DES NOMBRES CONGRUENTS À LA FORMULE DE GROSS–ZAGIER

Une Épopée Arithmétique : Courbes Elliptiques et Formes Modulaires

17 janvier 2026

Yunjie LUO

Résumé

Cet article retrace l'évolution historique des idées mathématiques centrées sur les courbes elliptiques et les formes modulaires jusqu'à la formule de Gross-Zagier en 1986, résultat emblématique de la théorie des nombres du XX^{e} siècle. Suivant un déroulement chronologique, il examine le problème des nombres congruents (avant 972), la conjecture de Gauss sur les nombres de classes (1801), le théorème de Mordell concernant les courbes elliptiques (1922), les travaux précurseurs de Heegner (1952), les conjectures de Birch et Swinnerton-Dyer (années 1960), le théorème de Coates-Wiles (1977), la formule de Gross-Zagier (1986) et les développements ultérieurs issus de ceux-ci. À travers cette synthèse, cet article vise à rendre accessible le déroulement et la portée de cette histoire mathématique.

TABLE DES MATIÈRES

1 INTRODUCTION

La théorie des nombres, souvent qualifiée de « reine des mathématiques », a connu aux XX^{e} et XXI^{e} siècles des avancées spectaculaires, nourries par la fertilisation croisée avec la géométrie algébrique. Parmi les résultats phares de cette période figure la formule de Gross-Zagier (1986), qui établit un lien profond entre la hauteur de points spéciaux (points de Heegner) sur les courbes elliptiques et la dérivée première de leur fonction L en un point central. En fournissant un outil puissant pour attaquer la conjecture de Birch et Swinnerton-Dyer, ce théorème est devenu une pierre angulaire de la théorie des nombres moderne.

Cet article se propose de retracer, dans une perspective historique, l'enchaînement d'idées qui a conduit à ce résultat. Pour ce faire, nous prendrons comme fil conducteur deux outils centraux : les courbes elliptiques et les formes modulaires. Notre parcours, chronologique, partira d'un problème ancien – celui des nombres congruents – pour aboutir aux développements les plus récents. Il nous permettra de croiser les travaux de figures majeures telles que **Gauss**, **Mordell**, **Heegner**, **Birch**, **Swinnerton-Dyer** et **Wiles**, et d'apprécier comment leurs contributions se sont imbriquées pour construire un édifice mathématique aussi cohérent qu'élégant.

2 DEUX PROBLÈMES CÉLÈBRES

2.1 Le Problème des Nombres Congruents

Nous débuterons par l'étude du célèbre problème diophantien connu sous le nom de « problème des nombres congruents », dont la formulation initiale remonte à un manuscrit anonyme arabe remontant avant 972 [3, Chap. XVI].

Définition 2.1 (Nombres congruents)**.** Un entier positif n est dit *congruent* s'il est l'aire d'un triangle rectangle dont les trois côtés sont des nombres rationnels. Autrement dit, s'il existe des nombres rationnels positifs a, b et c tels que :

$$a^2 + b^2 = c^2 \quad \text{et} \quad n = \frac{1}{2}ab.$$

À l'aide du tableau suivant, nous pouvons vérifier que $5, 6$ et 7 sont des nombres congruents.

n	Triangle rectangle rationnel (a, b, c)	Équation
5	$(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$	$(\frac{3}{2})^2 + (\frac{20}{3})^2 = (\frac{41}{6})^2$
6	$(3, 4, 5)$	$3^2 + 4^2 = 5^2$
7	$(\frac{24}{5}, \frac{35}{12}, \frac{337}{60})$	$(\frac{24}{5})^2 + (\frac{35}{12})^2 = (\frac{337}{60})^2$

Table 1 – Exemples de nombres congruents

De plus, au XVII^{e} siècle, **Fermat** a démontré, à l'aide de la méthode de *descente infinie*, le théorème suivant.

Théorème 2.2 (Fermat)**.** 1 *n'est pas un nombre congruent.*

Cela nous amène à poser la question suivante.

Problème (Problème des nombres congruents)**.** Étant donné un entier positif n, comment déterminer s'il s'agit d'un nombre congruent ?

