Intégration sur $\mathcal{H}_p \times \mathcal{H}$ et applications arithmétiques

Fabien Pazuki

2 octobre 2003

d'après un article de Henri Darmon

Mémoire de DEA sous la direction de Marc Hindry

Université Pierre et Marie Curie Paris VI - D.E.A. Méthodes algébriques

Table des matières

Introduction

Ce mémoire est consacré à l'étude de l'article "Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic application" de Henri Darmon, paru dans "Annals of Mathematics" (154) en 2001. Nous cherchons en priorité à rendre compte avec concision des constructions qu'il propose afin de permettre au lecteur une approche plus rapide de ses travaux. Nous invitons le lecteur intéressé à consulter l'article original ainsi que les autres articles du même auteur (que l'on peut trouver aisément sur Internet par exemple). Nous proposons ensuite, en ouverture, de traiter une question prolongeant cet article. Enfin, une partie annexe expose les conjectures de Birch et Swinnerton-Dyer et leurs liens avec ce qui précéde.

Soit E une courbe elliptique sur $\mathbb{Q}$ de conducteur N. On sait depuis les publications de Wiles entre autres (d'après les travaux [7, 6, 5]) que E est une courbe modulaire, i.e. on a l'existence d'un morphisme non constant φ :

$$\varphi : \mathcal{H}^*/\Gamma_0(N) \longrightarrow E(\mathbb{C})$$

avec $\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$ le demi-plan de Poincaré et $\Gamma_0(N) \subset PSL_2(\mathbb{Z})$ le sous-groupe de congruence de Hecke qui agit sur $\mathcal{H}^*$ par transformation de Möbius.

$\mathcal{H}^*/\Gamma_0(N)$ est une surface de Riemann compacte ; c'est la compactifiée de $\mathcal{H}/\Gamma_0(N)$ laquelle paramètre les paires (A_τ, G_τ) où $A_\tau = \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ est une courbe elliptique sur $\mathbb{C}$ et $G_\tau =< \frac{\tau}{N} >$ est un sous-groupe de $A_\tau(\mathbb{C})$ cyclique d'ordre N. Cela permet d'identifier $\mathcal{H}^*/\Gamma_0(N)$ à la courbe modulaire $X_0(N)$ définie sur $\mathbb{Q}$.

Soit K un corps quadratique imaginaire. Lorsqu'on choisit $\tau \in \mathcal{H} \cap K$ on peut construire une paire (A_τ, G_τ) définie sur le corps de classe H de K grâce à la théorie de la multiplication complexe. On sait alors que le point dit de Heegner $\varphi(\tau) \in E(\mathbb{C})$ est aussi défini sur H (voir aussi le paragraphe 4.1).

Le but de l'article que nous étudions est de proposer une construction conjecturale (p-adique) de tels points globaux, en se plaçant cette fois dans le cas où K est un corps quadratique réel.

Je remercie Marc Hindry pour ses conseils et sa gentillesse, ainsi que toute l'équipe de théorie des nombres de Chevaleret (en particulier mes professeurs MM. Nekovar et Oesterlé). Enfin grand merci à Henri Darmon pour ses encouragements.

1 Cadre général et notations

- p est un nombre premier.
- $N = pM$ et p ne divise pas M.
- $\mathcal{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$.
- Partant de $\mathbb{Q}$, on construit sa complétion $\mathbb{Q}_p$ pour la valuation p-adique. On en prend alors la clôture algébrique $\overline{\mathbb{Q}_p}$ qui n'est plus complète. On considère donc sa complétion p-adique et on obtient $\mathbb{C}_p$. C'est un corps complet et algébriquement clos. On pose alors :

  $$\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p).$$

  Remarque : c'est en fait l'analogue de $\mathcal{H}' = \mathbb{C} - \mathbb{R}$ sur lequel on peut construire comme sur $\mathcal{H}$ une théorie des formes modulaires.

- Soit $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}[\frac{1}{p}]) \mid c \equiv 0\,(modM) \right\}$ On considère alors Γ l'image dans $PSL_2(\mathbb{Z}[\frac{1}{p}])$ du groupe des éléments de déterminant 1 de $R^\times$. Ce groupe agit sur $\mathcal{H}_p$ et sur $\mathcal{H}^*$ par transformation de Möbius (voir plus bas).
- On supposera que la courbe E est seule dans sa classe de $\mathbb{Q}$-isogénie. Cette hypothèse est technique, mais semble cependant nécessaire lorsqu'on cherche à vérifier la conjecture de nature cohomologique (3.9) dans des cas particuliers [8].
- La transformation de Möbius : soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ et $z \in \mathbb{P}_1(\mathbb{Q})$, on définit alors une action, dite transformation de Möbius :

  $$\gamma.z := \frac{az+b}{cz+d}.$$

- Une forme modulaire (ou cuspidale) de poids 2 : Une application holomorphe sur $\mathcal{H}$ vérifiant :

  $$f(\frac{az+b}{cz+d}) = (cz+d)^2 f(z)$$

- L'opérateur de Hecke : soit $n \in \mathbb{N}^*$. On appelle $T(n)$ le n-ième opérateur de Hecke agissant sur un réseau Λ :

  $$T(n)\Lambda = \sum_{\Lambda' \subset \Lambda,\, [\Lambda:\Lambda'] = n} (\Lambda').$$

On peut déduire son action sur les formes modulaires de poids $2k$ qui prend la forme suivante (voir [12]) :

$$(T_{2k}(n)f)(\tau) = n^{2k-1} \sum_{ad=n,\, a\geq 1,\, 0\leq b<d} d^{-2k} f(\frac{a\tau + b}{d})$$

2 Intégration sur $(\mathcal{H}_p \times \mathcal{H})/\Gamma$

Nous cherchons à intégrer des formes satisfaisant certaines propriétés. Il faut pour cela détailler la structure de $\mathcal{H}_p$, ce qui peut se faire en introduisant $\mathcal{T}$ l'arbre de Bruhat-Tits de $PGL_2(\mathbb{Q}_p)$. En effet il existe une application de réduction :

$$red : \mathcal{H}_p \longrightarrow \mathcal{T}$$

L'image réciproque d'une arête est un "anneau ouvert de base" de $\mathcal{H}_p$ et l'image inverse d'un sommet est un affinoïde de $\mathcal{H}_p$ (voir [13]).

