3 \cdot 2^{2k+1}$ si les carrés sont différents.

(iii) Un nombre s'écrit uniquement comme somme de trois carrés identiques seulement s'il est de la forme $3 \cdot 4^k$.

Remarque 5 Avertissement.
Dans la preuve ci-dessous, nous utiliserons la formule de Jacobi permettant de compter les carrés, qui ne sera démontrée que bien plus tard. Plutôt que d'estimer que cette preuve est déplacée, nous préférons la considérer comme une motivation pour l'étude du théorème de Jacobi.

Preuve.
Commençons par préciser ce que veut dire le théorème. Pour cela, notons $\mathscr{N}$ l'application

$$\begin{array}{rccl} \mathscr{N}: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \#\left\{(x_1,x_2,x_3,x_4) \in \mathbb{Z}^4,\ \sum_{i=1}^{4} {x_i}^2 = n\right\} \end{array}$$

qui à un nombre fait correspondre son nombre de décompositions en somme de quatre carrés, certains des carrés pouvant être nuls [16].

- Soit $n \in \mathbb{N}$ tel que n s'écrive uniquement comme un carré : $n = k^2$. Alors $n = 0$ ou $\mathscr{N}(n) = 8$, en effet

$$\begin{aligned} n &= k^2 + 0^2 + 0^2 + 0^2 \\ &= 0^2 + k^2 + 0^2 + 0^2 \\ &= 0^2 + 0^2 + k^2 + 0^2 \\ &= 0^2 + 0^2 + 0^2 + k^2 \\ &= (-k)^2 + 0^2 + 0^2 + 0^2 \\ &= 0^2 + (-k)^2 + 0^2 + 0^2 \\ &= 0^2 + 0^2 + (-k)^2 + 0^2 \\ &= 0^2 + 0^2 + 0^2 + (-k)^2. \end{aligned}$$

16. Et même négatifs à partir de maintenant.

Réciproquement, si $\mathscr{N}(n) = 8$ alors n ne peut s'écrire autrement qu'uniquement comme somme d'un carré, sinon on aurait immédiatement que $\mathscr{N}(n) > 8$.

La clé de la démonstration de ce théorème est d'appliquer le théorème 7, qui donne que

$$\mathscr{N}(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d. \qquad (\star)$$

Donc si $\mathscr{N}(n) = 8$, alors

$$\sum_{\substack{d|n \\ 4\nmid d}} d = 1.$$

Or $1 \mid n$, donc d'après cette somme, n n'a aucun diviseur d différent de 1, sauf si $4 \nmid d$.
Ainsi, n s'écrit sous la forme 4^k.
Réciproquement, d'après $(\star)$ on a bien $\mathscr{N}(4^k) = 8 \cdot 1 = 8$, ce qui prouve (i).

- Supposons que n s'écrive comme somme de deux carrés : $n = a^2 + b^2$.

Alors en dénombrant les écritures possibles de n (par exemple $n = 0^2 + (-b)^2 + a^2 + 0^2 ...$), on trouve que $\mathscr{N}(n) = 48$ si $a \neq b$, et $\mathscr{N}(n) = 24$ si $a = b$. En effet, on peut remarquer que si $a = b$ les écritures $n = a^2+b^2+0^2+0^2$ et $n = b^2+a^2+0^2+0^2$ sont identiques par exemple.

Réciproquement, si $\mathscr{N}(n) = 24$, alors avec un peu de dénombrement on trouve que n s'écrit comme uniquement comme somme de deux carrés identiques ou n s'écrit comme somme de quatre carrés identiques et n est un carré. Le second cas sera exclu par la suite.

On a d'après $(\star)$

$$\begin{cases} \mathscr{N}(n) = 24 \iff \displaystyle\sum_{\substack{d|n \\ 4\nmid d}} d = 3 \\ \\ \mathscr{N}(n) = 48 \iff \displaystyle\sum_{\substack{d|n \\ 4\nmid d}} d = 6. \end{cases}$$

Il faut donc trouver des partitions de 3 et de 6 contenant 1 car 1 divise tout nombre. De plus les partitions ne peuvent contenir plusieurs fois 1.
Les partitions restantes sont donc

$$\begin{cases} 3 = 2 + 1 \\ 6 = 5 + 1 = 3 + 2 + 1. \end{cases}$$

Pour $\mathscr{N}(n) = 3$, on trouve donc que les diviseurs de n sont 1,2 et tous les diviseurs divisibles par 4.
Pour $\mathscr{N}(n) = 6$, on trouve donc que les diviseurs de n sont 1,5 et tous les diviseurs divisibles par 4, ou 1,2,3 et tous les diviseurs divisibles par 4.
Donc

$$\begin{cases} \mathscr{N}(n) = 3 \iff \exists k \quad n = 2 \cdot 4^k = 2^{2k+1} \\ \\ \mathscr{N}(n) = 6 \iff \exists k \quad \begin{cases} n = 5 \cdot 4^k \\ \text{ou} \\ n = 2 \cdot 3 \cdot 4^k = 3 \cdot 2^{2k+1}. \end{cases} \end{cases}$$

Chose promise chose due, revenons au cas que nous avions promis d'exclure. Si n est de la forme 2^{2k+1}, alors $\mathscr{N}(n) = 24$, et n est déjà somme de deux carrés identiques : $n = (2^k)^2 + (2^k)^2$, donc n ne peut pas aussi être un carré et somme de quatre carrés identiques, sinon $\mathscr{N}(n) > 24$.

Ce qui démontre (ii).

- Supposons que n s'écrive comme somme de trois carrés identiques : $n = a^2+a^2+a^2$.
  Alors en démontrant encore les écritures possibles de n, on trouve que $\mathscr{N}(n) = 4 + 4 \times 3 + 4 \times 3 + 4 = 32$.
  Réciproquement, si $\mathscr{N}(n) = 32$, alors on peut remarquer par dénombrement que la seule possibilité est que n soit somme de trois carrés identiques.
  Comme nous avons fait précédemment, on utilise la formule $(\star)$ pour montrer que

$$\sum_{\substack{d|n \\ 4\nmid d}} d = 4,$$

avec pour seule partition acceptable $4 = 3 + 1$. Les diviseurs de n sont donc 3 et les puissances de 4, donc n est de la forme $3 \cdot 4^k$.
Ce qui démontre (iii). □

Remarque 6 Nous venons de d'imposer des formes à un entier n pour qu'il ait un certain nombre de décompositions comme sommes de carrés. Dans presque tous les cas, nous avons montré des équivalences, car $\mathscr{N}(n)$ était petit, ce qui permettait de faire correspondre la valeur de $\mathscr{N}(n)$ avec un unique type de décomposition, ce qui n'est plus le cas dès que $\mathscr{N}(n)$ grandit.

Trouver des formes pour les antécédents n par $\mathscr{N}$ pour un entier m fixé est en revanche possible, et c'est ce que nous faisons dans le théorème à venir.

Théorème 6 Soit $m \in \mathbb{N}_{>4}$.
Si un entier n vérifie $\mathscr{N}(n) = m$ alors

$$\exists k \in \mathbb{N} \quad \exists Q \subset \mathbb{N} \quad n = 4^k \prod_{q \in Q} q,$$

où Q vérifie les conditions suivantes

$$\begin{cases} 1 \in Q \\ \\ 4 \notin Q \\ \\ \displaystyle\sum_{q \in Q} q = \frac{m}{8} \\ \\ \forall q \in Q \quad \forall d \mid q \quad d \in Q. \end{cases}$$

Preuve.
On a

$$\mathscr{N}(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d,$$

donc

$$\mathscr{N}(n) = m \iff \frac{m}{8} = \sum_{\substack{d \mid n \\ 4 \nmid d}} d.$$

Construisons Q l'ensemble des diviseurs admissibles pour n qui ne sont pas de la forme 4^k. *A fortiori* $4 \notin Q$. En effet, nous pouvons d'ores et déjà dire que si n vérifie alors $\mathscr{N}(n) = m$, alors $\mathscr{N}(4^k n) = m$ pour tout k.
On a $1 \in Q$ obligatoirement, et on doit bien avoir la relation

$$\sum_{q \in Q} q = \frac{m}{8}.$$

De plus, si $q \in Q$, alors $q \mid n$, donc pour tout $d \mid q$, on a $d \mid n$ donc $d \in Q$, ce qui impose la troisième condition.

Remarque 7 Lors de notre soutenance, Olivier Fouquet nous a fait remarquer, et nous l'en remercions, qu'un entier qui s'écrirait uniquement comme somme de deux carrés différents n'existerait pas d'après la fin de la démonstration de la formule de Jacobi à venir. Ainsi il n'existe aucun entier dont la seule décomposition en somme de quatre carrés serait une somme de deux carrés distincts. Pour toute question sur ce point ou sur un autre, vous pouvez nous contacter aux adresses citées en page 4 de ce mémoire.

Métamathématiques

Nous avons travaillé.

Nous avons lu des pages et des pages d'articles et de livres. Nous avons gratté des dizaines de feuilles de papier à la mine de notre crayon de bois. Nous avons jonglé avec les formules mathématiques pour leur donner la forme recherchée.

Et puis nous nous sommes interrogés.

Quel sens donner à notre recherche ? Quel est l'intérêt d'un mémoire qui ne fait que reprendre les idées que d'autres ont eu avant nous ? Notre travail n'était-il pas qu'une longue suite insipide de lettres et de symboles froids et figés ?
Nous avons alors pensé à Joël Merker, qui nous avait enseigné la théorie de l'intégration en licence. Il nous avait donné une intuition de sa philosophie des mathématiques, et celle-ci pouvait peut-être venir nourrir notre réflexion. Il a accepté de partager avec nous le fruit de son expérience philosophique. Voici un résumé de notre échange.

Les mathématiques sont comme une forêt vierge traversée de grandes avenues. Les textes écrits sont des chemins linéaires et les calculs des arbres. Mais on ne peut avoir cette vision qu'avec une longue expérience et un long cheminement philosophique.
L'insatisfaction qu'on ressent en lisant des mathématiques sans en comprendre le sens profond est importante et à garder précieusement. En effet, "on peut mettre dix ans à se convaincre que quelque chose est vrai". On crée ou invente rarement des choses. Cependant, certains ont "le génie de récréer les choses", comme Hardy et Wright. On peut donc dire que "le bon écrivain fait sentir les choses de manière intelligente".
Joël Merker est le seul, ou quasiment, à défendre que les calculs sont importants. Il considère d'ailleurs que c'est sa spécificité. Pourquoi est-ce si important ? Quand on fait du calcul, souvent, on ne peut pas tout calculer, on extrait une partie squelettique du calcul. Mais "quand on pense que c'est l'information essentielle, on peut se tromper". C'est pour cette raison qu'il faut effectuer les calculs en entier. D'ailleurs, Lagrange, Gauss et Euler "étaient des génies parce qu'ils faisaient énormément de calculs".
On a toujours tendance à cacher la façon dont on a obtenu les théorèmes. Au contraire, il faut faire comprendre où est la porte une fois qu'on est à l'intérieur, car de l'extérieur on ne voit que les murs qui se dressent devant soi. Pour nous, il faut "multiplier les sources", déchiffrer le sens profond des mots. Il nous a incités à aller à la bibliothèque universitaire afin de trouver des textes qui redisent notre travail mais autrement, de les lire et d'essayer de saisir l'idée qu'ils expriment. En fait, Joël Merker "se bat en permanence pour réarticuler les questions initiales".

Pour conclure, ce qui nous aura marqué au cours de cet entretien, c'est une phrase que nous devons à Joël Merker et qui donne sens à notre travail tout entier :

"Vous êtes extrêmement jeunes...
...ça ne veut pas dire que je suis extrêmement vieux ! [rires]"

4 Des choses sérieuses

On a ri des calembours. On a souri en savourant les citations. On a dévoré les remarques. On s'est impregné des exhalaisons des théorèmes.
Il est temps de se jeter tout entier dans des choses cocassement plus sérieuses.

Un, deux, trois, nous irons au bois ;
Quatre, cinq, six, cueillir des cerises ;
Sept, huit, neuf, dans mon panier neuf ;
Dix, onze, douze, elles seront toutes rouges.

4.1 Un, deux, trois...

De tout temps l'homme compte.
Il compte les caillous, il compte les moutons, il compte même les carrés.

Théorème 7 (Formule de Jacobi) Pour tout entier n, on a

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d$$

Remarque 8 Le théorème de Lagrange fut initialement conjecturé par Claude-Gaspard Bachet de Méziriac en 1621. Fermat, dans toute sa splendeur, clama haut et fort avoir une preuve de cette conjecture. Il jura même pouvoir proposer une généralisation aux nombres polygonaux et promis d'écrire un livre qui révolutionnerait l'arithmétique. Aucun livre ne parut.
Euler démontra partiellement le théorème en 1751, et la démonstration fut achevée en 1770 par Lagrange qui donna son nom à ce résultat.
La formule de Jacobi qui raffine le théorème de Lagrange en comptant les décompositions en plus d'affirmer qu'il en existe une, dut attendre 1834.

4.2 ....nous irons au bois.

Dans cette partie, nous allons démontrer le théorème 7 à l'aide des formes modulaires.

Définition 18 On définit :

$$\begin{array}{rccc} \theta\colon & \mathbb{H} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \displaystyle\sum_{m\in\mathbb{Z}} e^{2i\pi m^2 z} \end{array}$$

On remarque alors que :

$$\theta^4(z) = \left(\sum_{m_1\in\mathbb{Z}} e^{2i\pi m_1^2 z}\right)\left(\sum_{m_2\in\mathbb{Z}} e^{2i\pi m_2^2 z}\right)\left(\sum_{m_3\in\mathbb{Z}} e^{2i\pi m_3^2 z}\right)\left(\sum_{m_4\in\mathbb{Z}} e^{2i\pi m_4^2 z}\right)$$
$$\theta^4(z) = \sum_{(m_1,m_2,m_3,m_4)\in\mathbb{Z}^4} e^{2i\pi(m_1^2+m_2^2+m_3^2+m_4^2)z}$$
$$\theta^4(z) = \sum_{n\in\mathbb{Z}} r_4(n) e^{2i\pi n z}$$

Théorème 8 L'application θ^4 est une forme modulaire de poids 2 pour $\Gamma_0(4)$.

Commençons par donner le plan de cette preuve, afin que nul, lecteur ou auteur, n'oublie ce qui est démontré.

- θ est holomorphe
- $\forall z \in \mathbb{H} \quad \forall \gamma \in \Gamma_0(4) \quad \theta^4(\gamma z) = (cz+d)^2\theta^4(z)$
  - preuve avec $\gamma_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
  - preuve avec $\gamma_1 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$
    - calcul pour reformuler et faire apparaître une fonction f
    - calcul de la transformée de Fourier de f
      - reformulation pour se ramener à un calcul d'intégrale
      - recherche de primitive pour la calculer
        - on dérive une fonction candidate à être primitive
        - on calcule ses limites aux bornes de l'intégrale en calculant l'intégrale de Gauss grâce à un calcul d'intégrale double
      - on finit le calcul de la transformée de Fourier
    - on lie le calcul de $\hat{f}$ à notre problème initial
      - on périodise f en posant une application φ_t
      - on calcule les coefficients de Fourier de φ_t
      - quelques manipulations nous donnent une relation entre $\sum f$ et $\sum \hat{f}$
    - on termine le calcul initial
  - on montre une relation montrant que la formule se comporte bien avec la multiplication
  - on prouve que γ_1 et γ_2 engendrent $\Gamma_0(4)$
  - on traite le cas général par récurrence sur le nombre de γ_i nécessaires pour écrire un γ quelconque

---

FIGURE 6 – Plan de la preuve du théorème 8

La fonction θ est holomorphe sur $\mathbb{H}$ comme limite uniforme de fonctions holomorphes.
Montrons que pour tout $z \in \mathbb{H}$ et tout $\gamma \in \ \Gamma_0(4)$, on a

$$\theta^4(\gamma z) = (cz+d)^2\theta^4(z),$$

où

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Montrons d'abord ceci pour $\gamma_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et pour $\gamma_1 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$.
Il suffira alors de montrer que ces deux matrices engendrent $\Gamma_0(4)$.

