

# SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

**Points rationnels des courbes modulaires  $X_0(N)$**

*Séminaire N. Bourbaki*, 1979, exp. n° 511, p. 89-100

[http://www.numdam.org/item?id=SB\\_1977-1978\\_\\_20\\_\\_89\\_0](http://www.numdam.org/item?id=SB_1977-1978__20__89_0)

© Association des collaborateurs de Nicolas Bourbaki, 1979, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

POINTS RATIONNELS DES COURBES MODULAIRES  $X_0(N)$

[d'après Barry MAZUR [3], [4], [5]]

par Jean-Pierre SERRE

Le présent exposé fait suite à ceux de 1970 et 1975 ([8], [6]). On conserve les notations de [6]. En particulier :

$\bar{\mathbb{Q}}$  est une clôture algébrique de  $\mathbb{Q}$  ;

$N$  est un nombre premier ;

$Y_0(N)$  est la courbe algébrique sur  $\mathbb{Q}$  dont les points paramètrent les couples  $(E, A)$  formés d'une courbe elliptique  $E$  et d'un sous-groupe  $A$  d'ordre  $N$  de  $E$  ; on a

$$Y_0(N)(\mathbb{C}) = \{z \mid \text{Im}(z) > 0\} / \Gamma_0(N) ;$$

$X_0(N)$  est la courbe projective obtenue en compactifiant  $Y_0(N)$  par adjonction des " pointes "  $0$  et  $\infty$  (qui correspondent à des couples  $(E, A)$  dégénérés, cf. [1]) ; son corps des fonctions est  $\mathbb{Q}(j, j_N)$ , où  $j = j(z)$  est l'invariant modulaire usuel, et  $j_N(z) = j(-1/Nz) = j(Nz)$  ;

$w$  est l'involution canonique de  $X_0(N)$  ; elle échange les pointes  $0$  et  $\infty$ , ainsi que les fonctions  $j$  et  $j_N$ .

§ 1. Résultats

Le plus important est le suivant ([5], th. 1) :

THÉOREME 1.- Si le nombre premier  $N$  n'appartient pas à l'ensemble

$$\mathfrak{S} = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\} ,$$

la courbe modulaire  $Y_0(N)$  n'a aucun point rationnel sur  $\mathbb{Q}$ .

Vu la propriété universelle de  $Y_0(N)$ , ceci équivaut à :

THÉOREME 1'.- Soient  $E$  une courbe elliptique sur  $\mathbb{Q}$  et  $A$  un sous-groupe d'ordre  $N$  de  $E$  rationnel sur  $\mathbb{Q}$ . On a alors  $N \in \mathfrak{S}$ .

Remarques.- 1) Dire que  $A$  est rationnel sur  $\mathbb{Q}$  équivaut à dire que  $A$ , considéré comme sous-groupe de  $E(\bar{\mathbb{Q}})$ , est stable par  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ .

2) Lorsque  $N$  appartient à  $\mathfrak{S}$ , la situation est la suivante :

- a) pour  $N = 2, 3, 5, 7, 13$ , la courbe  $Y_0(N)$  est unicursale, donc a une infinité de points rationnels ;
- b) pour  $N = 19, 43, 67, 163$ ,  $Y_0(N)$  a un seul point rationnel, correspondant à une courbe elliptique à multiplications complexes par l'anneau des entiers de  $\mathbb{Q}(\sqrt{-N})$  ;
- c) pour  $N = 17, 37$ ,  $Y_0(N)$  a deux points rationnels, échangés par l'involution  $w$  ;
- d) pour  $N = 11$ ,  $Y_0(N)$  a trois points rationnels ; l'un d'eux est du type b) ; les deux autres sont du type c).

Avant de donner la démonstration des théorèmes 1 et 1' (ce qui sera l'objet du § 2), en voici quelques applications, tirées de [5] :

THÉORÈME 2.- Il existe une constante  $C$  telle que toute courbe elliptique sur  $\mathbb{Q}$  soit  $\mathbb{Q}$ -isogène à au plus  $C$  courbes elliptiques (à isomorphisme près).

Cela résulte du th. 1 et d'un théorème de Manin (cf. [8]).

THÉORÈME 3 ([3], [4]).- Si une courbe elliptique sur  $\mathbb{Q}$  contient un point rationnel d'ordre premier  $N$ , on a  $N \leq 7$ .

En effet, d'après le th. 1', il suffit de prouver que  $N$  est différent de 11, 13, 17, 19, 37, 43, 67, 163, ce qui est connu (voir par exemple [2]).