2.1 L'arbre de Bruhat-Tits $\mathcal{T}$

Il s'agit en fait de l'ensemble $\mathcal{T}_p = GL_2(\mathbb{Z}_p)\mathbb{Q}_p^* \setminus GL_2(\mathbb{Q}_p)$ que l'on munit d'une structure particulière. On peut le voir comme un arbre constitué d'un ensemble de sommets $\mathcal{V}(\mathcal{T})$ identifié à l'ensemble des $\mathbb{Z}_p$-modules de rang 2 dans $\mathbb{Q}_p^2$ à $\mathbb{Q}_p^*$-homothétie près [3, 4]. Deux sommets $v_1 = [\Lambda_1]$ et $v_2 = [\Lambda_2]$ sont reliés par une arête ($\in \varepsilon(\mathcal{T})$) si et seulement si $p\Lambda_1 \subsetneq \Lambda_2 \subsetneq \Lambda_1$. On pose $v_0 = [\mathbb{Z}_p^2]$.

2.2 Formes cuspidales

Une forme cuspidale de poids 2 sur $(\mathcal{T} \times \mathcal{H})/\Gamma$ est une fonction :

$$f : \varepsilon(\mathcal{T}) \times \mathcal{H} \longrightarrow \mathbb{C}$$

satisfaisant les conditions suivantes :

1. $\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, f(\gamma e, \gamma z) = (cz + d)^2 f(e, z)$

2. $\forall v \in \mathcal{V}(\mathcal{T}), \sum_{s(e)=v} f(e, z) = 0$

3. $\forall e \in \varepsilon(\mathcal{T}),\ f(\overline{e}, z) = -f(e, z)$ où $\overline{e}$ est l'arête e orientée dans le sens opposé.

4. $\forall e \in \varepsilon(\mathcal{T}), f_e(z) := f(e, z)$ est forme cuspidale de poids 2 pour $\Gamma_e := Stab_\Gamma(e)$

5. $\forall \gamma \in \Gamma, f(\gamma e, \gamma z) d(\gamma z) = f_e(z) dz$

On appelle $S_2(\mathcal{T}, \Gamma)$ l'ensemble de telles formes. On va de plus définir un groupe de congruence un peu plus gros que Γ : nous noterons $\widetilde{\Gamma}$ l'image de $R_+^\times$ dans $PGL_2(\mathbb{Q}_p)$, le groupe des matrices inversibles de déterminant positif.

Introduisons ici la notation : $\mid \gamma \mid := ord_p(det(\gamma))$. On a alors :

$$\Gamma = \{\gamma \in \widetilde{\Gamma}, \mid \gamma \mid = 0(mod 2)\}$$

Donc $[\widetilde{\Gamma} : \Gamma] = 2$.

Soit alors $S_2(\varepsilon, \widetilde{\Gamma})$ l'espace des formes :

$$f : \varepsilon(\mathcal{T}) \times \mathcal{H} \longrightarrow \mathbb{C}$$

vérifiant seulement :

1. $\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, f(\gamma e, \gamma z) = \frac{(cz+d)^2}{det(\gamma)} f(e, z)$

2. $\forall e \in \varepsilon(\mathcal{T}) f_e(z) := f(e, z)$ est forme cuspidale pour $\Gamma_e := \widetilde{\Gamma} \cap Stab_\Gamma(e)$

On introduit enfin l'espace $S_2(\mathcal{V}, \widetilde{\Gamma})$ qui se présente de la même manière que le précédent.

Ces espaces forment une suite exacte naturelle :

$$0 \longrightarrow S_2(\mathcal{T}, \Gamma) \longrightarrow S_2(\varepsilon, \widetilde{\Gamma}) \longrightarrow S_2(\mathcal{V}, \widetilde{\Gamma}) \oplus S_2(\mathcal{V}, \widetilde{\Gamma})$$

On va alors pouvoir se ramener à des formes modulaires classiques en associant à chaque $f(e, z)$ une $f_0(z) := f_{e_*}(z)$ où e_* est l'arête dont l'origine est en $v_0 = [\mathbb{Z}_p^2]$ et à chaque $f(v, z)$ une $f_0(z) := f_{v_0}(z)$

On obtient le diagramme suivant résumant la situation :

$$\begin{array}{ccccccc}
0 & \longrightarrow & S_2(\mathcal{T}, \Gamma) & \longrightarrow & S_2(\varepsilon, \widetilde{\Gamma}) & \longrightarrow & S_2(\mathcal{V}, \widetilde{\Gamma}) \oplus S_2(\mathcal{V}, \widetilde{\Gamma}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & S_2^{p-new}(\Gamma_0(N)) & \longrightarrow & S_2(\Gamma_0(N)) & \longrightarrow & S_2(\Gamma_0(M)) \oplus S_2(\Gamma_0(M))
\end{array}$$

Soit alors $w = 1$ si E est à réduction multiplicative déployée en p, $w = -1$ si E est à réduction multiplicative non-deployée en p.

Lemme 2.1. *On peut décrire l'action de* Γ *:*

$$\forall f \in S_2(\mathcal{T}, \Gamma)\ \forall \gamma \in \widetilde{\Gamma}\ f(\gamma e, \gamma z) d(\gamma z) = w^{|\gamma|} f(e, z) dz$$

Preuve : L'involution d'Atkin-Lehner est une action sur $X_0(N)$ en p donnée par (avec $\alpha e_* = \overline{e}_*$) :

$$W_p f_0(z) dz = f_0(\alpha z) d(\alpha z).$$

Considérons donc W_p l'involution d'Atkin-Lehner. Soit e une arête paire, on a donc $\gamma \in \Gamma$ tel que $e = \gamma e_*$:

$$\begin{aligned}
W_p f(e,z)dz &= W_p f_0(\gamma^{-1}z)d(\gamma^{-1}z) \\
&= f_0(\alpha\gamma^{-1}z)d(\alpha\gamma^{-1}z) \\
&= f(e_*, \alpha\gamma^{-1}z)d(\alpha\gamma^{-1}z) \\
&= -f(\overline{e}_*, \alpha\gamma^{-1}z)d(\alpha\gamma^{-1}z) \\
&= -f(\overline{e}, \gamma\alpha\gamma^{-1}z)d(\gamma\alpha\gamma^{-1}z) \\
&= -f(\gamma\alpha\gamma^{-1}e, \gamma\alpha\gamma^{-1}z)d(\gamma\alpha\gamma^{-1}z) \\
&= -f(\alpha e, \alpha z)d(\alpha z).
\end{aligned}$$

On mène un calcul similaire avec e une arête impaire. On a alors d'après [19] : si E a réduction multiplicative déployée en p, $W_p f_0 = -f_0$, si E a réduction multiplicative non déployée en p, $W_p f_0 = f_0$. Ceci démontre le lemme.

2.3 Mesures p-adiques

Une mesure p-adique sur $\mathbb{P}_1(\mathbb{Q}_p)$ à valeur dans $\mathbb{Z}_p$ est une application additive

$$\mu : \{compacts\, ouverts\, de\, \mathbb{P}_1(\mathbb{Q}_p)\} \longrightarrow \mathbb{Z}_p.$$

Soit ω_E une différentielle de Néron de E. On a alors :

$$\varphi^*(\omega_E) = 2\pi i c_\varphi f_0(z)dz,$$

où c_φ est la constante de Manin [15].