Ce problème, d'apparence élémentaire, s'avère d'une difficulté remarquable. Il possède une reformulation élégante en termes de courbes elliptiques, comme nous le verrons plus tard dans la section 3.2. Précisément, cette connexion avec la théorie des courbes elliptiques explique l'intérêt soutenu qu'il suscite encore aujourd'hui. En effet, le problème général reste non résolu à ce jour. Toutefois, grâce aux vérifications numériques par ordinateur et aux progrès théoriques partiels, les mathématiciens ont formulé une conjecture moderne, que nous énonçons ci-dessous.

Conjecture. Soit n un entier positif.
— Si $n \equiv 5, 6, 7 \pmod 8$, alors il est congruent.
— La probabilité que $n \equiv 1, 2, 3 \pmod 8$ soit congruent est nulle.

2.2 La Conjecture des Nombres de Classes

Cette section présente la conjecture des nombres de classes de Gauss et les idées arithmétiques qu'elle a inspirées.

Au tournant du XIX$^{\text{e}}$ siècle, **Carl Friedrich Gauss**, dans son œuvre fondamentale *Disquisitiones Arithmeticae* (1801), introduit la notion de classe d'équivalence pour les formes quadratiques entières.

Définition 2.3 (Formes quadratiques entières)**.** Une *forme quadratique entière* est une expression $f(x, y) = ax^2 + bxy + cy^2$ avec $a, b, c \in \mathbb{Z}$. Son discriminant est défini par $D := b^2 - 4ac$.

Définition 2.4 (Équivalence de formes quadratiques entières)**.** Deux formes quadratiques entières sont dites équivalentes si l'on peut passer de l'une à l'autre par une transformation linéaire de déterminant 1, c'est-à-dire par l'action du groupe $\mathrm{SL}_2(\mathbb{Z})$, i.e.

$$g(x, y) = f(ax + by, cx + dy), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Pour un discriminant D non nul, Gauss définit le *nombre de classes*, noté $h(D)$, comme le nombre de classes d'équivalence de formes quadratiques entières de discriminant D. C'est cette définition historique, purement arithmético-géométrique, que nous utilisons dans ce chapitre.

En langage moderne, cette notion a été généralisée et refondée en théorie algébrique des nombres : le nombre de classes $h(D)$ s'interprète alors comme le cardinal du *groupe des classes d'idéaux* de corps $\mathbb{Q}(\sqrt{D})$.

Gauss formula la conjecture suivante concernant les discriminants négatifs pour lesquels $h(D) = 1$, c'est-à-dire les cas où la forme quadratique principale est, à équivalence près, la seule :

Conjecture (Gauss, 1801)**.** Soit $D < 0$ un discriminant tel que $h(D) = 1$. Alors

$$-D \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\},$$

ou bien

$$-D \in \{12, 16, 27, 28\}.$$

La démonstration complète de cette conjecture, qui résistait depuis plus d'un siècle et demi, a finalement été obtenue au milieu du XX$^{\text{e}}$ siècle. La preuve fait appel de manière cruciale à la théorie des formes modulaires et à l'étude des courbes modulaires. L'approche pionnière de **Kurt Heegner** [6] en 1952 – de formation initiale d'ingénieur radio et mathématicien autodidacte – reposait sur la construction de points spéciaux (dits *points de Heegner*) sur ces courbes (nous en donnerons un exposé détaillé dans la section 4.2). Cependant, en raison de son style technique obscur et de sa marginalité académique, ses travaux restèrent largement méconnus et ne furent pas immédiatement acceptés par la communauté mathématique.

Ce n'est qu'une quinzaine d'années plus tard que **Harold Stark** [11], reprenant et clarifiant des idées voisines de celles de Heegner, fournit une démonstration indépendante et reconnue, confirmant par là même la pleine validité de l'argument originel.

Par ailleurs, dans le même article de 1952, Heegner établit un résultat remarquable liant la théorie des nombres congruents à la théorie des formes modulaires :

Proposition 2.5 (Heegner, 1952)**.** *Tout nombre premier p tel que $p \equiv 5$ ou $7 \pmod 8$ est un nombre congruent.*

Ce lien précoce entre points spéciaux sur des courbes et propriétés arithmétiques préfigurait déjà les développements ultérieurs de la théorie des nombres.