Compte tenu du th. IV.1.2 de [2], le th. 3 entraîne :

THÉORÈME 4.- Soient  $E$  une courbe elliptique sur  $\mathbb{Q}$ , et  $E_{\text{tor}}(\mathbb{Q})$  le sous-groupe de torsion de  $E(\mathbb{Q})$ . Alors  $E_{\text{tor}}(\mathbb{Q})$  est isomorphe à l'un des groupes suivants :

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & (m \leq 10 \text{ et } m = 12) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & (m \leq 4). \end{array}$$

Ces quinze groupes interviennent effectivement : les courbes modulaires correspondantes sont unicursales, cf. [2], p. 217.

Le th. 3, combiné à la prop. 21 de [9], entraîne :

THÉORÈME 5.- Soit  $E$  une courbe elliptique sur  $\mathbb{Q}$ . Si  $E$  est semi-stable, et si  $N \geq 11$ , le groupe de Galois des points de  $N$ -division de  $E$  est isomorphe à  $GL_2(\mathbb{F}_N)$ .

L'hypothèse de semi-stabilité signifie que le conducteur de  $E$  est sans facteur carré, ou encore que l'on peut représenter  $E$  comme une cubique plane dont toutes les réductions modulo  $p$  sont non singulières ou ont un point double à tangentes distinctes.

Questions

- 1) Le th. 2 est-il vrai avec  $C = 8$  ?
- 2) Le th. 5 reste-t-il valable si l'on remplace les hypothèses  
 " E est semi-stable " et "  $N \geq 11$  "  
 par  
 " E n'a pas de multiplications complexes " et "  $N \geq 41$  " ?
- 3) Si M n'est pas premier, est-il vrai que  $Y_0(M)$  n'a pas de point rationnel en dehors des cas connus  $M = 1, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 21, 27$  ? Compte tenu de [2], et du th. 1, il suffirait de traiter les cinq cas suivants :  
 $M = 3.13, 5.13, 7.13, 13^2$  et  $5^3$ .
- 4) Pour tout corps de nombres K, existe-t-il un ensemble fini  $S_K$  de nombres premiers tel que, si  $N \notin S_K$ , la courbe  $Y_0(N)$  n'ait aucun point rationnel sur K, à part ceux provenant des courbes à multiplications complexes ? Lorsque K est quadratique imaginaire, on trouvera dans [5] un résultat partiel dans cette direction, basé sur un théorème de Goldfeld.

§ 2. Démonstration des théorèmes 1 et 1'

Soit E une courbe elliptique sur  $\mathbb{Q}$ , munie d'un sous-groupe A rationnel sur  $\mathbb{Q}$ , d'ordre N. Il nous faut montrer que N appartient à l'ensemble  $\mathcal{S}$  du th. 1.

a) Propriétés de bonne réduction

PROPOSITION 1.- Supposons N différent de 2, 3, 5, 7, 13. Alors E a potentiellement bonne réduction en tout nombre premier  $p \neq 2, N$ .

Remarques.- 1) Dire que E a potentiellement bonne réduction en p signifie (cf. [10]) qu'il existe une extension finie du corps p-adique  $\mathbb{Q}_p$  sur laquelle E acquiert bonne réduction, ou encore que l'invariant modulaire  $j(E)$  de E est p-entier.

2) L'hypothèse  $p \neq N$  n'est en fait pas nécessaire, cf. [5]. Il en est de même de  $p \neq 2$ , sauf lorsque  $N = 17$ .

Démonstration

Notons x le point de  $X_0(N)$  associé à (E,A) ; on a  $x \neq 0, \infty$ , puisque x n'est pas une "pointe". Soit J la jacobienne de  $X_0(N)$ , et soit f l'application de  $X_0(N)$  dans J définie par  $f(P) = \text{cl}((P - (\infty)))$ .

