Courbes elliptiques et groupes de classes d'idéaux de certaines corps quadratiques.

MESTRE, Jean-François

in: Journal für die reine und angewandte Mathematik - 343 | Periodical
13 page(s) (23 - 35)

Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques

Par *Jean-François Mestre* à Talence

En 1922, Nagell ([6]) a montré que, si n est un entier naturel, il existe une infinité de corps quadratiques imaginaires dont le nombre de classes d'idéaux est divisible par n. Il a fallu attendre 1970 pour que ce résultat soit étendu aux corps quadratiques réels, par Yamamoto ([12]), qui prouve également que, pour tout n, il existe une infinité de corps quadratiques imaginaires dont le groupe des classes d'idéaux contient un sous-groupe de type (n, n). En particulier, pour tout nombre premier p, il existe une infinité de corps quadratiques imaginaires (resp. réels) dont le p-rang du groupe des classes d'idéaux est supérieur ou égal à 2 (resp. 1).

Si $p=2$, on sait que le p-rang d'un corps quadratique de discriminant D est égal à $t-1$ ou $t-2$, t étant le nombre de facteurs premiers de D. Par suite, il existe une infinité de corps quadratiques réels (resp. imaginaires) dont le 2-rang du groupe des classes d'idéaux est égal à un entier donné. D'autre part, si D est le discriminant d'un corps quadratique, on voit donc que le 2-rang du groupe des classes d'idéaux de ce corps est majoré par $\log D/\log\log D$.

En revanche, si p est un nombre premier impair, on ignore tout sur la croissance du p-rang du groupe des classes d'un corps quadratique, réel ou imaginaire, lorsque la valeur absolue de son discriminant croît.

Depuis une dizaine d'années, néanmoins, quelques résultats ont été obtenus dans le cas où $p=3$: Craig ([2]) a montré qu'il existe une infinité de corps quadratiques imaginaires dont le 3-rang du groupe des classes d'idéaux est supérieur ou égal à 4, résultat étendu aux corps quadratiques réels par Diaz y Diaz ([4]), qui a également découvert de nombreux exemples explicites de tels corps ([5]), ainsi que Shanks et Serafin ([9]). D'autre part, Buell ([1]) trouve dans les tables qu'il a réalisées des exemples de corps quadratiques imaginaires dont le p-rang est égal à 2 pour $p=5$, 7, 11, 13, 17 et 19. (Voir aussi [8] et [10].)

Le but de cet article est de montrer comment trouver, à l'aide de la théorie des courbes elliptiques, une infinité de corps quadratiques imaginaires (resp. réels) dont le p-rang du groupe des classes d'idéaux est supérieur ou égal à 2, pour $p=5$ et 7. Cette méthode permet également de trouver de nombreux exemples de corps quadratiques imaginaires dont le 5-rang du groupe des classes d'idéaux est égal à 3.

A des changements mineurs près, ce texte est extrait du séminaire de Théorie des Nombres de Bordeaux, 1970—1980. Je remercie les organisateurs de ce séminaire de m'avoir autorisé à le reproduire.

I. Exposé de la méthode

Soit A une variété abélienne définie sur $\mathbb{Q}$, possédant un point P défini sur $\mathbb{Q}$ d'ordre p, p premier impair. Si A' est la variété abélienne quotient de A par le groupe d'ordre p engendré par P, on a une isogénie définie sur $\mathbb{Q}$:

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow A \xrightarrow{\varphi} A' \longrightarrow 0.$$

Si $A/_{\mathbb{Z}}$ désigne le modèle de Néron de A sur $\mathbb{Z}$, on en déduit, par exemple d'après Oort-Tate ([7]) une immersion, sur Spec $\mathbb{Z}$, du schéma en groupes constant $\mathbb{Z}/p\mathbb{Z}$ dans $A/_{\mathbb{Z}}$, et il existe un schéma en groupes $A'/_{\mathbb{Z}}$, de fibre générique A', tel qu'on a une isogénie:

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow A/_{\mathbb{Z}} \xrightarrow{\varphi} A'/_{\mathbb{Z}} \longrightarrow 0.$$

Notons que $A'/_{\mathbb{Z}}$ n'est pas en général le modèle de Néron de A' sur $\mathbb{Z}$, ni même, si A n'a pas une réduction semi-stable en p, un sous-schéma ouvert de ce modèle de Néron.

Considérant à présent la suite exacte précédente comme une suite exacte de faisceaux pour la topologie *fppf*, on en déduit que, si K est un corps de nombres et O_K son anneau d'entiers, on a la suite exacte de cohomologie suivante:

$$0 \longrightarrow A'(O_K)/\varphi A(O_K) \longrightarrow H^1(\mathrm{Spec}\, O_K, \mathbb{Z}/p\mathbb{Z}).$$

Or, si Cl_K désigne le groupe de classes d'idéaux de K, on sait que

$$H^1(\mathrm{Spec}(O_K), \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(Cl_K, \mathbb{Z}/p\mathbb{Z}).$$

D'où la suite:

$$0 \longrightarrow A'(O_K)/\varphi A(O_K) \longrightarrow \mathrm{Hom}(Cl_K, \mathbb{Z}/p\mathbb{Z})$$

et donc une minoration du p-rang de Cl_K par le rang de $A'(O_K)/\varphi A(O_K)$.

