From quadratic functions to modular functions par Don Zagier

Janvier - Février 2022
M. Garnier

Deuxième commentaire à un ami, l'esprit reste le même : expliquer "linéairement" (tout en s'expliquant) une matière dense; prendre chaque point du texte sujet à interprétation et le détailler; se permettre de multiples ouvertures (conjecturales, historiques, philosophiques...) qui permettent de mieux apprécier l'ambiance du papier analysé.

Après Poincaré ([1]), l'intérêt se porte désormais sur Don Zagier ([2]), après quelques bribes de géométries voyons quelque peu des matières algébriques et arithmétiques.

Ce papier est une succession de surprises : partant de considérations élémentaires (aux démonstrations astucieuses), Don Zagier construit et rassemble des objets hautement sophistiqués (formes modulaires, arithmétique de fonction zêta, sommes de Dedekind...). Des notions qui pourraient sans doute permettre de s'approcher (une nouvelle fois) de la philosophie de la conjecture de Shimura-Taniyama-Weil selon [3].

La tâche est ardue : expliquer des choses que l'on ne comprend pas. La tâche est dangereuse : ne pas induire en erreur. Bref, on est dans la merde. Voyons ce que nous allons bien pouvoir faire...

Un dernier petit mot : plus j'écrivais plus je me rendais compte qu'il n'était peut-être pas bon que quiconque lise cela. Écrire demande du temps et de la réflexion, écrire proprement demande des choses que je n'ai pas (encore). Ce commentaire est surtout pour moi un moyen d'apprendre à faire tout et n'importe quoi (surtout n'importe quoi).

Table des matières

Avant de s'engouffrer dans l'analyse de l'article, peut-être, convient-il de dire que sa construction est magnifique ainsi qu'étonnement claire. Son fil narratif repose sur la surprise. On est tout d'abord surpris que (sous certaines hypothèses décrites par la suite) la somme de polynômes quadratiques puisse résulter en une constante ! Ensuite, lorsque l'on considère une première exponentiation (au sens strict, c'est-à-dire élevé par une puissance) de nos polynômes quadratiques (vérifiant certaines hypothèses similaires à précédemment) et que l'on en forme la somme, nous sommes encore surpris de voir résulter une constante ! On s'attendrait dès lors à ce que "toute" exponentiation de nos polynômes quadratique conduise à une valeur constante ! Que nenni... Mais ! Don Zagier réussit tout de même à trouver différents liens entre les objets qui siéent sous nos mains ; et, explique même pourquoi le processus d'exponentiation ne marche plus (une histoire de formes cuspidales et de séries de Fourier sur le groupe modulaire $\mathrm{SL}(2,\mathbb{Z})$... bref de belles rencontres imbitables à l'heure actuelle (nous verrons bien comment percer le mystère)).

En gros, on va (initialement) réfléchir sur ce type d'objet et en tirer des conséquences :

$$F_{k,D}(x) = \sum_{\substack{(a,b,c)\in\mathbb{Z}^3, a<0 \\ b^2-4ac=D}} \max\left\{0, (ax^2+bx+c)^{k-1}\right\}$$

On essaiera de pousser la chansonnette et aller sur des terres inconnues en étudiant la fonction τ de Ramanujan (définie telle qu'elle représente les coefficient de la série en q à droite) [4–6] :

$$q\prod_{n=1}^{+\infty}(1-q^n)^{24} = \sum_{n=1}^{+\infty}\tau(n)q^n$$

ou encore, des fonctions zêta :

$$\zeta_D(s) = \zeta(2s)\sum_{n=1}^{+\infty}\frac{N_D(n)}{n^s}$$

voire même des séries d'Eisenstein :

$$G_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{+\infty}\sigma_{k-1}(n)q^n$$

Ça fait plein de jolies petites formules mais toute une lourde artillerie à décortiquer. Le plus dur ne sera aucunement de voir les choses (Zagier nous ouvre la voie [1]) mais de s'approprier un vocabulaire technique. Bon... on a tout de même de la chance : l'article est très pédagogique !

N'oublions pas, enfin, que l'article de Zagier est une motivation : donc, tout détour est bon. On s'empressera ainsi d'aller fouiller dans l'état de la recherche. (Mon but sera clairement d'aller voir un max de sources.)

1. Encore que... y'a pas mal de choses laissées au lecteur. Donc article pédagogique dans ses explications certes ; mais, tout n'y est évidemment pas détaillé : c'est là notre travail.

Dans une pure optique de faciliter la compréhension de l'article de Zagier [2] je t'invite tout d'abord à y jeter un coup d'oeil ; mais, pour que tu n'aies pas constamment à jongler entre l'article et son commentaire l'entièreté du papier de Zagier figurera d'une manière plus ou moins dissimulée, plus ou moins explicite dans les pages qui vont suivre. En gros : tu auras lu le papier de Zagier sans trop t'en rendre compte. Toutefois, par soucis de minimiser les bêtises que je vais bien pouvoir dire, je t'enjoins sincèrement à aller checker l'article de Zagier après coup pour voir si ça paraît clair.

Je m'efforcerai d'être le plus clair possible (quitte à en faire peut-être un peu trop en étant légèrement lourd). Allons-y donc. [2]

1 Sommes de polynômes quadratiques

Tu sais ce qu'est un **polynôme**, ou du moins tu en as une certaine intuition (notamment due au discours rébarbatif auquel tout lycéen a droit dès l'introduction des polynômes du second degré fin seconde [3]). En revanche, sais-tu les construire (formellement) et énoncer la différence entre polynôme et fonction polynomiale [4] ? Admettons que oui, mais rappelons tout de même les bases.

1.1 Bases (théoriques) d'arithmétique sur les polynômes

A priori tu devrais savoir tout ce que je vais dire [5], donc mon seul but va être de te surprendre et de poser deux trois résultats (soit d'intérêt pour la suite soit de pur intérêt intellectuel).

Nul doute qu'un **polynôme** peut se représenter de la manière suivante :

$$\sum_{k=0}^{n} a_k X^k \tag{1.1}$$

2. Les toutes premières sous-sections de la section ci-dessus : *Sommes de polynômes quadratiques* ne seront pas vraiment intéressantes en elles-mêmes dans la mesure où elles commentent strictement la démarche de Zagier (enfin, on essaie tout de même de motiver quelque peu sa démarche et faire quelques ouvertures). C'est ensuite, que des explications en bonnes et dues formes feront leur apparition, tout particulièrement à partir de la sous-section *Généralisations à d'autres discriminants et valeurs spéciales de séries L*. Il s'agira de démontrer proprement des arguments de base pour un chercheur mais nouveaux pour nous.

3. Même si on avait vu plein d'exemple de polynômes et que des pans entiers de notre cours parlaient de polynômes, ce n'est qu'en fin d'année que le mot est apparue dans un cours en demi-classe. La professeure était toute contente de nous dire : "vous verrez, l'année prochaine vous allez vous servir de polynômes". Enfin... c'est quand même une aberration de voir que l'on a quelque chose sous les yeux mais qu'il faille attendre (au moins) une année pour que le mot soit enfin lâché... À toute poids toute mesure, bien évidemment, Peter Schölze concocte le même raisonnement avec un cas particulier de quotient d'ensembles profinis vis-à-vis de son *Liquid tensor experiment*.

4. On pourrait résumer cette différence à du verbiage (mais qui a son importance).

5. En 2015 - 2016 (peut-être que tu as eu le même cours quelques années plus tard ?), J. Royer (L1. Parcours Spécial) avait une section de son cours dénommée *Quand les polynômes deviennent un objet compliqué, mais en fait pas tant que ça...* En fait, ça peut devenir très très compliqué en définissant une application polynomiale comme la capacité qu'à son "extension linéaire" à se "factoriser par sa projection". Cette définition est très énigmatique.

mais qui sont les a_k (les **coefficients**) ? Qui est le X (l'**indéterminée**[6]) ? Dans quoi tout cela vit ? Bon dieu de merde, "ça fait beaucoup là"[7].[8]

Mêlons un peu les réponses que nous allons apporter afin de voir l'interconnexion entre ces trois objets que l'on va manipuler. Que sont les coefficients a_k ? Ce sont les éléments attachés à une indéterminée d'un certain degré et vivant dans un espace suffisamment "stable" pour qu'une arithmétique puisse naître. Mais, au juste, qu'est-ce qu'une **arithmétique** ? Naïvement, peut-être, les règles fondamentales de la gestion et la transformation de quantités primordiales. En gros : c'est de la cuisine avec des éléments (insécables). Habituellement (dans les petites classes), cette cuisine se résume en quelques notions (j'en veux pour exemple quelques cours de MPSI de Louis-Le-Grand ou encore du Lycée Montaigne) : nombres et opérations (usuelles, division euclidienne, pgcd, ppcm, parité, irréductibilité, décomposition) voire même quelques constructions (idéaux). Le plus beau est que chacun de ses éléments se retrouve lié et propose, en son ensemble, un cadre de réflexion proprement problématique : beaucoup (énormément) de questions se posent : valeurs spéciales (par exemple : les racines), représentations géométriques, transformations (plus ou moins) algébriques...