L'hypothèse faite sur  $N$  entraîne que  $\dim J \geq 1$ , et que  $f$  est un plongement. Notons  $\pi : J \rightarrow \tilde{J}$  la projection de  $J$  sur son quotient d'Eisenstein  $\tilde{J}$  (cf. [3], [6]) ; soit  $\tilde{f}$  l'application composée

$$X_0(N) \xrightarrow{f} J \xrightarrow{\pi} \tilde{J}.$$

Posons  $S = \text{Spec}(\mathbf{Z}) - \{2, N\} = \text{Spec}(\mathbf{Z}[1/2N])$ . On sait ([1]) que  $X_0(N)$  et  $J$  (donc aussi  $\tilde{J}$ , cf. [10]) ont bonne réduction sur  $S$  (et même sur  $\text{Spec}(\mathbf{Z}) - \{N\}$ ), i.e. se prolongent en des schémas projectifs et lisses sur  $S$ , que nous noterons  $X_0(N)_S$ ,  $J_S$  et  $\tilde{J}_S$ . Les points  $x$ ,  $f(x)$ ,  $\tilde{f}(x)$  s'interprètent comme des S-sections de ces schémas, et l'on peut parler de leurs valeurs  $x_p$ ,  $f(x_p)$ ,  $\tilde{f}(x_p)$  en un nombre premier  $p \neq 2, N$ . Supposons alors que  $E$  n'ait pas potentiellement bonne réduction en  $p$  ; cela équivaut à dire que  $x_p$  est égal à l'une des deux pointes  $0_p$  et  $\infty_p$  de la fibre de  $X_0(N)_S$  en  $p$ . Quitte à remplacer  $x$  par  $w(x)$ , on peut supposer que  $x_p = \infty_p$ , d'où  $\tilde{f}(x_p) = 0$ . Ainsi,  $\tilde{f}(x)$  s'annule en  $p$ . Or  $\tilde{f}(x)$  appartient au groupe  $\tilde{J}(\mathbf{Q})$ , qui est fini ([6], th. 2) ; on en tire, par un argument facile (où l'hypothèse  $p \neq 2$  intervient),  $\tilde{f}(x) = 0$ . On a donc

$$\tilde{f}(x) = \tilde{f}(\infty) \quad \text{et} \quad x_p = \infty_p ;$$

les deux sections  $x$  et  $\infty$  de  $X_0(N)_S$  ont même image par  $\tilde{f}$  et coïncident en  $p$ .

Comme le morphisme  $\tilde{f} : X_0(N)_S \rightarrow \tilde{J}_S$  est non ramifié, au sens de EGA IV.7.3.1 en tout point de la section  $\infty$  ([5], prop. 3.1 - voir Appendice), cela entraîne  $x = \infty$  d'après EGA IV.17.4.7. Cette contradiction établit la prop. 1.

#### b) Action de $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ sur $A$

Cette action est définie par un caractère

$$r : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathbf{F}_N^* = \text{Aut}(A).$$

Du fait que  $\mathbf{F}_N^*$  est abélien,  $r$  se factorise à travers

$$\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})^{\text{ab}} = \text{Gal}(\mathbf{Q}_{\text{cycl}}/\mathbf{Q}),$$

où  $\mathbf{Q}_{\text{cycl}}$  désigne le corps obtenu par adjonction à  $\mathbf{Q}$  de toutes les racines de l'unité. On a

$$\text{Gal}(\mathbf{Q}_{\text{cycl}}/\mathbf{Q}) = \prod_p \mathbf{Z}_p^* ;$$

si l'on note  $r_p : \mathbf{Z}_p^* \rightarrow \mathbf{F}_N^*$  la restriction de  $r$  à  $\mathbf{Z}_p^*$ , on a  $r_p = 1$  pour presque tout  $p$ , et

$$r = \prod_p r_p.$$

PROPOSITION 2.- i) Si  $p \neq N$ , le caractère  $r_p$  est d'ordre 1, 2, 3, 4 ou 6.

ii) Soit  $\chi$  le caractère canonique  $\mathbb{Z}_N^* \rightarrow \mathbb{F}_N^*$ . Il existe un entier  $e$ , égal à 1, 2, 3, 4 ou 6, tel que

$$(*) \quad (r_N)^e = \chi^c, \quad \text{avec } 0 \leq c \leq e.$$

Le caractère  $\chi$  est celui qui donne l'action de  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  sur le groupe  $\mu_N$  des racines  $N$ -ièmes de l'unité.

Démonstration de i)

Du fait que  $r_p$  ne dépend que de l'action du groupe d'inertie en  $p$ , la question est locale. Si  $j(E)$  n'est pas  $p$ -entier,  $E$  est une "courbe de Tate" sur  $\mathbb{Q}_p$  (à torsion quadratique près), et la structure d'une telle courbe montre que  $r_p$  est d'ordre  $\leq 2$ . Si  $j(E)$  est  $p$ -entier, il résulte de [10], § 2 (voir aussi [9], n° 5.6) que le groupe d'inertie en  $p$  opère sur les points de  $N$ -division de  $E$  à travers un groupe  $\Phi_p$  d'automorphismes d'une courbe elliptique en caractéristique  $p$ ; un tel groupe  $\Phi_p$  est cyclique d'ordre 1, 2, 3, 4 ou 6, ou non abélien d'ordre 12 ou 24; son image dans  $\mathbb{F}_N^*$  est cyclique d'ordre 1, 2, 3, 4 ou 6.