II. Cas des courbes elliptiques

II. 1. Obtention de corps quadratiques dont le nombre de classes est divisible par 5

Les courbes elliptiques E munies d'un point d'ordre p sont classifiées par la courbe modulaire $X_1(p)$ ([3]). On sait que pour $p>7$ il n'existe pas de courbe elliptique définie sur $\mathbb{Q}$ munie d'un point d'ordre p rationnel sur $\mathbb{Q}$. Par contre, $X_1(5)$ et $X_1(7)$ sont de genre 0, et il existe donc une infinité de courbes elliptiques définies sur $\mathbb{Q}$ munies d'un point d'ordre 5 (resp. 7) rationnel sur $\mathbb{Q}$.

Plus précisément, soit (u, v), u et v entiers premiers entre eux, un point de $\mathbb{P}^1(\mathbb{Q}) = X_1(5)(\mathbb{Q})$. Soit $E(u, v)$ la cubique d'équation:

$$y^2 + uxy + v^2(u-v)y = x^3 + v(u-v)x^2 \tag{1}$$

et de discriminant $\Delta(E(u, v)) = -v^5(u-v)^5(u^2+9uv-11v^2)$.

Nous supposons désormais $v(u-v)\neq 0$; $E(u, v)$ est donc une courbe elliptique. Le point $P(0, 0)$ est d'ordre 5 sur $E(u, v)$. On calcule une équation de la courbe quotient par les formules de Vélu ([11]), dont j'utilise ici les notations:

$$b_2(u, v)=u^2+4uv-4v^2,\ b_4(u, v)=v^2u(u-v),\ b_6(u, v)=v^4(u-v),$$

$$t_P=v^2u(u-v), \qquad u_P=v^4(u-v)^2$$

$$t_{2P}=-v(u-v)^2\,(u-2v), \qquad u_{2P}=v^2(u-v)^4,$$

$$t=-v(u-v)^2\,(2u^2-5uv+4v^2), \qquad w=v^2(u-v)^2\,(2u^2-5uv+4v^2).$$

La courbe quotient $F(u, v)$ a alors comme équation:

$$(2)\quad y^2+uxy+v^2(u-v)y=x^3+v(u-v)x^2+5v(u-v)\,(u^2-4uv+2v^2)x$$
$$+v(u-v)\,(u^4-14u^3v+31u^2v^2-39uv^3+20v^4).$$

Son discriminant $\Delta(F(u, v))$ est égal à $v(v-u)\,(u^2+9uv-11v^2)^5$. Si l'on note par des majuscules $B_2, \ldots$ les coefficients $b_2, \ldots$ de $F(u, v)$, on a les formules:

$$B_2(u, v)=u^2+4uv-4v^2,$$
$$B_4(u, v)=v(u-v)\,(10u^2-39uv+20v^2),$$
$$B_6(u, v)=v(u-v)\,(4u^4-56u^3v+124u^2v^2-155uv^3+79v^4),$$
$$C_4(u, v)=u^4-232u^3v+1184u^2v^2-1448uv^3+496v^4,$$
$$C_6(u, v)=-u^6-516u^5v+12600u^4v^2-45220u^3v^3+75240u^2v^4-62112uv^5+20008v^6.$$

D'autre part, l'isogénie entre $E(u, v)$ et $F(u, v)$ est donnée par:

$$\begin{cases} X=x+t_P/x+u_P/x^2+t_{2P}/(x+uv-v^2)+u_{2P}/(x+uv-v^2)^2, \\ Y=y-u_P(2y+ux+v^2(u-v))/x^3-t_P(ux+y)/x^2-v^4u(u-v)^2/x^2 \\ \qquad -u_{2P}(2y+ux+v^2(u-v))/(x+uv-v^2)^3-t_{2P}(ux+y)/(x+uv-v^2)^2 \\ \qquad +v^2(u-v)^3\,(u^2-2uv-v^2)/(x+uv-v^2)^2. \end{cases}$$

Cette isogénie se prolonge en une isogénie du modèle de Néron $E(u, v)/_{\mathbb{Z}}$ de $E(u, v)$ sur un certain schéma en groupes $F'(u, v)/_{\mathbb{Z}}$ de fibre générique $F(u, v)$, isogénie dont le noyau est le schéma en groupes constant $\mathbb{Z}/5\mathbb{Z}$. Si K est un corps de nombres, les points de $F'(u, v)\,(O_K)$ correspondent aux points de $F(u, v)\,(K)$ vérifiant certaines congruences.

Exemple. $u=0$, $v=1$. On trouve alors $E(0, 1)=X_1(11)$, $F(0, 1)=X_0(11)$, les deux courbes modulaires classifiant respectivement les courbes elliptiques munies d'un point d'ordre 11 et les courbes elliptiques munies d'une isogénie de degré 11. Ici $F'(0, 1)/_{\mathbb{Z}}$ est le sous-schéma en groupes ouvert du modèle de Néron sur $\mathbb{Z}$ de $X_0(11)$ complémentaire des quatre composantes connexes de la fibre en 11 de ce modèle de Néron autres que la composante neutre.

Dans le cas général, il est facile d'établir la proposition suivante:

Proposition II. 1. 1. *Soient u et v deux entiers premiers entre eux. L'équation* (1) *est un modèle minimal de Weierstrass de $E(u, v)$ pour tout nombre premier l, y compris pour $l=5$. L'équation* (2) *est un modèle minimal de Weierstrass de $F(u, v)$ pour tout nombre premier $l \neq 5$.*

Soit l un nombre premier. Si l ne divise pas $v(u-v)(u^2+9uv-11v^2)$, la réduction en l de $E(u, v)$ et $F(u, v)$ est bonne. Si l est différent de 5 et divise $v(u-v)(u^2+9uv-11v^2)$, la réduction en l est multiplicative. Si $l=5$, et si l divise $v(u-v)$, (2) *est un modèle minimal de Weierstrass en $l=5$, et $E(u, v)$ et $F(u, v)$ ont une réduction multiplicative en* 5. *Si $l=5$, et si $u \equiv 3v$ modulo* 5, *deux cas se présentent:*

$u \not\equiv 8v$ modulo 25: *$E(u, v)$ est de type de Kodaira II (réduction additive), et l'équation* (2) *est un modèle minimal de Weierstrass de $F(u, v)$ en* 5.

