which determines unique integers (α, β, γ), coprime with $\alpha \geqslant 1$. Then

$$\{pQ(x,y)-qQ(u,v)\}\alpha^2 = (px^2-qu^2)\{A\alpha^2+B\alpha\beta+C\beta^2-Cpq\gamma^2\}. \tag{29}$$

Thus a solution of (26) which satisfies (27) gives rise to a unique set of coprime integers (α, β, γ) $(\alpha \geqslant 1)$ such that

$$A\alpha^2+B\alpha\beta+C\beta^2-Cpq\gamma^2 = 0. \tag{30}$$

For special values of x and u it may happen that (30) is properly solvable. But the solutions α, β, γ must also be such that

$$\beta x+\gamma qu \equiv 0 \pmod{\alpha}, \tag{31}$$

$$\beta u+\gamma qx \equiv 0 \pmod{\alpha}. \tag{32}$$

If, for appropriate x and u, equation (30) and the two congruences (31) and (32) can be solved, we reach solutions of (26). This method is often useful in proving the existence of infinitely many solutions of equations of the form (26).

References

[1] L. E. Dickson, *Introduction to the Theory of Numbers*, (Dover), p. 117.

[2] G. H. Hardy and E. M. Wright, *Introduction to the Theory of Numbers*, 4th Ed., Oxford 1960, pp. 199-201.

Reçu par la Rédaction le 13. 11. 1963

ACTA ARITHMETICA
IX (1964)

Sur quelques catégories d'équations diophantiennes résolubles par des identités

par

T. NAGELL (Uppsala)

Dédié au 75ième anniversaire de L. J. Mordell

1. Courbes unicursales. Il est bien connu que la solution complète de l'équation diophantienne

$$x^2+y^2-z^2 = 0 \tag{1}$$

dans un corps quelconque Ω est donnée par les formules

$$x = t(t_1^2-t_2^2), \quad y = 2tt_1t_2, \quad z = t(t_1^2+t_2^2), \tag{2}$$

les paramètres t, t_1, t_2 parcourant tous les nombres du corps Ω, indépendamment entre eux; voir p. ex. Nagell [1](1), p. 217. Ainsi la *solution complète* de (1) en Ω est donnée par une *identité*.

Ce résultat n'est qu'un cas particulier de la proposition plus générale (voir p.ex. Nagell [1], p. 216):

Soit $C(x,y,z) = 0$ l'équation d'une conique en coordonnées homogènes x, y, z à coefficients appartenant au corps Ω. Si celle-ci admet un point (ξ, η, ζ), où ξ, η, ζ appartiennent à Ω, toutes les solutions de l'équation $C(x,y,z) = 0$ en nombres x, y, z appartenant à Ω sont données par un système de formules

$$\begin{aligned} x &= t(at_1^2+bt_1t_2+ct_2^2), \\ y &= t(a_1t_1^2+b_1t_1t_2+c_1t_2^2), \\ z &= t(a_2t_1^2+b_2t_1t_2+c_2t_2^2), \end{aligned} \tag{3}$$

où $a, b, c, a_1, b_1, c_1, a_2, b_2, c_2$ sont des nombres de Ω, et où les paramètres t, t_1, t_2 parcourent tous les nombres de Ω, indépendamment entre eux. Ainsi la solution complète en Ω est donnée par une identité.

(1) Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce travail.

D'après un résultat classique de Hurwitz, Hilbert [2] et Poincaré [3] il existe un résultat analogue pour toutes les courbes unicursales.

Supposons ensuite que Ω est un anneau. Dans ce cas la proposition sur la conique $C(x, y, z) = 0$ aura la forme réduite:

Il existe une représentation de la conique du type (3), où les coefficients appartiennent à l'anneau Ω. Lorsque les paramètres t, t_1, t_2 parcourent tous les nombres de Ω, on aura une infinité de solutions de l'équation $C(x, y, z) = 0$. Cependant, on n'a pas la certitude d'obtenir la solution complète dans Ω de cette manière. D'ailleurs, si Ω est l'anneau des nombres entiers rationnels les formules (2) donnent la solution complète de (1); voir Nagell [1], p. 226.

