

DIDIER NORDON

Points rationnels de la cubique $y^2 = x^3 - Ax - B$ dans les corps p -adiques

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. n° 4, p. 1-12

http://www.numdam.org/item?id=STNB_1970-1971____A4_0

© Université Bordeaux 1, 1970-1971, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Bordeaux 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 DE LA CUBIQUE $y^2 = x^3 - Ax - B$
DANS LES CORPS $\mathbb{P}$ -ADIQUES

par

Didier NORDON

-:-:-

Cet exposé est une reproduction à peine modifiée d'une partie d'un article de M^{lle} Elisabeth Lutz [sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathbb{P}$ -adiques, J. Reine angew. Math., 1937, n° 177].

Soit k un corps. A toute courbe algébrique définie sur k (c'est-à-dire dont l'équation est à coefficients dans k) on associe un entier positif, son genre. On appelle courbe elliptique définie sur k une courbe projective, sans point multiple, de genre 1, définie sur k et ayant au moins un point à coordonnées dans k . On montre qu'une telle courbe est isomorphe (en un sens qu'on peut préciser) à une cubique sans point multiple admettant le point à l'infini sur Oy comme point d'inflexion, la droite de l'infini étant tangente d'inflexion. Si la caractéristique de k est différente de 2 et de 3, en changeant de coordonnées on peut donner à une telle cubique une équation de la forme

$$y^2 = x^3 - Ax - B \quad , \quad A, B \in k \quad , \quad \Delta = 4A^3 - 27B^2 \neq 0 .$$

On appelle point rationnel d'une courbe définie sur k tout point de la courbe dont les coordonnées sont dans k , ou bien le point à l'infini de la courbe.

On sait (nous le verrons plus loin) que l'ensemble des points rationnels d'une cubique de genre 1, $y^2 = x^3 - Ax - B$, $A, B \in k$, $\Delta \neq 0$ peut être muni d'une structure de groupe abélien, qu'on notera G .

OBJET DE L'EXPOSE

Il s'agit d'étudier le groupe des points rationnels d'une telle cubique et plus spécialement d'en rechercher les points d'ordre fini dans le cas où le corps k est un corps $\mathbb{P}$ -adique, $k_{\mathbb{P}}$.

Un corps $\mathbb{P}$ -adique est une extension d'un corps p -adique usuel ($p \in \mathbb{Z}$, p premier). Si $[k_{\mathbb{P}} : k_p] = d$, on a $d = ef$ où e est l'indice de ramification de p dans $k_{\mathbb{P}}$ et où $N(\mathbb{P}) = p^f$. On désignera par π une uniformisante : $\mathbb{P} = (\pi)$ et par φ la valuation $\mathbb{P}$ -adique dans $k_{\mathbb{P}}$ déterminée par exemple par la condition $\varphi(\pi) = w < 1$. Le corps résiduel d'un tel corps est fini.

