GLASNIK MATEMATIČKI
Vol. 41(61)(2006), 31 – 49

# 2-RANG DU GROUPE DES CLASSES ET COURBES ELLIPTIQUES

Aïni Laoudi
Université Paris 6, France and Université des Sciences et de la Technologie Houari Boumediène, Algérie

Abstract. We study the relationship between the 2-rank of class groups of a family of cubic fields and the rank of a family of elliptic curves.

Résumé. Dans cet article, nous étudions la relation qui existe entre le 2-rang du groupe des classes d'une famille de corps cubiques et le rang d'une famille de courbes elliptiques.

## 1. Introduction

Soient $k$ un corps de nombres, $C(k)$ le groupe des classes d'idéaux de $k$, et $p$ un nombre premier. Le $p$-rang du groupe des classes d'idéaux de $k$, que l'on note $r_p$, est, par définition, la dimension de $C(k)/C(k)^p$ sur $\mathbb{F}_p$, qui est aussi la dimension de la $p$-torsion du sous-groupe du groupe des classes d'idéaux, noté $C_p(k)$. Depuis quelques années, plusieurs mathématiciens ont essayé de trouver des corps quadratiques avec un 3-rang assez élevé. Le problème correspondant dans le cas de degré 3, est de chercher des corps cubiques cycliques avec un 2-rang assez grand. Dans [21], L. C. Washington considère la famille de corps cubiques cycliques définis par les polynômes $P_a(x) = x^3 - (a+3)x^2 + ax + 1$, avec $a \in \mathbb{Z}$. Sous certaines conditions, le groupe des unités est explicitement déterminé. Il associe alors la famille de courbes elliptiques $C_a$ sur $\mathbb{Q}$ d'équation $y^2 = P_a(x)$. Le corps de définition des points d'ordre 2 de $C_a$ est le corps cubique défini par $P_a$. Il établit par une 2-descente une relation entre le 2-rang du groupe des classes des corps cubiques et le rang des courbes elliptiques. Par ailleurs, il choisit $a$ tel que les réductions de la courbe $C_a$ modulo les petits nombres premiers possèdent un grand nombre

2000 *Mathematics Subject Classification.* 14H52, 14G05, 11R29.
*Key words and phrases.* Elliptic curves, rank, class groups.

de points. Ces exemples donnent lieu à des courbes elliptiques de rang élevé, ce qui donne des corps cubiques avec un 2-rang assez grand. Les résultats de L. C. Washington ont été généralisés à d'autres corps cubiques par Kawachi et Nakano [10].

Dans cet article, nous étudierons le lien entre les courbes elliptiques $E_n$ données par l'équation: $y^2 = G_n(x)$ et le 2-rang du groupe des classes des corps cubiques $K_n$ engendrés par une racine $\rho$ du polynôme

$$G_n(x) = x^3 - n^2x^2 + (n^3 - 2n^2 + 3n - 3)x + 1.$$

Une construction modulaire explicite de ces corps cubiques a été donnée par Lecacheux dans [12] et [11]. L. C. Washington a étudié dans [20] l'arithmétique de ces corps cubiques.

Dans les paragraphes 2, 3 et 4, nous donnons quelques propriétés arithmétiques de ces corps cubiques et étudions les courbes elliptiques $E_n$ et les homomorphismes liés à la 2-descente.

Dans le paragraphe 5, on définit un sous-groupe $S_2'(\mathbb{Q})$ du 2-groupe de Selmer $S_2(\mathbb{Q})$, et un sous-groupe $H$ de $E_n(\mathbb{Q})$. Par une méthode classique (par exemple [2]), on montre une majoration du rang des courbes elliptiques $E_n$ par une fonction du nombre de facteurs premiers de $|n-1|$ et du 2-rang $r_2$ du groupe des classes de $K_n$.

Dans le paragraphe 6, on montre, sous certaines conditions, portant sur $n$, que les suites

$$1 \longrightarrow \langle [0,1] \rangle \longrightarrow S_2'(\mathbb{Q}) \xrightarrow{\nu} C_2(K) \longrightarrow 1,$$

$$1 \longrightarrow (E_n'(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q}) \xrightarrow{\mu} C_2(K) \longrightarrow Ш_2' \longrightarrow 1,$$

$$\nu : [\alpha] \mapsto \overline{I_\alpha},$$

$$\mu : [(x,y)] \mapsto \overline{I_x},\ (x-\rho) = I_x^2,$$

sont des suites exactes, où $Ш_2'$ est le conoyau de l'application $f_1 : H/2E_n(\mathbb{Q}) \to S_2'(\mathbb{Q})$ et $E_n'(\mathbb{Q}) = 2E_n(\mathbb{R}) \cap E_n(\mathbb{Q})$. On montre alors qu'il existe une relation entre le 2-rang de $H/2E_n(\mathbb{Q})$, c'est-à-dire la dimension de $H/2E_n(\mathbb{Q})$ en tant que $\mathbb{F}_2$-espace vectoriel, et le 2-rang du groupe des classes de $K_n$. Dans le dernier paragraphe, on explicite quelques exemples. Nous remercions A. Dujella [7] pour son aide dans les calculs sur les courbes $E_n$, en particulier pour l'exemple de courbe de rang 7, qui correspond à la courbe $E_{626}$. Pour trouver cet exemple, il sélectionne les courbes $E_n$ dont la réduction possèdent de nombreux points modulo un nombre premier.

## 2. Arithmétique des corps cubiques $K_n$

Soit $n$ un entier relatif différent de 1. Soit $K_n$ le corps cubique défini par le polynôme irréductible sur $\mathbb{Q}$

$$G_n(x) = x^3 - n^2x^2 + (n^3 - 2n^2 + 3n - 3)x + 1.$$

Le discriminant de $G_n(x)$ est égal à $(n-1)^2d^2$ où $d=(n^2+3)(n^2-3n+3)$. Notons $\rho_1$ la racine négative de $G_n(x)$. Alors $\rho_2 = \dfrac{n^2-n+1-n\rho_1}{-\rho_1+1}$ et $\rho_3 = \dfrac{n^2-n+1-\rho_1}{-\rho_1+n}$ sont les deux autres racines. Donc $K_n=\mathbb{Q}(\rho_i)$ est une extension cubique cyclique, on note alors $\sigma$ l'unique générateur de $Gal(K_n/\mathbb{Q})$ vérifiant $\rho_2=\sigma(\rho_1), \rho_3=\sigma^2(\rho_1)$.

Dans tout le reste de l'article, par commodité d'écriture on utilisera $K$ au lieu de $K_n$ et on travaillera sous l'hypothèse suivante: $n$ non nul, pair, différent de 2 et $d/9^\delta$ est sans facteurs carrés, où $\delta=0$ si $n\not\equiv 0 \bmod 3$ et $\delta=1$ sinon. Sous cette hypothèse, on montre dans [12, 20], que l'anneau des entiers $\mathbb{Z}_K$ de $K$ n'est pas monogène et $\{1,\rho_1,\rho_2\}$ est une base d'entiers de $K$; que l'indice de $\mathbb{Z}[\rho_i]$ dans $\mathbb{Z}_K$ est égale à $|n-1|$ et que le discriminant du corps est égal à $d^2$. L. C. Washington montre dans [20], que le groupe des unités de $K$ est engendré par les trois racines du polynôme $G_n(x)$. De plus, en reprenant les même arguments donnés dans la preuve du [19, lemme 4], on montre que toute unité totalement positive de $K$ est un carré dans $K$. Il en résulte alors que le nombre de classes et le nombre de classes strictes de $K$ sont égaux et d'autre part, d'après [22], que $r_2$ est toujours pair.

La proposition suivante donne la décomposition dans $\mathbb{Z}_K$ du nombre premier 2 et des nombres premiers qui divisent $n-1$.

PROPOSITION 2.1. *(1) Soit $p$ un nombre premier impair qui divise $n-1$. Alors $p$ est totalement décomposé dans $K/\mathbb{Q}$ et l'on a*

$$p\mathbb{Z}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,$$

*où on note $\mathfrak{p}_1=p\mathbb{Z}_K+(\rho+1)\mathbb{Z}_K$, $\mathfrak{p}_2=\mathfrak{p}_1{}^\sigma, \mathfrak{p}_3=\mathfrak{p}_1{}^{\sigma^2}$ et $\mathfrak{p}_2\mathfrak{p}_3=p\mathbb{Z}_K+(\rho-1)\mathbb{Z}_K$, où $\rho$ est une racine du polynôme $G_n(x)$.*

*(2) Le nombre premier 2 est inerte dans l'extension $K/\mathbb{Q}$.*

## 3. Famille de courbes elliptiques

Considérons les courbes elliptiques $E_n$ définies par l'équation $y^2=G_n(x)$. Les points d'ordre 2 de $E_n$ ne sont pas rationnels sur $\mathbb{Q}$ mais définis sur $K$. Le discriminant de $E_n$ est égal à $16(n-1)^2d^2$ et son invariant modulaire $j$ est égal à $\dfrac{16^2d^2}{(n-1)^2}$. La courbe elliptique $E_n$ a mauvaise réduction en les nombres premiers qui divisent $2(n-1)d$, cette réduction est additive en les nombres premiers qui se ramifient dans $K$ c'est-à-dire les nombres premiers qui divisent $d$ et en le nombre premier 2; elle est multiplicative en les nombres premiers qui divisent $(n-1)$, dans ce cas la réduction est déployée (resp. non déployée) si 2 est un carré (resp. n'est pas un carré) mod $p$.