- On a

$$\begin{aligned} \theta^4\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot z\right) &= \theta^4(z+1) \\ &= \sum_{n\in\mathbb{Z}} r_4(n) e^{2i\pi n(z+1)} \\ &= \sum_{n\in\mathbb{Z}} r_4(n) e^{2i\pi nz} \times 1 \\ &= \theta^4(z) \\ &= (0z+1)^2\theta^4(z). \end{aligned}$$

- Et

$$\begin{aligned} \theta\left(\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \cdot z\right) &= \theta\left(\frac{z}{4z+1}\right) \\ &= \sum_{n\in\mathbb{Z}} e^{2i\pi n^2 \frac{z}{4z+1}} \\ &= \sum_{n\in\mathbb{Z}} e^{2i\pi n^2\left(\frac{1}{4} - \frac{1}{4(4z+1)}\right)} \\ &= \sum_{n\in\mathbb{Z}} e^{2i\pi\left(\frac{m}{2}\right)^2} e^{-2i\pi\left(\frac{m}{2}\right)^2 \frac{1}{4z+1}} \\ &= \sum_{\varepsilon\in\{0,1\}} \sum_{t\in\mathbb{Z}} e^{2i\pi\left(\frac{\varepsilon}{2}+t\right)^2} e^{-2i\pi\left(\frac{\varepsilon}{2}+t\right)^2 \frac{1}{4z+1}} \\ &= \sum_{\varepsilon\in\{0,1\}} \sum_{t\in\mathbb{Z}} e^{2i\pi\left(\left(\frac{\varepsilon}{2}\right)^2+mt+t^2\right)} e^{-2i\pi\left(\frac{\varepsilon}{2}+t\right)^2 \frac{1}{4z+1}} \\ &= \sum_{\varepsilon\in\{0,1\}} e^{2i\pi\left(\frac{\varepsilon}{2}\right)^2} \sum_{t\in\mathbb{Z}} \underbrace{\left(e^{2i\pi}\right)^{mt+t^2}}_{=1} e^{-2i\pi\left(\frac{\varepsilon}{2}+t\right)^2 \frac{1}{4z+1}}. \end{aligned}$$

On pose

$$\begin{array}{rccc} f\colon & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & t & \longmapsto & e^{-\frac{2i\pi}{4z+1}\left(\frac{\varepsilon}{2}+t\right)^2}. \end{array}$$

On cherche à calculer la transformée de Fourier de f.
On a

$$\begin{aligned} \hat{f}(\xi) &= \int_{\mathbb{R}} f(t)e^{-i\xi t}\mathrm{d}t \\ &= \int_{\mathbb{R}} e^{-\frac{2i\pi}{4z+1}\left(\frac{\varepsilon}{2}+t\right)^2} e^{-i\xi t}\mathrm{d}t \\ &= \int_{\mathbb{R}} e^{-\frac{2i\pi}{4z+1}u^2} e^{-i\xi\left(u-\frac{\varepsilon}{2}\right)}\mathrm{d}u \\ &= e^{i\xi\frac{\varepsilon}{2}} \int_{\mathbb{R}} e^{-\frac{2i\pi}{4z+1}u^2-i\xi u}\mathrm{d}u \\ &= e^{i\xi\frac{\varepsilon}{2}} \int_{\mathbb{R}} g(u)\mathrm{d}u \end{aligned}$$

en posant

$$\begin{array}{rccc} g\colon & \mathbb{R} & \longrightarrow & \mathbb{C} \\ & u & \longmapsto & e^{-\frac{2i\pi}{4z+1}u^2-i\xi u}. \end{array}$$

On pose aussi

$$\begin{array}{rccc} G\colon & \mathbb{R} & \longrightarrow & \mathbb{C} \\ & u & \longmapsto & \left(\frac{1}{4}-\frac{i}{4}\right)\sqrt{4z+1}e^{\frac{i\xi^2(4z+1)}{8\pi}}\operatorname{erf}\left(\dfrac{\left(\frac{1}{4}+\frac{i}{4}\right)\left(\xi(4z+1)+4\pi u\right)}{\sqrt{\pi(4z+1)}}\right), \end{array}$$

avec

$$\begin{array}{rccc} \operatorname{erf}\colon & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & x & \longmapsto & \dfrac{2}{\sqrt{\pi}}\displaystyle\int_0^x e^{-t^2}\mathrm{d}t, \end{array}$$

où $\sqrt{\cdot}$ désigne une racine quelconque du nombre complexe.
L'application G est de classe C^∞ par composition de fonctions C^∞, et on a pour tout $u \in \mathbb{R}$,

$$
\begin{aligned}
G'(u) &= \left(\frac{1}{4}-\frac{i}{4}\right)\sqrt{4z+1}e^{\frac{i\xi^2(4z+1)}{8\pi}}\frac{\left(\frac{1}{4}-\frac{i}{4}\right)4\pi}{\sqrt{\pi(4z+1)}}\frac{2}{\sqrt{\pi}}e^{-\frac{\left(\frac{1}{4}+\frac{i}{4}\right)^2(\xi(4z+1)+4\pi u)^2}{\pi(4z+1)}} \\
&= \underbrace{\left(\frac{1}{16}+\frac{1}{16}\right)\frac{8\pi\sqrt{4z+1}}{\pi\sqrt{4z+1}}}_{=1}e^{\frac{i\xi^2(4z+1)}{8\pi}}e^{-\frac{\left(\frac{1}{16}-\frac{1}{16}+\frac{2i}{16}\right)\left(\xi^2(4z+1)^2+16\pi^2u^2\right)}{\pi(4z+1)}} \\
&= e^{\frac{i\xi^2(4z+1)}{8\pi}-\frac{i}{8\pi(4z+1)}\left(\xi^2(4z+1)^2+16\pi^2u^2+8\pi u\xi(4z+1)\right)} \\
&= e^{\frac{i\xi^2(4z+1)}{8\pi}-\frac{i\xi^2(4z+1)}{8\pi}-\frac{2i\pi}{4z+1}u^2-i\xi u} \\
&= g(u).
\end{aligned}
$$

Ainsi,

$$\hat{f}(\xi) = e^{i\xi\frac{\varepsilon}{2}}[G(u)]_{-\infty}^{+\infty}. \tag{3}$$

Considérons

$$I := \int_0^\infty \int_0^\infty e^{-x^2+y^2}\mathrm{d}x\mathrm{d}y.$$

Alors en effectuant un changement de variables en coordonnées polaires, on a

$$
\begin{aligned}
I &= \int_{\theta=0}^{\pi/2}\int_{r=0}^{\infty} e^{-r^2(\cos^2(\theta)+\sin^2(\theta))}\,|r|\,\mathrm{d}r\mathrm{d}\theta \\
&= -\frac{1}{2}\int_{\theta=0}^{\pi/2}\int_{r=0}^{\infty}(-2r)e^{-r^2}\mathrm{d}r\mathrm{d}\theta \\
&= -\frac{1}{2}\int_{\theta=0}^{\pi/2}[e^{-r^2}]_{r=0}^{+\infty}\mathrm{d}\theta \\
&= -\frac{1}{2}\frac{\pi}{2}(0-1) \\
&= \frac{\pi}{4}.
\end{aligned}
$$

Or l'intégrale I est à variables séparées, donc on a aussi

$$I = \left(\int_0^\infty e^{-x^2}\mathrm{d}x\right)\left(\int_0^\infty e^{-y^2}\mathrm{d}y\right) = \left(\int_0^\infty e^{-x^2}\mathrm{d}x\right)^2.$$

Donc

$$\int_0^\infty e^{-x^2}\mathrm{d}x = \sqrt{\frac{\pi}{4}} = \frac{\sqrt{\pi}}{2},$$

donc

$$\operatorname{erf}(u) \xrightarrow[u\to\pm\infty]{} \pm\frac{2}{\sqrt{\pi}}\frac{\sqrt{\pi}}{2} = \pm 1.$$

Ainsi,

$$\begin{aligned}\lim_{u\to\pm\infty} G(u) &= \left(\frac{1}{4}-\frac{i}{4}\right)\sqrt{4z+1}e^{\frac{i\xi^2(4z+1)}{8\pi}} \lim_{u\to\pm\infty}\left(\operatorname{erf}\left(\frac{\left(\frac{1}{4}+\frac{i}{4}\right)(\xi(4z+1)+4\pi u)}{\sqrt{\pi(4z+1)}}\right)\right)\\ &= \left(\frac{1}{4}-\frac{i}{4}\right)\sqrt{4z+1}e^{\frac{i\xi^2(4z+1)}{8\pi}}(\pm 1).\end{aligned}$$

Donc en revenant à l'équation (3)

$$\begin{aligned}\hat{f}(\xi) &= e^{i\xi\frac{\varepsilon}{2}}\left(\lim_{u\to+\infty} G(u) - \lim_{u\to-\infty} G(u)\right)\\ &= e^{i\xi\frac{\varepsilon}{2}}\left(\frac{1}{4}-\frac{i}{4}\right)\sqrt{4z+1}e^{\frac{i\xi^2(4z+1)}{8\pi}}(1-(-1))\\ &= \frac{(1-i)\sqrt{4z+1}}{2}e^{i\xi\frac{\varepsilon}{2}}e^{\frac{i\xi^2(4z+1)}{8\pi}}. \qquad (4)\end{aligned}$$

Posons maintenant pour tout $t \in \mathbb{Z}$,

$$\begin{array}{rccc}\varphi_t\colon & \mathbb{R} & \longrightarrow & \mathbb{C}\\ & x & \longmapsto & f(t+x)\end{array}.$$

On a pour tout $x \in \mathbb{R}$,

$$\begin{aligned}\sum_{t\in\mathbb{Z}} \|\varphi_t(x)\|_\infty &= \sum_{t\in\mathbb{Z}} \left\|e^{-\frac{2i\pi}{4z+1}\left(\frac{\varepsilon}{2}+t+x\right)}\right\|_\infty\\ &= \sum_{t\in\mathbb{Z}} e^{-\frac{2i\pi}{4z+1}\left(\frac{\varepsilon}{2}+t\right)}\\ &< +\infty,\end{aligned}$$

donc la série $\sum \varphi_t$ est normalement convergente.
Or chaque φ_t est continue (car f l'est).
En posant

$$S\colon x \mapsto \sum_{t\in\mathbb{Z}} \varphi_t(x),$$

l'application S est donc continue.
De plus, un changement d'indice dans la somme montre que $S(x+1) = S(x)$, et donc S est 1-périodique.

On peut ainsi calculer les coefficients de Fourier de S, ce que nous faisons.

$$\begin{aligned} c_m &= \int_0^1 S(x)e^{-2i\pi mx}\mathrm{d}x \\ &= \int_0^1 \sum_{t\in\mathbb{Z}} \varphi_t(x)e^{-2i\pi mx}\mathrm{d}x \\ &= \int_0^1 \sum_{t\in\mathbb{Z}} f(t+x)e^{-2i\pi mx}\mathrm{d}x. \end{aligned}$$

On a déjà vu que S est définie par une série normalement convergente, on peut donc intervertir somme et intégrale, ce qui donne par 2π-périodicité de l'exponentielle

$$\begin{aligned} c_m &= \sum_{t\in\mathbb{Z}} \int_0^1 f(t+x)e^{-2i\pi mx}\mathrm{d}x \\ &= \sum_{t\in\mathbb{Z}} \int_0^1 f(t+x)e^{-2i\pi m(x+t)}\mathrm{d}x. \end{aligned}$$

On effectue le changement variable $u = x + t$:

$$\begin{aligned} c_m &= \sum_{t\in\mathbb{Z}} \int_t^{t+1} f(u)e^{-2i\pi mu}\mathrm{d}u \\ &= \int_{\mathbb{R}} f(u)e^{-2i\pi mu}\mathrm{d}u \\ &= \hat{f}(2\pi m). \end{aligned}$$

On obtient alors

$$\begin{aligned} S(x) &= \sum_{m\in\mathbb{Z}} c_m e^{2i\pi mx} \\ &= \sum_{m\in\mathbb{Z}} \hat{f}(2\pi m)e^{2i\pi mx}. \end{aligned}$$

Donc

$$\sum_{t\in\mathbb{Z}} f(t) = \sum_{t\in\mathbb{Z}} f(t+0) = S(0) = \sum_{m\in\mathbb{Z}} \hat{f}(2\pi m)e^{2i\pi m0} = \sum_{m\in\mathbb{Z}} \hat{f}(2\pi m).$$

On se sert alors du calcul de $\hat{f}$ à l'équation (4), et on revient au calcul initial :

$$\begin{aligned}
\theta\left(\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}\cdot z\right) &= \sum_{\varepsilon\in\{0,1\}} e^{\frac{i\pi\varepsilon^2}{2}} \sum_{t\in\mathbb{Z}} f(t)\\
&= \sum_{\varepsilon\in\{0,1\}} e^{\frac{i\pi\varepsilon^2}{2}} \sum_{t\in\mathbb{Z}} \hat{f}(2\pi t)\\
&= \sum_{\varepsilon\in\{0,1\}} e^{\frac{i\pi\varepsilon^2}{2}} \sum_{t\in\mathbb{Z}} \frac{(1-i)\sqrt{4z+1}}{2} e^{2i\pi t\frac{\varepsilon}{2}} e^{\frac{i(4\pi^2t^2)(4z+1)}{8\pi}}\\
&= \frac{(1-i)\sqrt{4z+1}}{2} \sum_{t\in\mathbb{Z}} \sum_{\varepsilon\in\{0,1\}} e^{\frac{i\pi\varepsilon^2}{2}} e^{2i\pi t\frac{\varepsilon}{2}} e^{\frac{i\pi}{2}t^2(4z+1)}\\
&= \frac{(1-i)\sqrt{4z+1}}{2} \sum_{t\in\mathbb{Z}} \left(e^{\frac{i\pi 0^2}{2}} e^{2i\pi t\frac{0}{2}} e^{\frac{i\pi}{2}t^2(4z+1)} + e^{\frac{i\pi 1^2}{2}} e^{2i\pi t\frac{1}{2}} e^{\frac{i\pi}{2}t^2(4z+1)}\right)\\
&= \frac{(1-i)\sqrt{4z+1}}{2} \sum_{t\in\mathbb{Z}} \left(e^{\frac{i\pi}{2}t^2(4z+1)} + i(-1)^t e^{\frac{i\pi}{2}t^2(4z+1)}\right)\\
&= \frac{(1-i)\sqrt{4z+1}}{2} \sum_{t\in\mathbb{Z}} (1+i(-1)^t) e^{2i\pi t^2 z + \frac{i\pi}{2}t^2}\\
&= \frac{(1-i)\sqrt{4z+1}}{2} \sum_{t\in\mathbb{Z}} e^{2i\pi t^2 z} \underbrace{(1+i(-1)^t) e^{\frac{i\pi}{2}t^2}}_{=:\rho(t)}.
\end{aligned}$$

Distinguons deux cas.

