ARKIV FÖR MATEMATIK Band 8 nr 7

1.68 11 3 Communiqué le 11 septembre 1968

Remarques sur une catégorie d'équations diophantiennes à deux indéterminées

Par TRYGVE NAGELL

§ 1. Sur la résolubilité de l'équation $y^2-1=z^p$

1. Dans un travail publié en 1921 j'ai étudié la possibilité de résoudre l'équation diophantienne

$$y^2-1=z^p \tag{1}$$

en nombres naturels y et z, lorsque p est un nombre premier $\geqslant 5$. Pour certaines catégories de nombres premiers p j'ai pu montrer dans le dit travail que cette équation n'a pas de solutions. La démonstration s'appuie sur des propriétés du corps quadratique engendré par $\sqrt{\varepsilon p}$, où $\varepsilon=+1$ ou $=-1$ suivant que $p\equiv 1$ ou $\equiv -1 \pmod 4$; voir Nagell [1][1]. Nous allons revenir sur une partie de ce travail plus loin dans le numéro **3**.

Ensuite en 1935, par une autre méthode très simple, j'ai pu établir le résultat suivant (voir Nagell [2]):

Théorème 1. *Si p est un nombre premier $\geqslant 5$, qui n'est pas $\equiv 1 \pmod 8$, l'équation (1) n'admet aucune solution en nombres naturels y et z.*

Vu que ce résultat semble être resté inconnu je me permets d'en recapituler la démonstration.

On voit aisément que le nombre z dans (1) est nécessairement pair, abstraction faite de la solution $y=0$, $z=-1$. En effet, si z est impair, cette équation entraîne

$$y-1=a^p, \quad y+1=b^p,$$

où a et b sont des nombres naturels, tels que $ab=z$. Donc

$$a^p-b^p=-2,$$

d'où résulte $a=-1$, $b=1$. Si z est pair on aura

$$y\mp 1=2a^p, \quad y\pm 1=2^{p-1}b^p,$$

où a et b sont des nombres naturels, tels que $2ab=z$, donc

$$a^p-2^{p-2}b^p=\mp 1. \tag{2}$$

[1] Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce mémoire.

Alors, vu que le quotient $(a^p \pm 1)/(a \pm 1)$ est impair, il résulte de cette équation que $a \pm 1$ est divisible par 2^{p-2}, donc $a \geqslant 2^{p-2} - 1$ et

$$z = 2ab \geqslant 2^{p-1} - 2 > 2^{p-2}. \tag{3}$$

Nous allons ensuite montrer que le nombre y est nécessairement divisible par p. En effet, si y n'est pas divisible par p, l'équation (1) entraîne

$$\frac{z^p + 1}{z+1} = c^2, \quad z + 1 = d^2, \tag{4}$$

où c et d sont des nombres naturels impairs, tels que $y = cd$.

Or, j'ai montré dans une note antérieure que la première de ces équations est impossible pour $|z| > 2^{p-3}$; voir Nagell [3]. Cela étant en contradiction avec l'inégalité (3), on en conclut que le nombre y doit être divisible par p. On peut d'ailleurs aussi obtenir ce résultat en utilisant le théorème suivant dû à C. Störmer (voir [4]):

Désignons par u_1, v_1 les solutions fondamentales de l'équation

$$u^2 - Dv^2 = 1.$$

Alors, parmi toutes les solutions v, il n'y aura aucune ou bien il y en aura une seule, à savoir v_1, jouissant de la propriété que chacun de ces diviseurs premiers divise D.

En effet, d'après (4), l'équation (1) peut s'écrire

$$y^2 - (d^2-1)[(d^2-1)^h]^2 = 1, \tag{5}$$

où $h = \frac{1}{2}(p-1)$. Les solutions fondamentales de l'équation

$$u^2 - (d^2-1)v^2 = 1$$

étant $u_1 = d$ et $v_1 = 1$, il résulte du théorème de Störmer que l'équation (5) est impossible.

Le nombre y étant ainsi divisible par p, il résulte de (1)

$$z + 1 = pc^2, \quad \frac{z^p + 1}{z+1} = pd^2, \tag{6}$$

où c et d sont des nombres naturels impairs. En écrivant (1) de la manière suivante

$$y^2 - 2 = z^p - 1 = (z-1)(z^{p-1} + \ldots + z + 1),$$

on voit que $z - 1$ est nécessairement $\equiv \pm 1 \pmod 8$, ce qui entraîne ou $z \equiv 2$ ou $z \equiv 0 \pmod 8$. En combinant ceci avec la première des équations (6) on aura ou $p \equiv 3$ ou $p \equiv 1 \pmod 8$. L'équation (1) est par conséquent impossible pour $z > 0$, lorsque $p \equiv 5$ ou $p \equiv 7 \pmod 8$.