3
LES COURBES ELLIPTIQUES

3.1 Le Théorème de Mordell

Dans cette section, nous introduisons formellement la notion de courbe elliptique, en présentons les propriétés fondamentales et énonçons les principaux théorèmes qui y sont associés. Parmi ces résultats, le plus important est le théorème de Mordell, qui est le fondement de l'arithmétique des courbes elliptiques.

Définition 3.1 (Courbe elliptique)**.** Une *courbe elliptique* sur $\mathbb{Q}$ est donnée par une équation :

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q}, \quad \Delta = -16(4a^3 + 27b^2) \neq 0.$$

Le discriminant Δ non nul assure que la courbe est non singulière.

On note

$$E(\mathbb{Q}) \coloneqq \{(x, y) \in E \mid x, y \in \mathbb{Q}\} \cup \{\infty\},$$

où ∞ désigne le point à l'infini, élément neutre pour la loi de groupe. L'ensemble $E(\mathbb{Q})$ forme un groupe abélien via la construction géométrique *corde-tangente*, explicitée par la figure 1. Cette construction, dont la formulation moderne remonte à **Christian Juel** (1896), donne à $E(\mathbb{Q})$ une riche structure algébrique.

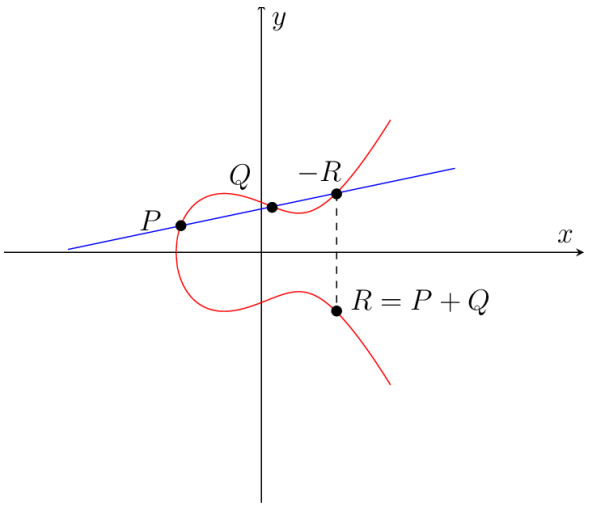

Figure 1 – Addition de points sur une courbe elliptique

En 1922, **Louis Mordell** [9] démontra le théorème fondamental suivant :

Théorème 3.2 (Mordell, 1922)**.** *Soit E une courbe elliptique sur $\mathbb{Q}$. Alors le groupe $E(\mathbb{Q})$ est de type fini.*

Autrement dit, il existe un entier $r \geq 0$ (appelé le *rang*) et un sous-groupe fini $E(\mathbb{Q})_{\text{tors}}$ (le sous-groupe de *torsion*) tels que :

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r.$$

Dans [9], Mordell a également formulé sa célèbre conjecture, qui fut résolue en 1983 par **Gerd Faltings** [4], mais comme elle ne constitue pas le cœur de notre propos, nous n'en développerons pas davantage ici.

La structure de $E(\mathbb{Q})$ nous amène à deux problèmes distincts :

1. Déterminer le sous-groupe de torsion fini $E(\mathbb{Q})_{\text{tors}}$.
2. Déterminer le rang r.

Le premier problème a été complètement résolu par **Barry Mazur** [8] en 1977.

Théorème 3.3 (Mazur, 1977)**.** *Le groupe de torsion $E(\mathbb{Q})_{tors}$ est isomorphe à l'un des quinze groupes suivants :*

$$\mathbb{Z}/N\mathbb{Z}, \quad N = 1, 2, \ldots, 9, 10, 12;$$

$$(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2N\mathbb{Z}), \quad N = 1, 2, 3, 4.$$

En revanche, le second problème – déterminer le rang r – est beaucoup plus profond et demeure largement ouvert. Nous ne savons même pas s'il existe une borne uniforme pour le rang des courbes elliptiques sur $\mathbb{Q}$. Cette question est au cœur de la conjecture de Birch et Swinnerton-Dyer, qui sera présentée dans la section 5.1.

3.2 Retour sur les Nombres Congruents

Dans cette section, nous détaillons le lien profond entre les nombres congruents et les courbes elliptiques.

Proposition 3.4. *Un entier positif n (sans facteur carré) est congruent si et seulement si la courbe elliptique*

$$E_n : y^2 = x^3 - n^2 x$$

possède un point rationnel (x, y) avec $y \neq 0$.

