SUR LES PROPRIÉTÉS ARITHMÉTIQUES DES CUBIQUES PLANES DU PREMIER GENRE.

Par

TRYGVE NAGELL

à OSLO.

I.

Généralités.

1. *Introduction.* Le point (x, y, z) de la courbe algébrique en coordonnées homogènes $f(x, y, z) = 0$ est appelé point rationnel quand les coordonnées sont proportionnelles à trois nombres rationnels. Les points rationnels à l'infini sont donnés par l'équation $f(x, y, 0) = 0$.

Deux courbes algébriques à coefficients rationnels sont dites *équivalentes* quand elles sont reliées par une *transformation birationnelle à coefficients rationnels.* Les courbes équivalentes ont le même genre.

Dans l'étude des points rationnels des courbes algébriques, c'est plutôt le *genre* que le degré qui intervient. Le problème de trouver les points rationnels d'une courbe algébrique unicursale est complètement résolu.[1] Au contraire, les résultats sur les points rationnels des courbes de genre $\geqq 1$ sont très incomplets. Les résultats les plus importants sur les courbes du premier genre sont dus à POINCARÉ[2], à HURWITZ[3] et à M. MORDELL[4]. Poincaré a montré qu'une courbe

[1] Voir D. HILBERT et A. HURWITZ, »*Ueber die diophantischen Gleichungen vom Geschlecht Null*», *Acta Mathematica*, t. 14, p. 217 (1890).

[2] H. POINCARÉ: »*Sur les propriétés arithmétiques des courbes algébriques*», *Journal de Mathématiques*, 5e série, t. 17, p. 161 (1901).

[3] A. HURWITZ: »*Ueber ternäre diophantische Gleichungen dritten Grades*», *Vierteljahrschrift d. Naturf. Gesellschaft in Zürich*, t. 62, p. 207 (1917).

[4] L. J. MORDELL, »*On the rational solutions of the indeterminate equations of the third and fourth degrees*», *Proc. of the Cambridge Philos. Soc.*, vol. XXI, p. 179 (1922).

Pour la Bibliographie détaillée de notre sujet voir L. E. DICKSON, *History of the theory of numbers*, vol. II, Washington 1920.

Voir aussi ma monographie »*L'Analyse Indéterminée de degré supérieur*», qui paraîtra prochainement dans la Collection »*Mémorial des Sciences Mathématiques*».

du premier genre qui admet un point rationnel, est équivalente à une cubique. Ainsi on peut se borner à considérer les cubiques. Cependant, dans le cas général, nous n'avons pas de moyen pour reconnaître si une courbe du premier genre admet un point rationnel ou non, même dans le cas d'une cubique.

Le but des pages suivantes est de préciser et compléter les recherches de Poincaré et Hurwitz et développer les premiers éléments d'une théorie des points rationnels des cubiques planes du premier genre.

Dans ce qui suit nous entendons par nombre rationnel un nombre d'un domaine de rationalité quelconque donné.

2. *La représentation paramétrique des cubiques.* Soit donnée la cubique plane du premier genre à coefficients rationnels $f(x,y)=0$. Pour étudier la distribution des points rationnels sur la courbe il est indispensable d'introduire les fonctions elliptiques représentant paramétriquement la courbe. Nous allons montrer comment on peut choisir cette représentation d'une manière commode. Il est facile d'établir la proposition suivante:

Si la cubique admet un point rationnel, elle est toujours équivalente à une autre cubique de la forme

$$y^2=4x^3-g_2x-g_3, \tag{1}$$

à coefficients rationnels g_2 et g_3. Soit en effet P_0 un point rationnel de la cubique. La tangente à la cubique en ce point rencontre la cubique en un second point P_1 qui est évidemment aussi rationnel.[1] (Si P_0 est un point d'inflexion les deux points coincident.) Si P_1 est pris pour origine des coordonnées, l'équation de la cubique peut être ramenée, par une transformation linéaire à coefficients rationnels, à la forme

$$\varphi_3(x,y)+\varphi_2(x,y)+\varphi_1(x,y)=0,$$

$\varphi_i(x,y)$ désignant un polynôme homogène de degré i à coefficients rationnels. Coupons par la sécante $y=tx$; x est déterminé par l'équation du second degré

$$x^2\varphi_3(1,t)+x\varphi_2(1,t)+\varphi_1(1,t)=0,$$

d'où l'on tire

$$x=\frac{-\varphi_2(1,t)\pm\sqrt{R(t)}}{2\varphi_3(1,t)},\quad y=tx,$$

[1] En effet, si deux des racines d'une équation cubique à coefficients rationnels sont rationnelles, la troisième racine est aussi rationnelle.

$R(t)$ désignant le polynome $\varphi_2^2(1,t)-4\varphi_1(1,t)\varphi_3(1,t)$, qui est en général du quatrième degré. Les zéros de ce polynôme sont précisément les coefficients angulaires des tangentes à la cubique qui passent par l'origine. Nous connaissons *a priori* un zéro de ce polynome, le coefficient angulaire t_0 de la droite qui joint l'origine au point P_0; ce nombre t_0 est rationnel. (Si $t_0=\infty$ le polynôme est du troisième degré.) En posant $t=t_0+\frac{1}{\tau}$, il vient

$$\sqrt{R(t)}=\tau^{-2}\cdot\sqrt{R_1(\tau)},$$

le polynôme $R_1(\tau)$ n'étant plus que du troisième degré. Or, on peut, par une transformation linéaire à coefficients rationnels, ramener ce polynôme à la forme

$$c^2(4x^3-g_2x-g_3),$$

les nombres c, g_2 et g_3 étant rationnels. Donc, la cubique $f(x,y)=0$ et la cubique (1) sont équivalentes. A chaque point rationnel de $f(x,y)=0$ correspond un et un seul point rationnel de la cubique (1), et inversement. Le point P_0 correspond au point d'inflexion à l'infini de la courbe (1). Il suffit ainsi de considérer les cubiques de la forme (1).

La courbe (1) étant du premier genre, nous avons la représentation paramétrique par la fonction $\wp(u)$ correspondante,

$$x=\wp(u),\quad y=\wp'(u).$$

Pour la cubique $f(x,y)=0$ nous aurons la représentation

$$x=F(\wp(u),\wp'(u)),\quad y=G(\wp(u),\wp'(u)),$$

$F(\xi,\eta)$ et $G(\xi,\eta)$ étant des fonctions rationnelles de ξ et η à coefficients rationnels. Le point d'inflexion de la cubique (1), ainsi que le point P_0 de $f(x,y)=0$ correspondent à l'argument $u=0$.

Dans la suite la représentation paramétrique est toujours choisie de cette manière.

Il résulte de la théorie générale des fonctions elliptiques:

Pour que les deux cubiques du premier genre

$$4x^3-g_2x-g_3=y^2$$

et

$$4x^3-G_2x-G_3=y^2$$

soient équivalentes, il faut et il suffit qu'on ait $G_2 = c^4 g_2$ *et* $G_3 = c^6 g_3$, *c étant un nombre rationnel, différent de zéro.*

Le problème de l'équivalence est ainsi complètement résolu pour les cubiques qui admettent un point rationnel.

3. *Les arguments elliptiques des points rationnels.* Soit u_1 l'argument d'un point rationnel. Alors, en vertu de la formule d'addition de la fonction $\wp(u)$, tous les points d'arguments mu_1 sont aussi rationnels, m étant un nombre entier quelconque. Pour que ces points soient tous distincts il faut et il suffit que u_1 ne soit pas commensurable avec une période. Dans ce cas on aura une infinité de points rationnels. Or, on n'a pas de méthode générale pour reconnaître si l'argument d'un point donné (x, y) est commensurable avec une période ou non. En général, si on a les n points rationnels d'arguments $u_1, u_2, \ldots, u_n$, tous les points d'arguments

$$m_1 u_1 + m_2 u_2 + \cdots + m_n u_n, \tag{2}$$

les m_i étant des nombres entiers quelconques, sont rationnels. Dans le cas du domaine de rationalité ordinaire, M. Mordell a démontré le théorème très important que voici[1]:

Il existe un nombre fini de points rationnels fondamentaux d'arguments $u_1, u_2, \ldots, u_n$, *tel que tous les points rationnels soient donnés par la formule* (2).

Poincaré avait déjà soupçonné ce résultat; il appelait la plus petite valeur possible de n le *rang* de la cubique.[2] Malheureusement, la méthode de M. Mordell ne donne aucun moyen dans le cas général pour effectivement déterminer un tel système de points rationnels fondamentaux.

Dans le cas d'un domaine de rationalité quelconque, nous ne connaissons pas encore les conditions générales dans lesquelles il existe un tel système d'un nombre fini de points rationnels fondamentaux. Quand il n'y a qu'un nombre fini de points rationnels, il est triviel que le rang de la cubique est fini. Dans ce cas les arguments de tous les points rationnels sont nécessairement commensurables avec une période. Si la cubique admet une infinité de points rationnels, et si le rang est fini, il faut qu'il y ait au moins un point fondamental dont l'argument ne soit pas commensurable avec une période.

4. *Interprétation géométrique de la formule* (2). Soient u_1, u_2 et u_3 les arguments des trois points d'intersection de la cubique avec une droite. D'après la

[1] MORDELL, l. c.

