ARKIV FÖR MATEMATIK Band 1 nr 16

Communiqué le 23 Novembre 1949

# Sur les restes et les non-restes quadratiques suivant un module premier

Par TRYGVE NAGELL

## § 1. Démonstration de quelques lemmes

Si $a$ est un nombre entier $\equiv 1 \pmod 8$ et si $h$ est un nombre entier $\geqq 3$, il est bien connu que la congruence

$$u^2 \equiv a \pmod{2^h} \tag{1}$$

admet exactement quatre racines incongrues modulo $2^h$. Si $u_0$ est une racine de cette congruence, les trois nombres

$$2^{h-1} - u_0, \quad 2^{h-1} + u_0, \quad 2^h - u_0$$

satisfont aussi à la congruence. De plus, on voit sans peine que les quatre nombres

$$u_0, \quad 2^{h-1} - u_0, \quad 2^{h-1} + u_0, \quad 2^h - u_0 \tag{2}$$

sont incongrus entre eux deux à deux modulo $2^h$. Il en résulte

**Lemme 1.** *Si $u_0$ est la plus petite racine positive de la congruence (1), les quatre nombres (2) représentent les solutions incongrues modulo $2^h$, et ils satisfont aux inégalités*

$$0 < u_0 < 2^{h-1} - u_0 < 2^{h-1} + u_0 < 2^h - u_0. \tag{3}$$

*

On doit à THUE le théorème suivant [1]:[1]

**Lemme 2.** *Soit $p$ un nombre premier. Si $a$ est un nombre entier non divisible par $p$, on peut trouver deux nombres entiers positifs $x$ et $y < \sqrt{p}$ et tels qu'on ait*

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

$$ay \equiv \pm x \pmod{p} \tag{4}$$

*pour l'un ou l'autre des deux signes.*

**Démonstration:** Considérons la totalité des nombres de la forme $ay + x$, où $x$ et $y$ sont des nombres dans la suite 0, 1, 2, . . ., $[\sqrt{p}]$. (Comme d'ordinaire $[c]$ signifie le plus grand nombre entier $\leqq c$.) Le nombre de ces nombres étant égal à $([\sqrt{p}] + 1)^2 > p$, il y en a au moins deux qui sont congrus modulo $p$. Si nous supposons

$$ay_1 + x_1 \equiv ay_2 + x_2 \pmod{p},$$

nous aurons

$$a(y_1 - y_2) \equiv x_2 - x_1 \pmod{p}. \tag{5}$$

Ici on a évidemment

$$0 < |y_1 - y_2| \leqq [\sqrt{p}], \quad 0 < |x_1 - x_2| \leqq [\sqrt{p}].$$

En effet, si l'une des différences $x_1 - x_2$ et $y_1 - y_2$ était égale à zéro, l'autre le serait aussi. Si nous posons dans (5) $x_1 - x_2 = x$ et $y_1 - y_2 = y$, nous aurons une congruence du type (4) et le lemme se trouve démontré.

*

Dans un travail antérieur nous avons établi le résultat suivant [2]:

**Lemme 3.** *Soit $p$ un nombre premier de la forme $8t + 3$. Pour que le nombre des classes d'idéaux du corps quadratique imaginaire $\mathbf{K}(\sqrt{p})$ soit égal à 1, il faut et il suffit qu'il n'y ait aucun nombre premier*

$$q \leqq \sqrt{\frac{p + 16}{3}} - 2,$$

*qui est reste quadratique modulo $p$.*

Pour la démonstration je renvoie au travail cité.

*

Un autre lemme, qui nous sera utile, est le suivant:

**Lemme 4.** *Si $p$ est un nombre premier de la forme $12t - 1$, il existe deux nombres entiers positifs $u$ et $v$, tels qu'on ait*

$$p = 3v^2 - u^2 \tag{6}$$

*et*

$$u < \sqrt{\tfrac{1}{2}p}, \quad v < \sqrt{\tfrac{1}{2}p}.$$

**Démonstration:** Le nombre des classes d'idéaux du corps quadratique réel $K(\sqrt{3})$ étant égal à 1, on voit facilement que l'équation (6) est résoluble en nombres entiers $u$ et $v$. Dans un autre Mémoire, qui vient de paraître, j'ai démontré [3]: Soient $D$ et $N$ des nombres entiers positifs. Si l'équation

$$u^2 - Dv^2 = -N$$

est résoluble en nombres entiers $u$ et $v$, elle admet une solution qui satisfait aux inégalités suivantes:

$$(7) \qquad \begin{aligned} 0 < v &\leqq y_1 \sqrt{\frac{N}{2(x_1 - 1)}}, \\ 0 \leqq u &\leqq \sqrt{\tfrac{1}{2}(x_1 - 1)N}, \end{aligned}$$

où $x = x_1$, $y = y_1$ est la solution fondamentale de l'équation

$$x^2 - Dy^2 = 1.$$

Quand $D = 3$, on a $x_1 = 2$, $y_1 = 1$. En prenant $N = p$ les inégalités (7) deviennent $0 < v < \sqrt{\frac{1}{2}p}$ et $0 < u < \sqrt{\frac{1}{2}p}$; on ne peut pas avoir $u = 0$, puisque $p \neq 3$.