Démonstration de ii)

L'argument est analogue. Si  $j(E)$  n'est pas  $p$ -entier, la structure des courbes de Tate montre que  $(r_N)^2 = 1$  ou  $\chi^2$ . Si  $j(E)$  est  $p$ -entier, il existe une extension finie de  $\mathbb{Q}_p$ , d'indice de ramification  $e$  égal à 1, 2, 3, 4 ou 6, sur laquelle  $E$  acquiert bonne réduction (du moins si  $N \neq 2, 3$ , ce que l'on peut supposer, la prop. 2 étant triviale pour  $N < 11$ ). En appliquant à cette extension la prop. 10 de [9] (ou le cor. 3.4.4 de [7]), on obtient le fait que  $(r_N)^e$  est de la forme  $\chi^c$ , avec  $0 \leq c \leq e$ .

Remarques.- 1) Le fait que  $(r_p)^{12} = 1$  pour  $p \neq N$  peut aussi se déduire des propriétés de ramification du revêtement  $X_1(N) \rightarrow X_0(N)$ , cf. [5], § 5.

2) Tout caractère  $\mathbb{Z}_N^* \rightarrow \mathbb{F}_N^*$  est une puissance du caractère canonique  $\chi$ , qui est d'ordre  $N-1$ . On a donc  $r_N = \chi^k$ , avec  $k \in \mathbb{Z}/(N-1)\mathbb{Z}$ , et la condition (\*) de ii) peut s'écrire :

$$(*)' \quad ek \equiv c \pmod{(N-1)}, \quad \text{avec } 0 \leq c \leq e.$$

c) Exploitation de a) et b)

On suppose à partir de maintenant que  $N \neq 2, 3, 5, 7, 13$ . Soit  $p$  un nombre premier distinct de 2 et de  $N$ , et décomposons le caractère  $r$  en :

$$r = r_p \varphi_p, \quad \text{où } \varphi_p = r_N \prod_{\ell \neq p, N} r_\ell.$$

Soit  $K_p$  l'extension cyclique de  $\mathbb{Q}$  associée au noyau de  $r_p$ . C'est une sous-extension du corps cyclotomique  $\mathbb{Q}(\mu_p)$  de degré égal à l'ordre de  $r_p$ . Elle est totalement ramifiée en  $p$ . Notons  $\mathfrak{p}$  son unique idéal premier de norme  $p$ .

PROPOSITION 3.- Sur  $K_p$ , la courbe  $E$  a bonne réduction en  $\mathfrak{p}$ .

En effet, la prop. 1 montre que  $E$  a potentiellement bonne réduction en  $\mathfrak{p}$ , et le groupe local  $\mathfrak{G}_\mathfrak{p}$  correspondant ([9], n° 5.6) fixe un point d'ordre  $N$ , donc est réduit à  $\{1\}$ , ce qui entraîne la propriété de bonne réduction cherchée, cf. [10], § 2.

On peut donc parler de la réduction mod.  $\mathfrak{p}$  de  $E$ ; c'est une courbe elliptique sur  $\mathbb{F}_p$ . Notons  $a_p$  la trace de son endomorphisme de Frobenius. On a l'inégalité de Hasse :

$$(**) \quad |a_p| \leq 2\sqrt{p}$$

et de plus :

PROPOSITION 4.- 
$$a_p \equiv \varphi_p(p) + p\varphi_p(p)^{-1} \pmod{N}.$$

(On identifie  $\varphi_p$  à un caractère de  $\prod_{\ell \neq p} \mathbb{Z}_\ell^*$ , ce qui donne un sens à  $\varphi_p(p)$ .)

Comme  $\varphi_p(p) = r_N(p) \prod_{\ell \neq p, N} r_\ell(p)$ , et  $r_\ell(p)^{12} = 1$  pour  $\ell \neq p, N$ , on en déduit :

COROLLAIRE.- Avec les notations de (\*)', on a

$$(***) \quad a_p \equiv \omega_p p^k + \omega_p^{-1} p^{1-k} \pmod{N},$$

où  $\omega_p \in \mathbb{F}_N^*$  est tel que  $\omega_p^{12} = 1$ .