Comment synthétiser tout cela ? Usuellement, on va se prendre un "ensemble" $\mathbb{K}$ duquel vont émaner nos coefficients. Ensuite : schéma classique, c'est-à-dire qu'une construction algébrique intervient et entérine et fixe le tout. On a donc un cadre stable. En particulier, on construit un **anneau commutatif sur** $\mathbb{K}$ et on va se donner un entier positif n représentant le **degré** de notre polynôme (on va voir que le degré peut se définir comme l'entier maximal pour lequel tous les a_k, avec $k > n$, sont nuls).

En admettant la notion de suite, un coefficient n'est rien d'autre qu'un élément d'une suite[9] à valeur dans l'anneau $\mathbb{K}$. Suite à ça, par linéarité de l'opération somme, une somme de polynôme ne se résume qu'à de simples considérations sur les coefficients (en faisant attention à ce que le degré de l'indéterminée d'un coefficient soit identique à celui d'un autre pour que la somme s'opère). Pas plus de problèmes que ça pour la multiplication, tout roule. Ensuite, c'est ce que l'on disait : on fait toute la cuisine et on a finalement sous les yeux un truc relativement opérant (on pourrait même procéder "similairement" à la définition de polynômes à plusieurs indéterminées). Une chose néanmoins plus subtile est la division de polynômes ; et là ça fait mal. Il faut ruser[10] pour construire proprement

6. Pour quelques réflexions sur la notion de variable (ce que ne serait pas X) on pourra aller voir Godement ou encore le cours de *Logique catégorique* d'Alain Prouté (p. 31). (J'essaie de me le faire petit à petit.)

7. Je réfléchis, et... si je vais autant dans le détail (et encore... j'esquive beaucoup de choses), à moins de travailler à plein temps pendant deux mois jamais je n'aurai fini gné. Une autre chose : à chaque fois qu'il va dire des choses type "il est évident que" gné... va falloir que je m'emploie à le démontrer.

8. Et d'ailleurs, si on veut pousser les questions, on peut sans doute se demander pourquoi est-ce que l'on somme ? Peut-être car c'est la chose la plus naturelle (et qu'une grande partie de problèmes "primitifs" demandaient l'accès à des structures qui s'en-codent dans une telle somme) ?

9. Les suites ayant un nombre "infini" de termes (puisque de domaine de définition $\mathbb{N}$), lorsque l'on parlera de **séries**, on se rendra compte que la proposition de définition de polynôme n'est qu'un cas particulier de celle de série.

10. Voir [7], p. 19 et suivantes par exemple.

le **corps des fractions rationnelles** : construire une relation d'équivalence et faire un passage au quotient [11]. On va assimiler deux jeux de polynômes (P_1, Q_1) et (P_2, Q_2) si la relation (d'équivalence) suivante $P_1Q_2 = P_2Q_1$ est vérifiée. En faisant bien attention à ne pas multiplier des choses par zéro (c'est-à-dire si on renverse le processus : ne pas diviser par zéro) on construit l'ensemble quotient lié à la relation d'équivalence ci-dessus. Grâce aux classes d'équivalence on a pleinement caractérisé la notion de division sur / dans $\mathbb{K}(X)$. Mieux encore ! grâce l'ensemble des classes d'équivalence réalise une partition des polynômes. Donc, nous ne perdons pas d'information. Nickel. Au contraire, on a structuré le tout. En revanche, tout cela n'est que théorique et la mise en pratique de tels principes est loin d'être aussi simple (voire même scabreuse...). Mais le plus important ici est que l'on sache que les choses existent décemment.

Mais, qu'est-ce qui existe ? Des **polynômes** bien entendu. Cela dit, les choses ne s'arrêtent pas ici. On va pouvoir également prendre en considération la notion de **fonction polynomiale**. Un exemple va nous permettre de voir la différence (avant de tenter de la saisir) : considérons le polynôme $F_p(X) = X^p - X$ dans $\mathbb{F}_p$ alors le polynôme F_p n'est pas nul alors que sa fonction polynomiale l'est (en effet, par exemple : si $p = 2$ alors $0^2 - 0 = 1^2 - 1 = 0$). Une fonction polynomiale résulte de l'évaluation du polynôme pour tous les éléments de son domaine de définition. [12]

1.2 Présentation du problème initial de Don Zagier (discriminant 5)

Typiquement, dès les premières lignes, Don Zagier se sert de la distinction entre polynômes et fonctions polynomiales [13] (sans douter par déformation professionnelle). (Cette remarque, en relation avec ce qui vient d'être dit ci-dessus, sera sans doute utile à l'avenir ; ici, elle peut très bien s'oublier.)

On va se fixer un nombre entier D, disons 5 (le choix n'est anodin qu'en l'apparence, attendons un peu avant de voir pourquoi est-ce là intéressant). Nous allons raisonner sur les polynômes du second degré $Q(X) = aX^2 + bX + c$, où a, b et c sont tous les trois des entiers relatifs. Jusque là, ça pourrait faire problème niveau lycée ; rien de nouveau sous les tropiques. Admettons que l'on veuille s'amuser à attribuer une valeur (souvent le début de

11. Je pense avoir un problème monstre avec le passage au quotient, néanmoins, un passage de chez Godement m'a pas mal aidé à commencer à saisir le truc :

> Notons [...] que la méthode de construction de E/R, qui pourra sembler étrange au débutant, s'utilise cependant dans la vie de tous les jours, comme le montre l'exemple (non mathématique !) que voici : on prend pour E la collection des hommes, et pour R la relation «x et y sont compatriotes» ; on obtient ainsi évidemment une relation d'équivalence sur E. Pour un $x \in E$, la classe F_x est l'ensemble de tous les compatriotes de x ; autrement dit c'est la nation à laquelle x appartient ; par suite, l'ensemble quotient E/R est ici la collection des diverses nations existantes, et l'application canonique de E sur E/R consiste à associer à chaque homme la nation à laquelle il appartient...

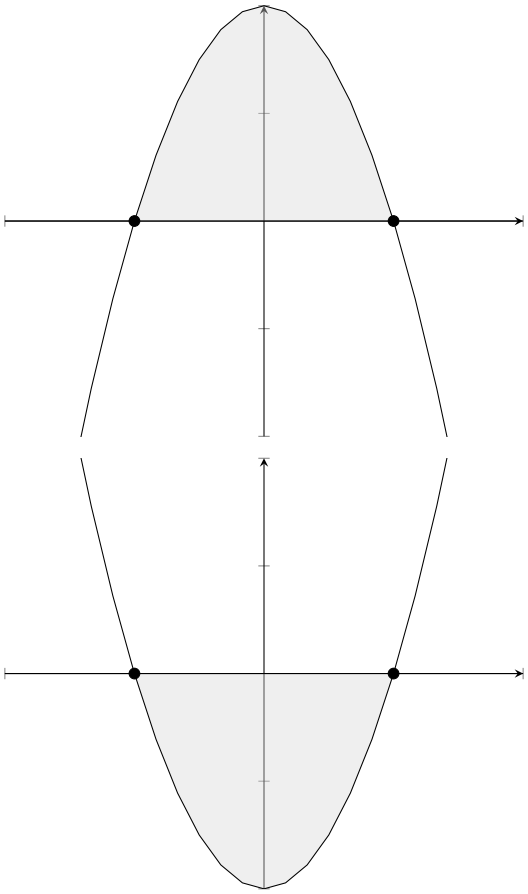
12. Si le corps n'est pas de dimension finie, alors no pb on va pouvoir tout mélanger mais si au contraire la dimension est finie : la notion de polynôme et celle de fonctions polynomiales ne sont plus équivalentes (comme le montre l'exemple dans $\mathbb{F}_p$ par ailleurs).

13. Enfin à peut-être un petit détail que l'on omet tout de suite.

beaucoup de problèmes...) à la somme suivante :

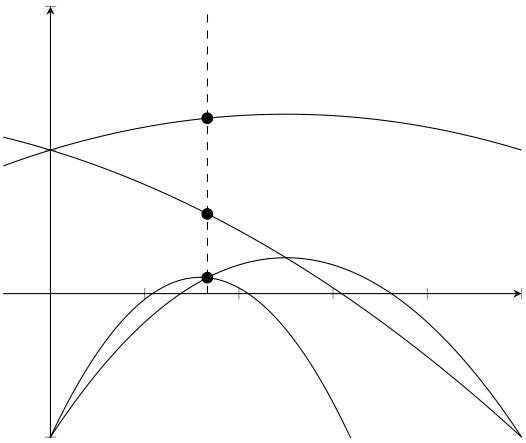
$$A(x) = \sum_{\Delta} Q(x) \tag{1.2}$$

où Δ représente les conditions que l'on va se poser pour que la somme soit digne d'intérêt (et ne diverge pas grossièrement et salement). On est loin des réelles motivations de Zagier en se posant des questions ainsi (les histoires de formes modulaires ne sont pas pour tout de suite...). Le but va être de fictivement donner des raisons d'intérêt à cette somme (bien évidemment, chaque étape est orientée par l'article). Par convenance, disons que l'on veuille un résultat fini (et positif). Une étude géométrique de la représentation d'un polynôme permet de voir qu'en fonction du signe de a la courbe représentative (une parabole) sera orientée vers le bas ($a < 0$) ou vers le haut ($a > 0$). De plus, en fonction du discriminant ($b^2 - 4ac$), et donc par définition de la multiplicité des racines (et du fait qu'elles soient dans $\mathbb{R}$ ou $\mathbb{C}$), on va venir "encadrer" une certaine zone.