$u \equiv 8v$ modulo 25: *$E(u, v)$ est de type III, et* (2) *n'est pas un modèle minimal de Weierstrass de $F(u, v)$ en* 5.

Soit K un corps de nombres. La proposition suivante énonce des conditions suffisantes pour qu'un point de $F(u, v)(K)$ se prolonge en un point de $F'(u, v)(O_K)$:

Proposition II. 1. 2. *Soit K un corps de nombres et soit $P(x, y)$ un point de $F(u, v)(K)$. Supposons que, pour toute place w de K divisant $u^2+9uv-11v^2$, x ne soit pas congru à $5u-6v$ modulo w. Alors P se prolonge en un point de $F'(u, v)(O_K)$.*

Nous avons donc à présent un critère simple permettant d'assurer qu'un point de $F(u, v)(K)$ provient de $F'(u, v)(O_K)$, pour K un corps de nombres. Il reste à trouver des critères permettant d'affirmer qu'un tel point n'est pas l'image d'un point de $E(u, v)(O_K)$ par φ. A toute place w de K où $E(u, v)$ a bonne réduction est associé un tel critère, consistant en une série de congruences.

Exemple. Supposons u pair, v impair. Il est alors clair que $E(u, v)$ et $F(u, v)$ ont bonne réduction en 2. Supposons qu'une place w de K au-dessus de 2 soit de degré absolu 1 ou 2 (ce qui est toujours le cas si K est quadratique). Alors, comme

$$E(u, v)(\mathbb{F}_2) = E(u, v)(\mathbb{F}_4) = F(u, v)(\mathbb{F}_2) = F(u, v)(\mathbb{F}_4) = \mathbb{Z}/5\mathbb{Z},$$

on en déduit immédiatement qu'un point $P(x, y)$ de $F(u, v)(K)$ d'abscisse x entière en w ne provient pas d'un point de $E(u, v)(K)$.

Sous certaines conditions de congruences, la donnée d'un x rationnel permet donc d'obtenir un corps quadratique $\mathbb{Q}(y)$ de nombre de classes divisible par 5. L'exemple précédent permet par exemple d'établir la proposition suivante:

Proposition II. 1. 3. *Soit le polynôme*

$$D(x, u, v) = 4x^3 + B_2(u, v)x^2 + 2B_4(u, v)x + B_6(u, v).$$

Soient u un entier pair et v entier impair. Soit d'autre part x un rationnel vérifiant les conditions de congruence suivantes:

i) *pour tout premier l divisant $u^2+9uv-11v^2$, x n'est pas congru à $5u-6v$ modulo l*;

ii) *x est entier en 2.*

Alors le corps $K=\mathbb{Q}(\sqrt{D(x,u,v)})$ a un nombre de classes divisible par 5. De plus, les racines du polynôme

$$X^5+(2uv-2v^2-x)X^4+v(u-v)(-u^2+5uv-3v^2-2x)X^3+v^2(u-v)^2(3uv-x)X^2$$
$$+v^4(u-v)^3(u+2v)X+v^6(u-v)^4$$

engendrent une extension abélienne non ramifiée de degré 5 de K. Le discriminant du polynôme ci-dessus est $(u-v)^{14}D(x,u,v)$.

Evidemment, la condition, u pair sert uniquement à assurer la bonne réduction en 2. Pour u, v entiers quelconques, il suffit de chercher un nombre premier où $E(u,v)$ a bonne réduction, et de calculer les conditions de congruence correspondantes.

D'autre part, l'extension abélienne non ramifiée de K décrite dans la proposition est obtenue en prenant l'image réciproque par φ du point $P(x,y)$ de $F(u,v)(K)$: on trouve ainsi le corps où le torseur image de P dans $H^1_{fppf}(\mathrm{Spec}(O_K), \mathbb{Z}/5\mathbb{Z})$ se trivialise.

Exemple. Reprenons l'exemple $u=0$, $v=1$. Alors $D(x,0,1)=4x^3-4x^2-40x-79$, et le polynôme dont les racines engendrent l'extension non ramifiée correspondante est $X^5-(2+x)X^4+(3+2x)X^3-xX^2-2X+1$. Pour tout rationnel x non congru à 5 modulo 11 et entier en 2, le corps $K=\mathbb{Q}(\sqrt{4x^3-4x^2-40x-79})$ a un nombre de classes divisible par 5, et l'extension $K(\alpha)$, α racine du polynôme de degré 5 ci-dessus, est une extension abélienne non ramifiée de K.

Nous donnons ici quelques exemples pour illustrer ce qui précède:

x	0	1	2	3	4	6	7	8	9	10
$D(x,0,1)$	−79	−119	−143	−127	−47	401	817	1393	2153	3121
$h(K)$	5	10	10	5	5	5	5	5	5	5

où $h(K)$ désigne le nombre de classes du corps $K=\mathbb{Q}(\sqrt{D(x,0,1)})$.

