

MATHÉMATIQUES

Le problème des nombres congruents

Pierre Colmez

Résumé. — Ce texte est une introduction à la conjecture de Birch et Swinnerton-Dyer, à travers le problème des nombres congruents (à quelle condition un entier donné est-il l'aire d'un triangle rectangle à côtés rationnels?) qui est probablement le plus vieux problème non résolu à ce jour. C'est une version commentée d'un exposé donné, en mai 2005, au séminaire des élèves de l'École Polytechnique.

Introduction

Définition 1. *Un entier D , sans facteur carré (divisible par le carré d'aucun nombre premier), est congruent, s'il existe un triangle rectangle de côtés rationnels dont l'aire est D ; autrement dit, si et seulement si il existe $a, b, c \in \mathbf{Q}$ avec $a^2 + b^2 = c^2$ et $D = \frac{ab}{2}$.*

Pour étudier les nombres congruents, on peut commencer par étudier l'ensemble des triangles rectangles à côtés rationnels, c'est-à-dire résoudre l'équation $a^2 + b^2 = c^2$ en nombres rationnels. On pose $u = \frac{a}{c}$ et $v = \frac{b}{c}$, et on est ramené à trouver les points rationnels sur le cercle $u^2 + v^2 = 1$ avec $u > 0$ et $v > 0$. Pour cela, on note t la pente de la droite joignant (u, v) à $(-1, 0)$, dont l'équation est donc $v = t(u + 1)$; on a $t \in \mathbf{Q}$ et $(u, v) = (\frac{1-t^2}{t^2+1}, \frac{2t}{t^2+1})$. En conclusion, $a, b, c \in \mathbf{Q}$ sont les côtés d'un triangle rectangle si et seulement si il existe $t \in \mathbf{Q}$, $0 < t < 1$, tel que $a = \frac{1-t^2}{t^2+1}c$ et $b = \frac{2t}{t^2+1}c$. En posant $x = -t$ et $y = \frac{t^2+1}{c}$, ce qui précède permet presque¹ de démontrer le résultat suivant.

Proposition 2. *Si D est un entier positif sans facteur carré, alors les conditions suivantes sont équivalentes :*

- (i) D est congruent
- (ii) L'équation $Dy^2 = x^3 - x$ a une solution dans \mathbf{Q}^2 avec $y \neq 0$.

Déterminer si un entier est congruent ou pas, est un problème très ancien et très difficile. On a par exemple le résultat suivant « conjecturé » par FIBONACCI (1175-1240).

Théorème 3 (FERMAT (1601-1665)). *1 n'est pas un nombre congruent.*

C'est une des nombreuses utilisations que FERMAT a trouvées pour sa méthode² de « la descente infinie ». Remarquons que si a, b, c sont des entiers non nuls vérifiant $a^4 - b^4 = c^4$, et si $x = \frac{a^2}{b^2}$, $y = \frac{ac^2}{b^3}$, alors $y = x^3 - x$. Le fait que 1 n'est pas congruent implique donc le théorème de Fermat³ pour l'exposant 4.

Exemple 4 (ZAGIER). L'entier 157 est congruent, mais le triangle (a, b, c) le plus simple d'aire 157 est

$$a = \frac{6803298487826435051217540}{411340519227716149383203}, \quad b = \frac{411340519227716149383203}{21666555693714761309610},$$

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Cet exemple montre que la chasse aux triangles rectangles à côtés rationnels d'aire D risque d'être un peu acrobatique... Le résultat suivant de TUNNELL (1983) n'en est que plus remarquable.

Théorème 5. *Soit D un entier impair sans facteur carré. Si D est congruent, alors*

$$|\{x, y, z \in \mathbf{Z}, 2x^2 + y^2 + 8z^2 = D\}| = 2 \cdot |\{x, y, z \in \mathbf{Z}, 2x^2 + y^2 + 32z^2 = D\}|. \quad (*)$$

Réciproquement, si D vérifie (), et si (une forme faible de) la conjecture de Birch et Swinnerton-Dyer est vraie, alors D est congruent.*

Il y a un résultat similaire pour D pair. Comme il est très facile de décider si D vérifie ou non (*), cela fournit un critère effectif permettant de décider qu'un nombre donné est non congruent, ou (sous Birch et Swinnerton-Dyer) congruent, et ce, sans exhiber de triangle rectangle d'aire D . Un entier congru à 5 ou 7 modulo 8 vérifie (*) car les deux ensembles sont vides, mais on ne sait pas montrer que cela implique que D est congruent...

Comme le lecteur le constatera, la démonstration de ce théorème emprunte des chemins très détournés (ce qui en fait le charme); on peut légitimement se demander si une preuve plus directe ne serait pas possible, maintenant qu'on connaît la réponse.

1. Arithmétique des courbes elliptiques

Si C est une conique, on peut étudier l'ensemble $C(\mathbf{Q})$ des points à coordonnées rationnelles de C comme on l'a fait pour le cercle. On trouve un point $P \in C(\mathbf{Q})$ sur la conique et on paramètre les points de la conique par la pente d'une droite variable passant par P . Cette stratégie ne marche plus pour une courbe C donnée par une équation de degré 3 (comme la courbe C_D d'équation $Dy^2 = x^3 - x$) car, si on coupe par une droite passant par un point de $C(\mathbf{Q})$, et qu'on élimine y entre les deux équations, on obtient une équation de degré 3 en x dont on sait seulement qu'une des solutions est rationnelle; les deux autres vivent donc, en général, dans une extension quadratique de \mathbf{Q} , mais pas dans \mathbf{Q} . Par contre, si on prend une droite passant par deux points rationnels de C ou tangente à un point rationnel de C , alors on obtient une équation dont deux des solutions (ou une solution double) sont rationnelles; comme la somme des racines est aussi rationnelle, cela montre que cette droite recoupe C en un point rationnel.

Une *courbe elliptique* E sur un corps K est une courbe d'équation $y^2 = P(x)$, avec $P \in K[X]$, de degré 3, sans racine double⁴. On note $E(K)$ l'ensemble des solutions dans K^2 de $y^2 = P(x)$, et $\overline{E}(K) = E(K) \cup \{\infty\}$, avec la convention qu'une droite passe par ∞ si et seulement si elle est verticale⁵. On munit $\overline{E}(K)$ d'une loi de composition $+$ qui en fait un groupe commutatif⁶ avec ∞ comme élément neutre et $P + Q + R = \infty$ si et seulement si (P, Q, R) sont alignés (avec

les conventions évidentes si deux ou trois des points sont confondus ; en particulier, P est d'ordre 2 si et seulement si ∞ appartient à la tangente à E en P , c'est-à-dire si et seulement si $y = 0$; de même, P est d'ordre 3 si et seulement si la tangente en P à E a un contact d'ordre 3).