Au regard de nos attentes, c'est évidemment la première figure qui nous intéresse (positivité de $ax^2 + bx + c$ bien gré mal gré la négativité de a et discriminant positif (5 par exemple héhé) ainsi que finitude de la somme). En l'espèce, il est impossible de saisir en quoi ces considérations vont nous intéresser tout particulièrement. Il faudrait rajouter une idée dans le calcul de $A(x)$: on veut trouver toutes les fonctions quadratiques qui respectent

un jeu de relation (celui au dessus) et on sommera ensemble toutes ses fonctions. Ainsi notre problème devient une histoire d'intersection entre une droite $x = p$ et la fonction polynomiale évaluée en p. Voyons graphiquement comment, et l'on va détailler ensuite plus précisément pourquoi.



Sur le graphique ci-dessus sont représentées quatre fonctions polynomiales toutes évaluées en une certaine valeur (la même). Lorsque nous sommerons les résultats obtenus, nous aurons le droit à notre **première surprise** mais c'est encore un peu tôt pour apporter un quelconque élément de réponse (étant donné que l'on est encore en train de former la question). Visuellement, on "somme des points" (sur une courbe) sélectionnés par le résultat d'une section verticale. L'avantage de cette formulation est que, tout de suite, on peut penser à une généralisation (attendons un peu). En revanche, son problème est qu'elle fait disparaître toute la profondeur du problème pour ne considérer que le résultat que l'on souhaite. En effet, cette formulation ne permet pas d'entrevoir la problématique de sélection des fonctions polynomiales idoines. D'un côté on fête un problème purement géométrique, de l'autre on est bien embêté parce que l'on a perdu la saveur algébrique. De fait, forçons un énoncé géométrique plus général avant de chercher une traduction algébrique.

Essentiellement, soient n courbes (algébriques) et soit une droite. On considère l'ensemble des points appartenant au résultat de la section entre la droite et les n courbes. On pourrait peut-être remplacer la notion de courbe algébrique (classique) par une variété algébrique et la droite par une autre variété algébrique. En attendant et en gros on chercherait, d'abord, l'ensemble des points à la fois sur une des n courbes et sur la droite. Ensuite, il serait question d'effectuer la somme d'une certaine caractéristique de ces points (dans le cas du problème de don Zagier c'est "simplement" l'ordonnée). Tout de suite on pense à quoi ? Au **théorème de Bézout** [14] pour une constatation sur l'ordre de grandeur du nombre de points d'intersection entre deux courbes algébriques de degré fixé (le tout considéré dans le plan projectif). Et encore, nous n'aurions même pas l'ordre de grandeur mais plutôt une borne supérieure dans la mesure où, sur le lot total de point que l'on est en droit d'attendre, tous ne vérifient pas nécessairement certaines conditions (positivité, négativité, une condition équivalente au discriminant et peut-être d'autres ?). Bref, si on pousse le truc, on serait

14. Pas le truc que l'on apprend en Terminale spé Maths avec le pgcd.

en train de faire de la **géométrie algébrique** (*intersection theory*). Notons peut-être que l'on se ramène (plus simple de constater que de résoudre quoi que ce soit) à tout un ensemble de problématiques sur les courbes elliptiques (en tant que cas très très particulier). Bref, une bonne grosse question qui mériterait sans doute bien plus de précision (mais en l'état actuel de mes connaissances, oublions vite vite vite avant de démontrer magistralement mais surtout faussement quoique ce soit ; espérons tout de même y revenir un jour). Ce serait quand même beau de réussir à trouver des liens entre toutes ces choses. Bref, revenons à nos choux.

Si l'on se sert de tout ce dont on a parlé précédemment, modulo un peu de sucre syntaxique, on peut enfin donner une expression à Δ. De fait :

$$A(x) = \sum_{\Delta} Q(x) = \sum_{\substack{(a,b,c)\in\mathbb{Z}^3, a<0 \\ b^2-4ac=5}} \max\left\{0, ax^2+bx+c\right\} \tag{1.3}$$

Enfin ![15]

Le terme de «*surprise*» a déjà été utilisé trois fois mais toujours rien de vraiment étonnant (au sens de contre intuitif peut-être).

Première surprise. La fonction $A(x)$ est constante et vaut 2. La démonstration sera vue dans la deuxième section (*Démonstrations, raffinements et compléments* ; il faudra également s'attarder sur diverses questions telle la convergence d'une telle somme). Pour le moment nous allons plutôt essayer de nous convaincre que cela est vrai ainsi qu'investiguer divers moyens de mieux cerner le problème (c'est-à-dire essentiellement la fonction $A(x)$).

1.3 Balade algorithmique : se convaincre de la véracité

Afin d'alléger et de simplifier la suite des discussions, posons par convention que $Q(X) := [a,b,c] := aX^2+bX+C$. Ainsi par exemple $8X^2-2X+1$ se résume en $[8,-2,1]$.

Don Zagier fournit un stock de polynômes vérifiant les conditions adéquates. Nous verrons dans la prochaine sous-section comment les retrouver nous même. Pour l'instant, il est seulement le temps de se convaincre que le résultat pourrait effectivement être vrai. Quatre valeurs de x vont être investiguées : 0, 1/2, 1/3 et $1/\pi$. On résume dans le tableau suivant les résultats obtenus par Zagier.

15. Pour indication, nous venons de faire les sept premières lignes de l'article ainsi que deux trois choses à droite à gauche ; je suppose que c'est surtout au début que je vais prendre beaucoup de temps, ensuite, certes ce sera long, mais ça devra avancer nettement plus (espérons le sinon ce ne sera jamais fini).

Q vérifiant Δ	$Q(0)$	$Q(1/2)$	$Q(1/3)$	$Q(1/\pi)$
$[-1,1,1]$	1	5/4	11/9	1.21699
$[-1,-1,1]$	1	1/4	5/9	0.58037
$[-5,5,-1]$		1/4	1/9	0.08494
$[-11,7,-1]$			1/9	0.11364
$[-1,3,-1]$		1/4		
$[-409,259,-41]$				0.00190
$[-541,345,-55]$				0.00215
$[-117731,74951,-11929]$				0.00001
$[-133351,84893,-13511]$				0.00001
[...]				...
Somme	2	2	2	~ 2

Convaincant n'est-ce pas ? C'est c'la oui...

En tout cas ça donne envie d'y croire. Mais tout ça c'est bien gentil mais c'est du pur recopiage de l'article de Zagier là. Va falloir mettre les mains dans le cambouis.

1.4 Balade algorithmique : programmons un peu

Tout d'abord il faut que l'on sache exactement ce que l'on veut. On veut des polynômes : ceux vérifiant les conditions Δ.

On risque de se poser quelques questions :

- est-il possible de quantifier le nombre de Q vérifiant Δ ?
- peut-on trouver un algorithme suffisamment performant [16] nous renvoyant l'ensemble des Q satisfaisant Δ ?
- existe-t'il une construction "géométrique" des Q vérifiant Δ ?
- existe-t'il des liens "algébriques" entre différents Q pour un même réel x donné [17] ?
- comment s'interprète (dans notre contexte) algébriquement l'évaluation de Q en des valeurs rationnelles (ou pas) ?
- ...

1.4.1 Préparer le terrain

Dans le cas rationnel (aussi bien que dans le cas irrationnel, mais sous certaines limites), toute la problématique repose sur la manière d'exprimer le **discriminant** de Q. Naïvement, pour un polynôme du second degré, on se retrouve avec notre traditionnel $D = b^2 - 4ac$. Il y a juste un petit problème : les seules informations dont nous disposons (directement pour mieux cerner le discriminant) portent sur a. Et encore... elles sont bien maigres : a est négatif. Donc tout au mieux peut-on ré-écrire le discriminant sous la forme $D = b^2 + 4|a|c$.

16. Sous-entendu pas du bruteforce.

17. Apparemment, dans certains cas, il serait au moins possible de former une relation de récurrence entre polynômes en utilisant un élément de $\mathrm{SL}(2,\mathbb{Z})$, ça fait charabia pour l'instant mais il va falloir clairement démontrer ça par la suite. Va falloir se creuser les méninges étant donné que, dans les environs d'une telle question, Zagier n'a pas réussi à conclure à quelque chose de totalement fonctionnel.

Ça ne nous avance que guère... En revanche, si nous disposions d'une formule où, d'une manière ou d'une autre, plus d'information apparaissait : ce serait un miracle. En d'autres termes, on va chercher à exprimer D comme une fonction dépendant à la fois de x et $Q(x)$ ainsi que des coefficients a, b et c.