II. 2. Obtention de corps quadratiques dont le 5-rang du groupe de classes d'idéaux est supérieur ou égal à 2

II. 2. 1. La méthode employée

Soit E une courbe elliptique définie sur $\mathbb{Q}$, écrite sous la forme

$$\eta^2=x^3+b_2x^2/4+b_4x/2+b_6/4.$$

A tout rationnel x correspond un corps au plus quadratique sur lequel $P(x,\eta)$ est défini. Si l'on trace une droite horizontale passant par P, elle coupe la courbe en deux autres points $P_2(x_2,\eta)$ et $P_3(x_3,\eta)$.

Le lemme suivant donne une condition nécessaire et suffisante sur les coefficients de la courbe E pour qu'il existe x rationnel tel que x_2 et x_3 soient encore rationnels:

Lemme II. 2. 1. 1. *Soit E une courbe elliptique définie sur $\mathbb{Q}$, d'équation*

$$\eta^2 = x^3 + (b_2/4)\, x^2 + (b_4/2)\, x + b_6/4 = f(x).$$

Les deux conditions suivantes sont équivalentes:

i) *on peut trouver x_1, x_2, x_3 non tous égaux et rationnels tel que*

$$f(x_1) = f(x_2) = f(x_3);$$

ii) *$c_4 = b_2^2 - 24 b_4$ est une norme non nulle l'extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ (ou, ce qui revient au même, c_4 peut s'écrire $\rho^2 + 3\zeta^2$, ρ et ζ rationnels non tous les deux nuls).*

Par ailleurs si i) *ou* ii) *est réalisée, l'ensemble des solutions rationnelles de* i) *est dense dans l'ensemble des solutions réelles de* i).

En effet, l'équation $(f(x_1) - f(x_2))/(x_1 - x_2) = 0$ est l'équation d'une conique, et un rapide calcul montre qu'elle est birationnellement équivalente à la conique $X^2 + 3Y^2 = c_4$.

Supposons la condition ii) réalisée; on peut préciser le lemme ci-dessus en indiquant dans quels cas on peut trouver (x_1, x_2, x_3) tel que $f(x_1) = f(x_2) = f(x_3)$ est positif:

Lemme II. 2. 1. 2. *Soit E la courbe elliptique du lemme* II. 2. 1. 1, *et supposons la condition* ii) *de ce lemme réalisée. Les deux conditions suivantes sont équivalentes*:

i) *il existe un triplet (x_1, x_2, x_3) de $\mathbb{Q}^3$ tel que $f(x_1) = f(x_2) = f(x_3)$ et $f(x_1)$ positif*;

ii) *le discriminant Δ de E est positif, ou bien il est négatif ainsi que c_6.*

De plus, si ii) *est réalisée, il existe une infinité de triplets vérifiant* i).

En effet, remarquons que $f(x) = X^3 - (c_4/48)\, X - c_6/864$, où l'on a posé

$$X = x + b_2/12.$$

Il est alors clair que $\Delta > 0$ si et seulement si f a trois racines réelles, que c_4 est négatif si et seulement si f est monotone, et que, si Δ est négatif et c_4 positif, f est alors du signe contraire à c_6 sur l'intervalle où f' est négatif. Par suite, dans le lemme ci-dessus, ii) est équivalent à i) si $\mathbb{Q}^3$ est remplacé par $\mathbb{R}^3$, et donc à i) par la dernière assertion du lemme II. 2. 1. 1.

II. 2. 2. Application aux courbes paramétrées par $X_1(5)$ $(\mathbb{Q})$

On applique ce qui précède aux courbes $F(u, v)$: on choisit donc (u, v) tels que $C_4(u, v)$ soit une norme de $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$. On peut alors paramétrer les triplets tels que la condition i) du lemme II. 2. 1. 1 est réalisée par des formules du type $x_i = a_i(t)/b_i(t)$, a_i et b_i polynômes du second degré, $i = 1, 2, 3$.

Moyennant de bonnes congruences sur t modulo les nombres premiers divisant $u^2 + 9uv - 11v^2$, on est assuré que $P_i(x_i, \eta)$ se prolonge en un point de

$$F'(u, v)\,(O_K),\ i = 1, 2, 3 \quad \text{et} \quad K = \mathbb{Q}(\eta), \quad \text{avec} \quad \eta^2 = f(x_i).$$

Les trois points P_i étant alignés, ils ne sont pas indépendants. On peut néanmoins trouver des conditions nécessaires pour que deux d'entre eux le soient, modulo $\varphi(E(u, v)(K))$; par exemple, supposons que 3 soit de degré 1 dans K, et que $E(u, v)$ ait bonne réduction modulo 2 et 3. Alors, si t est tel que $P_1 \equiv P_2$ modulo 2 et $P_1 \not\equiv P_2$ modulo 3, il est facile de voir que P_1 et P_2 sont non seulement indépendants dans le groupe de Mordell-Weil de $F(u, v)$ sur K, mais même dans ce groupe modulo

$$\varphi(E(u, v)(K)).$$

Exemple. Reprenons l'exemple $u=0$, $v=1$. Alors l'équation

$$(f(x_1)-f(x_2))/(x_1-x_2)=0 \quad \text{s'écrit} \quad x_1^2+x_1x_2+x_2^2-x_1-x_2-10=0,$$

conique qu'on peut paramétrer par:

$$\begin{cases} x_1=(4t^2-2t-10)/(t^2+3), \\ x_2=-(t^2-12t-5)/(t^2+3). \end{cases}$$

La condition $(t-2)(t-6)(t-7) \not\equiv 0$ modulo 11 assure que les points P_1 et P_2 proviennent de points de $F'(u, v)(O_K)$.