[2] POINCARÉ, l. c., p. 171.

manière dont nous avons choisi la représentation paramétrique, la somme de ces arguments doit être égale à une période. Si les points u_1 et u_2 sont rationnels, le point u_3 l'est aussi. (Pour abréger nous parlons dans la suite du point u au lieu du point P d'argument u.) La sécante par les points u_1 et o coupe la cubique en le point $-u_1$. La tangente en le point u_1 coupe la cubique en le point $-2u_1$. La sécante par les points $-2u_1$ et o donne le point $+2u_1$. La sécante par les points $-u_1$ et $-2u_1$ coupera la cubique en le point $+3u_1$. En continuant ce procédé on aura évidemment tous les points mu_1, m étant un nombre entier quelconque. En général, en partant des n points initiaux $u_1, u_2, \ldots, u_n$, on aura par ces constructions géométriques simples tous les points

$$m_1 u_1 + m_2 u_2 + \cdots + m_n u_n,$$

les m_i étant des entiers quelconques. On le démontre sans difficulté par induction.

5. *Cubiques réelles.* Dans la suite nous nous bornons à considérer les cubiques réelles. Résumons quelques résultats de la théorie de ces courbes. Nous choisissons la représentation paramétrique comme au n° **2**. On sait qu'on peut choisir une paire de périodes primitives ω et ω' telle que ω soit réelle et positive et ω' imaginaire. Les cubiques réelles se partagent en deux catégories: les unes ont une seule branche où les arguments elliptiques sont réels; les autres ont deux branches, tous les points de la branche »impaire» ont leurs arguments réels, tous ceux de la branche »paire» (l'ovale) ont leurs arguments de la forme $u+\frac{\omega'}{2}$, où u est réel et où ω' est la période (purement) imaginaire.

Rappelons aussi le fait suivant: Soit la cubique donnée dans la forme

$$4(x-e_1)(x-e_2)(x-e_3)=y^2.$$

Si e_1 est réel, et si e_2 et e_3 sont complexes, on a $e_1=\wp\left(\frac{\omega}{2}\right)$. Si toutes les quantités e_1, e_2 et e_3 sont réelles, et si $e_1>e_2>e_3$, on a

$$e_1=\wp\left(\frac{\omega}{2}\right),\ e_2=\wp\left(\frac{\omega+\omega'}{2}\right),\ e_3=\wp\left(\frac{\omega'}{2}\right).$$

Supposons aussi que le domaine de rationalité est réel.

On peut partager les cubiques en deux catégories suivant qu'elles ont une infinité ou seulement un nombre fini de points rationnels. Mais nous n'avons

pas de moyen général pour reconnaître si une cubique donnée appartient à la première ou à la seconde catégorie, même si on connait déjà un certain nombre de points rationnels sur la courbe. Quand la cubique est réelle et bipartite, il se pose aussi la question de la distribution des points rationnels entre les deux branches. Soit P_0 un point rationnel de l'ovale. La sécante par P_0 coupe la branche impaire en le point P_1 et la branche paire en le point P_2. Si P_1 est rationnel, P_2 l'est aussi, et inversement. Il résulte de là qu'il se présente trois possibilités: 1° Tous les points rationnels sont sur la branche impaire. 2° Il y a une infinité de points rationnels sur chacune des deux branches. 3° Il y a un nombre limité de points rationnels et autant de points sur la branche paire que sur la branche impaire. Nous allons montrer par des exemples numériques que toutes ces possibilités existent réellement.

Supposons que le rang r de la cubique est fini. Alors, dans un système réduit de r points rationnels fondamentaux, il ne peut être qu'un seul point fondamental sur la branche impaire, dont l'argument est commensurable avec la période ω. En effet, soient $\frac{a\omega}{l}$ et $\frac{b\omega}{m}$ deux points rationnels quelconques sur la branche impaire, les nombres, l, m, a et b étant des entiers tels que les fractions $\frac{a}{l}$ et $\frac{b}{m}$ soient irréductibles. Or, il est facile de voir que les points $\lambda\frac{a\omega}{l}+\mu\frac{b\omega}{m}$, $\lambda=0, 1, 2, \ldots, l-1$, $\mu=0, 1, 2, \ldots, m-1$, sont identiques aux points $\frac{ku}{n}$, $k=0, 1, 2, \ldots, n-1$, où n désigne le plus petit multiple de l et m. Il résulte de là que tous les points rationnels de la branche impaire, dont les arguments sont commensurables avec une période, sont donnés par la formule $\frac{k\omega}{n}$, $k=0, 1, 2, \ldots,$ $n-1$. Alors, le nombre de ces points est exactement n.

Nous pouvons toujours supposer qu'il n'y a qu'un seul des points rationnels fondamentaux sur la branche paire. Si, en effet, nous avions sur cette branche deux points fondamentaux d'arguments v_1 et v_2, nous pourrions les remplacer par les points dont les arguments sont v_1 et $-v_1-v_2$, et le second de ces nouveaux points fondamentaux serait sur la branche impaire. Mais, s'il y a des points rationnels sur la branche paire, il y a toujours un point fondamental sur cette branche, puisque les quantités ω et ω' sont incommensurables.

Les classes de cubiques pour lesquelles nous savons déterminer un système de points fondamentaux, sont très spéciales; et presque tous les résultats sont

dans le domaine de rationalité ordinaire. C'est un fait très remarquable que, dans tous ces cas, c'est la méthode classique de la »*descente infinie*» qui conduit au but. On sait que cette méthode est due à Fermat, qui l'a appliqué pour démontrer l'impossibilité en nombres entiers de certaines équations biquadratiques à trois indéterminées, p. ex. celle de l'équation

$$x^4 - y^4 = z^2.$$

La méthode consiste à déduire d'une solution qu'on suppose donnée, une seconde solution de la même équation. Si l'on peut montrer que les valeurs absolues de cette seconde solution sont nécessairement plus petites que celles de la solution initiale, il est évident que l'équation proposée est impossible en nombres entiers, puisqu'il n'y a qu'un nombre limité d'entiers positifs au-dessous d'un nombre donné. Si ce procédé est en défaut pour certaines valeurs des inconnues, l'équation proposée peut avoir des solutions en nombre fini. Lagrange a montré le premier par un exemple numérique comment la même méthode peut servir à la résolution complète de l'équation quand il y a une infinité de solutions.[1] M. Mordell, pour établir son résultat du n° **3**, se sert aussi de cette méthode.

II.

Les cubiques qui admettent une infinité de points rationnels.

6. *Le cas général.* Hurwitz a démontré le théorème suivant[2]: Soient a, b, c et d des nombres entiers, tels que abc soit sans facteurs quadratiques > 1. Au plus un seul des nombres a, b et c peut prendre les valeurs ± 1. Alors, si la cubique

$$ax^3 + by^3 + cz^3 + dxyz = 0 \qquad (1)$$

admet un point rationnel, elle en admet une infinité. (Domaine de rationalité ordinaire.)

Il résulte de là qu'il existe réellement des cubiques admettant une infinité de points rationnels. En effet, si nous posons $b = a + 1, c = 1$ et $d = 0$, la cubique (1) admet le point rationnel $x = 1, y = -1, z = 1$, et par conséquent une infinité de points rationnels, sous les conditions données. Or, nous avons antérieurement

[1] *Œuvres de* LAGRANGE t. IV, p. 377.
[2] HURWITZ l. c., p. 226.

démontré qu'il existe une infinité de nombres entiers a tels que le nombre $a(a+1)$ soit sans facteurs quadratiques >1.[1] Donc nous avons le théorème:

Il existe une infinité de cubiques inéquivalentes

$$ax^3+(a+1)y^3+z^3=0 \tag{2}$$

admettant une infinité de points rationnels.

(Quant à l'inéquivalence de ces cubiques on peut l'établir sans peine à l'aide du dernier théorème du n° **2**.)

Poincaré et Hurwitz ont énoncé la proposition suivante[2]:

Si une cubique réelle admet une infinité de points rationnels, il y en a une infinité sur tout arc de sa branche impaire, et sur tout arc de sa branche paire, pourvu que cette branche en admette un.

Cependant la démonstration de Hurwitz n'est pas complète. Elle est basée sur la supposition qu'il y ait toujours un point rationnel dont l'argument ne soit pas commensurable avec une période. Or, cela n'est pas démontré dans le cas général. Il résulte évidemment du théorème précité de M. Mordell que la supposition est vraie dans le cas du domaine de rationalité ordinaire. Car la formule (2) du n° **3** ne donne qu'un nombre limité de valeurs si toutes les quantités $u_1, u_2, \ldots, u_n$ sont commensurables avec une période.

Il est facile de compléter la démonstration de Hurwitz. Il suffit de considérer la branche impaire. Si u_1 est l'argument d'un point rationnel de la branche impaire, et si $\frac{u_1}{\omega}$ est irrationnel (dans le sens ordinaire), le théorème est évident. Car, si nous posons $R(x)=x-E(x)$, où $E(x)$ désigne le plus grand nombre entier $\leqq x$, il est bien connu que les nombres $R\left(m\frac{u_1}{\omega}\right)$, m étant un nombre entier quelconque, couvrent l'intervalle $0-1$ partout.

