Courbes modulaires et 11-rang de corps quadratiques

Franck Leprévost

TABLE DES MATIÈRES

Introduction
1. Structure galoisienne de courbes modulaires
2. Le cas $p = 23$
3. Méthode et Résultats
Remerciements
Bibliographie

Nous construisons 53 corps quadratiques imaginaires ayant un 11-rang égal à 3, et sept corps quadratiques réels de 11-rang égal à 2. Ce sont, à notre connaissance, les premiers exemples de tels corps.

We construct 53 imaginary quadratic fields of 11-rank equal to 3, and seven quadratic fields of 11-rank equal to 2. These appear to be the first examples of such fields.

INTRODUCTION

Soient K un corps de nombres, Cl_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 est, par définition, la dimension de $\mathrm{Cl}_K/p\,\mathrm{Cl}_K$ sur $\mathbf{F}_p$. Par abus de langage, nous entendrons par p-rang de K le p-rang du groupe des classes d'idéaux de K.

Gauß a montré que le 2-rang d'un corps quadratique de discriminant D est $t-1$ ou $t-2$, où t est le nombre de facteurs premiers de D. Par conséquent, pour chaque entier $n \geq 1$, il existe une infinité de corps quadratiques réels (ou imaginaires) dont le 2-rang soit égal à n.

Shanks [1972] a trouvé les premiers exemples de corps quadratiques imaginaires dont le 3-rang est ≥ 3. Depuis, divers auteurs (*e.g.* [Diaz y Diaz 1973 ; Craig 1977]) ont trouvé d'autres exemples de corps quadratiques de 3-rang supérieur à 3. Quer [1987] a trouvé trois corps quadratiques imaginaires dont le 3-rang est 6. A chacun d'entre eux est associé, par un théorème de Scholz, un corps quadratique réel dont le 3-rang est 5.

Les cas $p = 5$ et $p = 7$ ont été étudiés par Mestre [1983 ; 1992]. Schoof [1983] a découvert le

1058-6458/96 \$0.50 per page

premier exemple de corps quadratique imaginaire dont le 5-rang est ≥ 4, et Solderitsch [1977] le premier corps quadratique imaginaire dont le 7-rang est ≥ 3. Pour d'autres exemples de tels corps, voir [Llorente et Quer].

Nous construisons ici 53 corps quadratiques imaginaires ayant un 11-rang égal à 3, et sept corps quadratiques réels de 11-rang égal à 2. Ce sont, à notre connaissance, les premiers exemples de tels corps.

1. STRUCTURE GALOISIENNE DE COURBES MODULAIRES

Nous renvoyons à [Ling et Oesterlé 1991] pour cette partie. Soient K un corps et N un entier ≥ 1. Pour E une courbe elliptique définie sur K, notons $Y_0(N)(K)$ l'ensemble des classes de $\bar{K}$-isomorphisme de couples (E, C), où C est un sous-groupe de E défini sur K et cyclique d'ordre N ; et notons $Y_1(N)(K)$ l'ensemble des classes de $\bar{K}$-isomorphisme de couples (E, P), où P est un point de E défini sur K et d'ordre N.

Soient

$$\begin{aligned} \Gamma &= \mathrm{SL}_2(\mathbf{Z}), \\ \Gamma_0(N) &= \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \,;\, c \equiv 0 \bmod N \right\}, \\ \Gamma_1(N) &= \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \,;\, a \equiv d \equiv 1 \bmod N \right\}. \end{aligned}$$

Alors $Y_0(N)(\mathbf{C})$ et $Y_1(N)(\mathbf{C})$ sont isomorphes aux quotients de l'action des groupes $\Gamma_0(N)/\{\pm 1\}$ et $\Gamma_1(N)/\{\pm 1\}$, respectivement, sur le demi-plan de Poincaré. En rajoutant les pointes aux courbes $Y_0(N)(\mathbf{C})$ et $Y_1(N)(\mathbf{C})$ on obtient les compactifiées $X_0(N)(\mathbf{C})$ et $X_1(N)(\mathbf{C})$.

Enfin, notons J_1 et J_0 les jacobiennes des courbes $X_1(N)$ et $X_0(N)$.

La courbe modulaire $X_0(p)$

Prenons $N = p$, où p est un nombre premier impair, et posons $(p-1)/12 = a/b$, où a et b sont des entiers ≥ 1 et premiers entre eux. Si

$$\eta(z) = q^{1/24} \prod_{n \geq 1} (1 - q^n),$$

où $q = e^{2i\pi z}$, la fonction

$$f(z) = \left(\frac{\eta(z)}{\eta(pz)} \right)^{2b} = q^{-a} \prod_{(n,p)=1} (1 - q^n)^{2b}$$

est une fonction modulaire pour le groupe $\Gamma_0(p)$, de diviseur

$$a[(0) - (\infty)],$$

où ∞ et 0 représentent les pointes correspondantes de $X_0(p)$. On peut montrer que le sous-groupe engendré par le diviseur $(0) - (\infty)$ est exactement le groupe de torsion C de la jacobienne de $X_0(p)(\mathbf{Q})$, et est d'ordre exactement a.

