

# La constante de Manin et le degré modulaire d'une courbe elliptique

Karim Belabas, Dominique Bernardi, Bernadette Perrin-Riou

# ▶ To cite this version:

Karim Belabas, Dominique Bernardi, Bernadette Perrin-Riou. La constante de Manin et le degré modulaire d'une courbe elliptique. Publications Mathématiques de Besançon. Algèbre et Théorie des Nombres, A paraître. hal-01766202v2

# HAL Id: hal-01766202 https://hal.science/hal-01766202v2

Submitted on 4 May 2018 (v2), last revised 8 Sep 2019 (v3)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# La constante de Manin et le degré modulaire d'une courbe elliptique

Karim Belabas<sup>\*</sup>, Dominique Bernardi<sup>\*\*</sup> et Bernadette Perrin-Riou<sup>\*\*\*</sup>

<sup>\*</sup>Univ. Bordeaux, CNRS, INRIA, IMB, UMR 5251, F-33400 Talence, France <sup>\*\*</sup>IMJ-PRG, UPMC, 4 place Jussieu, F-75005 Paris, France <sup>\*\*\*\*</sup>Laboratoire de Mathématiques d'Orsay, Univ. Paris-Sud, CNRS, Université Paris-Saclay, F-91405 Orsay, France.

## 4 mai 2018

#### Abstract

We revisit the calculation of the strong Weil curve in an isogeny class of elliptic curves over  $\mathbb{Q}$ , of the Manin constant and modular degree of an elliptic curve, using modular symbols as defined in [9], now implemented in Pari/GP. There is no innovation claim.

On revisite les procédures de calcul de la courbe de Weil forte d'une classe d'isogénie de courbes elliptiques sur Q, de la constante de Manin et du degré modulaire d'une courbe elliptique en utilisant les symboles modulaires tels qu'ils sont décrits dans [9] et désormais implémentés dans Pari/GP. Il n'y a aucune prétention à une nouveauté quelconque.

Le troisième auteur (en particulier) remercie chaleureusement Bill Allombert pour l'avoir lancée sur cette question, ce qui l'a obligée à relire les articles fondateurs des années 1970 sur cette question.

Les calculs présentés à la fin de cet article ont été réalisés sur la plateforme PLAFRIM, portée par l'action de développement INRIA PlaFRIM avec le soutien de l'IMB, du LaBRI et d'autres entités : Conseil Régional d'Aquitaine, FeDER, Université de Bordeaux et CNRS (voir https://www.plafrim.fr/en/home/).

# Table des matières

1	Rap	pels sur les constantes de Manin et le degré modulaire	2
2	Espa	ace des symboles modulaires	2
	2.1	Lien entre l'espace des symboles modulaires et les cohomologies	2
	2.2	Structure entière de l'espace des symboles modulaires	3
3	Espa	ace associé à une forme modulaire et à une courbe elliptique	3
	3.1	Structure rationnelle	3
	3.2	Structure entière $\mathcal{L}_f$ associée à une forme modulaire propre	4
	3.3	Quelques bases particulières de l'homologie de <i>E</i>	4
	3.4	Structure entière $\mathcal{L}_E$ associée à une courbe elliptique	5
	3.5	Calcul de $\mathcal{L}_E$	6
4	Con	séquences	7
	4.1	Critère de calcul de la courbe de Weil forte et de sa constante de Manin	7
	4.2	Graphe orienté des isogénies admissibles	7
	4.3	Degré modulaire et constante de Manin	8
A	Prog	grammes	9

#### **B** Quelques exemples

# **1** Rappels sur les constantes de Manin et le degré modulaire

Reprenons quelques définitions et énoncés de [6].

**Définition 1.1.** Une paramétrisation modulaire  $\pi$  d'une courbe elliptique  $E/\mathbb{Q}$  de conducteur N est un morphisme non constant  $\pi_{\text{mod}} : X_0(N) \to E$  défini sur  $\mathbb{Q}$  tel que l'image de  $\infty$  est 0 et tel que si  $\omega$  est une forme différentielle invariante non nulle de E sur  $\mathbb{Q}$ , l'image réciproque  $\pi^* \omega$  sur  $X_0(N)$  vue comme une forme modulaire parabolique est de niveau exactement N. Autrement dit, il existe un rationnel c non nul et une forme f primitive de niveau N(vecteur propre pour tous les opérateurs de Hecke de niveau N et normalisée par  $a_1(f) = 1$ ) tels que  $\pi^*_{\text{mod}}\omega = c\omega_f$ avec  $\omega_f = 2i\pi f(z)dz \in (1 + q\mathbb{Z}[[q]])dq$  pour  $q = \exp(2i\pi z)$ .

**Définition 1.2.** — Le degré modulaire deg(E) de E est le degré minimal parmi les paramétrisations modulaires de E.

— Soit  $\omega_E$  une forme différentielle de Néron de *E*. La *constante de Manin* de *E* est le rationnel  $c_E > 0$  tel que  $\pi^*_{\min E} \omega_E = c_E \omega_f$  pour une paramétrisation minimale  $\pi_{\min,E}$  de *E*.

Soit  $\mathcal{E}$  une classe d'isogénie de courbes elliptiques sur  $\mathbb{Q}$ . Il existe une unique courbe  $E_1$  dans  $\mathcal{E}$  et une unique paramétrisation modulaire  $\pi_1 : X_0(N) \to E_1$  (à isomorphisme près) telle que toute paramétrisation modulaire  $\pi : X_0(N) \to E$ pour  $E \in \mathcal{E}$  se factorise par  $\pi_1$ .



Le degré de  $\pi_1 : X_0(N) \to E_1$  est minimal parmi les degrés des paramétrisations modulaires des courbes elliptiques de la classe d'isogénie  $\mathcal{E}$ . Si f est la forme modulaire parabolique associée à  $\mathcal{E}$ , la courbe  $E_1$  est la courbe de Weil forte associée à f.

On la construit de la manière suivante. Soit  $\pi' : X_0(N) \to E'$  une paramétrisation modulaire de E' dans la classe d'isogénie  $\mathcal{E}$ . Par passage à la jacobienne, on en déduit un homomorphisme de variétés abéliennes  $\pi : J_0(N) \to E'$ . Soit A le noyau de  $\pi$ . La composante connexe  $A^0$  de l'élément neutre dans A est une variété abélienne qui ne dépend pas de la paramétrisation  $\pi', E_1 = J_0(N)/A^0$  est une courbe elliptique et on a le diagramme commutatif



**Lemme 1.3.** Soit  $\pi$  :  $X_0(N) \to E$  une paramétrisation modulaire minimale. Alors, E est une courbe elliptique de Weil forte si et seulement si  $H_1(X_0(N), \mathbb{Z}) \to H_1(E, \mathbb{Z})$  est surjective.

Voir lemme 3, § 4 de [6].

# 2 Espace des symboles modulaires

#### 2.1 Lien entre l'espace des symboles modulaires et les cohomologies

Soit  $\Delta = \mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]$  le groupe des diviseurs sur  $\mathbb{P}^1(\mathbb{Q})$  et  $\Delta_0$  le sous-module des diviseurs de  $\Delta$  de degré 0. Les éléments de  $\Delta_0$  peuvent être vus comme des combinaisons linéaires dans  $\mathbb{Z}$  de chemins (a,b) pour a et b dans  $\mathbb{P}^1(\mathbb{Q})$ . Les modules  $\Delta$  et  $\Delta_0$  sont munis d'une action de  $SL_2(\mathbb{Z})$  et donc de  $\Gamma = \Gamma_0(N)$ . On a une suite exacte

$$0 \to \operatorname{Hom}_{\Gamma}(\mathbb{Z},\mathbb{Q}) \to \operatorname{Hom}_{\Gamma}(\Delta,\mathbb{Q}) \to \operatorname{Hom}_{\Gamma}(\Delta_{0},\mathbb{Q}) \to \operatorname{Ext}_{\Gamma}^{1}(\mathbb{Z},\mathbb{Q}) \to \operatorname{Ext}_{\Gamma}^{1}(\Delta,\mathbb{Q}) \to \operatorname{Ext}_{\Gamma}^{1}(\Delta_{0},\mathbb{Q}) \to 0$$