On construit alors une mesure p-adique à valeurs dans $\mathbb{C}$ en posant pour $\gamma \in GL(\mathbb{Q}_p)$:

$$\widetilde{\mu}_f\{x \to y\}(\gamma\mathbb{Z}_p) := 2\pi i c_\varphi \int_x^y f_0(\gamma z)d(\gamma z)$$

On souhaite ensuite pouvoir intégrer contre cette mesure p-adique. Il faut pour cela que les valeurs prises soient entières ou du moins p-entières. Ceci peut être réalisé en prenant x et y dans $\mathbb{P}_1(\mathbb{Q})$: on définit en effet le symbole modulaire :

$$\widetilde{\lambda}_E(a,b) := 2\pi i c_\varphi \int_\infty^{-\frac{a}{b}} f_0(z)dz \in \mathbb{C}$$

On peut alors exprimer la mesure en fonction de ces $\widetilde{\lambda}_E$ en posant $\gamma x = -\frac{a}{b}$ et $\gamma y = -\frac{c}{d}$:

$$\widetilde{\mu}_f\{x \to y\}(\gamma \mathbb{Z}_p) = w^{|\gamma|}(\widetilde{\lambda}_E(c,d) - \widetilde{\lambda}_E(a,b))$$

On peut à présent dire grâce au théorème de Drinfeld-Manin que les $\widetilde{\lambda}_E$ sont des éléments du réseau de Néron $\Omega =< \Omega_+, \Omega_- >$.
On peut donc écrire :

$$\widetilde{\lambda}_E(a,b) = \lambda_E^+(a,b)\Omega_+ + \lambda_E^-(a,b)\Omega_-,$$

avec $\lambda_E^{\pm}(a,b) \in \mathbb{Z}$. Choisissons alors $w_\infty = \pm 1$. Posons $\lambda_E(a,b) := \lambda_E^+(a,b)$ si $w_\infty = +1$ et $\lambda_E(a,b) := \lambda_E^-(a,b)$ si $w_\infty = -1$.
De tout ceci on déduit une mesure à valeurs dans $\mathbb{Z}$:

$$\mu_f\{x \to y\}(\gamma \mathbb{Z}_p) = w^{|\gamma|}(\lambda_E(c,d) - \lambda_E(a,b))$$

2.4 Approche cohomologique

Prenons x et y dans $\mathcal{H}^*$ et f dans $S_2(\mathcal{T}, \Gamma)$. La fonction de $\varepsilon(\mathcal{T})$ dans $\mathbb{C}$ définie par :

$$\widetilde{\kappa}_f\{x \to y\}(e) := 2\pi i c_\varphi \int_x^y f_e(z)dz$$

est un cocycle sur $\mathcal{T}$ (ceci vient des propriétés harmoniques de f).
Soit $\gamma \in R^\times$. Posons $sgn(\gamma) := 0$ lorsque $det(\gamma) > 0$ et $sgn(\gamma) = 1$ lorsque $det(\gamma) < 0$.

Proposition 2.2. *La formule suivante définit une action de $R^\times$ sur κ_f :*

$$\kappa_f\{\gamma x \to \gamma y\}(\gamma e) = w^{|\gamma|} w_\infty^{sgn(\gamma)} \kappa_f\{x \to y\}(e)$$

2.5 Intégrale p-adique multiplicative

On définit une "intégrale double" grâce à la mesure précedente en choisissant un logarithme p-adique (nous allons nous affranchir de ce choix au paragraphe suivant, on peut fixer par exemple $\log(p) = 0$). Pour $z_1, z_2 \in \mathcal{H}_p$ et $x, y \in \mathbb{P}_1(\mathbb{Q})$:

$$\int_{z_1}^{z_2} \int_x^y \omega := \int_{\mathbb{P}_1(\mathbb{Q}_p)} \log\left(\frac{t - z_2}{t - z_1}\right) d\mu_f\{x \to y\}(t) \in \mathbb{C}_p$$

La forme ω doit être considérée comme une forme de poids (2,2) sur $\mathcal{H}_p \times \mathcal{H}/\Gamma$, bien qu'on ne définisse que les applications f, ses résidus p-adiques (on pourra penser à une analogie avec les surfaces modulaires de Hilbert).

Lemme 2.3. *Cette intégrale double est additive et vérifie :*

$$\int_{\gamma z_1}^{\gamma z_2} \int_{\gamma x}^{\gamma y} \omega = w^{|\gamma|} w_{\infty}^{sgn(\gamma)} \int_{z_1}^{z_2} \int_{x}^{y} \omega$$

Preuve : La double additivité se vérifie directement. La relation supplémentaire est une conséquence directe de la proposition 2.2.

Pour éviter le choix d'un logarithme p-adique on pose ensuite :

$$\oint_{z_1}^{z_2} \int_{x}^{y} \omega := \oint_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{t - z_2}{t - z_1} \right) d\mu_f \{x \to y\}(t) \in \mathbb{C}_p^{\times}$$

Dans la définition de l'intégrale multiplicative la limite de sommes de Riemann est remplacée par la limite d'un produit, plus précisément :

$$\oint_{\mathbb{P}_1(\mathbb{Q}_p)} g(t) d\mu(t) := \lim_{U} \prod_{U_\alpha \in U} g(t_\alpha)^{\mu(U_\alpha)},$$

où la limite est prise sur des recouvrements de compacts ouverts $U = \{U_\alpha\}_\alpha$ de $\mathbb{P}_1(\mathbb{Q}_p)$ avec $t_\alpha \in U_\alpha$.

Lemme 2.4. *On obtient alors en partant des relations du lemme précédent :*

$$\oint_{z_1}^{z_3} \int_{x}^{y} \omega = \oint_{z_1}^{z_2} \int_{x}^{y} \omega \times \oint_{z_2}^{z_3} \int_{x}^{y} \omega$$

$$\oint_{z_1}^{z_2} \int_{x_1}^{x_3} \omega = \oint_{z_1}^{z_2} \int_{x_1}^{x_2} \omega \times \oint_{z_1}^{z_2} \int_{x_2}^{x_3} \omega$$

$$\oint_{\gamma z_1}^{\gamma z_2} \int_{\gamma x}^{\gamma y} \omega = \left(\oint_{z_1}^{z_2} \int_{x}^{y} \omega \right)^{w^{|\gamma|} w_{\infty}^{sgn(\gamma)}}$$

3 Périodes

Dans cette partie nous présentons différentes périodes associées à E ainsi qu'une idée de "l'information arithmétique" qu'elles contiennent. Par "information arithmétique" nous entendons ici des renseignements sur l'existence de points de la courbe elliptique, sur l'extension de $\mathbb{Q}$ dans laquelle ils pourraient être définis, sur leur ordre, etc.
Comme E est à réduction multiplicative en p, on a d'après les travaux de Tate :

$$\exists! q \in \mathbb{Q}_p^* \quad | q |< 1, \;\; E(\overline{\mathbb{Q}}_p) \simeq \overline{\mathbb{Q}}_p^* / < q > .$$

Cet isomorphisme sera dorénavant noté Φ_{Tate}.
On attire l'attention sur le fait que la forme différentielle ω n'est pas tout à fait définie dans l'article, mais que cela n'empêche pas de définir l'intégrale double comme cela a été fait en 2.5.