Supposons ensuite que tous les arguments des points rationnels sont commensurables avec ω. Si le point $\frac{k\omega}{n}$, k et n étant des entiers positifs premiers entre eux, est rationnel, le point $\frac{ak\omega}{n}$ l'est aussi, a étant entier. Si nous prenons $ak\equiv 1 \pmod{n}$, le point $\frac{\omega}{n}$ est aussi rationnel. Il existe ainsi un nombre infini

[1] Voir notre Mémoire, »*Zur Arithmetik der Polynome*», *Abhdl. aus dem Math. Seminar d. Universität Hamburg*, t. 1 (1922), p. 188.

[2] POINCARÉ l. c., p. 173, sans démonstration; HURWITZ l. c., p. 225.

de points rationnels

$$\frac{\omega}{n_1}, \frac{\omega}{n_2}, \frac{\omega}{n_3}, \cdots,$$

où les n sont des entiers positifs tels que $n_1 < n_2 < n_3 < \cdots$. Soit maintenant u l'argument d'un point quelconque de la branche impaire, $0 < u < \omega$, et soit ε une quantité positive aussi petite qu'on veut. Choisissons enfin $n_r > \frac{\omega}{\varepsilon}$. Alors, si l'on a

$$\frac{t-1}{n_r} < \frac{u}{\omega} \leqq \frac{t}{n_r},$$

t étant un nombre entier tel que $1 \leqq t \leqq n_r - 1$, on a

$$\left| u - \frac{t\omega}{n_r} \right| < \frac{\omega}{n_r} < \varepsilon.$$

Ainsi on peut approcher le point u par une infinité de points rationnels $\frac{t\omega}{n_r}$. Le théorème se trouve ainsi démontré.

D'après le numéro précédent il y a, pour une cubique réelle admettant une infinité de points rationnels, les trois possibilités suivantes: 1° Il n'y a que la branche impaire. 2° Il y a deux branches, qui admettent chacune une infinité de points rationnels. 3° Il y a deux branches, et tous les points rationnels sont sur la branche impaire.

La première catégorie est réalisée par les cubiques (2). Car, il est évident que ces cubiques n'ont pas de branche paire. Dans le numéro suivant nous allons donner un exemple numérique réalisant la deuxième catégorie.

Nous allons aussi montrer par un exemple numérique que la troisième catégorie existe réellement.

7. *La cubique* $x(2x^2-1)=y^2$. Cette cubique a deux branches. Nous allons montrer qu'il y a une infinité de points rationnels sur chacune des deux branches. Considérons d'abord la branche impaire. x étant rationnel et positif, nous pouvons poser $x=\frac{a}{b}$, où a et b sont des nombres entiers positifs, premiers entre eux. Alors la cubique peut s'écrire

$$ab(2a^2-b^2)=(b^2y)^2=E^2, \tag{1}$$

E étant un nombre entier. Si b est pair, cette équation entraîne

$$b = 2u^2, a = v^2, 2a^2 - b^2 = 2w^2,$$

u, v et w étant des nombres entiers, premiers entre eux deux à deux; v et w sont impairs. En éliminant a et b, on tire de là

$$v^4 - 2u^4 = w^2. \tag{2}$$

Nous allons montrer que cette équation a une infinité de solutions en nombres entiers positifs u, v, w, premiers entre eux deux à deux. Une solution de l'équation est $v = 3, u = 2, w = 7$. Quand on connaît une solution en nombres entiers positifs u_1, v_1, w_1, on peut en déduire une autre par les formules

$$\left.\begin{aligned} v &= v_1^4 + 2u_1^4, \\ u &= |2u_1 v_1 w_1| \\ w &= |w_1^4 - 8u_1^4 v_1^4|, \end{aligned}\right\} \tag{3}$$

ainsi qu'on le vérifie sans peine. Supposons que les nombres u_1, v_1 et w_1 sont premiers entre eux deux à deux, u_1 pair et $v_1 w_1$ impair. Cela posé, il résulte des équations (3) que u, v et w sont premiers entre eux deux à deux; u est pair, tandis que vw est impair. On a de plus $u \geqq 2u_1$. Ainsi, en partant de la solution initiale $v_1 = 3, u_1 = 2, w_1 = 7$, nous aurons à l'aide des formules (3) une infinité de solutions de l'équation (2) en nombres entiers positifs u, v, w, premiers entre eux deux à deux. Puisque $u \geqq 2u_1$ on ne retombera jamais sur la même solution. On vérifie aisément que l'interprétation géométrique du système (3) est la suivante: La tangente à la cubique en le point $x_1 = \frac{v_1^2}{2u_1^2}$, $y_1 = \frac{v_1 w_1}{2u_1^3}$, rencontre la cubique en le point $x = \frac{v^2}{2u^2}$, $y = \frac{vw}{2u^3}$. Ainsi, si l'argument du point (x_1, y_1) est β, l'argument du point (x, y) est -2β. Aux valeurs $u = 2, v = 3, w = 7$ correspond le point rationnel $x = \frac{9}{8}$, $y = \frac{21}{16}$. Soit α l'argument de ce point. Alors nous venons de montrer que tous les points d'arguments $(-2)^n \alpha$, n entier $\geqq 0$, sont distincts. On conclut de là que α est incommensurable avec les périodes. Il résulte de ce qui précède, qu'il y a une infinité de points rationnels sur la branche impaire. Or, le point rationnel $x = y = 0$, d'argument $\frac{\omega + \omega'}{2}$, est sur la branche paire. Nous pouvons ainsi énoncer la proposition:

La cubique

$$x(2x^2-1)=y^2$$

admet une infinité de points rationnels sur chacune des deux branches.

Nous pouvons compléter ce résultat et montrer que le rang de la cubique (4) est égal à 2 et qu'on peut choisir pour points fondamentaux les points $x=y=1$ (sur la branche impaire) et $x=y=0$ (sur la branche paire). Nous reviendrons prochainement sur cette question.

8. *La cubique* $(x-1)(7x^2-3)=y^2$. Cette cubique a deux branches. Nous allons montrer qu'il y a une infinité de points rationnels sur sa branche impaire et qu'il n'y a aucun point rationnel sur sa branche paire. (Rationalité dans le sens ordinaire.) x étant rationnel, nous pouvons poser $x=\frac{a}{b}$, où a et b sont premiers entre eux, b positif. Alors la cubique peut s'écrire

$$b(a-b)(7a^2-3b^2)=(b^2y)^2=A^2, \tag{1}$$

A étant un nombre entier. Il faut distinguer deux cas.

1. b est indivisible par 7. Dans ce cas les nombres b et $7a^2-3b^2$ sont premiers entre eux. b est aussi premier à $a-b$. Si a et b sont impairs, le nombre $7a^2-3b^2$ est divisible par 4, mais non par 8; il faut donc que $a-b$ soit divisible par 4. L'équation (1) entraîne par suite

$$b=u^2,\ a-b=\pm v^2,\ 7a^2-3b^2=\pm w^2,$$

u, v et w étant des nombres entiers, premiers entre eux deux à deux, si $a-b$ est impair; si $a-b$ est pair le plus grand commun diviseur de v et w est 2. Or, il faut prendre le signe supérieur, puisque le nombre 3 est reste non-quadratique de 7. On aura donc $a-b=v^2\geqq 0$.

2. b est divisible par 7. Dans ce cas les nombres b et $7a^2-3b^2$ ont le plus grand commun diviseur 7. Le plus grand commun diviseur des nombres $a-b$ et $7a^2-3b^2$ est 4 ou 1 suivant que $a-b$ est pair ou impair. L'équation (1) entraîne par suite

$$b=7u^2,\ a-b=\pm v^2,\ 7a^2-3b^2=\pm 7w^2. \tag{2}$$

Il faut prendre le signe supérieur, puisque a^2+w^2 est indivisible par 3. On aura donc $a-b=v^2\geqq 0$.

Dans tous les deux cas on a ainsi $x=\frac{a}{b}\geqq 1$. *Donc, tous les points rationnels sont sur la branche impaire.*

En éliminant a et b du système (2) on aura l'équation

$$v^4 + 14\, v^2 u^2 + 28\, u^4 = w^2. \tag{3}$$

Nous allons montrer que cette équation a une infinité de solutions en nombres entiers positifs u, v, w, premiers entre eux deux à deux. Une solution de l'équation est $u = 10$, $v = 3$, $w = 541$. Quand on connait une solution en nombres entiers positifs u_1, v_1, w_1, de l'équation (3) on peut en déduire une autre par les formules

$$\left.\begin{aligned} v &= |\, v_1^4 - 28\, u_1^4 \,|, \\ u &= |\, 2\, u_1 v_1 w_1 \,|, \\ w &= |\, w_1^4 - 84\, u_1^4 v_1^4 \,|, \end{aligned}\right\} \tag{4}$$

ce qu'on vérifie sans difficulté. Supposons que les nombres u_1, v_1 et w_1 sont premiers entre eux deux à deux, u_1 pair, $v_1 w_1$ impair et indivisible par 7. Cela posé, il résulte des équations (4) que u, v et w sont premiers entre eux deux à deux, u est pair, $v\,w$ est impair et indivisible par 7. De plus on a $u \geqq 2\, u_1$. Ainsi, en partant de la solution initiale $u_1 = 10$, $v_1 = 3$, $w_1 = 541$, nous aurons à l'aide des formules (4) une infinité de solutions de l'équation (3) en nombres entiers positifs u, v, w, premiers entre eux deux à deux. Puisque $u \geqq 2\, u_1$ on ne retombera jamais sur la même solution. Il résulte de tout ce qui précède:

La cubique

$$(x - 1)(7\, x^2 - 3) = y^2$$

admet une infinité de points rationnels qui sont tous sur la branche impaire.