- Si $t \equiv 0 \pmod 2$, alors $t^2 \equiv 0 \pmod 4$.
  Donc
  $$\rho(t) = (1+i)\cdot 1 = 1+i.$$
- Si $t \equiv 1 \pmod 2$, alors $t^2 \equiv 1 \pmod 4$.
  Donc
  $$\rho(t) = (1-i)\cdot i = i-(-1) = 1+i.$$

Dans tous les cas, $\rho(t) = 1+i$.
Donc

$$\begin{aligned}
\theta\left(\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}\cdot z\right) &= \frac{(1-i)\sqrt{4z+1}}{2} \sum_{t\in\mathbb{Z}} e^{2i\pi t^2 z}(1+i)\\
&= \frac{(1-i)(1+i)\sqrt{4z+1}}{2} \sum_{t\in\mathbb{Z}} e^{2i\pi t^2 z}\\
&= \frac{(1+1)\sqrt{4z+1}}{2}\theta(z)\\
&= \sqrt{4z+1}\theta(z).
\end{aligned}$$

Finalement,

$$\theta^4\left(\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}\cdot z\right) = (4z+1)^2\theta^4(z),$$

ce qui est bien ce que nous souhaitions démontrer dans un premier temps.
Posons j l'application

$$\begin{array}{rccc} j: & \Gamma_0(4)\times\mathbb{H} & \longrightarrow & \mathbb{H} \\ & \left(\begin{pmatrix}a & b\\ c & d\end{pmatrix},z\right) & \longmapsto & (cz+d)^2. \end{array}$$

Soit $\left(\alpha = \begin{pmatrix}a & b\\ c & d\end{pmatrix}, \beta = \begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}\right) \in \Gamma_0(4)^2$, $z \in H$, on a

$$\begin{aligned} j(\alpha\beta,z) &= j\left(\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix},z\right) \\ &= j\left(\begin{pmatrix}aa'+bc' & ab'+bd'\\ ca'+dc' & cb'+dd'\end{pmatrix},z\right) \\ &= ((ca'+dc')z+(cb'+dd'))^2 \\ &= (ca'+dc')^2z^2+(ca'+dc')(cb'+dd')2z+(cb'+dd')^2 \\ &= (c^2a'^2+2cda'c'+d^2c'^2)z^2 \\ &\quad +(c^2a'b'+cda'd'+cdb'c'+d^2c'd')2z \\ &\quad +c^2b'^2+2cdb'd'+d^2d'^2. \end{aligned}$$

Donc

$$\begin{aligned} j(\alpha,\beta\cdot z)j(\beta,z) &= j\left(\begin{pmatrix}a & b\\ c & d\end{pmatrix},\frac{a'z+b'}{c'z+d'}\right)(c'z+d')^2 \\ &= \left(c\left(\frac{a'z+b'}{c'z+d'}\right)+d\right)^2(c'z+d')^2 \\ &= (c(a'z+b')+d(c'z+d'))^2 \\ &= c^2(a'z+b')^2+2cd(a'z+b')(c'z+d')+d^2(c'z+d')^2 \\ &= c^2(a'^2z^2+2a'b'z+b')+2cd(a'c'z^2+a'd'z+b'c'z+b'd') \\ &\qquad +d^2(c'^2z^2+2c'd'z+d'^2) \\ &= (c^2a'^2+2cda'c'+d^2c'^2)z^2 \\ &\quad +(c^2a'b'+cda'd'+cdb'c'+d^2c'd')2z \\ &\quad +c^2b'^2+2cdb'd'+d^2d'^2 \\ &= j(\alpha\beta,z). \end{aligned}$$

On a montré que

$$j(\alpha,\beta\cdot z)j(\beta,z)=j(\alpha\beta,z). \tag{5}$$

On utilise le fait que

$$\Gamma_0(4)/\{\pm 1\}=\langle\gamma_1,\gamma_2\rangle$$

d'après le théorème 1.
Donc, si $\gamma\in\Gamma_0(4)$, γ ou $-\gamma$ s'écrit comme un produit fini de puissances de γ_1 et γ_2, dans tous les cas seuls des carrés nous intéressent, le signe n'a donc aucune importance. Faisons comme si c'était γ qui s'écrivait ainsi.
Il existe donc $n\geqslant 0$ et $(i_k)_{1\leqslant k\leqslant n}\in\{1,2\}^n$ tels que

$$\gamma=\prod_{k=1}^{n}\gamma_{i_k}.$$

Enfin, comme nous avons déjà vérifié la formule pour γ_1 et γ_2, on peut raisonner par récurrence sur n (la formule étant triviale si $n=0$).
Ainsi,

$$\begin{aligned}
\theta^4(\gamma\cdot z)&=\theta^4\left(\left(\prod_{k=1}^{n}\gamma_{i_k}\right)\cdot z\right)\\
&=\theta^4\left(\gamma_{i_1}\cdot\left(\prod_{k=2}^{n}\gamma_{i_k}\right)\cdot z\right)\\
&=j\left(\gamma_{i_1},\left(\prod_{k=2}^{n}\gamma_{i_k}\right)\cdot z\right)\quad\underbrace{\theta^4\left(\left(\prod_{k=2}^{n}\gamma_{i_k}\right)\cdot z\right)}_{\text{on utilise l'hypothèse de récurrence}}\\
&=\underbrace{j\left(\gamma_{i_1},\left(\prod_{k=2}^{n}\gamma_{i_k}\right)\cdot z\right)j\left(\prod_{k=2}^{n}\gamma_{i_k},z\right)}_{\text{on applique la formule (5)}}\theta^4(z)\\
&=j\left(\gamma_{i_1}\prod_{k=2}^{n}\gamma_{i_k},z\right)\theta^4(z)\\
&=j\left(\prod_{k=1}^{n}\gamma_{i_k},z\right)\theta^4(z)\\
&=j\left(\gamma,z\right)\theta^4(z).
\end{aligned}$$

Par définition de j, on a (enfin !) montré la relation voulue.

Finalement, l'application θ^4 est une forme modulaire de poids 2 pour $\Gamma_0(4)$, ce qui conclut la (longue ?) démonstration du théorème 8.

Théorème 9 θ^4 est une forme modulaire de poids 2 avec $\theta^4(\infty) = 1$, $\theta^4(0) = -1$ et $\theta^4(-\frac{1}{2}) = 0$.

Preuve.
La première partie du théorème a déjà été prouvée, montrons les trois points restants.

- La série définissant θ converge uniformément sur tout voisinage de l'infini car elle converge normalement.

  Commençons par expliquer ce qu'est l'infini [17].

  Nous faisons en quelque sorte de la géométrie hyperbolique dans le demi-plan $\mathbb{H}$, ainsi en voyant ce demi plan comme un disque privé de son centre, l'infini est en fait le centre de ce disque. Tendre vers l'infini signifie donc se rapprocher du centre de ce disque, et donc avoir sa partie imaginaire qui tend vers l'infini.

  Dans notre cas on a donc avec $z = x + iy \in \mathbb{H}$,

$$\begin{aligned}\theta(z) &= \sum_{m\in\mathbb{Z}} e^{2i\pi m^2 z} \\ &= \sum_{m\in\mathbb{Z}} e^{-2\pi m^2 y} e^{2i\pi m^2 x},\end{aligned}$$

  donc car $y > 0$,

$$\sum_{m\in\mathbb{Z}} \left\| e^{-2\pi m^2 y} e^{2i\pi m^2 x} \right\| = \sum_{m\in\mathbb{Z}} e^{-2\pi m^2 y} < +\infty$$

  ce qui montre bien la convergence normale et donc la convergence uniforme.

  On peut donc inverser limite et somme, en gardant en tête que tendre vers le point à l'infini est équivalent à faire tendre la partie imaginaire vers l'infini.

  On a

$$\begin{aligned}\theta(\infty) &= \lim_{z\to\infty} \sum_{m\in\mathbb{Z}} e^{2i\pi m^2 z} \\ &= \sum_{m\in\mathbb{Z}} \lim_{y\to+\infty} e^{-2\pi m^2 y} e^{2i\pi m^2 x} \\ &= \sum_{m\in\mathbb{Z}^*} \underbrace{\lim_{y\to+\infty} e^{-2\pi m^2 y}}_{=0} e^{2i\pi m^2 x} + 1 \times 1 \\ &= 1.\end{aligned}$$

- Commençons par appliquer la formule de Poisson que nous avons montré au courant de la dernière preuve :

17. Malheureusement ceci n'est pas une invitation à la philosophie. Pour l'instant.

$$\sum_{m\in\mathbb{Z}} e^{-\pi m^2 y} = \sum_{m\in\mathbb{Z}} \int_{\mathbb{R}} e^{-\pi y x^2} e^{-2i\pi x m} \mathrm{d}x$$
$$= \sum_{m\in\mathbb{Z}} \int_{\mathbb{R}} e^{\pi x(yx+2im)} \mathrm{d}x.$$

Alors de façon très similaire à la preuve précédente (on trouve une primitive et tout et tout...), on montre par des calculs aussi fastidieux que les précédents que

$$\int_{\mathbb{R}} e^{\pi x(yx+2im)} \mathrm{d}x = \frac{1}{\sqrt{y}} e^{-\pi \frac{m^2}{y}}.$$

On effectue alors le changement de variable $y = -iz$, ainsi, en acceptant honteusement de déraciner les nombres complexes

$$\underbrace{\sum_{m\in\ \mathbb{Z}} e^{2\pi m^2 i \frac{z}{2}}}_{\theta\left(\frac{z}{2}\right)} = \frac{1}{\sqrt{-iz}} \sum_{m\in\mathbb{Z}} e^{-\pi \frac{m^2}{-iz}} = \frac{1}{\sqrt{-iz}} \underbrace{\sum_{m\in\mathbb{Z}} e^{-i\pi \frac{2m^2}{2z}}}_{\theta\left(-\frac{1}{2z}\right)},$$

ce qui nous donne

$$\sqrt{-iz}\theta\left(\frac{z}{2}\right) = \theta\left(-\frac{1}{2z}\right).$$

On obtient de cette façon la relation

$$\theta^4\left(-\frac{1}{2z}\right) = -z^2\theta^4\left(\frac{z}{2}\right).$$

□

Théorème 10 Toute forme parabolique de poids 2 pour $\Gamma_0(4)$ est nulle.

Corollaire 1 Les séries d'Eisenstein forment une base de l'espace des formes modulaires de poids 2 pour $\Gamma_0(4)$.

On cherche alors la série d'Eisenstein associée à 0.

Définition 19 Pour tout $a \in (\mathbb{Z}/4\mathbb{Z})^*$, on définit $G_2^{(0,a)}$ par :

$$G_2^{(0,a)} := \sum_{m_1\equiv 0[4]} \sum_{m_2\equiv a[4]} \frac{1}{(m_1 z + m_2)^2}.$$

Proposition 5 Pour tout $a \in (\mathbb{Z}/4\mathbb{Z})^*$, l'application $G_2^{(0,a)}$ est bien définie et holomorphe sur $\mathbb{H}$.

Lemme 10

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} = -4\pi^2 \sum_{j\geqslant 1} j e^{2i\pi jz}.$$

Preuve.
Dans toute la suite de la preuve, nous dirons que "$z \in \mathbb{C}$" pour signifier "$z \in \mathbb{C}$ là où tout est bien défini".
Commençons la formule suivante pour la cotangente.

Théorème 11 On a

$$\forall z \in \mathbb{C} \quad \pi \cot(\pi z) = \frac{1}{z} + \sum_{n \geqslant 1} \left(\frac{1}{z+n} + \frac{1}{z-n} \right). \tag{6}$$

Preuve.
Considérons la fonction

$$\begin{array}{rccc} f\colon & \mathbb{C} \setminus \{-a,a\} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \dfrac{a}{a^2 - z^2}, \end{array}$$

et la fonction

$$\begin{array}{rccc} g\colon & \mathbb{C} \setminus \mathbb{Z} \setminus \{-a,a\} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \pi \cot(\pi z) f(z). \end{array}$$

La fonction f est bien holomorphe sur $\mathbb{C}$ privé d'un nombre fini de points tous non entiers, que l'on note $(a_1, \ldots, a_k)$.
De plus, on a clairement

$$|f(z)| = \underset{|z| \to \infty}{O} \left(\frac{1}{|z|^2} \right).$$

Lemme 11 On a

$$\forall n \in \mathbb{N} \quad \operatorname{Res}(g,n) = f(n).$$

Preuve.
Soit $n \in \mathbb{N}$.
On sait que la fonction

$$z \mapsto \frac{1}{\sin(\pi z)}$$

admet un pôle simple en tout point de $\mathbb{Z}$.
Donc si $f(n) = 0$, alors g admet une singularité effaçable en n, donc

$$\operatorname{Res}(g,n) = f(n) = 0.$$

Sinon, car on a

$$\begin{aligned} \operatorname{Res}\left(\frac{1}{\sin(\pi.)}, n \right) &= \frac{1}{(\sin(\pi.))'(n)} \\ &= \frac{1}{\pi \cos(\pi n)} \\ &= \frac{1}{\pi (-1)^n}. \end{aligned}$$

Et, car g est holomorphe au voisinage de tout entier, on a

$$\begin{aligned}\mathrm{Res}(g,n) &= \pi\cos(\pi n)f(n)\,\mathrm{Res}\left(\frac{1}{\sin(\pi.)},n\right)\\ &= \pi(-1)^n f(n)\frac{1}{\pi(-1)^n}\\ &= f(n).\end{aligned}$$

Finalement, dans tous les cas, on a

$$\mathrm{Res}(g,n) = f(n),$$ □

ce qui conclut la preuve du lemme.

On note C_n le carré du plan complexe centré autour du nombre entier n et de côté 1. On note

$$I_n := \int_{C_n} g.$$

Lemme 12 On a

$$I_n \xrightarrow[n\to\infty]{} 0.$$

Preuve.
Soit $n \in \mathbb{N}$.
Commençons par montrer que la fonction $\cot(\pi.)$ est bornée sur C_n.
On a pour tout $z = x + iy \in C_n$:

$$\begin{aligned}|\cot(\pi z)| &= \left|\frac{e^{iz}+e^{-iz}}{e^{iz}-e^{-iz}}\right|\\ &\leqslant \frac{|e^{iz}|+|e^{-iz}|}{||e^{iz}|-|e^{-iz}||}\\ &= \frac{e^{\pi y}+e^{-\pi y}}{|e^{\pi y}-e^{-\pi y}|}\\ &= |\coth(\pi y)|\,.\end{aligned}$$

Si on se place sur un des côtés horizontaux de C_n, on a $|y| \geqslant \frac{1}{2}$, or la fonction coth est décroissante sur $\mathbb{R}_*^+$, donc $|\coth(\pi y)| \leqslant \coth(\frac{\pi}{2})$.
Si on se place sur un des côtés verticaux de C_n, z s'écrit de la forme $z = \pm(n+\frac{1}{2})+iy$, et donc :

$$\begin{aligned}|\cot(\pi z)| &= \left|\cot\left(\pm\pi\left(n+\frac{1}{2}\right)\ +i\pi y\right)\right|\\ &= \left|\cot\left(\frac{\pi}{2}+i\pi y\right)\right|\\ &= |\tan(i\pi y)|\\ &= \tanh(\pi\,|y|),\end{aligned}$$

qui est une fonction croissante sur $\mathbb{R}_+$, donc

$$\tanh(\pi\,|y|) \leqslant \tanh\left(\frac{\pi}{2}\right),$$

et numériquement

$$\tanh\left(\frac{\pi}{2}\right) \leqslant \coth\left(\frac{\pi}{2}\right).$$

Ce qui donne

$$\forall z \in C_n \quad |\coth(\pi z)| \leqslant \coth\left(\frac{\pi}{2}\right) =: \alpha.$$

De plus, f vérifie

$$|f(z)| \underset{|z|\to+\infty}{=} O\left(\frac{1}{|z|^2}\right).$$

Donc pour n assez grand, il existe $C \in \mathbb{R}$ tel que

$$|f(n)| \leqslant C\frac{1}{|n|^2}.$$

On considère donc maintenant n assez grand, on a alors :

$$\begin{aligned}
I_n &= \left|\int_{C_n} g(z)\mathrm{d}z\right| \\
&\leqslant \text{Longueur}(C_n) \cdot \sup_{z\in C_n} |g(z)| \\
&\leqslant 8\left(n+\frac{1}{2}\right)\pi\alpha \sup_{z\in C_n} |f(z)| \\
&\leqslant 8\left(n+\frac{1}{2}\right)\pi\alpha \sup_{z\in C_n} \frac{C}{|z|^2} \\
&\leqslant 8\left(n+\frac{1}{2}\right)\pi\alpha \frac{C}{\left(n+\frac{1}{2}\right)^2} \\
&\leqslant \frac{8C\alpha\pi}{n+\frac{1}{2}} \\
&\xrightarrow[n\to\infty]{} 0.
\end{aligned}$$

□

Ce qui prouve le lemme.