Théorème 6. *Si E est une courbe elliptique sur \mathbf{Q} , le groupe $\overline{E}(\mathbf{Q})$ est engendré par un nombre fini d'éléments ; il est donc isomorphe à $\overline{E}(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^{r(E)}$, où $\overline{E}(\mathbf{Q})_{\text{tors}}$, sous-groupe des points d'ordre fini⁷, est un groupe fini, et $r(E) \in \mathbf{N}$.*

Ce résultat, conjecturé par POINCARÉ vers 1900, a été démontré par MORDELL en 1922 en adaptant⁸ la méthode de la descente infinie de FERMAT ; c'est un cas particulier du célèbre théorème de Mordell-Weil. Le groupe $\overline{E}(\mathbf{Q})_{\text{tors}}$ se calcule très facilement ; par contre la détermination du rang $r(E)$ et des générateurs de $\mathbf{Z}^{r(E)}$ est très délicate. À ce jour, il n'y a pas d'algorithme⁹ dont on puisse prouver qu'il va permettre de les déterminer, ce qui ne nous arrange pas en ce qui concerne le problème des nombres congruents, mais la conjecture de Birch et Swinnerton-Dyer, dont il sera question plus loin, fournirait un tel algorithme si elle était démontrée.

Exemple 7. On note C_D la courbe elliptique d'équation $Dy^2 = x^3 - x$. Alors $Q_1 = (-1, 0)$, $Q_2 = (0, 0)$ et $Q_3 = (1, 0)$ sont d'ordre 2, et $\overline{C}_D(\mathbf{Q})_{\text{tors}} = \{\infty, Q_1, Q_2, Q_3\}$. En conséquence, D est congruent si et seulement si $r(C_D) \geq 1$.

2. L'heuristique de BIRCH et SWINNERTON-DYER

Si p est un nombre premier, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est un corps. Si $r = \frac{a}{b} \in \mathbf{Q}$ et p ne divise pas b , on peut voir r comme un élément de \mathbf{F}_p en réduisant a et b modulo p (i.e. en prenant le quotient des images de a et b dans \mathbf{F}_p , ce qui ne dépend pas des choix de a et b). En particulier, si E est une courbe elliptique sur \mathbf{Q} d'équation $y^2 = P(x)$, on peut aussi considérer E comme une courbe elliptique sur \mathbf{F}_p pour tous les bons nombres premiers (ceux ne divisant ni les dénominateurs des coefficients de P , ni le numérateur de son discriminant (note 4)).

Si E est une courbe elliptique sur \mathbf{F}_p , on a trivialement, $|\overline{E}(\mathbf{F}_p)| \leq 2p + 1$, mais on dispose du résultat plus précis suivant.

Théorème 8 (HASSE). *Si E est une courbe elliptique sur \mathbf{F}_p , et si $a_p = p + 1 - |\overline{E}(\mathbf{F}_p)|$, alors $|a_p| \leq 2\sqrt{p}$*

L'idée de BIRCH et SWINNERTON-DYER (1960-1965), est que, si $r(E) \geq 1$, alors il devrait y avoir en moyenne plus de points dans $E(\mathbf{F}_p)$ que si $r(E) = 0$, à cause de la réduction modulo p des éléments de $E(\mathbf{Q})$. Comme ce nombre de points est à peu près p d'après le théorème de Hasse, le produit $\prod_p \frac{p}{|\overline{E}(\mathbf{F}_p)|}$ devrait avoir des chances de diverger (d'être nul), si $r(E) \geq 1$, et de converger, si $r(E) = 0$. Pour donner un sens à tout ceci, nous allons avoir besoin de passer par les fonctions holomorphes.

3. Fonctions holomorphes

Définition 9. *Si Ω est un ouvert connexe de \mathbf{C} , on dit que $f : \Omega \rightarrow \mathbf{C}$ est holomorphe sur Ω , si pour tout $z_0 \in \Omega$, il existe $r > 0$ et une suite $(a_n(z_0))_{n \in \mathbf{N}}$ de nombres complexes tels que $f(z) = \sum_{n=0}^{+\infty} a_n(z_0)(z - z_0)^n$ si $z \in \Omega$ et $|z - z_0| < r$.*

Les fonctions holomorphes ont des propriétés miraculeuses et représentent un petit paradis (bien caché des taupins et des polytechniciens ; on se demande bien pourquoi...). En particulier, elles vérifient les propriétés suivantes :

(H0) Si f atteint son maximum en un point de Ω , alors f est constante. (*Principe du maximum*).

(H1) Si f_n est une suite de fonctions holomorphes sur Ω convergeant uniformément sur tout compact, alors la limite est holomorphe sur Ω .

(H2) Si $f(x, s) : X \times \Omega \rightarrow \mathbf{C}$ est sommable en x , holomorphe en s , et s'il existe g avec $\int_X |g(x)| dx < +\infty$ et $|f(x, s)| \leq |g(x)|$ quels que soient x et s , alors $F(s) = \int_X f(x, s) dx$ est holomorphe sur Ω .

(H3) Si f et g sont deux fonctions holomorphes sur Ω telles qu'il existe un compact $K \subset \Omega$ sur lequel $f - g$ a une infinité de zéros, alors $f = g$ sur Ω tout entier.

Si $\Omega \subset \Omega'$ sont connexes et si f est holomorphe sur Ω , il est en général impossible de prolonger f en une fonction holomorphe sur Ω' . Quand c'est possible, un tel prolongement est unique d'après la propriété (H3), et est appelé *prolongement analytique* de f à Ω' .

Exemple 10. La fonction gamma d'Euler. Si $\operatorname{Re}(s) > 0$, l'intégrale $\Gamma(s) = \int_0^{+\infty} e^{-t} t^s \frac{dt}{t}$ converge. La fonction Γ est holomorphe et ne s'annule pas sur le demi-plan $\operatorname{Re}(s) > 0$, et y vérifie l'équation fonctionnelle $\Gamma(s+1) = s\Gamma(s)$. On la prolonge en une fonction holomorphe sur $\mathbf{C} - \{0, -1, -2, \dots\}$ en posant $\Gamma(s) = \frac{\Gamma(s+n)}{s(s+1)\dots(s+n-1)}$, où $n \in \mathbf{N}$ est choisi de telle sorte que $\operatorname{Re}(s) + n > 0$. La fonction $\frac{1}{\Gamma(s)}$ est alors holomorphe sur \mathbf{C} avec des zéros simples aux entiers négatifs.