Aux valeurs $u = 10$, $v = 3$, $w = 541$ correspond le point rationnel

$$x = \frac{709}{700}, \quad y = \frac{1623}{7000}.$$

Il résulte de ce qui précède que l'argument de ce point est incommensurable avec une période. L'interprétation géométrique du système (4) est la suivante: La tangente à la cubique en le point

$$x_1 = \frac{7\, u_1^2 + v_1^2}{7\, u_1^2}, \quad y_1 = \frac{v_1 w_1}{7\, u_1^3},$$

rencontre la cubique en le point

$$x = \frac{7u^2 + v^2}{7u^2}, \quad y = \frac{vw}{7u^3}.$$

Très probablement il existe une infinité de cubiques jouissant de la même propriété. Mais il ne semble pas être très facile en donner la preuve.

III.

Les cubiques qui n'admettent qu'un nombre fini de points rationnels.

9. *Le cas général.* Soit donnée une cubique réelle qui admet exactement les n points rationnels d'arguments

$$u_0,\ u_1,\ u_2,\ \ldots,\ u_{n-1}. \tag{1}$$

La représentation paramétrique est choisie comme au n° **2.** Nous prenons $u_0 = 0$. Supposons d'abord que tous les n points sont sur la branche impaire. Alors nous savons d'après le n° **5** que tous les n points rationnels sont donnés par la formule

$$u = \frac{k\omega}{n}, \qquad k = 0, 1, 2, \ldots, n-1, \tag{2}$$

ω étant la période réelle.

Supposons ensuite qu'il y a aussi des points rationnels sur la branche paire de la courbe. Si ω' est la période imaginaire, les arguments des points de l'ovale ont la forme $u + \frac{\omega'}{2}$ où u est réel. *Il y a autant de points rationnels sur la branche paire que sur la branche impaire.* En effet, soit P_0 un point rationnel de l'ovale. La sécante par P_0 coupe la branche impaire en un point P_1 et l'ovale en un point P_2. Si P_1 est rationnel P_2 l'est aussi, et inversement. Ainsi, à chacun des points rationnels de l'une des branches correspond un et un seul point rationnel de l'autre branche. *Donc le nombre n est pair.* Il y a exactement $\frac{n}{2}$ points rationnels sur chacune des deux branches. Il résulte de là que tous les points rationnels de la branche impaire sont donnés par la formule

$$u = \frac{k\omega}{\frac{1}{2}n}, \qquad k = 0, 1, 2, \ldots, \frac{1}{2}n - 1. \tag{3}$$

Déterminons ensuite les points rationnels situés sur l'ovale. Soit $v_1 = w_1 + \frac{\omega'}{2}$ un point rationnel de l'ovale, w_1 étant réel. Alors le point $2\,v_1 \equiv 2\,w_1 \pmod{\omega, \omega'}$ est un point rationnel de la branche impaire, donc[1]

$$2\,w_1 \equiv \frac{l\,\omega}{\frac{1}{2}n},$$

l étant un nombre entier. Il résulte de là ou

$$w_1 \equiv \frac{l\,\omega}{n} \quad \text{ou} \quad w_1 \equiv \frac{l\,\omega}{n} + \frac{\omega}{2} \equiv \frac{(l + \frac{1}{2}n)\,\omega}{n}.$$

Dans tous les cas on a donc

$$w_1 \equiv \frac{l_1\,\omega}{n},$$

l_1 étant un nombre entier. Passons une sécante par le point v_1 et par chacun des points (3) et nous aurons tous les points rationnels de l'ovale dans la forme

$$v \equiv -\frac{k\,\omega}{\frac{1}{2}n} - v_1 \equiv -\frac{k\,\omega}{\frac{1}{2}n} - \frac{l_1\,\omega}{n} - \frac{\omega'}{2}. \qquad (k = 0, 1, 2, \ldots, \tfrac{1}{2}n - 1).$$

Si l_1 est pair on aura évidemment

$$v \equiv \frac{h\,\omega}{\frac{1}{2}n} + \frac{\omega'}{2}, \qquad h = 0, 1, 2, \ldots, \tfrac{1}{2}n - 1. \qquad (4)$$

Si l_1 est impair on aura

$$v \equiv \frac{(2h+1)\,\omega}{n} + \frac{\omega'}{2}, \qquad h = 0, 1, 2, \ldots, \tfrac{1}{2}n - 1. \qquad (5)$$

Il résulte de ce qui précède le théorème[2]:

Si la cubique réelle du premier genre admet exactement n points rationnels, les arguments de ces points sont donnés par l'une des trois formules suivantes

---

[1] Toutes les congruences sont modulo ω et ω'.

[2] Comparez les résultats de HURWITZ l.c., p. 215.

I. $$u = \frac{k\omega}{n}, \qquad k = 0, 1, 2, \ldots, n-1.$$

II. $$u = \frac{2k\omega}{n} + \varepsilon\frac{\omega'}{2}, \qquad k = 0, 1, 2, \ldots, \frac{n}{2} - 1;\ \varepsilon = 0, 1.$$

III. $$u = \frac{2k\omega}{n} + \varepsilon\left(\frac{\omega}{n} + \frac{\omega'}{2}\right), \qquad k = 0, 1, 2, \ldots, \frac{n}{2} - 1;\ \varepsilon = 0, 1.$$

Dans le premier cas, le rang de la cubique est égal à 1. (Cf. le n° **3**.) Dans le deuxième cas le rang est égal à 2; et on peut prendre pour points fondamentaux les points $\frac{2\omega}{n}$ et $\frac{\omega'}{2}$.

En désignant par 2^α la plus haute puissance de 2 qui divise n, on peut montrer que le dernier cas est équivalent à la formule

$$u = \frac{2^\alpha k\omega}{n} + h\left(\frac{\omega}{2^\alpha} + \frac{\omega'}{2}\right), \tag{6}$$

$$k = 0, 1, 2, \ldots, \frac{n}{2^\alpha} - 1;\ h = 0, 1, 2, \ldots, 2^\alpha - 1.$$

En effet, tous les n points (6) étant différents, il suffit de montrer que, k et h étant donnés, on peut toujours trouver les deux nombres entiers l et ε, tels que

$$\frac{2l\omega}{n} + \varepsilon\left(\frac{\omega}{n} + \frac{\omega'}{2}\right) = \frac{2^\alpha k\omega}{n} + h\left(\frac{\omega}{2^\alpha} + \frac{\omega'}{2}\right). \qquad (\varepsilon = 0, 1)$$

Si h est pair on aura $\varepsilon = 0$ et

$$l = k\cdot 2^{\alpha-1} + \frac{h}{2}\cdot\frac{n}{2^\alpha} = \text{entier}.$$

Si h est impair on aura $\varepsilon = 1$ et

$$l = k\cdot 2^{\alpha-1} + \frac{1}{2}\left(h\frac{n}{2^\alpha} - 1\right) = \text{entier}.$$

Ainsi le rang de la cubique est égal à 2; et on peut prendre pour points fondamentaux les points $\frac{2^\alpha\omega}{n}$ et $\frac{\omega}{2^\alpha} + \frac{\omega'}{2}$.

Considérons les demi-périodes $\frac{\omega}{2}, \frac{\omega'}{2}$ et $\frac{\omega+\omega'}{2}$. Pour que ces points soient rationnels il faut que n soit pair. Dans le cas I, le point $\frac{\omega}{2}$ est toujours rationnel, tandis que les points $\frac{\omega'}{2}$ et $\frac{\omega+\omega'}{2}$ sont irrationnels. Dans le cas II, si $\frac{n}{2}$ est impair, le point $\frac{\omega'}{2}$ est rationnel et les deux autres irrationnels; si $\frac{n}{2}$ est pair, tous les trois points sont rationnels. Dans le cas III, si $\frac{n}{2}$ est impair, le point $\frac{\omega+\omega'}{2}$ est rationnel et les autres irrationnels; si $\frac{n}{2}$ est pair, le point $\frac{\omega}{2}$ est rationnel et les autres irrationnels.

Il se pose naturellement la question suivante: Etant donné un nombre entier n quelconque, existe-t-il des cubiques qui admettent exactement n points rationnels? Quelles sont, parmi les catégories que nous venons d'énumerer dans notre théorème, celles qui existent réellement?