Démonstration de la prop. 4

Soit  $G \subset \text{GL}_2(\mathbb{F}_N)$  le groupe de Galois de l'extension de  $K_p$  obtenu par adjonction des points de  $N$ -division de  $E$ . Vu la prop. 3, cette extension est non ramifiée en  $\mathfrak{p}$ . Soit  $\sigma_\mathfrak{p} \in G$  l'élément de Frobenius correspondant. On sait que

$$\text{Tr}(\sigma_\mathfrak{p}) \equiv a_p \pmod{N}.$$

D'autre part,  $\sigma_\mathfrak{p}$  agit sur  $A$  par homothétie de rapport  $\varphi_p(p)$ . L'une des valeurs propres de  $\sigma_\mathfrak{p}$  est donc  $\varphi_p(p)$  et l'autre est  $p\varphi_p(p)^{-1}$  puisque  $\det(\sigma_\mathfrak{p}) \equiv p \pmod{N}$ . D'où

$$\text{Tr}(\sigma_\mathfrak{p}) \equiv \varphi_p(p) + p\varphi_p(p)^{-1} \pmod{N},$$

ce qui démontre la proposition.

d) Fin de la démonstration

Revenons aux notations de (\*)' : on a  $ek \equiv c \pmod{(N-1)}$ , avec  $e = 1, 2, 3, 4, 6$  et  $0 \leq c \leq e$  ; on en déduit que  $c$  est divisible par  $\text{pgcd}(e, N-1)$ , et le rapport  $c/e$  ne peut prendre que les valeurs suivantes :

$$c/e = 0 \text{ ou } 1$$

$$c/e = 1/3 \text{ ou } 2/3 \text{ (si } e = 3 \text{ ou } 6, \text{ et } 3 \nmid N-1)$$

$$c/e = 1/2 \text{ (si } e = 4 \text{ et } 4 \nmid N-1).$$

(Dans [5], § 5, Mazur remarque que ces cinq valeurs correspondent aux cinq possibilités de [6], th. 6 ; nous n'utiliserons pas ce fait.)

Nous allons examiner successivement ces différents cas :

d<sub>1</sub>) Le cas  $c/e = 0$  ou  $1$

Soient  $f_{i,p}(X)$ ,  $1 \leq i \leq 4$ , les polynômes suivants :

$$f_{1,p}(X) = X + p + 1 ;$$

$$f_{2,p}(X) = X^2 + (p-1)^2 ;$$

$$f_{3,p}(X) = X^2 + (p+1)X + p^2 - p + 1 ;$$

$$f_{4,p}(X) = X^4 - (p^2 + 4p + 1)X^2 + (p^2 + p + 1)^2 .$$

Lemme 1.- Supposons  $E$  de type  $d_1$ ) . Alors, pour tout  $p \neq 2, N$  , il existe  $i \in \{1, 2, 3, 4\}$  et  $a \in \mathbf{Z}$  tels que  $|a| \leq 2\sqrt{p}$  et  $N \nmid f_{i,p}(a)$  .

Démonstration

Puisque  $c/e = 0$  ou  $1$ , on a  $ek \equiv 0$  ou  $e \pmod{(N-1)}$ , et d'après (\*\*\*), on en déduit

$$a_p \equiv \epsilon_p + \epsilon_p^{-1} p \pmod{N} ,$$

où  $\epsilon_p \in \mathbb{F}_N^*$  est d'ordre  $1, 2, 3, 4, 6$  ou  $12$  . Supposons par exemple que  $\epsilon_p$  soit d'ordre  $3$  ou  $6$ , i.e. que

$$\epsilon_p + \epsilon_p^{-1} \pm 1 \equiv 0 \pmod{N} .$$

En développant le produit  $(a_p - \epsilon_p - \epsilon_p^{-1} p)(a_p - \epsilon_p^{-1} - \epsilon_p p)$ , on voit que

$$a_p^2 \pm (p+1)a_p + p^2 - p + 1 \equiv 0 \pmod{N} ,$$

ce qui montre que  $N$  divise  $f_{3,p}(\pm a_p)$  . D'où le lemme dans ce cas. Lorsque  $\epsilon_p$  est d'ordre  $1$  ou  $2$  (resp.  $4$ , resp.  $12$ ), on utilise le polynôme  $f_{1,p}$  (resp.  $f_{2,p}$ , resp.  $f_{4,p}$ ) .