Idée de la preuve. Si n est congruent, il existe un triangle rectangle rationnel d'aire n. En notant a, b, c ses côtés ($a^2 + b^2 = c^2$, $ab = 2n$), on vérifie que le point

$$\left(\frac{n(a-c)}{b}, \frac{2n^2(a-c)}{b^2} \right)$$

appartient à $E_n(\mathbb{Q})$ et a une ordonnée non nulle. Réciproquement, si $P = (x, y) \in E_n(\mathbb{Q})$ avec $y \neq 0$, on peut construire les nombres

$$a = \frac{x^2 - n^2}{y}, \quad b = \frac{2nx}{y}, \quad c = \frac{x^2 + n^2}{y},$$

qui vérifient $a^2 + b^2 = c^2$ et $\frac{1}{2}ab = n$. Ainsi n est l'aire du triangle rectangle de côtés $|a|, |b|, |c|$, donc n est congruent. □

Cette correspondance permet de traduire le problème des nombres congruents en un problème sur les points rationnels d'une famille de courbes elliptiques. En fait, l'existence d'un tel point est équivalente à ce que le groupe $E_n(\mathbb{Q})$ soit infini, c'est-à-dire que son rang r soit positif. Ainsi, le problème classique se traduit en un problème moderne sur le rang d'une famille de courbes elliptiques.

La conjecture évoquée précédemment sur la distribution des nombres congruents s'interprète alors comme une assertion sur la distribution des rangs des courbes E_n : pour $n \equiv 5, 6, 7 \pmod 8$, on s'attend à ce que $r \geq 1$, tandis que pour $n \equiv 1, 2, 3 \pmod 8$, on s'attend à ce que $r = 0$ dans la majorité des cas.

4
LES FORMES MODULAIRES

4.1 Les Définitions

Dans cette section, nous présentons les fonctions modulaires et les formes modulaires, qui jouent un rôle central dans le travail de Heegner.

Considérons le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Le groupe modulaire $\mathrm{SL}_2(\mathbb{Z})$ agit sur $\mathbb{H}$ par transformations linéaires fractionnaires. Pour un entier positif N, on définit le *sous-groupe de congruence*

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

Définition 4.1 (Fonctions modulaires)**.** Une *fonction modulaire* de niveau N est une fonction méromorphe sur $\mathbb{H}$ invariante sous l'action de $\Gamma_0(N)$. Elle peut être vue comme une fonction méromorphe sur la *courbe modulaire*

$$X_0(N) = \mathbb{H}^*/\Gamma_0(N),$$

où $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ désigne le demi-plan de Poincaré complété par les pointes.

Définition 4.2 (Formes modulaires)**.** Une *forme modulaire* de poids k et de niveau N est une fonction holomorphe $f : \mathbb{H} \to \mathbb{C}$ telle que :

1. Pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, on a
$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z);$$
2. f est holomorphe aux pointes. Cela signifie que pour chaque pointe de $X_0(N)$, le développement de Fourier (ou de q-développement, avec $q = e^{2\pi i z}$) de f ne comporte que des termes d'exposants ≥ 0.

Sans entrer dans des détails mathématiques complexes, on peut simplement voir les fonctions modulaires et les formes modulaires comme des fonctions jouissant d'une « belle symétrie ».

4.2 Les Points de Heegner

Dans cette section, nous donnons certains détails du travail de Heegner. Nous nous concentrons sur sa méthode de construction de points rationnels non triviaux sur les courbes elliptiques associées aux nombres congruents, qui a conduit à la démonstration partielle du problème des nombres congruents et dont les idées ont joué un rôle central dans la preuve de la formule de Gross-Zagier.

Rappelons la Proposition 3.4, le problème des nombres congruents se transforme en un problème sur les points rationnels d'une famille de courbes elliptiques. Ainsi, pour montrer la Proposition 2.5, Heegner a construit explicitement un tel point rationnel sur E_p.