Supposons désormais $p \equiv -1 \bmod 12$ (ce que vérifie, par exemple, $p = 23$), et considérons le revêtement

$$\begin{array}{c} X_1(p) \\ \pi \big\downarrow \\ X_0(p) \end{array}$$

prolongeant celui défini en dehors des pointes par :

$$\begin{array}{cc} Y_1(p) & (E, P) \\ \big\downarrow & \big\downarrow \\ Y_0(p) & (E, \langle P \rangle) \end{array}$$

Ce revêtement est abélien cyclique de groupe de Galois $\mathbf{Z}/a\mathbf{Z}$, où $a = \frac{1}{2}(p-1)$.

Ce revêtement induit, par fonctorialité de Picard :

$$\pi^* : J_0 \longrightarrow J_1.$$

Le revêtement π est cyclique de degré a. Donc [Ling et Oesterlé 1991, p. 172] il existe un sous-groupe Σ (dit de Shimura) de la jacobienne de $X_0(p)(\mathbf{Q}(\mu_a))$, isomorphe à μ_a en tant que $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module, et qui est le noyau de π^*. Ainsi obtient-on la suite exacte de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules :

$$1 \longrightarrow \mu_a \longrightarrow J_0 \longrightarrow J_1.$$

La jacobienne de la courbe modulaire $X_0(p)$ possède donc deux sous-groupes cycliques, rationnels sous l'action de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ et d'ordre a : le groupe

C engendré par $(0) - (\infty)$ et le groupe Σ de Shimura. $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ agit trivialement sur C, comme μ_a sur Σ.

Supposons désormais a impair (donc $C \cap \Sigma = \{0\}$) et premier. Les sous-groupes précédents permettent, dans certains cas, de construire, en utilisant la méthode décrite dans [Mestre 1982], des corps quadratiques dont le a-rang est ≥ 1.

Soit

$$1 \longrightarrow \mathrm{Ker}(\varphi) \longrightarrow C \xrightarrow{\varphi} J_0 \longrightarrow 1$$

une suite exacte, où C est une variété abélienne et φ une isogénie définies sur $\mathbf{Q}$. Supposons C semi-stable en tout l premier. Soit k un corps quadratique, O_k son anneau des entiers, $C/_{O_k}$ et $J_0/_{O_k}$ les modèles de Néron de C et J_0 sur O_k, et $\mathrm{Ker}(\varphi)/_{O_k}$ la clôture schématique de $\mathrm{Ker}(\varphi)/k$ dans $C/_{O_k}$. On a alors la suite exacte de schémas en groupes sur O_k

$$1 \longrightarrow \mathrm{Ker}(\varphi)/_{O_k} \longrightarrow C/_{O_k} \longrightarrow J_0'/_{O_k} \longrightarrow 1,$$

où $J_0'/_{O_k}$ est un sous-schéma en groupes ouvert de $J_0/_{O_k}$, contenant la composante neutre de $J_0/_{O_k}$ (ceci étend le lemme de [Mestre 1992, p. 371]).

Supposons dans la suite la courbe $X_0(p)$ hyperelliptique, d'équation

$$y^2 = f(x),$$

où f est un élément de $\mathbf{Q}[x]$ sans racines multiples. Notons k le corps $\mathbf{Q}\bigl(\sqrt{f(x)}\bigr)$ et O_k l'anneau des entiers de k.

Cas imaginaire

Supposons que k soit un corps quadratique imaginaire. Soit B la variété abélienne quotient de J_0 par le sous-groupe d'ordre a engendré par le diviseur $(0) - (\infty)$. On a une suite exacte :

$$1 \longrightarrow \mathbf{Z}/a\mathbf{Z} \longrightarrow J_0 \longrightarrow B \longrightarrow 1$$

qui, par dualité, donne une autre isogénie, définie sur k :

$$1 \longrightarrow \mu_a \longrightarrow {}^tB \longrightarrow J_0 \longrightarrow 1.$$

Posons $C = {}^tB$ et supposons C semi-stable en tout nombre premier l. Notons G le schéma en groupes quasi-fini clôture schématique de $\mu_{a/k}$ dans $C/_{O_k}$. Alors on a, pour un certain sous-schéma en groupes $J_0'/_{O_k}$ ouvert de $J_0/_{O_k}$ et contenant la composante neutre de $J_0/_{O_k}$, la suite exacte de schémas en groupes sur O_k :

$$1 \longrightarrow G \longrightarrow C/_{O_k} \longrightarrow J_0'/_{O_k} \longrightarrow 1.$$

En regardant cette suite exacte comme une suite exacte de faisceaux sur $\mathrm{Spec}(O_k)$ pour la topologie fppf, on en déduit une injection :

$$1 \longrightarrow J_0'(O_k)/C(O_k) \longrightarrow \mathrm{H}^1(\mathrm{Spec}(O_k), G).$$

D'autre part, on a la suite exacte

$$1 \longrightarrow G \longrightarrow \mu_a \longrightarrow \mu_{a\cdot} \longrightarrow 1,$$

où $\mu_{a\cdot}$ désigne un faisceau en gratte-ciel trivial en dehors des places de k divisant a. D'où l'injection

$$1 \longrightarrow \mathrm{H}^1(\mathrm{Spec}(O_k), G) \longrightarrow \mathrm{H}^1(\mathrm{Spec}(O_k), \mu_a).$$