ou en explicitant

$$0 \to \mathbb{Q} \to \bigoplus_{s \in C(\Gamma)} H^0(\Gamma_s, \mathbb{Q}) \to \operatorname{Hom}_{\Gamma}(\Delta_0, \mathbb{Q}) \to H^1(\Gamma, \mathbb{Q}) \to \bigoplus_{s \in C(\Gamma)} H^1(\Gamma_s, \mathbb{Q}) \to \operatorname{Ext}^1_{\Gamma}(\Delta_0, \mathbb{Q}) \to 0$$

où  $C(\Gamma)$  est un système de représentants de  $\Gamma \setminus \mathbb{P}^1(\mathbb{Q})$  et  $\Gamma_s$  le stabilisateur de *s* dans  $\Gamma$ . L'application  $\operatorname{Hom}_{\Gamma}(\Delta_0, \mathbb{Q}) \to H^1(\Gamma, \mathbb{Q})$  est donnée par  $\Phi \mapsto \left(\gamma \mapsto \Phi((0, \gamma^{-1}0))\right)$ . La formule des coefficients universels en cohomologie implique la suite exacte

$$0 \to \operatorname{Ext}^{1}(H_{0}(X_{0}(N),\mathbb{Z}),\mathbb{Z}) \to H^{1}(X_{0}(N),\mathbb{Z}) \to \operatorname{Hom}(H_{1}(X_{0}(N),\mathbb{Z}),\mathbb{Z}) \to 0$$

On en déduit que

$$H^1(X_0(N),\mathbb{Z}) = \operatorname{Hom}(H_1(X_0(N),\mathbb{Z}),\mathbb{Z})$$

Rappelons les résultats de Manin ([5]). Si *a* et *b* dans  $\mathbb{P}^1(\mathbb{Q})$  sont équivalents modulo  $\Gamma_0(N)$ , l'image de l'arc géodésique (a,b) joignant *a* à *b* dans  $\mathcal{H}$  définit un élément de  $H_1(X_0(N),\mathbb{Z})$ . De plus, si  $a \in \mathbb{P}^1(\mathbb{Q})$ , les éléments de la forme (a,b) avec *b* équivalent à *a* modulo  $\Gamma_0(N)$  engendrent  $H_1(X_0(N),\mathbb{Z})$  ([5], proposition 1.4). On peut prolonger cette application aux arcs géodésiques de la forme (a,b) avec *a* et *b* dans  $\mathbb{P}^1(\mathbb{Q})$  à condition d'étendre les valeurs à  $H_1(X_0(N),\mathbb{Q}) = \mathbb{Q} \otimes H_1(X_0(N),\mathbb{Z})$ . On en déduit une application surjective

$$\Delta_0 \to H_1(X_0(N), \mathbb{Q})$$

et par dualité un homomorphisme injectif

 $\operatorname{Hom}_{\mathbb{Q}}(H_1(X_0(N),\mathbb{Q}),\mathbb{Q}) \to \operatorname{Hom}_{\mathbb{Z}}(\Delta_0,\mathbb{Q})$ 

à valeurs dans les invariants par  $\Gamma_0(N)$ , donc un homomorphisme injectif

$$\operatorname{Hom}_{\mathbb{Q}}(H_1(X_0(N),\mathbb{Q}),\mathbb{Q}) \to \operatorname{Hom}_{\Gamma_0(N)}(\Delta_0,\mathbb{Q})$$

que l'on note provisoirement  $h \to \tilde{h}$ . Son image est d'intersection nulle avec l'image de  $\operatorname{Hom}_{\Gamma_0(N)}(\Delta, \mathbb{Q})$ . En effet, soit h un élément de  $\operatorname{Hom}_{\mathbb{Q}}(H_1(X_0(N), \mathbb{Q}), \mathbb{Q})$  tel que  $\tilde{h}$  est l'image de  $\tilde{h}_1 \in \operatorname{Hom}_{\Gamma_0(N)}(\Delta, \mathbb{Q})$ . Si c est un lacet partant de  $x_0 \in \mathbb{P}^1(\mathbb{Q})$ , son relèvement dans  $\mathcal{H}$  joint  $x_0$  à  $\gamma^{-1}x_0$  pour un  $\gamma$  dans  $\Gamma_0(N)$  et  $h(c) = \tilde{h}((x_0, \gamma^{-1}x_0)) = \tilde{h}_1([\gamma^{-1}x_0]) - \tilde{h}_1([x_0]) = 0$  puisque  $\tilde{h}_1$  est invariant par  $\Gamma_0(N)$ .

Pour une raison de dimension (les deux espaces sont de dimension 2 fois le genre de  $X_0(N)$ ), on en déduit les isomorphismes

 $H^{1}(X_{0}(N),\mathbb{Q}) \xrightarrow{\cong} \operatorname{Hom}_{\mathbb{Q}}(H_{1}(X_{0}(N),\mathbb{Q}),\mathbb{Q}) \xrightarrow{\cong} \operatorname{Hom}_{\Gamma_{0}(N)}(\Delta_{0},\mathbb{Q})/\operatorname{Hom}_{\Gamma_{0}(N)}(\Delta,\mathbb{Q})$ 

## 2.2 Structure entière de l'espace des symboles modulaires

Remarquons que le  $\mathbb{Z}$ -module  $H^1(\Gamma_0(N),\mathbb{Z})$  s'injecte dans  $H^1(\Gamma_0(N),\mathbb{Q})$ . Cela se voit facilement en écrivant la suite de cohomologie pour la suite exacte  $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$  de  $\Gamma_0(N)$ -modules.

On note  $W = \operatorname{Hom}_{\Gamma_0(N)}(\Delta_0, \mathbb{Q}) / \operatorname{Hom}_{\Gamma_0(N)}(\Delta, \mathbb{Q})$  et  $W_{par}$  le supplémentaire de  $\operatorname{Hom}_{\Gamma_0(N)}(\Delta, \mathbb{Q})$  dans  $\operatorname{Hom}_{\Gamma_0(N)}(\Delta_0, \mathbb{Q})$ stable par l'algèbre de Hecke. Soient  $\mathcal{W} \subset W$  et  $\mathcal{W}_{par} \subset W_{par}$  les sous- $\mathbb{Z}$ -modules formés des éléments dont l'image dans  $H^1(\Gamma_0(N), \mathbb{Q})$  appartient à l'image de  $H^1(\Gamma_0(N), \mathbb{Z})$  dans  $H^1(\Gamma_0(N), \mathbb{Q})$ .

**Lemme 2.1.** Les  $\mathbb{Z}$ -modules  $\mathcal{W}$  et  $\mathcal{W}_{par}$  sont de type fini et de rang maximal, respectivement dans  $\mathcal{W}$  et  $\mathcal{W}_{par}$ .

Pour une démonstration analogue, voir par exemple [11], Proposition 1.

# **3** Espace associé à une forme modulaire et à une courbe elliptique

### 3.1 Structure rationnelle

Soit *E* une courbe elliptique sur  $\mathbb{Q}$  de niveau *N*, *f* la forme modulaire parabolique normalisée de poids 2 pour  $\Gamma_0(N)$  qui lui est associée et  $\pi : X_0(N) \to E$  une paramétrisation modulaire de *E*.

Soit  $V_f$  le  $\mathbb{Q}$ -espace vectoriel de  $W = \text{Hom}_{\Gamma_0(N)}(\Delta_0, \mathbb{Q})$  associé obtenu par décomposition par les opérateurs de Hecke . Autrement dit,  $V_f$  est l'ensemble des éléments v de  $\text{Hom}_{\Gamma_0(N)}(\Delta_0, \mathbb{Q})$  tel que  $(T(n) - a_n(f))v = 0$  pour tout entier  $n \ge 1$ . Il est en fait contenu dans le sous-espace  $W_{par}$  de W.