D'autre part, $t \equiv 0$ modulo 2 implique $P_1 \not\equiv P_2$ modulo 2, et $t \equiv 1$ modulo 3 implique $P_1 \equiv P_2$ modulo 3. On en déduit donc la proposition suivante:

Proposition II. 2. 2. *Soit $m(t)$ le polynôme*

$$m(t)=(t^2+3)(-47t^6-240t^5-2887t^4+2400t^3+3659t^2-2160t-3733).$$

Soit t vérifiant les deux conditions suivantes:

i) $t \not\equiv 2, 6, 7$ *modulo* 11;

ii) $t \equiv 0$ *modulo* 2 *et* $t \equiv 1$ *modulo* 3.

Alors le corps $K=\mathbb{Q}(\sqrt{m(t)})$ a un groupe de classes d'idéaux dont le 5-rang est supérieur ou égal à 2. On peut d'autre part trouver explicitement deux polynômes dont les racines engendrent deux extensions abéliennes non ramifiées de degré 5 de K, extensions indépendantes lorsqu'on les pense comme éléments de $\mathrm{Hom}(Cl_K, \mathbb{Z}/5\mathbb{Z})$.

Les conditions ii) peuvent évidemment être remplacées par d'autres conditions modulo n'importe quel couple de nombres premiers où $E(0, 1)$ a bonne réduction.

A priori, le polynôme $m(t)$ permet d'obtenir des corps quadratiques dont le 5-rang du groupe de classes d'idéaux est supérieur ou égal à 2. Schoof a remarqué qu'environ une valeur de t sur 5 donne un corps quadratique dont le 5-rang est supérieur ou égal à 3, constatation malheureusement seulement expérimentale. Diaz y Diaz est le premier à s'être aperçu que la valeur $t=8$ (qui est exclue de la proposition ci-dessus) donne le corps quadratique $K=\mathbb{Q}(\sqrt{-3150719})$ dont le 5-rang du groupe des classes d'idéaux est égal à 3. Depuis, Schoof a trouvé, toujours à l'aide du polynôme ci-dessus, le corps $K=\mathbb{Q}(\sqrt{-258559351511807})$, dont le 5-rang du groupe de classes d'idéaux est égal à 4. C'est, à ma connaissance, le seul exemple que l'on ait d'un tel corps.

Le polynôme $m(t)$ est toujours négatif, et ne permet donc d'obtenir que des corps quadratiques imaginaires. D'après le lemme II. 2. 1. 2, pour obtenir des corps quadratiques réels dont le 5-rang du groupe des classes d'idéaux est supérieur ou égal à 2, il nous faut trouver des couples (u, v) tels que $C_4(u, v)$ soit une norme de $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$, et tels que $\Delta(u, v)$ soit positif, ou bien négatif avec $C_6(u, v)$ négatif. Il existe une infinité de tels couples: par exemple, $u=-12$, $v=1$ convient. On trouve alors

$$C_4 = 2^4 5^4 61 \quad \text{et} \quad C_6 = 2^3 5^5 19057.$$

Par suite:

Théorème II. 2. 2. *Il existe une infinité de corps quadratiques réels dont le 5-rang du groupe des classes d'idéaux est supérieur ou égal à 2.*

II. 3. Le cas $p=7$

La courbe modulaire $X_1(7)$ est de genre 0, comme $X_1(5)$. Les calculs sont donc semblables aux précédents: soit (u, v) un couple d'entiers premiers entre eux, correspondant à un point de $\mathbb{P}^1(\mathbb{Q}) = X_1(7)(\mathbb{Q})$. On lui associe la courbe $G(u, v)$ d'équation (3):

$$(3) \qquad y^2 + (-u^2 + uv + v^2)\, xy - v^3 u^2 (u-v)\, y = x^3 - u^2 v(u-v)\, x^2$$

de discriminant $\Delta(G(u, v)) = u^7 v^7 (u-v)^7 (u^3 - 8u^2 v + 5uv^2 + v^3)$.

Supposons désormais $uv(u-v) \neq 0$; $G(u, v)$ est alors une courbe elliptique, et le point $P(0, 0)$ est d'ordre 7. Soit $H(u, v)$ la courbe quotient de $G(u, v)$ par le groupe engendré par P, d'équation (4):

$$\begin{aligned}(4) \qquad & y^2 + (-u^2 + uv + v^2)\, xy - v^3 u^2 (u-v)\, y \\ & = x^3 - u^2 v(u-v)\, x^2 - 5uv(u-v)\, (u^5 + u^4 v - 6u^3 v^2 + 8u^2 v^3 - 6uv^4 + v^5)\, x \\ & - uv(u-v)\, (u^9 + 9u^8 v - 37u^7 v^2 + 70u^6 v^3 - 132u^5 v^4 + 211u^4 v^5 - 182u^3 v^6 + 76u^2 v^7 - 18uv^8 + v^9)\end{aligned}$$

de discriminant $\Delta(H(u, v)) = uv(u-v)\, (u^3 - 8u^2 v + 5uv^2 + v^3)^7$.