Enfin, k étant un corps quadratique imaginaire, $\mathrm{H}^1(\mathrm{Spec}(O_k), \mu_a)$ s'injecte dans ${}_a\mathrm{Cl}_k$, d'où l'existence d'un morphisme injectif

$$J_0'(O_k)/C(O_k) \longrightarrow {}_a\mathrm{Cl}_k.$$

Cas réel

Supposons ici k quadratique réel. La suite exacte

$$1 \longrightarrow \mu_a \longrightarrow J_0 \xrightarrow{\pi^*} J_1$$

montre qu'il existe une variété abélienne $B = \mathrm{Im}\,\pi^*$ telle que l'on ait la suite exacte :

$$1 \longrightarrow \mu_a \longrightarrow J_0 \longrightarrow B \longrightarrow 1,$$

qui donne par dualité, en notant $C = {}^tB$ et $\varphi = {}^t\pi^*$:

$$1 \longrightarrow \mathbf{Z}/a\mathbf{Z} \longrightarrow C \xrightarrow{\varphi} J_0 \longrightarrow 1,$$

(la variété abélienne J_0 étant une jacobienne, elle est isomorphe sur $\mathbf{Q}$ à sa duale).

Supposons C semi-stable en tout nombre premier l. Pour un certain sous-schéma en groupes

$J_0'/_{O_k}$ ouvert de $J_0/_{O_k}$ et contenant la composante neutre de $J_0/_{O_k}$, on a la suite exacte de schémas en groupes sur O_k :

$$1 \longrightarrow \mathbf{Z}/a\mathbf{Z} \longrightarrow C/_{O_k} \longrightarrow J_0'/_{O_k} \longrightarrow 1,$$

qui induit un homomorphisme de groupes :

$$0 \longrightarrow J_0'(O_k)/C(O_k) \longrightarrow \mathrm{Hom}(\mathrm{Cl}_k, \mathbf{Z}/a\mathbf{Z}),$$

car

$$\begin{aligned}\mathrm{H}^1_{\mathrm{fppf}}(\mathrm{Spec}(O_k), \mathbf{Z}/a\mathbf{Z}) &= \mathrm{H}^1_{\mathrm{et}}(\mathrm{Spec}(O_k), \mathbf{Z}/a\mathbf{Z})\\ &= \mathrm{Hom}(\mathrm{Cl}_k, \mathbf{Z}/a\mathbf{Z}).\end{aligned}$$

Par suite, l'image réciproque par φ de tout point de $J_0'(O_k)$ engendre une extension de k, abélienne non ramifiée et de degré divisant a.

De manière concrète : soit x un rationnel et Q l'un des deux points de $X_0(p)$ d'abscisse x. Supposons que Q ne se réduise pas modulo p en le point singulier de $X_0(p)/_{\mathbf{F}_p}$. Alors le théorème de Chevalley et Weil [1932] permet de montrer que l'extension $k\big(\varphi^{-1}(Q)\big)/k$, où $k = \mathbf{Q}\big(\sqrt{f(x)}\big)$, est non ramifiée et de degré a.

La courbe modulaire $X_0(2p)$

Si $N = N_1N_2$, où N_1 et N_2 sont des entiers ≥ 1 et premiers entre eux, nous pouvons définir sur $\mathbf{Q}$ une involution $\omega^N_{N_1}$ (dite d'Atkin–Lehner) de $X_0(N)$, en posant, pour tout $(E, C) \in Y_0(N)$:

$$\omega^N_{N_1}\big((E,C)\big) = (E/C_{N_1},\, E_{N_1} + C_{N_2}/C_{N_1}),$$

où C_{N_i}, pour $i = 1, 2$, est l'unique sous-groupe cyclique de C d'ordre N_i, et E_{N_1} est le groupe des points d'ordre N_1 de E.

La courbe modulaire $X_0(N)$ est donc revêtement de deux manières différentes de la courbe modulaire $X_0(N_2)$. En effet, un premier revêtement naturel, noté ici π_1, est donné, en dehors des pointes, par :

$$\begin{array}{ccc} X_0(N_1N_2) & & (E, C_N) \\ \pi_1\big\downarrow & & \pi_1\big\downarrow \\ X_0(N_2) & & (E, N_1C_N) \end{array}$$

Un second revêtement, π_2, s'obtient en composant le revêtement ci-dessus avec l'involution $\omega^N_{N_1}$ d'Atkin–Lehner :

$$\begin{tikzcd} X_0(N) \arrow[r, "\omega^N_{N_1}"] \arrow[dr, "\pi_2"'] & X_0(N) \arrow[d, "\pi_1"] \\ & X_0(N_2) \end{tikzcd}$$

Si $N = 2p$, la courbe modulaire $X_0(2p)$ est donc revêtement de deux manières de $X_0(p)$. De manière explicite, le morphisme π_1 est donné par

$$(E, C_2C_p) \longrightarrow (E, C_p), \tag{1.1}$$

et le morphisme π_2 par

$$(E, C_2C_p) \longrightarrow (E/C_2, C_2C_p/C_2). \tag{1.2}$$

Enfin l'involution ω^{2p}_2 de $X_0(2p)$ est donnée par

$$(E, C_2C_p) \longrightarrow (E/C_2, [E[2]/C_2].C_p),$$

où $E[2]$ désigne le noyau de la multiplication par 2 dans E.

Les revêtements π_1 et π_2 de $X_0(2p)$ sur $X_0(p)$ sont indépendants. Le calcul montre en effet que les images réciproques par π_1 et π_2 de l'espace vectoriel Ω_p sont supplémentaires dans Ω_{2p}, où, pour $N = p$ ou $N = 2p$, Ω_N désigne l'espace des formes différentielles de première espèce de $X_0(N)$.