Soit $\tilde{E}_n$ la réduction de $E_n$ mod $p$. Si la courbe a mauvaise réduction, on définit les sous-groupes de $E_n(\mathbb{Q}_p)$, $E_n^0(\mathbb{Q}_p) = \{P \in E_n(\mathbb{Q}_p) : \tilde{P}$ non singulier$\}$; $E_n^1(\mathbb{Q}_p) = \{P \in E_n^0(\mathbb{Q}_p) : \tilde{P} = \tilde{O}\}$ .

Quand $p|n-1$, la courbe $\tilde{E}_n$ a un point multiple de coordonnées $(1,0)$. On choisit de noter les racines $\rho_i$ de sorte que les points d'ordre 2 $(\rho_i, 0)$, $2 \leq i \leq 3$ se réduisent sur $(1,0)$ et le point d'ordre 2 $(\rho_1, 0)$ se réduit sur le point simple $(-1,0)$. On caractérise les éléments de $E_n^0(\mathbb{Q}_p)$, comme suit:

$$(x,y) \in E_n^0(\mathbb{Q}_p) \Leftrightarrow x \not\equiv 1 \bmod p.$$

## 4. Homomorphismes liés à la famille de courbes elliptiques $E_n$

Dans ce paragraphe, on étudie les homomorphismes liés à la 2-descente pour la famille de courbes elliptiques $E_n$. On utilisera la proposition suivante, cas particulier d'une proposition générale adaptée à notre étude.

Proposition 4.1. *Soit $k$ un corps de caractéristique différente de 2, $E$ une courbe elliptique définie sur $k$ donnée par l'équation $y^2 = f(x)$ avec $f$ un polynôme de degré 3 à coefficients dans $k$. Soit la $k$-algèbre $A_k = k[T]/(f(T))$, notons $A_k^*$ le groupe multiplicatif de $A_k$. Alors*

*(1) Si $E$ n'a pas de points d'ordre 2 sur $k$. On définit l'application $\lambda_k : E(k) \to A_k^*/A_k^{*2}$, par*

$$\lambda_k : (x,y) \mapsto (x-T) \mod A_k^{*2},\ O \mapsto 1.$$

*(2) Si $E$ a trois points d'ordre 2 sur $k$, $(\theta_i, 0), 1 \leq i \leq 3$, on définit l'application $\lambda_k : E(k) \to (k^*/k^{*2})^3$, par*

$$\lambda_k : (x,y) \mapsto (x-\theta_1, x-\theta_2, x-\theta_3) \mod (k^{*2})^3 si\ x \neq \theta_i,$$

$$(\theta_1, 0) \mapsto (f'(\theta_1), \theta_1-\theta_2, \theta_1-\theta_3) \mod (k^{*2})^3,\ O \mapsto 1,$$

*on définit de la même façon $(\theta_i, 0)$, $2 \leq i \leq 3$.*

*Dans les deux cas l'application $\lambda_k$ est un homomorphisme de groupes, de noyau égal à $2E(k)$.*

On utilise cette proposition dans les cas suivants:

(1) Si $k = \mathbb{Q}$ alors $A_{\mathbb{Q}} = K$ et on a l'homomorphisme $\lambda_{\mathbb{Q}} : E(\mathbb{Q}) \to K^*/K^{*2}$, défini par

$$(x,y) \mapsto (x-\rho_1) \mod K^{*2},\ O \mapsto 1.$$

(2) Si $p$ est une place finie de $\mathbb{Q}$, $\mathbb{Q}_p$ désignera le complété de $\mathbb{Q}$ en $p$. On désigne par $K_{\mathfrak{p}}$ le complété de $K$ pour tout idéal premier $\mathfrak{p}$ au dessus de $p$; et on identifie $K$ à un sous-corps de $K_{\mathfrak{p}}$.

En considérant $k = \mathbb{Q}_p$, la $\mathbb{Q}_p$-algèbre $A_{\mathbb{Q}_p}$ sera notée $K_p$ et on obtient les résultats suivants:

(a) Si l'idéal $p\mathbb{Z}_K$ ne se décompose pas dans $K/\mathbb{Q}$, alors $K_p$ est une extension de degré 3 de $\mathbb{Q}_p$. D'après la proposition 4.1, on a l'homomorphisme

$$\lambda_p : E_n(\mathbb{Q}_p) \to K_p^*/K_p^{*2},$$
$$(x,y) \mapsto (x-\rho_1) \mod K_p^{*2},$$
$$O \mapsto 1.$$

où $\rho_1$ est une racine de $K$.

(b) Si l'idéal $p\mathbb{Z}_K$ se décompose dans $K/\mathbb{Q}$, alors

$$K_p \backsimeq \mathbb{Q}_p[T]/(T-\rho_1) \times \mathbb{Q}_p[T]/(T-\rho_2) \times \mathbb{Q}_p[T]/(T-\rho_3).$$

Comme $\mathbb{Q}_p[T]/(T-\rho_i) \backsimeq K_{\mathfrak{p}_i} \backsimeq \mathbb{Q}_p$, pour $1 \leq i \leq 3$, alors $K_p = \mathbb{Q}_p^3$ et on a l'homomorphisme

$$\lambda_p : E_n(\mathbb{Q}_p) \to (\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2)^3,$$
$$(x,y) \mapsto (x-\rho_1, x-\rho_2, x-\rho_3) \mod (\mathbb{Q}_p^{*2})^3 \text{ si } x \neq \rho_i,$$
$$(\rho_1, 0) \mapsto (G_n'(\rho_1), \rho_1-\rho_2, \rho_1-\rho_3) \mod (\mathbb{Q}_p^{*2})^3,\ O \mapsto 1.$$

On définit de la même façon les images de $(\rho_2, 0)$ et $(\rho_3, 0)$.

Par la suite, pour $\alpha \in K^*$, $\alpha', \alpha''$ désigneront les conjugués de $\alpha$; $[\alpha]$ désignera la classe de $\alpha$ dans $K^*/K^{*2}$ et $[\alpha]_p$ la classe de $\alpha$ dans $K_p^*/K_p^{*2}$.

4.1. *Caractérisation de Im$\lambda_p$.* Nous caractérisons les éléments de Im$\lambda_p$, en distinguant deux cas $p \nmid n-1$ et $p | n-1$.

Cas où $p \nmid n-1$.

Lemme 4.2. *Soit $p$ un nombre premier tel que $p \nmid n-1$, $\mathfrak{p}$ un idéal premier au dessus de $p$. Soit $\alpha \in K^*$ tel que $[\alpha]_p \in \mathrm{Im}\lambda_p$ alors $\alpha$ a une valuation $\mathfrak{p}$-adique paire.*

Preuve. (1) Si $p\mathbb{Z}_K$ ne se décompose pas dans $K/\mathbb{Q}$, alors l'idéal $p\mathbb{Z}_K$ est inerte ou ramifié. Soit $\alpha$ un représentant de l'élément $[\alpha]_p$ de $K_p^*/K_p^{*2}$, où $[\alpha]_p \in \mathrm{Im}\lambda_p$. Alors il existe $\beta \in K_p^*$ et $(x,y) \in E_n(\mathbb{Q}_p)$ tel que $\alpha = (x-\rho_1)\beta^2$. Comme $K_p/\mathbb{Q}_p$ est une extension cubique et $x-\rho_i$, $1 \leq i \leq 3$ sont conjugués, alors les valuations $\mathfrak{p}$-adiques de $x-\rho_1, x-\rho_2$ et $x-\rho_3$ sont égales et le produit $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est un carré alors $v_p(x-\rho_i) \equiv 0 \mod 2$. Il en résulte que $\alpha$ a une valuation $\mathfrak{p}$-adique paire.

(2) Si $p\mathbb{Z}_K$ se décompose dans $K/\mathbb{Q}$ et $p$ ne divise pas $n-1$, alors $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Soit $(\alpha, \alpha', \alpha'')$ un représentant d'un élément $[\alpha]_p$ de $K_p^*/K_p^{*2}$, où $[\alpha]_p \in \mathrm{Im}\lambda_p$ alors il existe $\beta_i \in \mathbb{Q}_p^*$ et $(x,y) \in E_n(\mathbb{Q}_p)$ tels que $(\alpha, \alpha', \alpha'') = ((x-\rho_1)\beta_1^2, (x-\rho_2)\beta_2^2, (x-\rho_3)\beta_3^2)$. Posons $v_p(x-\rho_i) = m_i$, $1 \leq i \leq 3$. Comme le produit $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est un carré alors $m_1+m_2+m_3 \equiv 0 \mod 2$ $(*)$.