On a les formules:

$$\begin{aligned}
B_2(u, v) &= u^4 - 6u^3 v + 3u^2 v^2 + 2uv^3 + v^4, \\
B_4(u, v) &= uv(u-v)\, (-10u^5 - 10u^4 v + 61u^3 v^2 - 81u^2 v^3 + 59uv^4 - 10v^5), \\
B_6(u, v) &= uv(u-v)\, (-4u^9 - 36u^8 v + 148u^7 v^2 - 280u^6 v^3 + 528u^5 v^4 - 843u^4 v^5 + 727u^3 v^6 \\
&\qquad - 304u^2 v^7 + 72uv^8 - 4v^9), \\
C_4(u, v) &= u^8 + 228u^7 v + 42u^6 v^2 - 1736u^5 v^3 + 3395u^4 v^4 - 3360u^3 v^5 + 1666u^2 v^6 - 236uv^7 + v^8, \\
C_6(u, v) &= -u^{12} + 522u^{11} v + 8955u^{10} v^2 - 37950u^9 v^3 + 70998u^8 v^4 - 131562u^7 v^5 \\
&\qquad + 253239u^6 v^6 - 316290u^5 v^7 + 218058u^4 v^8 - 80090u^3 v^9 + 14631u^2 v^{10} - 510uv^{11} - v^{12}
\end{aligned}$$

De même que pour le cas $p=5$, on a la proposition suivante:

Proposition II. 3. 1. *Soit* (u, v) *un couple d'entiers premiers entre eux. Alors* $G(u, v)$ *admet l'équation* (3) *comme modèle minimal de Weierstrass sur* $\mathbb{Z}$. *De plus, pour tout nombre premier distinct de* 7, *l'équation* (4) *est un modèle minimal de Weierstrass de* $H(u, v)$.

Soit l *un nombre premier. Si* l *ne divise pas* $\Delta(G(u, v))$, $H(u, v)$ *et* $G(u, v)$ *ont bonne réduction en* l. *Si* l *divise* $\Delta(G(u, v))$, *et si* l *est distinct de* 7, *la réduction en* l *de* G *et* H *est multiplicative.*

Si $l=7$, *et si* l *divise* $uv(u-v)$, *la réduction de* G *et* H *est multiplicative, et l'équation* (4) *donne un modèle minimal de Weierstrass de* H *en* 7.

Si $l=7$, *et si* $u+2v\equiv 0$ *modulo* l, *la réduction de* G *et* H *en* l *est additive,* G *est de type de Kodaira II, et* (4) *n'est pas l'équation d'un modèle minimal de Weierstrass de* H *en* 7.

On obtient de même la proposition II. 3. 2.:

Proposition II. 3. 2. *Soit* K *un corps de nombres, et soit* $P(x, y)$ *un point de* $H(u, v)(K)$. *Supposons que, pour toute place* w *de* K *divisant* $u^3-8u^2v+5u^2+v^3$, x *ne soit pas congru à* $-28u^2+20uv+3v^2$ *modulo* w. *Alors* P *se prolonge en un point de* $H'(u, v)(O_K)$.

Modulo 2, G et H ont une réduction multiplicative. Modulo 3, H et G ont bonne réduction si et seulement si $uv(u-v)\not\equiv 0$ modulo 3. Par un raisonnement analogue à celui de II. 1. 3., on en déduit:

Proposition II. 3. 3. *Soit le polynôme*:

$$D(x, u, v)=4x^3+B_2(u, v)\,x^2+2B_4(u, v)\,x+B_6(u, v)$$

et soit u *congru à* 2 *modulo* 3, v *congru à* 1 *modulo* 3. *Soit un rationnel* x *vérifiant les deux conditions suivantes*:

i) *pour tout nombre* l *premier divisant* $u^3-8u^2v+5uv^2+v^3$, x *n'est pas congru à* $-28u^2+20uv+3v^2$ *modulo* l;

ii) x *est entier en* 3.

Alors le corps $K=\mathbb{Q}(\sqrt{D(x, u, v)})$ *a un nombre de classes divisible par* 7.

De même, pour trouver des corps quadratiques dont le 7-rang du groupe des classes d'idéaux est supérieur ou égal à 2, on procède comme dans II. 2. 1. Si l'on désire obtenir des corps quadratiques réels, on doit utiliser des couples (u, v) tels que:

i) $C_4(u, v)$ est une norme de $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$

et

ii) $\Delta(H(u, v))>0$, ou $(\Delta(H(u, v))<0$ et $C_6(u, v)<0)$.

Il existe une infinité de tels couples. D'où:

Théorème II. 3. 4. *Il existe une infinité de corps quadratiques réels dont le* 7*-rang du groupe de classes d'idéaux est supérieur ou égal à* 2.

Appendice

Cet appendice est extrait d'une rédaction de J. Martinet datant de juillet 1979. Il contient un certain nombre d'exemples illustrant les méthodes de l'exposé. En voici le mode d'emploi:

On donne un entier N qui est le conducteur d'une courbe elliptique A définie sur $\mathbb{Q}$ munie d'un point d'ordre n; B désigne la courbe quotient de A par son sous-groupe cyclique d'ordre n; son conducteur est également N. On donne des équations de A et de B, ainsi que les discriminants Δ_A et Δ_B de ces courbes, et les coordonnées modulo p du point singulier de B pour ceux des nombres premiers p où B a mauvaise réduction dont il faut tenir compte pour obtenir la surjectivité de φ sur les modèles de Néron (cf. § I).

Soit k un corps de nombres et x (resp. y) un élément de k. Le corps $k(x, y)$ où (x, y) est un point de B est une extension K_x (resp. K_y) de k de degré au plus 2 (resp. 3), et en fait de degré exactement 2 (resp. 3) et de nombre de classes divisible par n lorsque les conditions de congruences (i) et *une* des conditions de congruences $(\mathrm{ii})_p$ sont vérifiées. Sauf dans un exemple ($N=11$, $n=5$, $k=\mathbb{Q}(i)$), k est le corps $\mathbb{Q}$ des nombres rationnels. On donne dans chaque cas un polynôme m tel que $K_x=\mathbb{Q}(\sqrt{m(x)})$; les corps cubiques K_y (lorsqu'on les considère) sont définis par un polynôme P_y de discriminant d_{P_y}; l'extension non ramifiée peut alors être définie par un polynôme de degré 15, que nous n'avons pas explicité.