Exemple 11. La fonction thêta. On note $\mathcal{H} = \{z \in \mathbf{C}, \operatorname{Im}(z) > 0\}$ le demi-plan de Poincaré. On pose $q = e^{2i\pi z}$, et on définit $\Theta : \mathcal{H} \rightarrow \mathbf{C}$ par

$$\Theta(z) = \sum_{n \in \mathbf{Z}} q^{n^2}.$$

On a $\Theta(z+1) = \Theta(z)$ et $\sqrt{\frac{z}{2i}} \Theta\left(\frac{z}{2i}\right) = \Theta\left(\frac{-1}{2z}\right)$ d'après la formule de Poisson¹⁰.

Exemple 12. La fonction zêta de Riemann. Si $\operatorname{Re}(s) > 1$, la série

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1}$$

converge sur le demi-plan $\operatorname{Re}(s) > 1$, et y définit une fonction holomorphe d'après la propriété (H1). On montre¹¹ que cette fonction admet un prolongement analytique à $\mathbf{C} - \{1\}$, ce qui permet d'écrire les formules suivantes qui font la joie des théoriciens des nombres et des physiciens théoriciens.

$$\begin{aligned} 1 + 1 + 1 + 1 + 1 + \dots &= \zeta(0) = -1/2, \\ 1 + 2 + 3 + 4 + 5 + \dots &= \zeta(-1) = -1/12, \\ 1 + 4 + 9 + 16 + 25 + \dots &= \zeta(-2) = 0, \\ 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \dots &= \exp(-\zeta'(0)) = \sqrt{2\pi}. \end{aligned}$$

4. Fonction L d'une courbe elliptique

Soit E une courbe elliptique sur \mathbf{Q} . Si p est un bon nombre premier, soit a_p l'entier défini par $a_p = 1 + p - |\overline{E}(\mathbf{F}_p)|$. On définit la¹² fonction $L(E, s)$, et des entiers a_n , pour $n \in \mathbf{N} - \{0\}$ par

$$L(E, s) = \prod_{p \text{ bon}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

Il est facile de voir que le produit converge pour $\text{Re}(s) > 2$, et même $\text{Re}(s) > \frac{3}{2}$ si on utilise la majoration $|a_p| \leq 2\sqrt{p}$ de Hasse, et définit une fonction holomorphe sur ce demi-plan.

Théorème 13. *La fonction $L(E, s)$ admet un prolongement analytique à \mathbf{C} tout entier.*

Ce résultat a été conjecturé par HASSE vers 1935; c'est un cas particulier de la conjecture de Hasse-Weil. Le premier résultat dans sa direction est celui, dû à WEIL, de la famille¹³ des courbes C_D . SHIMURA (1958), inspiré par des travaux d'EICHLER (1954), a démontré de nombreux cas de cette conjecture en utilisant la théorie des formes modulaires dont il sera question plus loin. Le pas le plus important a été accompli par WILES en 1994, dans sa quête de la démonstration du théorème de Fermat, qui a démontré cette conjecture dans le cas où E est d'équation $y^2 = P(x)$ et P a toutes ses racines dans \mathbf{Q} . Le cas général a finalement été résolu par BREUIL, CONRAD, DIAMOND et TAYLOR en 1999.

La quantité $\prod_{p \text{ bon}} \frac{p}{|\overline{E}(\mathbf{F}_p)|}$ apparaissant dans l'heuristique de BIRCH et SWINNERTON-DYER est, au moins formellement, égale à $L(E, 1)$, et leur heuristique devient :

Conjecture 14 (Birch et Swinnerton-Dyer (forme faible)). « $r(E) \geq 1$ » si et seulement si « $L(E, 1) = 0$ ».

On peut préciser cet énoncé¹⁴. Notons $r_\infty(E)$ l'ordre du zéro en $s = 1$ de $L(E, s)$. La conjecture de Birch et Swinnerton-Dyer prend alors la forme suivante.

Conjecture 15 (Birch et Swinnerton-Dyer). *On a l'égalité $r(E) = r_\infty(E)$.*

C'est sous cette forme que le problème vaut un million de dollar. Il y a en fait une forme plus précise¹⁵ de cette conjecture (donnant une formule pour la quantité conjecturalement non nulle $\lim_{s \rightarrow 1} (s - 1)^{-r(E)} L(E, s)$), et plus générale (\mathbf{Q} peut être remplacé par une extension finie, ou même par des corps de caractéristique p , extensions finies du corps $\mathbf{F}_p(T)$).

Les résultats sont peu nombreux; ce sont les suivants.

- COATES et WILES (1977) ont démontré que, si $E = C_D$, ou plus généralement si E est une courbe elliptique définie sur \mathbf{Q} à multiplication complexe¹⁶, alors « $L(E, 1) \neq 0$ » \Rightarrow « $r(E) = 0$ ».

- GROSS et ZAGIER (1983) ont donné une formule explicite¹⁷ pour $L'(E, 1)$ en termes de certains points rationnels sur E , dits « de Heegner », et qui sont construits de manière purement analytique (ce sont ces points qui permettent d'amuser la galerie en exhibant des triangles rectangles à côtés rationnels avec un

nombre astronomique de chiffres). Comme conséquence, ils obtiennent l'implication : « $r_\infty(E) = 1$ » \Rightarrow « $r(E) \geq 1$ ».

• KOLYVAGIN (1989) a démontré, en utilisant ces points de Heegner, l'implication suivante « $r_\infty(E) \leq 1$ » \Rightarrow « $r(E) = r_\infty(E)$ ».

C'est tout ! On est dans la situation paradoxale où plus il est censé y avoir de points rationnels ($r_\infty(E) \geq 2$), moins on sait en construire... Mentionnons quand-même, qu'en général, le rang $r(E)$ est égal à 0 ou 1, mais qu'on connaît des courbes avec $r(E) \geq 24$, et il y a tout lieu de croire que $r(E)$ peut prendre des valeurs arbitrairement grandes.

5. La stratégie de TUNNELL

La théorème de Coates-Wiles mentionné ci-dessus fournit un critère pour que D ne soit pas congruent : il suffit que $L(C_D, 1) \neq 0$. Réciproquement, si la conjecture de Birch et Swinnerton-Dyer est vraie (même sous sa forme faible), alors la nullité de $L(C_D, 1)$ implique que D est congruent. C'est le point de départ de la démonstration du théorème de Tunnell. Le problème est donc de calculer $L(C_D, 1)$ et de décider si ce nombre est nul ou pas. Il y a deux problèmes sérieux qui se posent : le produit définissant $L(C_D, 1)$ converge beaucoup trop lentement (s'il converge..., cf. note 1) pour qu'on puisse l'utiliser pour le calcul de $L(C_D, 1)$, et de toute façon, il est impossible de prouver qu'un nombre réel est nul en le calculant de manière approchée, sauf si on sait par ailleurs qu'il s'agit d'un entier. La solution que TUNNELL apporte à ces deux problèmes est particulièrement élégante.