## § 2. Le plus petit reste quadratique premier impair

Soit $p$ un nombre premier impair. Désignons par $\pi_p$ le plus petit nombre premier impair, qui est un reste quadratique modulo $p$. Nous nous proposons de déterminer une borne supérieure de $\pi_p$ en fonction de $p$.

Dans un travail antérieur [4] nous avons déjà traité ce problème et établi le résultat suivant:

**Théorème 1.** *Si $p$ est un nombre premier $> 17$ de la forme $4t + 1$, on a*

$$\pi_p < \sqrt{p}.$$

**Démonstration:** Soient $c$ un nombre entier quelconque $\neq 0$ et $q$ un diviseur premier impair $\neq p$ de $p - c^2$. Alors on a d'après la loi de réciprocité quadratique

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{c^2}{q}\right) = +1.$$

Or, le nombre premier $p$, étant $\equiv 1 \pmod 4$, est la somme de deux carrés

$$p^2 = a^2 + 4b^2,$$

où $a$ et $b$ sont des nombres entiers positifs. Pour tout diviseur premier $q$ de $a$ on a donc

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

et par suite

$$\pi_p \leqq q \leqq \sqrt{p - 4b^2} \leqq \sqrt{p - 4}.$$

Si $a = 1$, il est évident que tout diviseur premier impair $q$ du nombre

$$b = \tfrac{1}{2}\sqrt{p - 1}$$

est un reste quadratique modulo $p$. Car on a $p \equiv 1 \pmod{q}$. Si enfin $p = 1 + 2^m$, l'exposant $m$ est nécessairement une puissance de 2, donc $m = 2^n$, où $n \geqq 3$. Soit $q$ un diviseur premier d'un des nombres

$$\sqrt[2^{n-i}]{p - 1} + 1 = 2^{2^i} + 1, \qquad (i = 2, 3, \ldots, n - 1).$$

Or, il est bien connu que tout diviseur premier impair du nombre $z^4 + 1$ est $\equiv 1 \pmod{8}$. On a donc $q \equiv 1 \pmod{8}$. Puisque $p \equiv 2 \pmod{q}$, on aura

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{2}{q}\right) = +1.$$

Le nombre premier $q$ est donc un reste quadratique modulo $p$, et le théorème 1 est démontré.

*

Prenons ensuite le cas de $p \equiv -1 \pmod{8}$ et regardons la congruence

$$u^2 \equiv -p \pmod{2^h},$$

où $h$ est un nombre entier $\geqq 3$. D'après le lemme 1 les quatre racines de cette congruence peuvent être représentées par les nombres

$$u_0, \quad 2^{h-1} - u_0, \quad 2^{h-1} + u_0, \quad 2^h - u_0,$$

qui satisfont aux inégalités

$$0 < u_0 < 2^{h-1} - u_0 < 2^{h-1} + u_0 < 2^h - u_0.$$

Si nous choisissons

$$h = 1 + \left[\frac{\log p}{\log 4}\right],$$

nous aurons évidemment

$$\sqrt{p} < 2^h < 2\sqrt{p}. \tag{8}$$

Comme $h$ doit être $\geqq 3$, il faut donc que $p > 7$.

Les nombres

$$a = \frac{p + u_0^2}{2^h}$$

et

$$b = \frac{p + (2^{h-1} - u_0)^2}{2^h}$$

sont entiers, et on a

$$b - a = 2^{h-2} - u_0 > 0.$$

Le nombre $u_0$ étant impair il en résulte que l'un des nombres $a$ et $b$ est pair et l'autre impair. Comme on a d'après (8)

$$a = \frac{p + u_0^2}{2^h} \geqq \frac{p+1}{2\sqrt{p}} > \tfrac{1}{2}\sqrt{p},$$

aucun des nombres $a$ et $b$ ne peut être égal à 1. Donc le produit $ab$ admet toujours un diviseur premier impair $q$. On a alors

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)$$

et d'après la loi de réciprocité quadratique

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{1}{2}(q-1)},$$

d'où

$$\left(\frac{q}{p}\right) = +1.$$

On a de plus

$$q \leqq b = \frac{p + (2^{h-1} - u_0)^2}{2^h} < \frac{p + (\sqrt{p} - 1)^2}{\sqrt{p}},$$

d'où

$$q < 2\sqrt{p} - 2 + \frac{1}{\sqrt{p}} < 2\sqrt{p} - 1.$$

Nous avons ainsi démontré la proposition suivante:

**Théorème 2.** *Si $p$ est un nombre premier $> 7$ de la forme $8t - 1$, on a*

$$\pi_p \leqq 2\sqrt{p} - 1.$$

*

Nous finissons par établir le résultat suivant:

**Théorème 3.** *Si $p$ est un nombre premier de la forme $8t + 3$, on a*

$$\pi_p \leqq \sqrt{\frac{p+16}{3}} - 2, \tag{9}$$

*exception faite pour les valeurs $p = 3, 11, 19, 43, 67, 163$ et peut-être pour une septième valeur de $p$.*

**Démonstration:** Il résulte du lemme 3 que l'inégalité (9) est vraie, si le nombre des classes d'idéaux dans le corps quadratique imaginaire $\boldsymbol{K}(\sqrt{-p})$ est $> 1$. Or, les seuls corps quadratiques imaginaires connus dont le nombre des classes d'idéaux est égal à 1 sont les suivants:

$$\boldsymbol{K}(\sqrt{-1}),\ \boldsymbol{K}(\sqrt{-2}),\ \boldsymbol{K}(\sqrt{-3}),\ \boldsymbol{K}(\sqrt{-7}),\ \boldsymbol{K}(\sqrt{-11}),$$
$$\boldsymbol{K}(\sqrt{-19}),\ \boldsymbol{K}(\sqrt{-43}),\ \boldsymbol{K}(\sqrt{-67}),\ \boldsymbol{K}(\sqrt{-163}).$$

D'après un résultat de HEILBRONN [5] ou ces neuf corps sont les seuls ou il existe encore un dixième corps quadratique imaginaire ayant ladite propriété. Si ce dixième corps existe, son discriminant est égal à $-q$, où $q$ est un nombre premier $> 10^7$ de la forme $8t + 3$.

## § 3. Le plus petit non-reste quadratique premier impair.

Soit $p$ un nombre premier impair. Désignons par $\psi_p$ le plus petit nombre premier impair, qui est un non-reste quadratique modulo $p$. Nous allons traiter la question analogue à la précédente de déterminer une borne supérieure de $\psi_p$ en fonction de $p$.

Nous commençons par démontrer la proposition suivante:

**Théorème 4.** *Si $p$ est un nombre premier de la forme $8n+1$, on a $\psi_p < \sqrt{p}$.*

**Démonstration:** Soit $a$ un non-reste quadratique modulo $p$. D'après le lemme 2 il existe deux nombres entiers $x$ et $y$, tels que

$$qy \equiv \pm x \pmod{p}$$

et $0 < x < \sqrt{p}$, $0 < y < \sqrt{p}$, $(x, y) = 1$. L'un des nombres $x$ et $y$ est donc un non-reste quadratique modulo $p$ et doit contenir au moins un diviseur premier impair $q$, qui est non-reste quadratique modulo $p$. Puisque $q < \sqrt{p}$, le théorème 4 est démontré.

*

**Théorème 5.** *Si $p$ est un nombre premier de la forme $8n + 5$, on a $\psi_p < \sqrt{2p}$.*

**Démonstration:** Le nombre premier $p$ peut s'écrire comme la somme de deux carrés

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

$a$ et $b$ étant des entiers positifs. On a alors

$$a^2 - b^2 \equiv -2b^2 \pmod{p},$$

d'où

$$\left(\frac{a^2 - b^2}{p}\right) = \left(\frac{-2}{p}\right) = -1.$$

Le nombre $a^2 - b^2$ admet donc au moins un diviseur premier impair $q$, qui est non-reste quadratique modulo $p$. Comme

$$q \leqq a + b = a + \sqrt{p - a^2} < \sqrt{\tfrac{1}{2}p} + \sqrt{\tfrac{1}{2}p} = \sqrt{2p},$$

le théorème 5 se trouve donc démontré.

*

Considérons ensuite le cas d'un nombre premier $p$ qui est $\equiv -1 \pmod 8$. Si nous posons $a = [\sqrt{p}]$ et $b = p - a^2$, nous avons

$$0 < b < p - (\sqrt{p} - 1)^2 = 2\sqrt{p} - 1$$

et

$$\left(\frac{b}{p}\right) = -1.$$

Le nombre $b$ a donc au moins un diviseur premier (impair), qui est un non-reste quadratique modulo $p$. Nous en concluons que

$$\psi_p < 2\sqrt{p} - 1. \tag{10}$$

On peut d'ailleurs préciser un peu ce résultat par le raisonnement suivant. Si $a$ est pair, le nombre $b$ est $\equiv -1 \pmod 4$ et admet donc au moins un diviseur premier $q \equiv -1 \pmod 4$. Si $a$ est impair, le nombre $\frac{1}{2}(p - a^2)$ est $\equiv -1 \pmod 4$ et admet donc au moins un diviseur premier $q \equiv -1 \pmod 4$. Dans tout les deux cas on aura en appliquant la loi de réciprocité quadratique

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{a}{q}\right)^2 = -1.$$

Comme $q \leqq b < 2\sqrt{p} - 1$, nous arrivons au résultat que voici:

**Théorème 6.** *Si $p$ est un nombre premier de la forme $8t - 1$, il existe un nombre premier $q \equiv -1 \pmod 4$ et $< 2\sqrt{p} - 1$, tel que $\left(\frac{q}{p}\right) = -1$.*

Le théorème suivant donne pour $\psi_p$ une borne supérieure meilleure que celle donnée par (10).