Soit (E, C_2C_p) un élément de $X_0(2p)(k)$ et (E, P) un élément de $X_1(p)$ au dessus de $\pi_1\big((E, C_2C_p)\big)$. En considérant l'isogénie de degré 2 définie sur k :

$$\psi : E \longrightarrow E/C_2,$$

on constate que $\psi(P)$ est un point de E/C_2, défini sur k et qui engendre le sous-groupe C_2C_p/C_2. Par suite la jacobienne de $X_0(2p)$ ne contient qu'une copie de Σ.

Une démonstration de cela se trouve également dans [Ling et Oesterlé 1991], que nous reproduisons ci-dessous.

Nous avons vu que le revêtement

$$\begin{array}{c} X_1(p) \\ \pi(p)\big\downarrow \\ X_0(p) \end{array}$$

induit, par fonctorialité de Picard, une suite exacte

$$1 \longrightarrow \Sigma(p) \longrightarrow J_0(p) \xrightarrow{\pi^*(p)} J_1(p).$$

De même, le revêtement

$$\begin{array}{c} X_0(2p) \\ \pi_1\big\downarrow \\ X_0(p) \end{array}$$

induit un morphisme

$$J_0(p) \xrightarrow{\pi_1^*} J_0(2p).$$

Or, on a $\pi_1^*\big(\Sigma(p)\big) \subset \Sigma(2p)$ [Ling et Oesterlé 1991, Th. 4, p. 175]. Mais

$$\begin{tikzcd} X_0(2p) \arrow[r, "\omega_2"] \arrow[dr, "\pi_2"'] & X_0(2p) \arrow[d, "\pi_1"] \\ & X_0(p) \end{tikzcd}$$

induit

$$J_0(p) \xrightarrow{\pi_2^*} J_0(2p),$$

et $\pi_2 = \pi_1 \circ \omega_2$ implique $\pi_2^* = \omega_2^* \circ \pi_1^*$, donc

$$\pi_2^*\big(\Sigma(p)\big) = \omega_2^*\big(\pi_1^*\big(\Sigma(p)\big)\big).$$

Par suite,

$$\pi_2^*\big(\Sigma(p)\big) \subset \omega_2^*\big(\Sigma(2p)\big) = \Sigma(2p),$$

car, d'après [Ling et Oesterlé 1991, Th. 3, p. 174], le sous-groupe de Shimura $\Sigma(2p)$ est stable sous ω_2^*.

Donc les images par π_1^* et par π_2^* du sous-groupe de Shimura de $J_0(p)$, $\Sigma(p)$, sont des sous-groupes de $\Sigma(2p)$, le sous-groupe de Shimura de $J_0(2p)$. Enfin, [Ling et Oesterlé 1991, Cor. 1, p. 173] permet de montrer que l'ordre de $\Sigma(2p)$ est encore a, ce qui établit que $J_0(2p)$ ne contient qu'une copie de $\Sigma(p)$.

Par contre, on peut verifier que les pointes de $X_0(2p)$ engendrent un sous-groupe de sa jacobienne qui, en tant que module galoisien, est isomorphe à $\big(\mathbf{Z}/a\mathbf{Z}\big)^2$.

Si la courbe $X_0(2p)$ est hyperelliptique, d'équation $y^2 = g(x)$, considérons le point Q de $X_0(2p)$ d'abscisse un rationnel x. Supposons que Q ne se réduise pas modulo p en un point singulier de la courbe $X_0(2p)/_{\mathbf{F}_p}$. Soit $k = \mathbf{Q}\big(\sqrt{g(x)}\big)$; si k est un corps quadratique imaginaire, le a-rang de k est supérieur ou égal à 2. Si k est un corps quadratique réel, on peut seulement affirmer que le a-rang de k est supérieur ou égal à 1.

2. LE CAS $p = 23$

La courbe modulaire $X_0(23)(\mathbf{Q})$

Considérons la courbe modulaire de genre deux, donc hyperelliptique, $X_0(23)(\mathbf{Q})$. Une équation de cette courbe est, par exemple,

$$Y^2 = X^6 - 14X^5 + 57X^4 - 106X^3 + 90X^2 - 16X - 19$$

[Fricke 1928]. Cette courbe a bonne réduction partout sauf en 23 où la réduction du modèle ci-dessus est une union de deux droites :

$$Y^2 \equiv (X+2)^2(X+5)^2(X+9)^2 \bmod 23,$$

donc n'est pas irréductible. Il convient donc d'éclater les singularités.

Dans un premier temps, considérons le point singulier modulo 23 d'abscisse $X = -2$. Posons $X = -2 + 23t$. Ainsi obtient-on la courbe :

$$Y^2 = 23^2(529t^3 - 207t^2 + 26t - 1) \times (529t^3 - 391t^2 + 78t - 5).$$

Le changement $Y = 23y$ mène à l'équation $y^2 = f_{-2}(t)$, où

$$f_{-2}(t) = (529t^3 - 207t^2 + 26t - 1) \times (529t^3 - 391t^2 + 78t - 5).$$

Alors $y^2 \equiv 4(t+2)(t+15) \bmod 23$; on a donc éclaté le point singulier modulo 23 d'abscisse $X = -2$.