On a un diagramme commutatif



## **3.2** Structure entière $L_f$ associée à une forme modulaire propre

Soit  $\mathcal{L}_f$  le  $\mathbb{Z}$ -sous-module de  $V_f$  défini par  $\mathcal{L}_f = V_f \cap \mathcal{W}$ . C'est donc l'ensemble des éléments  $\Phi$  de  $V_f$  tels que  $\Phi((0,\gamma^{-1}0)) \in \mathbb{Z}$  pour tout  $\gamma \in \Gamma_0(N)$ . C'est aussi  $H^1(X_0(N),\mathbb{Z}) \cap V_f$  (ici, on voit simplement  $H^1(X_0(N),\mathbb{Z})$  comme le dual sur  $\mathbb{Z}$  de  $H_1(X_0(N),\mathbb{Z})$ ).

## 3.3 Quelques bases particulières de l'homologie de E

Plusieurs bases de  $H_1(E,\mathbb{Z})$  sont construites. La première est définie à l'aide des sous-espaces propres par la conjugaison complexe sur  $E(\mathbb{C})$  dans un modèle minimal de Weierstrass, la seconde est liée à la paramétrisation modulaire de E.

#### 3.3.1 Réseau associé à un modèle minimal

Faisons quelques rappels sur les périodes complexes de *E*. On note  $c_{\infty}$  le nombre de composantes connexes de  $E(\mathbb{R})$ . Soit  $\Lambda_E$  le réseau des périodes de *E* dans un modèle minimal, autrement dit le sous- $\mathbb{Z}$ -module de rang 2 de  $\mathbb{C}$  formé des nombres  $\int_c \omega_E$  pour  $c \in H_1(E, \mathbb{Z})$ . Soient  $\Omega_E^+ \in \mathbb{R}^+$  et  $\Omega_E^- \in i\mathbb{R}^+$  tels que  $\mathbb{Z}\Omega_E^+ = \Lambda_E \cap \mathbb{R}$ ,  $\mathbb{Z}\Omega_E^- = \Lambda_E \cap i\mathbb{R}$ ; on note  $\Omega_1 = \Omega^+$  et <sup>1</sup>

$$\Omega_2 = \begin{cases} \frac{1}{2}(\Omega_E^+ + \Omega_E^-) & \text{si } c_\infty = 1, \\ \Omega_E^- & \text{si } c_\infty = 2. \end{cases}$$

On a  $\Lambda_E = \mathbb{Z}\Omega_1 + \mathbb{Z}\Omega_2$  et  $\Omega_E^+ \Omega_E^- = \frac{2}{c_{\infty}} \operatorname{Aire}(\Lambda_E)$ . Notons  $\delta_+, \delta_-, \delta_1$  et  $\delta_2$  les éléments de  $H_1(E, \mathbb{Z})$  tels que

$$\int_{\delta_+} \omega_E = \Omega_E^+, \quad \int_{\delta_-} \omega_E = \Omega_E^-, \quad \int_{\delta_1} \omega_E = \Omega_1, \quad \text{et} \quad \int_{\delta_2} \omega_E = \Omega_2.$$

Bien sûr,  $\delta_1 = \delta_+$  et

$$\frac{2}{c_{\infty}} \delta_2 = \begin{cases} \delta_- + \delta_+ & \text{si } c_{\infty} = 1, \\ \delta_- & \text{si } c_{\infty} = 2. \end{cases}$$

On note  $(\delta_+^*, \delta_-^*)$  (resp.  $(\delta_1^*, \delta_2^*)$ ) la base duale de  $(\delta_+, \delta_-)$  (resp.  $(\delta_1, \delta_2)$ ) dans  $H^1(E, \mathbb{Z}) = \operatorname{Hom}_{\mathbb{Z}}(H_1(E, \mathbb{Z}), \mathbb{Z})$ :  $(\delta_1, \delta_2)$  est une base de  $H_1(E, \mathbb{Z})$  et  $(\delta_1^*, \delta_2^*)$  est une base de  $H^1(E, \mathbb{Z})$ . Explicitement, on a

$$\delta_2^* = \frac{2}{c_\infty} \delta_-^* \quad \text{et} \quad \delta_1^* = \begin{cases} \delta_+^* - \delta_-^* & \text{si } c_\infty = 1, \\ \delta_+^* & \text{si } c_\infty = 2. \end{cases}$$

$$\omega_{2} = \begin{cases} \frac{1}{2} (\Omega_{E}^{+} - \Omega_{E}^{-}) = \Omega_{1} - \Omega_{2} & \text{si } c_{\infty} = 1, \\ -\Omega_{E}^{-} = -\Omega_{2} & \text{si } c_{\infty} = 2. \end{cases}$$

<sup>1.</sup> La normalisation de  $(\omega_1, \omega_2) = \mathbb{E}$ . omega dans Pari/GP change le signe de  $\Omega_E^-$ : on a  $\omega_1 = \Omega_1$  et

On en déduit l'action de la conjugaison complexe  $\sigma$  sur la base  $(\delta_1^*, \delta_2^*)$ 

$$\sigma \delta_2^* = -\delta_2^* \quad \text{et} \quad \begin{cases} \sigma \delta_1^* = \delta_1^* + \delta_2^* & \text{si } c_\infty = 1 \\ \sigma \delta_1^* = \delta_1^* & \text{si } c_\infty = 2. \end{cases}$$

#### 3.3.2 Réseau associé à la paramétrisation modulaire

Fixons une paramétrisation modulaire minimale  $\pi : X_0(N) \to E$ . On note  $(n_{1,E}, n_{2,E})$  les diviseurs élémentaires de l'image  $\pi_*H_1(X_0(N),\mathbb{Z})$  de  $H_1(X_0(N),\mathbb{Z})$  dans  $H_1(E,\mathbb{Z})$  : il existe une base  $(\delta_1, \delta_2)$  de  $H_1(E,\mathbb{Z})$  et une base  $(\pi_*(\beta_1), \pi_*(\beta_2))$  de  $\pi_*H_1(X_0(N),\mathbb{Z})$  telles que

$$\begin{cases} \pi_*(\beta_1) &= n_{1,E} \cdot \delta_1, \\ \pi_*(\beta_2) &= n_{2,E} \cdot \delta_2, \end{cases}$$

et les deux entiers positifs  $n_{1,E}$  et  $n_{2,E}$ ,  $n_{2,E} \mid n_{1,E}$ , sont uniques.

## 3.4 Structure entière $\mathcal{L}_E$ associée à une courbe elliptique

So it une base  $\mathcal{B} = (\delta_1, \delta_2)$  de  $H_1(E, \mathbb{Z})$ . On note  $(\delta_1^*, \delta_2^*)$  la base de  $H^1(E, \mathbb{Z})$  duale : on a donc pour  $\delta \in H_1(E, \mathbb{Q})$ 

$$\delta = \delta_1^*(\delta) \cdot \delta_1 + \delta_2^*(\delta) \cdot \delta_2$$

et si  $\omega \in H^0(E, \Omega^1_E)$ 

$$\int_{\delta} \omega = \delta_1^*(\delta) \int_{\delta_1} \omega + \delta_2^*(\delta) \int_{\delta_2} \omega$$

En particulier, si  $\omega_E$  est une forme différentielle de Néron de *E*, on a

$$\int_{\delta} \omega_E = \delta_1^*(\delta) \cdot \Omega_{E,1} + \delta_2^*(\delta) \cdot \Omega_{E,2}$$

avec  $\Omega_{E,i} = \int_{\delta_i} \omega_E$ . Soient  $\Phi_{E,1}^{\mathcal{B}}, \Phi_{E,2}^{\mathcal{B}}$  les éléments de  $V_f$  définis pour  $\beta \in H_1(X_0(N), \mathbb{Z})$  par

$$\int_{\beta} \omega_f = \Phi_{E,1}^{\mathcal{B}}(\beta) \int_{\delta_1} \omega_E + \Phi_{E,2}^{\mathcal{B}}(\beta) \int_{\delta_2} \omega_E \tag{1}$$

(seule la *f*-composante intervient).

**Définition 3.1.** Le sous- $\mathbb{Z}$ -module de  $V_f$  engendré par  $\Phi_{E,1}^{\mathcal{B}}$  et  $\Phi_{E,2}^{\mathcal{B}}$  ne dépend pas de la base choisie  $\mathcal{B}$ . On le note  $\mathcal{L}_E$ .