Les couples (N, n) considérés sont (11, 5), (14, 3), (17, 4), (26, 7), (38, 5), (123, 5). Dans le cas où $N=17$, on a considéré la divisibilité des groupes de classes de K_x et de K_y par 4 *et* 2.

$N=11$, $n=5$, $\Delta_A=-11$, $\Delta_B=-11^5$.

$$A: y^2-y=x^3-x^2; \qquad B: y^2-y=x^3-x^2-10x-20.$$

Point singulier modulo 11 : (5, 5).

Corps quadratique: $m(x)=4x^3-4x^2-40x-79$.

(i) : $x\not\equiv 5 \bmod 11$.

$(\mathrm{ii})_2$: $x\equiv 0,1 \bmod 2$; $((\mathrm{ii})_3 : x\equiv 1, -1 \bmod 3$; $(\mathrm{ii})_5 : x\equiv 0,1 \bmod 5$;

$(\mathrm{ii})_7$: $x\equiv -1, -2, 2, -3 \bmod 7$; $(\mathrm{ii})_{11}$: $x\equiv 0, 3, -5, -4 \bmod 11$.

L'extension non ramifiée de degré 5 de $\mathbb{Q}(\sqrt{m(x)})$ est définie par le polynôme $P(X)=X^5-(x+2)X^4+(2x+3)X^3-xX^2-2X+1$, de discriminant $m(x)^2$.

Remarque 1. Pour x entier en 2, puisque $P(0)=P(1)=1$, 2 reste inerte dans l'extension définie par P; par conséquent, un idéal au-dessus de 2 dans $\mathbb{Q}(\sqrt{m(x)})$ a une classe d'ordre multiple de 5.

Corps cubique: $P_y(X)=X^3-X^2-10X-(y^2+y+20)$, de discriminant

$$d_{P_y}=-2^2(27u^2+632u+2595) \quad \text{où} \quad u=(y^2+y)/2.$$

i) : $y\not\equiv 5 \bmod 11$.

$(\mathrm{ii})_2$: $y\equiv 0,1 \bmod 2$; $(\mathrm{ii})_3$: $y\equiv 0, -1 \bmod 3$; $(\mathrm{ii})_5$: $y\equiv 0, -1 \bmod 5, \ldots$

Exemples. Pour $y=12, 3, 0$, le discriminant de K_y est -1999, -2104, -2595. Pour $x=4, 6$, le discriminat de $\mathbb{Q}(\sqrt{m(x)})$ est -47, $+401$. Pour $x=-2+i$,

$$K=\mathbb{Q}(\sqrt{m(x)})=\mathbb{Q}(\sqrt{-19+20i})$$

est un corps totalement imaginaire de degré 4, de discriminant $d_K=2^4\cdot 761$, de nombre de classes divisibles par 5. Son corps de classes de Hilbert L est de degré 20, et

$$(d_L)^{1/20}=10{,}504\ldots$$

excède de 2,28% seulement la minoration de Odlyzko sous GRH (10, 270).

Sous-groupe de type (5, 5) *dans* $\mathbb{Q}(\sqrt{m(x)})$. Soit $m(t)$ comme dans la proposition II. 2. 2.

(i) $t\not\equiv 2, 6, 7 \bmod 11$

(ii) ($t\equiv 0 \bmod 2$ ou $t\equiv 3 \bmod 4$) et ($t\equiv 1 \bmod 3$ ou $t\equiv 0 \bmod 5$), ou encore $t\equiv 1 \bmod 4$ et $t\equiv -1 \bmod 3$,...

Pour $t=0$, on trouve le corps quadratique imaginaire de discriminant

$$-11\,199=-3\cdot 3733,$$

de groupe des classes de type (20, 5); c'est le premier discriminant que l'on rencontre pour lequel il y ait un sous-groupe de type (5, 5).

$N=14$, $n=3$, $\Delta_A=-2^2.7$, $\Delta_B=-2^6.7^3$.

$$A: y^2+xy+y=x^3-x; \qquad B: y^2+xy+y=x^3+4x-6.$$

Point singulier modulo 2 : (1, 1); modulo 7 : (2, 2).

Corps quadratique: $m(x)=4x^3+x^2+18x-23=(x-1)(4x^2+5x+23)$.

(i): $x\not\equiv 1 \bmod 2$ et $x\not\equiv 2 \bmod 7$

$(ii)_3$: $x\equiv 0, -1 \bmod 3$.

L'extension non ramifiée correspondante est définie par le polynôme

$$X^3-xX^2-X+1$$

de discriminant $m(x)$.

$N=17$, $n=4$, $\Delta_A=17$, $\Delta_B=-17^4$.

$$A: y^2+xy+y=x^3-x^2-x; \qquad B: y^2+xy+y=x^3-x^2-x-14.$$

Point singulier modulo 17 : (7, -4).

Corps quadratique: $m(x)=4x^3-3x^2-2x-55=(4x-11)(x^2+2x+5)$.

(i): $x\not\equiv 7 \bmod 17$.

$(ii)_2$: $4|h$: $x\equiv 0 \bmod 2$; $2|h$: $x\equiv 0 \bmod 2$ ou $x\equiv 1$ ou $-3 \bmod 8$.

$(ii)_3$: $4|h$: $x\equiv 1 \bmod 3$; $2|h$: $x\equiv \bmod 3$ ou $x\equiv -1$ ou $2 \bmod 9$.