Essayons de raisonner par élimination pour mieux cerner nos attentes [18]. Si $Q(x)$ apparaît dans le bins, étant de degré deux et étant donné que D ne dépend pas de x, on s'attend à ce qu'une soustraction vienne faire disparaître les x (de degré un et de degré deux). (Restons, par simplicité, dans le cadre où $Q(x)$ n'est aucunement élevé à une puissance quelconque.) Si l'on soustrait bêtement quelque chose du style $Q(x)$ avec $\mu x^2+\nu x+\kappa$, ça ne nous avance guère, les indéterminées n'ont aucunement disparu (et une identification coefficient par coefficient ne nous aide pas (à moins de poser $\kappa = b^2 - 4ac - c$ et $\mu = a$ et $\nu = b$, mais peut d'intérêt là)). Donc il va falloir ruser. Essayons de forcer quelque chose à apparaître dans $Q(x)$. Si on le multipliait par quatre, alors on aurait à la fois un $4a$ et un $4c$ qui apparaîtraient. Ça semble un pas trop mauvais compromis. De l'autre côté, que pourrions nous soustraire à $Q(x)$? Un truc de degré deux, assurément. Mais pouvons en dire plus encore ? Nous voulons obtenir une relation non "triviale" (entre tous les coefficients lorsque l'on forme la différence). Mieux, peut-être que l'on ne voudrait pas toucher au coefficient associé à l'indéterminée de degré 0 sauf si c'est pour faire apparaître une quantité manquante (comme un b^2 par exemple...) ! (À vrai dire, on a déjà un $4C$ qui a été formé, il ne manquerait plus que de multiplier par a pour obtenir ce que l'on veut, tiens tiens tiens.) En fin de compte, si l'on synthétise tout : peut-être que multiplier $Q(x)$ par $4a$ peut être plus intéressant afin de faire apparaître une partie du discriminant. Ensuite, tout va se jouer sur le polynôme que nous allons soustraire, et c'est très simple : on a un $4a^2x^2$ qui nous dérange (ainsi qu'un $4abx$), bah voilà, nous avons fini. On a trouvé ce que nous voulions : une réécriture du discriminant en fonction de x, $Q(x)$, a, b, c.

En somme : $4aQ(x) - (4a^2x^2 - 4abx + b^2) = 4ac - b^2$. Reste plus qu'à multiplier par moins un pour finalement obtenir que :

$$D = b^2 - 4ac = (4a^2x^2 - 4abx + b^2) - 4aQ(x) = (2ax - b)^2 - 4aQ(x) \tag{1.4}$$

Toutefois, l'on peut sans doute se poser la question si on tel raisonnement se généralise pour un polynôme de degré trois par exemple [19] ? Bahh... (en suivant la recette de cuisine décrite juste au dessus...) On trouve quelque chose de pas forcément très réjouissant (et pas exactement ce que l'on voulait) :

$$D_3 = (-4b^3 + 18abc - 27a^2d)Q(x) - \Big[a(-4b^3 + 18abc - 27a^2d)x^3 + b(-4b^3 + 18abc - 27a^2d)x^2 + c(-4b^3 + 18abc - 27a^2d)x + 4a^3 - b^2c^2\Big]$$

$$D_3 = b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2 \tag{1.5}$$

18. Si la suite est autant décrite pour un aussi petit calcul, c'est pour une raison bien précise : avoir une idée de la logique pour généraliser la chose par la suite.

19. Question n'apparaissant pas chez Zagier.

Il semble acceptable de dire que des généralisations pourraient être opérées, mais tout d'abord où en serait le sens, et ensuite, en pratique, les difficultés semblent s'élever terriblement à mesure que le degré augmente [20]. Revenons à nos histoires !

Il va convenir de distinguer deux cas : l'un où x est **rationnel** et l'autre où x est **irrationnel**. Dans un cas la somme $A(x)$ sera très agréable car finie et dans l'autre (en devant prouver que la somme converge) il y a un nombre non fini de termes (i.e. de polynômes satisfaisant Δ). Comment cela se justifie ? Soit par construction (et il va falloir attendre la section § 10 de l'article de Zagier [21] et l'utilisation de **fraction continue** (qui est vraiment le cadre classique pour réfléchir)), soit peut-on sans doute en donner au moins une intuition. Dans un cas ou dans l'autre, les mêmes conditions se posent (c'est-à-dire respect des conditions Δ). En revanche, la caractéristique même de x (rationalité ou irrationalité) va discriminer sur le choix probable de Q adéquats. Voyons pourquoi.

On rappelle que $5 = (2ax - b)^2 - 4aQ(x)$.

Cas x rationnel Présentement, dans un tel cas, x peut se représenter par p/q (avec $\text{pgcd}(p, q) = 1$ et $(p, q) \in \mathbb{Z} \times \{\mathbb{N} \setminus \{0\}\}$). En injectant dans la quantité D que $x = p/q$, on trouve évidemment [22] :

$$5q^2 = |2ap - bq|^2 + 4|a||ap^2 + bpq + cq^2| \tag{1.6}$$

Dans le cas particulier où $x = 0$, on peut même simplifier les choses et voir que $5 = b^2 + 4|a||c|$. Dès lors, ainsi que dans le cadre rationnel, ce n'est plus qu'une **question combinatoire** [23]. Mais illustrons cela sur l'exemple où $x = 0$. Ni a, ni c ne peuvent être strictement supérieurs à 1, autrement (par positivité de la fonction carrée), le membre de droite excéderait le membre de gauche et l'égalité serait impossible à réaliser. Donc, en toute généralité, a et c ne peuvent chacun prendre que trois valeurs possibles : -1, 0 et 1. Or, par définition $a < 0$ et par positivité de $a \cdot 0^2 + b \cdot 0 + c = c$, l'on trouve très aisément les valeurs que peuvent prendre a et c (à savoir $a = -1$ et $b = 1$). Désormais, la seule marge de variation réside dans b. Un examen similaire montre qu'il ne peut prendre que les valeurs -1 et 1. En s'appliquant un peu plus, on aurait pu montrer que le nombre total de polynômes vérifiant Δ est fini. Toutefois, ça semble être une trivialité que nous énonce notre intuition, donc nous sommes allés un peu vite en besogne.

Cas x irrationnel Ça se complique rudement plus. En théorie, ce sont les mêmes logiques qu'il faut appliquer. En pratique, les choses deviennent bien plus subtiles. Pourquoi est-ce

20. Et, un tel discours (de complexification du paysage), ne porte que sur les discriminants de polynômes... La notion est plus riche qu'il n'y paraît. À cet effet, on verra par exemple [8].

21. On risque très certainement de ne pas respecter l'ordre intrinsèque du papier de Zagier en traitant sous peu le cas irrationnel.

22. Modulo un signe moins qui ne pose aucun problème (dû aux valeurs absolues), on trouve exactement le même résultat que Zagier.

23. C'est évident dans l'article de Zagier que c'est une question combinatoire, toutefois cela n'est pas vraiment dit. Tout son intérêt ne se pose pas sur de si petites questions. La question mériterait sans doute d'être investiguée sous un point de vue combinatoire. D'un tout autre point de vue, ne serait-il pas possible de déduire les Q idoines par une construction plus "géométrique" ?

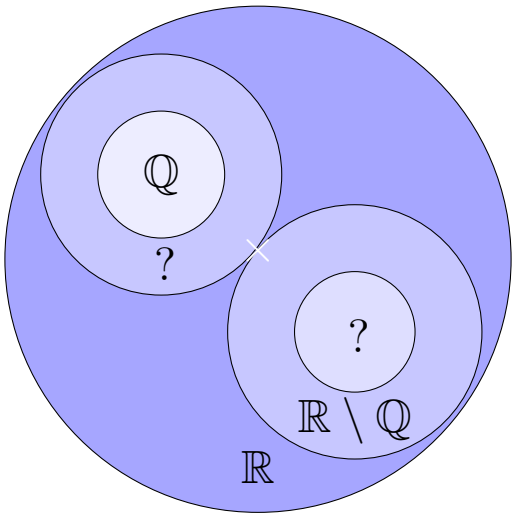
que, d'un coup, l'on aurait une infinité de polynômes vérifiant Δ possibles ? En somme, pourquoi Zagier pose-t'il le corollaire suivant ?

Corollaire. Soit x un nombre réel ni rationnel ni quadratique sur $\mathbb{Q}$. Alors il existe une infinité de polynômes $Q(X) = aX^2 + bX + c$ de discriminant 5 avec $a < 0$ et $Q(x) > 0$.

Ça paraît très anodin mais de **profondes dynamiques** se cachent sous une telle assertion. Intuitivement [24], on est en droit de s'attendre à ce que la quantité $D = |2ax - b|^2 + 4|a||Q(x)|$ soit désormais "plus riche" que dans le simple cas rationnel [25, 26].

Afin de mettre des mots plus précis sur ces histoires de "richesse", de nombre irrationnels... nous allons faire un "léger" détour par diverses théories (cf. [9–16]).