Il est maintenant facile de conclure. Prenons en effet  $p = 3$ . La condition  $|a| \leq 2\sqrt{p}$  signifie que  $a = 0, \pm 1, \pm 2, \pm 3$ ; les valeurs des  $f_{i,3}(X)$  en ces entiers sont les nombres

$$1, 2, 3, 4, 5, 6, 7; 4, 5, 8, 13; 3, 4, 7, 12, 19, 28; 52, 97, 148, 169.$$

Leurs diviseurs premiers sont  $2, 3, 5, 7, 13, 19, 37, 97$  qui appartiennent tous à  $\mathfrak{S}$ , sauf  $97$ . Pour montrer que  $N$  ne peut pas être égal à  $97$ , on peut, soit invoquer des résultats connus (cf. [2]), soit recommencer le même calcul pour  $p = 5$ ; on trouve alors pour valeurs des polynômes  $f_{i,5}(X)$  les entiers

$$2, 3, 4, 5, 6, 7, 8, 9, 10; 16, 17, 20, 25, 32; 12, 13, 16, 21, 28, 37, 48, 61; 481, 628, 793, 916, 961,$$

et l'on constate que  $97$  ne divise aucun d'eux.

$d_2$ ) Le cas  $c/e = 1/3$  ou  $2/3$  ( $3 \nmid N-1$ )

Soient  $f_{i,p}(X)$ ,  $i = 5, 6$ , les polynômes suivants :

$$f_{5,p}(X) = X^3 - 3pX + p^2 + p;$$

$$f_{6,p}(X) = (X^3 - 3pX)^2 + (p^2 - p)^2.$$

Lemme 2.- Supposons  $E$  de type  $d_2$ ). Alors, pour tout  $p \neq 2, N$ , il existe  $i \in \{5, 6\}$  et  $a \in \mathfrak{Z}$  tels que  $|a| \leq 2\sqrt{p}$  et  $N \mid f_{i,p}(a)$ .

Démonstration

On procède comme pour le lemme 1. On a d'après (iii),

$$a_p \equiv \epsilon_p^h + \epsilon_p^{-1} p^{1-h} \pmod{N},$$

avec  $3h \equiv 1 \pmod{(N-1)}$ , et  $\epsilon_p^{12} = 1$ . D'où :

$$a_p^3 - 3pa_p \equiv \epsilon_p^3 + \epsilon_p^{-3} p^2 \pmod{N}.$$

Si  $\epsilon_p^3$  est d'ordre 1 (resp. 2, resp. 4), cette congruence montre que  $N$  divise  $f_{5,p}(-a_p)$  (resp.  $f_{5,p}(a_p)$ , resp.  $f_{6,p}(a_p)$ ). D'où le lemme.

Comme ci-dessus, on applique le lemme avec  $p = 3$ . Les valeurs de  $f_{5,3}(X)$  et  $f_{6,3}(X)$  pour  $X = 0, \pm 1, \pm 2, \pm 3$  sont :

$$2, 4, 12, 20, 22; 36, 100, 136.$$

Leurs diviseurs premiers sont  $2, 3, 5, 11, 17$ , qui appartiennent tous à  $\mathfrak{S}$ .

$d_3$ ) Le cas  $c/e = 1/2$  ( $4 \nmid N-1$ )

Lemme 3.- Supposons  $E$  de type  $d_3$ ). Alors, pour tout  $p$  tel que  $2 < p < N/4$ , on a  $\left(\frac{p}{N}\right) = -1$ .

Démonstration

On a, d'après (iii),

$$a_p \equiv \epsilon_p^h p^h + \epsilon_p^{-1} p^{1-h} \pmod{N},$$

avec  $2h = 1 + (N-1)/2$  et  $\epsilon_p^{12} = 1$ . D'où :

$$a_p^2 - 2p \equiv (\epsilon_p^2 + \epsilon_p^{-2}) p^{1+(N-1)/2} \pmod{N}.$$

Du fait que 4 ne divise pas  $N-1$ , l'ordre de  $\epsilon_p$  divise 6 et celui de  $\epsilon_p^2$  divise 3. On a donc

$$\epsilon_p^2 + \epsilon_p^{-2} \equiv 2 \text{ ou } -1 \pmod{N}.$$

Supposons alors que  $\left(\frac{p}{N}\right) \equiv p^{(N-1)/2}$  soit égal à 1. Il vient :

$$a_p^2 - 2p \equiv 2p \text{ ou } -p \pmod{N},$$

d'où  $a_p^2 \equiv 4p$  ou  $p \pmod{N}$ . Si en outre on a  $N > 4p$ ,  $N$  est strictement plus grand que  $|a_p^2 - 4p|$  et  $|a_p^2 - p|$ , et la congruence ci-dessus entraîne que  $a_p^2$  est égal à  $4p$  ou à  $p$ , ce qui est absurde. D'où le lemme.