LE GROUPE G DES POINTS RATIONNELS

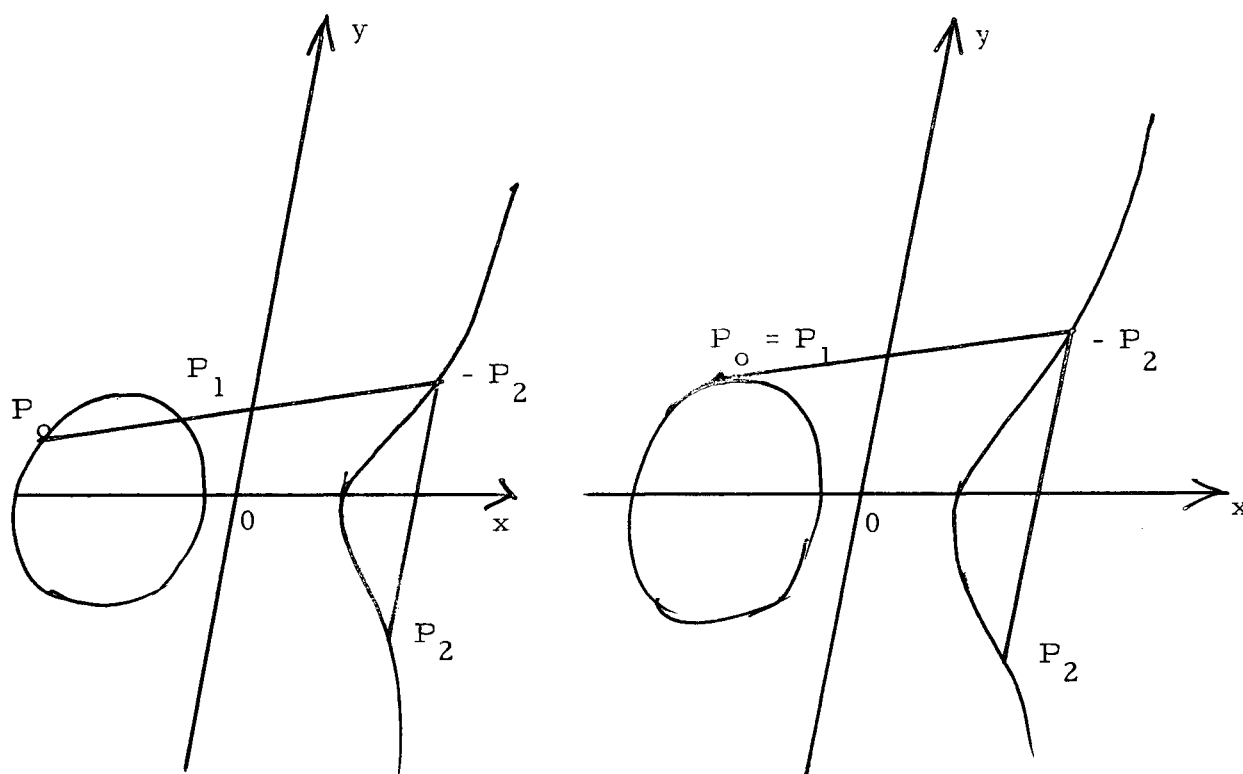
Soit la cubique de genre 1, $y^2 = x^3 - Ax - B$, A et B entiers de $k_{\mathbb{P}}$, $\Delta \neq 0$. A deux points rationnels $P_0(x_0, y_0)$ et $P_1(x_1, y_1)$ on fait correspondre le point $P_2(x_2, y_2)$ symétrique par rapport à Ox du troisième point d'intersection de la droite P_0P_1 avec la cubique et on écrit $P_2 = P_0 + P_1$. On trouve facilement les coordonnées de P_2 en fonction de celles de P_0 et P_1 ; en particulier

$$x_2 = \left(\frac{y_1 - y_0}{x_1 - x_0} \right)^2 - (x_1 + x_0)$$

Si P_1 et P_0 sont confondus, on prend au lieu de la droite P_0P_1 la tangente en P_0 à la cubique et on écrit $2P_0 = P_2$ avec

$$x_2 = \left(\frac{3x_0^2 - A}{2y_0} \right)^2 - 2x_0.$$

Le point $-P_0$ est le point de coordonnées $(x_0, -y_0)$ et le point à l'infini de la courbe étant considéré comme point rationnel est l'unité du groupe G .



L'ENTIER $n(P)$

LEMME 1. Tout point rationnel P sur la courbe a des coordonnées de la
forme $(\xi \pi^{-2n}, \eta \pi^{-3n})$ où $n \in \mathbb{N}$, ξ et η sont des entiers de k_P , premiers
à P si $n > 0$.