L'idée centrale de Heegner est de paramétrer les solutions de l'équation $E_p : y^2 = x^3 - p^2 x$ par des fonctions modulaires. Plus précisément, il existe des fonctions modulaires $f(z)$ et $g(z)$ (de niveau approprié) telles que

$$\big(f(z), g(z)\big) \in E_p \quad \text{pour tout } z \in \mathbb{H}.$$

Pour obtenir un point algébrique sur E_p, Heegner choisit un point $z_0 \in \mathbb{H}$ possédant des propriétés arithmétiques spéciales : un *point à multiplication complexe (CM)*. Concrètement, un tel point s'écrit

$$\tau = a + b\sqrt{-d}, \qquad a, b, d \in \mathbb{Q},\ b, d > 0.$$

La théorie de la multiplication complexe [10] assure que les valeurs $f(\tau)$ et $g(\tau)$ sont des nombres algébriques.

En appliquant cette idée à la courbe E_p et à un choix judicieux de point CM τ, Heegner obtient un point algébrique $P_\tau = (f(\tau), g(\tau))$ sur E_p. Pour passer à un point rationnel, il effectue ensuite une somme sur l'orbite de P_τ sous l'action du groupe de Galois absolu de $\mathbb{Q}$:

$$P = \sum_{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} P_\tau^\sigma.$$

Cette somme, appelée *point de Heegner*, est un point rationnel non trivial sur E_p (pourvu que certaines conditions soient remplies). La construction fournit ainsi une démonstration que p est congruent.

5
EXPLORATIONS MODERNES

5.1 La Conjecture de Birch et Swinnerton-Dyer

Dans cette section, nous présentons l'un des sept problèmes du Prix du Millénaire : la conjecture de Birch et Swinnerton-Dyer (BSD), et ses liens avec les courbes elliptiques et les formes modulaires.

Dans les années 1960, **Bryan Birch** et **Peter Swinnerton-Dyer**, munis des premiers ordinateurs (comme l'EDSAC II à Cambridge), entreprirent des calculs massifs sur les courbes elliptiques. Ils observèrent une corrélation frappante entre le rang r d'une courbe elliptique E et le comportement asymptotique du produit

$$\prod_{p \le X} \frac{N_p}{p},$$

où $N_p = |E(\mathbb{F}_p)|$ est le nombre de points de la courbe réduite modulo p. Intuitivement, plus le rang est grand, plus la courbe a de points rationnels, et donc plus elle a de points modulo p en moyenne, ce qui devrait faire diverger ce produit plus rapidement.

Sur la base de ces expériences numériques, ils formulèrent d'abord une version primitive :

Conjecture (BSD, version primitive, années 1960)**.** Soit E une courbe elliptique sur $\mathbb{Q}$ de rang r. Alors il existe une constante $C_E > 0$ telle que

$$\prod_{p \le X} \frac{N_p}{p} = C_E (\log X)^r + o((\log X)^r), \quad \text{quand } X \to \infty.$$

Cette intuition les conduisit à une formulation plus sophistiquée et plus profonde, faisant intervenir la fonction L de E. Nous donnons ici une description informelle de la fonction L de Hasse-Weil $L(E, s)$:

$$L(E, s) := \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s} = \prod_{p \text{ premier}} L_p(E, s)^{-1},$$

où $L_p(E, s)$ est un facteur local dépendant de $a_p(E) = p + 1 - N_p$.

On peut considérer cette fonction comme une généralisation de la fonction zêta de Riemann.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ premier}} \frac{1}{1 - p^{-s}}.$$

À partir de cette fonction L, leur conjecture originale peut être reformulée comme suit.

Conjecture (Conjecture de Birch et Swinnerton-Dyer, années 1960)**.** Soit E une courbe elliptique sur $\mathbb{Q}$. Alors l'ordre d'annulation de $L(E,s)$ en $s=1$ est égal au rang r de $E(\mathbb{Q})$:

$$\text{rang } E(\mathbb{Q}) = \text{ord}_{s=1} L(E,s).$$

Cette conjecture, d'une concision et d'une élégance remarquables, jette un pont entre l'algèbre et l'analyse au moyen d'une simple identité.

À l'époque, on ne savait pas si un prolongement analytique de cette fonction L était possible ; la conjecture supposait donc implicitement qu'un tel prolongement existait.

Pour que la conjecture BSD ait un sens, il faut d'abord savoir que $L(E,s)$ se prolonge analytiquement. Un progrès décisif vint d'une autre conjecture, formulée dans les années 1960 par **Yutaka Taniyama**, **Goro Shimura** et **André Weil**. Leur conjecture établit un pont entre les courbes elliptiques et les formes modulaires.