**Lemme 3.2.** Les diviseurs élémentaires (au sens généralisé) de  $\mathcal{L}_E$  dans  $\mathcal{L}_f$  sont  $(\frac{n_{1,E}}{c_E}, \frac{n_{2,E}}{c_E})$ .

*Démonstration.* Si  $n \in \mathbb{Z}$ ,  $\beta \in H_1(X_0(N), \mathbb{Z})$  et  $\delta \in H_1(E, \mathbb{Z})$  sont tels que  $n \cdot \delta = \pi_*(\beta)$ , on a

$$n\int_{\delta}\omega_E = \int_{\pi_*\beta}\omega_E = \int_{\beta}\pi^*\omega_E = c_E\int_{\beta}\omega_f$$

puisque  $\pi^* \omega_E = c_E \omega_f$ . Lorsque  $\mathcal{B} = (\delta_1, \delta_2)$  est une base de  $H_1(E, \mathbb{Z})$  adaptée aux diviseurs élémentaires de l'image de  $H_1(X_0(N), \mathbb{Z})$  dans  $H_1(E, \mathbb{Z})$  comme en 3.3.2, en appliquant cela à  $\beta_1$  et  $\beta_2$ , l'équation (1) devient pour tout  $\beta \in H_1(X_0(N), \mathbb{Z})$ 

$$\int_{\beta} \omega_f = \frac{c_E}{n_{1,E}} \Phi_{E,1}^{\mathcal{B}}(\beta) \int_{\beta_1} \omega_f + \frac{c_E}{n_{2,E}} \Phi_{E,2}^{\mathcal{B}}(\beta) \int_{\beta_2} \omega_f d\beta_{E,2}^{\mathcal{B}}(\beta) d\beta_{\mathcal{B}}^{\mathcal{B}}(\beta) d\beta_{\mathcal{B}}^{\mathcal{B}}(\beta)$$

Donc  $\frac{c_E}{n_{1E}} \Phi_{E,1}^{\mathcal{B}}, \frac{c_E}{n_{2E}} \Phi_{E,2}^{\mathcal{B}}$  est par définition une base de  $\mathcal{L}_f$ . On en déduit le lemme.

1

Remarquons que  $c_E \mathcal{L}_E$  est contenu dans  $\mathcal{L}_f$ , mais que  $\mathcal{L}_E$  ne l'est pas forcément (la constante de Manin d'une courbe de Weil forte est dans  $\mathbb{Z}$  et conjecturée égale à 1, mais pas celle d'une courbe elliptique quelconque).

## **3.5** Calcul de $L_E$

Le calcul de  $\mathcal{L}_E$  est fait à partir de bases  $\delta_{\pm}$  des espaces propres  $H^1(E,\mathbb{Z})^{\pm}$  pour la conjugaison complexe sur  $E(\mathbb{C})$ . Rappelons que si  $\psi$  est un caractère de Dirichlet de conducteur D premier à N,

$$\tau(\mathbf{\psi})L(E,\overline{\mathbf{\psi}},1) = \sum_{a \bmod D} \psi(a) \int_{\frac{a}{D}}^{\infty} 2i\pi f(z)dz$$

où  $\tau(\Psi) = \sum_{a \mod D} \Psi(a) e^{2i\pi a/D}$  est la somme de Gauss de  $\Psi$ . Choisissons deux caractères de Dirichlet  $\Psi_0$  et  $\Psi_1$  de conducteurs respectifs  $D_0$  et  $D_1$ , de signe  $\Psi_j(-1) = \varepsilon_j = (-1)^j$  et tels que  $L(E, \overline{\Psi_j}, 1)$  soit non nul pour j = 0, 1 (on les choisira de conducteur minimal pour cette propriété).

Les conditions

$$\tau(\Psi_j)L(E,\overline{\Psi}_j,1) = \sum_{a \bmod D_j} \Psi_j(a) \cdot \Phi_{E,\varepsilon_j}^{(\delta_+,\delta_-)} \left( (a/D_j,\infty) \right) \int_{\delta_{\varepsilon_j}} \omega_E$$

pour j = 0, 1 déterminent les symboles modulaires  $\Phi_{E,\pm}^{(\delta_+,\delta_-)}$  dans le Q-espace vectoriel  $V_f^{\pm}$  de dimension 1 de manière indépendante du choix des  $\psi_j$ : cela revient en effet à imposer les conditions

$$\begin{split} &\int_{\beta_0} \omega_f = \Phi_{E,+}^{(\delta_+,\delta_-)}(\beta_0) \int_{\delta_+} \omega_E, \\ &\int_{\beta_1} \omega_f = \Phi_{E,-}^{(\delta_+,\delta_-)}(\beta_1) \int_{\delta_-} \omega_E, \end{split}$$

avec  $\beta_j = \sum_{a \mod D_j} \psi_j(a) \left( \left( \frac{a}{D_j}, \infty \right) \right)$ . Par exemple, pour  $\Psi_0$  trivial et  $\beta_0 = (0, \infty)$ , la formule devient

$$\frac{L(E,1)}{\Omega_E^+} = \Phi_{E,+}^{(\delta_+,\delta_-)}\big((0,\infty)\big)$$

Le réseau  $\mathcal{L}_E$  de  $V_f$  associé à E est alors engendré par

$$\begin{cases} \Phi_{E,+}^{(\delta_+,\delta_-)} & \text{et } \Phi_{E,-}^{(\delta_+,\delta_-)} & \text{si } c_\infty = 2\\ \Phi_{E,+}^{(\delta_+,\delta_-)} - \Phi_{E,-}^{(\delta_+,\delta_-)} & \text{et } 2\Phi_{E,-}^{(\delta_+,\delta_-)} & \text{si } c_\infty = 1 \end{cases}$$

**Remarque 3.2.1.** Il est avantageux pour les calculs d'utiliser des caractères de Dirichlet de conducteur le plus petit possible. Il parait naturel d'utiliser un caractère quadratique mais ce n'est pas toujours possible ni optimal. Par exemple, soit la courbe E = 1225e1 de conducteur  $N = 1225 = 35^2$ . Le signe de l'équation fonctionnelle de E est 1. Montrons en utilisant Pari/GP que le signe de l'équation fonctionnelle des twists de E par un caractère quadratique impair  $\psi$  est -1, ce qui impliquera que  $L(E^{(\psi)}, 1) = 0$  pour tout D négatif. Pour D discriminant fondamental, on note  $E^{(D)}$  le twist de E par le caractère quadratique (D/.), w(E) le signe de l'équation fonctionnelle de E. On a la formule bien connue  $w(E^{(D)}) = \psi(-N)w(E)$  pour D premier à N, donc ici  $w(E^{(D)}) = \psi(-1)w(E) = \text{signe}(D)w(E)$ pour (D, 35) = 1.

```
? E = ellinit("1225e1");
? ellrootno(E)
%2 = 1
? E7 = ellinit(elltwist(E,-7)); ellidentify(E7)[1][1]
%3 = "1225g1"
? ellrootno(E7)
%4 = -1
? E5 = ellinit(elltwist(E,5)); ellidentify(E5)[1][1]
%5 = "1225f1"
```

? ellrootno(E5) %6 = 1 ? E35 = ellinit(elltwist(E,-35)); ellidentify(E35)[1][1] %7 = "1225h1" ? ellrootno(E35) %8 = -1

Ainsi, les twists de *E* par -7, 5, -35 sont encore de conducteur un carré.

— Si D = -7m avec m premier à 35 et positif,

$$w(E^{(D)}) = w(E^{(-7)}) = \text{signe}(m)w(E^{(-7)}) = w(E^{(-7)}) = -1.$$

— Si D = 5m avec m premier à 35 et négatif,

$$w(E^{(D)}) = w(E^{(5)}) = \operatorname{signe}(m)w(E^{(5)}) = -w(E^{(5)}) = -1.$$

— Si D = 35m avec m premier à 35 et positif,

$$w(E^{(D)}) = w(E^{(-35)}) = \operatorname{signe}(m)w(E^{(-35)}) = w(E^{(-35)}) = -1$$

Autrement dit,  $L(E, \psi, 1)$  est nul pour tous les caractères quadratiques impairs. On utilise alors pour le calcul de  $\Phi_{E,-}^{(\delta_+,\delta_-)}$  un caractère de Dirichlet impair de conducteur 9 et d'ordre 6.