Supposons ensuite que $p \equiv 3 \pmod 8$. Comme b est indivisible par p, l'équation (2) entraîne

$$a^{p-1} \mp a^{p-2} + \ldots + a^2 \mp a + 1 = f^p \tag{7}$$

et
$$a \pm 1 = 2^{p-2} g^p, \tag{8}$$

f et g étant des nombres naturels tels que $b = fg$. De la dernière de ces équations on aura $a \equiv \mp 1 \pmod 8$. La première équation donne par suite

$$p \equiv f^p \equiv f \equiv 3 \pmod 8.$$

Le nombre f est positif et $\equiv 1 \pmod p$. Avec le symbole de Jacobi nous aurons donc

$$\left(\frac{p}{f}\right) = -\left(\frac{f}{p}\right) = -\left(\frac{1}{p}\right) = -1. \tag{9}$$

Or, nous avons d'après (6)

$$z = 2ab = 2afg = pc^2 - 1,$$

ce qui entraîne évidemment

$$\left(\frac{p}{f}\right) = +1,$$

en contradiction avec (9). Le Théorème 1 se trouve donc démontré. D'ailleurs, nous avons aussi obtenu le résultat suivant :

Théorème 2. *Si p est un nombre premier $\geqslant 5$, qui n'est pas $\equiv 1 \pmod 8$, l'équation (2) n'admet aucune solution en nombres entiers rationnels a et b pour $b \neq 0$.*

Remarque. Il est bien connu que l'équation

$$x^3 - 2y^3 = 1$$

n'admet pas d'autres solutions en nombres entiers rationnels que $x = 1$, $y = 0$ et $x = -1$, $y = -1$; voir Legendre [18], t. 2, p. 8.

2. Il résulte de ce qui précède : Si l'équation (1) admet une solution avec $z \neq 0$, le nombre premier p, supposé > 3, doit être $\equiv 1 \pmod 8$. Dans ce cas il résulte de (6) que $z \equiv 0 \pmod 8$. Vu que $z = 2ab$ on en conclut que b est divisible par 4. Il en résulte que g est divisible par 4, vu que $b = fg$. De l'équation (8) on obtiendra donc

$$a \geqslant 2^{3p-2} - 1. \tag{10}$$

Encore, l'équation (7) donnera

$$b = fg \geqslant 4f \geqslant 4\sqrt[p]{(a^p+1)/(a+1)}.$$

Vu que la fonction $(x^p+1)/(x+1)$ croît de façon monotone pour $x > 1$, on aura, en profitant de l'inégalité (10),

$$b > 4(2^{3p-2} - 1) \cdot 2^{-3+2/p} > \tfrac{1}{2}(2^{3p-2} - 1).$$

Donc, s'il existe une solution de (1) on a

$$z = 2ab > (2^{3p-2} - 1)^2. \tag{11}$$

3. Dans le travail [1], cité plus haut, nous avons établi le résultat que voici :

Théorème 3. *Soit p un nombre premier $\equiv 1$ (mod 8), et désignons par $\varepsilon = u + v\sqrt{p}$ l'unité fondamentale, $\varepsilon > 1$, du corps quadratique $K(\sqrt{p})$. Alors, si la congruence $u + v \equiv 1$ (mod 8) n'est pas satisfaite, l'équation (1) n'admet aucune solution en nombres naturels y et z.*

Nous allons en reproduire la démonstration. D'après les conditions données et les résultets obtenus dans le numéro 1, il suffit de montrer que l'équation

$$\frac{x^p - 1}{x - 1} = py^2, \tag{13}$$

obtenue de (6) en y mettant $x = -z$ et $y = d$, est impossible lorsque x est pair et $u + v \not\equiv 1 \pmod 8$. Une conséquence de cette équation est alors que

$$x \equiv 0 \pmod 8. \tag{14}$$

En prenant la norme de l'unité ε on aura

$$u^2 - pv^2 = -1,$$

d'où il résulte que $u \equiv 0 \pmod 4$ et $v =$ nombre impair; u et v sont tous les deux positifs, vu que $\varepsilon > 1$.

D'après la théorie de la division du cercle nous avons l'identité suivante :

$$4\,\frac{x^p - 1}{x - 1} = [Y(x)]^2 - p\,[Z(x)]^2, \tag{15}$$

où $Y(x)$ et $Z(x)$ sont des polynomes en x à coefficients entiers rationnels, tels que

$$\left.\begin{aligned} Y(x) &= 2 + x + \tfrac{1}{4}(p+3)\,x^2 + \ldots + x^{p-1} + 2x^p, \\ Z(x) &= x + x^2 + \ldots + x^{p-1}, \end{aligned}\right\} \tag{16}$$

où $v = \frac{1}{2}(p-1)$. Pour la démonstration de ces faits voir p. ex. Dedekind–Dirichlet [5], p. 369–375.