Plaçons-nous maintenant sur le point singulier modulo 23 d'abscisse $X = -5$. Posons pour ce faire $X = -5 + 23u$. On obtient ainsi

$$Y^2 = 23^2(279841u^6 - 535348u^5 + 413678u^4 - 166658u^3 + 37105u^2 - 4342u + 209).$$

Si l'on pose $Y = 23y$, on se ramène à l'équation

$$y^2 = 279841u^6 - 535348u^5 + 413678u^4 - 166658u^3 + 37105u^2 - 4342u + 209,$$

pour laquelle $y^2 \equiv 6(u+10)^2 \bmod 23$. Il faut faire un second éclatement en posant $u = -10 + 23t$. On obtient $y^2 = f_{-5}(t)$, avec $f_{-5}(t)$ égal à

$$23(148035889t^3 - 198127428t^2 + 88389023t - 13144019) \times (12167t^3 - 16468t^2 + 7429t - 1117).$$

Formellement,

$$\frac{f_{-5}(t)}{23} \equiv 3 \bmod 23\,;$$

le deuxième point singulier est bien éclaté.

Ôtons enfin la singularité modulo 23 d'abscisse $X = -9$: en posant $X = -9 + 23t$, nous obtenons $y^2 = f_{-9}(t)$, avec

$$f_{-9}(t) = 23(12167t^3 - 20102t^2 + 10649t - 1837)(529t^3 - 690t^2 + 229t - 43).$$

Formellement on a

$$\frac{f_{-9}(t)}{23} \equiv 9 \bmod 23,$$

et donc le dernier point singulier modulo 23 est éclaté.

La courbe modulaire $X_0(46)(\mathbf{Q})$

La courbe modulaire hyperelliptique $X_0(46)$ est revêtement de $X_0(23)$ de deux manières différentes : voir (1.1) et (1.2). Une équation de cette courbe est

$$Y^2 = (X^3 + X^2 + 2X + 1)(X^3 + 4X^2 + 4X + 8) \times (X^6 + 5X^5 + 14X^4 + 25X^3 + 28X^2 + 20X + 8)$$

[Gonzàlez Rovira 1991], qui se réduit modulo 23 en

$$Y^2 \equiv (X+3)^2(X+5)^2(X+15)^2 \times (X+16)^2(X+17)^2(X+18)^2 \bmod 23.$$

Comme précédemment, nous éclatons la courbe $X_0(46)$ en les 6 points singuliers modulo 23 d'abscisses respectives -5, -3, 5, 6, 7 et 8 modulo 23. Nous obtenons ainsi, pour $m \in \{-5, -3, 5, 6, 7, 8\}$, les équations $y^2 = g_m(t)$, où les polynômes $g_m(t)$ sont donnés ci-dessous.

$$\begin{aligned}
g_{-5}(t) &= 23(12167t^3 - 7406t^2 + 1541t - 109)(12167t^3 - 5819t^2 + 897t - 37)\\
&\quad \times (6436343t^6 - 6996025t^5 + 3212088t^4 - 796145t^3 + 112194t^2 - 8510t + 271)\\
g_{-3}(t) &= 23(529t^3 - 184t^2 + 23t - 1)(12167t^3 - 2645t^2 + 161t + 5)\\
&\quad \times (148035889t^6 - 83672459t^5 + 20708234t^4 - 2834911t^3 + 224296t^2 - 9614t + 173)\\
g_5(t) &= (529t^3 + 368t^2 + 87t + 7)(529t^3 + 437t^2 + 119t + 11)\\
&\quad \times (148035889t^6 + 225272005t^5 + 143838274t^4 + 49337185t^3 + 9589712t^2 + 1001650t + 43933)\\
g_6(t) &= 23(12167t^3 + 10051t^2 + 2806t + 265)(12167t^3 + 11638t^2 + 3680t + 392)\\
&\quad \times (6436343t^6 + 11473481t^5 + 8565568t^4 + 3428449t^3 + 776066t^2 + 94208t + 4792)\\
g_7(t) &= 23(12167t^3 + 11638t^2 + 3749t + 407)(529t^3 + 575t^2 + 207t + 25)\\
&\quad \times (148035889t^6 + 302508121t^5 + 258573084t^4 + 118348409t^3 + 30594186t^2 + 4235726t + 245393)\\
g_8(t) &= 23(12167t^3 + 13225t^2 + 4830t + 593)(12167t^3 + 14812t^2 + 5980t + 808)\\
&\quad \times (6436343t^6 + 14831573t^5 + 14284058t^4 + 7359977t^3 + 2140012t^2 + 332948t + 21656)
\end{aligned}$$

Polynômes utilisés pour l'éclatement des singularités de la courbe $X_0(46)$.

3. MÉTHODE ET RÉSULTATS

Soient a_k et b_k les racines réelles de f_k, où $k = -9, -5, -2$, et c_m et d_m les racines réelles de g_m, où $m = -5, -3, 5, 6, 7, 8$. Substituons dans f_k un nombre rationnel $t = i/j$, où j est premier à 23 et $a_k < t < b_k$: le 11-rang du corps quadratique imaginaire $\mathbf{Q}\bigl(\sqrt{f_k(t)}\bigr)$ est ≥ 1. De même, par substitution dans g_m de nombres rationnels convenables, tels que $c_m < t < d_m$, l'on obtient des corps quadratiques imaginaires $\mathbf{Q}\bigl(\sqrt{g_m(t)}\bigr)$ dont le 11-rang est ≥ 2.

Il n'était pas désespéré de trouver, par une recherche systématique dans ces familles, des corps quadratiques imaginaires ayant un 11-rang ≥ 3.