# 4 Conséquences

## 4.1 Critère de calcul de la courbe de Weil forte et de sa constante de Manin

**Proposition 4.1.** *1.* La courbe E est une courbe de Weil forte si et seulement si les sous- $\mathbb{Z}$ -modules  $\mathcal{L}_f$  et  $\mathcal{L}_E$  de  $V_f \subset W$  sont homothétiques.

2. Si  $\mathcal{L}_E = \mathcal{L}_f$ , la courbe E est la courbe de Weil forte et la constante de Manin est égale à 1.

Démonstration. La courbe de Weil forte d'une classe d'isogénie sur  $\mathbb{Q}$  de courbes elliptiques est la courbe elliptique telle que  $\pi_* : H_1(X_0(N), \mathbb{Z}) \to H_1(E, \mathbb{Z})$  est surjective. Avec les notations précédentes, cela est le cas si et seulement  $n_{1,E} = n_{2,E} = 1$ . Les deux sous- $\mathbb{Z}$ -modules  $\mathcal{L}_E$  et  $\mathcal{L}_f$  de  $V_f$  sont alors homothétiques. Réciproquement, notons  $E_1$  la courbe de Weil forte (dont on sait qu'elle existe et vérifie que  $\mathcal{L}_{E_1}$  est homothétique à  $\mathcal{L}_f$ ) et  $\alpha$  une isogénie de E sur  $E_1$  de noyau cyclique. Les diviseurs élémentaires de  $\mathcal{L}_{E_1}$  dans  $\mathcal{L}_E$  sont alors deg $(\alpha)$  et 1. Si l'on suppose ces deux réseaux homothétiques,  $\alpha$  est un isomorphisme. Cela démontre la première partie.

Supposons maintenant que  $\mathcal{L}_E = \mathcal{L}_f$ . On a alors  $n_{1,E} = n_{2,E} = c_E$ . Mais il n'y a qu'une seule courbe de Weil forte à isomorphisme près. Donc, on a nécessairement  $n_{1,E} = n_{2,E} = c_E = 1$ .

### 4.2 Graphe orienté des isogénies admissibles

Prenons une classe d'isogénie de courbes elliptiques sur  $\mathbb{Q}$ . Le graphe des isogénies de degré premier peut être orienté de la manière suivante. Si  $\pi: E \to E'$  est une isogénie de degré premier et  $\pi'$  l'isogénie duale, on a  $\pi^* \omega_{E'} = \pm \omega_E$  ou  $\pi'^* \omega_E = \pm \omega_{E'}$ . L'arc entre E et E' est alors orienté comme  $E \to E'$  si et seulement si  $\pi^* \omega_{E'} = \pm \omega_E$  (appelé *admissible isogeny* dans [5], 6.11). Le calcul de ce graphe peut se faire par un calcul des modèles minimaux des courbes elliptiques de la classe d'isogénie et des réseaux des périodes complexes associés.

#### 4.3 Degré modulaire et constante de Manin

Soit  $E_1$  une courbe de Weil forte et E une courbe elliptique sur  $\mathbb{Q}$  dans sa classe d'isogénie. Une paramétrisation modulaire minimale  $X_0(N) \to E$  est obtenue comme composé  $X_0(N) \to E_1 \to E$  où  $E_1 \to E$  est de degré minimal. Le degré modulaire de E est égal au produit du degré modulaire de  $E_1$  par le degré de cette isogénie. D'autre part, le degré modulaire de la courbe de Weil forte  $E_1$  se calcule par la formule <sup>2</sup>

$$4\pi^2 ||f||^2 = \deg(\pi_1) \operatorname{Aire}(E_1) = \frac{c_{\infty}}{2} \deg(\pi_1) \Omega_{E_1}^+ \Omega_{E_1}^-$$
(2)

une fois qu'on a vérifié que la constante de Manin de  $E_1$  est bien 1. On obtient l'algorithme suivant.

#### Algorithm 1 Degré modulaire et constante de Manin

Entrée: Une courbe elliptique E.

**Sortie:** Le degré modulaire deg(E) et la constante de Manin  $c_E$ .

- 1: On calcule la courbe de Weil forte  $E_1$  dans la classe d'isogénie de E et on vérifie en même temps que  $c_{E_1} = 1$ . On calcule son degré modulaire  $d_1$  (par exemple par ellmoddegree dans Pari/GP).
- On calcule le graphe orienté des isogénies de degré premier de la classe d'isogénie. Si *a* est un arc, on note deg(*a*) le degré (premier) de l'isogénie.
- 3: On cherche le chemin le plus court de  $E_1$  vers E dans le graphe non orienté associé.
- 4:  $d \leftarrow d_1$ ;  $c \leftarrow 1$ ;

5: **pour** *a* arc du chemin **faire** 

6:  $d \leftarrow d \times \deg(a)$ 

- 7: si *a* est orienté négativement alors
- 8:  $c \leftarrow c \times \deg(a)$
- 9: retourner d et c.

Le graphe orienté calculé a une source (courbe optimale de Stevens, conjecturalement courbe de Weil forte relativement à  $X_1(N)$ , [10]). Si la courbe de Weil forte est la source du graphe orienté que l'on a construit, la constante de Manin pour une courbe elliptique quelconque isogène est toujours 1.

Prenons le cas où N = 11. La courbe de Weil forte est "11a1". Le graphe orienté des isogénies de degré premier est

$$11a3 \xrightarrow{5} 11a1 \xrightarrow{5} 11a2$$

La courbe optimale au sens de Stevens est "11a3". On a

? ellmoddegree(ellinit("11a1"))[1] %1 = 1

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
11a1	1	1	1,1	1,1	$\begin{pmatrix} 0 & 5 & 0 \end{pmatrix}$
11a2	5	1	5,1	5,1	0 0 0
11a3	5	5	1,1/5	5,1	$(5 \ 0 \ 0)$

 $11a3 \xrightarrow{5} 11a1 \xrightarrow{5} 11a2$ 

<sup>2.</sup> Si l'on désire rester dans le cadre algébrique, ce degré peut aussi être calculé à partir de la matrice de Gram sur une base de  $\mathcal{L}_f$  du produit de Petersson algébrique (ou produit d'intersection) défini sur l'espace  $\operatorname{Hom}_{\Gamma_0(N)}(\Delta_0, \mathbb{Q})$  (voir article à venir).

# **A** Programmes

Ces programmes sont écrits en PARI/GP [8].

```
/* plus court chemin entre x et y sans tenir compte de l'orientation */
dj(A, x, y) =
\{ my(v, w, n = #A); \}
  v = vector(n, i, n); v[x] = 0;
  w = vector(n);
  for (l=1, n-1, for (z=1, n,
    if (v[z] != 1-1, next);
    for (t=1, n, if (A[z,t] && v[t]>1, v[t]=1; w[t]=z))));
  /* Dijkstra: v[t] = d(x,t), w[t] = dernier point sur le chemin */
 my (m, res);
  m = v[y]+1; if (m > n, return([])); /* non connectés */
  res = vector (m);
  for (i=1, m, res[m+1-i] = y; y = w[y]);
  return(res);
}
/* SNF d'une matrice à entrées rationnelles */
Qsnf(M) = my(C = content(M)); C*matsnf(M/C);
/* matrice A du graphe d'isogénie de e, indices des réseaux associés dans L_f */
graphisogeny(e) =
{ my([Isoq, isomat] = ellisomat(e, 1));
 Isoq = [ ellminimalmodel(ellinit(e)) | e <- Isoq ];</pre>
 my([M, xpm] = msfromell(Isog));
 my(Lf, vL, Lindice, A, n);
 vL = [x[3] | x<-xpm ]; /* vecteur des réseaux L[i] */</pre>
 Lf = mslattice(M, vL[1]); /* réseau associé à la courbe de Weil dans Isoq*/
  Lindice = [ Qsnf(Lf^(-1)*L) | L<-vL ]; /* compare L[i] avec Lf */
  Isog = [ ellidentify(e)[1][1] | e<-Isog ];</pre>
  n = #Isog; A = matrix(n, n);
  for (i=1, n-1, for (j=i+1, n,
    if (!isprime(isomat[i,j]), next);
    my(C = Qsnf(vL[i]^(-1) * vL[j]), D = C[1]*C[2]);
    if (denominator(C) == 1, A[i,j] = D
                          , A[j,i] = 1/D));
  return([A, Isog, Lindice]);
};
ellmanin(e) =
{ my(i, i1, pc, c = 1, d, n);
 my([A, vE, Lindice] = graphisogeny(e)); /* matrice du graphe avec poids */
 A = A - mattranspose(A);
  /* il: numéro de la courbe de Weil forte el dans la classe d'isogénie
  * (vérifie aussi que la constante de Manin de courbe Weil forte est 1) */
  n = \#vE;
  [i1] = [ i | i<-[1..n], Lindice[i] == [1,1] ];
  e1 = ellinit(vecextract(vE, i1)[1]);
  ide = ellidentify(e)[1][1]; /* label de Cremona de la courbe */
```

```
[i] = [ i | i<-[1..n], vE[i] == ide ]; /* numero de la courbe */
pc = dj(A,i1,i); /* chemin le plus court entre i1 et i */
/* calcule le degré d entre e et el et le multiplie par ellmoddeg(e1) */
/* calcule la constante de Manin c de e */
[d] = ellmoddegree(e1);
for (j=1, #pc-1,
    my (t = A[ pc[j], pc[j+1] ], T = abs(t));
    d *= T; if (t < 0, c *= T));
return([d, c, Lindice[i]]);
}</pre>
```