Supposons que les nombres $Y(x_0)$ et $Z(x_0)$, x_0 entier rationnel quelconque, aient le commun facteur premier $q > 2$. Dans ce cas on obtient les deux congruences

$$Y(x) \equiv (x - x_0) f_1(x) \pmod q,$$

$$Z(x) \equiv (x - x_0) f_2(x) \pmod q,$$

et donc, vu que $q > 2$,

$$\frac{x^p - 1}{x - 1} \equiv (x - x_0)^2 f(x) \pmod q.$$

En vertu d'un théorème de la théorie des congruences de degré supérieur il en résulte que q divise le discriminant p^{p-2} du polynome $F_p(x) = (x^p - 1)/(x - 1)$; voir p. ex. Nagell [6], Theorem 48. Il faut donc que $q = p$; il en résulterait, en vertu de (15), que $F_p(x_0)$ serait divisible par p^2; or il est bien connu que cela est impossible ([6], Theorem 95). Donc, les nombres $Y(x)$ et $Z(x)$ sont premiers entre eux, s'ils sont tous les deux

impairs. S'ils sont tous les deux pairs, les nombres $\frac{1}{2}Y(x)$ et $\frac{1}{2}Z(x)$ sont premiers entre eux, vu que $F_p(x)$ est toujours impair. Dans ce qui suivra nous écrirons, pour raccourcir, Y et Z en omettant x.

Let coefficients des polynomes

$$U=\tfrac{1}{2}Y+\tfrac{1}{2}\sqrt{p}\,Z \text{ et } V=\tfrac{1}{2}Y-\tfrac{1}{2}\sqrt{p}\,Z$$

sont évidemment des entiers dans le corps $\mathbf{K}(\sqrt{p})$. On en conclut que le polynome

$$\tfrac{1}{2}(Y+Z)=U-\tfrac{1}{2}(\sqrt{p}-1)\,Z$$

a les coefficients entiers rationnels.

Les polynomes U et V sont positifs pour toute valeur réelle de x. En effet, les racines de $U=0$ et $V=0$ sont imaginaires, et les coefficients de x^ν sont $=1$.

Il résulte de l'équation (13) que le plus grand commun diviseur des idéaux (U) et (V) est égal à $(\sqrt{p})$, vu que le plus grand commun diviseur de Y et Z divise 2. Par conséquent, l'équation (13) entraîne

$$(U)=(\sqrt{p})\cdot\mathfrak{j}^2,$$

où $\mathfrak{j}$ est un idéal dans $\mathbf{K}(\sqrt{p})$. Vu que le nombre h des classes d'idéaux dans $\mathbf{K}(\sqrt{p})$ est impair, il est évident que $\mathfrak{j}$ est un idéal principal; voir p. ex. Sommer [7], p. 110. On aura par suite une équation de la forme

$$\tfrac{1}{2}Y+\tfrac{1}{2}\sqrt{p}\,Z=\eta\sqrt{p}\,(\tfrac{1}{2}a+\tfrac{1}{2}\sqrt{p}\,b)^2, \tag{17}$$

où η est une unité dans $\mathbf{K}(\sqrt{p})$, et où a et b sont des nombres entiers rationnels, premiers entre eux, tels que $\pm y=\frac{1}{4}(a^2-pb^2)$.

Il faut dans (17) que l'unité η soit positive, vu que U est toujours positif. Alors il suffit de considérer le cas où η est l'unité fondamentale $\varepsilon=u+v\sqrt{p}$. *D'ailleurs, on peut remplacer ε par une puissance quelconque ε^m, où m est positif et impair.* Par conséquent, en prenant dans (17) $\eta=\varepsilon$, on obtient le système

$$\left.\begin{aligned} 2\,Y&=pv(a^2+pb^2)+2\,abpu,\\ 2\,Z&=u(a^2+pb^2)+2\,abpv.\end{aligned}\right\} \tag{18}$$

Vu que $x\equiv 0 \pmod 8$, il résulte de (16) que les nombres Y et Z doivent satisfaire aux congruences

$$\left.\begin{aligned} &Y\equiv 2 \pmod 8,\ Z\equiv 0 \pmod 8,\\ &\tfrac{1}{2}(Y+Z)\equiv 1 \pmod 8.\end{aligned}\right\} \tag{19}$$

Supposons d'abord que a et b soient tous les deux impairs. Alors, il résulte de (18), u étant $\equiv 0 \pmod 4$,

$$2\,Y\equiv 2pv \pmod 8,$$

ce qui est impossible, le nombre à gauche étant divisible par 4. Soient ensuite a et b pairs, $a=2a_1$ et $b=2b_1$. Alors, on obtient de (18)

$$\tfrac{1}{2}(Y+Z)=(u+pv)(a_1^2+pb_1^2)+2(u+v)a_1b_1p,$$
$$\tfrac{1}{2}Y=pv(a_1^2+pb_1^2)+2a_1b_1pu.$$

Il en résulte modulo 8

$$\tfrac{1}{2}Y\equiv v(a_1^2+b_1^2)\pmod 8,$$
$$\tfrac{1}{2}(Y+Z)\equiv 1\equiv(u+v)(a_1+b_1)^2\pmod 8.$$

Puisque $\frac{1}{2}Y$ est impair, il s'ensuit que $a_1^2+b_1^2$ est impair. On obtient donc, vu que $(a_1+b_1)^2\equiv 1 \pmod 8$,

$$u+v\equiv 1\pmod 8.$$

Cela démontre le Théorème **3**.