3.1 L'algèbre $K \simeq \mathbb{Q} \times \mathbb{Q}$

Soit $\Psi : K \longrightarrow M_2(\mathbb{Q})$ un plongement de $\mathbb{Q}$-algèbres. On notera $\overline{\Psi} : K^\times \longrightarrow PGL_2(\mathbb{Q})$ l'homomorphisme induit. Le tore $\overline{\Psi}(K^\times)$ agit sur $\mathcal{H}^*$ avec exactement deux points fixes x_Ψ et y_Ψ dans $\mathbb{P}_1(\mathbb{Q})$. Le groupe $\overline{\Psi}(K^\times) \cap \Gamma$ est libre de rang 1, de générateur γ_Ψ. Choisissons alors $z \in \mathcal{H}_p$. On définit une période associée à Ψ par :

$$I_\Psi := \oint_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega.$$

On a alors le :

Lemme 3.1. *Cette période ne dépend que de la classe de conjugaison de Ψ.*

Preuve : Prenons z_1 et z_2 dans $\mathcal{H}_p$:

$$\oint_{z_1}^{\gamma_\Psi z_1} \int_{x_\Psi}^{y_\Psi} \omega \div \oint_{z_2}^{\gamma_\Psi z_2} \int_{x_\Psi}^{y_\Psi} \omega = \oint_{z_1}^{\gamma_{z_2}} \int_{x_\Psi}^{y_\Psi} \omega \div \oint_{\gamma_\Psi z_1}^{\gamma_\Psi z_2} \int_{x_\Psi}^{y_\Psi} \omega = 1\,,$$

ces égaliés provenant du lemme 2.4. Ceci montre l'indépendance en z. Prenons ensuite $\alpha \in \widetilde{\Gamma}$. Comme x_Ψ est point fixe pour Ψ, αx_Ψ est point fixe pour $\alpha\Psi\alpha^{-1}$. On a alors :

$$\oint_z^{\alpha\gamma_\Psi\alpha^{-1} z} \int_{\alpha x_\Psi}^{\alpha y_\Psi} \omega = \left(\oint_{\alpha^{-1} z}^{\gamma_\Psi \alpha^{-1} z} \int_{x_\Psi}^{y_\Psi} \omega \right)^{w^{|\alpha|}} = \left(\oint_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega \right)^{w^{|\alpha|}},$$

ce qui montre que I_Ψ ne dépend que de la Γ-classe de conjugaison de Ψ.
On a alors le théorème :

Théorème 3.2.

$$\log(I_\Psi) = \frac{\log(q)}{ord_p(q)} ord_p(I_\Psi).$$

C'est le théorème principal de l'article. Associé au fait que la courbe E est seule dans sa classe d'isogénie, ceci mène à la conjecture suivante :

Conjecture 3.3. *La période I_Ψ est dans $q^{\mathbb{Z}}$.*

On n'obtiendrait somme toute qu'assez peu d'information arithmétique sur la courbe. Ceci motivera donc une recherche de nouveaux invariants dans les parties suivantes. Avant cela nous exposons une esquisse de preuve de ce théorème : il s'agit d'évaluer les quantités $\log(I_\Psi)$ et $ord_p(I_\Psi)$ indépendament. Nous allons donc présenter les techniques employées.

3.1.1 $ord_p(I_\Psi)$

On introduit tout d'abord la somme suivante, prise sur toutes les arêtes joignant un certain sommet $v \in \mathcal{T}$ au sommet $\gamma_\Psi v$.

$$W_\Psi := \sum_{v \to \gamma_\Psi v} \kappa_f\{x_\Psi \to y_\Psi\}(e).$$

W_Ψ ne dépend que de la classe de conjugaison de Ψ. On montre alors que :

Proposition 3.4. $ord_p(I_\Psi) = W_\Psi$.

On peut en fait se concentrer sur des plongements particuliers $\Psi_\nu : K \longrightarrow M_2(\mathbb{Q})$ construits de la façon suivante, avec $pgcd(\nu, c) = 1$:

$$\Psi_\nu(a, a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

$$\Psi_\nu(c, 0) = \begin{pmatrix} c & \nu \\ 0 & 0 \end{pmatrix}.$$

Posons ensuite :

$$J := \{a \in (\mathbb{Z}/c\mathbb{Z})^* \mid \exists j = j(a),\ a/\nu \equiv p^j\ (mod\, c)\}.$$

Remarque : L'intégration p-adique se fait "par morceaux" sur des ouverts compacts par exemple. L'ensemble J sert ici à paramétrer les voisinages sur lesquels on décide d'intégrer. On verra plus bas que les ensembles J_n ont la même fonction.
On précise alors :

Proposition 3.5.

$$ord_p(I_{\Psi_\nu}) = W_{\Psi_\nu} = \sum_{a \in J} w^{j(a)} \lambda_E(a, c).$$

3.1.2 $\log(I_\Psi)$

Posons cette fois-çi :

$$J_n := \{a \in (\mathbb{Z}/p^n c\mathbb{Z})^* \mid \exists j = j(a),\ a/\nu \equiv p^j\ (mod\, c)\}.$$

On montre alors que :

Proposition 3.6.

$$\log(I_\Psi) = \int_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega = \lim_{n\to\infty} w^n \sum_{a\in J_n} w^{j(a)} \log(a)\lambda_E(a, p^n c).$$

3.1.3 Comment faire le lien

On est ramené à montrer que :

Lemme 3.7.

$$\lim_{n\to\infty} w^n \sum_{a\in J_n} w^{j(a)} \log(a)\lambda_E(a, p^n c) = \frac{\log(q)}{ord_p(q)} \sum_{a\in J} w^{j(a)}\lambda_E(a, c).$$

Preuve : Soit $\chi : (\mathbb{Z}/c\mathbb{Z})^* \longrightarrow \mathbb{C}_p^*$ un caractère de Dirichlet avec la particularité $\chi(p) = w$. On a alors deux cas. Si $\chi(-1) = -w_\infty$, un calcul direct montre alors avec la relation $\lambda_E(-a, b) = w_\infty \lambda_E(a, b)$:

$$\lim_{n\to\infty} w^n \sum_{a\in(\mathbb{Z}/p^n c\mathbb{Z})^*} \chi(a)\log(a)\lambda_E(a, p^n c) = \sum_{a\in(\mathbb{Z}/c\mathbb{Z})^*} \chi(a)\lambda_E(a, c) = 0.$$