Comme toujours, lorsque l'on découvre des choses, on aimerait bien 1) le définir proprement en lui attribuant un cadre d'étude, 2) être capable de l'utiliser et 3) s'en souvenir ainsi que d'avoir un cadre d'étude bien ordonné, rangé... Habituellement, en appliquant de tels questionnements aux ensembles de nombres (et plus particulièrement aux rationnels et irrationnels), il va convenir d'avoir une idée assez précise de leur nature, chercher leurs domaines de prédilections, avoir quelques idées de la *technicité* de tels objets et puis que tout soit bien classifié. Lorsque l'on s'attache à cette dernière opération, généralement, on se retrouve avec un graphique tel que le suivant :



Ainsi, après s'être fait une idée assez clair des concepts en jeu, nous allons quelque peu sortir des gongs de l'article de Zagier pour découvrir ce que pourraient être ces points d'interro-

24. En fait, non, en y réfléchissant, pas du tout. Je retire. Ça ne m'apparaît pas du tout intuitif donc il va falloir d'autant mieux justifier cela.

25. Étonnamment, lorsque l'on s'intéresse au cas irrationnel, la richesse de la structure de D se traduit directement par une information sur les coefficients (et plus précisément sur a comme on le verra dans la sous sous section suivante). (Formulation relativement équivalente au corollaire précédent.)

26. On exclut également le cas quadratique car autrement (si je n'ai pas une mauvaise définition des choses) : $\pm\sqrt{5} = 2ax - b$, auquel cas l'on retrouve effectivement que $x = \frac{-b\mp\sqrt{5}}{2a}$. Dans le cas où x n'est pas un entier quadratique, une telle équation ne peut ainsi jamais être vraie et donc posséder un nombre fini de polynôme Q vérifiant Δ ; on va alors devoir trouver une suite (infinie) de polynômes "approximant" ou plutôt "comblant" l'obstruction à être solution d'une telle équation.

gation : c'est tout de même étonnant de pouvoir penser qu'il y ait des choses "au-dessus" des rationnels ou "en-dessous" des irrationnels (bonjour chers **algébriques** et **transcendantaux**). Restera sans doute une petite question : que se passe-t'il au point de contact (s'il y a effectivement contact) entre cet "au-dessus" et cet "en-dessous" ? [27]

Ce serait trop simple si je balançais simplement les définitions (que tu connais pourtant) des quelques concepts fondamentaux qui vont nous intéresser... d'un autre côté, ce serait bien trop long si tout était passé au peigne fin. Donc, prenons un peu de hauteur afin d'éviter quelques "pathologies" et particularités qui nous obligeraient à d'amples développements alors que toute la saveur de la question en est bien loin.

Parlons d'un domaine que nous comprenons conjecturalement très bien [28], un domaine gorgé de théorie des nombres, d'algèbre de haute volée ainsi que de "calcul analytique" bien rebutant (ou passionnant, au choix). Réfléchissons un peu aux manières de *produire des nombres*. En acceptant **Peano et son axiomatique** (et sans entrer dans toute une ribambelle de conflits de logique pure), on est bien content de voir que les entiers se retrouvent à nos bras ; pour peu on passe aux entiers relatifs puis aux nombres rationnels. Aucun problème, tout roule. Ensuite, classiquement, on **complète** [29] le corps $\mathbb{Q}$ pour se retrouver avec $\mathbb{R}$. Voilà une première manière de "produire des nombres", simplement en les construisant (ou plutôt construire le concept associé). Il existe néanmoins diverses manières de "cibler" précisément la construction de certains nombres. Les notions de **lieu géométrique**, de **construction à la règle et au compas**, de **solutions d'une certaine équation**, de **résultat d'un processus mécanique**... Si l'on combine un peu toutes ces choses : patatras ! Le miracle se produit et on a un objet digne d'intérêt. Sans encore le mentionner, voyons-en quelques traces.

Intégrer peut surprendre ; par exemple, on voit évidemment la complémentarité avec l'opérateur de dérivation mais pour l'un aucune obstruction (tant que c'est dérivable on peut tout dériver, c'est-à-dire qu'il existe des relations et des recettes de cuisine adéquates)

27. Pour l'instant, je suis relativement déçu de ce que j'ai produit. Il n'y a rien de "virevoltant"... Je vais essayer de me rattraper en espérant que ça ne parte pas dans tous les sens.

28. L'expression semble être de Clément Dupont, dans un séminaire au laboratoire de Mathématiques de Polytechnique. J'avoue avoir bien rigolé en attendant cette expression.

29. De la même manière que l'opération de **compactification** se généralise, on peut donner un point de vue plus général sur la notion de **complétion** (en faisant un bon petit passage au quotient je suppose). Sauf que, sauf que... héhé oui et non tout roule. $\mathbb{R}$ n'est pas la seule complétion possible de $\mathbb{Q}$. (Enfin si on réfléchit de manière intuitive, on aurait tendance à se dire que "combler les trous entre les rationnels" ne peut se faire que d'une seule façon ! en ayant recours aux irrationnels bon dieu !) (C'est ce genre de pathologies que je voulais un peu éviter ; c'est intéressant mais je ne le développe pas assez pour que ça puisse vraiment servir, je t'invite donc à faire des recherches.) Néanmoins, faut pas oublier que la complétion dépend de la norme ! Et c'est le **théorème d'Ostrowski** qui nous dit tout (et un peu Pierre Colmez aussi héhé). On va pouvoir construire une infinité de complété de $\mathbb{Q}$ avec la norme p-adique. Ainsi, à chaque nombre premier p on va associer un complété de $\mathbb{Q}$. Et c'est peut-être en ce sens que l'on peut dire qu'à chaque nombre premier correspond une géométrie (je n'ai jamais compris cette phrase de Récoltes et semailles) ?

en revanche on peut rapidement se retrouver bloqué quand on intègre[30]. Bref, intégrer / mesurer une longueur, une aire, un volume... semble être un outil suffisamment riche pour espérer catégoriser différents nombres. Sans aucun soucis on peut construire plein de nombres divers et variés : $\pi = \int_{-\infty}^{+\infty} \frac{1}{1+x^2}\mathrm{d}x$, $\ln(t) = \int_1^t \frac{1}{x}\mathrm{d}x$... Bref on n'est pas en manque. Toutefois, ce serait sans doute tricher que se permettre toutes les constructions possibles avec des intégrales. Alors, nous allons appliquer le *sacro credo* : les polynômes c'est naturel donc restreignons nous à quelque chose de naturel, c'est-à-dire les polynômes. Plus précisément, au bout de la chaîne historique[31], nous allons porter notre attention sur les **périodes**.

Kontsevich et Zagier [17] (et bah tiens, qui voilà !) définissent une période comme un nombre complexe dont la partie réelle et imaginaire sont le résultat d'intégrales absolument convergentes de fonctions rationnelles à coefficients rationnels sur des domaines de $\mathbb{R}^n$ donnés par des inégalités polynomiales à coefficients rationnels. Ça fait un peu lourd, mais on va petit à petit s'y faire (et franchement on se restreint au cas réel). Un exemple de période :

$$\iiint_{0<x<y<z<1} \frac{\mathrm{d}x\mathrm{d}y\mathrm{d}z}{(1-x)yz} \tag{1.7}$$

Putain mais en quoi ça va nous aider avec nos histoires de nombres rationnels et irrationnels ? Nous venons tout juste de prendre un peu de hauteur, désormais tirons-en les conséquences. La philosophie est que :

> *many, if not almost all proofs of irrationality and transcendence results use periods and their associated differential equations in one form or another.*

Wooow mais c'est quoi cette histoire ? Il y a des équations différentielles dans le lot maintenant ? On perd le fil de nos petits $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$.

Remettons les pieds sur Terre et posons nous des questions simples : est-ce que tous les nombres sont des périodes ? Bon ce n'est pas une question simple et la réponse est encore plus compliquée (aussi bien théoriquement qu'en pratique). En un sens, la réponse est oui : il existe une manière "d'élargir" le cadre conceptuel des périodes à un nouveau nombre qui n'était en fait pas une période donc un nombre peut ne pas être une période. En fait, c'est très conjectural, mais il est suspecté que que des nombres comme e ou encore la constante d'Euler-Mascheroni ne soient pas des périodes au sens classique de Kontsevich Zagier. (Donc si ça n'en sont pas, on ne va tout de même pas les laisser toutes seules ces périodes ! D'où le développement de la notion de **périodes exponentielles** etc...)

Toutefois, si l'on se restreint au sens classique des périodes (ce que nous ferons par la suite), il semble conjecturalement se produire des choses étonnantes : e et π sont tous les deux irrationnels et même transcendentaux mais l'un ne serait pas une période alors que

30. Un exemple fameux peut être le calcul d'un arc d'**ellipse** : $\int_0^t \frac{\sqrt{1-e^2x^2}}{\sqrt{1-x^2}}\mathrm{d}x$, et plus généralement beaucoup d'**intégrales elliptiques** (c'est-à-dire de la forme $\int_0^t R(x, \sqrt{P(x)})\mathrm{d}x$ avec R une fraction rationnelle et P un certain polynôme).