Le résultat peut aussi être formulé de la manière suivante :

Théorème 3 bis. *Si p est un nombre premier $\equiv 1$ (mod 8) tel que le nombre 2 ne soit pas un reste biquadratique modulo p, l'équation (1) n'admet aucune solution en nombres naturels y et z.*

Démonstration. Dans la démonstration du Théorème **3** nous avons vu que l'unité fondamentale $\varepsilon\ (>1)$ peut être échangée contre la puissance ε^m, où m est un nombre *naturel impair* quelconque. Pour le but actuel nous choisissons $m=h=$au nombre des classes d'idéaux dans le corps $\mathbf{K}(\sqrt{p})$. Alors, si nous posons $\varepsilon^h=u_1+v_1\sqrt{p}$, la condition $u+v\not\equiv 1 \pmod p$ dans le Théorème **3** doit être échangée contre la condition $u_1+v_1\not\equiv 1 \pmod p$. Ici v_1 est impair et $u_1\equiv 0 \pmod 4$. Vu que $p\equiv 1 \pmod 8$ on a $p=A^2+16B^2$, où A et B sont des entiers rationnels; A peut être choisi $\equiv 1 \pmod 4$.

D'après un résultat de Hasse (voir [8], p. 407–408) on a alors les relations

$$\left.\begin{aligned} u_1&=\tfrac{1}{2}A(A_1^2-B_1^2)-4BA_1B_1,\\ v_1&=\tfrac{1}{2}(A_1^2+B_1^2),\end{aligned}\right\} \tag{20}$$

où A_1 et B_1 sont des entiers rationnels. Puisque v_1 est impair, A_1 et B_1 sont aussi impairs.

Supposons maintenant que $u_1+v_1\equiv 1 \pmod 8$. Alors on obtient de (20)

$$u_1+v_1=\tfrac{1}{2}(A+1)A_1^2-\tfrac{1}{2}(A-1)B_1^2-4BA_1B_1$$

et par suite

$$u_1+v_1\equiv 1\equiv 1-4B\pmod 8.$$

Il en résulte que B doit être pair. Inversement, si B est pair on aura $u_1+v_1\equiv 1 \pmod 8$. Par conséquent, si B est impair l'équation (1) n'a pas de solutions. Pour qu'il existe une solution il faut donc que B soit $=2C$. Dans ce cas on a alors

$$p=A^2+64C^2. \tag{21}$$

D'après un résultat de Gauss (comparez Hasse [9], § 14, p. 69) la condition nécessaire et suffisante pour que le nombre 2 soit un reste biquadratique modulo le nombre premier $p\equiv 1 \pmod 4$, est que p soit de la forme (21). Le Théorème **3bis** se trouve ainsi démontré.

D'après E. Lehmer (voir [10]) la densité des nombres premiers de la forme (21) est égale à $\frac{1}{8}$. Alors, le Théorème **3bis** montre que l'équation (1) n'a pas de solutions pour au moins la moitié des valeurs de $p \equiv 1 \pmod 8$.

4. Dans un travail publié en 1940 R. Obláth (voir [11]) a montré que l'équation (1) admet au plus une seule solution en nombres naturels y et z, lorsque p est un nombre premier $p \geqslant 5$. Sa démonstration repose principalement sur l'application d'un théorème de Siegel (voir [12]) sur l'inégalité diophantienne

$$|ax^n - by^n| \leqslant c, \tag{22}$$

où a, b, c et n sont des nombres naturels, $n \geqslant 3$. Le théorème en question dit que l'inégalité (22) admet au plus une seule solution en nombres naturels x et y, premiers entre eux, lorsque

$$|\sqrt{ab}| \geqslant 188\, nc^4.$$

Obláth applique ce résultat à l'équation (2). Il a connu mon premier travail [1]; cependant, il semble qu'il n'a pas observé mon travail [2] publié en 1935. Donc, le résultat de Obláth regarde seulement une classe particulière de nombres premiers $\equiv 1 \pmod 8$. Celui-ci peut être formulé ainsi qu'il suit (en ayant égard aux résultats antérieurs) :

Théorème 4. *Soit p un nombre premier $\equiv 1$ (mod 8) tel que le nombre 2 soit un reste biquadratique modulo p. Alors l'équation (1) admet au plus une seule solution en nombres naturels y et z.*

Jusqu'ici on ne connaît aucun cas dans lequel l'équation (1) est résoluble. Une solution eventuelle z doit satisfaire à l'inégalité (11).