Si $\chi(-1) = w_\infty$, on peut utiliser la conjecture des zéros exceptionnels de Mazur, Tate et Teitelbaum [1] démontrée par Greenberg et Stevens [2] et assurant, pour tout χ de cette forme :

$$\lim_{n\to\infty} w^n \sum_{a\in(\mathbb{Z}/p^n c\mathbb{Z})^*} \chi(a)\log(a)\lambda_E(a, p^n c) = \frac{\log(q)}{ord_p(q)} \sum_{a\in(\mathbb{Z}/c\mathbb{Z})^*} w^{j(a)}\lambda_E(a, c).$$

L'égalité est donc démontrée pour tout χ tel que $\chi(p) = w$. Par combinaison $\mathbb{C}_p$-linéaire on obtient le lemme 3.7. Le théorème 3.2 en découle.

3.2 Cas où p est décomposé dans K

Lorsque p est décomposé dans K, on a que $\overline{\Psi}(K^\times) \cap \Gamma$ est un $\mathbb{Z}$-module libre de rang 2. Soient (γ_1, γ_2) une base de ce $\mathbb{Z}$-module. On définit une nouvelle période I_Ψ, avec $\tau \in \mathcal{H}_p$ et $x \in \mathbb{P}_1(\mathbb{Q})$ comme suit :

$$I_\Psi := <\gamma_1, \gamma_2>_\Psi = \oint_\tau^{\gamma_1^{-1}\tau} \int_x^{\gamma_2 x} \omega \div \oint_\tau^{\gamma_2^{-1}\tau} \int_x^{\gamma_1 x} \omega$$

Cette période est indépendante du choix de τ et de x. $< .,. >_\Psi$ est un accouplement bilinéaire alterné et $\{I_\Psi, I_\Psi^{-1}\}$ est indépendant de la base choisie.
On a un théorème analogue à celui de la partie précédente :

Théorème 3.8.
$$\log(I_\Psi) = \frac{\log(q)}{ord_p(q)} ord_p(I_\Psi).$$

Arrivés à ce point, pour comprendre ce que renferme cette période il nous faut reprendre les considérations cohomologiques entrevues plus haut. Elles permettront de démontrer le théorème précédent et de formuler une conjecture précise au sujet de I_Ψ.

Cohomologie des M-symboles : Un M-symbole à valeur dans un groupe G est une application $m : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \longrightarrow G$ satisfaisant $\forall x, y, z \in \mathbb{P}_1(\mathbb{Q})$:

$$m\{x \to y\} + m\{y \to z\} = m\{x \to z\}$$

Et :
$$m\{x \to y\} = -m\{y \to x\}$$

On notera $\mathcal{M}(G)$ l'ensemble des M-symboles à valeur dans G. Les groupes $PSL_2(\mathbb{Q})$ et Γ agissent sur $\mathcal{M}(G)$ par :

$$(\gamma m)\{x \to y\} := m\{\gamma^{-1}x \to \gamma^{-1}y\}$$

Prenons $\tau \in \mathcal{H}_p, x \in \mathbb{P}_1(\mathbb{Q})$. On peut construire un cocycle $\widetilde{c}_{f,\tau} \in Z^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$ grâce à l'intégrale double multiplicative en posant :

$$\widetilde{c}_{f,\tau}(\gamma)\{x \to y\} = \oint_z^{\gamma z} \int_x^y \omega.$$

Ce cocycle est dans une classe $c_f \in H^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$.

On montre alors que $ord_p(c_f)$ et $\log(c_f)$ appartiennent tous deux au même sous-espace vectoriel de $H^1(\Gamma, \mathbb{C}_p)$, et que ce sous-espace $H^1(\Gamma, \mathbb{C}_p)^{f,w_\infty}$ est de dimension 1. En utilisant ensuite le théorème 3.2 on peut conclure :

$$\log(c_f) = \frac{\log(q)}{ord_p(q)} ord_p(c_f).$$

(plus précisément $H^f = \{c \in H \mid T_l(c) = a_l(f)c \ , \forall l \not| N\}$ et $H^{w_\infty} = \{f \in H \mid W_\infty(f) = w_\infty f\}$ avec T_l l'opérateur de Hecke et W_∞ l'involution d'Atkin-Lehner).
Ceci démontre le théorème 3.8. On fait alors la conjecture suivante :

Conjecture 3.9.

$$\exists \widetilde{e}_{f,\tau} \in Z^1(\Gamma, \mathcal{M}(\mathbb{Z}))\ , \exists \widetilde{\eta}_{f,\tau} \in \mathcal{M}((\mathbb{Q}_p(\tau))^\times)\ , \forall \gamma \in \Gamma\ , \forall x, y \in \mathbb{P}_1(\mathbb{Q}) :$$

$$\widetilde{c}_{f,\tau}(\gamma)\{x \to y\} = q^{\widetilde{e}_{f,\tau}(\gamma)\{x \to y\}} \times (\widetilde{\eta}_{f,\tau}\{\gamma^{-1}x \to \gamma^{-1}y\} \div \widetilde{\eta}_{f,\tau}\{x \to y\})$$

On obtient alors, en admettant cette conjecture que la nouvelle période I_Ψ est elle aussi dans $q^{\mathbb{Z}}$. L'information sur la courbe est donc bien faible là encore. Cependant c'est cette même conjecture qui rendra l'étude suivante plus heureuse.

3.3 Cas où p est inerte dans K

3.3.1 Une première idée

On considère K à la fois comme sous-corps de $\mathbb{R}$ et de $\mathbb{C}_p$. Pour tout $x \in K$ on note $\overline{x}$ le conjugué de x par l'action de Galois. Fixons $\Psi : K \longrightarrow M_2(\mathbb{Q})$. $\Psi^{-1}(R)$ est un $\mathbb{Z}[\frac{1}{p}]$-ordre de K. On l'appelle $\mathcal{O}$.
Le tore $\overline{\Psi}(K^\times)$ agissant sur $\mathcal{H}_p$ par Möbius a deux points fixes dans $\mathbb{P}_1(K_p) - \mathbb{P}_1(\mathbb{Q}_p)$ qui sont conjugués par $Gal(K_p \mid \mathbb{Q}_p)$. Notons les z_Ψ et $\overline{z_\Psi}$.
D'après le théorème des unités de Dirichlet, le sous-groupe des unités de norme 1 de $\mathcal{O}^\times$ est engendré par un élément u. Soit $\gamma_\Psi := \overline{\Psi}(u)$. On peut alors associer une période naturellement reliée à Ψ :

$$I_\Psi := \oint_{\overline{z_\Psi}}^{z_\Psi} \int_x^{\gamma_\Psi x} \omega \in K_p^\times$$

Lemme 3.10. *La période I_Ψ ne dépend que de la Γ-classe de conjugaison de Ψ.*

Cette construction va permettre de formuler une conjecture donnant, cette fois-çi, une méthode pour trouver des points algébriques sur la courbe. Notons H^+ le "strict ring class field" de conducteur c.