31. Peut-être après quelque chose comme les intégrales fractions rationnelles puis intégrales elliptiques puis intégrales abéliennes...

l'autre si. Tiens, donc les périodes *permettraient* de discriminer les nombres transcendentaux (entre eux et peut-être même avec d'autres classes de nombres) ? Plus généralement, ne faudrait-il pas *chaque fois que nous rencontrons un nouveau nombre et que nous voulons savoir s'il est transcendant, commencer par essayer de savoir si c'est une période* ? Si l'on raisonne dans l'autre sens : si un nombre n'est pas une période alors il sera transcendant. Pourquoi donc ? Il faut démontrer un résultat de structure sur l'ensemble des périodes $\mathcal{P}$![32] Il faut montrer que tous les nombres algébriques sont des périodes et que $\mathcal{P}$ est une sous-algèbre de $\mathbb{C}$.

On voit qu'un nombre rationnel est une période dans la mesure où $p/q = r = \int_{0\leq x\leq r} \mathrm{d}x$, mais qu'en est-il pour les nombres algébriques ? Il faut faire un jeu d'écriture et avoir une définition plus précise de la notion de période (à base d'**intégrales sur un domaine $\mathbb{Q}$-semi-algébrique**). Mettons ça sous le tapis et revenons à nos transcendentaux.

On est face à une petite folie[33] ! "Seul" problème : il est quasiment impossible de déterminer si un nombre est une période, enfin c'est d'une complexité monstre.

1.4.2 Programmer énergiquement

Vu que je n'ai pas été très doué pour déduire des choses sur des bornes convenables pour a et b (je ne comprends pas...[34]), quoi que mieux que la bonne vieille technique du forçage ? On teste toutes les combinaisons et on "admet" qu'on les a toutes lorsque l'on trouve bien une somme égale à 2 (ce qui présuppose que le résultat $A(x) = 2$ soit vrai).

```
1  from math import ceil, sqrt
2  from fractions import Fraction
3
4  # On peut, ou pas, utiliser le module fractions (y'a juste a changer la
       definition de x)
5  x = Fraction('9/4') # pour avoir une meilleure evaluation de x (et pas
       betement perdre de la valeur a cause de l'arithmetique flottante)
6  somme = 0 # le total, egal a 2 si on a trouve tous les Q verifiant les
       conditions idoines
7
8  r = 150 # borne pour la precision, l'augmenter tant que la somme est
       differente de 2
9
10 def verifRes(a, b, c):
11     return ((a < 0) and (b**2 - 4 * a * c == 5) and (a * x**2 + b * x + c >
        0))
```

32. C'est la seule fois (sur le petit nombre que je connais) où j'ai vraiment trouvé intéressante la preuve d'un résultat de structure. Il y a besoin d'utiliser Fubini par exemple ohoh.

33. Une folie pour les "enfants" du moins tel que je t'en parle du moins, tout reste conceptuellement très basique ; les périodes sont également liées à des objets tels les fonctions L et quand j'en parlerai je prendrai vraiment soin de ne pas partir dans tous les sens comme dans cette sous sous section. D'ailleurs, je tiens à m'excuser, là c'est le début je suis vraiment tout feu tout flamme et c'est pas mal bordélique. Petit à petit ça devrait se calmer.

34. C'était ce dont je me doutais pour borner b gné... une bête question de signe pas mentionné chez Zagier. Et comment borner a ? Parce que, en définitive, ça revient à savoir qui sera le plus gros coefficient possible sur x^2 pour un Q vérifiant Δ. Et cette question ne se pose que dans le cas où x est rationnel.

```
12
13 for a in range(-r, 0):
14     for b in range(ceil(2 * a * x - sqrt(5)), ceil(2 * abs(a) * x + sqrt(5)
   )):
15         for c in range(ceil(-a * x**2 - b * x), ceil(5/(4 * abs(a)))):
16             if verifRes(a, b, c):
17                 print(a, b, c)
18                 somme += a * x**2 + b * x + c
19
20 print("==== ", x, " ", somme)
```

1.4.3 Fuck la programmation : construisons directement les choses

On a programmé c'est bien beau tout joli ; mais, au fond, on ne fait que chercher des valeurs dans des bornes que l'on estime justes et pas trop mauvaise afin de procéder mécaniquement à la détermination de tous les Q vérifiant Δ. Toutefois, ne pourrions nous pas *directement* construire l'ensemble des Q vérifiant Δ ? Ou plutôt en donner une expression "séquentielle" (c'est-à-dire former explicitement les suites (pour un x donné de Q vérifiant Δ plutôt que les rechercher laborieusement [35])). [36]

Premier problème : Comment découper suffisamment bien x afin d'obtenir de quelconques informations ? En gros, quelle partition (du domaine de définition de x) choisir afin de pouvoir faire quoi que ce soit ? Déjà, simplifions nous les choses et ne considérons que le cas x rationnel, égal à p/q. En fait, quelques pages plus tôt on avait déjà donné la réponse : considérons les $x = p/q$ tel que pgcd(p, q) $= 1$ (avec évidemment q différent de zéro).

Cherchons quelques **symétries** à vertu de simplifier encore le problème (sous-entendu que si on "donne une solution" au problème, on devrait aussi théoriquement avoir une solution relativement similaire pour sa formulation symétrique ; d'une pierre deux coups). Après quelques coups de Python, on s'attendrait à avoir un lien (tempéré par le nombre total de Q adéquats) entre $x = p/q$ et $1/x = q/p$. [37] Mais est-là tout ? Une chose pouvant nous rebuter est que Q est un polynôme du second degré, donc on risque peu de se retrouver avec une autre situation symétrique très très évidente (quoique ? le problème est surtout mal posé).

Après quelques petites recherches pour le cas rationnel, j'ai la conviction que l'on peut très bien se débrouiller : il y a des symétries un peu partout mais tout devient très compliqué très rapidement. On trouve de jolies formules (pour les cas simples) qui semblent bien se généraliser. Aller faire ses petites recherches sur un tel problème simplement avec l'optique de le résoudre n'est pas bon. Il convient d'avoir de bons bagages afin de remarquer des choses qu'un oeil non entraîné ne pourrait voir. C'est exactement ce que Zagier a fait : plus tard il va se rendre compte qu'il n'y a aucune nécessité de limiter D à 5 (et il peut même

35. Mais pour les déterminer, il va falloir les chercher laborieusement puis chercher les patterns associés à chaque x.

36. On va tout de même se souhaiter bonne chance... Zagier concède qu'il n'y ait pas totalement arrivé même pour un cas très particulier page 1169.

37. Notons tout de même que penser à cette symétrie en ayant fait l'effort d'essayer de construire directement les Q donne sans doute un élément de réponse au pourquoi du comment on puisse utiliser cette symétrie dans la démonstration du résultat initial (notre première surprise).

encore généraliser). Après quelque peu de gymnastique et de cuisine, il se rend compte que les objets (dont l'équation 1.3) qui s'énoncent de manière très simple ont des réponses très compliquées.

1.5 Avant de généraliser, (re)voyons nos classiques

Ennnfinnnn ! Enfin nous allons voir des choses "nouvelles" et mettre salement les mains à la pâte. Néanmoins, il va falloir faire des choix : il va être impossible d'exposer "entièrement" les théories sous-jacentes. Toutefois, dans la limite du possible, des sortes de "mini cours introductif" vont être dispensé. Ainsi, nous n'aurons aucune gêne à nous appesantir longuement sur des théories connexes ou sous-jacentes qui n'apparaissent que partiellement dans le papier de Zagier tant qu'elles permettent ultérieurement une compréhension des sujets en jeux.

Les *gros mots* qui vont nous intéresser dans un premier temps seront : **fonction somme des diviseurs**, **théorie des nombres algébriques**, **invariant**, **discriminant fondamental**, **corps quadratique**, **idéaux de** $\mathcal{O}_K$ et pas mal de fonctions "spéciales" / arithmétiques : **séries de Dirichlet**, **fonctions zêta** ainsi que du vocabulaire provenant de différents domaines : **prolongement analytique ou méromorphe** (*analytic or meromorphic continuation*), choses **modulaires**, **développements de Fourier**... Il va falloir trouver une manière de présenter tout cela de manière "unifiée". Cela va prendre du temps, ça semble même difficilement possible [38] en si peu de temps mais avançons autant que nous le pouvons. Commençons à faire des mathématiques et non de la casuistique comme précédemment. On veut désormais montrer un cheminement intellectuel et ne rien laisser au hasard.