Les nombres premiers $\equiv 1 \pmod 8$ inférieurs à 600 pour lesquels le nombre 2 est un reste biquadratique sont : 73, 89, 113, 233, 257, 281, 337, 353, 577, 593. Parmi les 66 nombres premiers $\equiv 1 \pmod 8$ inférieurs à 2000 il y en a 32 pour lesquels le nombre 2 est un reste biquadratique; on a $\pi(2000) = 303$. La densité des nombres premiers p pour lesquels nous avons démontré l'impossibilité de l'équation (1) est égale à 7/8.

Il reste encore à traiter le cas où l'exposant p dans (1) sera remplacé par un nombre composé N. Dans le § 5 nous allons montrer que dans ce cas l'équation

$$y^2 - 1 = z^N$$

est impossible en nombres naturels y et z.

§ 2. Sur les équations du type $y^2 - 1 = tz^n$

5. Après nos recherches sur l'équation $y^2 - 1 = z^p$ il est naturel que l'intérêt se portera sur l'équation plus générale

$$y^2 - 1 = tz^n, \tag{23}$$

où t et n sont des nombres naturels, $t > 1$ et $n \geqslant 5$; y et z sont des nombres naturels

variables. Il est évident que cette équation présentera des difficultés beaucoup plus grandes que dans le cas $t=1$. On peut se demander s'il y a des possibilités pour obtenir des bornes bien basses pour le nombre des solutions. On voit aisément que le théorème de Siegel cité plus haut (voir [12]) peut servir à ce but. Il y a surtout les deux suppléments suivants dûs à Domar (voir [13]) qui peuvent faire bon service pour trouver de telles bornes :

1° L'équation diphantienne

$$|Ax^n - By^n| = 1,$$

où A, B et n sont des nombres naturels, $n \geqslant 5$, admet au plus deux solutions en nombres naturels x et y.

2° L'équation diophantienne

$$|x^n - My^n| = 1,$$

où M et n sont des nombres naturels, $n \geqslant 5$, admet au plus une seule solution en nombres naturels x et y, sauf peut-être pour $M=2$ et si $n=5$ ou $=6$ pour $M=2^n \pm 1$.

En effet, si y est pair (ce qui entraîne que t et z sont impairs) on obtient de (23) un nombre fini de systèmes

$$y \pm 1 = t_1 u^n, \quad y \mp 1 = t_2 v^n,$$

où t_1, t_2, u et v sont des nombres naturels tels que $t_1 t_2 = t$ et $uv = z$. Il en résulte

$$\pm 2 = t_1 u^n - t_2 v^n.$$

D'après le théorème de Siegel cette équation admet au plus une seule solution en nombres naturels u et v, lorsque

$$t \geqslant (3008n)^2.$$

Si y est impair on obtiendra de (23) un nombre fini de systèmes

$$y \pm 1 = 2t_1 u^n, \quad y \mp 1 = 2t_2 v^n,$$

où t_1, t_2, u et v sont des nombres naturels tels qu'on ait ou $4t_1 t_2 = t$, $uv = z$, ou $2^{n-2} t = t_1 t_2$ et $2uv = z$. Il en résulte

$$\pm 1 = t_1 u^n - t_2 v^n.$$

D'après le premier théorème de Domar cette équation admet au plus deux solutions.

On aura ainsi une borne supérieure du nombre des solutions de (23) qui dépend du nombre des diviseurs de t, une borne qui n'est pas très satisfaisante. Cependant, dans des cas particuliers on peut obtenir des bornes très basses. Considérons p. ex. l'équation

$$y^2 - 1 = 2qz^n, \tag{24}$$

où q est un nombre premier impair. Ici z est nécessairement pair. Une possibilité est donnée par le système

$$y \pm 1 = 2qu^n, \quad y \mp 1 = 2^n v^n,$$

où $2uv = z$. Il en résulte l'équation

$$\pm 1 = qu^n - 2^{n-1}v^n,$$

qui admet, d'après Domar, au plus deux solutions. L'autre possibilité est donnée par le système

$$y \pm 1 = 2u^n, \quad y \mp 1 = q2^n v^n,$$

où $2uv = z$. Il en résulte la relation

$$\pm 1 = u^n - q2^{n-1}v^n,$$

qui admet, d'après Domar, au plus une seule solution. Donc, l'équation (24) admet au plus trois solutions; cela se réduira à une seule solution si le nombre 2 n'est pas le reste d'une puissance n-ième modulo q.