Démonstration. Soit $P(x, y)$ un point rationnel. Si x est un entier P -adique, y l'est aussi. Si $\varphi(x) > 1$

$$\varphi(x^3) = [\varphi(x)]^3 > \varphi(Ax) \quad \text{et} \quad \varphi(x^3) > \varphi(B),$$

$$\text{donc} \quad \varphi(y^2) = \varphi(x^3 - Ax - B) = \varphi(x^3);$$

en ce point, nous avons donc

$$\varphi(x) = w^{-2n}, \quad \varphi(y) = w^{-3n}, \quad n > 0,$$

de sorte que les coordonnées (x, y) sont bien de la forme

$$x = \xi \pi^{-2n}, \quad y = \eta \pi^{-3n}$$

avec ξ et η entiers premiers à P ; ξ et η satisfont l'équation
 $\eta^2 = \xi^3 - A\xi \pi^{4n} - B \pi^{6n}.$

A tout point P correspond ainsi un entier $n \geq 0$ qu'on désignera par $n(P)$; si P est le point à l'infini, on pose $n(P) = \infty$.

POINTS TELS QUE $n(P) \geq m$

Soit m un entier > 0 quelconque. Alors :

THEOREME 1. Les points P pour lesquels $n(P) \geq m$ forment un sous-groupe G_m de G , d'indice fini dans G .

Démontrons d'abord le lemme 2

LEMME 2. Soient deux points rationnels P_0 et P_1 , et $P_2 = P_0 + P_1$. Alors $n(P_2) \geq \min[n(P_0), n(P_1)]$.

Démonstration. Distinguons deux cas

1er cas - $n(P_1) > n(P_0)$, donc $n(P_1) > 0$. Ecrivons la formule d'addition sous la forme

$$x_2 = \frac{x_0 x_1^2 + x_0^2 x_1 - A(x_0 + x_1) - 2B - 2y_0 y_1}{(x_0 - x_1)^2},$$

d'où

$$\varphi(x_2) = \frac{\varphi(x_1^2 x_0)}{\varphi(x_1^2)} = \varphi(x_0)$$

et par suite

$$n(P_0 + P_1) = \min[n(P_0), n(P_1)] \quad \text{si} \quad n(P_0) \neq n(P_1).$$

Nous aurions de même

$$n(P_0 - P_1) = \min[n(P_0), n(P_1)] \quad \text{si} \quad n(P_0) \neq n(P_1).$$

2ème cas - $n(P_1) = n(P_0)$; écrivons $P_0 = P_2 - P_1$; si $n(P_2) \neq n(P_1)$, on a

$$n(P_0) = \min[n(P_2), n(P_1)],$$

donc $n(P_2) \geq n(P_0)$.

On a donc dans tous les cas

$$n(P_2) \geq \min[n(P_0), n(P_1)].$$

De ce lemme résulte évidemment la première partie du théorème 1 :

G_m est un sous-groupe de G .

Pour en démontrer la seconde partie, nous devons examiner à quelles conditions deux points P_0, P_1 de G doivent satisfaire pour que $P_1 - P_0$ soit dans G_m , c'est-à-dire pour que $n(P_1 - P_0) \geq m$; nous pouvons supposer que ni P_0 ni P_1 ne sont dans G_m ; alors, on doit avoir, tout d'abord, $n(P_0) = n(P_1) = n < m$. Soient $(\xi_0 \pi^{-2n}, \eta_0 \pi^{-3n})$ et $(\xi_1 \pi^{-2n}, \eta_1 \pi^{-3n})$ les coordonnées de P_0 et P_1 ,

$$\eta_0^2 = \xi_0^3 - A \xi_0 \pi^{4n} - B \pi^{6n},$$

$$\eta_1^2 = \xi_1^3 - A \xi_1 \pi^{4n} - B \pi^{6n}.$$

Il est clair, d'après la formule d'addition, que la condition nécessaire et suffisante pour que $n(P_1 - P_0) \geq m$, si $n(P_0) = n(P_1) < m$ est

$$\frac{x_1 - x_0}{y_1 + y_0} \equiv 0 \pmod{\mathfrak{p}^m}$$

c'est-à-dire

$$\frac{\xi_1 - \xi_0}{\eta_1 - \eta_0} \equiv 0 \pmod{\mathfrak{p}^{m-n}}.$$

Or on a

$$\frac{\xi_1 - \xi_0}{\eta_1 + \eta_0} = \frac{\eta_1 - \eta_0}{\xi_0^2 + \xi_0 \xi_1 + \xi_1^2 - A \pi^{4n}}.$$