Motivations. Plus tôt dans le document, on a pu s'amuser à essayer de donner quelques bribes de définitions à ce que pouvait être *une* arithmétique. Désormais intéressons nous, graduellement, à ce que peut être **l'arithmétique**. De nos études passées, au lycée, très peu d'arithmétique élémentaire pour l'absolue majorité des lycéens. En spécialité (aujourd'hui "maths expertes"), on a eu le droit de découvrir quelques rudiments (que nous allons prendre le temps de reposer sur papier). Oui, nous allons partir de loin. Ensuite, si l'on part en classes préparatoires, une nouvelle fois de l'arithmétique très élémentaire (ce qui n'empêche aucunement ceux qui élaborent les sujets de pondre des sujets "bien inspirés" dans un tel domaine). De l'autre côté, en licence : *a priori* rien avant la troisième année (à Toulouse du moins). Puis, une fois arrivé(e) en Master, ou alors on en bouffe à-veux-tu-en-voilà ou alors on n'y touche que d'assez loin (dans la majorité des cas). Bref, en règle générale, la part belle n'est pas forcément faite à l'arithmétique. Je t'avoue que j'en avais moi même un point de vue assez biaisé, quelque chose où on ne réfléchit qu'avec des nombres, un peu rude et barbare sans aucune idée profonde. Aïe... j'étais bien à côté de la plaque.

38. Écrire ce *commentaire à un ami* me fait de plus en plus me rendre compte à quel point les choses peuvent être profondes et faire des mathématiques peut être compliqué. Et dire que ce commentaire ne fait que commencer...

Plan. 1 - **Survol de l'arithmétique et de ses déclinaisons**. 2 - **Arithmétique élémentaire**. 3 - **Quelques fonctions arithmétiques**. 4 - **Premiers pas en théorie des nombres**. 5 - **Bon dieu ! De l'algèbre ? !**. 6 - **Zagier ! Nous voilà !**

1.5.1 Survol de l'arithmétique et de ses déclinaisons

J'aurais vraiment aimé te faire tout un résumé historique mais je n'en ai pas la capacité. Donc, on va faire autrement : on va présenter les choses un peu par matière en agrémentant dès que possible de remarques historiques.

En arithmétique, logiquement on manipule des nombres. Toutefois cela peut aller bien plus loin que l'idée intuitive de nombre comme on peut l'entendre dans la vie de tous les jours.

Dans un premier temps on va essayer de comprendre les diverses propriétés qui régissent les nombres et qui les inter-connectent. On va par exemple se demander s'il existe une classe de nombre, un peu spéciale, qui permet de ré-écrire l'ensemble des nombres d'une certaine manière. Les **nombres premiers** font leur apparition. Par le **théorème fondamental de l'arithmétique**, l'on se rend compte qu'il existe une décomposition en facteurs premiers de tout nombre naturel (et même relatif). C'est quand même une chose assez saisissante : il existe certains nombres qui permettent de "comprendre" tous les autres nombres. Si ces nombres premiers étaient compris parfaitement clairement (répartition, propriétés analytiques, en quoi l'analyse complexe peut devenir utile (ça semble paradoxal), compréhension algébrique / géométrique...) alors ce devrait permettre de résoudre bon nombre de problèmes (de théorie des nombres, de théorie analytique des nombres [...], d'algèbre...) dont de très célèbres "hypothèses" [39].

Formellement, un nombre premier est un élément de l'**anneau des entiers relatifs** ; mais, qui nous oblige à nous restreindre à un **anneau** bien précis ? Et, au fond, les nombres premiers ne seraient-ils pas les éléments d'un sous-ensemble bien particulier de l'anneau à considérer ? Tout de suite la notion d'**idéal** fait son apparition [40]. Bon dieu ! De l'algèbre ? ! Et c'est parti pour un tour, mais c'est loin d'être fini. Suite à Kummer, Dedekind, Kronecker... on arrive à une notion assez stable de **théorie des anneaux** et beaucoup beaucoup de choses se développent autour (notamment pour essayer de démontrer le dernier théorème de Fermat [41]). On trouve même un énoncé "philosophiquement équivalent" au théorème fondamental de l'arithmétique mais cette fois ci pour les idéaux d'un anneau (non forcément celui des entiers relatifs). Bref, on va bouffer de la théorie des anneaux (mais ce n'est pas tout, on ira certainement pas jusqu'à la théorie du corps de classe / aux immixtions des groupes de Galois dans un "contexte arithmétique" [42], mais il va falloir déblayer beaucoup de choses autour).

39. Deligne à la suite de Weil, Grothendieck... a pu prouver l'hypothèse de Riemann sur les corps finis. Il y a un article de Milne (J.S.) (un collaborateur de Deligne notamment) qui paraît troooop bien : *The Riemann Hypothesis over Finite Fields From Weil to the Present Day*. Bref, l'histoire est loin d'être finie.

40. Ce n'est peut-être pas anodin si ça s'appelle "idéal" ?

41. Kummer prouvera par exemple que le théorème de Fermat est vrai pour une certaine classe de nombres premiers.

42. On n'a même pas encore parlé de Gauss d'ailleurs... mais du côté de son oeuvre également il va y avoir du chemin à parcourir.

D'un tout autre point de vue (mais qui ne manque pas de rencontrer le précédent), des phénomènes plus "analytiques" sont également à observer en arithmétique et plus précisément en théorie des nombres. Cela peut étonner mais, par exemple, le **théorème des nombres premiers**, énonçant que $x/\log(x)$ est une bonne approximation asymptotique de la fonction de compte des nombres premiers, a par exemple connu une démonstration usant de l'analyse complexe (Hadamard, de La Vallée Poussin) et (apparemment) tout particulièrement de la **fonction zêta de Riemann**[43].

Et le pire dans tout ça c'est que l'on est pas encore au bout de nos surprise ! Faudrait foutre le nez dans les **courbes elliptique**, **fonctions L**, **formes automorphes**, **programme de Langlands**, **théorie d'Iwasawa**, **variétés arithmétiques**, **géométrie diophantienne**, **géométrie d'Arakelov**... pour ne rien que commencer à avoir une vue vraiment d'ensemble sur ce que peut embrasser l'arithmétique.

En somme, encore une fois nous sommes dans la merde. Nous resterons évidemment sur des considérations ô combien plus élémentaires mais tenterons tout de même de, progressivement, nous approcher de certains de ces domaines (au moins pour piger quelque chose au papier de Zagier).

1.5.2 Arithmétique élémentaire

À vrai dire, nous allons faire deux fois de l'algèbre, de telle manière à ce que la sous-section *Bon dieu ! De l'algèbre ? !* ne soit pas tant que cela une surprise... Nous préparons le chemin dès maintenant ; bien que nous aurions pu attendre encore un peu. En effet, (au moins) deux manières de faire les choses s'offraient à nous : suivre la logique d'un cours de Terminale spé Maths voire de classe préparatoire en laissant tout au mieux présager qu'il existe des fondements plus algébriques qu'il n'y paraît ou alors tout de suite se dire : soyons algébriques. C'est exactement ce que nous allons être. En partant d'un **anneau**, on va plus ou moins reformuler l'arithmétique élémentaire sur ledit anneau. Ensuite, notre attention va se porter à un constituant fondamental de l'arithmétique : les nombres premiers ; cela va nous obliger à "monter" sur un **corps**. Mais si le but n'est que d'avoir une formulation annélique et sur un corps... boh où serait l'utilité ? Dès que nous allons nous éloigner du simple cas de $\mathbb{Z}$ et ce qui l'entoure tout devrait être soudainement plus intéressant (cf. [18]).

1. Arithmétique élémentaire sur un anneau. Commençons par une remarque : si l'on se place dans $\mathbb{Z}$, nous n'aurons aucun problème à affirmer que n'importe lequel de ses éléments peut se décomposer en facteurs premiers. Si l'on réfléchit désormais sur $\mathbb{Q}$ rien de fondamental intéressant ne se passe (la structure de $\mathbb{Q}$ est "trop proche" de celle de $\mathbb{Z}$ par construction même, on n'ajoute intuitivement rien à "la logique" de $\mathbb{Z}$). C'est un peu décevant mais l'on se réconforte en remarquant qu'il existe sans nul doute d'autres voies dans lesquelles nous pouvons nous engouffrer. Il doit bien exister des choses "pas trop loin" de $\mathbb{Z}$ qui permettent de faire de l'arithmétique ? Voyons deux exemples bien particuliers avant de considérer un cas quelque peu plus général.

43. Fonction connaissant, en tant que cas particulier, une arithmétique très riche et complexe et ayant un profond retentissement en algèbre.

Entiers de Gauss. Les entiers de Gauss sont les nombres complexes pouvant s'écrire sous la forme $a+ib$, avec $(a,b)\in\mathbb{Z}^2$. On note alors un tel anneau $\mathbb{Z}[i]$. Existe-t'il en ce lieu une forme similaire au théorème fondamental de l'arithmétique ? Nous laissons planer l'idée que chacun de ses éléments peut se factoriser (de manière unique) en "nombres premiers" (notion à bien cerner dans ce cas précis).