2. Quadriques. Remarques générales. Le résultat précédent sur les coniques peut être étendu aux quadriques; voir p. ex. Skolem [4], p. 30 et Conforto [5], p. 12. En effet, soit

$$F(x_1, x_2, \ldots, x_{n+1}) = 0 \tag{4}$$

l'équation d'une hypersurface du second degré en coordonnées (cartésiennes) homogènes $x_1, x_2, \ldots, x_{n+1}$ dans l'espace à n dimensions. Si les coefficients de la quadrique appartiennent au corps Ω, et si celle-ci admet un point $(\xi_1, \xi_2, \ldots, \xi_{n+1})$ en Ω, l'équation diophantienne (4) est satisfaite identiquement par un système de formules

$$x_i = tf_i(t_1, t_2, \ldots, t_n), \tag{5}$$

pour $i = 1, 2, \ldots, n+1$, où les f_i sont des formes quadratiques des paramètres $t_1, t_2, \ldots, t_n$ à coefficients appartenant à Ω. Lorsque les paramètres parcourent, indépendamment entre eux, tous les nombres de Ω, on aura la solution complète de (4) en Ω.

Ainsi, pour la quadrique

$$x_1^2 + x_2^2 + x_3^2 = x_4^2 \tag{6}$$

la solution complète dans un corps quelconque Ω est donnée par les formules

$$\begin{aligned} x_1 &= t(t_1^2 - t_2^2 - t_3^2), \\ x_2 &= 2tt_1t_2, \\ x_3 &= 2tt_1t_3, \\ x_4 &= t(t_1^2 + t_2^2 + t_3^2). \end{aligned} \tag{7}$$

Ce résultat ne reste plus vrai si Ω est un anneau. En effet, soit Ω l'anneau des nombres entiers (rationnels). Alors l'équation (6) a la solution $x_1 = 3$, $x_2 = 2$, $x_3 = 6$, $x_4 = 7$. Or, cette solution ne peut pas être obtenue par les formules (7) vu que le nombre 7 n'est pas la somme de trois carrés entiers. En fait, la solution complète de (6) dans l'anneau des nombres entiers est donnée par le système

$$\begin{aligned} x_1 &= t(t_1^2 - t_2^2 - t_3^2 + t_4^2), \\ x_2 &= t(2t_1t_2 - 2t_3t_4), \\ x_3 &= t(2t_1t_3 + 2t_2t_4), \\ x_4 &= t(t_1^2 + t_2^2 + t_3^2 + t_4^2), \end{aligned}$$

lorsque t, t_1, t_2, t_3, t_4 parcourent tous les nombres entiers; la démonstration est due à Carmichael, cf. [6], p. 38; il en résulte que le nombre des paramètres ne peut pas être diminué dans ce cas.

Soit $F(x_1, x_2, \ldots, x_m)$ un polynôme des variables $x_1, x_2, \ldots, x_m$. Si l'équation

$$F(x_1, x_2, \ldots, x_m) = 0 \tag{8}$$

représente une *hypersurface algébrique rationnelle*, celle-ci est (par définition) satisfaite identiquement par un système de formules

$$x_i = f_i(t_1, t_2, \ldots, t_r), \tag{9}$$

pour $i = 1, 2, \ldots, m$, où les f_i sont des fonctions rationnelles des paramètres $t_1, t_2, \ldots, t_r$.

On peut toujours supposer que 1° le polynôme F est homogène et 2° que les f_i sont des polynômes homogènes du même degré.

Supposons que les coefficients de F appartiennent au domaine Ω. Ici, domaine signifie ou un corps ou un anneau. Alors on peut se demander: Comment reconnaître si l'hypersurface (8) est rationnelle ou non? Lesquelles sont les conditions pour que les coefficients des f_i appartiennent à Ω? Comment déterminer le système (9) tel qu'il donne la *solution complète* de l'équation diophantienne (8) dans Ω?

Cependant, à l'état actuel des sciences mathématiques ces problèmes présentent des difficultés insurmontables dans le cas général.

On connaît un grand nombre d'équations diophantiennes résolubles par des identités sans que la solution ainsi obtenue soit complète; voir p. ex. Dickson [7], t. II, pp. 533-713. Comparez aussi Segre [8] et [9].

Dans les deux numéros suivants nous allons montrer comment on peut, d'une manière extrêmement simple, déterminer certains types d'équations diophantiennes à trois inconnues dont la solution complète est donnée par une identité.