D'après le théorème des résidus, on a que pour n assez grand (tel que C_n contient $a_1,\ldots,a_k$), car g est holomorphe sur $\mathbb{C} \setminus \{a_1,\ldots,a_k\} \setminus \mathbb{Z}$:

$$\frac{1}{2i\pi}\int_{C_n} g(z)\mathrm{d}z = \sum_{j=1}^{k} \mathrm{Res}(g,a_j)\underbrace{\mathrm{Ind}(g,a_j)}_{=1} + \sum_{j\in\mathbb{Z}} \mathrm{Res}(g,j)\underbrace{\mathrm{Ind}(g,j)}_{=1}.$$

Or d'après le lemme 12

$$\frac{1}{2i\pi}\int_{C_n} g(z)\mathrm{d}z \xrightarrow[n\to\infty]{} 0,$$

et le membre de gauche ne dépend pas de n.
De plus, on a montré dans le lemme 11 que

$$\forall j \in \mathbb{Z} \quad \mathrm{Res}(g,j) = f(j).$$

Finalement,

$$\sum_{n\in\mathbb{Z}} f(n) = -\sum_{j=1}^{k} \mathrm{Res}(g,a_j).$$

Dans notre, un peu moins général, on a en fait $a_1 = a$ et $a_2 = -a$.
Donc

$$\sum_{n\in\mathbb{Z}} f(n) = -\mathrm{Res}(g,a) - \mathrm{Res}(g,-a).$$

Or $a \notin \mathbb{Z}$, donc la fonction $z \mapsto \pi\cot(\pi z)a$ est holomorphe sur un voisinage de a, donc

$$\mathrm{Res}(g,a) = \pi\cot(\pi a)a\,\mathrm{Res}\left(\frac{1}{a^2-z^2},a\right).$$

Or

$$(z-a)\frac{1}{a^2-z^2} = \frac{z-a}{(a-z)(a+z)} = \frac{-1}{a+z} \xrightarrow[z\to a]{} \frac{-1}{2a}.$$

Donc $\mathrm{Res}(g,a) = -\frac{\pi}{2}\cot(\pi a)$.
De même, $\mathrm{Res}(g,-a) = \frac{\pi}{2}\cot(-\pi a) = -\frac{\pi}{2}\cot(\pi a)$.
Ce qui donne,

$$\sum_{n\in\mathbb{Z}} \frac{a}{a^2-n^2} = -\frac{\pi}{2}\cot(\pi a) - \frac{\pi}{2}\cot(\pi a) = \pi\cot(\pi a).$$

On a

$$\begin{aligned}\sum_{n\in\mathbb{Z}} \frac{1}{a^2-n^2} &= \sum_{n=-\infty}^{1} \frac{1}{a^2-n^2} + \frac{1}{a^2} + \sum_{n=1}^{\infty} \frac{1}{a^2-n^2} \\ &= 2\sum_{n=1}^{\infty} \frac{1}{a^2-n^2} + \frac{1}{a^2}.\end{aligned}$$

Donc

$$\frac{\pi}{a}\cot(\pi a) = 2\sum_{n=1}^{\infty} \frac{1}{a^2-n^2} + \frac{1}{a^2},$$

donc

$$\frac{\pi}{a}\cot(\pi a) = 2\sum_{n=1}^{\infty}\frac{1}{2a}\left(\frac{1}{a-n}+\frac{1}{a+n}\right)+\frac{1}{a^2}.$$

Finalement,

$$\pi\cot(\pi a) - \frac{1}{a} = \sum_{n=1}^{\infty}\left(\frac{1}{a-n}+\frac{1}{a+n}\right) \qquad \square$$

ce qui prouve le théorème 11.

Soit $z \in \mathbb{C}$.
On a

$$\begin{aligned}\cot(\pi z) &= \frac{\cos(\pi z)}{\sin(\pi z)}\\ &= \frac{2i}{2}\frac{e^{i\pi z}+e^{-i\pi z}}{e^{i\pi z}-e^{-i\pi z}}\\ &= i\frac{\cancel{e^{-i\pi z}}}{\cancel{e^{-i\pi z}}}\frac{e^{2i\pi z}+1}{e^{2i\pi z}-1}\\ &= i\frac{e^{2i\pi z}-1+2}{e^{2i\pi z}-1}.\end{aligned}$$

Ce qui nous donne l'équation

$$\cot(\pi z) = i + \frac{2i}{e^{2i\pi z}-1}. \tag{7}$$

Ainsi pour tout $z \in \mathbb{C}$,

$$i\pi + \frac{2i\pi}{e^{2i\pi z}-1} = \frac{1}{z} + \sum_{n\geqslant 1}\left(\frac{1}{z+n}+\frac{1}{z-n}\right).$$

On utilise alors la formule pour développer $(1-z)^{-1}$ en série entière. Cette formule est n'est certes valable que si $|z|<1$, mais nous la prolongeons analytiquement sur tout $\mathbb{C}$.
Nous obtenons

$$i\pi - 2i\pi\sum_{j\geqslant 0} e^{2i\pi z j} = \frac{1}{z} + \sum_{n\geqslant 1}\left(\frac{1}{z+n}+\frac{1}{z-n}\right).$$

Nous aurions pu prendre des sommes partielles pour aller ensuite regarder la limite, mais un soudain souci de clarté nous a fait choisir de dériver directement. Nous dérivons donc par rapport à z les deux membres de cette équation.

$$-2i\pi\sum_{j\geqslant 0} 2i\pi j e^{2i\pi z j} = -\frac{1}{z^2} + \sum_{n\geqslant 1}\left(-\frac{1}{(z+n)^2}-\frac{1}{(z-n)^2}\right),$$

donc

$$\begin{aligned} 4\pi^2 \sum_{j\geqslant 0} j e^{2i\pi jz} &= -\frac{1}{z^2} + \sum_{n\geqslant 1} -\frac{1}{(z+n)^2} + \sum_{n\leqslant -1} -\frac{1}{(z+n)^2} \\ &= \sum_{n\in\mathbb{Z}} \frac{-1}{(z+n)^2}. \end{aligned}$$

Finalement :

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} = -4\pi^2 \sum_{j\geqslant 1} j e^{2i\pi jz}.$$

□

Remarque 9 Dédaignant toute considération de convergence, nous utilisons les prolongements analytiques pour calculer de belles choses grâce au dernier lemme. En effet, en prenant $z = 0$, on a

$$\sum_{n\in\mathbb{Z}^*} \frac{1}{n^2} = -4\pi^2 \sum_{j\geqslant 1} j \times 1.$$

On se rappelle alors que

$$\sum_{n\in\mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6},$$

ce qui nous donne comme on pouvait s'y attendre

$$\sum_{j\geqslant 1} j = -\frac{1}{12}.$$

Preuve.
Prouvons la proposition 5.
Soit $a \in (\mathbb{Z}/4\mathbb{Z})^*$, on a

$$\begin{aligned} G_2^{(0,a)} &= \sum_{m_1\equiv 0[4]} \sum_{m_2\equiv a[4]} \frac{1}{(m_1 z + m_2)^2} \\ &= \underbrace{\sum_{m_2\equiv a[4]} \frac{1}{{m_2}^2}}_{\mathfrak{W}} + \underbrace{\sum_{\substack{m_1\equiv 0[4] \\ m_1\neq 0}} \sum_{m_2\equiv a[4]} \frac{1}{(m_1 z + m_2)^2}}_{\mathfrak{Y}}. \end{aligned}$$

Alors

$$\begin{aligned}\mathfrak{W} &= \sum_{m_2 \equiv a[4]} \frac{1}{{m_2}^2} \\ &= \sum_{\substack{m_2 \equiv a[4] \\ m_2 > 0}} \frac{1}{{m_2}^2} + \sum_{\substack{m_2 \equiv a[4] \\ m_2 < 0}} \frac{1}{{m_2}^2} \\ &= \sum_{\substack{m_2 \equiv a[4] \\ m_2 > 0}} \frac{1}{{m_2}^2} + \sum_{\substack{m_2 \equiv -a[4] \\ m_2 > 0}} \frac{1}{(-m_2)^2}.\end{aligned}$$

Distinguons trois cas.

- Si $a \equiv 1 \pmod 4$, alors

  $\{m_2 \equiv a \pmod 4, m_2 > 0\} \cup \{m_2 \equiv -a \pmod 4, m_2 > 0\} = \{m_2 \text{ impair}, m_2 > 0\}.$

- Si $a \equiv 2 \pmod 4$,

$$\begin{aligned}\mathfrak{W} &= \sum_{\substack{m_2 \equiv a[4] \\ m_2 > 0}} \frac{1}{{m_2}^2} + \sum_{\substack{m_2 \equiv -a[4] \\ m_2 > 0}} \frac{1}{{m_2}^2} \\ &= \sum_{k \in \mathbb{Z}} \frac{2}{(4k+2)^2} \\ &= \sum_{k \in \mathbb{Z}} \frac{1}{2} \frac{1}{(2k+1)^2} \\ &= \sum_{k \geqslant 1} \frac{1}{(2k+1)^2} \\ &= \sum_{\substack{m_2 \in \mathbb{N} \\ m_2 \text{ impair}}} \frac{1}{{m_2}^2}.\end{aligned}$$

- Si $a \equiv 3 \pmod 4$, alors

  $\{m_2 \equiv a \pmod 4, m_2 > 0\} \cup \{m_2 \equiv -a \pmod 4, m_2 > 0\} = \{m_2 \text{ impair}, m_2 > 0\}.$

  Or

$$\begin{aligned}\mathcal{S} &:= \sum_{n\geqslant 1} \frac{1}{n^2} \\ &= \sum_{\substack{n\geqslant 1 \\ n \text{ pair}}} \frac{1}{n^2} + \sum_{\substack{n\geqslant 1 \\ n \text{ impair}}} \frac{1}{n^2} \\ &= \sum_{k\geqslant 1} \frac{1}{(2k)^2} + \sum_{\substack{n\geqslant 1 \\ n \text{ impair}}} \frac{1}{n^2} \\ &= \frac{1}{4}\cdot \mathcal{S} + \sum_{\substack{n\geqslant 1 \\ n \text{ impair}}} \frac{1}{n^2},\end{aligned}$$

donc

$$\begin{aligned}\sum_{\substack{m_2\in\mathbb{N} \\ m_2 \text{ impair}}} \frac{1}{{m_2}^2} &= \frac{3}{4}\cdot \mathcal{S} \\ &= \frac{3}{4}\cdot \frac{\pi^2}{6} \\ &= \frac{\pi^2}{8}.\end{aligned}$$

Tout cela nous donne que

$$\mathfrak{W} = \frac{\pi^2}{8}.$$

De plus,

$$\begin{aligned}\mathfrak{Y} &= \sum_{\substack{m_1\equiv 0[4] \\ m_1\neq 0}} \sum_{m_2\equiv a[4]} \frac{1}{(m_1 z + m_2)^2} \\ &= \sum_{\substack{m_1\equiv 0[4] \\ m_1>0}} \sum_{n\in\mathbb{Z}} \frac{1}{(m_1 z + 4n + a)^2} + \sum_{\substack{m_1\equiv 0[4] \\ m_1>0}} \sum_{n\in\mathbb{Z}} \frac{1}{(-m_1 z + 4n + a)^2}.\end{aligned}$$

Or

$$\begin{aligned}\sum_{n\in\mathbb{Z}} \frac{1}{(m_1 z + 4n + a)^2} &= \sum_{n\in\mathbb{Z}} \frac{1}{4^2} \left(\frac{m_1 z + a}{4} + n\right)^{-2} \\ &= \frac{1}{16} \sum_{n\in\mathbb{Z}} \left(\frac{m_1 z + a}{4} + n\right)^{-2}.\end{aligned}$$

On applique alors le lemme 10 avec "$z = \frac{1}{4}(mz + a)$" :

$$\sum_{n\in\mathbb{Z}}\left(\frac{m_1z+a}{4}+n\right)^{-2} = -4\pi^2\sum_{j\geqslant 1} je^{2i\pi j\frac{m_1z+a}{4}}$$
$$= -4\pi^2\sum_{j\geqslant 1} je^{i\frac{\pi}{2}j(m_1z+a)},$$

et on fait de même dans l'autre cas.
Nous avons finalement obtenu

$$\begin{aligned}\mathfrak{Y} &= \sum_{\substack{m_1\equiv 0[4]\\ m_1>0}}\frac{1}{16}\left(-4\pi^2\sum_{j\geqslant 1} je^{i\frac{\pi}{2}j(m_1z+a)} - 4\pi^2\sum_{j\geqslant 1} je^{i\frac{\pi}{2}j(m_1z-a)}\right)\\ &= -\frac{\pi^2}{4}\sum_{\substack{m_1\equiv 0[4]\\ m_1>0}}\sum_{j\geqslant 1} je^{i\frac{\pi}{2}jm_1z}\left(e^{i\frac{\pi}{2}ja}+e^{-i\frac{\pi}{2}ja}\right)\\ &= -\frac{\pi^2}{2}\sum_{\substack{m_1\equiv 0[4]\\ m_1>0}}\sum_{j\geqslant 1} je^{i\frac{\pi}{2}jm_1z}\cos\left(\frac{\pi}{2}ja\right)\\ &= -\frac{\pi^2}{2}\sum_{\substack{m_1\equiv 0[4]\\ m_1>0}}\sum_{j\geqslant 1} q^{jm_1}j\cos\left(\frac{\pi}{2}ja\right),\end{aligned}$$

avec $q = e^{i\frac{\pi}{2}z}$.
On remarque les choses suivantes :

- Si $ja \equiv 0 \pmod 4$, alors

$$\begin{cases}\cos\left(\frac{\pi}{2}ja\right) = 1\\ \frac{1}{2}\left(i^{ja}+\frac{1}{i^{ja}}\right) = \frac{1}{2}(1+1) = 1.\end{cases}$$

- Si $ja \equiv 1 \pmod 4$, alors

$$\begin{cases}\cos\left(\frac{\pi}{2}ja\right) = 0\\ \frac{1}{2}\left(i^{ja}+\frac{1}{i^{ja}}\right) = \frac{1}{2}(i-i) = 0.\end{cases}$$

- Si $ja \equiv 2 \pmod 4$, alors

$$\begin{cases}\cos\left(\frac{\pi}{2}ja\right) = -1\\ \frac{1}{2}\left(i^{ja}+\frac{1}{i^{ja}}\right) = \frac{1}{2}(-2-1) = -1.\end{cases}$$

- Si $ja \equiv 3 \pmod 4$, alors

$$\begin{cases} \cos\left(\frac{\pi}{2}ja\right) = 0 \\ \frac{1}{2}\left(i^{ja} + \frac{1}{i^{ja}}\right) = \frac{1}{2}(-i+i) = 1. \end{cases}$$

Donc

$$\cos\left(\frac{\pi}{2}ja\right) = \frac{1}{2}\left(i^{ja} + \frac{1}{i^{ja}}\right).$$

On pose alors pour tout $n \geqslant 1$,

$$c_n := -\frac{\pi^2}{4}\sum_{j|n} j\left(i^{ja} + \frac{1}{i^{ja}}\right).$$

Donc

$$G_2^{(0,a)}(z) = \frac{\pi^2}{8} + \sum_{j\geqslant 1} c_n q^n. \tag{8}$$

□

Le rayon de convergence de la série de terme général c_n étant supérieur à 1, nous obtenons que la fonction $G_2^{(0,a)}$ est bien définie et holomorphe sur $\mathbb{H}$, ce qui prouve la proposition.