Dans la pratique, on a imposé aussi la condition $1 \leq j \leq B$, où B est une borne convenablement choisie. Pour chaque valeur de t ainsi obtenue, on a calculé de discriminant d correspondant. Pour les discriminants appartenant à $\bigl[-10^{20},\ -25\,10^6\bigr]$, dans le cas des f_k, ou à $\bigl[-10^{23},\ -25\,10^6\bigr]$, dans le cas des g_k, on a alors calculé le 11-rang de $\mathbf{Q}(\sqrt{d})$. (La borne supérieure de ces intervalles est imposée par les travaux de Buell [1987].) L'implémentation de cette méthode sera considerée ci-dessous.

Le tableau 1 fournit le nombre de corps quadratiques imaginaires obtenus à l'aide de chaque polynôme f_k ou g_k, et le nombre de ceux qui ont 11-rang égal à 1, 2, 3.

Nous avons également cherché, à l'aide des trois courbes associées à $X_0(23)$, des exemples de corps quadratiques *réels* ayant un 11-rang ≥ 2. Pour ce faire, nous avons substitué dans f_k des rationnels $t = i/j$, où $-B \leq j \leq B$, j non nul premier à 23, $1 \leq i \leq B$, i premier avec j tel que $i < a_k j$ ou $i > b_k j$, en ne retenant que les discriminants $\leq 10^{15}$. Le tableau 2 résume nos résultats dans cette direction (la même méthode, appliquée aux courbes issues de $X_0(46)$, a donné des discriminants dont la taille rendait le temps de calcul prohibitif par rapport au résultat escompté).

Le tableau 3 contient l'information suivante pour chaque corps imaginaire de 11-rang égal a 3 : le discriminant d ; le polynôme et les valeurs de i et j qui ont permis de trouver d, selon le procédé ci-dessus ; et la structure du groupe des classes. (Dans la dernière colonne, chaque expression entre parenthèses désigne un group cyclique, de sorte que $(2)^4(3^2)(11)^3$ doit être interpreté comme le groupe $(\mathbf{Z}/2\mathbf{Z})^4 \times (\mathbf{Z}/9\mathbf{Z}) \times (\mathbf{Z}/11\mathbf{Z})^3$.) Les discriminants obtenus avec $g_7(t)$ et $g_8(t)$, étant les mêmes que ceux obtenus, respectivement, avec $g_{-3}(t)$ et $g_6(t)$, ne sont donc pas reproduits.

	B	1	2	3	total
f_{-2}	2000	325073	35545	29	360647
f_{-5}	10000	48672	5390	7	54069
f_{-9}	2000	115775	13065	9	128849
g_{-5}	5000		85	2	87
g_{-3}	5000		163	2	165
g_5	5000		241	3	244
g_6	5000		159	1	160
g_7	5000		163	2	165
g_8	5000		159	1	160

TABLEAU 1. Nombre de corps quadratiques imaginaires de la forme $\mathbf{Q}\bigl(\sqrt{f_k(t)}\bigr)$ ou $\mathbf{Q}\bigl(\sqrt{g_k(t)}\bigr)$, avec $t = i/j$ et $j \leq B$ premier à 23. Le nombre de corps ayant 11-rang 1, 2, et 3 est également indiqué.

	B	1	2	total
f_{-2}	20	446	4	450
f_{-5}	50	70	0	70
f_{-9}	20	288	3	291

TABLEAU 2. Nombre de corps quadratiques réels obtenus à l'aide des polynômes f_k.

Le tableau 4 comporte les mêmes données pour les corps quadratiques réels de de 11-rang égal a 2, le groupe des classes étant pris au sens restreint.

Implémentation

Nous avons exploité pour nos calculs deux programmes écrits en langage C et utilisant la bibliothèque PARI [Batut et al. 1992].

Le premier construit les discriminants satisfaisant les conditions décrites ci-dessus, et les stocke dans des fichiers, un pour chaque f_k ou g_k.