Pour $q=2$ et $q=1$ le raisonnement sera encore plus simple; lorsque $q=2$ l'équation (24) n'a pas de solution; lorsque $q=1$ il y a au plus une seule solution.

D'une manière analogue on montrera aussi que le nombre des solutions de chacune des équations

$$y^2 - 1 = 4qz^n \quad \text{et} \quad y^2 - 1 = 8qz^n$$

est au plus égal à trois.

Il serait facile de généraliser ces résultats, mais nous nous bornons à ces exemples.

§ 3. Sur les équations du type $y^2 - q^2 = z^p$

6. Considérons une autre généralisation de l'équation $y^2 - 1 = z^p$, donnée par

$$y^2 - q^2 = z^p, \tag{25}$$

où p et q désignent des nombres premiers impairs, $p \geqslant 5$; y et z sont des nombres naturels variables.

Supposons d'abord que y ne soit pas divisible par q. Si y est pair l'équation (25) entraîne le système

$$y + q = u^p, \quad y - q = v^p,$$

où $uv = z$, et par suite

$$2q = u^p - v^p.$$

Il en résulte ou le système

$$2q = u - v, \quad \frac{u^p - v^p}{u - v} = 1,$$

ou le système

$$2 = u - v, \quad \frac{u^p - v^p}{u - v} = q. \tag{26}$$

La seconde équation du premier système entraîne évidemment $uv = 0$, donc $z = 0$.

Le système (26) donnera

$$2q = (v+2)^p - v^p, \tag{27}$$

où le membre à droite est une fonction de v qui croît d'une façon monotone pour

$v>0$. Il en résulte que l'équation (27) possède au plus une seule solution v; une condition nécessaire pour l'existence d'une solution est évidemment que $q\equiv 1 \pmod p$.

Soit maintenant y impair. Alors, on obtient de (25) le système

$$y\pm q = 2u^p, \quad y\mp q = 2^{p-1}v^p$$

où $2uv=z$. Il s'ensuit

$$\pm q = u^p - 2^{p-2}v^p.$$

Si nous supposons que le nombre 2 ne soit pas le reste d'une puissance p-ième modulo q, cette équation n'a pas de solutions.

Supposons ensuite que y soit divisible par q. Si y est pair nous aurons le système suivant

$$y\pm q = qu^p, \quad y\mp q = q^{p-1}v^p,$$

où $quv=z$. Il s'ensuit que

$$2 = u^p - q^{p-2}v^p.$$

Cette équation est impossible si le nombre 2 n'est pas le reste d'une puissance p-ième modulo q.

Si y est impair on obtient l'un ou l'autre des deux systèmes

$$y\pm q = 2qu^p, \quad y\mp q = (2q)^{p-1}v^p;$$

$$y\pm q = 2^{p-1}qu^p, \quad y\mp q = 2q^{p-1}v^p,$$

où $z=2quv$. Le premier système donnera

$$\pm 1 = u^p - (2q)^{p-2}v^p,$$

équation qui admet au plus une seule solution d'après Domar. Du second système on aura

$$\pm 1 = 2^{p-2}u^p - q^{p-2}v^p,$$

équation qui est impossible si le nombre 2 n'est pas le reste d'une puissance p-ième modulo q.

Donc, dans ce numéro nous avons obtenu le résultat suivant : L'équation (25) admet au plus deux solutions, si le nombre 2 n'est pas le reste d'une puissance p-ième modulo q.

§ 4. Sur les équations du type $x^3 - 1 = ty^n$

7. Dans un travail antérieur, publié en 1921, j'ai démontré que les équations

$$x^3 \mp 1 = y^n,$$

$n\geqslant 2$, sont impossibles en nombres naturels x et y, sauf pour $n=2$, $x=2$, $y=3$ avec le signe inférieur; voir Nagell [13], p. 12–14.

Nous allons examiner certains cas de l'équation plus générale

$$x^3-1=ty^n, \tag{28}$$

où t est un nombre naturel >1, qui n'est divisible par aucun nombre premier $\equiv 1 \pmod 6$. L'exposant n sera supposé impair.

Nous allons déterminer toutes les solutions de cette équation en nombres entiers rationnels x et y, avec $y \neq 0$, à l'aide des théorèmes suivants :

Si n n'est pas une puissance de 3, l'équation diophantienne

$$x^2+x+1=y^n \tag{29}$$

est impossible en nombres entiers rationnels x et y, sauf pour $y=1$ et $x=0$ ou $=-1$.

L'équation diophantienne

$$x^2+x+1=3y^n, \tag{30}$$

où $n>2$, est impossible en nombres entiers rationnels x et y, sauf pour $y=1$ et $x=1$ ou $=-2$.

On trouvera la démonstration de ces théorèmes dans Nagell [15], p. 1–12.