Une condition nécessaire pour que $n(P_1 - P_0) \geq m$ est donc

$$\xi_1 \equiv \xi_0, \quad \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{m-n}}.$$

Cela est même suffisant si $n > 0$ car alors

$$\eta_1 + \eta_0 \equiv 2\eta_0 \not\equiv 0 \pmod{\mathfrak{p}} \quad \text{si } p \neq 2,$$

$$\text{et} \quad \xi_0^2 + \xi_0 \xi_1 + \xi_1^2 - A \pi^{4n} \equiv 3\xi_0^2 \not\equiv 0 \pmod{\mathfrak{p}} \quad \text{si } p \neq 3.$$

On en déduit que $\frac{G_{m-1}}{G_m}$ est un groupe fini si $m > 1$, donc que G_m est d'indice fini dans G_1 .

Il reste à montrer que $\frac{G}{G_1}$ est fini. Cela est une conséquence immédiate du lemme suivant :

LEMME 3. Soit $\mathfrak{p}^R$ la plus haute puissance de $\mathfrak{p}$ qui divise $2(4A^3 - 27B^2)$.
 Soient P_0 et P_1 tels que $n(P_0) = n(P_1) = 0$; alors

$$\left\{ \begin{array}{l} r > R \\ \xi_1 \equiv \xi_0 \pmod{\mathfrak{p}^{r+m}} \\ \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{r+m}} \end{array} \right. \Rightarrow n(P_1 - P_0) \geq m.$$

Démonstration. Supposons en effet

$$n(P_1 - P_0) < m$$

$$\xi_1 \equiv \xi_0 \pmod{\mathfrak{p}^{r+m}}$$

$$\eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{r+m}}.$$

On a, d'après ce qui précède

$$\eta_1 + \eta_0 \equiv 0 \quad \text{et} \quad \xi_0^2 + \xi_0 \xi_1 + \xi_1^2 - A \equiv 0 \pmod{\mathfrak{p}^r}.$$

On en déduit

$$2\eta_0 \equiv 0 \quad \text{et} \quad 3\xi_0^2 - A \equiv 0 \pmod{\mathfrak{p}^r}.$$

Mais on a l'identité

$$4A^3 - 27B^2 = (x^3 - Ax - B) \cdot P(x) + (3x^2 - A) \cdot Q(x)$$

où $P(x) = -18Ax + 27B$ et $Q(x) = 6Ax^2 - 9Bx - 4A^2$

sont des polynômes à coefficients entiers ; en y faisant $x = \xi_0$, on voit donc que

$$2(4A^3 - 27B^2) \equiv 0 \pmod{\mathfrak{p}^r}.$$

Comme on a supposé $4A^3 - 27B^2 \neq 0$, cette dernière congruence entraîne bien $r \leq R$.

Ceci achève la démonstration du théorème 1.

PARAMETRE DE LA COURBE

Nous utilisons le paramétrage suivant

$$x = \frac{1}{t^2}, \quad y = \frac{\varepsilon(t)}{t^3}$$

où $\varepsilon(t)$ est défini par

$$\varepsilon(t) = (1 - At^4 - Bt^6)^{\frac{1}{2}} = 1 + \sum_{\nu=2}^{\infty} \gamma_{\nu} t^{2\nu}$$

avec $\gamma_2 = -\frac{A}{2}$, $\gamma_3 = -\frac{B}{2}$, etc. Il est clair que si $t \equiv 0 \pmod{\mathfrak{p}^m}$ et si la série $\varepsilon(t)$ est convergente, les formules ci-dessus définissent un point P de la courbe, et que ce point appartient à G_m .