d	k	i	j	groupe de classes
-107212102879	f_{-2}	23	152	$(2)^4(3^2)(11)^3$
-6009498285655	f_{-2}	35	401	$(2)^3(2^4)(7)(11)^3$
-3273815151496615	f_{-2}	205	1006	$(2^2)(2)^5(3^3)(7)(11)^3$
-11705648783592155	f_{-2}	106	293	$(2)^3(2^4)(3^5)(11)^3$
-15983136910670819	f_{-2}	74	895	$(2)^2(2^3)(11)^3(1171)$
-45917006295607387	f_{-2}	138	523	$(2^2)(2)^4(11)^3(13)(29)$
-128303784590905631	f_{-9}	119	158	$(2)^3(2^3)(11)^3(3943)$
-221930700346928435	f_{-2}	266	1593	$(2^2)^2(2)^3(11)^3(599)$
-240993755376321431	f_{-2}	181	464	$(2)^2(2^2)(11^2)(11)^2(17)(137)$
-259906958807885179	f_{-9}	783	1429	$(2)^4(2^7)(3)(11^2)(11)^2$
-329291663794278515	f_{-9}	133	223	$(2^6)(2)^4(3^2)(11^2)(11)^2$
-369255782670095911	f_{-2}	189	1613	$(2^6)(2)^4(11)^3(251)$
-767924965669088755	f_{-2}	300	1637	$(2)^3(2^6)(3)(11)^3(53)$
-859176261382499495	f_{-2}	215	622	$(2)^3(2^4)(3)(5)(11)^3(257)$
-1053991934262106015	f_{-2}	211	1873	$(2)^6(11)^3(4001)$
-1388624107376355751	g_{-5}	3	25	$(2)^3(2^2)(2^3)(3)(11)^3(733)$
-1689531290879523071	f_{-5}	1065	2384	$(2)(2^2)(3)(7)(11)^3(5653)$
-1788386963820377771	f_{-9}	179	303	$(2)^3(3)(11)^3(14009)$
-1858557024305974751	f_{-2}	169	1926	$(2)^4(2^3)(5)(11)^3(19)(127)$
-2051939044103994599	f_{-2}	347	1864	$(2)^2(2^2)^2(7)(11)^3(2089)$
-2378163971730283483	f_{-2}	274	1099	$(2)^3(3)(5)(11)^3(1451)$
-3672446254951263379	f_{-2}	294	1175	$(2)^2(2^2)(11)^3(15467)$
-5277472009435747079	f_{-2}	337	1508	$(2)^3(2^2)(11)^3(29)(2897)$
-6223112851448049611	f_{-5}	821	1827	$(2)(2^7)(5^4)(7)(11)^3$
-7612626093344267531	f_{-2}	532	1781	$(2)(2^2)(11)^3(13)(9829)$
-8592703740928325387	f_{-5}	1283	2877	$(2)^5(2^4)(11)^3(1429)$
-10893680997458041703	f_{-5}	4029	9082	$(2)^2(7)(11)^3(59557)$
-12134995031308874287	f_{-9}	403	662	$(2)^2(3)(11)^3(59)(2579)$
-12280492000465528715	f_{-2}	338	1149	$(2)^5(3^2)(11)^3(17)(163)$
-15175819545558957391	f_{-5}	1501	3362	$(2)(2^2)^2(3^2)(5)(7)(11^2)(11)^2(13)$
-16523040683771963671	f_{-2}	351	1097	$(2)^4(47)(11)^2(11^2)(149)$
-16690063420707862759	f_{-2}	361	955	$(2)^4(2^2)(11)^3(37)(821)$
-16713560136722037895	f_{-9}	466	1229	$(2)^4(11^2)(11)^2(47)(179)$
-16829732115140025191	f_{-5}	1490	3339	$(2^2)(2)^2(3)(11)^3(84857)$
-17549249288784625511	f_{-2}	361	1259	$(2)^3(11)^3(17)(109)(211)$
-23492548617875798615	f_{-2}	379	1322	$(2)^4(2^3)(7)(11)^3(61)(71)$
-28531121405097223255	f_{-5}	679	1502	$(2)^5(2^3)(3)(11^2)(11)^2(197)$
-36906219151810186103	f_{-2}	431	1716	$(2)^4(2^2)(2^4)(3^3)(11)^2(11^2)(13)$
-39834983794677106991	g_{-3}	8	81	$(2)^3(2^2)(3^2)(11^2)(11)^2(1709)$
-45160241220675305095	f_{-9}	669	1454	$(2)^5(3)(11)^3(19)(1181)$
-48914763189846648191	f_{-9}	458	1169	$(2)^3(5)(11)^3(131)(1321)$
-71073211716178669795	f_{-2}	450	1279	$(2^2)(2)^2(3)(7)(11)^3(3119)$
-71490861398199543571	f_{-2}	606	1337	$(2)^4(2^2)(3^2)(5)(11)^3(17)(37)$
-72513155510468696639	f_{-2}	481	1905	$(2)^6(3)(11)^3(79)(461)$
-74405260502618147759	f_{-9}	713	1526	$(2^2)(2)^2(5^3)(7)(11)^3(677)$
-80745015529084838443	f_{-2}	474	1229	$(2^2)(2)^2(5)(11)^3(9769)$
-92749971271765303855	f_{-2}	469	1507	$(2)^2(11)^2(11^2)(13)(6079)$
-99269440143264816311	g_5	-17	60	$(2^3)(2)^4(3)(5)(7)(11)^3(947)$
-450449172744992498303	g_6	-24	73	$(2^4)(2^2)(2)^2(5)(11)^3(13)(607)$
-4046043347830059995927	g_{-3}	6	59	$(2^4)(2)^3(3)(11)^3(85751)$
-12673958283032810545943	g_{-5}	8	53	$(2)^5(2^3)(3)(11)^3(47)(2293)$
-37299763559484163584607	g_5	-29	106	$(2)^4(2^2)(11)^3(961241)$
-62101651572868998047063	g_5	-29	81	$(2)^2(2^3)(3^2)(11)^3(37)(47)(283)$

TABLEAU 3. Données pour les 53 corps quadratiques imaginaires ayant 11-rang égal à 3.

d	k	i	j	groupe de classes
317019341	f_{-2}	2	-7	$(2)(11)^2$
78990264001	f_{-2}	7	-6	$(2)^2(11)^2$
3628885436065	f_{-9}	2	-7	$(2)^3(11)^2$
11153056789873	f_{-2}	17	-8	$(2)(3)(11)^2$
27362217255701	f_{-2}	18	-19	$(11)^2$
39112346819681	f_{-9}	9	2	$(2)(2^2)(11)^2$
720826508942753	f_{-9}	15	4	$(2)^2(2^2)(11)^2$

TABLEAU 4. Données pour les sept corps quadratiques réels ayant 11-rang égal à 2.