Conjecture 3.11. *Le point local $P_\Psi^- := \Phi_{Tate}(I_\Psi) \in E(K_p)$ est un point global dans $E(H^+)$.*

3.3.2 Vers une réciprocité à la Shimura

On ne s'arrête cependant pas là. En effet, cherchant à généraliser la construction des points de Heegner, on voudrait que nos points conjecturaux vérifient le même type de relation, dite "loi de réciprocité de Shimura". Cette loi décrit en fait l'action de $Gal(H^+ \mid K)$ sur les points P_Ψ. On va donc

poursuivre en ce sens :
Choisissons une Γ-orbite dans $\mathbb{P}_1(\mathbb{Q})$, par exemple $\Gamma\infty$. Pour $x \in \Gamma\infty$ on pose alors :

$$J_\Psi := \oint^{z_\Psi} \int_x^{\gamma_\Psi x} \omega \in K_p^\times/Q.$$

Remarque : J_Ψ est en fait $\eta_{f,z_\Psi}\{x \to \gamma_\Psi x\}$ si on utilise les notations de la partie précédente. On insiste ici sur le fait que c'est la conjecture 3.9 qui permet cette définition (il suffit de réduire l'énoncé de la conjecture modulo $q^{\mathbb{Z}}$).

Lemme 3.12. *La période J_Ψ ne dépend que de la classe de conjugaison de Ψ.*

Nous devons introduire quelques notations à présent :

- $\gamma \in \Gamma$ est dit rationnel si ses points fixes pour l'action de Möbius sont dans $\mathbb{P}_1(\mathbb{Q})$.
- Soit $\Gamma' \subset \Gamma$ le plus petit sous-groupe distingué contenant les commutateurs et les rationnels de Γ. Alors Γ/Γ' est un groupe abélien fini. Notons e_Γ son exposant.
- Soit $L = \mathbb{Q}_p(\tau)$. On pose $Q_0 := (L^\times/q^{\mathbb{Z}})[e_\Gamma]$ (éléments de e_Γ-torsion).
- On note enfin Q l'image réciproque de Q_0 par la projection naturelle de $L^\times$ sur $L^\times/q^{\mathbb{Z}}$.

On a alors le :

Lemme 3.13. *Pour tout plongement Ψ de K dans $M_2(\mathbb{Q})$ on a :*

$$J_\Psi/\overline{J_\Psi} = \oint_{\overline{z_\Psi}}^{z_\Psi} \int_x^{\gamma_\Psi x} \omega = I_\Psi \ (mod\, Q) \ \in K_p^\times.$$

On n'a jusqu'ici obtenu qu'un élément J_Ψ défini modulo Q. Introduisons alors t l'exposant du groupe Q_0. Elever à la puissance t envoie Q dans $q^{\mathbb{Z}}$ donc $J_\Psi^t \in K_p^\times/q^{\mathbb{Z}}$. On peut donc conjecturer la chose suivante :

Conjecture 3.14. *Le point local $P_\Psi := \Phi_{Tate}(J_\Psi^t) \in E(K_p)$ est un point global de $E(H^+)$.*

Or on dispose d'un isomorphisme, en introduisant $Pic^+(\mathcal{O})$ le groupe de Picard strict (groupe des classes d'équivalence stricte d'idéaux fractionnaires de $\mathcal{O}$) :

$$rec : Pic^+(\mathcal{O}) \longrightarrow^{\simeq} Gal(H^+ \mid K)$$

On va alors raffiner la conjecture en énonçant :

Conjecture 3.15. *Les points* $P_\Psi \in E(H^+)$ *satisfont :*

$$\forall c \in Pic^+(\mathcal{O}), \quad P_{c*\Psi} = rec(c)^{-1}(P_\Psi).$$

On appelle ces points des points de Stark-Heegner car la contribution de H.M.Stark aux méthodes utilisées ici est importante [16]. Elle est valable pour p inerte dans K ainsi que pour p ramifié dans K.

4 Ouverture

Nous allons nous pencher, en ouverture, sur la question de la non-trivialité des points de Heegner. Un point sera dit non-trivial s'il n'est pas de torsion. Nous présentons brièvement ce qui se passe dans le cas imaginaire, où les choses sont connues depuis peu, pour aborder ensuite le cas réel, en gardant à l'esprit que les points de Stark-Heegner sont encore une conjecture.

4.1 Non-trivialité dans le cas imaginaire

Dans le cas où K est un corps quadratique imaginaire, on sait désormais qu'il existe des points de Heegner non-triviaux, c'est-à-dire des points d'ordre infini. Ceci a fait l'objet d'un travail de C.Cornut [9] suite à une conjecture de B.Mazur [11] . Nous en rappelons ici quelques étapes.

Reprenons :

$$\varphi : X_0(N) \longrightarrow E(\mathbb{C}).$$

Soit $\mathcal{N}$ un idéal de $\mathcal{O}_K$ (au-dessus de N) tel que $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Alors $\mathbb{C}/\mathcal{O}_K$ et $\mathbb{C}/\mathcal{N}^{-1}$ sont N-isogènes. Prenons alors $c \in \mathbb{N}^*$ premier à N et posons :

$$\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$$

(ordre de conducteur c)

$$\mathcal{N}_c = \mathcal{O}_c \cap \mathcal{N}$$

On a ainsi :

$$x_c := [\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathcal{N}_c^{-1}] \in X_0(N)$$

et le point de Heegner :

$$y_c := \varphi(x_c) \in E(K[c])$$

où on a noté $K[c]$ le "ring class field" de conducteur c.
On sait d'après les travaux de Gross-Zagier [17] que l'on a l'équivalence :

$$Tr_{K[1]/K}(y_1) \notin E(K)_{tors} \Leftrightarrow L^{'}(E/K, 1) \neq 0$$

Soit alors p de divisant pas N ; on pose $K[p^\infty] = \bigcup_{n \geq 0} K[p^n]$. C'est une extension finie de la $\mathbb{Z}_p$-extension anticyclotomique H_∞ de K.
Le théorème est le suivant :

Théorème 4.1.

$$\exists n \geq 0 \;\; Tr_{K[p^\infty]/H_\infty}(y_{p^n}) \notin E(H_\infty)_{tors} \, ,$$

ce qui veut précisément dire qu'il existe un point de Heegner non-trivial, donc une infinité de points non-triviaux.