Ljunggren a établi le résultat suivant, supplément au premier de ces théorèmes :

Soit n une puissance de 3. Alors l'équation (29) admet pour $y>1$ seulement les solutions suivantes : $n=3$, $y=7$ et $x=18$ ou $=-19$.

Pour la démonstration voir Ljunggren [16].

Si $x-1$ n'est pas divisible par 3 on obtient de (28) le système

$$x^2+x+1=u^n, \quad x-1=tv^n,$$

où $uv=y$. D'après les théorèmes que nous venons de citer, il résulte de ce système qu'on a les trois possibilités suivantes :

1° $u=1$, $x=-1$, $t=2$, $v=-1$ et $y=-1$;

2° $u=7$, $x=18$, $n=3$, $t=17$, $v=1$ et $y=7$;

3° $u=7$, $x=-19$, $n=3$, $t=20$, $v=-1$ et $y=-7$.

Le cas $u=1$, $x \leqslant 0$ donnera pour t la valeur 1 que nous avons exclue.

Si $x-1$ est divisible par 3 on aura le système

$$x^2+x+1=3u^n, \quad x-1=\tfrac{1}{3}tv^n.$$

Il faut donc que $u=1$. On aura par suite $x=-2$, $v=-1$, $t=9$ et $y=-1$. Il faut exclure le cas $x=1$ qui donnera $v=0$ et $y=0$.

Les solutions de (28) sont donc données par les relations

$$\begin{gathered}(-1)^3-1=2\cdot(-1)^n,\\ 18^3-1=17\cdot 7^3,\\ (-19)^3-1=20\cdot(-7)^3,\\ (-2)^3-1=9\cdot(-1)^n.\end{gathered}$$

§ 5. Sur l'équation $y^2 - 1 = z^N$

8. Nous allons finalement ajouter aux résultats obtenus dans le § 1 le théorème suivant :

Théorème 5. *Si N est un nombre naturel composé, l'équation*

$$y^2 - 1 = z^N \tag{29}$$

n'admet aucune solution en nombres naturels y et z.

Démonstration. Ce théorème est banal lorsque N est pair. Il est évident lorsque N est divisible par 3; en effet, Euler a montré que, pour $N=3$, l'équation (29) n'admet pas d'autres solutions en nombres naturels que $y=3$, $x=2$; voir Euler [17], Theorema 10, p. 56.

Alors, on voit aisément qu'il suffit de considérer les deux cas suivants : 1° $N=p^2$ et 2° $N=pq$, où p et q sont des nombres premiers différents $\geqslant 5$.

Vu que N est impair, on peut en général raisonner sur l'équation (29) de la même manière qu'auparavant sur l'équation (1) dans le numéro 1. Ainsi il se montre que z est nécessairement pair. Alors l'équation (2) restera vraie si l'on y remplace p par N. L'équation (29) peut s'écrire

$$y^2 - 1 = z_1^p,$$

où $z_1 = z^{N/p}$. On en déduit, comme au numéro 1, que y est divisible par p; et dans le second cas on aura d'une façon analogue que y est aussi divisible par q. Donc z n'est jamais divisible ni par p et ni par q.

Premier cas : $N = p^2$.

Par la même méthode que nous avons employée plus haut au numéro 1 dans le cas de $N=p$, nous montrons que y doit être divisible par p. Donc, on obtient de (29), en posant $z_1 = z^p$, le système

$$\frac{z_1^p + 1}{z_1 + 1} = pc^2, \quad z^p + 1 = z_1 + 1 = dp^2,$$

où c et d sont des nombres naturels, tels que $y = pcd$. De la dernière de ces équations on aura le système

$$\frac{z^p + 1}{z+1} = pc_1^2, \quad z + 1 = p^2 d_1^2 = p^2 d_1^2 = e^2,$$

c_1, d_1 et e étant des nombres naturels. Alors, l'équation (29) peut s'écrire

$$y^2 - (e^2-1)[(e^2-1)^h]^2 = 1,$$

où $h = \frac{1}{2}(p^2-1)$. Donc, on peut appliquer le même théorème de Störmer que plus haut dans le numéro 1. On en conclut que l'équation (29) est impossible pour $N=p^2$.

Second cas : $N = pq$.

Il est évident que dans ce cas l'équation (2) sera remplacée par

$$a^N - 2^{N-2}b^N = \mp 1, \tag{30}$$

où a et b sont des nombres naturels tels que $z = 2ab$. z n'est divisible ni par p ni par q. En y posant $a_1 = a^q$ et $b_1 = b^p$ nous aurons le système

$$\frac{a_1^p \pm 1}{a_1 \pm 1} = c^q, \quad a_1 \pm 1 = 2^{N-2}d^q,$$

où c et d sont des nombres naturels, tels que $cd = b_1$. Nous aurons donc une solution $u = a$ et $v = d$ de l'équation

$$u^q - 2^{N-2}v^q = \mp 1. \tag{31}$$

D'après le second théorème de Domar, cité dans le numéro 5, l'équation (31) admet au plus une seule solution en nombres naturels u et v. Or, l'équation (30) fournit déjà la solution $u = a^p$ et $v = b^p$ de l'équation (31). En vertu de cette contradiction nous concluons que l'équation (30) est impossible. Donc l'équation (29) l'est aussi. Le Théorème 5 se trouve ainsi démontré.