Théorème 16 (TUNNELL). Soit $\Omega = \int_1^{+\infty} \frac{dx}{\sqrt{x^3-x}}$, et soit $\sum_{n=0}^{+\infty} b_n q^n$ le développement de

$$\Theta(z) \cdot \Theta(2z) \cdot (2\Theta(32z) - \Theta(8z)),$$

alors, si D est impair (il y a une formule similaire pour les entiers pairs) sans facteur carré,

$$L(C_D, 1) = \frac{\Omega}{16\sqrt{D}} \cdot b_D^2.$$

Comme b_D est la différence des deux termes apparaissant dans la condition (*) du th. 5, cela explique comment ledit théorème peut se déduire du théorème de Coates-Wiles. La démonstration du théorème 16 repose sur la théorie des formes modulaires dont il est question au § suivant.

6. Formes modulaires

Si f est holomorphe sur \mathcal{H} et vérifie $f(z+1) = f(z)$, alors f a un développement de Fourier (q -développement)

$$f(z) = \sum_{n \in \mathbf{Z}} a_n q^n, \quad \text{avec } q = e^{2i\pi z}.$$

On dit que f est à croissance lente à l'infini si $a_n = 0$ pour tout $n < 0$ et s'il existe $C \in \mathbf{R}$ tel que $a_n = O(n^C)$.

Si N est un entier, on note $\Gamma_0(N)$ le sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ des $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec c divisible par N . On note $T = \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}$.

Définition 17. Si $k \in \frac{1}{2}\mathbf{N}$ et $j : \Gamma_0(N) \rightarrow \{\text{racines de l'unité}\}$ vérifie $j(T) = 1$, l'espace $M_k(\Gamma_0(N), j)$ des formes modulaires de poids k et type j pour $\Gamma_0(N)$ est l'espace des fonctions f , holomorphes sur \mathcal{H} , vérifiant

$$f\left(\frac{az+b}{cz+d}\right) = j\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(cz+d)^k f(z), \quad \text{quels que soient } z \in \mathcal{H} \text{ et } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

et qui sont à croissance lente à l'infini.

Remarque 18. (i) Il n'est pas du tout clair que de telles formes existent ; et de fait, il faut choisir correctement la fonction j pour $M_k(\Gamma_0(N), j)$ soit non nul.

(ii) $M_k(\Gamma_0(N), j)$ est un \mathbf{C} -espace vectoriel de dimension $\leq 1 + \frac{Nk}{12} \prod_{p|N} (1 + \frac{1}{p})$.

(iii) Les formes modulaires ont un don d'ubiquité assez remarquable. On les rencontre en théorie des nombres¹⁸, en combinatoire ou en physique théorique, bien que ce soient des objets définis de manière purement analytique.

Exemple 19. La fonction Θ est une forme modulaire de poids $\frac{1}{2}$ pour $\Gamma_0(4)$ et un j un peu compliqué (cela suit facilement des deux équations fonctionnelles déjà mentionnées). Plus généralement, si P est un polynôme homogène de degré d en n_1, \dots, n_r , et si Q est une forme quadratique définie positive à coefficients entiers, alors la fonction thêta $\Theta_{Q,P}(z) = \sum_{(n_1, \dots, n_r) \in \mathbf{Z}^r} P(n_1, \dots, n_r) q^{Q(n_1, \dots, n_r)}$ est une forme modulaire de poids $d + \frac{r}{2}$.

Si $t \in \mathbf{C}$ et $n \in \mathbf{N} - \{0\}$, soit $\sigma_t(n) = \sum_{d|n, d \geq 1} d^t$.

Exemple 20. (i) Si k est un entier pair ≥ 3 , on définit¹⁹ la série d'Eisenstein G_k par $G_k(z) = \frac{(k-1)!}{2 \cdot (2i\pi)^k} \sum_{m,n} \frac{1}{(mz+n)^k}$. C'est un élément de $M_k(\mathbf{SL}_2(\mathbf{Z}), 1)$; son q -développement est $G_k = \frac{(k-1)! \zeta(k)}{(2i\pi)^k} + \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n$.

(ii) Pour $k = 2$, la série ci-dessus ne converge plus, mais on peut définir une série d'Eisenstein $G_2^*(z) = \lim_{s \rightarrow 0} \frac{1}{2 \cdot (2i\pi)^2} \sum_{m,n} \frac{1}{(mz+n)^k} \cdot \frac{y^s}{|cz+d|^{2s}}$, qui vérifie la loi de transformation pour appartenir à $M_2(\mathbf{SL}_2(\mathbf{Z}), 1)$, mais n'est pas holomorphe (elle n'en est pas très loin). Son développement de Fourier est donné par

$$G_2^*(z) = \frac{1}{8\pi y} + \frac{\zeta(2)}{(2i\pi)^2} + \sum_{n=1}^{+\infty} \sigma_1(n) q^n.$$

Comme échauffement pour le théorème de Tunnell, mentionnons l'identité de JACOBI (1829) :

$$4G_2^*(4z) - G_2^*(z) = \frac{3\zeta(2)}{(2i\pi)^2} \Theta^4,$$

qui se démontre en constatant que les deux membres appartiennent à $M_2(\Gamma_0(4), 1)$ qui est de dimension 2, et que la différence est divisible par q^2 . On en tire, en comparant les q -développements, une forme effective du théorème des 4 carrés de LAGRANGE (1770).

$$|\{(a, b, c, d) \in \mathbf{Z}^4, a^2 + b^2 + c^2 + d^2 = n\}| = 8 \sum_{d|n, 4 \nmid d} d.$$

7. Courbes elliptiques et formes modulaires

Théorème 21. *Si E est une courbe elliptique définie sur \mathbf{Q} et $L(E, s) = \sum_{n=1}^{+\infty} a_n n^{-s}$, alors $f = \sum_{n=1}^{+\infty} a_n q^n \in M_2(N_E, 1)$, où N_E est un entier explicite ne dépendant que des p mauvais.*

Autrement dit, *une courbe elliptique définie sur \mathbf{Q} est modulaire*. Ce résultat, conjecturé de manière vague par TANIYAMA en 1955, et précisé par WEIL en 1966 suite aux travaux de SHIMURA sus-mentionnés, est celui que démontrent WILES²⁰ et BREUIL-CONRAD-DIAMOND-TAYLOR. Le prolongement analytique de $L(E, s)$ s'en déduit en utilisant la formule (cf. note 1)

$$L(E, s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{+\infty} f(iy) y^s \frac{dy}{y},$$

ce qui permet d'utiliser les propriétés analytiques de f pour étudier $L(E, s)$. C'est un cas particulier de la philosophie de LANGLANDS sur les fonctions L arithmétiques (elle devraient provenir de *formes automorphes*, généralisations des formes modulaires, et donc avoir des tas de propriétés miraculeuses). Dans le cas de la courbe C_D , la forme modulaire que l'on obtient est une combinaison linéaire de fonctions thêta.