Définition 20

$$\forall (m_1,m_2) \in \mathbb{Z}^2 \quad a_{m_1,m_2} := \frac{1}{m_1 z + m_2 - 4} - \frac{1}{m_1 z + m_2}.$$

$$B(z) := \sum_{a\in(\mathbb{Z}/4\mathbb{Z})^\times} \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0\ [4]} a_{m_1,m_2}(z).$$

$$C(z) := \sum_{a\in(\mathbb{Z}/4\mathbb{Z})^\times} \sum_{m_2\equiv 0[4]} \sum_{m_1\equiv a\ [4]} a_{m_1,m_2}(z).$$

Lemme 13

$$\forall (b,m_1) \in\ \mathbb{Z}^2 \quad \sum_{m_2\equiv b[4]} a_{m_1,m_2} = 0.$$

Preuve.
Soit $(b,m_1) \in \mathbb{Z}^2$.
On a

$$\begin{aligned}\sum_{m_2\equiv b[4]} a_{m_1,m_2} &= \sum_{m_2\equiv b[4]} \left(\frac{1}{m_1 z + m_2 - 4} - \frac{1}{m_1 z + m_2}\right) \\ &= \sum_{k\in\mathbb{Z}} \left(\frac{1}{m_1 z + 4k + b - 4} - \frac{1}{m_1 z + 4k + b}\right) \\ &= \sum_{k\in\mathbb{Z}} \left(\frac{1}{m_1 z + 4(k-1) + b} - \frac{1}{m_1 z + 4k + b}\right) \\ &= 0.\end{aligned}$$

□

Proposition 6

$$\forall z \in \mathbb{H} \quad B(z) = C(z) = -i\frac{\pi}{z}.$$

Preuve.
On a

$$\begin{aligned}\sum_{m_2\equiv a[4]} \left(\frac{1}{m_2 - 4} - \frac{1}{m_2}\right) &= \sum_{k\in\mathbb{Z}} \left(\frac{1}{4(k-1) + a} - \frac{1}{4k + a}\right) \\ &= 0\end{aligned}$$

car la série se télescope.
On obtient alors

$$\begin{aligned}
\sum_{m_2\equiv a[4]}\sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z) &= \sum_{m_2\equiv a[4]}\sum_{\substack{m_1\equiv 0[4]\\ m_1\neq 0}}\left(\frac{1}{m_1 z+m_2-4}-\frac{1}{m_1 z+m_2}\right)\\
&= \sum_{k\in\mathbb{Z}}\sum_{n\in\mathbb{Z}^*}\left(\frac{1}{4nz+4k+a-4}-\frac{1}{4nz+a+4k}\right)\\
&= \lim_{N\to\infty}\sum_{k=-N+1}^{N}\sum_{n\neq 0}\left(\frac{1}{4nz+4(k-1)+a}-\frac{1}{4nz+a+4k}\right)\\
&= \lim_{N\to\infty}\sum_{n\neq 0}\left(\sum_{k=-N+1}^{N}\frac{1}{4nz+4(k-1)+a}-\sum_{k=-N+1}^{N}\frac{1}{4nz+a+4k}\right)\\
&= \lim_{N\to\infty}\sum_{n\neq 0}\left(\sum_{k=-N}^{N-1}\frac{1}{4nz+4k+a}-\sum_{k=-N+1}^{N}\frac{1}{4nz+a+4k}\right)\\
&= \lim_{N\to\infty}\sum_{n\neq 0}\left(\frac{1}{4nz+a-4N}-\frac{1}{4nz+a+4N}\right)\\
&= \lim_{N\to\infty}\sum_{n\neq 0}\frac{1}{4z}\left(\frac{1}{n+\frac{a-4N}{4z}}+\frac{1}{-n+\frac{-a-4N}{4z}}\right)\\
&= \lim_{N\to\infty}2\sum_{n\geqslant 1}\frac{1}{4z}\left(\frac{1}{n+\frac{a-4N}{4z}}+\frac{1}{-n+\frac{-a-4N}{4z}}\right)\\
&= \frac{1}{2z}\lim_{N\to\infty}\sum_{n\geqslant 1}\left(\left(n+\frac{a-4N}{4z}\right)^{-1}+\left(-n+\frac{-a-4N}{4z}\right)^{-1}\right).
\end{aligned}$$

Ainsi, en utilisant la formule (6) pour la cotangente, on a

$$\begin{aligned}
2zB(z) &= \lim_{N\to\infty}\sum_{n\geqslant 1}\left(\left(n+\frac{1-4N}{4z}\right)^{-1}+\left(-n+\frac{-1-4N}{4z}\right)^{-1}\right.\\
&\qquad\left.+\left(n+\frac{3-4N}{4z}\right)^{-1}+\left(-n+\frac{-3-4N}{4z}\right)^{-1}\right)\\
&= \lim_{N\to\infty}\left(\frac{4z}{4N-1}+\pi\cot\left(\pi\frac{1-4N}{4z}\right)+\frac{4z}{4N-3}+\pi\cot\left(\pi\frac{3-4N}{4z}\right)\right).
\end{aligned}$$

Or (en se rappelant une autre vieille formule 7 pour la cotangente) :

$$\begin{cases} \dfrac{4z}{4N-1} \xrightarrow[n\to\infty]{} 0 \\ \cot\left(\pi\dfrac{1-4N}{4z}\right) = i + \dfrac{2i}{\underbrace{e^{2i\pi\frac{1-4N}{4z}}}_{\to 0} - 1} = i - 2i = -i \\ \dfrac{4z}{4N-3} \xrightarrow[n\to\infty]{} 0 \\ \cot\left(\pi\dfrac{3-4N}{4z}\right) = i + \dfrac{2i}{\underbrace{e^{2i\pi\frac{3-4N}{4z}}}_{\to 0} - 1} = i - 2i = -i. \end{cases}$$

Donc

$$2zB(z) = -2\pi i.$$ □

Ce qui conclut la démonstration, car on fait de même pour C d'après [8].

Définition 21 On définit $E_2^{(0)}$ la série d'Eisenstein associée à 0 comme

$$E_2^{(0)}(z) := \frac{4}{\pi^2}\left(4\sum_{a\in(\mathbb{Z}/4\mathbb{Z})^*} G_2^{(a,0)}(4z)\right).$$

Définition 22 Posons

$$F(z) := E_2^{(\infty))}(z) - E_2^{(0)}(z).$$

Lemme 14 On a

$$4G_2^{(a,0)}(4z) = G_2^{(a,0)}(z).$$

Preuve.
Nous admettons ce lemme, dont nous doutons de la véracité même. □

Lemme 15 Pour tout $z \in \mathbb{H}$, on a

$$-\frac{1}{4z^2}F\left(-\frac{1}{4z}\right) = F(z).$$

Preuve.
On a, d'après ce qui précède :

$$\sum_{m_2\equiv a[4]} a_{m_1,m_2}(z) = 0.$$

D'où

$$\begin{aligned} G_2^{(0,a)}(z) &= \sum_{m_1\equiv 0[4]} \sum_{m_2\equiv a[4]} (m_1 z + m_2)^{-2} \\ &= \sum_{m_1\equiv 0[4]} \sum_{m_2\equiv a[4]} (m_1 z + m_2)^{-2} - \sum_{m_1\equiv 0[4]} \sum_{m_2\equiv a[4]} a_{m_1,m_2}(z) \\ &= \sum_{m_1\equiv 0[4]} \sum_{m_2\equiv a[4]} (m_1 z + m_2)^{-2} - a_{m_1,m_2}(z). \end{aligned}$$

Or la série double de terme général $(m_1 z+m_2)^{-2} - a_{m_1,m_2}(z)$ est absolument convergente.
En effet,

$$\begin{aligned} (m_1 z + m_2)^{-2} - a_{m_1,m_2}(z) &= \frac{1}{(m_1 z + m_2)^2} - \frac{1}{m_1 z + m_2 - 4} + \frac{1}{m_1 z + m_2} \\ &= \frac{m_1 z + m_2 - 4 - (m_1 z + m_2)^2 + (m_1 z + m_2)(m_1 z + m_2 - 4)}{(m_1 z + m_2)^2 (m_1 z + m_2 - 4)} \end{aligned}$$

$$= \frac{m_1 z + m_2 - 4 - {m_1}^2 z^2 - {m_2}^2 - 2m_1 m_2 z + {m_1}^2 z^2 - 4m_1 z + 2m_2 m_1 z + {m_2}^2 - 4m_2}{(m_1 z + m_2)^2 (m_1 z + m_2 - 4)},$$

donc

$$(m_1 z + m_2)^{-2} - a_{m_1,m_2}(z) = \frac{-3m_1 z - 3m_2 - 4}{(m_1 z + m_2)^2 (m_1 z + m_2 - 4)}$$

qui est le terme général d'une série absolument convergente.
On peut donc intervertir les sommes

$$\begin{aligned} G_2^{(0,a)}(z) &= \sum_{m_1\equiv 0[4]} \sum_{m_2\equiv a[4]} (m_1 z + m_2)^{-2} - a_{m_1,m_2}(z) \\ &= \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0[4]} (m_1 z + m_2)^{-2} - a_{m_1,m_2}(z) \\ &= \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0[4]} (m_1 z + m_2)^{-2} + \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z) \\ &= \frac{1}{z^2} \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0[4]} \left(m_1 + m_2 \frac{1}{z} \right)^{-2} + \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z) \\ &= \frac{1}{z^2} \sum_{m_2\equiv -a[4]} \sum_{m_1\equiv 0[4]} \left(-m_1 + m_2 \frac{1}{z} \right)^{-2} + \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z) \\ &= \frac{1}{z^2} G_2^{(-a,0)} \left(-\frac{1}{z} \right) + \sum_{m_2\equiv a[4]} \sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z). \end{aligned}$$

Ainsi,

$$4\frac{1}{4z^2}G_2^{(a,0)}\left(-\frac{1}{z}\right) = G_2^{(0,-a)}(z) - \sum_{m_2\equiv -a[4]}\sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z). \tag{9}$$

De même, on obtient

$$\frac{1}{4z^2}G_2^{(0,a)}\left(-\frac{1}{4z}\right) = 4G_2^{(-a,0)}(4z) - 4\sum_{m_2\equiv 0[4]}\sum_{m_1\equiv -a[4]} a_{m_1,m_2}(4z). \tag{10}$$

On peut alors conclure la preuve car

$$\begin{aligned}
-\frac{1}{4z^2}F\left(-\frac{1}{4z}\right) &= -\frac{1}{4z^2}\left(E_2^{(\infty)}\left(-\frac{1}{4z}\right) - E_2^{(0)}\left(-\frac{1}{4z}\right)\right)\\
&= -\frac{1}{4z^2}\left(G_2^{(0,1)}\left(-\frac{1}{4z}\right) + G_2^{(0,-1)}\left(-\frac{1}{4z}\right) - G_2^{(1,0)}\left(-\frac{1}{4z}\right) - G_2^{(-1,0)}\left(-\frac{1}{4z}\right)\right)\\
&= -\frac{1}{4z^2}\left(G_2^{(0,1)}\left(-\frac{1}{4z}\right) + G_2^{(0,-1)}\left(-\frac{1}{4z}\right) - 4G_2^{(1,0)}\left(-\frac{1}{z}\right) - 4G_2^{(-1,0)}\left(-\frac{1}{z}\right)\right),
\end{aligned}$$

d'après le lemme 14.
Donc d'après (9) et (10), on a

$$\begin{aligned}
-\frac{1}{4z^2}F\left(-\frac{1}{4z}\right) &= -4G_2^{(-1,0)}(4z) + 4\sum_{m_2\equiv 0[4]}\sum_{m_1\equiv -1[4]} a_{m_1,m_2}(4z)\\
&\quad - 4G_2^{(1,0)}(4z) + 4\sum_{m_2\equiv 0[4]}\sum_{m_1\equiv 1[4]} a_{m_1,m_2}(4z)\\
&\quad + G_2^{(0,-1)}(z) - \sum_{m_2\equiv -1[4]}\sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z)\\
&\quad + G_2^{(0,1)}(z) - \sum_{m_2\equiv 1[4]}\sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z)\\
&= G_2^{(0,-1)}(z) + G_2^{(0,1)}(z) - 4G_2^{(-1,0)}(4z) - 4G_2^{(1,0)}(4z)\\
&\quad + 4\left(\sum_{m_2\equiv 0[4]}\sum_{m_1\equiv -1[4]} a_{m_1,m_2}(4z) + \sum_{m_2\equiv 0[4]}\sum_{m_1\equiv 1[4]} a_{m_1,m_2}(4z)\right)\\
&\quad - \left(\sum_{m_2\equiv -1[4]}\sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z) + \sum_{m_2\equiv 1[4]}\sum_{m_1\equiv 0[4]} a_{m_1,m_2}(z)\right)\\
&= E_2^{(\infty)}(z) - 4E_2^{(0)}(4z) + 4C(4z) - B(z)\\
&= E_2^{(\infty)}(z) - E_2^{(0)}(z) - i\frac{\cancel{4}\pi}{\cancel{4}z} - \left(-i\frac{\pi}{z}\right)\\
&= F(z)
\end{aligned}$$

□

Proposition 7 La seule forme parabolique de poids 2 pour $\Gamma_0(4)$ est la forme nulle.

Preuve.
Cette proposition est ici admise, car nous en avons trouvé une démonstration merveilleuse mais les marges de cet écrit sont trop étroites pour la contenir. □

Proposition 8 Pour tout $a \in (\mathbb{Z}/4\mathbb{Z})^\times$, la fonction $G_2^{(0,a)}$ est bien définie et est holomorphe sur $\mathbb{H}$.
De plus, en notant $q = e^{2i\pi z}$,

$$4G_2^{(a,0)}(4z) = -\pi^2 \sum_{n \geqslant 1} d_n q^n$$

où

$$d_n = \sum_{\substack{j|n \\ n/j \text{ impair}}} j.$$

Preuve.
Pour une preuve plus détaillée, venir se plaindre aux auteurs. □

Proposition 9

$$\theta^4 = F$$

Preuve.
L'idée de la démonstration est de montrer que $\theta^4 - F$ est une forme parabolique de poids 2.
On sait que $\theta^4 - F$ est une forme modulaire.
On vérifie que celle-ci s'annule bien au pointe.
Alors comme on sait déjà que la seule forme parabolique de poids 2 est la forme nulle, on a que $\theta^4 - F = 0$ ce qui conclut. □

On rappelle le théorème que l'on va finalement démontrer :

Théorème 12 (Formule de Jacobi)

$$\forall n \ \in \mathbb{N} \quad r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid 4}} d.$$

Preuve.
Comme la proposition 9 donne que $\theta^4 = F$, on peut identifier leurs coefficients de Fourier trouvés précédemment, et en se servant de bon nombre de relations établies, on trouve (en admettant quelques calculs) que la suite $(r_4(n))_{n\in\mathbb{N}}$ des coefficients de Fourier de θ^4 vaut pour tout $n \in \mathbb{N}$

$$\begin{aligned} r_4(n) &= \frac{8}{\pi^2}(c_n - d_n) \\ &= 8 \underbrace{\sum_{\substack{j|n \\ n/j \text{ impair}}} j}_{\mathscr{S}_1} - 2 \underbrace{\sum_{j|n} j(i^j + i^{-j})}_{\mathscr{S}_2}. \end{aligned}$$

On distingue deux cas.

- Si n est impair, alors

$$\mathscr{S}_1 = \sum_{j|n} j$$

et

$$\mathscr{S}_2 = \sum_{j|n} j \underbrace{(i^j + i^{-j})}_{=0} = 0.$$

- Si n est pair, alors il existe n_0 impair et $r \geqslant 1$ tel que $n = 2^r n_0$.
On a

$$\mathscr{S}_1 = \sum_{j|n_0} 2^r j = 2^r \sum_{j|n_0} j.$$

Pour la seconde somme $\mathscr{S}_2$, on distingue quatre cas :

- si $j \equiv 0 \pmod 4$, alors $(i^j + i^{-j}) = 2$,
- si $j \equiv 1 \pmod 4$, alors $(i^j + i^{-j}) = 0$,
- si $j \equiv 2 \pmod 4$, alors $(i^j + i^{-j}) = -2$,
- si $j \equiv 3 \pmod 4$, alors $(i^j + i^{-j}) = 0$.