#### B **Quelques exemples**

Nous avons fait une sélection de quelques exemples. Ainsi, nous donnons des exemples de courbes elliptiques ayant beaucoup de courbes isogènes et pour chaque valeur possible de degré d'isogénie (2,3,5,7,13,1,17,19,37,43,67,163, voir [7]), La construction des graphes a été inspirée des programmes de F. Brunault ([1]). Nous renvoyons à [12], §4, pour une analyse de familles de courbes où la courbe optimale pour  $X_0(N)$  n'est pas la source de l'arbre.

Le dernier exemple en niveau 130050 est un cas laissé ouvert par Cremona [4]. Il faut environ 26h de calcul pour confirmer que la courbe optimale est bien 130050em1. Comme l'indique Cremona, une classe d'isogénie fixée dans l'intervalle couvert par ses tables (conducteur inférieur à 400000) peut être raisonablement certifiée en quelques jours par le calcul complet de l'espace des symboles modulaires comme nous l'avons fait ci-dessus. Quand le niveau N augmente, 100% du temps de calcul dans les programmes de l'annexe A est utilisé par la commande msfromell, qui calcule l'espace des symboles modulaires de poids 2 et niveau N puis le symbole normalisé attaché à la classe d'isogénie considéré. La complexité asymptotique de cette implantation est  $\tilde{O}(N^{\log_2 7})$ .

				deg	$c_E$	$[L_f:$	$\mathcal{L}_E$ ]	$[H_1(E,\mathbb{Z}):\pi^*H$	$I_1(X_0)$	$\mathbb{N}),\mathbb{Z}$	)]		Mat	rice				
		11:	a1	1	1	1	,1	1,1	-			/	) 5	5 (	)			
		11:	a2	5	1	5	,1	5,1					) (	) (				
		11:	a3	5	5	1,	1/5	5,1				(4	5 (	) (	)/			
								5 5										
						1.	$a_3 -$	$\rightarrow$ 11a1 $\rightarrow$	$\rightarrow 11a^2$	2								
		0	leg	$c_E$	$[L_f]$	$: \mathcal{L}_E]$	$[H_1]$	$(E,\mathbb{Z})$ : $\pi^*H_1(X_0($	$(N),\mathbb{Z})$	]	,		Mat	rice				
	14a	1	1	1		1,1		1,1			$\left( 0 \right)$	0	3	2	0	0		
	14a	4	3	3	1	,1/3		3,1			3	0	0	0	2	0		
	14a	3	3	1		3,1		3,1			0	0	0	0	0	2		
	14a	2	2	1		2,1		2,1			0	0	0	0	0	3		
	14a	6	6	3	2	,1/3		6,1			0	0	0	3	0	0		
	14a	5	6	I		6,1		6,1			(0	0	0	0	0	0/		
					1.	4aA =	3	$4a1 \xrightarrow{3} 14a3$										
					1.	+4+ -	2	$\sim 2$	> 2									
							$\searrow$			X								
							1	$4a6 \xrightarrow{3} 14a2$	3	→ 14a	a5							
		deg	CE	· []	.f: [	<sub>F</sub> ] [F	$H_1(E_1)$	$\overline{\mathbb{Z}}): \pi^* H_1(X_0(N)).$	Z)]				Mat	rice				
15	5a1	1	1		1.1		-1(-)	1.1	_/]	/0	0	0	0	2	2	0	0\	
15	5a3	2	2		1,1/2			2,1		2	0	2	0	0	0	0	0	
15	5a7	4	2		2,1/2			4,1		0	0	0	0	0	0	0	0	
15	5a8	4	4		1,1/4			4,1		0	2	0	0	0	0	0	0	
15	5a4	2	1		2,1			2,1		0	0	0	0	0	0	0	0	
15	5a2	2	1		2,1			2,1		0	0	0	0	0	0	2	2	
15	ia6	4	1		4,1			4,1		0	0	0	0	0	0	0	0	
15	5a5	4	1		4,1			4,1		0	0	0	0	0	0	0	0/	
					-	2		2 2		. 2			-					
				150	a8 —	$\xrightarrow{2}$ 15	5a3 –	$\xrightarrow{2}$ 15al $\xrightarrow{2}$	$\rightarrow 15a^2$	2	$\rightarrow$	15 <i>a</i>	6					
									~1		2							
								15a7	15 <i>a</i> 4	ŀ	ĸ	15 <i>a</i>	5					
	Ē		1			[ <i>I</i>	- 1 ]	$[II (E \mathbb{Z}), \pi^* II]$	$(\mathbf{V} (\mathbf{N}))$	<u>(</u> 77)1			Mat					
	-	17.1		eg	$\frac{c_E}{1}$	$L_f$ : $I$	-E]	$\frac{[\Pi_1(E,\mathbb{Z}):\pi^*H_1(\mathbb{Z})]}{1}$	$\Lambda_0(N)$	),⊿)]		/0	iviat		0)			
		17a1		2	$\frac{1}{2}$	1,1 1 1 //	<b>,</b>	1,1				$\begin{bmatrix} 0 \\ 2 \end{bmatrix}$	0	0	2)			
		17a4		4	$\begin{array}{c} 2 \\ 1 \end{array}$	1,1/.	4	2,1 1					2	0	<u>_</u>			
		1793		4	$\frac{1}{2}$	21/2	2	4,1 4 1					$\stackrel{\sim}{0}$	0	0			
		1 / u.J			-		-	1,1				10	0	0	0,			



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice				:
20a1	1	1	1,1	1,1	1	0	3	0	0)
20a3	3	1	3,1	3,1		0	0	0	0
20a2	2	2	1,1/2	2,1		2	0	0	3
20a4	6	2	3,1/2	6,1		0	2	0	0/



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$		Matrice					
21a1	1	1	1,1	1,1	1	0	2	0	2	0	0)
21a3	2	1	2,1	2,1		0	0	0	0	0	0
21a4	2	2	1,1/2	2,1		2	0	0	0	0	0
21a2	2	1	2,1	2,1		0	0	0	0	2	2
21a6	4	1	4,1	4,1		0	0	0	0	0	0
21a5	4	1	4,1	4,1		0	0	0	0	0	0/

$$21a4 \xrightarrow{2} 21a1 \xrightarrow{2} 21a2 \xrightarrow{2} 21a6$$

$$21a3 \xrightarrow{2} 21a3 \xrightarrow{2} 21a5$$

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
26b1	2	1	1,1	1,1	$\begin{pmatrix} 0 & 7 \end{pmatrix}$
26b2	14	1	7,1	7,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$