La modularité d'une courbe elliptique E en fournit²¹ une description analytique en termes du demi-plan de Poincaré. Ceci est à la base de la construction des points de Heegner (ce sont les images²² des points $\tau \in \mathcal{H}$ solutions d'une équation du second degré à coefficients dans \mathbf{Q} qui, comme nous l'avons déjà mentionné, jouent un rôle essentiel dans la démonstration du résultat de KOLYVAGIN ($r(E) = r_\infty(E)$ si $r_\infty(E) \leq 1$); ce résultat n'est donc devenu valable pour toutes les courbes elliptiques sur \mathbf{Q} que depuis les travaux de WILES et BREUIL-CONRAD-DIAMOND-TAYLOR.

Une autre application de la modularité des courbes elliptiques est le résultat suivant qui permet, modulo un calcul numérique, de déterminer la valeur de $L(E, 1)$, ce qui fournit, modulo la conjecture de Birch et Swinnerton-Dyer (sous sa forme faible), un algorithme pour décider de l'existence de solutions en nombres rationnels pour une équation $y^2 = P(x)$, avec P de degré 3.

Corollaire 22 (MANIN-DRINFELD). *Si E est d'équation $y^2 = P(x)$, et si α est la plus grande racine réelle de P , alors*

$$\left(\int_\alpha^{+\infty} \frac{dx}{\sqrt{P(x)}} \right)^{-1} L(E, 1)$$

est un nombre rationnel de dénominateur explicite.

Le point de départ de la démonstration du théorème 16 est un théorème de WALDSPURGER (1979). Si $f = \sum_{n=1}^{+\infty} a_n q^n \in M_{2k}(\Gamma_0(N), 1)$, k entier, si D est sans facteur carré et premier à N , et si χ_D est le caractère de Legendre (cf. note 1), on peut montrer que $f \otimes \chi_D$, défini par $f \otimes \chi_D = \sum \chi_D(n) a_n q^n$, est un élément de $M_{2k}(\Gamma_0(ND^2), 1)$. Le théorème de WALDSPURGER dit, de manière vague, que les $L(f \otimes \chi_D, k)$ sont, quand D varie, les carrés de coefficients de Fourier de formes modulaires de poids $k + \frac{1}{2}$ pour $\Gamma_0(N')$, avec N' explicite. « Il n'y a plus

qu'à » exhiber une base de l'espace de ces formes modulaires et calculer quelques coefficients pour obtenir une identité valable pour tout D .

Le lecteur désireux d'en apprendre plus sur ce sujet fascinant est invité à consulter les ouvrages suivants; en particulier, celui de KOBLITZ, dont le présent texte est fortement inspiré.

8. Références

- [1] Y. HELLEGOUARCH, *Invitation aux mathématiques de Fermat-Wiles*, Masson, Paris, 1997.
- [2] D. HUSEMÖLLER, *Elliptic curves*, GTM 111 Springer-Verlag, 1987.
- [3] N. KOBLITZ, *Introduction to Elliptic Curves and Modular Forms*, GTM 97, Springer-Verlag, 1984.
- [4] S. LANG, *Introduction to modular forms*, Corrected reprint of the 1976 original, Grundlehren der Mathematischen Wissenschaften 222, Springer-Verlag, 1995.
- [5] J. SILVERMAN, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.

Notes

1. On a en fait démontré que D est congruent si et seulement si l'équation $Dy^2 = x^3 - x$ a une solution dans \mathbf{Q}^2 avec $-1 < x < 0$. La courbe $C_D(\mathbf{R})$ a deux composantes connexes : un ovale dans la région $-1 \leq x \leq 0$, et une courbe avec une direction asymptotique verticale dans la région $x \geq 1$. L'application qui, à $P = (x, y) \in C_D(\mathbf{R})$, associe $P' = (x', y')$, intersection de la droite $(P, (-1, 0))$ avec C_D , échange les deux composantes connexes comme le montre un petit dessin (ou un calcul explicite), et envoie $C_D(\mathbf{Q})$ dans lui-même comme il est expliqué au § 1 (ou comme le montre un calcul explicite). Ceci permet de montrer que l'existence d'une solution dans \mathbf{Q}^2 avec $-1 < x < 0$ est équivalente à celle d'une solution dans \mathbf{Q}^2 avec $x > 1$. On en déduit la proposition.

2. Soit $(x, y) \in C_D(\mathbf{Q})$, avec $x > 1$. Si on écrit $x = \frac{a}{b}$ avec $a, b \in \mathbf{N}$, premiers entre eux, on obtient $b^4 y^2 = ab(a-b)(a+b)$ et donc a et b sont des carrés dans \mathbf{N} [car a est premier à $b(a-b)(a+b)$ et b est premier à $a(a-b)(a+b)$], et donc x est un carré dans \mathbf{Q} . De plus, comme $\text{pgcd}(a-b, a+b) \mid 2$, cela implique que $a-b$ est soit un carré, auquel cas $x+1$ et $x-1$ sont des carrés, soit le double d'un carré, auquel cas $x+1$ et $x-1$ sont aussi le double d'un carré.

Si K est un sous-corps de \mathbf{C} , soit $X(K) = \{(t, u, v) \in K^3, t^2 - u^2 = 1, v^2 - t^2 = 1\}$. Des petits calculs amusants montrent que l'application

$$(t, u, v) \mapsto f(t, u, v) = ((t+u)(t+v), (t+u)(t+v)(u+v))$$

induit une bijection de $X(\mathbf{Q})$ sur $C_1(\mathbf{Q}) - \{(-1, 0), (0, 0), (1, 0)\}$; la bijection réciproque étant donnée par

$$(x, y) \mapsto g(x, y) = \left(\frac{x^2 + 1}{2y}, \frac{x^2 - 2x - 1}{2y}, \frac{x^2 + 2x - 1}{2y} \right).$$

De plus, si $(x, y) = f(t, u, v)$, alors $x - 1 = (u + t)(u + v)$ et $x + 1 = (v + t)(v + u)$.