Soit E une courbe elliptique sur $\mathbb{Q}$. On associe la série

$$f_E(z) = \sum_{n=1}^{\infty} a_n(E) e^{2\pi i n z}, \quad z \in \mathbb{H},$$

où les $a_n(E)$ sont les coefficients de la fonction L avec $a_p(E) = p + 1 - N_p$ pour p premier.

Conjecture (Conjecture de modularité, Taniyama-Shimura-Weil, années 1960)**.** Soit E une courbe elliptique sur $\mathbb{Q}$, alors la fonction holomorphe $f_E(z)$ est une forme modulaire de poids 2.

Rappelons la conjecture de Birch et Swinnerton-Dyer (BSD) :

$$\text{rank}\, E(\mathbb{Q}) = \text{ord}_{s=1}\, L(E,s).$$

Pour $\text{Re}(s) > 3/2$, cette fonction est absolument convergente (vers une fonction analytique).

Supposons que E soit *modulaire*, c'est-à-dire qu'elle vérifie la conjecture de modularité. Alors la fonction L

$$L(E,s) = L(f_E, s)$$

admet un prolongement analytique à une fonction entière sur $s \in \mathbb{C}$, et satisfait une *équation fonctionnelle* centrée en $s=1$. Dans ce cas, le membre droit de la conjecture de BSD est bien défini.

En 1993, Wiles annonça une preuve de la conjecture de modularité pour les courbes elliptiques à réduction semi-stable, ce qui aurait suffi pour établir le dernier théorème de Fermat. Malheureusement, la preuve contenait une lacune sérieuse. En 1995, Wiles et Taylor publièrent un article conjoint, qui corrigea la faille de la preuve originale de Wiles [13]. Cela confirma finalement le dernier théorème de Fermat, un problème resté ouvert pendant près de 350 ans. C'est une autre histoire – passionnante – mais que nous n'aborderons pas ici.

Le résultat de Wiles et Taylor a ensuite été étendu à toutes les courbes elliptiques sur $\mathbb{Q}$ par **Christophe Breuil**, **Brian Conrad**, **Fred Diamond** et **Richard Taylor** [2] en 1999. Dès lors, le théorème de modularité est pleinement établi, ce qui confère à la conjecture de Birch et Swinnerton–Dyer un statut de conjecture rigoureusement formulée.

5.2 Le Théorème de Coates-Wiles

Dans cette section, nous présentons le premier résultat important concernant la conjecture de Birch et Swinnerton-Dyer : le théorème de Coates-Wiles, qui traite du cas où le rang de la courbe elliptique est zéro.

Une condition technique importante de ce théorème est que la courbe elliptique possède une *multiplication complexe* (CM). Cela signifie que son anneau d'endomorphismes est plus riche que d'habitude : non seulement on peut multiplier un point par un entier n (l'application $P \mapsto nP$), mais il existe également des endomorphismes « supplémentaires » correspondant à la multiplication par des nombres algébriques non réels. Concrètement, pour une courbe à CM, cet anneau contient l'anneau des entiers d'un corps quadratique imaginaire. Ces courbes, plus symétriques, sont plus accessibles aux calculs analytiques et arithmétiques ; c'est pourquoi elles ont servi de terrain d'essai pour les premières attaques sur la conjecture BSD.

Théorème 5.1 (Coates et Wiles, 1977)**.** *Soit E une courbe elliptique sur $\mathbb{Q}$ ayant multiplication complexe. Si $L(E,1) \neq 0$, alors le rang de $E(\mathbb{Q})$ est nul.*

En d'autres termes, sous l'hypothèse CM, si la fonction L ne s'annule pas en $s = 1$, alors la courbe n'a qu'un nombre fini de points rationnels (le rang est zéro). Ce résultat fournit une implication partielle de la conjecture BSD ($L(E,1) \neq 0 \Rightarrow \text{rang} = 0$) pour les courbes à CM. La preuve utilise de manière cruciale la construction de points de Heegner et des techniques de théorie d'Iwasawa.

5.3 La Formule de Gross-Zagier

Dans cette section, nous présentons le résultat central de notre récit - la formule démontrée par **Benedict Gross** et **Don Zagier** en 1986.