Cette question semble d'être très difficile; et c'est seulement pour les quatre premières valeurs de n que nous pouvons la résoudre complètement. Pour $n=1$ il n'y a que la possibilité $u=0$. Pour $n=2$ il y a les trois possibilités suivantes:

$$0, \frac{\omega}{2}; \quad 0, \frac{\omega'}{2}; \quad 0, \frac{\omega+\omega'}{2}.$$

Si $n=3$, les points rationnels sont $0, \frac{\omega}{3}, \frac{2\omega}{3}$. Si $n=4$, il y a les trois possibilités suivantes[1]:

$$0, \frac{\omega}{2}, \frac{\omega'}{2}, \frac{\omega+\omega'}{2}; \quad 0, \frac{\omega}{4}, \frac{\omega}{2}, \frac{3\omega}{4}; \quad 0, \frac{\omega}{2}, \frac{\omega}{4}+\frac{\omega'}{2}, \frac{3\omega}{4}+\frac{\omega'}{2}.$$

On a déjà longtemps connu une infinité de cubiques inéquivalentes admettant un seul point rationnel. On a en effet établi le théorème suivant[2]: *Si p est un nombre premier de la forme $18m+5$ ou de la forme $18m+11$, la cubique*

$$x^3+y^3=pz^3$$

[1] La dernière catégorie manque chez HURWITZ, l. c., p. 222—223.

[2] Voir HURWITZ, l. c., p. 217—220.

n'admet aucun point rationnel en dehors de $x=1$, $y=-1, z=0$. (Rationalité dans le sens ordinaire.)

Nous allons montrer l'existence d'une infinité de cubiques inéquivalentes vérifiant toutes les autres catégories que nous venons de citer, sauf les deux dernières pour $n=4$. Nous allons aussi examiner les cas de $n=5$ et $n=6$.

Dans la suite le mot rationnel s'entend toujours dans le sens ordinaire.

10. *Les deux cas* $0, \frac{\omega}{2}$ et $0, \frac{\omega+\omega'}{2}$. Le premier exemple d'une cubique qui n'admet pas d'autres points rationnels que 0 et $\frac{\omega}{2}$, a été donné par Euler. En effet, il a montré que la cubique

$$x^3+y^3=2z^3$$

ne porte aucun point rationnel en dehors de $x=1, y=-1, z=0$ et $x=y=z=1$. Dans une note antérieure nous avons généralisé ce résultat en démontrant la proposition suivante[1]:

Si p *est un nombre premier de la forme* $12m+5$, *la cubique*

$$x^3+1=py^2 \tag{1}$$

n'admet pas d'autres points rationnels que 0 *et* $\frac{\omega}{2}$.

Il existe ainsi une infinité de cubiques inéquivalentes qui n'admettent que ces deux points rationnels.

Nous allons ajouter à ce théorème le résultat suivant:

Si p *est un nombre premier de la forme* $8m+3$, *la cubique*

$$x(px^2-1)=y^2 \tag{2}$$

n'admet pas d'autres points rationnels que 0 *et* $\frac{\omega+\omega'}{2}$.

Il y a ainsi une infinité de cubiques inéquivalentes réalisant ce cas.

x étant rationnel, nous pouvons poser $x=\frac{a}{b}$, a et b étant des nombres entiers, premiers entre eux, b positif. Alors, nous aurons à résoudre l'équation

$$ab(pa^2-b^2)=A^2 \tag{3}$$

[1] Voir notre Note: »*Ueber die rationalen Punkte auf einigen kubischen Kurven,*» *The Tôhoku Math. Journal,* vol. 24, p. 48 (1924).

en nombres entiers a, b, et A. Il suffit de considérer la branche impaire. Donc x et a sont positifs. Si b est indivisible par p, cette équation entraîne

$$b=u^2, a=v^2, pa^2-b^2=w^2,$$

u, v et w étant des nombres entiers, premiers entre eux deux à deux.

Or, la dernière de ces équations est impossible, puisque b^2+w^2 est indivisible par un nombre premier de la forme $8m+3$.

Si b est divisible par p, l'équation (3) entraîne

$$a=u^2, b=pv^2, pa^2-b^2=pw^2,$$

u, v et w étant premiers entre eux deux à deux. En éliminant a et b, on tire de là

$$u^4-pv^4=w^2. \tag{4}$$

Le nombre u ne peut pas être pair, puisque pv^4+w^2 congru à 4 modulo 8 n'est pas divisible par 16. Si w est pair, on aura $u^4-3v^4\equiv 0 \pmod 4$, congruence impossible. Il faut donc que v soit pair. Alors, l'équation (4) entraîne

$$u^2 \pm w = 2\alpha c^4, u^2 \mp w = 8\beta d^4,$$

les nombres αc et βd étant premiers entre eux, $v=2cd, p=\alpha\beta$.

En éliminant w, il vient

$$u^2=\alpha c^4+4\beta d^4.$$

Le cas $\alpha=p, \beta=1$ conduit à la congruence impossible $u^2\equiv pc^4 \pmod 4$. Si $\alpha=1$ et $\beta=p$, on aura l'équation

$$u^2=c^4+4pd^4,$$

d'où l'on conclut

$$u\pm c^2=2f^4, u\mp c^2=2pg^4,$$

les nombres f et g étant premiers entre eux, $d=fg$, donc

$$f^4-pg^4=\pm c^2.$$

Il faut évidemment y prendre le signe supérieur. Cette équation est de la même forme que l'équation (4). Or, nous avons $|v|=|2cd|=|2cfg|>|g|$. On conclut de là

que l'équation (4) est impossible sauf pour $v=0$. Ainsi le seul point rationnel à distance finie de la cubique (2) est $x=y=0$.

11. Le cas $0, \frac{\omega'}{2}$. Une infinité de cubiques inéquivalentes réalisant ce cas sont données par le théorème suivant:

Si p est un nombre premier de la forme $24m+7$, la cubique

$$(x+1)(3x^2-1)=py^2 \qquad (1$$

n'admet pas d'autres points rationnels que 0 et $\frac{\omega'}{2}$.

x étant rationnel, nous posons $x=\frac{a}{b}$, où a et b sont premiers entre eux, b positif. Alors, l'équation (1) peut s'écrire

$$b(a+b)(3a^2-b^2)=pA^2, \qquad (2)$$

A étant un nombre entier. Si $x \neq -1$, le nombre $a+b$ est positif. Nous allons distinguer huit cas.

1) b est divisible par p et indivisible par 3; $a+b$ est impair. Dans ce cas l'équation (2) entraîne le système suivant:

$$b=pu^2, a+b=v^2, 3a^2-b^2=w^2,$$

u, v et w étant des nombres entiers, premiers entre eux deux à deux. Or, la dernière équation est impossible, b^2+w^2 étant indivisible par 3.

2) b est divisible par $3p$; $a+b$ est impair. Alors l'équation (3) entraîne le système

$$b=3pu^2, a+b=v^2, 3a^2-b^2=3w^2,$$

u, v et w étant premiers entre eux deux à deux. En éliminant a et b on aura donc

$$v^4-6pv^2u^2+6p^2u^4=w^2.$$

Nous reviendrons tout à l'heure sur cette équation.

3) b est divisible par p et indivisible par 3; $a+b$ est pair.

Dans ce cas l'équation (3) entraîne

$$b=pu^2, a+b=2v^2, 3a^2-b^2=2w^2.$$

En éliminant a et b on aura par suite

$$6v^4 - 6pv^2u^2 + p^2u^4 = w^2.$$

Cette équation est impossible, puisque $\left(\frac{6}{p}\right) = -1$.

4) b est divisible par $3p$; $a+b$ est pair. Dans ce cas on aura

$$b = 3pu^2,\ a+b = 2v^2,\ 3a^2 - b^2 = 6w^2.$$

La dernière équation est impossible puisque $a^2 - 2w^2$ est indivisible par 3.

5) b n'est divisible ni par 3 ni par p; $a+b$ est impair.

Dans ce cas on aura le système

$$b = u^2,\ a+b = pv^2,\ 3a^2 - b^2 = w^2.$$

Or, la dernière équation est impossible modulo 3.

6) b est divisible par 3 et indivisible par p; $a+b$ est impair.

Alors on aura le système

$$b = 3u^2,\ \ a+b = pv^2,\ 3a^2 - b^2 = 3w^2,$$

d'où, en éliminant a et b,

$$p^2v^4 - 6pv^2u^2 + 6u^4 = w^2,$$

équation impossible puisque $\left(\frac{6}{p}\right) = -1$.

7) b est divisible par 3 et indivisible par p; $a+b$ est pair.

Dans ce cas on aura le système

$$b = 3u^2,\ a+b = 2pv^2,\ 3a^2 - b^2 = 6w^2.$$

Or, la dernière équation est impossible puisque $a^2 - 2w^2$ est indivisible par 3.