Soit alors $(t, u, v) \in X(\mathbf{Q})$. Les 8 points $(\pm t, \pm u, \pm v)$ appartiennent à $X(\mathbf{Q})$; on peut donc s'arranger pour que $t > 0$ et $v > 0$. Dans ce cas, $x^+ = (t + u)(t + v)$ et $x^- = (t - u)(t + v)$ sont tous deux positifs et donc sont des carrés d'après la discussion ci-dessus. Par ailleurs, $(x^+ + 1)(x^- + 1) = 2$ et comme $x^+ + 1$ et $x^- + 1$ sont soit des carrés, soit le double de carrés, l'un d'eux est un carré (et l'autre le double d'un carré). En conclusion, si $C_D(\mathbf{Q})$ contient un point $P = (x, y)$, avec $y \neq 0$, alors il contient un point $P_0 = (x_0, y_0)$ tel que l'on ait $x_0 = t_1^2$, $x_0 + 1 = u_1^2$ et $x_0 - 1 = v_1^2$, avec $t_1, u_1, v_1 \in \mathbf{Q}$. Soit $P_1 = (x_1, y_1) = f(t_1, u_1, v_1) \in C_1(\mathbf{Q})$. On peut de plus, d'après la discussion précédente,

choisir les signes de t_1, u_1, v_1 de telle sorte que $x_1, x_1 + 1$ et $x_1 - 1$ soient des carrés dans \mathbf{Q} .

On a alors $x_0 = t_1^2 = \left(\frac{x_1^2+1}{2y_1}\right)^2$. Écrivons $x = \frac{a_1}{b_1}$, avec a_1 et b_1 premiers entre eux. Alors $x_0 = \frac{(a_1^2+b_1^2)^2}{4a_1b_1(a_1^2-b_1^2)}$. Comme a_1b_1 est premier à $a_1^2 + b_1^2$, on a $\text{pgcd}((a_1^2 + b_1^2)^2, 4a_1b_1(a_1^2 - b_1^2)) = 1$ ou 4 suivant que l'un des nombres a_1, b_1 est pair ou que les deux sont impairs (s'ils sont tous les deux impairs, alors $a_1^2 + b_1^2$ est divisible par 2 et pas par 4). En conclusion, si on écrit $x_0 = \frac{a_0}{b_0}$, avec a_0 et b_0 premiers entre eux, alors $a_0 \geq \frac{1}{4}(a_1^2 + b_1^2)^2$, et il faut 4 fois moins de chiffres pour écrire x_1 que x_0 .

En partant d'une solution, ceci permet de construire une solution beaucoup plus simple, et finalement de montrer qu'il n'y en a pas (méthode de la descente infinie).

3. Il semble que FERMAT se soit légèrement laissé emporté par son enthousiasme quand il a découvert ce fait...

4. Ceci se traduit par la non nullité du discriminant $\Delta(P)$ du polynôme P . Si $P(x) = ax^3 + bx^2 + cx + d$, on a

$$\Delta(P) = \begin{vmatrix} a & 0 & 3a & 0 & 0 \\ b & a & 2b & 3a & 0 \\ c & b & c & 2b & 3a \\ d & c & 0 & c & 2b \\ 0 & d & 0 & 0 & c \end{vmatrix}.$$

La matrice ci-dessus est celle de l'application $(U, V) \mapsto UP + VP'$, où U est de degré ≤ 1 , V de degré ≤ 2 . La nullité de $\Delta(P)$ est donc équivalente à l'existence de (U, V) avec $UP = -VP'$ et U de degré ≤ 1 , V de degré ≤ 2 , ce qui est possible si et seulement si P et P' ne sont pas premiers entre eux.

5. Cette définition de $\overline{E}(K)$ est parfaitement artificielle. Une définition naturelle demande de travailler dans le plan projectif \mathbf{P}^2 , espace des droites de l'espace vectoriel de dimension 3. Celui-ci peut être vu comme la réunion du plan affine et d'une droite (projective) à l'infini dont les points correspondent aux directions de droites du plan affine; notre ∞ est le point de cette droite à l'infini correspondant à la direction verticale.

6. L'associativité n'est pas une évidence. Elle peut se vérifier par un calcul explicite assez pénible (mais on peut demander l'aide d'un ordinateur...). Une solution plus élégante consiste, si K est un sous-corps de \mathbf{C} , à passer par les fonctions elliptiques. (Dans le cas général, il y a une jolie démonstration passant par la géométrie projective.)

Si $\Lambda \subset \mathbf{C}$ est un réseau (i.e. $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, avec $\frac{\omega_1}{\omega_2} \notin \mathbf{R}$), la série $\frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$ converge uniformément sur tout compact de $\mathbf{C} - \Lambda$. Elle définit donc une fonction $\wp(z, \Lambda)$, dite « de Weierstrass », holomorphe sur $\mathbf{C} - \Lambda$ et périodique de période Λ . De plus, au voisinage de 0, on a

$$\wp(z, \Lambda) = z^{-2} + \sum_{n=1}^{+\infty} (2n+1)G_{2n+2}(\Lambda)z^{2n}, \quad \text{avec } G_k(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \omega^{-k}.$$

On a alors $\wp'(z, \Lambda) = -2z^{-3} + \sum_{n=1}^{+\infty} 2n(2n+1)G_{2n+2}(\Lambda)z^{2n-1}$, et un petit calcul montre que $H(z) = \wp'(z, \Lambda)^2 - 4\wp(z, \Lambda)^3 - 60G_4(\Lambda)\wp(z, \Lambda) - 140G_6(\Lambda)$ s'annule en $z = 0$. On peut donc étendre H en une fonction holomorphe, périodique de période Λ , sur \mathbf{C} tout entier. Par compacité de \mathbf{C}/Λ , H atteint son maximum et donc est constante d'après le principe du maximum; par suite elle est identiquement nulle. En conclusion $(\wp(z, \Lambda), \wp'(z, \Lambda)) \in E(\mathbf{C})$ si \mathbf{C} est la courbe elliptique d'équation $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$. Le même genre d'arguments montre que l'on obtient une bijection $\mathbf{C}/\Lambda \rightarrow \overline{E}(\mathbf{C})$ en envoyant $z \bmod \Lambda$ sur $(\wp(z, \Lambda), \wp'(z, \Lambda))$, et $0 \bmod \Lambda$ sur ∞ , et que l'addition sur

\mathbf{C} donne naissance, via cette bijection, à l'addition sur $\overline{E}(\mathbf{C})$ définie en termes d'alignement de points.