4.2 Et dans le cas réel

La construction proposée fournit de nombreux points conjecturaux. On a vu qu'ils ne dépendaient que de la classe de conjugaison de Ψ modulo Γ. Rappelons que $\Psi : K \longrightarrow M_2(\mathbb{Q})$ est un plongement de $\mathbb{Q}$-algèbres. On peut décrire cet ensemble par la bijection suivante :

$$\{\Psi : K \to M_2(\mathbb{Q})\}/\Gamma \simeq \{\tau \in \mathcal{H}_p \cap K\}/\Gamma,$$

qui à Ψ associe τ un point fixe de l'action de $\Psi(K^*)$. On a ainsi une infinité de points.
H^+ est une extension de degré fini de K. L'ensemble $E(H^+)_{tors}$ est donc un ensemble fini. Il faut cependant prendre un ensemble plus gros, susceptible d'englober tous les points de Stark-Heegner : en effet ils ne sont, conjecturalement, pas à coordonnées dans le même "ring class field" ! On va donc utiliser un autre résultat présent dans les travaux de C.Cornut : on pose $K[\infty] = \bigcup_{c \geq 1} H_c$, où H_c est le "ring class field" de conducteur c. On a alors :

Théorème 4.2.

$$E(K[\infty])_{tors} \; est \; fini.$$

On a donc que les $P_\Psi \in E(K[\infty])$ sont presque-tous d'ordre infini. Ceci est un résultat de non-trivialité.

On peut donc énoncer :

Théorème 4.3. *Le groupe engendré par les P_Ψ est d'ordre infini.*

5 Annexe : Les conjectures de Birch et Swinnerton-Dyer

La construction de ces points de Stark-Heegner est basée sur de l'analyse, de l'anayse p-adique plus précisément. Or la conjecture formulée plus haut annonce que ces points sont, ou seraient en fait algébriques. Ceci participe d'un mouvement plus profond des recherches présentes et passées visant à établir des liens entre les contructions analytiques et algébriques touchant à l'arithmétique.

En 1900, au congrès international de mathématiques (Paris), David Hilbert propose à la communauté mathématique une liste de 23 problèmes qui ont orienté les travaux du XXe siècle. Parmi ceux-ci le 12e : comment construire par des moyens analytiques l'extension abélienne maximale d'un corps de nombres (par exemple d'un corps quadratique réel, ce qui est intimement lié avec les points de Stark-Heegner) ? Nous allons voir que ces ponts entre approche analytique et algébrique ont donné d'autres idées importantes et en particulier les conjectures qui vont suivre. Il existe en fait plusieurs formulations, nous avons tenté ici de les réunir pour constituer un "bestiaire" de référence.
On peut associer à une courbe elliptique une fonction L regroupant toutes les "informations" locales. On a ainsi :

$$L(E,s) := \prod_{p \notin S} L_p(E,s) = \prod_{p \notin S} \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

avec S un ensemble fini de places contenant celles de mauvaise réduction, N_p le nombre de points dans $E_p(\mathbb{F}_p)$ et $a_p = p + 1 - N_p$.

Les conjectures de Birch et Swinnerton-Dyer relient les fonctions L associées aux courbes elliptiques (ou plus généralement aux variétés abéliennes) au rang du groupe de Mordell-Weil. Or les constructions de points de Heegner ou Stark-Heegner fournissent des renseignements sur le rang de ce groupe puisqu'on peut exhiber des points d'ordre infini. On va présenter ici plusieurs formes de ces conjectures. Nous verrons qu'en plus de proposer un lien entre des êtres analytiques et des êtres algébriques, elles permettent de lier l'aspect local et l'aspect global de l'étude. (Cette question est elle aussi centrale dans la conjecture des points de Stark-Heegner.)

Voici tout d'abord la forme faible de la conjecture sur les courbes elliptiques. Le groupe $E(\mathbb{Q})$ se décompose en une partie de torsion et une partie libre de rang r. On conjecture alors l'égalité du rang et du "rang analytique" :

Conjecture 5.1.
$$ord_{s=1}(L(E,s)) = r$$

Il existe une conjecture plus forte, en admettant la première, dont nous donnons la forme :

Conjecture 5.2.

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\mid sha(E)\mid reg(E)}{\mid E(\mathbb{Q})_{tors}\mid^2} \left(\prod_{p\notin S} \int_{E(\mathbb{Q}_p)} \mid \omega \mid\right) \int_{E(\mathbb{R})} \mid \omega \mid,$$

avec $\omega = \frac{dx}{2y}$, $sha(E)$ le groupe de Tate-Shafarevitch **supposé** fini, $reg(E)$ le régulateur de la courbe, $L(E,s)$ la fonction L de la courbe, r le rang du groupe de Mordell-Weil et S un ensemble fini de places contenant celles de mauvaise réduction.
Cette conjecture a été démontrée dans le cas elliptique, forme faible, pour $r \in \{0,1\}$ par Kolyvagin [18].
Donnons maintenant une forme plus générale de cette conjecture, portant cette fois sur une variété abélienne A quelconque. On note qu'il faut ici supposer en plus que la fonction L admet un prolongement en une fonction entière, chose qui est connue pour une courbe elliptique sur $\mathbb{Q}$ mais déjà difficile à démontrer.

Conjecture 5.3.

$$\lim_{s\to 1} \frac{L(A_U,s)}{(s-1)^r} = \frac{reg(A)\mid sha(A)\mid}{\mid A(K)_{tors}\mid\mid A^\vee(K)_{tors}\mid} \frac{1}{\parallel \mu \parallel^d} \prod_{v\, place\, de\, K} \int_{A(K_v)} \mid \omega \mid_{\mu_v} L_v(A_U,1),$$

si $v \in U$; on remplace $L_v(A_U,1)$ par 1 sinon. On a ici K un corps global, A une variété abélienne sur K de dimension d, X le schéma associé à K, U ouvert de X, A_U schéma abélien sur U de fibre générique A, μ_v mesure de Haar sur K_v telle que $\mu_v(\mathcal{O}_v) = 1$, μ le produit tensoriel des μ_v sur les adèles de K et ω une forme différentielle non nulle de degré d sur A.
On peut enfin citer une autre forme, dite conjecture de Birch et Swinnerton-Dyer p-adique [10, 1]. L'idée est cette fois-ci d'utiliser l'analyse p-adique en lieu et place de l'analyse réelle. En effet pourquoi privilégier la place réelle dans la construction même d'un objet cherchant justement à relier les comportements de toutes les places ? La fonction L a une autre forme :

$$L_p(E,\Psi,s) := \sum_{r=0}^{\infty} \frac{(s-1)^r}{r!} \sum_{a\, mod\, p^\nu M} \Psi(a) \int_{D(a,\nu)} (log_p(x_p))^r.$$

Il y a un phénomène nouveau par rapport à la conjecture non p-adique que l'on nomme “zéro exceptionnel”. Lorsque E est à réduction multiplicative déployée la forme change comme on peut le voir dans l'article [1] dont on garde les notations : on prendra $\Omega_E^+ = \int_{E(\mathbb{C})^+} \omega_E$ et $m_l = l+1-Card(E_l(\mathbb{F}_l))$. La définition de $\mathcal{S}_p(E)$, la “p-adic sparsity", est assez longue et est détaillée dans [1].