Si $m_1 < 0$, comme $v_p(\rho_1) = 0 \neq m_1$ alors $v_p(x) = \inf(v_p(x - \rho_1), v_p(\rho_1)) = m_1$. De plus, $v_p(\rho_2) = 0$ donc $v_p(x - \rho_2) = \inf(v_p(x), v_p(\rho_2)) = m_1$, et de même $v_p(x - \rho_3) = m_1$. En remplaçant dans $(*)$, on déduit alors que $m_1$ est pair. Si $m_1 > 0$, comme l'idéal $p\mathbb{Z}_K$ se décompose dans l'extension $K/\mathbb{Q}$ alors $p$ ne divise pas le discriminant du corps, il en résulte que $v_p(\rho_i - \rho_j) = 0$ si $i \neq j$. On a alors $v_p(x - \rho_j) = \inf(v_p(x - \rho_1), v_p(\rho_1 - \rho_j)) = 0$, $2 \leq j \leq 3$. On en déduit alors que $m_i \equiv 0 \mod 2$ pour $1 \leq i \leq 3$.

□

REMARQUE 4.3. La condition "$p$ ne divise pas $n-1$" est seulement essentielle pour la preuve du cas $m_1 > 0$.

PROPOSITION 4.4. *Supposons que $p \nmid n-1$ et $p$ décomposé. Soit $\alpha \in K^*$, alors $[\alpha]_p$ est dans $\mathrm{Im}\lambda_p$ si et seulement si le produit $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$.*

PREUVE. Soit $(\alpha, \alpha', \alpha'')$ un représentant de l'élément $[\alpha]_p$ de $Im\lambda_p$ alors il existe $\beta_i \in \mathbb{Q}_p^*$ et $(x, y) \in E_n(\mathbb{Q}_p)$ tels que $(\alpha, \alpha', \alpha'') = ((x - \rho_1)\beta_1^2, (x - \rho_2)\beta_2^2, (x - \rho_3)\beta_3^2)$, on déduit alors que le produit $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$. De plus, d'après le lemme 4.2, $\alpha = p^{2m}u, \alpha' = p^{2m'}u'$ et $\alpha'' = p^{2m''}u''$, où $u, u', u'' \in \mathbb{Z}_p^*$ et $m, m', m'' \in \mathbb{Z}$.

Considérons l'application $\mu : \mathrm{Im}\lambda_p \to (\mathbb{Z}_p^*/\mathbb{Z}_p^{*2})^3$, définie par

$$(\alpha_1, \alpha_2, \alpha_3) \mod (\mathbb{Q}_p^{*2})^3 \mapsto (u_1, u_2, u_3) \mod (\mathbb{Z}_p^{*2})^3,$$

où $\alpha_i = p^{2m_i}u_i$, $m_i \in \mathbb{Z}, u_i \in \mathbb{Z}_p^*, 1 \leq i \leq 3$. L'application $\mu$ est un homomorphisme injectif, et le 2-rang de $\mathrm{Im}\lambda_p$ est égal à 2. En effet, les racines de $G_n$ sont dans $K$ et $K \hookrightarrow \mathbb{Q}_p$. Les points d'ordre 2 sont dans $E_n(\mathbb{Q}_p)$, ce qui entraîne que $(\mathbb{Z}/2\mathbb{Z})^2 \subset \mathrm{Im}\lambda_p$. Comme $\mu$ n'est pas surjectif alors $\mathrm{Im}\lambda_p \backsimeq (\mathbb{Z}/2\mathbb{Z})^2$. Comme $[\alpha]_p \in K_p^*/K_p^{*2}$ alors $\alpha = p^j u, \alpha' = p^{j_1}u', \alpha" = p^{j_2}u''$ $(j, j_1, j_2 \in \mathbb{Z}$ et $u, u', u'' \in \mathbb{Z}_p^*)$. D'autre part $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$, donc $uu'u''$ est un carré de $\mathbb{Z}_p^*$, d'où $[\alpha]_p \in \mathrm{Im}\lambda_p$. Ce qui termine la démonstration de la proposition. □

CAS OÙ $p|n-1$.

PROPOSITION 4.5. *Soit $p$ un nombre premier tel que $p|n-1$. Soit l'application $\lambda_p : E_n(\mathbb{Q}_p) \to (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3$, définie par*

$$R = (x, y) \mapsto (x - \rho_1, x - \rho_2, x - \rho_3) \mod (\mathbb{Q}_p^{*2})^3.$$

*Si la réduction est déployée en $p$, alors $x - \rho_1$ est un carré de $\mathbb{Q}_p^*$. Si la réduction n'est pas déployée en $p$ et $(x, y) \in E_n^0(\mathbb{Q}_p)$, alors $x - \rho_1$ est un carré de $\mathbb{Q}_p^*$.*

PREUVE. Soit $R = (x, y) \notin E_n^0(\mathbb{Q}_p)$ alors $(x, y)$ se réduit sur le point $(1, 0)$. Donc $x - \rho_1 \equiv \rho_2 - \rho_1 \mod p$ et comme $\rho_2 - \rho_1 \equiv 2 \mod p$ et 2 est un carré mod $p$, on déduit alors que $x - \rho_1$ est un carré mod $p$. C'est donc un carré de $\mathbb{Z}_p^*$ car $p \neq 2$.

Si $R \in E_n^0(\mathbb{Q}_p)$ et $R \notin E_n^1(\mathbb{Q}_p)$ alors $v_p(x - \rho_2) = v_p(x - \rho_3) = 0$ et $x - \rho_2 \equiv x - \rho_3 \mod p$, donc $(x - \rho_2)(x - \rho_3)$ est un carré dans $\mathbb{Q}_p^*$, comme le produit $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est aussi un carré, alors $x-\rho_1$ est un carré de $\mathbb{Q}_p^*$.

Si $R \in E_n^1(\mathbb{Q}_p)$ alors les valuations de $x - \rho_i$ sont négatives et $x - \rho_i = p^{-2n} e_i$ avec $1 \leq i \leq 3$ et $e_i \in \mathbb{Z}_p^*$. Comme $e_i \equiv e_j \mod p$ et $e_i^3 \equiv \eta^2 \mod p$ alors $e_i$ est un carré. □

COROLLAIRE 4.6. *Soit $(x, y) \in E_n(\mathbb{Q})$. L'idéal principal $(x - \rho_1)$ a pour décomposition*

$$(x - \rho_1) = \mathfrak{a}\mathfrak{b}^2$$

*où* $\mathfrak{a} = \prod_{p|n-1} (\mathfrak{p}_2\mathfrak{p}_3)^{\gamma_p}$ *et* $\gamma_p \in \{0, 1\}$.

PREUVE. La preuve se déduit du lemme 4.2, de la proposition 4.5 et du fait que si $(x, y) \notin E_n^0(\mathbb{Q}_p)$ alors $v_{\mathfrak{p}_1}(x - \rho_1) = 0$. □

REMARQUE 4.7. Donnons un exemple de $n$ et $p$ tels que $\gamma_p = 1$.

EXEMPLE 4.8. Considérons la courbe elliptique $E_8$ donnée par l'équation:

$$y^2 = x^3 - 64x^2 + 405x + 1.$$

Le point $(64, 161)$ est un point de la courbe $E_8$. La décomposition en idéaux premiers de l'idéal principal $(64 - \rho_1)$ est la suivante:

$$(64 - \rho_1) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{c}^2,$$

avec $\mathfrak{c} = 23\mathbb{Z}_K + (5 + \rho_1)\mathbb{Z}_K$, et $\mathfrak{p}_1 = 7\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$, $\mathfrak{p}_2 = \mathfrak{p}_1^{\sigma}, \mathfrak{p}_3 = \mathfrak{p}_1^{\sigma^2}$. On déduit alors que les valuations $\mathfrak{p}_i$-adique, pour $2 \leq i \leq 3$, de $64 - \rho_1$ sont impaires.

Si $p|n - 1$, deux difficultés apparaissent:

1. La première est liée à la non parité de $v_p(x-\rho_1)$ montrée dans l'exemple précédent.
2. La deuxième est liée au fait qu'on ne peut plus utiliser les points d'ordre 2 pour étudier $Im\lambda_p$.

La proposition suivante donne un équivalent de la proposition 4.4 avec des hypothèses sur $n$ et en restreignant $\lambda_p$.

Soit

$$H_p = \{[\alpha]_p \in (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3 : \alpha \in K^*, v_p(\alpha) \equiv v_p(\alpha') \equiv v_p(\alpha'') \equiv 0 \mod 2\}.$$

Posons $H'_p = \lambda_p^{-1}(H_p)$. Soit l'homomorphisme $\lambda'_p : H'_p \to (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3$.