**Théorème 7.** *Si $p$ est un nombre premier $> 7$ de la forme $8t - 1$, on a*

$$\psi_p < \sqrt{2p} - 1.$$

**Démonstration:** Il suffit de démontrer le théorème pour $p \equiv -1 \pmod{24}$. En effet, si $p \equiv 7 \pmod{24}$, le nombre 3 est un non-reste quadratique modulo $p$. Alors, d'après le lemme 4 l'équation

$$p = 3v^2 - u^2$$

admet une solution en nombres entiers positifs $u$ et $v$, tels que

$$u < \sqrt{\tfrac{1}{2}p}, \quad v < \sqrt{\tfrac{1}{2}p}.$$

Puisque

$$3(v^2 - u^2) = p - 2u^2 > 0,$$

on voit que $v > u$. De plus, on aura

$$\left(\frac{p - 2u^2}{p}\right) = \left(\frac{-2}{p}\right) = -1,$$

donc

$$-1 = \left(\frac{3(v^2 - u^2)}{p}\right) = \left(\frac{v^2 - u^2}{p}\right).$$

Le nombre $v^2 - u^2$ a par suite un diviseur premier $q$, qui est non-reste quadratique modulo $p$. Puisque ce nombre premier $q$ satisfait aux inégalités

$$q \leqq v + u \leqq [\sqrt{\tfrac{1}{2}p}] + [\sqrt{\tfrac{1}{2}p}] - 1 < \sqrt{2p} - 1,$$

le théorème 7 se trouve démontré.

Nous finissons par démontrer le

**Théorème 8.** *Si $p$ est un nombre premier $> 3$ de la forme $8t + 3$, il existe un nombre premier $q \equiv -1$ (mod. 4) et $< 2\sqrt{p} + 1$, tel que $\left(\frac{q}{p}\right) = -1$.*

**Démonstration:** Posons $a = [\sqrt{p}]$. Si $a$ est pair, le nombre positif

$$\tfrac{1}{2}((a+1)^2 - p)$$

est $\equiv -1$ (mod. 4) et admet donc au moins un diviseur premier $q \equiv -1$ (mod. 4). On aura alors

$$q \leqq \tfrac{1}{2}((a+1)^2 - p) < \tfrac{1}{2}((\sqrt{p}+1)^2 - p) = \sqrt{p} + \tfrac{1}{2}$$

et en appliquant la loi de réciprocité quadratique

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{a+1}{q}\right)^2 = -1.$$

Si $a$ est impair, le nombre positif

$$\tfrac{1}{2}((a+2)^2 - p)$$

est $\equiv -1$ (mod. 4) et admet donc au moins un diviseur premier $q \equiv -1$ (mod. 4). On aura alors

$$q \leqq \tfrac{1}{2}(a+2)^2 - p) \leqq \tfrac{1}{2}((\sqrt{p-2}+2)^2 - p) = 2\sqrt{p-2} + 1$$

et d'après la loi de réciprocité quadratique

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{a+2}{q}\right)^2 = -1.$$

Ainsi le théorème 8 est démontré. Plus spécialement on aura $\psi_p < 2\sqrt{p} + 1$.

INDEX BIBLIOGRAPHIQUE. [1] **Axel Thue,** Et par antydninger til en talteoretisk methode, Vidensk. selsk. Forhandl., Christiania 1902, No 7. — [2] **T. Nagell,** Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abhdl. Mathem. Seminar der Hamburgischen Universität, Bd I, 1922, Satz VII. — [3] ——, Über die Darstellung ganzer Zahlen durch eine indefinite binäre quadratische Form, Archiv d. Mathematik, Bd II, 1950, Satz 2. — [4] ——, Zahlentheoretische Notizen, Vidensk. selsk. Skrifter, Matem.-naturv. Kl., Oslo 1923, No 13, II. — [5] **Hans Heilbronn,** On the class-number in imaginary quadratic fields, Quart. Journal of Mathematics, Oxford Ser. 5, 1934, p. 150—160.

Tryckt den 9 februari 1950

Uppsala 1950. Almqvist & Wiksells Boktryckeri AB