Donc

$$\begin{aligned}
\mathscr{S}_2 &= \sum_{j|n} j(i^j + i^{-j}) \\
&= 2 \sum_{2|d|n} j(-1)^{j/2} \\
&= 2 \sum_{k=1}^{r} \sum_{j|n_0} 2^k j(-1)^{\frac{2^k j}{2}} \\
&= 2 \sum_{k=1}^{r} \sum_{j|n_0} 2^k j(-1)^{2^{k-1} j} \\
&= 2 \sum_{j|n_0} 2j(-1) + \sum_{k=2}^{r} \sum_{j|n_0} 2^k j \times 1 \\
&= 2 \left(-2 + \sum_{k=2}^{r} 2^k \right) \sum_{j|n_0} j \\
&= 2 \left(-2 + (2^{r+1} - 2 - 2) \right) \sum_{j|n_0} j \\
&= \left(2^{r+2} - 12 \right) \sum_{j|n_0} j.
\end{aligned}$$

Tout cela nous donne

$$\begin{aligned} r_4(n) &= 8\mathscr{S}_1 - 2\mathscr{S}_2 \\ &= 8 \cdot 2^r \sum_{j|n_0} j - 2(2^{r+2} - 12) \sum_{j|n_0} j \\ &= \big(8 \cdot 2^r - 2(2^{r+2} - 12)\big) \sum_{j|n_0} j \\ &= \big(2^{r+3} - 2^{r+3} + 24)\big) \sum_{j|n_0} j \\ &= 24 \sum_{j|n_0} j. \end{aligned}$$

Enfin, si $j \mid n$ mais $4 \nmid j$, alors

$$j \mid n_0 \text{ ou } (j = 2j' \text{ et } j' \mid n_0).$$

Donc

$$\begin{aligned} 8 \sum_{\substack{d|n \\ 4\nmid d}} d &= 8 \left(\sum_{d|n_0} d + \sum_{d|n_0} 2d \right) \\ &= 8 \cdot 3 \sum_{d|n_0} d \\ &= r_4(n). \end{aligned}$$

Ce qui démontre la formule de Jacobi :

$$\forall n \in \mathbb{N} \quad r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d.$$

□

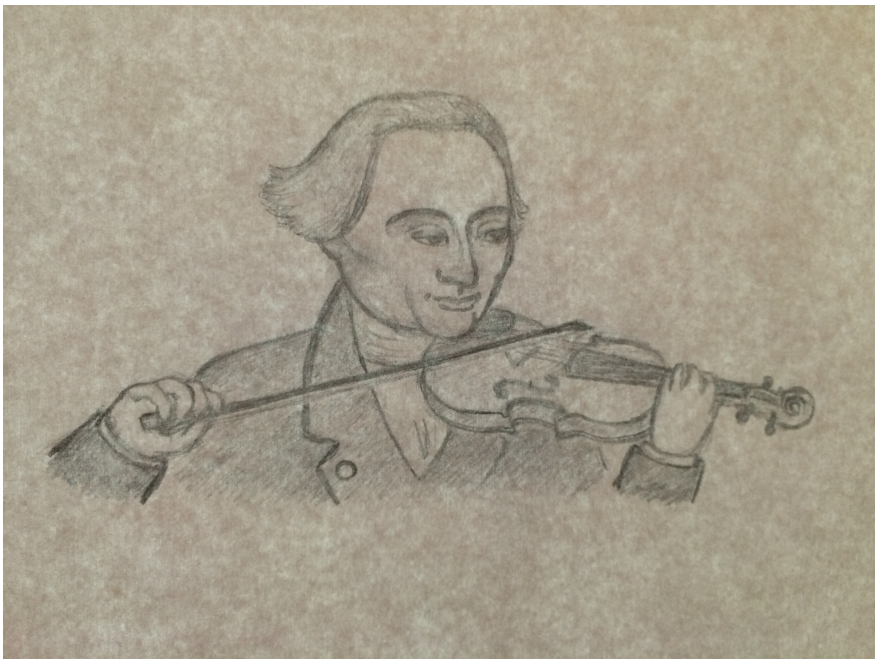


FIGURE 7 – Lagrange pratiquant son violon

5 Conjectures ouvertes

Poser l'impénétrabilité de la matière
c'est reconnaître la solidarité du nombre et de l'espace.
Essai sur les données immédiates de la conscience, Bergson.

Jouons.

Le jeu est simple. Olivier choisit un nombre assez grand [18] (noté n), et Florent commence à jouer. Il choisit un carré k^2 pour rester dans le thème du projet, de sorte que $n - k^2$ soit supérieur à 1. Le premier qui se retrouve avec le nombre 1 et qui ne peut donc plus rien retirer perd.

Exemple 2 Olivier choisit 29.
Florent retire 4^2 ce qui donne 13.
Olivier retire 3^2 ce qui donne 4.
Florent retire 1^2 ce qui donne 3.
Olivier retire 1^2 ce qui donne 2.
Florent retire 1^2 ce qui donne 1.
Olivier perd...

Notre but va alors être de faire gagner Olivier. Commençons par supposer que les deux joueurs jouent parfaitement [19], et déterminons qui gagne sur quel nombre. Pour cela nous procédons de façon récursive. Si Olivier choisit 1, il gagne, bien que ce ne soit pas très fair-play. S'il choisit 2, il perd etc.. Puis pour un plus grand nombre n choisi par Olivier, on regarde si Florent peut jouer un coup qui le ramène à un cas de victoire pour lui. Plus n augmente, plus il a de possibilités de victoires donc. S'il n'existe aucun tel coup, il perdra. Nous pouvons donc ainsi algorithmiquement déterminer quel nombre donne la victoire à quel joueur.
Nous implémentons cet algorithme en Sage.

```
def strat(n,L=[]):
    l=len(L)+1
    while l<n:
        suivant=True
        i=1
        while i^2<l and suivant:
            if L[l-i^2-1]==0:
                L.append(1)
                l+=1
                suivant=False
            i+=1
        if suivant:
            L.append(0)
            l+=1
    return L
```

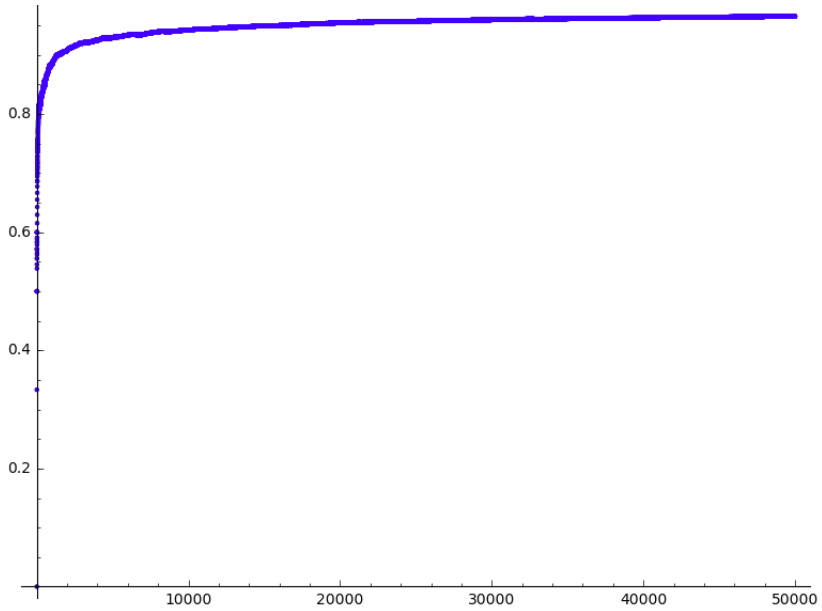
18. Pour que le jeu soit intéressant.
19. Ce dont nous ne doutons pas une seconde.

Grâce à cet algorithme, nous pouvons donner à titre indicatif la liste des nombres donnant la victoire à Olivier :

1, 3, 6, 8, 11, 13, 16, 18, 21, 23, 35, 40, 45, 53, 58, 63, 66, 68, 73, 86, 96...

Nous remarquons bien que Olivier n'a que peu de victoires contrairement à Florent. Peu nous en faut pour continuer, et un peu de programmation plus tard nous voilà en mesure de tracer la proportion de victoires de Florent $F(n)$ définie comme suit

$$F(n) = \frac{\#\{k, \text{ Florent gagne pour } k\}}{n}.$$

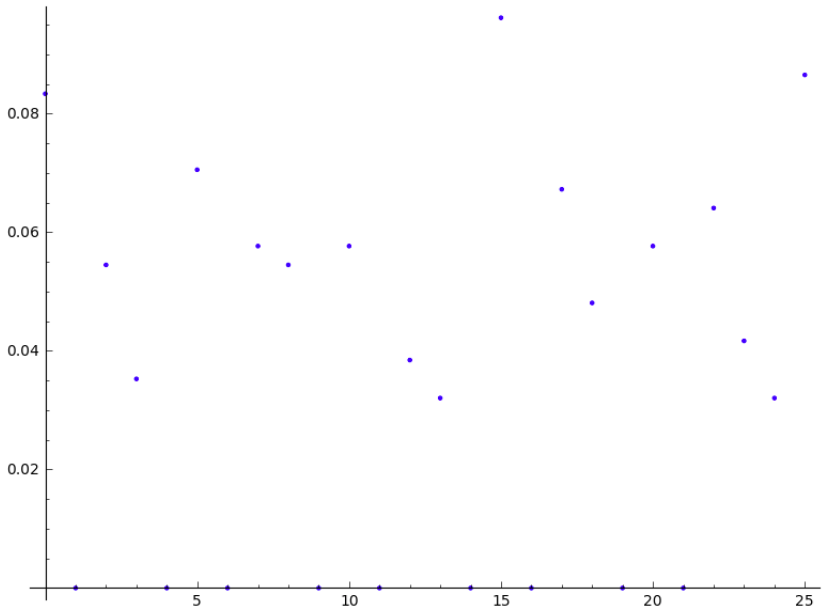


Graphe de $F(n)$

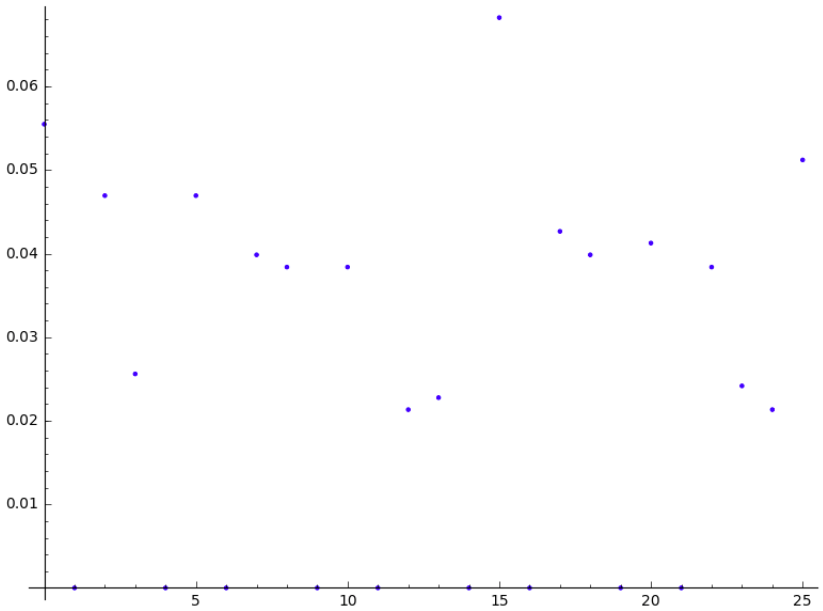
Nous observons que

$$F(n) \xrightarrow[n\to+\infty]{} 1,$$

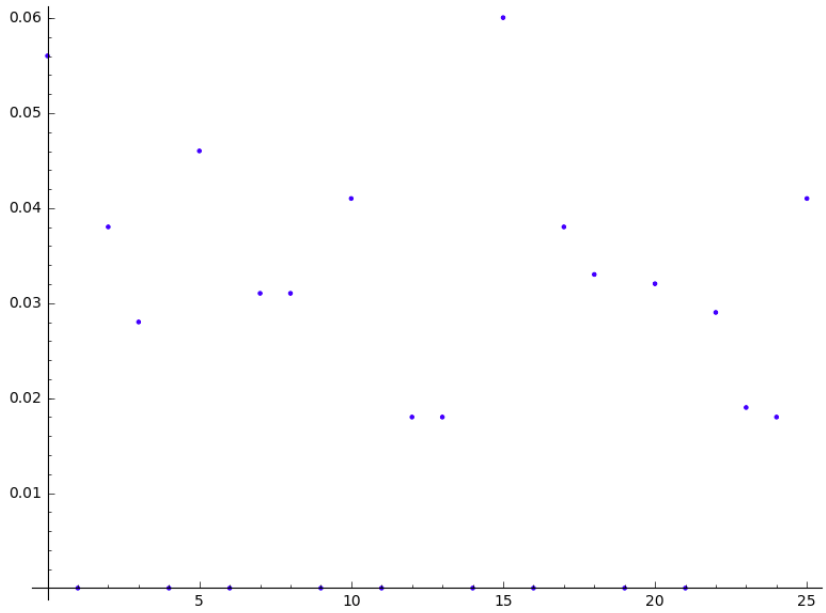
ce qui pourrait sûrement se démontrer.
Mais nous souhaitons tout de même qu'Olivier gagne par souci d'équité. Notre idée est alors de trouver des entiers k pour qu'en choisissant le nombre $n^2 + k$ au début du jeu, Olivier maximise ses chances de victoire.
Nous traçons le pourcentage de victoires pour Olivier quand il choisit le nombre $n^2 + k$ avec $n^2 \in \{10^5, 5 \cdot 10^5, 10^6\}$ et $k \in \{0, \ldots, 25\}$.



Pourcentage de victoires pour $n = 10^5$



Pourcentage de victoires pour $n = 5 \cdot 10^5$



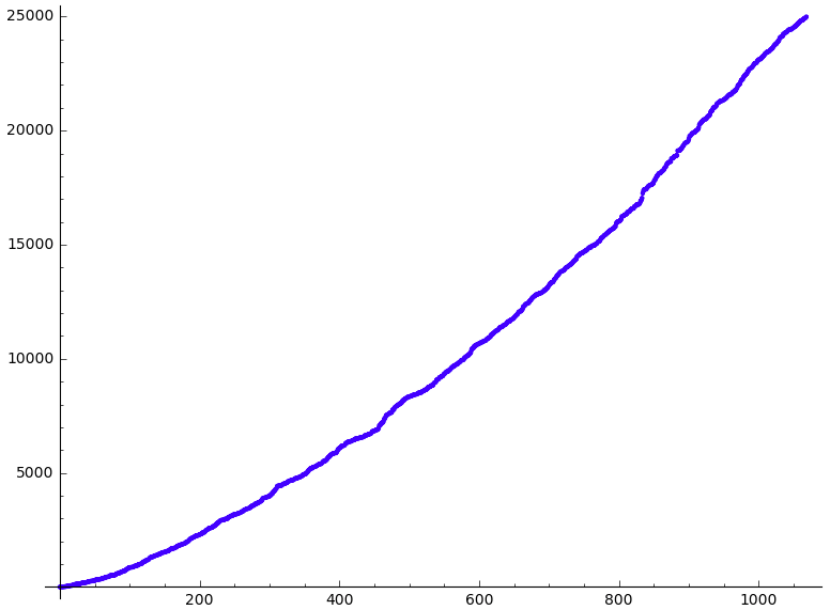
Pourcentage de victoires pour $n = 10^6$

C'est très intrigant. Avant tout, lorsque $k = 1$, Florent gagne à coup sûr, et c'est logique. En effet, il lui suffit de choisir n^2 et Olivier se retrouvera immédiatement avec le nombre 1.
Mais certaines valeurs de k semblent donner une bien plus grande probabilité de victoire pour notre ami Olivier. Typiquement $k = 0$ ou $k = 15$. La raison de tout ceci reste en revanche très mystérieuse. Le lecteur intéressé pour essayer d'y répondre ici : `http://math.stackexchange.com/questions/1803365/mathematical-game-with-numbers?noredirect=1#comment3686148_1803365`.

Nous pouvons aussi remarquer que pour certaines valeurs de k, c'est Florent qui gagne à coup sûr. Celles-ci sont 1, 4, 6, 9, 11, 13, 16, 19 et 21. Il semblerait que ce soient les multiples de 5 augmentés et diminués de 1. L'exception étant 24. Nous sommes perplexes face à tant de mystères.