Lemme 4.- Si  $4 \nmid N-1$ , et si  $\left(\frac{p}{N}\right) = -1$  pour tout  $p$  tel que  $2 < p < N/4$ , le nombre de classes du corps  $\mathbb{Q}(\sqrt{-N})$  est égal à 1.

Démonstration

L'hypothèse faite sur  $N$  équivaut à dire que tout idéal entier du corps  $\mathbb{Q}(\sqrt{-N})$  dont la norme est impaire et  $< N/4$  est engendré par un élément de  $\mathbb{Z}$ . Distinguons alors deux cas :

$\alpha$ )  $N \equiv 3 \pmod{8}$

On a  $\left(\frac{2}{N}\right) = -1$ , de sorte que tout idéal entier de  $\mathbb{Q}(\sqrt{-N})$  de norme  $< N/4$  est principal. D'après le théorème de Minkowski, cela entraîne que le nombre de classes du corps est 1.

$\beta$ )  $N \equiv -1 \pmod{8}$

Nous allons voir que ce cas est impossible ( $N$  étant supposé  $> 7$ ). Posons en effet  $x = (1 + \sqrt{-N})/2$  si  $N \equiv 7 \pmod{16}$ , et  $x = (3 + \sqrt{-N})/2$  si  $N \equiv -1 \pmod{16}$ . On vérifie que la norme de  $x$  est de la forme  $2m$ , avec  $m$  impair,  $1 < m < N/4$ . Il en résulte, d'après ce qui a été vu plus haut, que l'idéal  $(x)$  est produit d'un idéal de norme 2 par un idéal  $(a)$  engendré par un élément  $a$  de  $\mathbb{Z}$ , avec  $a > 1$ . L'élément  $x$  est donc divisible par  $a$ , ce qui est absurde puisque  $\{1, x\}$  est une base de l'anneau des entiers de  $\mathbb{Q}(\sqrt{-N})$ .

Une fois les lemmes 3 et 4 démontrés, on n'a plus qu'à appliquer le théorème de Heegner-Stark-Baker (cf. [11]) pour conclure que  $N$  est égal à 11, 19, 43, 67 ou 163 ; cela achève la démonstration des théorèmes 1 et 1' .

Remarque.- La démonstration ci-dessus se simplifie notablement si l'on n'a en vue que les th. 3, 4, 5 : les cas  $d_2$ ) et  $d_3$ ) n'interviennent pas. Par exemple, dans le cas du th. 3, on suppose que  $E$  a un point rationnel d'ordre  $N$ , i.e. que le caractère  $r$  est trivial. La prop. 3 montre alors que  $E$  a bonne réduction en tout  $p \neq 2, N$  d'où le fait que  $N$  divise  $p + 1 - a_p$  (cf. prop. 4) ; or c'est absurde si  $p = 3$ , car  $p + 1 - a_p$  est compris entre 1 et 7. On a donc  $N \in \{2, 3, 5, 7, 13\}$  et le cas  $N = 13$  est exclu par un théorème de Blass-Mazur-Tate (voir [2]). D'où  $N \leq 7$ .

### Appendice

Il s'agit de prouver le résultat suivant, utilisé dans la démonstration de la prop. 1 :

THÉORÈME.- Le morphisme  $\tilde{f} : X_0(N)_S \rightarrow \tilde{J}_S$  est non ramifié en tout point de la section  $\infty$ .

Rappelons que  $S = \text{Spec}(\mathbb{Z}) - \{2, N\}$ .

Soit  $B$  le noyau de  $\pi : J \rightarrow \tilde{J}$  ; c'est une sous-variété abélienne de  $J$ . Puisque  $J$  a bonne réduction sur  $S$ , il en est de même de  $B$  ; notons  $B_S$  son modèle de Néron. L'injection  $B \rightarrow J$  se prolonge en un morphisme  $B_S \rightarrow J_S$  dont l'image est l'adhérence  $\bar{B}$  de  $B$  dans  $J_S$ . Raynaud et Mazur ont démontré que le morphisme  $B_S \rightarrow \bar{B}$  ainsi défini est un isomorphisme, de sorte que  $\tilde{J}_S$  s'identifie au quotient  $J_S/B_S$ , et que le morphisme  $\pi : J_S \rightarrow \tilde{J}_S$  est lisse ; la démonstration utilise le th. 3.3.3 de [7], appliqué à un sous-schéma en groupes fini convenable de  $B_S$  (pour plus de détails, voir [5], § 1) ; le fait que  $\text{Spec}(S)$  ne contienne pas  $p = 2$  est ici essentiel.