PROPOSITION 4.9. *Supposons que $n-1=m^2$ (resp. $-m^2$) avec $m\in\mathbb{Z}$. Soit $p$ un nombre premier et $p\mid m$.*

1. *Si $p\equiv\pm 3$ mod 8, alors $[\alpha]_p$ est dans $\mathrm{Im}\lambda'_p$ si et seulement si le produit $\alpha\alpha'\alpha''$ est un carré de $\mathbb{Q}_p^*$ et $\alpha,\alpha',\alpha''$ ont des valuations $p$-adique paires.*
2. *Si $p\equiv -1$ mod 8, alors $[\alpha]_p$ est dans $\mathrm{Im}\lambda'_p$ si et seulement si $\alpha$ et $\alpha\alpha'\alpha''$ sont des carrés de $\mathbb{Q}_p^*$ et $\alpha,\alpha',\alpha''$ ont des valuations $p$-adique paires.*

Dans la preuve de cette proposition, on utilisera le résultat suivant, qu'on expliquera dans le dernier paragraphe: si $n-1=m^2$ (resp. $-m^2$) le point $(1,m^3)$ (resp. $(1-m^2,m^3)$) est un point de $E_n(\mathbb{Q})$.

PREUVE. Soit $(\alpha,\alpha',\alpha'')$ un représentant de l'élément $[\alpha]_p$ de $\mathrm{Im}\lambda'_p$ alors il existe $\beta_i\in\mathbb{Q}_p^*$ et $(x,y)\in H'_p$ tels que $(\alpha,\alpha',\alpha'')=((x-\rho_1)\beta_1^2,(x-\rho_2)\beta_2^2,(x-\rho_3)\beta_3^2)$ et les $x-\rho_i$, $1\leq i\leq 3$, ont des valuations paires. On déduit alors que les valuations $p$-adique de $\alpha$ et ses conjugués sont paires.

Réciproquement, considérons l'application définie par

$$\mu' : \mathrm{Im}\lambda'_p \to (\mathbb{Z}_p^*/\mathbb{Z}_p^{*2})^3,$$

$$(\alpha_1,\alpha_2,\alpha_3) \mod (\mathbb{Q}_p^{*2})^3 \mapsto (u_1,u_2,u_3) \mod (\mathbb{Z}_p^{*2})^3$$

où $\alpha_i=p^{2m_i}u_i$, $m_i\in\mathbb{Z}$, $1\leq i\leq 3$. L'application $\mu'$ est un homomorphisme injectif.

Étudions le 2-rang de $\mathrm{Im}\lambda'_{\mathrm{p}}$.

• Si $p\equiv\pm 3$ mod 8, alors 2 n'est pas un carré mod $p$ et on va distinguer deux cas:

1. Si $p\equiv 1 \bmod 4$ alors $-1$ est un carré mod $p$ et si $n-1=m^2$ (resp. $-m^2$), comme $\rho_1-\rho_i$, $2\leq i\leq 3$, et $1-\rho_1$ sont congrus respectivement à $-2$ mod $p$ et 2 mod $p$, alors $\rho_1-\rho_i$, $2\leq i\leq 3$, et $1-\rho_1$ ne sont pas des carrés dans $\mathbb{Q}_p^*$. On en déduit que les points $(\rho_1,0)$ et $(1,m^3)$ (resp. $(\rho_1,0)$ et $(1-m^2,m^3)$) ne sont pas dans $2E_n(\mathbb{Q}_p)$. D'autre part, les valuations $p$-adique de $\rho_1-\rho_i$, $2\leq i\leq 3$, et $1-\rho_j$, $1\leq j\leq 3$ sont paires, donc les points $(\rho_1,0)$ et $(1,m^3)$ (resp. $(\rho_1,0)$ et $(1-m^2,m^3)$) sont dans $H'_p$. La première composante de $\lambda'_p(\rho_1,0)$ est un carré et celles de $\lambda'_p(1,m^3)$ et $\lambda'_p(1-m^2,m^3)$ sont égales à $1-\rho_1$ qui est congru à 2 mod $p$ (non carré mod $p$). On en déduit que le 2-rang de $\mathrm{Im}\lambda'_{\mathrm{p}}$ est égal à 2.
2. Si $p\equiv 3 \bmod 4$ alors $-1$ n'est pas un carré mod $p$. Comme précédemment on montre que les points $(0,1)$ et $(1,m^3)$ (resp. $(0,1)$ et $(1-m^2,m^3)$) sont dans $H'_p$ et ne sont pas dans $2E_n(\mathbb{Q}_p)$. Leurs images par $\lambda'_p$ sont différentes, le 2-rang de $\mathrm{Im}\lambda'_p$ est égal à 2.

Comme $\alpha\alpha'\alpha''$ est un carré dans $\mathbb{Q}_p^*$, et $\alpha, \alpha', \alpha''$ ont des valuations paires alors $\alpha = p^{2j_1}u$, $\alpha' = p^{2j_2}u'$, $\alpha'' = p^{2j_3}u''$, $j_i \in \mathbb{Z}$, $1 \leq i \leq 3$ et $uu'u''$ est dans $\mathbb{Z}_p^{*2}$. D'où $[\alpha]_p \in \mathrm{Im}\lambda'_p$.

• Si $p \equiv -1 \bmod 8$ alors 2 est un carré mod $p$. D'après la proposition 4.9, on déduit que le 2-rang de $\mathrm{Im}\lambda'_p$ est strictement plus petit que 2. En reprenant les mêmes arguments utilisés dans 1), on montre alors que le point $(\rho_1, 0)$ est un point de $H'_p$ qui n'est pas dans $2E_n(\mathbb{Q}_p)$, que la première composante de $\lambda'_p(\rho_1, 0)$ est un carré et que les deux autres composantes ne sont pas des carrés. Donc le 2-rang de $\mathrm{Im}\lambda'_p$ est égal à 1.

Comme $\alpha$, $\alpha\alpha'\alpha''$ sont des carrés dans $\mathbb{Q}_p^*$, et $\alpha, \alpha', \alpha''$ ont des valuations paires alors $\alpha = p^{2j_1}u$, $\alpha' = p^{2j_2}u'$, $\alpha'' = p^{2j_3}u''$, $j_i \in \mathbb{Z}$, $u$ et $uu'u''$ sont dans $\mathbb{Z}_p^{*2}$. D'où $[\alpha]_p \in \mathrm{Im}\lambda'_p$, ce qui montre la proposition. □

## 5. Rang de courbes elliptiques

Soit $p$ une place et $\alpha \in K^*$, le 2-*groupe de Selmer*, noté $S_2(\mathbb{Q})$, est défini par

$$S_2(\mathbb{Q}) = \{[\alpha] \in K^*/K^{*2} : \ \forall p \quad [\alpha]_p \in \mathrm{Im}\ \lambda_p\}.$$

Soit $U$ le sous-groupe de $K^*/K^{*2}$,

$$U = \{[u] \in K^*/K^{*2} : [u]_p \in \mathrm{Im}\lambda_p \text{ si } p \nmid n-1$$
$$\text{ou si } p \text{ est une place infinie}, [u]_p \in \mathrm{Im}\lambda'_p \text{ si } p|n-1\}.$$

Considérons le sous-groupe $S'_2(\mathbb{Q})$ de $S_2(\mathbb{Q})$ défini par:

$$S'_2(\mathbb{Q}) = \{[\alpha] \in S_2(\mathbb{Q}) : [\alpha] \in U\}.$$

Lemme 5.1. *Pour chaque élément $\alpha \in K^*$, tel que $[\alpha] \in S'_2(\mathbb{Q})$, il existe un idéal $I_\alpha$ tel que $(\alpha) = I_\alpha^2$. Si cet idéal est principal alors $\alpha$ ou $-\rho_1\alpha$ est un carré.*

Preuve. Soit $\alpha$ un représentant d'un élément de $S'_2(\mathbb{Q})$. Alors $[\alpha] \in U$; d'après le lemme 4.2 et la proposition 4.5, l'idéal principal $(\alpha)$ est un carré, donc $(\alpha) = I_\alpha^2$. On déduit alors que $\overline{I_\alpha} \in C_2(K)$.