Avant d'énoncer le théorème, nous devons d'abord étudier les points de Heegner sur les courbes modulaires. Heegner avait une manière systématique de construire des points rationnels sur $E(\mathbb{Q})$. Dans les années 1960–70, Birch a reformulé la construction de Heegner dans le langage moderne, et a également effectué des calculs numériques à son sujet. Si E est *modulaire* (c'est-à-dire si f_E est une forme modulaire comme dans la conjecture de modularité), on peut paramétrer E par des fonctions modulaires, comme dans la construction originale de Heegner. Birch a remplacé cette construction par une application algébrique élégante $X_0(N) \to E$.

La *hauteur de Néron-Tate* $\hat{h}(P)$: $E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ est une mesure arithmétique de la « taille » d'un point rationnel qui satisfait :

$$\hat{h}(P) = 0 \Longleftrightarrow P \text{ est un point de torsion dans } E(\mathbb{Q}).$$

Gross et Zagier établirent une formule reliant la hauteur d'un point de Heegner à la dérivée première de la fonction L.

Théorème 5.2 (Formule de Gross-Zagier, version simplifiée, 1986)**.** *Soit E une courbe elliptique modulaire et P un point de Heegner sur E. Supposons $L(E,1) = 0$. Alors il existe une constante explicite $\alpha_E > 0$ (liée aux périodes de E) telle que*

$$\hat{h}(P) = \alpha_E \cdot L'(E,1).$$

D'après la formule de Gross-Zagier, on obtient le résultat suivant :

$$\begin{aligned} \text{ord}_{s=1} L(E,s) = 1 &\Leftrightarrow L'(E,1) \neq 0 \Leftrightarrow \hat{h}(P) \neq 0 \\ &\Leftrightarrow P \text{ n'est pas un point de torsion } \Rightarrow \text{rank}(E(\mathbb{Q})) \geq 1. \end{aligned}$$

Ce résultat marque une étape cruciale vers la validation de la conjecture BSD dans le cas général des rangs non nuls.

Peu après Gross et Zagier, **Victor Kolyvagin** [7] développa la théorie des *systèmes d'Euler* pour exploiter pleinement l'information fournie par les points de Heegner.

Théorème 5.3 (Kolyvagin, 1988)**.** *Sous les conditions de Théorème 5.2, si P n'est pas un point de torsion, alors* $\text{rank}(E(\mathbb{Q})) = 1$.

La formule de Gross-Zagier, jointe au travail de Kolyvagin, a permis de démontrer la conjecture BSD pour les courbes de rang analytique 0 ou 1 (c'est-à-dire lorsque $\text{ord}_{s=1} L(E,s) \leq 1$), sous condition que E soit modulaire (on sait maintenant que toute courbe elliptique sur $\mathbb{Q}$ est modulaire). Il convient de souligner que, grâce aux travaux de Bhargava, Skinner et Zhang [1], on sait aujourd'hui qu'environ deux tiers de toutes les courbes elliptiques sur $\mathbb{Q}$ appartiennent à cette classe et vérifient donc la conjecture BSD. Ces résultats représentent l'un des succès les plus éclatants de la théorie des nombres du XXI$^{\text{e}}$ siècle.

Jusqu'à présent, nous ne savons presque rien du cas où $\text{ord}_{s=1} L(E,s) > 1$.

5.4 Évolutions du XXIe siècle

Le programme initié par Gross et Zagier n'a cessé de s'étendre et de s'approfondir au cours du XXIe siècle. L'une des généralisations majeures a été obtenue en 2012 par **Xinyi Yuan**, **Shou-Wu Zhang** et **Wei Zhang**, qui ont étendu la formule de Gross-Zagier aux variétés abéliennes de type GL(2) [14]. Ce travail s'appuie sur le travail antérieure de Shou-Wu Zhang ainsi que sur des idées de Gross, Kudla et Waldspurger. Cette version étendue a permis à **Ye Tian** de réaliser la même année une percée significative sur le problème des nombres congruents en produisant une famille explicite de nombres congruents d'un type nouveau [12].