3. Solution complète de quelques équations du type $X^N = F(Y, Z)$. Désignons par Ω un corps quelconque, et soit $F(y, z)$ une forme du degré $n \geqslant 2$ en y et z à coefficients appartenant à Ω. Nous allons établir le résultat suivant:

THÉORÈME 1. *Soit m un nombre naturel quelconque. L'équation*

$$X^{mn+1} = F(Y, Z) \tag{10}$$

est satisfaite identiquement par le système des formules

$$\begin{aligned} X &= F(U, V), \\ Y &= U[F(U, V)]^m, \\ Z &= V[F(U, V)]^m. \end{aligned} \tag{11}$$

Lorsque les paramètres U et V parcourent, indépendamment l'un de l'autre, tous les nombres de Ω, on aura la solution complète de l'équation (10) *en nombres X, Y et Z de Ω, sauf pour $X = 0$.*

Démonstration. Il est évident que les formules (11) satisfont identiquement à (10). Inversement, si les nombres X, Y et Z de Ω satisfont à (10), on aura

$$X = F(YX^{-m}, ZX^{-m}).$$

En y posant

$$U = YX^{-m}, \quad V = ZX^{-m}$$

on obtiendra évidemment les formules (11).

D'une façon tout à fait analogue on établira le

THÉORÈME 2. *Soit m un nombre naturel quelconque. L'équation*

$$X^{mn-1} = F(Y, Z) \tag{12}$$

est satisfaite identiquement par le système des formules

$$\begin{aligned} X &= [F(U, V)]^{-1}, \\ Y &= U[F(U, V)]^{-m}, \\ Z &= V[F(U, V)]^{-m}. \end{aligned} \tag{13}$$

Lorsque les paramètres U et V parcourent, indépendamment l'un de l'autre, tous les nombres de Ω, on aura la solution complète de l'équation (12) *en nombres X, Y et Z de Ω, sauf pour $X = 0$.*

Soit $F(y, z)$ une forme du second degré dont les coefficients appartiennent à Ω. Supposons que la conique

$$x^2 = F(y, z) \tag{14}$$

admet un point appartenant à Ω, et que la solution complète de l'équation (14) en Ω est donnée par les formules

$$x = WG(U, V), \quad y = WG_1(U, V), \quad z = WG_2(U, V), \tag{15}$$

où G, G_1 et G_2 signifient des formes quadratiques des paramètres U et V en Ω. D'après la proposition du numéro 1 les formules (15) satisfont identiquement à (14).

Cela étant, nous pouvons ajouter aux résultats précédents le

THÉORÈME 3. *Soit m un nombre naturel quelconque. Si l'équation* (14) *est résoluble en nombres x, y et z de Ω, qui ne sont pas tous $= 0$, l'équation*

$$X^{2m} = F(Y, Z) \tag{16}$$

est satisfaite identiquement par le système des formules

$$\begin{aligned} X &= G(U, V)W, \\ Y &= G_1(U, V)[G(U, V)]^{m-1}W^m, \\ Z &= G_2(U, V)[G(U, V)]^{m-1}W^m. \end{aligned} \tag{17}$$

Lorsque les paramètres U, V et W parcourent, indépendamment entre eux, tous les nombres de Ω, on aura la solution complète de l'équation (16) *en nombres X, Y et Z de Ω, sauf pour $X = 0$.*

Démonstration. En vertu de la définition des formes G, G_1 et G_2 il est évident que les formules (17) satisfont identiquement à (16). Inversement, si les nombres X, Y et Z satisfont à (16) on aura

$$X^2 = F(YX^{-m+1}, ZX^{-m+1}).$$

En y posant

$$x = X, \quad y = YX^{-m+1}, \quad z = ZX^{-m+1}$$

on tombera sur l'équation (14), dont la solution complète est donnée par les formules (15). Ainsi on aura pour X, Y et Z les expressions (17). Cela démontre le théorème 3.

Il serait facile de généraliser les résultats obtenus ci-dessus dans plusieurs directions. Nous allons retourner sur cette question prochainement.

Dans les théorèmes 1-3 Ω est un corps. *Supposons maintenant que Ω est un anneau.*

Considérons l'équation (10). Alors il est évident que les formules (11) nous donnerons une infinité de solutions en Ω de cette équation lorsque U et V parcourent tous les nombres de Ω. Cependant, on n'a plus la certitude d'obtenir la solution complète en Ω.

Considérons ensuite l'équation (12). Ici on peut évidemment remplacer le système (13) par le système

$$\begin{aligned} x &= [F(U, V)]^{n-1}, \\ y &= U[F(U, V)]^{mn-m-1}, \\ z &= V[F(U, V)]^{mn-m-1}. \end{aligned}$$

Par ces formules on aura une infinité de solutions de l'équation (12) en Ω, lorsque U et V parcourent tous les nombres de Ω.