En résumant tous les résultats obtenus sur l'équation

$$y^2 - 1 = z^n, \tag{32}$$

nous pouvons énoncer le

Théorème 6. *Soit n un nombre naturel > 3, et supposons que l'équation (32) ait la solution en nombres naturels $y = y_1$, $z = z_1$. Alors, n est nécessairement un nombre premier $\equiv 1$ (mod 8) tel que le nombre 2 soit un reste biquadratique modulo n. De plus, la solution z_1 est divisible par 8 et doit satisfaire à l'inégalité (11). Outre y_1, z_1 il n'y a pas d'autres solutions.*

Une conséquence immédiate de ce résultat est la généralisation suivante du Théorème 2 dans le numéro 1 :

Théorème 7. *Soit n un nombre naturel > 3, et supposons que l'équation*

$$a^n - 2^{n-2}b^n = \mp 1$$

ait la solution en nombres naturels $a = a_1$, $b = b_1$. Alors, n est nécessairement un nombre premier $\equiv 1$ (mod 8) tel que le nombre 2 soit un reste biquadratique modulo n. De plus, la solution b_1 est divisible par 4. Outre a_1, b_1 il n'y a pas d'autres solutions.

L'Institut de mathématiques de l'Université Uppsala.

INDEX BIBLIOGRAPHIQUE

1. NAGELL, T., Sur l'impossibilité de l'équation indéterminée $z^p + 1 = y^2$, *Norsk Matematisk Forenings Skrifter*, Ser. 1, Nr. 4, Kristiania 1921.
2. NAGELL, T., Sur une équation diophantienne à deux indéterminées, *Det kgl. Norske Videnskabers Selskab, Forhandl.* Bd. VII, Nr. 38, Trondhjem 1935.

3. NAGELL, T., Sur l'équation indéterminée $(x^n-1)/(x-1)=y^2$, *Norsk Matematisk Forenings Skrifter*, Ser. 1, Nr. 3, Kristiania 1921.
4. STÖRMER, C., Solution d'un problème curieux qu'on rencontre dans la théorie élémentaire des logarithmes, *Nyt Tidsskrift for Matematik*, Bd. XIXB, Köbenhavn 1908.
5. DEDEKIND–DIRICHLET, *Zahlentheorie*, 4 éd., Braunschweig 1894.
6. NAGELL, T., *Introduction to number theory*, New York 1951.
7. SOMMER, J., *Vorlesungen über Zahlentheorie*, Leipzig 1907.
8. HASSE, H., Vorlesungen über Zahlentheorie, *Grundlehren d. mathem. Wissenschaften*, Bd. 59, Berlin 1950.
9. HASSE, H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetze, *Jahresber. d. Deutschen Mathem. Vereinigung*, Bd. 36, Berlin 1930.
10. LEHMER, E., Criteria for cubic and quartic residuacity, *Mathematika*, Vol. 5, London 1958.
11. OBLÁTH, R., Über die Zahl x^2-1, *Mathematica*, Zutphen, Bd. 8, 1939–1940.
12. SIEGEL, C. L., Die Gleichung $ax^n-by^n=c$, *Mathem. Annalen*, Bd. 114, 1937.
13. DOMAR, Y., On the Diophantine equation $|Ax^n-By^n|=1$, $n\geqslant 5$, *Mathematica Scandinavica*, t. 2, 1954.
14. AF EKENSTAM, A., *Contributions to the theory of the Diophantine equation* $Ax^n-By^n=C$, Dissertation, Uppsala 1959.
15. NAGELL, T., Des équations indéterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$, *Norsk Matematisk Forenings Skrifter*, Ser. 1, Nr. 2, Kristiania 1921.
16. LJUNGGREN, W., Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante, *Acta mathematica*, t. 75, Stockholm 1942.
17. EULER, L., Opera omnia, *Commentationes Arithmetica* I, Basel 1912.
18. LEGENDRE, A. M., *Théorie des nombres*, Paris 1798.

Addition pendant les épreuves

L. J. Mordell vient de me communiquer que le mathematicien chinois Chao Ko a établi l'impossibilité de l'équation (1) pour $p\equiv 1 \pmod 8$; le résultat a été publié dans Scientia Sinica 14 (1965), 457–460.

Tryckt den 20 maj 1969

Uppsala 1969. Almqvist & Wiksells Boktryckeri AB