Conjecture 5.4. *Cas non-exceptionnel, i.e. E a bonne réduction en p (cas b=2) ou réduction multiplicative non-déployée en p (cas b=1), i.e. $\alpha \neq 1$:*

$$L_p^{(r)}(E) = (1 - \frac{1}{\alpha})^b \mid sha(E) \mid \mathcal{S}_p(E)(\prod_l m_l)\Omega_E^+,$$

avec r le rang de E.

Conjecture 5.5. *Cas exceptionnel, i.e. E a réduction multiplicative déployée en p, i.e. $\alpha = 1$:*

$$L_p^{(r+1)}(E) = \mid sha(E) \mid \mathcal{S}_p(E)(\prod_l m_l)\Omega_E^+.$$

6 Annexe-2 : A propos des noms rencontrés

Voici pour finir un récapitulatif des noms cités dans ce texte, ainsi que les dates (et parfois les lieux) de naissance et de mort (le cas échéant !).

- François *Bruhat* : né en 1929.
- Christophe *Cornut* : né en 1972.
- Henri *Darmon* : né en 1965 à Paris (France).
- Vladimir *Drinfeld* : né en 1954.
- Peter Gustav Lejeune-*Dirichlet* : né en 1805 à Düren (Allemagne), mort en 1859 à Göttingen (Allemagne).
- Evariste *Galois* : né en 1811 et mort en 1832.
- Benedict H. *Gross* : né en 1950.
- Alfred *Haar* : né en 1885 à Budapest (Hongrie) et mort en 1933 à Szeged (Hongrie).
- Erich *Hecke* : né en 1887 à Posen (Allemagne à l'époque, Poznen en Pologne à présent) mort en 1947 à Copenhague (Danemark).
- Marc *Hindry* : né en 1957.
- David *Hilbert* : né en 1862 à Königsberg (Prusse, à présent Kalingrad, Russie) mort en 1943 à Göttingen (Allemagne).
- Joseph *Lehner* : né en 1912.
- Juriz Ivanovitch *Manin* : né en 1937.
- Barry *Mazur* : né en 1937 à New York (Etats-Unis).
- August Ferdinand *Möbius* : né en 1790 à Schulpforta (saxe, Allemagne), mort à Leipzig (Allemagne) en 1868.
- Louis Joël *Mordell* : né en 1888 à Philadelphia (Etats-Unis) mort en 1972 à Cambridge (Angleterre).
- Jan *Nekovàř* : né en 1963.
- Joseph *Oesterlé* : né en 1954.
- Jules Henri *Poincaré* : né en 1854 à Nancy (France), mort en 1912 à Paris (France).
- Georg Friedrich Bernhard *Riemann* : né en 1826 à Breselenz (Allemagne), mort en 1866 à Selesca (Italie).
- Igor Rostislavovitch *Shafarevitch* : né en 1923 en Russie.
- Goro *Shimura* : né en 1930.
- Glenn *Stevens* : né en 1953.
- John *Tate* : né en 1925.
- Jeremy *Teitelbaum* : né en 1959.

- Jacques *Tits* : né en 1930.
- André *Weil* : né en 1906 à Paris (France) et mort en 1998 à Princeton (Etats-Unis).
- Andrew John *Wiles* : né en 1953 à Cambridge (Angleterre).
- Don B. *Zagier* : né en 1951.

Les suivants ont certes existé, on n'en sait pas plus...

- *Néron*
- *Greenberg*
- *Kolyvagin*
- *Stark*
- *Heegner*
- *Birch*
- *Swinnerton-Dyer*

Références

[1] B.Mazur, J.Tate et J.Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* **84**(1986), 1-48.

[2] R.Greenberg et G.Stevens. p-adic L-functions and p-adic periods of modular forms, *Invent. Math.* **111** (1993), 407-447.

[3] L.Gerritzen et M.Van der Put. Schottky Groups and Mumford Curves, *Lecture Notes in Math.* **817**, Springer-Verlag, New York, 1980.

[4] J.P.Serre. Arbres et amalgames.

[5] A.Wiles. Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), 443-551.

[6] R.Taylor and A.Wiles. Ring-theoretic propeties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553-572.

[7] C.Breuil, B.Conrad, F.Diamond and R.Taylor. On the modularity of elliptic curves over (Q) : Wild 3-adic exercices, *J.Amer. Math. Soc.* **14** (2001), 843-939.

[8] H.Darmon et P.Green. Elliptic curves and class fields of real quadratic fields : algorithm and evidence, *J. of Experimental Math.*

[9] C.Cornut. Mazur's conjecture on higher Heegner points, *Invent. Math.* **148** (2001), 495-523.

[10] B.Mazur et J.Tate. Refined conjectures of the "Birch and Swinnerton-Dyer" type, *Duke Math.J.* **54** (1987), 711-750.

[11] B.Mazur. Modular curves and arithmetic, *Proceedings in the international Congress of Math.* Warsaw 1983, PWN, 549-556 (1984).

[12] J.H.Silverman. Advanced topics in the arithmetic of elliptic curves, *Grad. Texts in Math.*, Springer-Verlag, New York, 1994.

[13] H.Darmon. Integration on $\mathcal{H}_p \times \mathcal{H}$ and its arithmetic applications, *Ann. of Math.* **154** (2001), 589-639.

[14] H.Darmon. Rationnal points on modular elliptic curves, *NSF-CBMS Lectures*, August 2001, to appear.

[15] B.Edixhoven. On the Manin constants of modular elliptic curves, in *Arithmetic Algebraic Geometry* (Texel 1989) 25-39, *Progr.Math.*, Birkhäuser Boston, MA, 1991.

[16] H.M.Stark. Modular forms and related objects, in *Number Theory* (Montreal, Quebec 1985), 421-455, *CMS Conf.Proc.* **7** A.M.S., Providence, R.I. 1987.

[17] B.H.Gross et D.B.Zagier. Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225-320.

[18] V.A.Kolyvagin. Euler systems, The Grothendieck Festschrift, *Prog. in Math.*,Boston, Birkhäuser (1990).

[19] Modular functions of one variable II, *Lecture notes in mathematics*, University of Antwerp (1972).