Remarque. Soit $F(Y_1, Y_2, \dots, Y_r)$ une forme du degré $n \geqslant 2$ dans les r variables $Y_1, Y_2, \dots, Y_r$, à coefficients appartenant à Ω. Si nous posons, comme plus haut, $N = mn+1$, il est évident que le théorème 1 peut être généralisé de la manière suivante:

La solution complète dans Ω de l'équation diophantienne

$$X^N = F(Y_1, Y_2, \dots, Y_r) \tag{10'}$$

est donnée par l'identité réalisée par les formules

$$X = F(u_1, u_2, \dots, u_r), \qquad Y_i = u_i[F(u_1, u_2, \dots, u_r)]^m, \tag{11'}$$

pour $i = 1, 2, \dots, r$, lorsque les paramètres $u_1, u_2, \dots, u_r$, indépendamment entre eux, parcourent tous les nombres de Ω, excepté les solutions pour lesquelles $X = 0$.

Si l'hypersurface (10') est donnée sous la forme homogène

$$X^N = X_1^{N-n} F(Y_1, Y_2, \dots, Y_r),$$

les formules (11') doivent être remplacées par

$$X = [F(u_1, u_2, \dots, u_r)]v^{N-n}, \qquad X_1 = v^N,$$
$$Y_i = u_i[F(u_1, u_2, \dots, u_r)]^m; \qquad i = 1, 2, \dots, r.$$

Ainsi le nombre des paramètres s'est augmenté d'une unité.

Le théorème 2 peut être généralisé d'une façon analogue.

4. Solution de quelques équations du type $AX^M+BY^N+CZ^P = 0$. Désignons par Ω ou un anneau ou un corps, et soient a, b et c des nombres différents de zéro dans Ω. Soient encore M, N et P des nombres naturels $\geqslant 2$, tels que $(MN, P) = 1$. Nous allons étudier l'équation

$$ax^M + by^N = cz^P. \tag{18}$$

On vérifie aisément que cette équation est satisfaite identiquement par le système des formules

$$x = u(au^M + bv^N)^{Np} c^{Ns},$$
$$y = v(au^M + bv^N)^{Mp} c^{Ms}, \tag{19}$$
$$z = (au^M + bv^N)^q c^r,$$

où p, q, r et s sont des nombres entiers rationnels satisfaisant aux équations

$$MNp - Pq = -1 \quad \text{et} \quad MNs - Pr = 1. \tag{20}$$

Il en résulte

THÉORÈME 4. *Soit Ω un anneau. Si nous choisissons des valeurs positives pour les nombres p, q, r et s, les polynômes en u et v qui figurent dans* (19), *appartiendront à l'anneau Ω. Ainsi, on aura une infinité de solutions x, y et z de* (18), *lorsque les paramètres u et v parcourent tous les nombres de Ω.*

En général, on n'aura pas toutes les solutions de (18) par les formules (19), même si on suppose que Ω est un corps.

Considérons ensuite les cas lorsque P a une des valeurs $MNt+1$ ou $MNt-1$, t étant un nombre naturel. Nous allons établir le

THÉORÈME 5. *Soit Ω un corps. Si $P = MNt+1$, l'équation* (18) *est satisfaite identiquement par le système des formules*

$$x = u(au^M + bv^N)^{Nt} c^{-Nt},$$
$$y = v(au^M + bv^N)^{Mt} c^{-Mt}, \tag{21}$$
$$z = (au^M + bv^N) c^{-1}.$$

Lorsque les paramètres u et v, indépendamment l'un de l'autre, parcourent tous les nombres de Ω, on aura la solution complète de l'équation (18) *en nombres x, y et z de Ω, sauf pour $z = 0$.*

Démonstration. Vu que $P = MNt+1$ on peut satisfaire aux équations (20) en prenant $p = t$, $q = 1$ et $r = -1$, $s = -t$. Alors le système (19) aura la forme (21). D'autre part, si les nombres x, y et z de Ω satisfont à (18) pour $P = MNt+1$, on aura

$$a(xz^{-Nt})^M + b(yz^{-Mt})^N = cz.$$

En y posant

$$u = xz^{-Nt}, \qquad v = yz^{-Mt}$$

on obtiendra évidemment les formules (21).