Par curiosité, traçons les différents nombres gagnants d'Olivier, peut-être que cela nous donnera des informations [20]. Nous utilisons les données de la suite A224839 de la base de donnée OEIS, qui correspond exactement à notre problème.

20. Cela nous donnera des informations.



Les nombres gagnants d'Olivier

Pour comprendre ce graphique, il faut comprendre que le millième nombre gagnant d'Olivier est de l'ordre de 20 000. Ce qui montre bien qu'au bout de 20 000 nombres, Olivier n'aura gagné que mille fois. Le fait que la "dérivée" de cette fonction augmente signifie que plus les nombres grandissent, moins ils sont favorables à Olivier.

Les mathématiciens ont montré qu'en notant $\mathscr{O}(n)$ le n-ième nombre gagnant d'Olivier, la suite $\mathscr{O}(n)$ a un ordre compris de la sorte :

$$n \log(n)^{(1/12)\log\log\log\log n} < \mathscr{O}(n) < n^{1.365}.$$

Finalement...

On vit rarement [...] l'ours [...] et [...] la crème brûlée [...] nucléaire pour son appréciation égale de l'harmonie des mathématiques et des accords.
Tours de courbes de Shimura, systèmes d'Euler et théorie d'Iwasawa des formes modulaires ordinaires, Olivier Fouquet [1].

On ne compte plus le nombre de fois où notre écrit a été traité de dépotoire. Il n'en reste pas moins un très beau dépotoire. Un débeautoire d'après nous.

Recette du gâteau magique

Temps de préparation : 16 minutes
Temps de cuisson : 49 minutes
Ingrédients (pour 9 personnes) :

- 1 pincée de sel
- 1 cuillère à soupe d'eau
- 1 sachet de sucre vanillé
- 4 oeufs
- 49 cl de lait
- 100 g de farine
- 121 g de beurre
- 144 g de sucre en poudre.

Préparation de la recette :

Choisir un joli moule carré de côté $2\pi\sqrt{3}$ cm [21].
Préchauffer le four (2^2) à 144°C.
Séparer les (255,255,255) d'oeufs des (242,238,5).
Permuter les (242,238,5) avec le sucre en poudre, l'eau et le sucre vanillé jusqu'à en augmenter la composante bleue.
Intégrer le beurre fondu.
Additionner la farine et le sel.
Après permutation circulaire, additionner délicatement le lait sous l'action de $\mathfrak{S}_n$ avec n suffisamment grand.
Monter les (255,255,255) en neige puis les additionner au résultat précédent.
Versez la préparation dans le moule en lissant les maxima locaux.
Enfourner 49 minutes à 144°C.
La magie opère.
A la sortie du four (2^2) le gâteau sinusoïde frénétiquement mais il reste asymptotiquement doré.
Attendre qu'il refroidisse pour que sa dérivée s'annule.

21. Afin d'avoir la même contenance qu'un moule circulaire de diamètre 24 cm.

Pour écourter cette attente, nous vous proposons une conclusion qui viendra couronner notre travail. Vous aurez sans doute remarqué que certaines pages de ce mémoire étaient plus nobles et plus pures que les autres. Nous parlons évidemment des pages 1, 4, 9, 16, 25, 36, 49, 64, 81 et 100. Mais cela ne ternit pas l'éclat des autres, et les mathématiques demeurent la vérité et la perfection incarnées en des signes vaporeux. Néanmoins, malgré son apparence cabalistique, le théorème de Lagrange est parfaitement accessible à un enfant de 13 ans. Nous l'avons d'ailleurs testé sur une classe de quatrièmes, et ceux-ci ont eu grand plaisir à trouver moult décompositions d'entiers inférieurs à 100 en somme de 4 carrés. Moralité [22], le théorème de Lagrange est une approche ensorcelante d'un paysage vivant dont nous voudrions atteindre, un jour, l'horizon.

Mais le gâteau magique est maintenant tout à fait refroidi, il est temps d'achever cette péroraison pour passer aux choses essentielles.

Régalez-vous puis démoulez les restes.

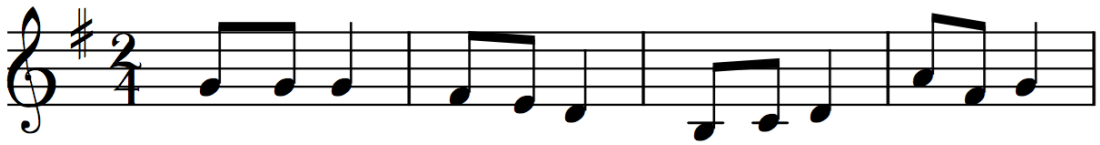


FIGURE 8 – Ode au projet

22. Il est vrai que le lit est un endroit où l'on meurt souvent.

Annexe A

Cette partie vise à étendre l'algorithme d'Euclide aux entiers relatifs.

Définition 23 Division euclidienne prime (DEP).

$$\forall a \in \mathbb{Z} \quad \forall b \in \mathbb{Z}^* \quad \exists (q,r) \in \mathbb{Z}^* \times \mathbb{Z} \quad a = bq + r \quad \text{et} \quad |r| < |b| .$$

Preuve.
Soient a et b dans $\mathbb{Z}$, b non nul.
On sait qu'il existe q et r entiers tels que $a = bq + r$ et $|r| < |b|$.
Supposons que q est nul, *i.e.* $|a| < |b|$.
Alors on choisit $q' = 1$. Ainsi on a $a = b + r'$, avec $r' = a - b$ et $|r'| < |b|$.

Algorithme d'Euclide Prime.

Soit $a,b \in \mathbb{Z}$ non nuls [23].
On définit par récurrence la suite (a_n) comme

$$\begin{cases} a_0 = a \text{ et } a_1 = b \\ a_n = r \text{ où } r \text{ est le reste de la DEP de } a_{n-2} \text{ par } a_{n-1}. \end{cases}$$

On note d le dernier terme non nul de la suite a, s'il existe.

Théorème 13 On a

$$d = (a,b).$$

Preuve.
Par définition de la DEP et de la suite (a_n)

$$a_n = q_{n+2} \times a_{n+1} + a_{n+2} \quad \text{et} \quad 0 \leq |a_{n+2}| < |a_{n+1}| .$$

La suite $(|a_n|)$ est donc strictement décroissante, puis vaut donc 0 à partir d'un certain rang.
Nous notons d le dernier terme non nul.
Montrons par récurrence sur $n \in \mathbb{N}$ l'assertion :

$$\mathscr{P}(n) : (a_n,a_{n+1}) = (a,b).$$

- **Initiation :** Evident.
- **Hérédité :** Supposons $\mathscr{P}(n)$.
  On a $a_n = a_{n+1} \times q + a_{n+2}$.
  Or $(a_n,a_{n+1}) \mid a_n$ donc $(a_n,a_{n+1}) \mid a_{n+1}q + a_{n+2}$ et $(a_n,a_{n+1}) \mid a_{n+1}$.
  D'où $(a_n,a_{n+1}) \mid a_{n+2}$.
  Donc $(a_n,a_{n+1}) \mid (a_{n+1},a_{n+2})$.

23. Le cas où a ou b est nul ne nécessite aucun algorithme ; on l'exclut.

Réciproquement, $(a_{n+1},a_{n+2}) \mid a_{n+1}$ et $(a_{n+1},a_{n+2}) \mid a_{n+2}$.
Donc $(a_{n+1},a_{n+2}) \mid a_{n+1}q + a_{n+2}$ d'où $(a_{n+1},a_{n+2}) \mid a_n$.
Donc $(a_{n+1},a_{n+2}) \mid (a_n,a_{n+1})$.
Finalement, $(a_n,a_{n+1}) = (a_{n+1},a_{n+2})$.
Or $(a_n,a_{n+1}) = (a,b)$ par hypothèse de récurrence.
D'où $\mathscr{P}(n+1)$.

- **Conclusion :**

$$\forall n \in \mathbb{N} \quad \mathscr{P}(n).$$

□

Finalement, $|d| = (d,0) = (a,b)$.

Annexe B

Comme deuxième annexe, nous nous proposons de discuter d'un résultat sur les sous-groupes multiplicatifs réels.

Commençons par une définition qui nous servira à énoncer un théorème sous de correctes hypothèses. A trop vouloir restreindre les hypothèses on finit par énoncer des bêtises.

Définition 24 On dit que $(a,b) \in (\mathbb{R}_+^*)^2$ est log-*libre* si

$$\frac{\log a}{\log b} \notin \mathbb{Q}^*.$$

Remarque 10 On remarque en particulier que $(a,b) \in {\mathbb{N}_{\geqslant 2}}^2$ est log-libre dès que a et b ont un de leurs facteurs premiers différents.
En effet, si par l'absurde

$$\frac{\log a}{\log b} = \frac{p}{q} \in \mathbb{Q},$$

alors

$$a^q = b^p$$

ce qui est absurde d'après le théorème fondamental de l'arithmétique si a et b ont un facteur en premier différent.

Théorème 14 Soit G un sous-groupe multiplicatif de $\mathbb{R}^*$.
S'il existe $(a,b) \in G^2$ log-libre, alors G est dense dans un intervalle de $\mathbb{R}$.

Remarque 11 Avant d'attaquer la preuve, le lecteur pourra ici se motiver de l'utilité de l'hypothèse de log-liberté. Le lecteur pressé pourra même se convaincre de la véracité du théorème à travers ces quelques (contre-)exemples.

(i) $\langle 2 \rangle = \{2^k, k \in \mathbb{Z}\}$ n'est pas dense, mais pour tous k,k', $\dfrac{\log(2^k)}{\log(2^{k'})} = \dfrac{k}{k'} \in \mathbb{Q}$ ce qui contredit l'hypothèse de log-liberté.

(ii) $\langle e^2, e^3 \rangle$ n'est pas dense... mais l'hypothèse de log-liberté n'est pas non plus vérifiée.

(iii) $\langle \sqrt{2}, \sqrt[3]{2} \rangle$ n'est pas dense... mais l'hypothèse de log-liberté n'est pas non plus vérifiée.

Preuve.
Faisant fi de toute sorte d'approche méta-mathématique de la chose nous choisissons $x > 0$ pour essayer de construire une suite $(\delta_n)_{n\in\mathbb{N}}$ d'éléments de G telle que

$$\delta_n \in G \xrightarrow[n\to+\infty]{} x \in \mathbb{R}_+^*.$$

En effet, par souci de clarté nous éviterons de gérer les ennuyeux problèmes de signes, en évinçant d'entrée de jeu toutes les histoires d'$\varepsilon = \pm 1$. On considère ainsi dans toute la suite que $G \subset \mathbb{R}_+$. Le lecteur rigoureux aura le droit de se plaindre.

Par hypothèse, il existe $(\alpha,\beta) \in G^2$ log-libre. Fixons un tel couple d'éléments de G dans toute la suite. Si par le plus grand des malheurs $\beta < 1$, alors on peut remarque que $\beta^{-1} \in G$ et est strictement plus grand que 1. De plus le couple (α,β^{-1}) reste log-libre. On remplace donc au besoin β par son inverse pour s'assurer d'avoir $\beta > 1$.

Dernier petit préliminaire avant d'attaquer sérieusement les choses, parlons de beta-numérotation, ou encore de base non entière. De la même manière qu'en base 10, on peut parler de base β. Car $\beta > 1$, chaque réel positif aura au moins une écriture en base β, bien que les "chiffres" de cette écriture ne seraient entiers que par un pur hasard.
Ainsi,

$$\forall y \geqslant 0 \quad \exists (y_i)_{i\in\ \mathbb{Z}} \in (\mathbb{R}_+)^{\mathbb{Z}} \quad y = \sum_{i\in\mathbb{Z}} y_i \beta^i,$$

où $y_i := \left\lfloor \frac{x}{\beta^i} \right\rfloor$, ce qui assure que la somme est finie "vers le haut".

Nous allons construire la suite $(\delta_n)_{n\in\mathbb{N}}$ tant désirée telle que

$$\forall n \in \mathbb{N} \quad |x - \delta_n| \leqslant \frac{(1+n)}{n} \beta^{-n}.$$

On a $x > 0$, donc d'après les préliminaires sur la beta-numérotation, il existe $m \in \mathbb{Z}$ et $(x_i)_{i\leqslant m} \in (\mathbb{R}_+)^{\{i\leqslant m\}}$ tels que

$$x = \sum_{i=-\infty}^{m} x_i \beta^i.$$

Nous allons encore avoir besoin de lemmes que nous énonçons et démontrons par prévoyance.

Lemme 16 Soit H un sous-groupe de $(\mathbb{R},+)$.
L'ensemble H est soit monogène, soit dense dans $\mathbb{R}$.

Preuve.
Soit H un sous-groupe additif de $\mathbb{R}$.
On a clairement $H \cap \mathbb{R}^+ \neq \emptyset$.
Posons

$$\eta := \inf\{h \in H \cap \mathbb{R}_+^*\}.$$

Distinguons deux cas.

- Si $\eta > 0$.
  Soit $h \in H$, et $k \in \mathbb{Z}$ tel que

$$k\eta \leqslant |h| < (k+1)\eta.$$

  Si $|h| = k\eta$, alors $h = \pm k\eta$.
  Sinon,

$$k\eta < |h| < (k+1)\eta,$$

  donc pour tout ε assez petit,

$$k(\eta+\varepsilon) \leqslant |h| < (k+1)(\eta+\varepsilon).$$

  En particulier, vu la définition de η, il existe ε aussi petit que voulu de telle sorte que $\eta + \varepsilon \in H$.
  On a alors $|h| - k(\eta+\varepsilon) \in H$, et

$$\begin{aligned} 0 &\leqslant |h| - k(\eta+\varepsilon) \\ &< (k+1)(\eta+\varepsilon) - k(\eta+\varepsilon) \\ &= \eta + \varepsilon. \end{aligned}$$

  On fait tendre ε vers 0, ce qui nous donne

$$0 \leqslant |h| - k\eta < \eta.$$

  Donc par définition de η, $|h| - k\eta = 0$, donc on a aussi $h = \pm k\eta$.
  Donc $H = \langle \eta \rangle$, et donc en particulier H est monogène.
- Si $\eta = 0$.
  Soit $r \in \mathbb{R}$, $\varepsilon > 0$.
  Comme $\eta = 0$, il existe $h \in]0,\varepsilon] \cap H$.
  On considère $r \geqslant 0$, le cas r négatif se traitant exactement de la même façon.
  Soit $k \in \mathbb{N}$ tel que

$$kh \leqslant r < (k+1)h.$$

  On a bien $kh \in H$, et de plus

$$\begin{aligned} 0 &\leqslant r - kh \\ &\leqslant (k+1)h - kh \\ &= h \\ &\leqslant \varepsilon \end{aligned}$$

  Donc $|r - kh| \leqslant \varepsilon$, ce qui montre que H est dense dans $\mathbb{R}$. □

Lemme 17 L'ensemble

$$\begin{aligned} H &:= \mathbb{Z}[\log(\alpha), \log(\beta)] \\ &= \{a\log(\alpha) + b\log(\beta),\ (a,b) \in \mathbb{Z}^2\} \end{aligned}$$

est dense dans $\mathbb{R}$.