 $26b1 \xrightarrow{7} 26b2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$		:				
27a1	1	1	1,1	1,1	1	0	0	0	3	
27a3	3	3	1,1/3	3,1		3	0	3	0	
27a4	9	3	3,1/3	9,1		0	0	0	0	
27a2	3	1	3,1	3,1		0	0	0	0/	

$$27a3 \xrightarrow{3} 27a1 \xrightarrow{3} 27a2$$

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice									
30a1	2	1	1,1	1,1	1	0	2	0	0	3	0	0	0)	١
30a2	4	1	2,1	2,1		0	0	2	2	0	3	0	0	
30a5	8	1	4,1	4,1		0	0	0	0	0	0	3	0	
30a4	8	1	4,1	4,1		0	0	0	0	0	0	0	3	
30a3	6	1	3,1	3,1		0	0	0	0	0	2	0	0	
30a6	12	1	6,1	6,1		0	0	0	0	0	0	2	2	
30a8	24	1	12,1	12,1		0	0	0	0	0	0	0	0	
30a7	24	1	12,1	12,1		0	0	0	0	0	0	0	0	/



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$		Matrice				
32a1	1	1	1,1	1,1	1	0	0	0	0)	
32a2	2	2	1,1/2	2,1		2	0	2	2	
32a4	4	2	2,1/2	4,1		0	0	0	0	
32a3	4	2	2,1/2	4,1		0	0	0	0/	



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
37b1	2	1	1,1	1,1	$\begin{pmatrix} 0 & 0 & 3 \end{pmatrix}$
37b3	6	3	1,1/3	3,1	$[3 \ 0 \ 0]$
37b2	6	1	3,1	3,1	

 $37b3 \xrightarrow{3} 37b1 \xrightarrow{3} 37b2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
38b1	2	1	1,1	1,1	$\begin{pmatrix} 0 & 5 \end{pmatrix}$
38b2	10	1	5,1	5,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$

 $\frac{38b1}{38b2} \xrightarrow{5} 38b2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$		;		
49a1	1	1	1,1	1,1	/0	2	7	0)
49a2	2	1	2,1	2,1	0	0	0	7
49a3	7	1	7,1	7,1	0	0	0	2
49a4	14	1	14,1	14,1	$\setminus 0$	0	0	0/



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice							
75b1	6	1	1,1	1,1	/0	2	0	0	0	0	0	0
75b2	12	1	2,1	2,1	0	0	2	2	0	0	0	0
75b4	24	1	4,1	4,1	0	0	0	0	0	0	0	0
75b3	24	1	4,1	4,1	0	0	0	0	2	2	0	0
75b6	48	1	8,1	8,1	0	0	0	0	0	0	0	0
75b5	48	1	8,1	8,1	0	0	0	0	0	0	2	2
75b8	96	1	16,1	16,1	0	0	0	0	0	0	0	0
75b7	96	1	16,1	16,1	0/	0	0	0	0	0	0	0/

$$75b1 \xrightarrow{2} 75b2 \xrightarrow{2} 75b3 \xrightarrow{2} 75b5 \xrightarrow{2} 75b8$$

$$2 \xrightarrow{2} 75b4 \xrightarrow{2} 75b6 \xrightarrow{2} 75b7$$

75b675b7

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
121a1	6	1	1,1	1,1	$\begin{pmatrix} 0 & 11 \end{pmatrix}$
121a2	66	1	11,1	11,1	

 $121a1 \xrightarrow{11} 121a2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$				Mat	rice	:			
195a1	24	1	1,1	1,1	0	2	0	0	0	0	0	0)	1
195a2	48	1	2,1	2,1	0	0	2	2	0	0	0	0	
195a4	96	1	4,1	4,1	0	0	0	0	0	0	0	0	
195a3	96	1	4,1	4,1	0	0	0	0	2	2	0	0	
195a6	192	1	8,1	8,1	0	0	0	0	0	0	0	0	
195a5	192	1	8,1	8,1	0	0	0	0	0	0	2	2	
195a8	384	1	16,1	16,1	0	0	0	0	0	0	0	0	
195a7	384	1	16,1	16,1	0	0	0	0	0	0	0	0,	/

 $195a1 \xrightarrow{2} 195a2 \xrightarrow{2} 195a3 \xrightarrow{2} 195a5 \xrightarrow{2} 195a8$ 195*a*4

195*a*6 . 195a7

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Mat	rice
208d1	48	1	1,1	1,1	(0	7)
208d2	336	1	7,1	7,1	0	0)

# $\frac{208d1}{\longrightarrow} \frac{7}{208d2}$

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
294a1	84	1	1,1	1,1	$\begin{pmatrix} 0 & 7 \end{pmatrix}$
294a2	588	1	7,1	7,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice	_
361a1	20	1	1,1	1,1	$\begin{pmatrix} 0 & 19 \end{pmatrix}$	
361a2	380	1	19,1	19,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$	

 $294a1 \xrightarrow{7} 294a2$ 

 $361a1 \xrightarrow{19} 361a2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
464e1	60	1	1,1	1,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$
464e2	120	2	1,1/2	2,1	$\begin{pmatrix} 2 & 0 \end{pmatrix}$

 $464e2 \xrightarrow{2} \mathbf{464}e1$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
507a1	312	1	1,1	1,1	$\begin{pmatrix} 0 & 7 \end{pmatrix}$
507a2	2184	1	7,1	7,1	

 $507a1 \xrightarrow{7} 507a2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice								
585f1	192	1	1,1	1,1		(0	2	0	0	0	0	0	0)
585f2	384	1	2,1	2,1		0	0	2	0	0	0	0	2
585f3	768	1	4,1	4,1		0	0	0	2	0	0	2	0
585f5	1536	1	8,1	8,1		0	0	0	0	2	2	0	0
585f7	3072	1	16,1	16,1		0	0	0	0	0	0	0	0
585f8	3072	1	16,1	16,1		0	0	0	0	0	0	0	0
585f6	1536	1	8,1	8,1		0	0	0	0	0	0	0	0
585f4	768	1	4,1	4,1		0	0	0	0	0	0	0	0/

 $585f1 \xrightarrow{2} 585f2 \xrightarrow{2} 585f3 \xrightarrow{2} 585f5 \xrightarrow{2} 585f7$   $2 \xrightarrow{2} 585f4 \xrightarrow{2} 585f6 \xrightarrow{2} 585f8$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
681b1	375	1	1,1	1,1	$\begin{pmatrix} 0 & 2 & 2 & 0 \end{pmatrix}$
681b3	750	1	2,1	2,1	0 0 0 0
681b4	750	1	2,1	2,1	0 0 0 0
681b2	750	2	1,1/2	2,1	$(2 \ 0 \ 0 \ 0)$

$$681b2 \xrightarrow{2} 681b1 \xrightarrow{2} 681b3$$

$$\xrightarrow{2} 681b4$$

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
692a1	123	1	1,1	1,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$
692a2	246	2	1,1/2	2,1	$\begin{pmatrix} 2 & 0 \end{pmatrix}$

 $692a2 \xrightarrow{2} 692a1$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
848d1	84	1	1,1	1,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$
848d2	168	2	1,1/2	2,1	$\begin{pmatrix} 2 & 0 \end{pmatrix}$

848 <i>d</i> 2	$\xrightarrow{2}$	848 <i>d</i> 1
----------------	-------------------	----------------

														_
	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$\left[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})\right]$					Mat	rice				
960e1	384	1	1,1	1,1	1	0	2	0	0	3	0	0	0)	
960e2	768	1	2,1	2,1		0	0	2	2	0	3	0	0	
960e5	1536	1	4,1	4,1		0	0	0	0	0	0	3	0	
960e4	1536	1	4,1	4,1		0	0	0	0	0	0	0	3	
960e3	1152	1	3,1	3,1		0	0	0	0	0	2	0	0	
960e6	2304	1	6,1	6,1		0	0	0	0	0	0	2	2	
960e8	4608	1	12,1	12,1		0	0	0	0	0	0	0	0	
960e7	4608	1	12,1	12,1	$  \langle$	0	0	0	0	0	0	0	0/	



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice			
990h3	1728	1	1,1	1,1	/0	3	2	0/
990h1	5184	1	3,1	3,1	0	0	0	2
990h4	3456	1	2,1	2,1	0	0	0	3
990h2	10368	1	6,1	6,1	0	0	0	0/