Si $I_\alpha$ est principal, alors il existe une unité $\epsilon$ et un élément $\gamma_1$ de $K^*$ tel que $I_\alpha = (\gamma_1)$ et $\alpha = \epsilon\gamma_1^2$. Comme $[\alpha] \in S'_2(\mathbb{Q})$ alors localement $[\alpha]_\infty \in \mathbb{R}$, il existe donc $(x, y) \in E_n(\mathbb{R})$ et $\beta_i \in \mathbb{R}$ tels que $(\alpha, \alpha', \alpha'') = ((x-\rho_1)\beta_1^2, (x-\rho_2)\beta_2^2, (x-\rho_3)\beta_3^2)$, et $(x-\rho_1)(x-\rho_2)(x-\rho_3)$ est un carré dans $\mathbb{R}$. Comme $x-\rho_1 > x-\rho_2 > x-\rho_3$, alors les signes de $\alpha$, $\alpha'$, $\alpha''$ sont: +, +, + ou +, -, -. Il en résulte alors que $\epsilon$ ou $-\rho_1\epsilon$ est totalement positif. Donc $\alpha$ ou $-\rho_1\alpha$ est un carré, ce qui termine la démonstration du lemme. □

On énonce le lemme suivant qu'on utilisera dans la preuve de la proposition suivante. La preuve de ce lemme reprend la même idée que [21, page 377].

Lemme 5.2. *Soit $x \in K$ premier avec 2.*

(1) *Il existe une unité $\epsilon$ de $K$ tel que $x\epsilon$ est un carré dans $\mathbb{Z}_K/4\mathbb{Z}_K$.*
(2) *Soit $T = \{c_0+c_1\rho_1+c_2\rho_2 : c_i \in \{0, \pm 1, 2\}\}$ un système de représentants des éléments de $\mathbb{Z}_K/4\mathbb{Z}_K$.*
   - *Si $n \equiv 0$ mod 4, si $\beta \in T$ alors $\rho_3\beta^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2$ mod 4, avec $c_2 \not\equiv 0$ mod 4.*
   - *Si $n \equiv 2$ mod 4, si $\beta \in T$ alors $\rho_2\beta^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2$ mod 4, avec $c_2 \not\equiv 0$ mod 4.*

PROPOSITION 5.3. *Soit $n_p$ le nombre de facteurs premiers de $n-1$. Le rang $r$ de $E_n(\mathbb{Q})$ satisfait l'inégalité*

$$r \leq 1 + n_p + r_2.$$

*Si de plus on pose $H = \cap_{p|n-1} H'_p \cap E_n(\mathbb{Q})$, alors*

$$\mathrm{rg}_2(H/2E_n(\mathbb{Q})) \leq 1 + r_2.$$

PREUVE. D'après la proposition 4.1, on déduit que $|\mathrm{Im}\lambda_{\mathbb{Q}}| = 2^{\mathrm{r}}$. Comme $(x, y) \in E_n(\mathbb{Q})$ alors $x = \dfrac{m}{e^2}, y = \dfrac{l}{e^3}$ où $m, l, e \in \mathbb{Z}$ et $(m, e) = (l, e) = 1$. Il en résulte que $l^2 \equiv m^3 + m(-n+1)e^4 + e^6 \bmod 4$. On déduit alors que $l$ est toujours impair.

Si $e$ est pair alors $m$ et $l$ sont impairs et en remplaçant dans l'équivalence précédente, on déduit la congruence suivante $l^2 \equiv m^3 \bmod 4$, il en résulte alors que $m - \rho_1 e^2 \equiv m \equiv 1 \bmod 4$. Si $e$ est impair alors $m - \rho_1 e^2 \equiv c_0 - \rho_1 \bmod 4$ où $c_0 \in \{0, \pm 1, 2\}$. D'après le corollaire 4.6, on obtient:

$$(m - \rho_1 e^2) = \mathfrak{a}\mathfrak{b}'^2,$$

où $\mathfrak{a} = \prod_{p|n-1} (\mathfrak{p}_2\mathfrak{p}_3)^{\gamma_p}$, $\mathfrak{b}' = (e)\mathfrak{b}$, $\mathfrak{a}$ et $\mathfrak{b}'$ sont des idéaux entiers premiers à 2 et $\gamma_p \in \{0, 1\}$, ce qui montre que l'inverse de la classe de $\mathfrak{a}$ dans le groupe des classes d'idéaux est un carré. Ainsi pour chaque $\mathfrak{a}$ choisissons $\mu_{\mathfrak{a}} > 0$ et $\mathfrak{b}'_{\mathfrak{a}}$ tels que

$$(\mu_{\mathfrak{a}}) = \mathfrak{a}(\mathfrak{b}'_{\mathfrak{a}})^2.$$

Le nombre de possibilités de l'idéal $\mathfrak{a}$ et donc de $\mu_{\mathfrak{a}}$ est au plus égal à $2^{n_p}$. Donc

$$(m - \rho_1 e^2) = (\mu_{\mathfrak{a}})(\mathfrak{b}'(\mathfrak{b}'_{\mathfrak{a}})^{-1})^2,$$

ce qui entraîne que $\mathfrak{b}'(\mathfrak{b}'_{\mathfrak{a}})^{-1} \in C_2(K)$. Soit $J_1, J_2, \cdots, J_{r_2}$ des idéaux dont les classes forment une base de $C_2(K)$ en tant que $\mathbb{F}_2$-espace vectoriel, tels que $J_i^2 = (\xi_i)$ où $\xi_i \in \mathbb{Z}_K$ et $\xi_i > 0$ alors

$$(\mathfrak{b}'(\mathfrak{b}'_{\mathfrak{a}})^{-1})^2 = (\alpha^2 \xi_1^{\nu_1} \cdots \xi_{r_2}^{\nu_{r_2}}),$$

où $\alpha \in K^*$ et $\nu_i \in \{0, 1\}$. Donc

$$m - \rho_1 e^2 = u\alpha^2\gamma \tag{5.1}$$

où $u \in \mathbb{Z}_K^*$ et $\gamma = \mu_{\mathfrak{a}} \xi_1^{\nu_1} \cdots \xi_{r_2}^{\nu_{r_2}}$. En reprenant le raisonnement fait dans la deuxième partie du lemme 5.1, on montre alors que $u$ est positive. Comme le groupe des unités positives est de rang égal à 2. On déduit alors que le nombre de $m - \rho_1 e^2$ mod $K^{*2}$ est au plus égal à $2^{2+n_p+r_2}$. On peut réduire l'exposant de 1 en tenant compte du lemme précédent et de la [18, proposition 1.3]. On compte alors, modulo 4, le nombre de classes des unités positives et on compare au reste modulo 4 de $m - \rho_1 e^2$.

(1) Si $n \equiv 0 \bmod 4$, alors $m - \rho_1 e^2 \equiv 1$ ou $c_0 - \rho_1 \bmod 4$ et $\rho_3 \beta^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2 \bmod 4$, où $c_2 \not\equiv 0 \bmod 4$.
(2) Si $n \equiv 2 \bmod 4$, alors $m - \rho_1 e^2 \equiv 1$ ou $c_0 - \rho_1 \bmod 4$ et $\rho_2 \beta^2 \equiv c_0 + c_1\rho_1 + c_2\rho_2 \bmod 4$, où $c_2 \not\equiv 0 \bmod 4$,

ce qui prouve que $r \leq 1 + n_p + r_2$, ce qui termine la démonstration de la première partie de la proposition.

Considérons la restriction $\lambda_1$ de l'application $\lambda_{\mathbb{Q}}$ au sous-groupe $H$, $\lambda_1 : H \to K^*/K^{*2}$. Alors $Im\lambda_1 \backsimeq H/2E_n(\mathbb{Q})$. Comme $(x, y) \in H$ alors $(m - \rho_1 e^2) = ((e)\mathfrak{b})^2$. En reprenant le raisonnement fait précédemment, on déduit que le nombre de $(m - \rho_1 e^2)K^{*2}$ est au plus égal à $2^{1+r_2}$, ce qui termine la preuve de la proposition. □

Exemple 5.4. Considérons la courbe elliptique $E_{-14}$ donnée par l'équation:

$$y^2 = x^3 - 196x^2 - 3181x + 1.$$

D'après le programme mwrank de Cremona [6], les points $Q_1 = (459, 7345)$, $Q_2 = (0, 1)$, $Q_3 = (3661, 215475)$, forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Les décompositions des idéaux principaux $(459 - \rho_1), (3661 - \rho_1)$ sont les suivantes:

$$(459 - \rho_1) = \mathfrak{r}_1^2 \mathfrak{r}_2^2 \mathfrak{r}_3^2,$$

tels que $\mathfrak{r}_1 = 5\mathbb{Z}_K + (1 + \rho_1)\mathbb{Z}_K, \mathfrak{r}_2 = 13\mathbb{Z}_K + (-4 + \rho_1)\mathbb{Z}_K, \mathfrak{r}_3 = 113\mathbb{Z}_K + (-7 + \rho_1)\mathbb{Z}_K$,

$$(3661 - \rho_1) = \mathfrak{r}_1^{\sigma}(\mathfrak{r}_1^{\sigma^2})^3 \mathfrak{r}_4^{\sigma} \mathfrak{r}_4^{\sigma^2} \mathfrak{r}_5^2 \mathfrak{r}_6^2,$$

avec $\mathfrak{r}_4 = 3\mathbb{Z}_K + (1+\rho_1)\mathbb{Z}_K$, $\mathfrak{r}_5 = 13\mathbb{Z}_K + (\rho_1+5)\mathbb{Z}_K$, $\mathfrak{r}_6 = 17\mathbb{Z}_K + (\rho_1-6)\mathbb{Z}_K$.