Or on sait que dans la série

$$(1+u)^{\frac{1}{2}} = 1 + \frac{1}{2}u - \frac{1}{8}u^2 + \frac{1}{16}u^3 - \dots$$

les dénominateurs des coefficients ne contiennent pas d'autre facteur premier que 2, et que le dénominateur du coefficient de u^v divise 2^{2v} . Il en résulte que

si $p \neq 2$, la série $\varepsilon(t)$ converge dès que $t \equiv 0 \pmod{\mathfrak{p}}$

si $p = 2$, la série $\varepsilon(t)$ converge dès que $t \equiv 0 \pmod{\mathfrak{p}^\mu}$,

μ étant le plus petit entier plus grand que $\frac{e}{2}$; posons $\mu = 1$ pour $p \neq 2$ de sorte que, dans tous les cas, les formules ci-dessus définissent pour $t \equiv 0 \pmod{\mathfrak{p}^\mu}$, un point de G_μ .

Réciproquement, tout point P de G_μ correspond ainsi à une valeur de t , définie par les formules

$$t = \frac{x}{y} \varepsilon$$

$$\varepsilon = \left(1 - \frac{A}{2x} - \frac{B}{3x}\right)^{\frac{1}{2}} = 1 + \sum_{v=2}^{\infty} \gamma_v x^{-v}$$

la série étant convergente pourvu que P appartienne à G_μ .

Ce paramètre met en évidence le nombre $n(P)$ défini plus haut; en effet, $n(P)$ est l'exposant de l'uniformisante π dans la décomposition de t

$$\varphi(t) = n(P) \cdot \varphi(\pi)$$

(φ , rappelons-le, est la valuation $\mathfrak{p}$ -adique).

Notation - Dans toute la suite, nous désignons par α le plus petit entier plus grand que $\frac{e}{4}$ dans le cas $p \neq 2$, et nous posons $\alpha = e$ dans le cas $p = 2$.

STRUCTURE DE G_α

Soient P_0 et P_1 deux points de G_μ , de paramètres respectifs t_0 et t_1 ; posons $\varepsilon_0 = \varepsilon(t_0)$, $\varepsilon_1 = \varepsilon(t_1)$ et calculons le paramètre t_2 du point $P_2 = P_0 + P_1$ en fonction de t_0 et t_1 .

Posons

$$\theta = \sum_{v=2}^{\infty} \gamma_v \frac{t_1^{2v-3} - t_o^{2v-3}}{t_1 - t_o}.$$

Alors

$$\begin{aligned} \frac{y_1 - y_o}{x_1 - x_o} &= \frac{\varepsilon_1 t_o^3 - \varepsilon_o t_1^3}{t_o t_1 (t_o^2 - t_1^2)} = \frac{t_o^3 - t_1^3 + t_o^3 t_1^3 \sum_{v=2}^{\infty} \gamma_v (t_1^{2v-3} - t_o^{2v-3})}{t_o t_1 (t_o^2 - t_1^2)} \\ &= \frac{t_o^2 + t_o t_1 + t_1^2 - t_o^3 t_1^3 \theta}{t_o t_1 (t_o + t_1)}. \end{aligned}$$

La formule d'addition pour x s'écrit alors

$$x_2 = \frac{1}{t_2^2} = \frac{1}{(t_o + t_1)^2} [1 - 2t_o t_1 (t_o^2 + t_o t_1 + t_1^2) \theta + t_o^4 t_1^4 \theta^2].$$

L'ambiguïté de signe pour t_2 se lève en considérant y_2 ; d'où

$$\frac{t_2}{t_o + t_1} = [1 - 2t_o t_1 (t_o^2 + t_o t_1 + t_1^2) \theta + t_o^4 t_1^4 \theta^2]^{-\frac{1}{2}}$$

le second membre représentant le développement en série qui lui correspond au moyen de la formule du binôme, pourvu que ce développement soit convergent ; il en est évidemment ainsi pour $p \neq 2$ car alors θ est entier.