Preuve.
Car tout ce qui a besoin d'être nul a déjà été choisi non nul, car tout ce qui a besoin d'être différent de 1 a déjà été choisi différent de 1, toutes les opérations que nous mèneront pas la suite ont été déclarée licites par une haute instance.
On a clairement que H est un sous-groupe additif de $\mathbb{R}$.
Or d'après le lemme 16, H est soit monogène, soit dense dans $\mathbb{R}$.
Il suffit donc de montrer que H n'est pas monogène.
Supposons par l'absurde qu'il existe $\gamma \in \mathbb{R}$ tel que $H = \langle\gamma\rangle$.
On a $(\log(\alpha), \log(\beta)) \in H^2$, donc il existe $(u,v) \in \mathbb{Z}^2$ tel que

$$\begin{cases} \log(\alpha) = u\gamma \\ \log(\beta) = v\gamma, \end{cases}$$

donc

$$\frac{\log\alpha}{\log\beta} = \frac{u}{v} \in \mathbb{Q}.$$

Or on a choisi (α,β) de telle sorte que le couple soit log-libre.
Nous avons donc foncé tête baissée dans une absurdité.
L'ensemble H est donc dense dans $\mathbb{R}$. □

Revenons à la construction de notre suite.
Posons pour tout $n \in \mathbb{N}$

$$N_n := \sum_{i=-n}^{m} x_i \beta^{i+n}.$$

Soit $\dfrac{1}{n} > 0$.
On veut trouver $(a,b) \in \mathbb{N}^2$ tel que

$$\left(N_n - \frac{1}{n}\right)\beta^b \leqslant \alpha^a < \left(N_n + \frac{1}{n}\right)\beta^b. \tag{11}$$

En passant au logarithme, cela revient à vouloir

$$\log\left(N_n - \frac{1}{n}\right) + b\log(\beta) \leqslant a\log(\alpha) < \log\left(N_n + \frac{1}{n}\right) + b\log(\beta),$$

soit

$$\log\left(N_n - \frac{1}{n}\right) \leqslant a\log(\alpha) - b\log(\beta) < \log\left(N_n + \frac{1}{n}\right).$$

Or $\left|\ln(N_n + \frac{1}{n}) - \ln(N_n - \frac{1}{n})\right| > 0$.
Donc d'après le lemme 17, un tel couple (a,b) existe.
Ce couple vérifie alors l'équation (11).
On a donc

$$N_n - \frac{1}{n} \leqslant \alpha^a\beta^{-b} < N_n + \frac{1}{n}.$$

Posons

$$\begin{aligned}\delta_n &:= \alpha^a\beta^{-b}\beta^{-n}\\ &= \alpha^a\beta^{-b-n}.\end{aligned}$$

On a bien $\delta_n \in G$, car G est un groupe (donc stabilité par produit et inverse).
De plus,

$$|x - \delta_n| = \left|\sum_{i=-\infty}^{m} x_i\beta^i - \underbrace{\alpha^a\beta^{-b}}_{\in[N_n-\frac{1}{n},N_n+\frac{1}{n}]}\beta^{-n}\right|,$$

donc il existe $\varepsilon \in [-1,1]$ (il suffit de prendre le maximum de sur $[-1,1]$ borné) tel que

$$\begin{aligned}|x - \delta_n| &\leqslant \left|\sum_{i=-\infty}^{m} x_i\beta^i - \left(N_n + \frac{\varepsilon}{n}\right)\beta^{-n}\right|\\ &= \left|\sum_{i=-\infty}^{m} x_i\beta^i - \left(\frac{\varepsilon}{n} + \sum_{i=-n}^{m} x_i\beta^{i+n}\right)\beta^{-n}\right|\\ &= \left|\sum_{i=-\infty}^{m} x_i\beta^i - \frac{\varepsilon}{n}\beta^{-n} - \sum_{i=-n}^{m} x_i\beta^i\right|\\ &= \left|-\frac{\varepsilon}{n\beta^n} + \sum_{i=-\infty}^{-(n+1)} x_i 10^i\right|\\ &\leqslant |\varepsilon|\,\frac{1}{n\beta^n} + \beta^{-n}\\ &\leqslant \frac{1}{n\beta^n} + \beta^{-n}\\ &= \frac{1+n}{n\beta^n}\end{aligned}$$

Ainsi, nous avons bien construit une suite $(\delta_n)_{n\in\mathbb{N}}$ telle que

$$\forall n \in \mathbb{N} \quad \delta_n \in G \text{ et } |x - \delta_n| \leqslant \frac{(1+n)}{n\beta^{-n}} \xrightarrow[n\to+\infty]{} 0.$$

Donc le groupe G est dense, ce qui conclut la preuve du théorème.

Remarque 12 S'il n'était pas l'heure de dîner, nous pourrions sûrement prouver la réciproque de ce théorème.

Remarque 13 Cette preuve nous a permis de comprendre quelque chose d'essentiel. Il est très souvent plus facile de travailler avec le groupe additif $(\mathbb{R},+)$ puis de transposer les résultats grâce au logarithme.

Annexe C

Donnons un corollaire à l'annexe précédente.

Corollaire 2 L'ensemble des nombres décimaux inversibles est dense dans l'ensemble des nombres réels :

$$\overline{\mathbb{D}^\times} = \mathbb{R}.$$

Pour cela, commençons par rappeler ce qu'est un nombre décimal.

Définition 25 Un nombre réel d est appelé *nombre décimal* s'il existe $n \in \mathbb{N}$ tel que $10^n d \in \mathbb{Z}$.
On note $\mathbb{D}$ l'ensemble des nombre décimaux, et $\mathbb{D}^\times$ l'ensemble des nombres décimaux inversibles dans $\mathbb{D}$.

Essayons maintenant de caractériser les décimaux inversibles.

Proposition 10

$$\mathbb{D}^\times = \{\varepsilon 2^\alpha 5^\beta,\ \ (\varepsilon,\alpha,\beta) \in \{-1,1\} \times \mathbb{Z}^2\}.$$

Preuve.
Notons $E := \{\varepsilon 2^\alpha 5^\beta,\ \ (\varepsilon,\alpha,\beta) \in \{-1,1\} \times \mathbb{Z}^2\}$.
Soit $d_1 \in \mathbb{D}^\times$. Il existe donc $d_2 \in \mathbb{D}$ tel que $d_1 d_2 = 1$
Par définition d'un nombre décimal, il existe donc $(k_1,k_2) \in \mathbb{Z}^2$ tel que $10^{k_i} d_i \in \mathbb{Z}$ pour $i = 1,2$. Même mieux, on peut choisir $\varepsilon_i \in \{-1,1\}$ tel que $n_i := \varepsilon_i 10^{k_i} d_i \in \mathbb{N}$ pour $i = 1,2$.
On a donc

$$n_1 n_2 = \varepsilon_1\varepsilon_2 10^{k_1+k_2} = \varepsilon_1\varepsilon_2 2^{k_1+k_2} 5^{k_1+k_2} \in \mathbb{N},$$

et d'après le théorème fondamental de l'arithmétique, il existe donc $(\varepsilon,\alpha,\beta) \in \{-1,1\} \times \mathbb{Z}^2$ tel que $n_1 = \varepsilon 2^\alpha 5^\beta$.
Donc

$$d_1 = \varepsilon \frac{n_1}{10^{k_1}} = \varepsilon 2^\alpha 5^\beta 10^{-k_1} = \varepsilon 2^{\alpha-k_1} 5^{\beta-k_1} \in E.$$

Donc $\mathbb{D}^\times \subset E$.
Réciproquement, soit $(\varepsilon,\alpha,\beta) \in \{-1,1\} \times \mathbb{Z}^2$.
On a

$$\begin{cases} \dfrac{1}{\varepsilon} = \varepsilon \\ \dfrac{1}{2^\alpha} = \dfrac{5^\alpha}{10^\alpha} \\ \dfrac{1}{5^\beta} = \dfrac{2^\beta}{10^\beta}, \end{cases}$$

donc

$$\frac{1}{\varepsilon 2^{\alpha}5^{\beta}} = \varepsilon 2^{\beta}5^{\alpha}10^{-\alpha-\beta}.$$

Donc $10^{\alpha+\beta}(\varepsilon 2^{\alpha}5^{\beta})^{-1} \in \mathbb{Z}$, ce qui donne bien que $\varepsilon 2^{\alpha}5^{\beta} \in \mathbb{D}^{\times}$.
Finalement, $\mathbb{D}^{\times} = E$. □

Habillés, nous démontrons le corollaire.

Preuve.
L'ensemble des nombres décimaux inversibles est un sous-groupe multiplicatif de $\mathbb{R}$. En effet, d'après la proposition 10, si d et d' sont deux décimaux inversibles, alors il existe $(\varepsilon,\alpha,\beta) \in \{-1,1\} \times \mathbb{Z}^2$ et $(\varepsilon',\alpha',\beta') \in \{-1,1\} \times \mathbb{Z}^2$ tels que $d = \varepsilon 2^{\alpha}5^{\beta}$ et $d' = \varepsilon' 2^{\alpha'}5^{\beta'}$.
Donc $d^{-1}d' = \frac{\varepsilon'}{\varepsilon}2^{\alpha'-\alpha}5^{\beta'-\beta} \in \mathbb{D}^{\times}$ d'après la proposition 10.

De plus, d'après la remarque 10, (2,5) est log-libre.
On peut donc appliquer le théorème de l'annexe précédente.
Donc $\mathbb{D}^{\times}$ est dense ce qui prouve le théorème.

Annexe D

Application : étude d'un groupe original.

Définition 26 On appelle *Groumpf* et on note G l'ensemble :

$$G := \left\{ \frac{a^2+b^2}{c^2+d^2} \; ; \; ((a,b),(c,d)) \in (\mathbb{N}^2 - \{(0;0)\})^2 \right\}.$$

Exercice : On se propose d'étudier les propriétés de *Groumpf*.

1) Montrer que le produit de deux sommes de deux carrés est toujours une somme de deux carrés.
2) Montrer que $(G,\times)$ est un groupe abélien.
   Dans toute la suite, on notera $\mathbb{P}$ l'ensemble des nombres premiers.

   Théorème 15 (des deux carrés) Soit $n = \prod_{p\in\mathbb{P}} p^{v_p(n)}$.

   Alors

   $$\left(\exists (a,b) \in \mathbb{N}^2 \quad n = a^2+b^2\right) \iff \left(\forall p \in \mathbb{P} \quad (p \equiv 3 \pmod 4 \Rightarrow v_p(n) \in 2\mathbb{N})\right).$$

   Autrement dit, si les facteurs premiers de n de la forme $4k+3$ sont tous à une puissance paire.

3) En utilisant le théorème 15, montrer qu'on a $G \neq \mathbb{Q}_+^*$.
4) Parlons maintenant un peu d'adhérence : en utilisant le résultat de l'annexe C, montrer que $\overline{G} = \mathbb{R}_+$.

   Définition 27 On définit l'indice de Lagrange de $n \in \mathbb{N}$ et on note $\mathrm{Lag}(n)$ l'entier défini par :

   $$\mathrm{Lag}(n) = \min\{k \in \mathbb{N}, \exists (a_1,...,a_k) \in \mathbb{N}^2 \quad n = a_1^2 + ... + a_k^2\}$$

   Théorème 16 Soit $r \in \mathbb{Q}_+^*$, $r = \frac{p}{q}$.
   Alors

   $$(p,q) = 1 \Rightarrow (r \in G \iff \mathrm{Lag}(p) + \mathrm{Lag}(q) \leqslant 4)$$

5) Prouver le théorème 16.

   Proposition 11 Chaque élément de $\mathbb{Q}^*$ se décompose de façon unique comme suite presque nulle de $\mathbb{Z}$.
   Par exemple $5/9 = 2^0 + 3^{-2} + 5^1 + 7^0 + ...$ que l'on note $f(5/9) = (0,-2,1,0...)$.

   Théorème 17 On a

   $$x \in G \iff \forall k \in \mathbb{N} \quad f(x)_{4k+3} \in 2\mathbb{Z}.$$

6) En admettant la proposition 11, prouver le théorème 17. Conclure.

Solution.

Remarque 14 Nous ne prétendons pas apporter ici une solution souveraine à cette étude, et nous espérons intensément que le lecteur séduit aura pris du plaisir à construire sa propre solution.

1) Montrons que le produit de deux sommes de deux carrés est toujours une somme de deux carrés.
Soient $x = a^2 + b^2$ et $y = c^2 + d^2 \in \mathbb{N}$.
Alors on remarque que :

$$\begin{aligned}(ac + bd)^2 + (bc - ad)^2 &= (ac)^2 + (bd)^2 + 2abcd + (bc)^2 + (ad)^2 - 2abcd \\ &= (ac)^2 + (bd)^2 + (bc)^2 + (ad)^2 \\ &= (a^2 + b^2)(c^2 + d^2),\end{aligned}$$

donc

$$xy = (ac + bd)^2 + (bc - ad)^2.$$

Remarque 15 Cette preuve est constructive.

2) D'après la proposition 1.1, $\times$ est bien une loi interne pour G.
De plus, on sait que $\times$ est associative et commutative, et

$$1 = \frac{1^2 + 0^2}{1^2 + 0^2} \in G$$

est élément neutre pour $\times$.
Soit $x = \dfrac{a^2 + b^2}{c^2 + d^2} \in G$.
On pose $y = \dfrac{c^2 + d^2}{a^2 + b^2} \in G$.
Alors on a

$$xy = \frac{a^2 + b^2}{c^2 + d^2} \times \frac{c^2 + d^2}{a^2 + b^2} = \frac{1}{1} = 1.$$

Ainsi y est le symétrique de x pour la loi $\times$.
Finalement, $(G,\times)$ est bien un groupe abélien.

Remarque 16 *Groumpf* est un sous-groupe de $(\mathbb{Q}_+^*,\times)$.

3) On va montrer que $\frac{2}{3} \notin G$.
En effet, pour tout $k \in \mathbb{N}$ on a

$$v_3(2k) + 1 = v_3(3k).$$

Donc $v_3(2k)$ et $v_3(3k)$ n'ont pas la même parité.

Or 3 est congru à 3 modulo 4, donc $\frac{2}{3}$ a nécessairement un facteur premier (3 en l'occurence) congru à 3 modulo 4 à une puissance impaire, soit au numérateur, soit au dénominateur.

Donc d'après le théorème des deux carrés, soit le numérateur ne s'écrit pas comme somme de deux carrés, soit c'est le dénominateur.

Donc $\frac{2}{3} \notin G$, or $\frac{2}{3} \in \mathbb{Q}$.

Donc $G \neq \mathbb{Q}_+^*$.

4) D'après les résultats sur les décimaux inversibles établis en annexe C, on a :

$$\mathbb{D}_+^\times = \{2^\alpha 5^\beta, (\alpha,\beta) \in \mathbb{Z}^2\}.$$

Or

$$\begin{cases} 2 \not\equiv 3 \pmod 4 \\ 5 \not\equiv 3 \pmod 4 \end{cases}$$

donc d'après le théorème des deux carrés,

$$\mathbb{D}_+^\times \leqslant G.$$

Or on sait déjà que $\overline{\mathbb{D}_+^\times} = \mathbb{R}_+$.

Finalement, $\overline{G} = \mathbb{R}_+$.

5) Question immolée à la réflexion du lecteur.

6) Le théorème 17 est une conséquence directe de la proposition 11 et du théorème des deux carrés.

On en déduit que :

$$\forall (p,q) \in \mathbb{P}^2 \quad \left(\frac{p}{q} \notin G \Rightarrow \forall k \in \mathbb{Z}^* \ \frac{kp}{kq} \notin G \right).$$

Remarque 17 Ce qui conclut.

Références

[1] Olivier Fouquet. *Tour de courbes de Shimura, systèmes de Kolyvagin et théorie d'Iwasawa des formes modulaires ordinaires.* PhD thesis, Paris VI, 2007.

[2] Olivier Fouquet. Une brève introduction à la combinatoire algébrique. *Math 314*, 2014/2015.

[3] E.M. Wright G.H. Hardy. *Introduction à la Théorie des Nombres.* Vuibert, 5th edition, 2007.

[4] Michael Rosen Kenneth Ireland. *A Classical Introduction to Modern Number Theory.* Number 84 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 1990.

[5] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Number 97 in Graduate Texts in Mathematics. Springer, second edition, 1993.

[6] Frédéric Laroche. *Escapades Arithmétiques.* Ellipses, 2010.

[7] Lebreton Romain, Benoît Louise. Décomposition d'un entier en somme de carrés. *Mémoire ENS*, 2006.

[8] Josef Yusupov. *Les calculs similaires*, volume 2. Editions Flammarion, 1984.

[9] D. Zagier. A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. *The American Mathematical Monthly*, 97(2) :144, Feb 1990.