Les points $Q_1, Q_2$ sont dans $H$ et on montre que leurs classes forment une base de $H/2E_{-14}(\mathbb{Q})$, donc $rg_2(H/2E_{-14}(\mathbb{Q})) = 2$. Comme $r_2$ est pair, on déduit d'après la proposition 5.3 que $r_2 \geq 2$. D'après le programme pari [16], on trouve que $r_2 = 2$.

## 6. Sous-groupe du 2-groupe de Selmer et 2-rang du groupe de classes

Dans [21], L. C. Washington a étudié la famille de courbes elliptiques $C_a$ définies par l'équation $y^2 = P_a(x)$, où $P_a(x) = x^3 - (a + 3)x^2 + ax + 1$; et il a montré le résultat suivant.

THÉORÈME 6.1. *Le rang $rg(C_a(\mathbb{Q}))$ de la courbe elliptique $C_a(\mathbb{Q})$ est au plus égal à $1+r_2$. En fait la suite suivante est exacte:*

$$1 \longrightarrow C_a^0(\mathbb{Q})/2C_a(\mathbb{Q}) \longrightarrow C_2 \longrightarrow Ш_2 \longrightarrow 1,$$

*où $C_a^0(\mathbb{Q}) = 2C_a(\mathbb{R}) \cap C_a(\mathbb{Q})$, $Ш_2$ est la 2-torsion du groupe de Tate-Shafarevich et $C_2$ le 2-groupe des classes des corps définis par les polynômes $P_a(x)$.*

Dans ce paragraphe, sous les hypothèses de la proposition 4.9, la proposition suivante donne un équivalent du théorème 6.1.

PROPOSITION 6.2. *Si $n-1=m^2$ (resp. $-m^2$), soit $p$ un nombre premier qui divise $n-1$, $p \equiv \pm 3$ mod 8 ou $p \equiv -1$ mod 8. Alors la suite*

$$1 \longrightarrow \langle[(0,1)]\rangle \longrightarrow S_2'(\mathbb{Q}) \xrightarrow{\nu} C_2(K) \longrightarrow 1,$$
$$\nu : [\alpha] \mapsto \overline{I_\alpha},$$

*est une suite exacte.*

PREUVE. D'après le lemme 5.1, pour chaque $[\alpha] \in S_2'(\mathbb{Q})$ il existe un idéal $I_\alpha$ tel que $I_\alpha^2 = (\alpha)$, donc $\overline{I_\alpha} \in C_2(K)$.

Montrons que $\nu$ est surjective. Soit $\overline{I_\alpha} \in C_2(K)$, alors $(\alpha) = I_\alpha^2$.

Nous allons montrer que $[\alpha]_p \in \mathrm{Im}\lambda_{\mathrm{p}}$ si $p \nmid n-1$, $[\alpha]_p \in \mathrm{Im}\lambda'_{\mathrm{p}}$ si $p|n-1$.

(1) Si $p\mathbb{Z}_K$ n'est pas décomposé (resp. est décomposé et $p$ ne divise pas $n-1$), on reprend la même preuve faite dans [21, pages 377, 378].
(2) Supposons que $p\mathbb{Z}_K$ se décompose dans $K/\mathbb{Q}$ et $p$ divise $n-1$. Alors on distingue deux cas:
   (a) Si $p \equiv \pm 3$ mod 8, alors comme précédemment on reprend la même preuve faite dans [21, page 378], on montre que $\alpha\alpha'\alpha''$ est un carré dans $\mathbb{Q}_p^*$. D'après la proposition 4.9, on déduit que $[\alpha]_p \in \mathrm{Im}\lambda'_{\mathrm{p}}$.
   (b) Si $p \equiv -1$ mod 8, $I_\alpha^2 = (\alpha)$ avec $\alpha = p^{2m}u$ où $u \in \mathbb{Z}_p^*$. Si $u \notin \mathbb{Z}_p^{*2}$, comme $\rho_1 \equiv -1$ mod $p$ alors $\rho_1 u \equiv -u$ mod $p$, donc $-u$ est un carré mod $p$. Il en résulte que $\rho_1\rho_2\alpha$ est un carré mod $p$. La norme de $\rho_1\rho_2\alpha$ est un carré alors d'après la proposition 4.9, $[\rho_1\rho_2\alpha]_p \in \mathrm{Im}\lambda'_{\mathrm{p}}$ et de plus $(\rho_1\rho_2\alpha) = (\alpha) = I_\alpha^2$.

D'après le lemme 5.1, $ker\ \nu = \{1, -\rho_1\}K^{*2}/K^{*2} \backsimeq \langle[(0,1)]\rangle$, ce qui termine la démonstration de la proposition. □

Maintenant considérons la restriction $\lambda_1$ de l'application $\lambda_{\mathbb{Q}}$ au sous-groupe $H = \cap_{p|n-1} H_p' \cap E_n(\mathbb{Q})$,

$$\lambda_1 : H \to K^*/K^{*2}.$$

Montrons que $\mathrm{Im}\lambda_1 \subseteq \mathrm{S}_2'(\mathbb{Q})$. Soit $[\alpha] \in \mathrm{Im}\lambda_1$ alors il existe $(x,y) \in H$, $\beta_1 \in \mathbb{Q}$ tel que $\alpha = (x-\rho_1)\beta_1^2$, donc $[\alpha] \in U$ il en résulte que $[\alpha] \in S_2'(\mathbb{Q})$.

Donc $\lambda_1$ induit un homomorphisme injectif

$$f_1 : H/2E_n(\mathbb{Q}) \to S_2'(\mathbb{Q}).$$

Et on obtient alors la suite exacte suivante:

$$1 \longrightarrow H/2E_n(\mathbb{Q}) \longrightarrow S_2'(\mathbb{Q}) \longrightarrow Ш_2' \longrightarrow 1,$$

où $Ш_2'$ est le conoyau de $f_1$.

PROPOSITION 6.3. *Soit $E_n'(\mathbb{Q}) = 2E_n(\mathbb{R}) \cap E_n(\mathbb{Q})$ et $rg_2(H/2E_n(\mathbb{Q}))$ la dimension de $H/2E_n(\mathbb{Q})$ en tant que $\mathbb{F}_2$-espace vectoriel. Sous les hypothèses de la proposition 6.2, la suite*

$$1 \longrightarrow (E_n'(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q}) \xrightarrow{\mu} C_2(K) \longrightarrow Ш_2' \longrightarrow 1,$$
$$\mu : [(x,y)] \mapsto \overline{I_x},\ (x-\rho_1) = I_x^2,$$

*est exacte. De plus,*

$$\mathrm{rg}_2(H/2E_n(\mathbb{Q})) \leq 1 + r_2.$$

PREUVE. Considérons le diagramme commutatif suivant, dont les deux lignes sont exactes.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \langle[(0,1)]\rangle & \xrightarrow{\nu_1} & S_2'(\mathbb{Q}) & \xrightarrow{\nu} & C_2(K) & \longrightarrow & 1 \\
\downarrow & & \downarrow{\scriptstyle\sigma} & & \downarrow & & \downarrow{\scriptstyle\tau} & & \downarrow \\
1 & \longrightarrow & H/2E_n(\mathbb{Q}) & \longrightarrow & S_2'(\mathbb{Q}) & \longrightarrow & Ш_2' & \longrightarrow & 1
\end{array}$$

où $\sigma$ est l'injection canonique, $\tau$ est la surjection naturelle.

Comme $H/2E_n(\mathbb{Q}) = \langle[0,1]\rangle \oplus (E_n'(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q})$, alors la suite suivante est exacte:

$$1 \to (E_n'(\mathbb{Q}) \cap H)/2E_n(\mathbb{Q}) \to C_2(K) \to Ш_2' \to 1.$$

On déduit alors que $\mathrm{rg}_2(H/2E_n(\mathbb{Q})) \leq 1 + r_2$, ce qui termine la démonstration de la proposition. □

## 7. EXEMPLES

Les résultats du paragraphe précédent montrent que pour trouver des corps cubiques $K$ de 2-rang élevé, on peut essayer de construire des courbes elliptiques ($y^2 = G_n(x)$) de rang grand. Pour cela, il est habituel de partir d'une courbe sur $\mathbb{Q}(t)$ de rang non nul et de spécialiser $t$. Nous avons cherché pour la famille de Washington à élever le rang et obtenons une relation entre les deux familles expliquée ci-dessous.