Supposons maintenant que  $\tilde{f}$  soit ramifié en un point de la section  $\infty$ , dont l'image dans  $S$  est le nombre premier  $p$ . Si l'on convient de noter par un indice  $p$  les fibres en  $p$ , cela signifie que l'application tangente en  $\infty_p$  à  $\tilde{f}_p : X_0(N)_p \rightarrow \tilde{J}_p$  est nulle. Cette propriété peut se reformuler en termes de formes différentielles (i.e. de formes modulaires de poids 2) :

Notons  $\Omega_p$  (resp.  $\tilde{\Omega}_p$ ) l'espace des formes invariants sur  $J_p$  (resp.

sur  $\tilde{J}_p$  ) ; du fait que  $J_p \rightarrow \tilde{J}_p$  est lisse, on peut identifier  $\tilde{\Omega}_p$  à un sous-espace de  $\Omega_p$ , qui lui-même s'identifie à l'espace des formes de première espèce sur  $X_0(N)_p$ . Si  $\omega \in \Omega_p$ , on développe  $\omega$  au voisinage de  $\infty_p$  à la manière habituelle (qui garde un sens en caractéristique  $p$ , on le sait) :

$$\omega = (a_1(\omega)q + \dots + a_n(\omega)q^n + \dots) \frac{dq}{q}.$$

Le fait que la différentielle de  $\tilde{f}_p$  soit nulle en  $\infty_p$  se traduit par la propriété :

$$a_1(\omega) = 0 \quad \text{pour tout } \omega \in \tilde{\Omega}_p.$$

Mais  $\tilde{\Omega}_p$  est non nul (car  $\dim \tilde{J} \geq 1$ ), et stable par les opérateurs de Hecke. Comme ces opérateurs commutent entre eux, ils ont un vecteur propre commun  $\omega \neq 0$  dans  $\tilde{\Omega}_p$ . Des formules standard permettent alors d'exprimer les  $a_n(\omega)$  comme des multiples de  $a_1(\omega)$  ; comme  $a_1(\omega)$  est nul, il en est de même de tous les  $a_n(\omega)$ , et l'on a  $\omega = 0$  ; contradiction !

## BIBLIOGRAPHIE

- [1] P. DELIGNE et M. RAPOPORT - Les schémas de modules de courbes elliptiques,  
Lecture Notes in Math. n° 349, p. 143-316, Springer-Verlag, 1973.
- [2] D. KUBERT - Universal bounds on torsion of elliptic curves, Proc. London Math.  
Soc. (3), 33 (1976), p. 193-237.
- [3] B. MAZUR - Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S.,  
47 (1978), p. 35-193.
- [4] B. MAZUR - Rational points on modular curves, Lecture Notes in Math., n° 601,  
p. 107-148, Springer-Verlag, 1977.
- [5] B. MAZUR - Rational Isogenies of Prime Degree, Invent. Math., 44(1978), 129-162.
- [6] B. MAZUR et J.-P. SERRE - Points rationnels des courbes modulaires  $X_0(N)$ ,  
Séminaire Bourbaki, 27e année, 1974/75, exposé 469, Lecture Notes in Math.  
n° 514, p. 238-255, Springer-Verlag, 1976.
- [7] M. RAYNAUD - Schémas en groupes de type  $(p, \dots, p)$ , Bull. Soc. Math. France,  
102(1974), p. 241-280.
- [8] J.-P. SERRE -  $p$ -torsion des courbes elliptiques (d'après Y. MANIN), Séminaire  
Bourbaki, 22e année, 1969/70, exposé 380, Lecture Notes in Math. n° 180,  
p. 281-294, Springer-Verlag, 1971.
- [9] J.-P. SERRE - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,  
Invent. Math., 15 (1972), p. 259-331.
- [10] J.-P. SERRE and J. TATE - Good reduction of abelian varieties, Ann. of Math.,  
88 (1968), 492-517.
- [11] H. M. STARK - A complete determination of the complex quadratic fields of  
class-number one, Mich. Math. J., 14 (1967), p. 1-27.