8) b n'est divisible ni par 3 ni par p; $a+b$ est pair. Ce cas conduit au système

$$b = u^2,\ a+b = 2pv^2,\ 3a^2 - b^2 = 2w^2,$$

d'où l'on tire en éliminant a et b,

$$u^4 - 6pu^2v^2 + 6p^2v^4 = w^2. \tag{4}$$

Les nombres u, v et w sont premiers entre eux deux à deux; u et w sont nécessairement impairs; alors il résulte de (4) modulo 8:

$$1+6v^2+6v^4\equiv 1 \pmod 8,$$

p étant $\equiv -1 \pmod 4$. Il résulte de là que v est pair. L'équation (4) peut s'écrire

$$(u^2-3pv^2)^2-w^2=3p^2v^4.$$

On conclut de là que

$$u^2-3pv^2+w=\pm 2\alpha c^4,\ u^2-3pv^2-w=\pm 8\beta d^4,$$

les nombres αc et βd étant premiers entre eux, $v=2cd$ et $3p^2=\alpha\beta$. Par addition on aura

$$u^2=12pc^2d^2\pm(\alpha c^4+4\beta d^4).$$

Si $\alpha=3$ et $\beta=p^2$, on aura $u^2\equiv\pm 4p^2d^4 \pmod 3$; donc il faut prendre le signe supérieur. Or, cela conduit à la congruence impossible $u^2\equiv 3c^4 \pmod 4$. Si $\alpha=3p^2$, $\beta=1$, on aura $u^2=\pm 4d^4 \pmod 3$; il faut donc prendre le signe supérieur. Or, cela conduit à la congruence impossible $u^2\equiv 3p^2c^4 \pmod 4$. Si $\alpha=p^2$, $\beta=3$, il faut aussi prendre le signe supérieur, ce qui conduit à la congruence impossible $u^2\equiv 12d^4 \pmod p$. Si $\alpha=1$, $\beta=3p^2$, il faut aussi prendre le signe supérieur, et l'équation devient

$$u^2=c^4+12pc^2d^2+12p^2d^4,$$

ou bien

$$(c^2+6pd^2)^2-u^2=24p^2d^4.$$

Cette équation entraîne

$$c^2+6pd^2\pm u=2\alpha f^4,\ c^2+6pd^2\mp u=4\beta g^4,$$

les nombres αf et βg étant premiers entre eux, $d=fg$ et $\alpha\beta=3p^2$. En éliminant u, il vient

$$c^2=-6pf^2g^2+\alpha f^4+2\beta g^4.$$

Si α est divisible par 3, on aura $c^2\equiv 2\beta g^4 \pmod 3$, congruence impossible, puisque $\beta=1$ ou $=p^2$. Si $\alpha=p^2$, $\beta=3$, on aura $c^2\equiv 6g^4 \pmod p$, congruence impossible. Si $\alpha=1$, $\beta=3p^2$, il vient

$$c^2=f^4-6pf^2g^2+6p^2g^4.$$

Cette équation est de la même forme que l'équation (4). Or, nous avons $|v|=|2cd|=|2cfg|>|g|$. Nous avons ainsi par une descente infinie établi

l'impossibilité de l'équation (4) en nombres entiers u, v, w, premiers entre eux deux à deux. Il résulte de là que l'équation (3) n'est possible que pour $a+b=0$ ou $b=0$. Le théorème se trouve ainsi démontré.

12. *Le cas de* $n=3$. Dans ce cas il y a la seule possibilité :0, $\frac{\omega}{3}$ et $\frac{2\omega}{3}$. Un exemple bien connu depuis Fermat est la cubique

$$x^3+y^3=z^3,$$

qui n'admet que les trois points rationnels $x=0, y=1, z=1$; $x=1, y=0, z=1$; $x=1, y=-1, z=0$. Nous allons généraliser ce résultat.

Nous pouvons évidemment écrire la cubique la plus générale, admettant les trois points rationnels 0, $\frac{\omega}{3}$ et $\frac{2\omega}{3}$, dans la forme

$$Ax^3+Bx^2+Cx+1=y^2,$$

à coefficients rationnels A, B et C, les deux points rationnels à distance finie correspondant à $x=0, y=\pm 1$. Pour que ces deux points soient des points d'inflexion il faut et il suffit qu'on ait $B=t^2$ et $C=2t$, le nombre t étant le coefficient angulaire de la tangente d'inflexion au point $x=0, y=1$. Si t est différent de zéro, nous pouvons remplacer tx par x et A par At^3. Il résulte de là le théorème suivant:

Les cubiques les plus générales, admettant les points rationnels 0, $\frac{\omega}{3}$ *et* $\frac{2\omega}{3}$ *sont données par*

$$Ax^3+1=y^2 \tag{1}$$

et

$$Ax^3+(x+1)^2=y^2, \tag{2}$$

A étant un nombre rationnel, différent de zéro, et, dans le dernier cas, différent de $\frac{4}{27}$.

Nous ne connaissons pas les conditions générales, dans lesquelles ces cubiques n'admettent pas d'autres points rationnels.

Posons dans l'équation (1) $\frac{u}{w}=\frac{1}{x}$ et $\frac{v}{w}=\frac{y-1}{2x}$, et il vient

$$uv(u+v)=\frac{1}{4}Aw^3. \tag{3}$$

Choisissons ici $\frac{1}{4}A = p =$ nombre premier de la forme $18m+5$. Cela posé, l'équation (3) n'a pas d'autres solutions en nombres entiers u, v et w, que $u=0, v=0$ et $u+v=0$. En effet, nous pouvons supposer u, v et w premiers entre eux deux à deux, et si u est divisible par p, l'équatiou (3) entraîne

$$u = pa^3,\ v = b^3,\ u+v = c^3,$$

d'où

$$pa^3 + b^3 = c^3.$$

Or, on sait que cette équation est impossible sauf pour $a=0$, quand p est de la forme $18\ m+5$.[1] Dans les autres cas où v ou $u+v$ est divisible par p, on aura une équation analogue.

Nous tirons de là la conclusion suivante:

Si p est un nombre premier de la forme $18m+5$, la cubique

$$4px^3 + 1 = y^2$$

n'admet pas d'autres points rationnels que $0, \frac{\omega}{3}$ et $\frac{2\omega}{3}$.

On aura ainsi une infinité de cubiques inéquivalentes qui n'admettent que ces trois points rationnels.

13. *Le cas* $0, \frac{\omega}{2}, \frac{\omega'}{2}, \frac{\omega+\omega'}{2}$. Il est évident que la cubique la plus générale admettant ces quatre points rationnels peut s'écrire dans la forme

$$x(x+a)(x+b) = y^2,$$

a et b étant des nombres rationnels différents. Il se pose la question dans quelles conditions cette cubique n'admet pas d'autres points rationnels. Nous ne les connaissons pas. Hurwitz a donné l'exemple suivant[2]

$$x(x^2-1) = y^2.$$

Nous allons établir le résultat plus général que voici:

Si p est un nombre premier de la forme $8m+3$, la cubique

$$x(x^2-1) = py^2 \qquad (1)$$

[1] Hurwitz, l. c., p. 220.

[2] Hurwitz, l. c., p. 224.

n'admet pas d'autres points rationnels que $0, \frac{\omega}{2}, \frac{\omega'}{2}, \frac{\omega+\omega'}{2}$.

Posons dans (1) $x=\frac{a}{b}$, a et b étant des nombres entiers premiers entre eux, b positif. Alors l'équation (1) peut s'écrire

$$ab(a^2-b^2)=pA^2, \tag{2}$$

A étant un nombre entier. Si ab est indivisible par p, on aura

$$b=u^2,\ a=\pm v^2,\ a^2-b^2=\pm pw^2,$$

d'où, en éliminant a et b,

$$u^4-v^4=\mp pw^2. \tag{3}$$

Il suffit de prendre le signe inférieur. Si v est pair on aura la congruence impossible $u^4\equiv 3w^2 \pmod 8$, u ne peut être pair non plus, puisque v^4+3w^2 est indivisible par 8. Il faut donc que w soit pair. Donc, l'équation (3) conduit à l'un ou l'autre des deux systèmes

$$u\pm v=2pc^2,\ u\mp v=4d^2,\quad u^2+v^2=2e^2,$$

ou

$$u\pm v=2c^2,\quad u\mp v=4pd^2,\ u^2+v^2=2e^2,$$

les nombres c, d et e étant premiers entre eux deux à deux; c et e sont impairs. En éliminant u et v, le premier système donne

$$p^2c^4+4d^4=e^2,$$

d'où l'on tire

$$e\pm pc^2=2g^4,\ e\mp pc^2=2f^4,$$

ou

$$\pm pc^2=g^4-f^4,$$

équation impossible, puisque c est impair.

Le second système conduit à l'équation

$$4p^2c^4+d^4=e^2,$$

d'où l'on tire

$$e\pm 2pc^2=g^4,\ e\mp 2pc^2=f^4,$$

donc

$$g^4-f^4=\pm p(2c)^2.$$

Cette équation est de la même forme que l'équation (3). Or, nous avons $|w| = |4cde| > |2c|$. Cela conduit à une contradiction si w est la plus petite solution positive de l'équation (3). Cette équation est par suite seulement possible pour $w = 0$.

Supposons ensuite que b est divisible par p. Dans ce cas l'équation (2) entraîne

$$b = pv^2,\ a = \pm u^2,\ a^2 - b^2 = \pm w^2,$$

d'où, en éliminant a et b,

$$u^4 - p^2 v^4 = \pm w^2. \tag{4}$$

Il faut prendre le signe supérieur, puisque p ne divise pas $u^4 + w^2$. Si w est pair, il est nécessairement divisible par 4; on aura donc $u^4 \equiv p^2 v^4 \equiv 9v^4$ (mod. 16), ce qui est impossible. u ne peut pas être pair non plus, puisque $p^2 v^4 + w^2$ est indivisible par 4. Il faut donc que v soit pair, et on aura ou

$$u^2 \pm w = 2p^2 c^4,\ u^2 \mp w = 8d^4,$$

ou

$$u^2 \pm w = 8p^2 c^4,\ u^2 \mp w = 2d^4.$$

Le premier système conduit à

$$u^2 = p^2 c^4 + 4d^4,$$

d'où l'on tire

$$u \pm pc^2 = 2f^4,\ u \mp pc^2 = 2g^4,$$

ou

$$\pm pc^2 = f^4 - g^4.$$

Or, nous venons de montrer l'impossibilité de cette équation. Le second système conduit à

$$u^2 = d^4 + 4p^2 c^4,$$

d'où l'on tire

$$u \pm 2pc^2 = f^4,\ u \mp 2pc^2 = g^4,$$

ou

$$f^4 - g^4 = \pm p(2c)^2,$$

équation impossible d'après ce qui précède. L'équation (4) est par suite impossible sauf pour $v = 0$.

