ANNALES

DE LA

FACULTÉ DES SCIENCES DE TOULOUSE.

SUR LE

CARACTÈRE QUADRATIQUE DU NOMBRE 2,

PAR T.-J. STIELTJES (¹),

1. Soit p un nombre premier impair. Les nombres plus petits que p, à l'exception de $p-1$,

$$1,\ 2,\ 3,\ \ldots,\ p-2,$$

peuvent être partagés en deux groupes, suivant qu'ils sont des résidus ou des non-résidus quadratiques de p. Le premier groupe

$$(A) \qquad a,\ a',\ a'',\ \ldots$$

contient alors tous les résidus, le second groupe

$$(B) \qquad b,\ b',\ b'',\ \ldots$$

tous les non-résidus qui se trouvent parmi les nombres $1, 2, \ldots, p-2$. Si $p-1$ ou -1 est résidu quadratique, le groupe (A) contient tous les résidus de p, excepté $p-1$, et le groupe (B) est formé de l'ensemble de tous les non-résidus de p. Si, au contraire, -1 est non-résidu quadratique, alors le groupe (A) contient tous les résidus, le groupe (B) tous les non-

(¹) Traduction du travail suivant : *Over het quadratische rest-karakter van het getal* 2 (*Nieuw Archief voor Wiskunde*, t. IX, p. 193-195; 1882).

résidus, excepté $p-1$. Dans le premier cas, le groupe (A) contient alors $\frac{p-3}{2}$ nombres et le groupe (B) en contient $\frac{p-1}{2}$; dans le second cas, (A) en contient $\frac{p-1}{2}$ et (B) $\frac{p-3}{2}$.

Mais il est maintenant facile de voir que le groupe (B) est toujours formé d'un nombre pair de nombres. On peut, en effet, réunir les nombres de (B) en couples, en assemblant deux nombres b et b' de (B) lorsque

$$bb' \equiv 1 \pmod{p}.$$

Les nombres d'un couple sont toujours inégaux; car de $b = b'$ suivrait $b^2 \equiv 1$ d'où $b = 1$ ou $b = p-1$; mais le nombre 1 ne se présente jamais dans le groupe (B) pendant que $p-1$ ne se présente ni dans (A), ni dans (B).

Donc, si $\frac{p-1}{2}$ est pair, c'est-à-dire si p est de la forme $4n+1$, alors $\frac{p-1}{2}$ est le nombre des non-résidus (mod p); (B) contient tous les non-résidus de p et -1 est résidu de p. Si, au contraire, $\frac{p-1}{2}$ est impair, c'est-à-dire si p est de la forme $4n+3$, alors nécessairement -1 est non-résidu de p.

On a maintenant établi à la fois les conclusions suivantes :

Pour $p = 4n+1$, (A) contient tous les résidus, excepté le résidu $p-1$; le nombre des nombres de (A) est $2n-1$; (B) contient tous les non-résidus, leur nombre est $2n$.

Et pour $p = 4n+3$, (A) contient tous les résidus, leur nombre est $2n+1$; (B) contient tous les non-résidus, excepté le non-résidu $p-1$; le nombre des nombres (B) est $2n$.

2. En ajoutant l'unité à tous les nombres $a, a', a'', \ldots, b, b', b'', \ldots$, on obtient les groupes de nombres

(A') $\quad a+1, \quad a'+1, \quad a''+1, \quad \ldots,$

B') $\quad b+1, \quad b'+1, \quad b''+1, \quad \ldots,$

qui forment ensemble tous les nombres

$$2, \quad 3, \quad 4, \quad \ldots, \quad p-1,$$

de sorte que dans (A′) et (B′), simultanément, on trouve les $\frac{p-1}{2}$ non-résidus et les $\frac{p-3}{2}$ résidus de p, c'est-à-dire tous les résidus excepté 1.

Le nombre des nombres (B′) est pair, et, parmi les nombres de (B′), on trouve autant de résidus que de non-résidus de p. Car, si b et b' sont deux nombres de (B) qui forment un couple

$$bb' \equiv 1,$$

alors, on a

$$b+1 \equiv b(b'+1),$$

et, si b est non-résidu, un des nombres $b+1$, $b'+1$ est ainsi résidu, l'autre non-résidu.

En liaison avec ce précède, on a cette conséquence que pour $p = 4n+1$

$$\text{(B′) est formé de } \frac{p-1}{4} = n \text{ résidus et de } \frac{p-1}{4} = n \text{ non-résidus,}$$

et, par conséquent,

$$\text{(A′) de } \frac{p-5}{4} = n-1 \text{ résidus et de } \frac{p-1}{4} = n \text{ non-résidus.}$$

Mais, si $p = 4n+3$, alors

$$\text{(B′) contient } \frac{p-3}{4} = n \text{ résidus et } n \text{ non-résidus,}$$

et, par conséquent,

$$\text{(A′) contient } \frac{p-3}{4} = n \text{ résidus et } \frac{p+1}{4} = n+1 \text{ non-résidus.}$$

3. Le caractère quadratique de 2 peut maintenant être déterminé comme il suit. Les cas de $p = 4n+1$, $p = 4n+3$ doivent être traités séparément.

I. $p = 4n+1$.

Dans ce cas, (B) contient tous les non-résidus de p, donc

$$(x-b)(x-b')(x-b'')\ldots \equiv x^{\frac{p-1}{2}}+1 \pmod{p}.$$

En posant ici $x = -1$, il vient

$$(b+1)(b'+1)(b''+1)\ldots \equiv 2 \pmod{p}.$$

Mais, d'après le n° 2, parmi les $2n$ nombres $b+1$, $b'+1$, ..., on trouve n non-résidus, tandis que les autres sont des résidus.

Si donc n est pair, c'est-à-dire si $p = 8k+1$, alors 2 est résidu de p.

Si n est impair, c'est-à-dire si $p = 8k+5$, alors 2 est non-résidu de p.

II. $p = 4n+3$.

Dans ce cas, (A) contient tous les résidus de p; donc

$$(x-a)(x-a')(x-a'')\ldots \equiv x^{\frac{p-1}{2}} - 1 \pmod{p}.$$

Si l'on pose ici $x = -1$, il vient

$$(a+1)(a'+1)(a''+1)\ldots \equiv 2 \pmod{p}.$$

Mais, d'après le n° 2, parmi les $2n+1$ nombres $a+1$, $a'+1$, ... on trouve $n+1$ non-résidus, tandis que les autres sont des résidus.

Si donc n est pair, c'est-à-dire si $p = 8k+3$, alors 2 est non-résidu de p.

Si n est impair, c'est-à-dire si $p = 8k+7$, alors 2 est résidu de p.