PROPOSITION. G_α est un module sur l'anneau des entiers p -adiques.

Démonstration. Nous allons démontrer la proposition dans le cas $p \neq 2$.

Supposons $n(P_o) \leq n(P_1)$; alors

$$\frac{t_2}{t_o + t_1} \equiv 1 \pmod{\mathfrak{p}^{3n(P_o) + n(P_1)}}.$$

Si P_o et P_1 appartiennent tous deux à G_m , on a donc, a fortiori,

$$t_2 \equiv t_o + t_1 \pmod{\mathfrak{p}^{5m}}$$

et en particulier par récurrence sur ℓ

$$t(\ell P_o) \equiv \ell t(P_o) \pmod{\mathfrak{p}^{5m}}$$

d'où, pour $\ell = p$ et en posant $n(P_o) = n$

$$\frac{t(p P_o)}{p t(P_o)} \equiv 1 \pmod{p^{4n-e}}$$

et par récurrence sur v

$$\frac{t(p^v P_o)}{p^v t(P_o)} \equiv 1 \pmod{p^{4n-e}}$$

donc, enfin, en combinant les résultats ci-dessus

$$\frac{t(\ell P_o)}{\ell t(P_o)} \equiv 1 \pmod{p^{4n-e}}$$

quel que soit ℓ . En particulier, si $4n > e$ et si p^v est la plus haute puissance de p contenue dans ℓ

$$n(\ell P_o) = n(P_o) + v e.$$

De ce qui précède résulte que si P_o appartient à G_α , et si la suite d'entiers ordinaires ℓ_i converge p -adiquement vers un entier p -adique L , les nombres $t(\ell_i P_o)$ convergent p -adiquement vers une certaine valeur de t : le point de la courbe qui correspond à celle-ci est désigné par LP et on voit ainsi que G_α est un module sur l'anneau des entiers p -adiques.

Dans le cas où $p = 2$, on a des résultats un peu moins précis. Supposons que P_o et P_1 appartiennent à G_m avec $m \geq e$; alors $t_2 \equiv t_o + t_1 \pmod{p^{5m-2e}}$.

D'où successivement

$$\begin{aligned} t(\ell P_o) &\equiv \ell t(P_o) \pmod{p^{5m-2e}} \\ \frac{t(2 P_o)}{2 t(P_o)} &\equiv 1 \pmod{p^{4n(P_o)-3e}} \\ \frac{t(\ell P_o)}{\ell t(P_o)} &\equiv 1 \pmod{p^{4n(P_o)-3e}} \end{aligned}$$

et si 2^v est la plus grande puissance de 2 qui divise ℓ

$$n(\ell P_o) = n(P_o) + v e \quad \text{pour } n(P_o) \geq e.$$

D'où, dans ce cas aussi, la proposition.

STRUCTURE DE G_β

Désignons par β un entier $\geq \alpha$. On a alors le théorème suivant :

THEOREME 2. G_β est isomorphe au groupe additif des entiers p -adiques.

Démonstration. Il suffit de montrer que G_β possède une base de $d = ef$ éléments sur l'anneau des entiers p -adiques.

Soit donc $t_i^{(\rho)} \dots t_f^{(\rho)}$ une base de $\frac{p^{\beta+\rho}}{p^{\beta+\rho+1}}$ ($\rho = 0, 1, \dots, e-1$), on a $t_i^{(\rho)} \equiv 0 \pmod{p^{\beta+\rho}}$ ($i = 1, \dots, f$).