Maintenant, si K est un sous-corps de \mathbf{C} et si E est une courbe elliptique sur K , un changement linéaire de variables permet de mettre l'équation de E sous la forme $y^2 = 4x^3 - \alpha x - \beta$, avec $\alpha, \beta \in K$. Par ailleurs, des techniques de base de fonctions holomorphes permettent de montrer qu'il existe un unique réseau Λ de \mathbf{C} tel que $\alpha = 60G_4(\Lambda)$ et $\beta = 140G_6(\Lambda)$. Ceci permet d'identifier $\overline{E}(K)$ à un sous-groupe de \mathbf{C}/Λ . Il faut quand-même faire attention au fait que, \wp étant une fonction transcendante, l'appartenance de $\wp(z, \Lambda)$ à K ne permet pas de dire quoi que ce soit en ce qui concerne le sous-corps de \mathbf{C} engendré par z .

7. Si K est un sous-corps de \mathbf{C} , et si $\overline{E}(K) \cong \mathbf{C}/\Lambda$, alors le sous-groupe des points de n -torsion de $\overline{E}(K)$ s'identifie à un sous-groupe de $\frac{1}{n}\Lambda/\Lambda \cong (\mathbf{Z}/n\mathbf{Z})^2$; en particulier il est de cardinal $\leq n^2$.

8. La preuve que nous avons donnée du fait que 1 n'est pas congruent peut se réinterpréter en utilisant la loi de groupe sur $\overline{C}_1(\mathbf{Q})$. Les 8 automorphismes de $X(\mathbf{Q})$ donnés par $(t, u, v) \mapsto (\pm t, \pm u, \pm v)$ sont induits par les automorphismes $P \mapsto \pm P + Q$, où Q est un des 4 points de 2-torsion. Par ailleurs, le point P_1 que l'on a construit à partir du point P_0 vérifie $2P_1 = \pm P_0$. On a donc démontré que, si $P = (x, y) \in C_1(\mathbf{Q})$ est tel que $x, x+1$ et $x-1$ sont des carrés dans \mathbf{Q} , alors il existe $P' \in C_1(\mathbf{Q})$ tel que $P = 2P'$; plus généralement, on a prouvé, en utilisant le fait que $x, x+1$ et $x-1$ sont presque des carrés dans \mathbf{Q} , qu'il existe un point Q de 2-torsion, et $P' \in C_1(\mathbf{Q})$ tel que $P = 2P' + Q$. Le dernier argument de la démonstration montre que P' est nettement plus simple que P . En itérant le procédé en partant de P' , cela permet de prouver que $\overline{C}_1(\mathbf{Q})$ est engendré par les points de 2-torsion. La démonstration du théorème de Mordell suit exactement le même schéma.

9. Lors du congrès international des mathématiciens de 1900, HILBERT a énoncé une série de 23 problèmes, dont le 10-ième était de produire un algorithme permettant de décider si une équation polynomiale (en plusieurs variables), à coefficients entiers, a, ou non, des solutions en nombres entiers. Ce problème fut finalement résolu par MATIYASEVICH en 1970, qui prouva qu'un tel algorithme ne peut pas exister, au grand soulagement des arithméticiens qui voyaient d'un mauvais œil l'idée qu'un ordinateur puisse les mettre au chômage. En poussant plus loin les méthodes de MATIYASEVICH, on peut construire des polynômes explicites pour lesquels on peut décider arbitrairement de l'existence ou de la non existence de solutions en nombres entiers, sans rajouter de contradiction dans les mathématiques... C'est un peu ennuyeux, car cela veut dire qu'on n'est jamais sûr que le problème auquel on s'attaque n'est pas de ce type.

Le théorème de Matiyasevich n'exclut pas, a priori, l'existence d'un algorithme pour décider si un polynôme (en plusieurs variables) a des solutions rationnelles ou pas. Les courbes elliptiques fournissent le premier test non trivial dans cette direction; la conjecture de Birch et Swinnerton-Dyer fournissant un tel algorithme (cf. cor. 22), si elle est vraie...

10. La transformée de Fourier de $e^{-\pi x^2}$ est $e^{-\pi x^2}$; celle de $e^{-\pi t x^2}$ est donc $t^{-1/2} e^{-\pi t^{-1} x^2}$, et la formule de Poisson nous fournit l'identité

$$\sum_{n \in \mathbf{Z}} e^{-\pi t n^2} = t^{-1/2} \sum_{n \in \mathbf{Z}} e^{-\pi t^{-1} n^2}.$$

Ceci se traduit en l'identité $\sqrt{\frac{z}{2i}} \Theta\left(\frac{z}{2}\right) = \Theta\left(\frac{-1}{2z}\right)$ si $z \in i\mathbf{R}_+^*$, et comme les deux membres sont holomorphes sur \mathcal{H} cette identité est vraie pour tout $z \in \mathcal{H}$ d'après la propriété (H3).

11. Une manière de procéder est de partir de l'identité $\int_0^{+\infty} e^{-at} t^s \frac{dt}{t} = \Gamma(s) a^{-s}$ valable si $\operatorname{Re}(s) > 0$ et $\operatorname{Re}(a) > 0$. Ceci permet d'écrire

$$\xi(s) = \Gamma\left(\frac{s}{2}\right) \pi^{-s/2} \zeta(s) = \frac{1}{2} \int_0^{+\infty} \left(\Theta\left(\frac{it}{2}\right) - 1\right) t^{s/2} \frac{dt}{t}.$$

En coupant cette intégrale en deux à $t = 1$, et en utilisant l'équation fonctionnelle de Θ , cela permet de montrer que ξ a un prolongement analytique à $\mathbf{C} - \{0, 1\}$, a des pôles simples en 0 et 1, et vérifie l'équation fonctionnelle $\xi(s) = \xi(1-s)$. Comme $\Gamma\left(\frac{s}{2}\right)^{-1}$ s'annule en $0, -2, -4, \dots$, on en déduit que $\zeta(-2n) = 0$ si $n \in \mathbf{N}$.

12. Cette fonction n'est pas celle qui est habituellement considérée; elle en diffère par la multiplication par des facteurs en les mauvais p , mais comme ceux-ci ne s'annulent pas en $s = 1$, cela ne change rien en ce qui concerne la conjecture de Birch et Swinnerton-Dyer. La bonne fonction $L(E, s)$ a une équation fonctionnelle plus sympathique que celle considérée dans cet article : il existe $\varepsilon \in \{\pm 1\}$ et $N \in \mathbf{N}$ tel que, si $\Lambda(E, s) = \frac{\Gamma(s)}{(2\pi)^s} N^{s/2} L(E, s)$, alors $\Lambda(E, 2-s) = \varepsilon \Lambda(E, s)$; en particulier, si $\varepsilon = -1$, alors $r_\infty(E)$ est impair et $L(E, 1) = 0$.