Tout d'abord il va falloir déterminer qui sont ces **nombres premiers de Gauss** et ensuite assurer le résultat dans ce cas bien précis. On s'attend (logiquement) à ce que ces "nombres premiers" ne possèdent comme diviseur qu'eux-même et l'unité (et soient également différents de l'unité)[44]. Cherchons donc $\mathbb{Z}[i]^\times$, c'est-à-dire l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ (autrement dit, l'ensemble des $p_1\in\mathbb{Z}[i]$ tel qu'il existe un élément $p_2\in\mathbb{Z}[i]$ afin que $p_1p_2=\mathrm{Id}$ (on se fiche de la question de la commutativité là)). On écrit alors que, pour $p_1=a_1+ib_1$ et $p_2=a_2+ib_2$, $p_1p_2=1$, ce qui se résume à :

$$(a_1+ib_1)(a_2+ib_2)=1 \tag{1.8}$$

autrement dit (on passe sur certaines hypothèses) :

$$a_1+ib_1=\frac{a_2-ib_2}{a_2^2+b_2^2}=\frac{a_2}{a_2^2+b_2^2}+\frac{-b_2}{a_2^2+b_2^2}i \tag{1.9}$$

Ensuite, par un simple raisonnement déductif en se basant sur le fait qu'à la fois $\frac{a_2}{a_2^2+b_2^2}$ et $\frac{-b_2}{a_2^2+b_2^2}$ doivent être des entiers naturels (et non rationnels !), on trouve que $\mathbb{Z}[i]^\times=\left\{\pm1;\pm i\right\}$. Avec ça, on a quasiment tous les éléments pour déduire les premiers de $\mathbb{Z}[i]$. Toutefois, ce n'est pas la classification qui va retenir notre intérêt : c'est surtout le fait que ce soit possible. En effet, nous allons donc avoir un théorème similaire à celui de la décomposition (qui plus est unique) en facteurs premiers dans ce cas.

En fait, on va pouvoir faire tout un tas d'opérations arithmétiques similaires à celles sur $\mathbb{Z}$. Cela va se traduire par une certaine propriété sur l'anneau en question (mais nous verrons plus tard).

Entiers d'Eisenstein. Même logique avec les entiers d'Eisenstein : nous laissons planer l'idée que chacun de ses éléments peut se factoriser (de manière unique ?) en "nombres premiers" (notion à bien cerner dans ce cas précis).

Un entier d'Eisenstein est un nombre complexe de la forme $a+\omega b$, avec $(a,b)\in\mathbb{Z}^2$ et $\omega=\frac{-1+i\sqrt{3}}{2}$ (ainsi $\omega^3=1$). On note alors un tel anneau $\mathbb{Z}[\omega]$.

Là encore on va pouvoir faire bon nombres d'opérations arithmétiques élémentaires similaires à celles sur $\mathbb{Z}$. Encore une fois, l'on va se retrouver avec une propriété sur l'anneau relativement équivalente que dans le cas des entiers de Gauss (à une subtilité près gné).

44. Ou, dit de manière équivalente, les nombres premiers de Gauss sont les nombres n'étant pas inversible (sinon ce serait une unité comme on va le voir) et que toute décomposition de ce nombre en deux autres nombres de $\mathbb{Z}[i]$ implique qu'au moins un des deux soit inversible (faut écrire correctement les choses pour voir comment ça marche).

D'autres "entiers" ? Plus généralement, l'on peut considérer les nombres complexes de la forme $a + \zeta b$, avec $(a, b) \in \mathbb{Z}^2$ et ζ un nombre complexe. On notera cet anneau $\mathbb{Z}[\zeta]$ et par exemple, les entiers d'Eisenstein se notent : $\mathbb{Z}[i\sqrt{3}] = \mathbb{Z}[\sqrt{-3}]$.

On peut être tenter de savoir ce qu'il se passe sur d'autres anneaux que ceux des entiers de Gauss ou d'Eisenstein. Néanmoins, la notion de "premier" va se complexifier quelque peu. On est habitué à ce qu'une décomposition en facteurs "premiers" soit unique. Mais est-ce possible qu'elle ne le soit plus pour certains anneaux ? Si l'on se place dans $\mathbb{Z}[\sqrt{-5}]$ alors :

$$2 \cdot 3 = 6 = (1 - i\sqrt{5}) \cdot (1 + i\sqrt{5}) \tag{1.10}$$

45 , 46

2. Arithmétique élémentaire sur un corps et nombres premiers.

3. Entrevues arithmétiques.

4.

5.

1.5.3 Quelques fonctions arithmétiques

1.5.4 Premiers pas en théorie des nombres

1.5.5 Bon dieu ! De l'algèbre ? !

1.5.6 Zagier ! Nous voilà !

1.6 Généralisations à d'autres discriminants et valeurs spéciales de séries L

Les séries L et des histoires d'arithmétique et d'algèbre, normalement, ça ne devrait plus nous faire peur (en fait si, mais un peu moins en théorie).

45. J'ai fait une petite pause, j'écris ça après 12 petits jours sans penser à ce commentaire. En parlant à Félix, une phrase m'est venue : "*tant que je n'ai pas ça de bien posé, je ferme ma gueule*" (où "ça" représente grossièrement le "langage topologique"). C'est essentiellement la réaction à deux éléments : un qui m'est inné, l'autre provenant de ta mise en garde. Ce document va être pour moi une sorte d'échappatoire, tu ne le liras sans doute jamais. C'est mon "petit jardin secret" où je me défoule. En public, je vais être "plus rangé" disons : je ferme ma gueule si je ne maîtrise pas parfaitement le langage usité.

46. Par un certain "syncrétisme" (lecture des *Confessions* de Saint Augustin, de *Analysis I* de Terence Tao et ayant quelques idées grothendickiennes en tête : je me rends compte que je confonds tout. Je ne sais pas si j'ai oublié ou bien jamais vraiment su ce qu'étaient les mathématiques. Même maintenant je ne sais pas vraiment ce que c'est mais au moins il y a des choses qui me viennent en tête. Les Mathématiques seraient essentiellement une acceptation de l'abstrait. On accepte de travailler avec des objets sans se poser la question de pourquoi ils existent (ce qui est différent du comment ils existent et peut-être même différent des motivations de leur existence). On prend les choses, les incorpore et les développe. À aucun moment, à moins de faire de la philosophie des Mathématiques, on ne va chercher le pourquoi du comment d'un tel ou d'un autre objet (c'est tout d'abord une question trop vague mais surtout elle n'apporte strictement rien et n'est aucunement en accord avec l'idée que les Mathématiques soient sensées être "pures" (ne "servir à rien"). À voir...

2 Démonstrations, raffinements et compléments

3 La connexion modulaire

Références

[1] M. Garnier, *Commentaire pour un ami et explications d'un article d'Henri Poincaré, Sur les hypothèses fondamentales de la géométrie, Bulletin de la S.M.F., tome 15 (1887), page 203-216. (14 pages)*

[2] Don Zagier, *From quadratic functions to modular functions in Number Theory in Progress. Vol 2 (K. Győry, H. Iwaniec and J. Urbanowicz, eds.), Proceedings of Internat. Conference on Number Theory, Zakopane 1997, de Gruyter, Berlin (1999) 1147-1178.*

[3] Chao Li, *https://www.math.columbia.edu/∼chaoli/doc/ZagierQuadraticModular.html.*

[4] Jean-Pierre Serre, *Une interprétation des congruences relatives à la fonction tau de Ramanujan, Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, no 1 (1967-1968), exp. no 14, p. 1-17.*

[5] Nik Lygeros et Olivier Rozier, *Odd prime values of the Ramanujan tau function. The Ramanujan Journal An International Journal Devoted to the Areas of Mathematics Influenced by Ramanujan ISSN 1382-4090 Ramanujan J DOI 10.1007/s11139-012-9420-8.*

[6] Bruce C. Berndt et Ken Ono, *RAMANUJAN'S UNPUBLISHED MANUSCRIPT ON THE PARTITION AND TAU FUNCTIONS WITH PROOFS AND COMMENTARY .*

[7] Didier Piau et Bernard Ycart, *Polynômes et fractions rationnelles, Maths en Ligne, Université Joseph Fourier, Grenoble.*

[8] Fernando Q. Gouvêa et Jonathan Webster, *Determining the determinant.*

[9] Michel Waldschmidt, *An Introduction to irrationality and transcendence methods.*

[10] Michel Waldschmidt, *QUESTIONS DE TRANSCENDANCE : GRANDES CONJECTURES PETITS PROGRÈS.*

[11] Michel Waldschmidt, *TRANSCENDANCE DE PERIODES : ÉTAT DES CONNAISSANCES.*

[12] Ivan Niven, *Numbers : rational and irrational.*

[13] Pierre Lairez, *Thèse de doctorat, Périodes d'intégrales rationnelles, algorithmes et applications.*

[14] Stéphane Fischler et Tanguy Rivoal, *UN EXPOSANT DE DENSITÉ EN APPROXIMATION RATIONNELLE, 2006.*

[15] Stéphane Fischler, *Irrationalité de valeurs de zêta [d'après Apéry, Rivoal, ...], 2002.*

[16] Stéphane Fischler, *Irrationality of values of L-functions of Dirichlet characters.*

[17] Maxim Kontsevich et Don Zagier, *Periods.*

[18] Vera Bulankina, Ivan Frolov, Timofei Zaitsev, Aleksei Petukhov et Ruslan Salimov, *Generalizations of the fundamental theorem of arithmetic.*

[19] , .

[20] , .

[21] , .

[22] , .

[23] Author, *Title.*