D'une manière analogue on établira le

THÉORÈME 6. *Soit Ω un corps. Si $P = MNt-1$, l'équation* (18) *est satisfaite identiquement par le système des formules*

$$x = u(au^M + bv^N)^{-Nt} c^{Nt},$$
$$y = v(au^M + bv^N)^{-Mt} c^{Mt}, \tag{22}$$
$$z = (au^M + bv^N)^{-1} c.$$

Lorsque les paramètres u et v, indépendamment l'un de l'autre, parcourent tous les nombres de Ω, on aura la solution complète de l'équation (18) *en nombres x, y et z de Ω, sauf pour $z = 0$.*

Pour la démonstration on se sert du fait que les équations (20) ont les solutions $p = -t$, $q = -1$ et $r = 1$, $s = t$.

5. Exemples numériques. Pour illustrer les théorèmes 1 et 2 nous prenons l'équation

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

où $(N, 3) = 1$. La solution complète (pour $x \neq 0$) est donnée par les formules

$$x = (u^3+v^3)^r, \quad y = u(u^3+v^3)^\mu, \quad z = v(u^3+v^3)^\mu,$$

où $r = 1$ et $\mu = \frac{1}{3}(N-1)$ si $N \equiv 1 \pmod 3$ et où $r = -1$ et $\mu = -\frac{1}{3}(N+1)$ si $N \equiv -1 \pmod 3$.

Considérons ensuite l'équation

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

D'après le théorème 3 la solution complète de celle-ci (sauf pour $x = 0$) est donnée par les formules

$$x = (u^2+v^2)w, \quad y = (u^4-v^4)w^2, \quad z = 2uv(u^2+v^2)w^2.$$

Le théorème 4 peut être illustré par l'équation

$$x^6+179y^4 = z^5, \tag{23}$$

qui est satisfaite identiquement par les formules

$$x = u(u^6+179v^4)^4, \quad y = v(u^6+179v^4)^6, \quad z = (u^6+179v^4)^5.$$

Celles-ci ne donnent pas la solution complète de l'équation (23) lorsque Ω est le corps des nombres rationnels ordinaires. En effet, on vérifie aisément qu'on n'obtient pas la solution $x = 2$, $y = 1$, $z = 3$ de (23) par ces formules.

D'après le théorème 5 la solution complète de l'équation

$$x^2+y^2 = z^5,$$

sauf pour $z = 0$, est donnée par les formules

$$x = u(u^2+v^2)^2, \quad y = v(u^2+v^2)^2, \quad z = u^2+v^2.$$

Considérons finalement l'équation

$$x^2+y^3 = z^5.$$

D'après le théorème 6 celle-ci possède la solution complète (sauf pour $z = 0$) donnée par les formules

$$x = u(u^2+v^3)^{-3}, \quad y = v(u^2+v^3)^{-2}, \quad z = (u^2+v^3)^{-1}.$$

Dans la théorie de la résolution de l'équation générale du cinquième degré, la relation

$$T^2+H^3 = 1728F^5$$

joue un rôle important; voir Weber [10], t. 2, p. 485 et Perron [11], t.2, p. 233-240. Cette relation peut s'écrire

$$(2^{-3}\cdot 3^6\cdot T)^2+(2^{-2}\cdot 3^4\cdot H)^3 = (3^3\cdot F)^5.$$

Remarque. Il est évident que tous les théorèmes précédents sont aussi valables lorsque Ω est un domaine abstrait commutatif.

Travaux cités

[1] T. Nagell, *Introduction to number theory*, New York 1951.
[2] D. Hilbert und A. Hurwitz, *Über die diophantischen Gleichungen vom Geschlecht Null*, Acta Math. 14 (1891).
[3] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, Journ. de math. (5), 7 (1901).
[4] Th. Skolem, *Diophantische Gleichungen*, Ergebnisse der Mathematik, Bd. 5, Berlin 1938.
[5] F. Conforto, *Le superficie razionali*, Bologna 1939.
[6] R. Carmichael, *Diophantine Analysis*, New York 1915.
[7] L. E. Dickson, *History of the theory of numbers*, New York 1920.
[8] B. Segre, *Questions arithmétiques sur les variétés algébriques*, Colloque internat. d'algèbre et de théorie des nombres, Paris 1949.
[9] — *Arithmetical questions on algebraic varieties*, London 1951.
[10] H. Weber, *Lehrbuch der Algebra*, Braunschweig 1899.
[11] O. Perron, *Algebra*, Berlin 1927.

Reçu par la Rédaction le 16. 11. 1963