Soit $P_a(x) = x^3 - (a+3)x^2 + ax + 1$, avec $a \in \mathbb{Q}$, on considère la courbe elliptique $y^2 = P_a(x)$. Les points d'ordonnée 1 sont rationnels si $P_a(x) - 1 = x(x^2 - (a+3)x + a)$ a trois racines rationnels c'est à dire si $(a+3)^2 - 4a$ est un carré dans $\mathbb{Q}$. En paramétrant la conique $(a+3)^2 - 4a = b^2$, on trouve que $a = (k+1)(k-2)/k$. En remplaçant la valeur de $a$ obtenue dans le

polynôme $P_a(x)$, et en posant le changement de variable $x=(u-1)/k$, on a $P_a(x)=Q_1(x)$ avec

$$k^3Q_1(u)=G_{k+1}(u)=u^3-(k+1)^2u^2+(k^3+k^2+2k-1)u+1.$$

La courbe $y^2=P_a(x)$ admet trois points rationnels

$$x=0,y=1 \text{ et } x=k+1,y=1 \text{ et } x=-2/k+1,y=1$$

dont la somme est nulle.

On montre la proposition suivante:

PROPOSITION 7.1. *Soit $n-1=m^2$ (resp. $-m^2$). Le rang des courbes elliptiques $E_n(\mathbb{Q})$, sauf pour un nombre fini de courbes, est supérieur ou égal à 3 (resp. 2). Les points $(0,1),(1,m^3),(-1+m^2,m^3)$ (resp. $(0,1),(1-m^2,m^3)$) sont des points rationnels de $E_n(\mathbb{Q})$ indépendants.*

PREUVE. Si $n-1=m^2$ (resp. $-m^2$) les points

$$u=1,y=m^3 \text{ et } u=-1+m^2,y=m^3 \text{ et } u=1+m^2+m^4,y=m^3$$

(resp. $(1-m^2,m^3)$) sont sur la courbe $y^2=G_n(u)$.

En spécialisant pour $m=3$ les points $(0,1)$, $(1,m^3)$, $(-1+m^2,m^3)$ (resp. $(0,1),(1-m^2,m^3)$) sont indépendants. Donc si $n-1$ est un carré (resp. $n-1=-m^2$) et d'après [17], sauf peut-être pour un nombre fini de courbes le rang est supérieur ou égal à 3 (resp. à 2). □

A. Dujella a utilisé la méthode suivante pour construire l'exemple de la courbe $E_{626}$ de rang égal à 7, en spécialisant à partir des familles $E_{m^2+1}$ et $E_{-m^2+1}$. Pour $l$ un entier fixé, $E$ une courbe elliptique et $a_p=p+1-|E(\mathbb{F}_p)|$, on définit

$$\begin{aligned}
S_1(l) &= S_1(l,E)=\sum_{p\leq l,\ p \text{ premier}} \frac{-a_p+2}{p+1-a_p}\ \log(p),\\
S_2(l) &= S_2(l,E)=\sum_{p\leq l,\ p \text{ premier}} \frac{-a_p+2}{p+1-a_p},\\
S_3(l) &= S_3(l,E)=\sum_{p\leq l,\ p \text{ premier}} -a_p\ \log(p).
\end{aligned}$$

Il est alors expérimentalement connu [14] et [15], qu'on peut espérer obtenir des courbes de grand rang si $S_{i=1,2,3}(N)$ est grand. Dans [4], des arguments étayent le fait que c'est la conjecture de Birch et Swinnerton-Dyer qui fonde cette idée. Le rang est alors minoré par construction effective de points indépendants, utilisant les programmes mwrank de Cremona [6] et ratpoints de Stoll. La même méthode a été utilisée par O. Lecacheux [13] et A. Dujella [8] pour construire des courbes elliptiques de rang élevé.

La proposition suivante caractérise les éléments qui sont dans $2E_n(\mathbb{Q})$ et pour la preuve voir [21].

PROPOSITION 7.2. *Soient $E$ la courbe elliptique d'équation $y^2 = f(x)$, où $f(x)$ est un polynôme cubique, qui possède des racines distinctes. Soient $(d, e) \in E(\mathbb{Q})$ et*

$$f(x + d) = ax^3 + bx^2 + cx + e^2$$

*avec $a, b, c \in \mathbb{Q}$. Alors $(d, e) \in 2E(\mathbb{Q})$ si et seulement si*

$$q(x) = x^4 - 2bx^2 - 8aex + b^2 - 4ac$$

*a des racines rationnelles.*

Dans tous les exemples traités par la suite, en utilisant le programme mwrank et après simplification, on obtient une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Le programme pari nous donne les décompositions des idéaux principaux en facteurs d'idéaux premiers, et le 2-rang $r_2$ du groupe des classes de $K$. Ce programme utilise l'algorithme sous-exponentielle du nombre de classes et du régulateur, introduit par Hafner et McCurley [9], généralisé par Buchmann [3] et amélioré par Cohen, Diaz Y Diaz et Olivier [5]. Le principe de cet algorithme est de décomposer les idéaux de normes plus petite qu'une constante $B$ donnée par le théorème de [1], et de déterminer les relations entre ces idéaux.

I. Considérons la courbe elliptique $E_{-8}$ donnée par l'équation :

$$y^2 = x^3 - 64x^2 - 667x + 1.$$

Les points $P_1 = (-8, 27), P_2 = (0, 1), P_3 = (22473/256, -1446661/4096)$ forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Les décompositions des idéaux principaux $(-8 - \rho_1)$ et $(22473/256 - \rho_1)$ sont les suivantes:

$$(-8 - \rho_1) = (\mathfrak{q}_1^{\sigma})^2 (\mathfrak{q}_1^{\sigma^2})^4,$$

où $\mathfrak{q}_1 = 3\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$.

$$(22473/256 - \rho_1) = \mathfrak{q'}_1^2 \mathfrak{q'}_2^2 \mathfrak{q'}_3^2,$$

avec $\mathfrak{q'}_1 = 2\mathbb{Z}_K, \mathfrak{q'}_2 = 761\mathbb{Z}_K + (153 + \rho_1)\mathbb{Z}_K, \mathfrak{q'}_3 = 1901\mathbb{Z}_K + (484 + \rho_1)\mathbb{Z}_K$.

Les points $P_1, P_2, P_3$ sont dans $H$ et on montre que leurs classes forment une base de $H/2E_{-8}(\mathbb{Q})$. On déduit que $rg_2(H/2E_{-8}(\mathbb{Q})) = 3$. Comme $r_2$ est pair, d'après la proposition 6.3, il en résulte que $r_2 \geq 2$. D'après le programme pari, on obtient $r_2 = 2$.

II. Considérons la courbe elliptique $E_{10}$ donnée par l'équation :

$$y^2 = x^3 - 100x^2 + 827x + 1.$$

Les points $G = (0, 1), G_1 = (1, 27), G_2 = (8, 27)$ forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Les décompositions des idéaux principaux $(1 - \rho_1), (8 - \rho_1)$ sont les suivantes:

$$(1 - \rho_1) = (\mathfrak{b}_1^{\sigma})^2 (\mathfrak{b}_1^{\sigma^2})^4,$$

où $\mathfrak{b}_1 = 3\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$,

$$(8 - \rho_1) = \mathfrak{b}_1^6.$$

Les points $G, G_1, G_2$ sont dans $H$ et on montre que leurs classes forment une base de $H/2E_{10}(\mathbb{Q})$. On déduit que $\mathrm{rg}_2(H/2E_{10}(\mathbb{Q})) = 3$. Comme précédemment, on trouve que $r_2 \geq 2$ et $r_2$ calculé par pari est égal à 2.

III. Considérons la courbe elliptique $E_{50}$ donnée par l'équation :

$$y^2 = x^3 - 2500x^2 + 120147x + 1.$$

Les points $D = (0,1), D_1 = (1,343), D_2 = (48,343), D_3 = (5265, 277991)$ forment une base d'un sous-groupe d'indice fini du groupe de Mordell-Weil. Les idéaux $(1 - \rho_1)$, $(5265 - \rho_1)$, $(48 - \rho_1)$ ont pour décompositions:

$$(1 - \rho_1) = (\mathfrak{h}_1^{\sigma})^2(\mathfrak{h}_2^{\sigma^2})^4,$$

avec $\mathfrak{h}_1 = 7\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K$,

$$(5265 - \rho_1) = \mathfrak{h}_1^{\sigma}\mathfrak{h}_2^{\sigma^2}\mathfrak{h}'^2_1\mathfrak{h}'^2_2,$$

avec $\mathfrak{h}'_1 = 151\mathbb{Z}_K + (20 + \rho_1)\mathbb{Z}_K$, $\mathfrak{h}'_2 = 263\mathbb{Z}_K + (-5 + \rho_1)\mathbb{Z}_K$,

$$(48 - \rho_1) = \mathfrak{h}_1^6.$$

Les points $D, D_1, D_2$ sont des points de $H$ et on montre que leurs classes forment une base de $H/2E_{50}(\mathbb{Q})$. On déduit alors que $\mathrm{rg}_2(H/2E_{50}(\mathbb{Q})) = 3$.