Soient $P_i^{(\rho)}$ les points correspondant à ces ef valeurs de t ; soit $t_i^{(\rho+\nu e)}$ la valeur du paramètre t qui correspond au point $P_i^{(\rho+\nu e)} = p^\nu P_i^{(\rho)}$. Soit P_o un point quelconque de G_β , et t_o son paramètre; il existe des entiers $n_i^{(o)}$, bien déterminés mod. p , tels que

$$t_o \equiv \sum_i n_i^{(o)} t_i^{(o)} \pmod{p^{\beta+1}};$$

le point $P_1 = P_o - \sum_{i=1}^f n_i^{(o)} P_i^{(o)}$ appartient à $G_{\beta+1}$; soit t_1 le paramètre de P_1 ; il existe des entiers $n_i^{(1)}$, bien déterminés modulo p tels que

$$t_1 \equiv \sum_i n_i^{(1)} t_i^{(1)} \pmod{p^{\beta+2}};$$

en continuant ainsi, on voit que le point

$$P_n = P_o - \sum_{\nu=0}^{n-1} \sum_i n_i^{(\nu)} P_i^{(\nu)}$$

appartient à $G_{\beta+n}$; d'où

$$P_o = \sum_{\rho=0}^{e-1} \sum_{i=1}^f \left(\sum_{\nu=0}^{\infty} n_i^{(\rho+\nu e)} p^\nu \right) P_i^{(\rho)}$$

expression unique de P_o en fonction des ef points $P_i^{(\rho)}$.

COROLLAIRE. Un point P de G_β ne peut être d'ordre fini dans G ; en particulier, si $e = 1$, un point d'ordre fini dans G est à coordonnées entières.

CAS DE $\mathbb{Q}$

Étudions les points à coordonnées dans $\mathbb{Q}$ de la cubique $y^2 = x^3 - Ax - B$ ($A, B \in \mathbb{Z}$). Ils forment un groupe qui est contenu dans le groupe des solutions p -adiques de la même équation, et cela pour tout p . Un point à coordonnées rationnelles ne peut être d'ordre fini que si x et y sont entiers dans tout corps p -adique, c'est-à-dire s'ils appartiennent à $\mathbb{Z}$. La détermination effective de ces points est fournie par le théorème suivant.

THEOREME 3. Soit $y^2 = x^3 - Ax - B$ une cubique de genre 1, $A, B \in \mathbb{Z}$. Tout point $P(x, y)$ à coordonnées rationnelles d'ordre fini dans le groupe des points rationnels sur la cubique est à coordonnées entières et tel que y^2 soit égal à 0 ou à un diviseur de $4A^3 - 27B^2$.

Démonstration. Le début a déjà été vu. Voyons le second point. Si P est d'ordre fini, il en est de même de $2P$, qui doit donc être aussi à coordonnées entières, s'il n'est à l'infini ; ce dernier cas se présente si $y = 0$; s'il n'en est pas ainsi il est à coordonnées entières si et seulement si