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
1089e1	120	1	1,1	1,1	$\begin{pmatrix} 0 & 11 \end{pmatrix}$
1089e2	1320	1	11,1	11,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$

 $\frac{1089e1}{1000} \xrightarrow{11} 1089e2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
1225e1	1680	1	1,1	1,1	$\begin{pmatrix} 0 & 37 \end{pmatrix}$
1225e2	62160	1	37,1	37,1	

 $\begin{array}{c} 1225e1 \xrightarrow{37} 1225e2 \end{array}$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
1849a1	264	1	1,1	1,1	$\begin{pmatrix} 0 & 43 \end{pmatrix}$
1849a2	11352	1	43,1	43,1	

$1849a1 \xrightarrow{43} 18$
------------------------------

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
1913b1	309	1	1,1	1,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$
1913b2	618	2	1,1/2	2,1	$\begin{pmatrix} 2 & 0 \end{pmatrix}$

# $1913b2 \xrightarrow{2} 1913b1$

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
1936k1	384	1	1,1	1,1	$\begin{pmatrix} 0 & 11 \end{pmatrix}$
1936k2	4224	1	11,1	11,1	

 $1936k1 \xrightarrow{11} 1936k2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
2089b1	219	1	1,1	1,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$
2089b2	438	2	1,1/2	2,1	$\begin{pmatrix} 2 & 0 \end{pmatrix}$

 $2089b2 \xrightarrow{2} 2089b1$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$				Mat	rice	;			
2145e1	19968	1	1,1	1,1	0	2	0	0	0	0	0	0)	
2145e2	39936	1	2,1	2,1	0	0	2	2	0	0	0	0	
2145e4	79872	1	4,1	4,1	0	0	0	0	0	0	0	0	
2145e3	79872	1	4,1	4,1	0	0	0	0	2	2	0	0	
2145e6	159744	1	8,1	8,1	0	0	0	0	0	0	0	0	
2145e5	159744	1	8,1	8,1	0	0	0	0	0	0	2	2	
2145e8	319488	1	16,1	16,1	0	0	0	0	0	0	0	0	
2145e7	319488	1	16,1	16,1	0	0	0	0	0	0	0	_0/	



	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
2273a1	392	1	1,1	1,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$
2273a2	784	2	1,1/2	2,1	$\begin{pmatrix} 2 & 0 \end{pmatrix}$

 $2273a2 \xrightarrow{2} 2273a1$ 

	deg	$c_E$	$\begin{bmatrix} L_f : \mathcal{L}_E \end{bmatrix} \begin{bmatrix} H_1(E,\mathbb{Z}) : \pi^* H_1(X_0(N),\mathbb{Z}) \end{bmatrix}$					Mat	rice	;		
2310g1	13824	1	1,1	1,1	/0	2	0	0	3	0	0	0)
2310g2	27648	1	2,1	2,1	0	0	2	2	0	3	0	0
2310g5	55296	1	4,1	4,1	0	0	0	0	0	0	3	0
2310g4	55296	1	4,1	4,1	0	0	0	0	0	0	0	3
2310g3	41472	1	3,1	3,1	0	0	0	0	0	2	0	0
2310g6	82944	1	6,1	6,1	0	0	0	0	0	0	2	2
2310g8	165888	1	12,1	12,1	0	0	0	0	0	0	0	0
2310g7	165888	1	12,1	12,1	0/	0	0	0	0	0	0	0/



 $2352j1 \xrightarrow{13} 2352j2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
3249a1	640	1	1,1	1,1	$\begin{pmatrix} 0 & 19 \end{pmatrix}$
3249a2	12160	1	19,1	19,1	

 $3249a1 \xrightarrow{19} 3249a2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
4489a1	1292	1	1,1	1,1	$\begin{pmatrix} 0 & 67 \end{pmatrix}$
4489a2	86564	1	67,1	67,1	

 $4489a1 \xrightarrow{67} 4489a2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice	
14450p1	12240	1	1,1	1,1	$\begin{pmatrix} 0 & 17 \end{pmatrix}$	
14450p2	208080	1	17,1	17,1		

 $14450p1 \xrightarrow{17} 14450p2$ 

	deg	$c_E$	$[L_f:\mathcal{L}_E]$	$[H_1(E,\mathbb{Z}):\pi^*H_1(X_0(N),\mathbb{Z})]$	Matrice
16641e1	8448	1	1,1	1,1	$\begin{pmatrix} 0 & 43 \end{pmatrix}$
16641e2	363264	1	43,1	43,1	$\begin{pmatrix} 0 & 0 \end{pmatrix}$

 $\frac{16641e1}{16641e2} \xrightarrow{43} 16641e2$ 

	deg $c_E$		deg $c_E \mid [L_f : \mathcal{L}_E] \mid [H_1(E,\mathbb{Z}) : \pi^* H_1(X_0(N),\mathbb{Z})]$			
26569a1	59368	1	1,1	1,1	$(0 \ 163)$	
26569a2	9676984	1	163,1	163,1		

 $26569a1 \xrightarrow{163} 26569a2$ 

	deg	$c_E$	$\begin{bmatrix} L_f : \mathcal{L}_E \end{bmatrix} \begin{bmatrix} H_1(E,\mathbb{Z}) : \pi^* H_1(X_0(N),\mathbb{Z}) \end{bmatrix}$					Mat	rice			
130050em1	1769472	1	1,1	1,1	/0	2	0	0	3	0	0	0)
130050em2	3538944	1	2,1	2,1	0	0	2	2	0	3	0	0
130050em4	7077888	1	4,1	4,1	0	0	0	0	0	0	3	0
130050em5	7077888	1	4,1	4,1	0	0	0	0	0	0	0	3
130050em3	5308416	1	3,1	3,1	0	0	0	0	0	2	0	0
130050em6	10616832	1	6,1	6,1	0	0	0	0	0	0	2	2
130050em7	21233664	1	12,1	12,1	0	0	0	0	0	0	0	0
130050em8	21233664	1	12,1	12,1	0	0	0	0	0	0	0	0/



# Références

- François Brunault, Graphes d'isogénies entre courbes elliptiques, http://perso.ens-lyon.fr/francois. brunault/parigp
- [2] John Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve*, Mathematics of computation volume 64, number 211 (1995), p. 1235-1250.
- [3] John Cremona, Appendice à l'article de Amod Agashe, Kenneth Ribet et William A. Stein, The Manin Constant, Pure and Applied Mathematics Quarterly Volume 2, Number 2 (Special Issue : In honor of John H. Coates, Part 2 of 2) 617-636, 2006.
- [4] John Cremona, *Elliptic curve data*, Optimality and the Manin constant, 2017, http://johncremona.github. io/ecdata/#optimality.
- [5] Ju. I. Manin, Parbolic points and zeta-functions of modular curves, Math. USSR Izvestija, vol 6 (1972), No 1, 19-64.
- [6] Barry Mazur, Courbes elliptiques et symboles modulaires. Séminaire Bourbaki 14 (1971-1972), p.277-294. http://eudml.org/doc/109817
- [7] Barry Mazur, *Rational Isogenies of Prime Degree*, Inventiones mathematicae, June 1978, Volume 44, Issue 2, pp 129-162
- [8] The PARI Group, PARI/GP version 2.10.0, Univ. Bordeaux, 2018, http://pari.math.u-bordeaux.fr
- [9] Robert Pollack, Glenn Stevens, Overconvergent modular symbols and p-adic L-functions, Annales scientifiques de l'ENS 44, fascicule 1 (2011), 1-42.
- [10] Glenn Stevens, Stickelberger elements and modular parametrizations of elliptic curves, Invent. Math. 98 (1989), no. 1, 75-106
- [11] Goro Shimura, *Sur les intégrales attachées aux formes automorphes*, Journal of the Mathematical Society of Japan Vol. 11, No. 4, October, 1959
- [12] W. Stein and M. Watkins, A Data-base of Elliptic Curves- First Report, In Algorithmic Number Theory (Sydney, 2002), pp. 267-275, Lecture Notes in Comput. Sci. 2369. Berlin : Springer-Verlag, 2002.