IV. Considérons la courbe elliptique $E_{626}$ donnée par l'équation:

$$y^2 = x^3 - 391876x^2 + 244532499x + 1.$$

Les points

$$(0,1), (1,15625), (624,15625), (349,194045), (133,159979)$$

$$(63153799/49, 418730031875/343), (177607161/64, 2193522042995/512),$$

forment une base d'un sous-groupe d'indice fini de $E_{626}(\mathbb{Q})$. Les décompositions en idéaux premiers des idéaux principaux

$$(1 - \rho_1), (391251 - \rho_1), (349 - \rho_1), (133 - \rho_1), (236656201/576 - \rho_1)$$

sont les suivantes:

$$(1 - \rho_1) = (\mathfrak{g}_1^{\sigma})^8(\mathfrak{g}_1^{\sigma^2})^4,$$

$$(391251 - \rho_1) = (\mathfrak{g}_1^{\sigma})^4(\mathfrak{g}_1^{\sigma^2})^8,$$

$$(349 - \rho_1) = \mathfrak{g}_1^2\mathfrak{g}_4^4,$$

où $\mathfrak{g}_1 = 5\mathbb{Z}_K + (\rho_1 + 1)\mathbb{Z}_K, \mathfrak{g}_4 = 197\mathbb{Z}_K + (\rho_1 + 45)\mathbb{Z}_K$,

$$(133 - \rho_1) = \mathfrak{g}_5^2,$$

où $\mathfrak{g}_5 = 159979\mathbb{Z}_K + (\rho_1 + 159846)\mathbb{Z}_K$,

$$(177607161/64 - \rho_1) = \mathfrak{g}_1^2\mathfrak{g}_6^{-6}\mathfrak{g}_7^2,$$

$\mathfrak{g}_6 = 2\mathbb{Z}_K, \mathfrak{g}_7 = 438704408599\mathbb{Z}_K + (\rho_1 - 116533633646)\mathbb{Z}_K,$

$$(63153799/49 - \rho_1) = (\mathfrak{g}_1^{\sigma})^4(\mathfrak{g}_1^{\sigma^2})^4\mathfrak{g}_8^{-2}\mathfrak{g}_9^2,$$

avec $\mathfrak{g}_8 = 7\mathbb{Z}_K, \mathfrak{g}_9 = 669968051\mathbb{Z}_K + (\rho_1 + 149112138)\mathbb{Z}_K$. Donc les 7 points sont dans $H$, et on montre que leurs classes forment une base de $H/2E_{626}(\mathbb{Q})$. On déduit alors que $rg_2(H/2E_{626}(\mathbb{Q})) = 7$. Il en résulte alors que $r_2 \geq 6$. Comme dans les exemples 4.8, 5.4, $r_2$ calculé par pari est 6.

Tableau 7.1.

| $n$ | $r$ | $r_2$ | $rg_2(H_1/2E_n(\mathbb{Q}))$ | $s$ |
|---|---|---|---|---|
| $-92$ | $1 \leq \leq 2$ | 0 | 1 | 3 |
| $-88$ | 2 | 0 | 1 | 2 |
| $-70$ | 2 | 0 | 1 | 2 |
| $-68$ | 2 | 2 | $\leq 3$ | 5 |
| $-58$ | 3 | 2 | 3 | 4 |
| $-56$ | $1 \leq \leq 3$ | 2 | $\leq 3$ | 4 |
| $-52$ | $1 \leq \leq 3$ | 2 | $\leq 3$ | 4 |
| $-50$ | 2 | 2 | 2 | 5 |
| $-46$ | 2 | 0 | 1 | 2 |
| $-38$ | $1 \leq \leq 3$ | 2 | $\leq 3$ | 5 |
| $-34$ | 2 | 0 | 1 | 3 |
| $-32$ | 3 | 2 | 2 | 5 |
| $-22$ | 4 | 2 | 3 | 4 |
| $-20$ | 2 | 2 | 2 | 5 |
| $-16$ | 2 | 0 | 1 | 2 |
| $-14$ | 3 | 2 | 2 | 5 |
| $-8$ | 3 | 2 | 3 | 4 |
| 8 | $2 \leq \leq 4$ | 2 | 2 | 4 |
| 10 | 3 | 2 | 3 | 4 |
| 22 | 2 | 0 | 1 | 3 |
| 26 | 3 | 2 | 2 | 4 |
| 44 | 3 | 2 | 3 | 4 |
| 50 | 4 | 2 | 3 | 4 |
| 52 | 2 | 2 | 2 | 5 |
| 80 | 2 | 0 | 1 | 2 |
| 88 | $1 \leq \leq 3$ | 2 | $\leq 3$ | 5 |
| 92 | 2 | 0 | 1 | 3 |
| 94 | 2 | 0 | 1 | 3 |
| 98 | $2 \leq \leq 4$ | 0 | 1 | 2 |
| 100 | $1 \leq \leq 3$ | 2 | $\leq 3$ | 5 |

REMARQUE 7.3. Quand $\mathrm{rg}_2(H/2E_n(\mathbb{Q}))$ est égal au rang de la courbe elliptique $E_n$, alors on obtient dans ce cas une minoration de $r_2$; comme on l'a vu dans les exemples 4.8 et 5.4.

On résume dans le tableau 7.1 suivant les résultats obtenus par ces méthodes pour $-100 \leq n \leq 100$; $s$ désigne la borne supérieure donnée dans la proposition 5.3.

REMARQUE 7.4. • Pour $n = -68$, d'après le programme mwrank de Cremona le rang $r$ de la courbe est égal à 2, donc $rg_2(H_1/2E_n(\mathbb{Q})) \leq 2$. Ce qui donne une meilleure borne que la proposition 5.3.

• Pour $n = 98$, le programme mwrank de Cremona donne seulement un encadrement de $r$: $2 \leq r \leq 4$, et d'après la proposition 5.3, $r \leq 1 + n_p + r_2$ donc $r = 2$.

## REFERENCES


[1] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 355-380.

[2] G. Billing, *Beiträge zur arithmetischen Theorie der ebenen Kubischen Kurven vom Geschlecht eins*, Nova Acta Regiae Soc. Sci. Upsaliensis **4** 11 (1938), No.1, Diss. 165.

[3] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris, 1988-89, 27-41.

[4] G. Campbell, *Finding Elliptic Curves and Families of Elliptic Curves over* $\mathbb{Q}$ *of Large Rank*, Dissertation, Rutgers, 1999.

[5] H. Cohen, F. Diaz y Diaz and M. Olivier, *Subexponential algorithms for class group and unit computations*, J. Symbolic Comput. **24** (1997), 433-441.

[6] J. Cremona, mwrank. `http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/` (2002).

[7] A. Dujella, *High rank elliptic curves with prescribed torsion*, `http://www.math.hr/~duje/tors/tors.html`

[8] A. Dujella, *An example of elliptic curve over* $\mathbb{Q}$ *with rank equal to* 15, Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), 109-111.

[9] J. L. Hafner, K. S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2** (1989), 837-850.

[10] M. Kawachi and S. Nakano, *The 2-class groups of cubic fields and* 2*-descents on elliptic curves*, Tohoku Math. J. (2) **44** (1992), 557-565.

[11] A. Laoudi and O. Lecacheux, *Surfaces elliptiques modulaires associés au groupe* $\Gamma_0(9) \cap \Gamma_1(3)$, preprint.

[12] O. Lecacheux, *Units in number fields and elliptic curves*. Advances in number theory. (Kingston, ON, 1991). Oxford Univ. Press, New York, 1993, 293-301.

[13] O. Lecacheux, *Rang de courbes elliptiques avec groupe de torsion non trivial*, J. Théor. Nombres Bordeaux **15** (2003), 231-247.

[14] J. F. Mestre, *Construction d'une courbe elliptique de rang* $\geq 12$, C. R. Acad. Sci. Paris Ser. I **295** (1982), 643-644.

[15] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* $\geq 20$, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), 291-293.

[16] PARI/GP, version 2.1.5, Bordeaux, 2004, `http://pari.math.u-bordeaux.fr/`.

[17] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag New York, 1986.

[18] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002), 7-17.
[19] K. Uchida, *Class numbers of cubic cyclic fields*, J. Math. Soc. Japan **26** (1974), 447-453.
[20] L. C. Washington, *A family of cubic fields and zeros of* 3*-adic L-functions*, J. Number Theory **63** (1997), 408-417.
[21] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), 371-384.
[22] L. C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

A. Laoudi
Équipe de Théorie des Nombres
Institut de Mathématiques de Jussieu
Université Paris 6
175 rue du Chevaleret, 75013 Paris
France,
et
Université des Sciences et de la Technologie Houari Boumediène
Faculté de Mathématiques
B.P. 32, El Allia, Bab Ezzouar-16111-Alger
Algérie
*E-mail*: laoudi@math.jussieu.fr & laoudia@yahoo.fr

*Received*: 13.7.2005.
*Revised*: 17.11.2005.