Extension non ramifiée. Pour $n=2$, le polynôme est $X^2-(x-1)X-(x+1)$. Pour $n=4$, le polynôme est $X^4-(x+1)X^3+xX^2+2x-1$, de discriminant $(4x-11)(x^2+2x+5)^2$.

Corps cubique: Il est défini par le polynôme $P_y = X^3 - X^2 - (y+1)X - (y^2+y+14)$, de discriminant $-27y^4 - 68y^3 - 810y^2 - 1016y - 5595$.

(i): $y \not\equiv -4 \bmod 17$.

$(ii)_2$: $4|h: y \equiv 0 \bmod 2$; $2|h: y \equiv 0 \bmod 2$ ou $y \equiv 1 \bmod 2$

$(ii)_3$: $4|h: y \equiv 1 \bmod 3$; $2|h: y \equiv 1 \bmod 3$ ou $y \equiv 0$ ou $3 \bmod 9$.

Pour $x = 2, 4$ on obtient les corps quadratiques de discriminants -39, $+145$, avec $h=4$; pour $y=-3$, on trouve le corps cubique de discriminant -283, avec $h=2$.

$N=26$, $n=7$, $\Delta_A = -2^7 \cdot 13$, $\Delta_B = -2.13^7$.

$A: y^2 + xy + = x^3 - x^2 - 3x + 3$; $\quad B: y^2 + xy + y = x^3 - x^2 - 213x - 1257$.

Point singulier modulo 13 : $(-5, 2)$.

L'application définie par l'isogénie $A \to B$ sur les modèles de Néron restreinte à la fibre au-dessus de 2 est $(x, y) \mapsto x : \mathbb{G}_m \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{G}_m$. Comme elle est surjective, il n'y a pas de condition (i) due au nombre premier 2; le même phénomène se produit en 2 pour $N=38$, $n=5$ et en 3 pour $N=123$, $n=5$.

Corps quadratique: $m(x) = 4x^3 - 3x^2 - 850x - 5027$.

(i): $x \not\equiv -5 \bmod 13$.

$(ii)_3$: $x \equiv 0, 1, -1 \bmod 3$; $(ii)_5$: $x \equiv 1, -1, -2 \bmod 5$;

$(ii)_7$: $x \equiv 1, -1, 3 \bmod 7$.

$N=38$, $n=5$, $\Delta_A = -2^5 \cdot 19$, $\Delta_B = -2 \cdot 19^5$.

$A: y^2 + xy + y = x^3 + x^2 + 1$; $\quad B: y^2 + xy + y = x^3 + x^2 - 70x - 279$.

Point singulier modulo 19 : $(7, -4)$.

Corps quadratique: $m(x) = 4x^3 + 5x^2 - 278x - 1115$.

(i): $x \not\equiv 7 \bmod 19$.

$(ii)_3$: $x \equiv 0, -1 \bmod 3$; $(ii)_5$: $x \equiv 1, -1, 2, -2 \bmod 5$;

$(ii)_7$: $x \equiv 1, -1 \bmod 7$.

L'extension non ramifiée de degré 5 de $\mathbb{Q}(\sqrt{m(x)})$ est définie par le polynôme $X^5 - xX^4 + 12X^3 + 2(x+15)X^2 + 11X + 10 - x$, de discriminant $[2^7 m(x)]^2$.

$N=123$, $n=5$, $\Delta_A = -3^5 \cdot 41$, $\Delta_B = -3 \cdot 41^5$.

$A: y^2 + y = x^3 + x^2 - 10x + 10$; $\quad B: y^2 + y = x^3 + x^2 + 20x - 890$.

Point singulier modulo 41: (16, 20).

Corps quadratique: $m(x) = 4x^3 + 4x^2 + 80x - 3559$.

(i): $x \not\equiv 16 \bmod 41$.

$(ii)_2$: $x \equiv 0, 1 \bmod 2$.

Bibliographie

[1] *D. A. Buell*, Class groups of quadratic fields, Math. of Comp. **30** (1976), 610—623.
[2] *M. Craig*, A construction for irregular discriminants, Osaka J. Math. **14** (1977), 365—402.
[3] *P. Deligne, M. Rapoport*, Les schémas de modules de courbes elliptiques, Modular functions of one variable. II, Lecture Notes in Math. **349**, Berlin-Heidelberg-New York 1973, 143—316.
[4] *F. Diaz y Diaz*, Sur le 3-rang des corps quadratiques réels, Preprint.
[5] *F. Diaz y Diaz*, On some families of imaginary quadratic fields, Math. of Comp. **32** (1973), 636—650.
[6] *T. Nagell*, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Hamburg Univ. **1** (1922), 140—150.
[7] *F. Oort, J. Tate*, Group schemes of prime order, Ann. Scient. Ec. Norm. Sup. (4) **3** (1970), 1—21.
[8] *D. Shanks*, New Types of Quadratic Fields Having Three Invariants Divisible by 3, J. Number Theory **4** (1972), 537—556.
[9] *D. Shanks, R. Serafin*, Quadratic fields with four invariants divisible by 3, Math. of Comp. **27** (1973), 183—187.
[10] *D. Shanks, P. Weinberger*, A quadratic field of prime discriminant requiring three generators for its class group, and related theory, Sierpinski Memorial Volume, Acta Arith. **21** (1972), 71—87.
[11] *J. Vélu*, Isogénies entre courbes elliptiques, C. R. Acad. Sc. Paris **273** (26 juillet 1971), 238—241.
[12] *Y. Yamamoto*, On unramified galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57—76.

Laboratoire de Mathématiques, Université de Bordeaux I, F-33405 Talence Cedex

Eingegangen 27. Juli 1982