Le cas où a est divisible par p, se traite exactement de la même manière. Notre théorème se trouve ainsi démontré; et nous avons une infinité de cubiques inéquivalentes jouissant de la propriété demandée.

14. *Les deux cas* $0, \pm\frac{\omega}{4}, \frac{\omega}{2}$ et $0, \pm\frac{\omega}{4}+\frac{\omega'}{2}, \frac{\omega}{2}$.

Si nous plaçons les trois points rationnels à distance finie dans les points $(1,0)$ et $(0, \pm 1)$, la cubique la plus générale, admettant l'un ou l'autre de ces groupes de quatre points, peut s'écrire dans la forme

$$(ax^2+bx-1)(x-1)=y^2,$$

a et b étant des nombres rationnels. La tangente en $(0,+1)$ est

$$y=t(x-1).$$

Elle doit passer par $(1,0)$, donc $t=-1$. L'équation

$$(ax^2+bx-1)(x-1)=(x-1)^2$$

doit avoir, en dehors de la solution $x=1$, la racine double $x=0$, donc $b=1$. Si a est positif, l'équation $ax^2+x-1=0$ a toujours deux racines réelles, l'une positive et <1, l'autre négative. Si a est négatif, nous remplaçons a par $-a$ et x par $-x$. Alors, si $a>\frac{1}{4}$, l'équation $ax^2+x+1=0$ a ses racines complexes; si $0<a<\frac{1}{4}$, l'équation a deux racines négatives et <-1.

Il résulte de là le théorème:

La cubique la plus générale, admettant les quatre points rationnels $0, \pm\frac{\omega}{4}+\frac{\omega'}{2}$ *et* $\frac{\omega}{2}$ *est donnée par*

$$(ax^2+x-1)(x-1)=y^2, \tag{1}$$

a étant un nombre rationnel positif quelconque.

La cubique la plus générale, admettant les quatre points rationnels $0, \pm\frac{\omega}{4}$ *et* $\frac{\omega}{2}$ *est donnée par*

$$(ax^2+x+1)(x+1)=y^2, \tag{2}$$

a étant un nombre rationnel positif, différent de $\frac{1}{4}$.

Si l'on pose, dans l'équation (2), $a=\frac{1}{2}$, $t=1+\frac{2}{x}$ et $s=\frac{4y}{x^2}$, on tombera sur la quartique

$$t^4-1=s^2.$$

Or, il est bien connu que Fermat a montré que cette courbe n'admet pas d'autres points rationnels à distance finie que $t=\pm 1$, $s=0$. Il résulte de là la proposition: *La cubique*

$$\left(\frac{1}{2}x^2+x+1\right)(x+1)=y^2$$

n'admet pas d'autres points rationnels que $0, \pm\frac{\omega}{4}$ *et* $\frac{\omega}{2}$.[1]

Nous allons y ajouter le résultat suivant: *La cubique*

$$x^3-2x+1=y^2 \tag{3}$$

n'admet pas d'autres points rationnels que $0, \pm\frac{\omega}{4}+\frac{\omega'}{2}$ *et* $\frac{\omega}{2}$.

On aura cette cubique en prenant dans l'équation (1) $a=1$. En posant dans l'équation (3) $x=\frac{a}{b}$, où a et b sont premiers entre eux, b positif, on obtient l'équation

$$b(a-b)(a^2+ab-b^2)=E^2, \tag{4}$$

E étant un nombre entier. Il résulte de cette équation

$$b=u^2,\ a-b=\pm v^2,\ a^2+ab-b^2=\pm w^2, \tag{5}$$

u, v et w étant premiers entre eux deux à deux. Si x est sur la branche impaire, il faut évidemment prendre le signe supérieur. En éliminant a et b, on aura donc

$$u^4+3u^2v^2+v^4=w^2. \tag{6}$$

Il est évident que, dans cette équation, les nombres u et v ne peuvent pas être tous les deux impairs. Supposons que v est pair. Alors, l'équation peut s'écrire

$$(u^2+\tfrac{3}{2}v^2)^2-w^2=\tfrac{5}{4}v^4,$$

[1] Cet exemple se trouve aussi chez HURWITZ, l. c., p. 225.

d'où l'on tire

$$u^2+\frac{3}{2}v^2\pm w=2c^4,\quad u^2+\frac{3}{2}v^2\mp w=10d^4,$$

c et d étant premiers entre eux, $v=2cd$, donc

$$u^2=-6c^2d^2+c^4+5d^4.$$

Ici c doit être impair. L'équation peut s'écrire

$$(c^2-3d^2)^2-u^2=4d^4,$$

d'où

$$c^2-3d^2+u=\pm 2f^4,\quad c^2-3d^2-u=\pm 2g^4,$$

f et g étant premiers entre eux, $d=fg$. On aura ainsi

$$c^2=3f^2g^2\pm(f^4+g^4).$$

Si fg est pair, il faut prendre le signe supérieur. Dans ce cas on aura une équation de la même forme que (6). Or, si nous supposons que v soit la plus petite solution positive et paire de l'équation (6), cela est impossible, puisque $|v|=|2cd|=|2cfg|>|fg|$. Il faut donc que fg soit impair. Or, dans ce cas, nous aurons $\pm u=f^4-g^4=$ nombre pair, ce qui est contre la supposition faite sur u.

Il résulte de là que l'équation (6) est impossible en nombres entiers, sauf pour $uv=0$. Par conséquent, les seuls points rationnels sur la branche impaire de la cubique (3) sont 0 et $\frac{\omega}{2}$.

15. *Le cas de* $n=6$. Dans ce cas il y a les trois possibilités suivantes

$$0,\pm\frac{\omega}{6},\pm\frac{\omega}{3},\frac{\omega}{2};\quad 0,\pm\frac{\omega}{6}+\frac{\omega'}{2},\pm\frac{\omega}{3},\frac{\omega+\omega'}{2};\quad 0,\pm\frac{\omega}{3}+\frac{\omega'}{2},\pm\frac{\omega}{3},\frac{\omega'}{2}.$$

La première possibilité est réalisée par la cubique

$$x^3+1=y^2. \tag{1}$$

En effet, Euler a montré qu'*elle n'admet que les points rationnels* $x=0,y=\pm 1$; $x=-1,y=0$; $x=2,y=\pm 3$, *à distance finie.*

Nous avons montré au n° **12** que les cubiques admettant les trois points rationnels $0,\pm\frac{\omega}{3}$, sont données par

$$Ax^3+1=y^2,$$

et

$$Ax^3+(x+1)^2=y^2. \qquad \left(A\neq\frac{4}{27}\right) \tag{2}$$

Pour que la première de ces cubiques admette le point rationnel $\frac{\omega}{2}$ il faut que A soit le cube d'un nombre rationnel, $A=B^3$. Or, dans ce cas, en remplaçant x par $\frac{x}{B}$, on tombera sur la cubique (1).

En remplaçant x par $\frac{x}{A}$ et y par $\frac{y}{A}$ la cubique (2) peut s'écrire

$$x^3+(x+A)^2=y^2.$$

Déterminons A tel que l'équation $x^3+(x+A)^2=0$ ait une racine rationnelle $x=\xi$. Il faut donc que $\xi=-\alpha^2$ et $\xi+A=\beta^3$, α et β étant des nombres rationnels, et par suite $\alpha=\beta$ et $A=\alpha^2+\alpha^3$. La cubique la plus générale, admettant l'un des groupes précités de six points rationnels est donc

$$x^3+(x+\alpha^2+\alpha^3)^2=y^2, \tag{3}$$

abstraction faite de la cubique (1). Pour que cette cubique soit du premier genre, il faut et il suffit que α soit différent des quatre nombres $-1, -\frac{2}{3}, 0$ et $\frac{1}{3}$. Si $\alpha>\frac{1}{3}$ ou <-1, la cubique n'a qu'une seule branche. Si $-1<\alpha<\frac{1}{3}$, $\alpha\neq 0$ et $\neq -\frac{2}{3}$, la cubique a deux branches. Si $-1<\alpha<-\frac{2}{3}$, l'équation

$$x^3+(x+\alpha^2+\alpha^3)^2=0 \tag{4}$$

a, en dehors de la racine $x=-\alpha^2$ correspondant à l'argument $\frac{\omega'}{2}$, deux racines réelles qui sont $>-\alpha^2$. Si $0>\alpha>-\frac{2}{3}$, l'équation (4) a, en dehors de la racine $x=-\alpha^2$ correspondant à l'argument $\frac{\omega+\omega'}{2}$, deux racines réelles dont l'une est $>-\alpha^2$ et l'autre $<-\alpha^2$. Si enfin $0<\alpha<\frac{1}{3}$, l'équation (4) a, en dehors de la

racine $x=-a^2$ correspondant à l'argument $\frac{\omega}{2}$, deux racines réelles qui sont $<-a^2$.