Le second est conçu sur le modèle « maître-esclave ». Le programme-maître lit dans les fichiers les discriminants et les distribue sur différentes machines. Le programme-esclave, exécuté sur ces machines, calcule, à la réception d'un discriminant d, le nombre de classes et le 11-rang du corps quadratique de discriminant d. Il retourne alors au programme-maître les quantités d et le rang. Celui-ci range d dans différents fichiers selon la valeur du rang.

Voici comme fonctionne le programme-esclave. Nous utilisons la procédure `classno` (basée sur l'algorithme de [Shanks 1971] et implémentée dans le système PARI) pour déterminer l'ordre du groupe des classes. Nous construisons ensuite un nombre, inférieur ou égal à 3, de formes quadratiques indépendantes et d'ordre 11.

Enfin la structure du groupe des classes des corps quadratiques imaginaires de discriminants d et de 11-rang égal à 3 a été obtenue, sous PARI-GP, avec la procédure `buchimag` (fondée, ainsi que la procédure `buchreal`, sur l'algorithme sous-exponentiel de Buchmann) ; nous avons examiné, pour chaque tel d, la concordance du nombre de classes obtenu *via* la procédure `classno` avec celui obtenu *via* la procédure `buchimag`.

Dans le cas des corps réels, nous n'avons pas eu recours au calcul distribué. Pour chacun des 811 discriminants retenus, nous avons déterminé la structure du groupe des classes correspondant (au sens restreint) grâce à la procédure `buchreal`.

Nous avons utilisé une implémentation distribuée sur vingt stations de travail Sparc de l'Ecole Normale Supérieure, en adaptant le programme conçu (et utilisé dans [Fermigier 1992]) par Stéfane Fermigier. Les calculs ont nécessité moins d'une semaine.

REMERCIEMENTS

Je tiens à remercier Stéfane Fermigier pour m'avoir permis d'utiliser son programme de calculs distribués (voir le paragraphe 3), et Jean-François Mestre, mon directeur de thèse, pour l'aide considérable et les encouragements qu'il m'a prodigués dans ce travail.

Les diagrammes de cet article ont été realisés à l'aide du programme `diagrams.tex`, conçu par Paul Taylor.

BIBLIOGRAPHIE

[Batut et al. 1992] C. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI-GP*, 1992. Ce manuel fait partie de la distribution du programme, disponible sur le serveur `snekkar.ens.fr`.

[Buell 1987] D. A. Buell, "Class groups of quadratic fields II", *Math. Comp.* **48** (1987), 85–93.

[Chevalley et Weil 1932] C. Chevalley et A. Weil, "Un théorème d'arithmétique sur les courbes algébriques", *Comptes R. Acad. Sci. Paris* **195** (1932), 570–572.

[Diaz y Diaz 1973] F. Diaz y Diaz, "On some families of imaginary quadratic fields", *Math. Comp.* **32** (1973), 636–650.

[Fermigier 1992] S. Fermigier, "Un exemple de courbe elliptique définie sur $\mathbf{Q}$ de rang ≥ 19", *Comptes R. Acad. Sci. Paris* **315** (1992), 719-722.

[Fricke 1928] R. Fricke, *Lehrbuch der Algebra*, 3.ter Band, Vieweg, Braunschweig, 1928.

[Gonzàlez Rovira 1991] J. Gonzàlez Rovira, "Equations of hyperelliptic modular curves", *Ann. Inst. Fourier*, **41**(4) (1991), 779–795.

[Ling et Oesterlé 1991] S. Ling et J. Oesterlé, "The Shimura subgroup of $J_0(N)$", pp. 171–203 *in Courbes modulaires et courbes de Shimura*, Astérisque **196–197** (1991).

[Llorente et Quer] P. Llorente et J. Quer, Tables (non publié).

[Mestre 1982] J.-F. Mestre, "Groupes de classes d'idéaux non cycliques de corps de nombres", *Séminaire de Théorie des Nombres de Paris* (1982), 189–200.

[Mestre 1983] J.-F. Mestre, "Courbes elliptiques et groupes de classes de certains corps quadratiques", *J. reine angew. Math.* **343** (1983), 23–35.

[Mestre 1992] J.-F. Mestre, "Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3", *Comptes R. Acad. Sci. Paris* **315** (1992), 371–374.

[Quer 1987] J. Quer, "Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12", *Comptes R. Acad. Sci. Paris* **305** (1987), 215-218.

[Schoof 1983] R. Schoof, "Class groups of complex quadratic fields", *Math. Comp.* **43** (1983), 295–302.

[Shanks 1971] D. Shanks, "Class number, a theory of factorisation and genera", pp. 415–440 *in* 1969 *Number Theory Institute*, *Proc. Sympos. Pure Math.* **20**, Amer. Math. Soc., Providence, RI, 1971.

[Shanks 1972] D. Shanks, "A quadratic field of prime discriminant requiring three generators for its class group, and related theory", *Acta Arithm.* **21** (1972), 71–87.

[Solderitsch 1977] J. J. Solderitsch, "Quadratic fields with special class groups", Thesis, Lehigh University, 1977.

Franck Leprévost, Université Paris 7, Département de Mathématiques, Tour 45-55, 5e étage, 2 place Jussieu, 75252 Paris Cedex 05, France (leprevot@mathp7.jussieu.fr)

Received April 7, 1993 ; accepted in revised form August 31