$$3x^2 - A \equiv 0 \pmod{2y}.$$

Or

$$(3x^2 - A)^2 (3x^2 - 4A) \equiv -4A^3 + 27B^2 \pmod{x^3 - Ax - B}$$

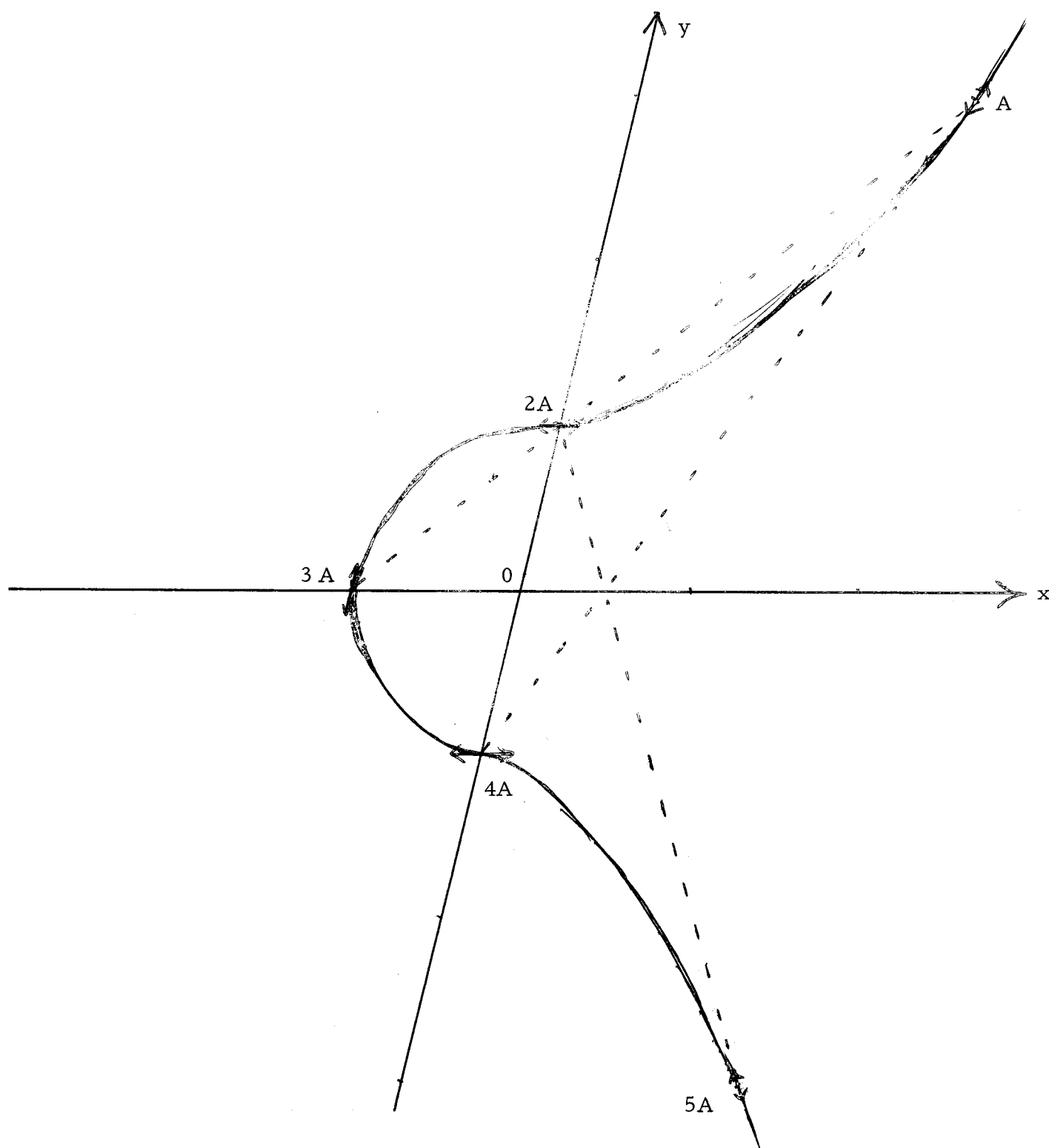
et par conséquent, dans le cas présent

$$-4A^3 + 27B^2 \equiv 0 \pmod{y^2}$$

ce qu'il fallait démontrer.

Exemple : points rationnels d'ordre fini sur la cubique $y^2 = x^3 + 1$.

Dans ce cas, $\Delta = 27$ et les seuls points rationnels d'ordre fini ont une ordonnée égale à 0, ± 1 , ± 3 . D'où le groupe des points d'ordre fini, qui a 6 éléments. Le point A est d'ordre 6.



Didier NORDON
U. E. R. de Mathématiques
et d'Informatique
Université de Bordeaux 1
351, cours de la Libération
33 - TALENCE