Parallèlement, le cadre conjectural s'est considérablement élargi. Dans les années 2000–2010, **Benedict Gross** et **Dipendra Prasad**, puis **Wee Teck Gan**, **Benedict Gross** et **Dipendra Prasad**, ont formulé une conjecture de type Gross-Zagier pour les groupes unitaires de dimension supérieure, visant à relier des périodes automorphes à des dérivées de fonctions L [5]. Pour attaquer cette conjecture arithmétique, **Wei Zhang** a proposé une version arithmétique de la formule des traces de Jacquet–Rallis et a démontré le lemme fondamental relatif arithmétique, établissant ainsi les bases d'un programme de preuve [16].

Une avancée spectaculaire a eu lieu en 2017, lorsque **Zhiwei Yun** et **Wei Zhang** ont établi la première formule de type Gross-Zagier pour les dérivées d'ordre supérieur (dite « formule de dérivées hautes ») sur les corps de fonctions [15]. Ce résultat, qui dépasse largement le cadre originel de la formule de Gross-Zagier, ouvre la voie à l'étude des cas où l'ordre d'annulation de la fonction L est supérieur à 1, un domaine qui reste encore largement mystérieux sur les corps de nombres.

Ces développements récents montrent que l'héritage de la formule de Gross-Zagier continue de fertiliser l'interface entre la géométrie arithmétique, la théorie des formes automorphes et la théorie des nombres, en fournissant un paradigme puissant pour relier des objets algébriques à des objets analytiques.

6 CONCLUSION

Le chemin parcouru, du problème des nombres congruents à la formule de Gross-Zagier, illustre la puissance de l'unification des idées en mathématiques. Des questions diophantiennes concrètes ont motivé le développement de théories abstraites – courbes elliptiques, formes modulaires, fonctions L – qui à leur tour ont permis de résoudre des problèmes anciens et d'en poser de nouveaux.

La formule de Gross-Zagier se situe au carrefour de l'arithmétique, de l'analyse et de la géométrie algébrique. Elle est le fruit d'un siècle de progrès, depuis les intuitions de Heegner jusqu'aux techniques raffinées de cohomologie galoisienne et de théorie des formes modulaires. Bien que la conjecture BSD dans sa généralité reste ouverte, les résultats partiels obtenus grâce à cette formule et à ses généralisations constituent l'une des plus belles réussites des mathématiques contemporaines.

Cette épopée historique témoigne de la nature cumulative et collaborative de la recherche mathématique, où chaque génération bâtit sur les travaux de ses prédécesseurs pour repousser les frontières de la connaissance.

RÉFÉRENCES

[1] Manjul Bhargava, Christopher Skinner, and Wei Zhang. A majority of elliptic curves over $\mathbb{Q}$ satisfy the birch and swinnerton-dyer conjecture. *arXiv :1407.1826*, 2014.

[2] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4) :843–939, 2001.

[3] Leonard Eugene Dickson. *History of the Theory of Numbers*, volume 1. University of Pennsylvania Press, 1999.

[4] Gerd Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones mathematicae*, 73(3) :349–366, 1983.

[5] Wee Teck Gan, Benedict H Gross, and Dipendra Prasad. Symplectic local root numbers, central critical l-values, and restriction problems in the representation theory of classical groups. *Astérisque*, pages No–pp, 2011.

[6] Kurt Heegner. Diophantische analysis und modulfunktionen. *Mathematische Zeitschrift*, 56(3) :227–253, 1952.

[7] Viktor Alexandrovich Kolyvagin. Finiteness of and for a subclass of weil curves. *Mathematics of the USSR-Izvestiya*, 32(3) :523, 1989.

[8] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1) :33–186, 1977.

[9] Louis Joel Mordell. On the rational resolutions of the indeterminate equations of the third and fourth degree. In *Proc. Cambridge Phil. Soc.*, volume 21, pages 179–192, 1922.

[10] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 2013.

[11] Harold M Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Mathematical Journal*, 14(1) :1–27, 1967.

[12] Ye Tian. Congruent numbers and heegner points. *Cambridge Journal of Mathematics*, 2(1) :117–161, 2014.

[13] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141(3) :443–551, 1995.

[14] Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang. *The gross-zagier formula on shimura curves*. Number 184. Princeton University Press, 2013.

[15] Zhiwei Yun and Wei Zhang. Shtukas and the taylor expansion of l-functions. *Annals of Mathematics*, 186(3) :767–911, 2017.

[16] Wei Zhang. On arithmetic fundamental lemmas. *Inventiones mathematicae*, 188(1) :197–252, 2012.