Il résulte de tout cela le théorème:

Les cubiques les plus générales admettant les six points rationnels

$$0, \pm\frac{\omega}{6}, \pm\frac{\omega}{3} \text{ et } \frac{\omega}{2}$$

sont données par l'équation (1) *et par l'équation* (3), a *étant un nombre rationnel* <-1 *ou* >0, *différent de* $\frac{1}{3}$.

Les cubiques les plus générales admettant les six points rationnels

$$0, \pm\frac{\omega}{6}+\frac{\omega'}{2}, \pm\frac{\omega}{3} \text{ et } \frac{\omega+\omega'}{2}$$

sont données par l'équation (3), a *étant un nombre rationnel négatif et* $>-\frac{2}{3}$.

Les cubiques les plus générales admettant les six points rationnels

$$0, \pm\frac{\omega}{3}+\frac{\omega'}{2}, \pm\frac{\omega}{3} \text{ et } \frac{\omega'}{2}$$

sont données par l'équation (3), a *étant un nombre rationnel,* $-1<a<-\frac{2}{3}$.

En posant dans l'équation (3) $a=-\frac{1}{3}$, et en substituant x par $\frac{x}{9}$ et y par $\frac{y}{27}$, nous aurons la cubique

$$x^3+(3x+2)^2=y^2. \tag{5}$$

Nous allons montrer que cette courbe n'admet pas d'autres points rationnels à distance finie que $x=-4$, $y=\pm 6$; $x=0$, $y=\pm 2$; $x=-1$, $y=0$. x étant rationnel, nous pouvons poser $x=\frac{a}{b}$, où a et b sont premiers entre eux, b positif. Alors, l'équation (5) peut s'écrire

$$b(a+b)(a^2+8ab+4b^2)=E^2,$$

E étant un nombre entier. Il suffit de considérer la branche impaire où $a+b$ est positif. Alors cette équation entraîne l'un ou l'autre des deux systèmes suivants

$$b = u^2,\ a + b = 3v^2,\ a^2 + 8ab + 4b^2 = 3w^2;$$

et

$$b = u^2,\ a + b = v^2,\quad a^2 + 8ab + 4b^2 = w^2,$$

u, v et w étant des nombres entiers, premiers entre eux deux à deux. La dernière équation du premier système peut s'écrire

$$\frac{1}{3}(a + 4b)^2 - 4b^2 = w^2,$$

ce qui est impossible puisque $4b^2 + w^2$ est indivisible par 3. En éliminant a et b, le second système conduit à l'équation

$$v^4 + 6v^2u^2 - 3u^4 = w^2. \tag{6}$$

Or, si nous posons

$$x + 1 = \frac{w^2}{4u^2v^2} \quad \text{et} \quad y = \frac{w(v^4 + 3u^4)}{8u^3v^3},$$

il vient

$$x^3 + 1 = y^2.$$

Nous savons déjà que cette équation n'a que les solutions $x = -1$, $y = 0$; $x = 0$, $y = \pm 1$; $x = 2$, $y = \pm 3$ en nombres rationnels. Il résulte de là que l'équation (6) n'a que la solution $u = v = 1$, $w = 2$, en nombres entiers positifs u, v et w, premiers entre eux deux à deux. La proposition suivante se trouve ainsi démontrée: *La cubique* (5) *n'admet pas d'autres points rationnels que*

$$0,\ \pm\frac{\omega}{6} + \frac{\omega'}{2},\ \pm\frac{\omega}{3} \quad \text{et} \quad \frac{\omega + \omega'}{2}.$$

Nous ne connaissons aucune cubique qui n'admet que les six points rationnels

$$0,\ \pm\frac{\omega}{3} + \frac{\omega'}{2},\ \pm\frac{\omega}{3} \quad \text{et} \quad \frac{\omega'}{2}.$$

16. *Le cas de* $n = 5$. Si une cubique admet exactement cinq points rationnels, ces points sont donnés par

$$0,\ \pm\frac{\omega}{5} \quad \text{et} \quad \pm\frac{2\omega}{5}.$$

Nous allons déterminer la forme la plus générale d'une cubique admettant ces points rationnels. Soit donnée la cubique

$$4x^3 - g_2 x - g_3 = y^2, \tag{1}$$

à coefficients rationnels g_2 et g_3. Soient donnés sur la cubique quatre points à distance finie jouissant de la propriété suivante:

P_1 d'argument u_1 étant un quelconque de ces points, la tangente en ce point rencontrera la cubique en le second point P_2 d'argument $u_2 = -2u_1$. La tangente en le point P_2 rencontre la cubique en le point P_3 d'argument $u_3 = -u_1$.

Ces points sont forcément sur la branche impaire. En effet, si P_1 était sur la branche paire, les points P_2 et P_3 seraient sur la branche impaire. Or, les deux points d'arguments $\pm u_1$ sont nécessairement sur la même branche. Il résulte de là $u_3 \equiv -2u_2 \equiv +4u_1 \equiv -u_1 \pmod{\omega}$, donc $5u_1 =$ période. Les quatre points sont, par suite, $\pm\frac{\omega}{5}$ et $\pm\frac{2\omega}{5}$. Le groupe de ces quatre points est donc caracterisé par la-dite propriété.

Soit maintenant $P_1(x = a,\ y = b)$ un quelconque des points $\pm\frac{\omega}{5}$ et $\pm\frac{2\omega}{5}$, à coordonnées rationnelles a et b. On a donc

$$4a^3 - g_2 a - g_3 = b^2. \tag{2}$$

La tangente en ce point a l'équation

$$y = b + (x - a)\frac{12a^2 - g_2}{2b}.$$

Elle coupe la cubique en le second point rationnel $P_2(x = c,\ y = d)$, c et d satisfaisant aux équations

$$d = b + (c - a)\frac{12a^2 - g_2}{2b}, \tag{3}$$

$$4c^3 - g_2 c - g_3 = d^2. \tag{4}$$

La tangente en le point P_2 doit couper la cubique en le point $P_3(x = a,\ y = -b)$, ce qui donne la condition

$$-b = d + (a - c)\frac{12c^2 - g_2}{2d}. \tag{5}$$

En éliminant g_3 entre les équations (2) et (4), il vient

$$(c - a)g_2 = 4c^3 - 4a^3 + b^2 - d^2. \tag{6}$$

Les équations (3) et (5) peuvent s'écrire

$$\left.\begin{aligned} \frac{1}{2}(c-a)\,g_2 &= -6a^3+6a^2c+b^2-bd, \\ \text{et} \\ \frac{1}{2}(c-a)\,g_2 &= 6c^3-6ac^2-d^2-bd, \end{aligned}\right\} \tag{7}$$

d'où par addition

$$(c-a)\,g_2 = -6a^3+6c^3+6a^2c-6ac^2+b^2-2bd-d^2.$$

En éliminant g_2 entre cette équation et l'équation (6), il vient

$$2bd = 2c^3-2a^3+6a^2c-6ac^2. \tag{8}$$

En éliminant g_2 entre les deux équations (7), il vient

$$b^2+d^2 = 6a^3+6c^3-6ac^2-6a^2c.$$

De cette équation et de l'équation (8) nous aurons par addition

$$b^2+2bd+d^2 = (b+d)^2 = 4(a-c)^2(2c+a)$$

et par soustraction

$$b^2-2bd+d^2 = (b-d)^2 = 4(a-c)^2(2a+c).$$

Il résulte de là que toutes les quantités a, b, c, d, g_2 et g_3 peuvent s'exprimer rationnellement des nombres

$$N = \frac{1}{2}\cdot\frac{b-d}{a-c} \quad \text{et} \quad M = \frac{1}{2}\cdot\frac{b+d}{a-c}.$$

Nous aurons en effet

$$a = \frac{1}{3}(2N^2-M^2),$$

$$c = \frac{1}{3}(2M^2-N^2),$$

$$b = (M+N)(N^2-M^2),$$

$$d = (M-N)(N^2-M^2),$$

et les »invariants» de la cubique la plus générale admettant les points rationnels $0, \pm\frac{\omega}{5}$ et $\pm\frac{2\omega}{5}$, sont donnés par

$$g_2 = \frac{4}{3}\,(N^4 - 3\,N^3 M - N^2 M^2 + 3\,N M^3 + M^4)$$

et

$$g_3 = \frac{1}{27}\,(-19\,N^6 + 18\,N^5 M + 15\,N^4 M^2 + 15\,N^2 M^4 - 18\,N M^5 - 19\,M^6),$$

N et M étant des nombres rationnels, différents de zéro, et $N \neq \pm M$.

Si l'on prend p. ex. $N = 2$ et $M = 1$, on aura $a = \frac{7}{3}$, $c = -\frac{2}{3}$, $b = 9$ et $d = -3$, et la cubique sera

$$4x^3 + \frac{20}{3}x + \frac{395}{27} = y^2.$$

Mais nous ne savons pas si cette cubique en admet d'autres points rationnels que $x = \infty$; $x = \frac{7}{3}$, $y = \pm 9$; $x = -\frac{2}{3}$, $y = \pm 3$.

Oslo, janvier 1928.