13. Dans ce cas, on a le résultat suivant. On définit $\delta : \mathbf{Z}[i] \rightarrow \{0, 1, i, -1, -i\}$ par

$$\begin{cases} \delta(\omega) = 0 & \text{si } \omega \text{ est divisible par } 1+i \text{ dans } \mathbf{Z}[i], \\ \omega\delta(\omega) - 1 \text{ est divisible par } (1+i)^3 & \text{sinon.} \end{cases}$$

On a alors

$$L(C_1, s) = \frac{1}{4} \sum_{\omega \in \mathbf{Z}[i] - \{0\}} \frac{\omega\delta(\omega)}{|\omega|^{2s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

Le cas D général se déduit facilement du cas $D = 1$: on a $L(C_D, s) = \sum_{n=1}^{+\infty} \chi_D(n) a_n n^{-s}$, où $\chi_D : \mathbf{Z} \rightarrow \{-1, 0, 1\}$ est le symbole de Legendre modulo D . Ce symbole de Legendre est caractérisé par les propriétés suivantes : $\chi_D(n+4D) = \chi_D(n)$, $\chi_D(n) = 0$ si $(D, n) \neq 1$, et

$$\chi_D(nm) = \chi_D(n)\chi_D(m), \quad \chi_D(p) = \begin{cases} 1 & \text{si } D \text{ est un carré dans } \mathbf{F}_p^*, \\ -1 & \text{si } D \text{ n'est pas un carré dans } \mathbf{F}_p^*. \end{cases}$$

L'existence de χ_D est une conséquence de la loi de réciprocité quadratique conjecturée par EULER en 1783 et démontrée par GAUSS en 1801.

14. En fait, BIRCH et SWINNERTON-DYER avaient été plus optimistes et avaient conjecturé que

$$\prod_{p \text{ bon}, p \leq x} \frac{p}{|\overline{E}(\mathbf{F}_p)|} \sim C(\log x)^{-r(E)}.$$

GOLDFELD (1982) a prouvé que, si c'est le cas, alors $r_\infty(E) = r(E)$, la fonction $L(E, s)$ vérifie l'hypothèse de Riemann (i.e. elle ne s'annule pas pour $\operatorname{Re}(s) > 1$), mais, de manière surprenante, que l'on a $C = \frac{L(E, 1)}{\sqrt{2}}$ au lieu de $C = L(E, 1)$, si $r(E) = 0$.

15. Celle-ci prend la forme $\lim_{s \rightarrow 1} (s-1)^{-r(E)} L(E, s) = |\text{III}(E)| \cdot R_\infty(E) \cdot \Omega_\infty(E) \cdot \prod_{p \text{ mauvais}} c_p$, où c_p est un nombre rationnel explicite, $\Omega_\infty(E)$ est la période réelle de E (donnée par $\Omega_\infty(E) = 2 \int_\alpha^{+\infty} \frac{dx}{\sqrt{P(x)}}$, si E est d'équation $y^2 = P(x)$ et α est la plus grande racine réelle de P), $R_\infty(E)$ est un « régulateur » mesurant la taille des générateurs de $\overline{E}(\mathbf{Q})$, et $\text{III}(E)$, le groupe de Tate-Shafarevich de E , est un groupe conjecturalement fini.

Prouver que ce groupe est fini suffira probablement à prouver la forme faible de la conjecture de Birch et Swinnerton-Dyer. Pour la courbe C_D , que cela suffise a été

démontré par GREENBERG (1983) si $r_\infty(C_D)$ est impair, et par RUBIN (1991) sans condition sur $r_\infty(E)$. Dans le cas E général, cela a été démontré par NEKOVÁŘ (2001) si $r_\infty(E)$ est impair; le cas « $r_\infty(E)$ pair » devrait suivre de travaux en cours de SKINNER et URBAN sur la « conjecture principale », et de LAUMON, NGÔ et al. sur un bout du « programme de Langlands ».

16. Si $(x, y) \in C_D(\mathbf{C})$, alors $(-x, iy) \in C_D(\mathbf{C})$. Si Λ est le réseau de \mathbf{C} correspondant à $\overline{C}_D(\mathbf{C})$ (cf. note 7), la remarque précédente se traduit par le fait que $i\Lambda = \Lambda$. On dit qu'une courbe elliptique E définie sur un sous-corps de \mathbf{C} a de la multiplication complexe si, Λ étant le réseau de \mathbf{C} qui lui correspond, il existe $\tau \in \mathbf{C} - \mathbf{R}$ tel que $\tau\Lambda \subset \Lambda$ (c'est donc le cas de C_D , avec $\tau = i$); un tel τ est alors racine d'un polynôme unitaire de degré 2 à coefficients dans \mathbf{Z} .

17. La démonstration de cette formule occupe une centaine de pages...

18. En particulier, elles jouent un rôle fondamental dans la démonstration de WILES du théorème de Fermat.

19. Si $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ est un réseau de \mathbf{C} (cf. note 7), on a $G_k(\Lambda) = \omega_2^{-k} G_k(\frac{\omega_1}{\omega_2})$, ce qui fournit un autre lien (plus ancien et plus transparent) entre courbes elliptiques et formes modulaires, que celui du th. 21. C'est d'ailleurs ce lien qui, couplé avec la théorie de la multiplication complexe (note 1), est à la base de la construction des points de Heegner.

20. Si $a^p + b^p = c^p$, avec $abc \neq 0$, est un contreexemple au théorème de Fermat, on peut considérer la courbe elliptique introduite par HELLEGOUARCH et FREY, d'équation $y^2 = x(x - a^p)(x + b^p)$. WILES montre que cette courbe est modulaire, ce qui est en contradiction avec la « conjecture ε » de SERRE (1984) démontrée par RIBET (1988). La « conjecture ε » décrit les congruences que l'on peut attendre entre formes modulaires. Dans le cas qui nous intéresse, cette conjecture prédit une congruence modulo p entre le q -développement de la forme modulaire attachée à la courbe de Frey et Hellegouarch, et celui de $g \in M_2(\Gamma_0(2), 1)$, ce qui n'est pas possible car cet espace est de dimension 1, et la divisibilité par p du terme constant du q -développement de g entraîne celle de tous les termes du q -développement.

21. Il s'agit d'un résultat profond qui demande d'utiliser les travaux de SHIMURA déjà mentionnés, et des résultats de SERRE (1968) et FALTINGS (1983) (ou CHUDNOVSKY (1985), ou encore BOST (2001)) selon lesquels une courbe elliptique sur \mathbf{Q} est (presque) déterminée par sa fonction L (et donc par le nombre de ses points dans \mathbf{F}_p pour suffisamment de nombres premiers p).

22. La théorie de la multiplication complexe (note 1) permet de déterminer le corps de définition de ces points; ce sont, d'après un théorème de SCHNEIDER (1937), les seuls éléments de \mathcal{H} , algébriques sur \mathbf{Q} , qui fournissent des points algébriques de E .