BULLETIN DE LA S. M. F.

FROLOV.

Sur les racines primitives

Bulletin de la S. M. F., tome 22 (1894), p. 241-245

<http://www.numdam.org/item?id=BSMF_1894__22__241_0>

SUR LES RACINES PRIMITIVES (¹)

(Suite et fin);

Par M. Frolov.

10. Nommons s le nombre de termes de la chaîne qui commence par le groupe [1].

Il est facile de démontrer :

1° Que la seconde chaîne ouverte, qui n'existe que pour les modules de la forme $m = 8q + 1$, où q est un nombre entier quelconque, a le même nombre de termes, c'est-à-dire s termes;

2° Que toute chaîne fermée a deux fois plus de termes, c'est-à-dire $2s$ termes;

3° Qu'il suffit d'avoir la première chaîne ouverte, pour reconnaître de suite le nombre f de chaînes fermées, qui est donné par les formules

$$f = \frac{m-1-s}{2s}, \qquad f = \frac{m-1-2s}{2s},$$

suivant qu'il n'y a qu'une seule chaîne ouverte ou qu'il y en a deux;

4° Que la première chaîne ouverte englobe tous les résidus d'un certain degré dont l'exposant j est donné par la formule

$$j = \frac{m-1}{s}.$$

Cet exposant j joue un grand rôle dans la recherche des racines primitives; s'il est composé, on déterminera tous ses diviseurs d_1, d_2, d_3, ...

Pour découvrir une ou quelques racines primitives, de n'importe quel module m, on n'a besoin de construire qu'une seule chaîne, celle qui se déploie au moyen du groupe [1] et que nous appellerons *chaîne principale*. Il est inutile de construire les autres chaînes et même de s'en occuper.

(¹) Le Mémoire, inséré sous ce titre dans le n° 7 du tome XXI du *Bulletin de la Société mathématique de France*, en 1893, étant inachevé, nous avons repris notre travail, et nous présentons maintenant cette Note supplémentaire, qui complète ledit Mémoire.

11. En déployant une chaîne au moyen du groupe [1], on ne peut pas prévoir si elle s'arrêtera avant d'avoir englobé tous les $(m-1)$ termes et ne sera pas unique, excepté un seul cas, celui où le module est de la forme $m = 8q + 1$; alors les nombres 2 et -2 sont des résidus quadratiques et la chaîne ne peut pas être unique.

Quand on a un module de cette forme, ou bien un module d'une forme quelconque, pour lequel $(m-1)$ n'a qu'un seul facteur impair, si la chaîne ne s'arrête pas d'elle-même, il faut la continuer jusqu'à ce qu'elle englobe $\frac{m-1}{2}$ termes; si elle ne s'arrête pas là, elle englobera évidemment tous les $m-1$ termes et sera unique. Mais quand on a un module n'appartenant pas à la forme $m = 8q + 1$, pour lequel $(m-1)$ a deux ou plusieurs facteurs impairs, dont le plus petit est p, on pourra arrêter la chaîne après avoir atteint $\frac{m-1}{p}$ termes. Par exemple pour

$$m = 71 = 2.5.7 + 1,$$

on a $p = 5$, et par suite on arrêtera la chaîne après avoir englobé $\frac{70}{5} = 14$ termes.

Si la chaîne s'arrête d'elle-même, elle sera la chaîne principale et tous ses s termes seront résidus du degré $j = \frac{m-1}{s}$. Outre cela, certains de ses termes seront résidus d'autres degrés, marqués par des exposants premiers avec j, tandis que les autres termes ne le seront pas. On le déterminera facilement, car les termes 1 et -1 sont résidus de tous les degrés impairs; pour $m = 4h + 1$ ils sont aussi résidus quadratiques; pour $m = 4h - 1$ le terme 1 est résidu et le terme -1 est non-résidu quadratique. Si l'on assigne à tous les groupes, en commençant par celui qui contient les termes 2 et -2, des numéros d'ordre 1, 2, 3, 4, ..., les groupes qui portent les n^{os} p, $2p$, $3p$, ... seront composés de résidus d'un degré impair p. Quant aux résidus quadratiques, pour $m = 4h + 1$ ils composeront les groupes aux numéros pairs 2, 4, 6, ...; et pour $m = 4h - 1$, si la chaîne est terminée par le groupe $[\nu]$, ce sont les deux premiers termes de tous les groupes qui seront résidus quadratiques, et si la chaîne est

terminée par le groupe $[u]$, dans les groupes aux numéros impairs 1, 3, 5, ... ce sont les deux derniers termes, et dans les groupes aux numéros pairs 2, 4, 6, ... ce sont les deux premiers termes qui seront résidus quadratiques.

La composition de la chaîne principale étant de cette manière complètement déterminée, on passera à la recherche des racines primitives.

Pour cela on déterminera d'abord tous les diviseurs d_1, d_2, d_3, ... de l'exposant j, et puis on prendra, parmi les petits nombres 3, 5, 6, 7, ... qui ne figurent pas dans la chaîne, un nombre quelconque t et l'on calculera ses résidus de tous les degrés marqués par ces diviseurs : t^{d_1}, t^{d_2}, ..., que nous appellerons *résidus partiels* de t. Si l'un d'eux t^d se trouve dans la chaîne, cela indiquera que t n'est pas une racine primitive, car on aura la congruence $t^d \equiv x^j$ ou $t \equiv x^{\frac{j}{d}}$, qui exprime que t est résidu du degré $\frac{j}{d}$ d'un certain nombre x. Si aucun des résidus partiels n'entre dans la chaîne, on observera si le résidu t^j, qui sera nommé *résidu principal* et qui se trouve nécessairement dans la chaîne, n'est résidu d'aucun degré dont l'exposant p est premier avec j. S'il l'est, cela indiquera évidemment que t est lui-même résidu du degré p et que, par conséquent, il n'est pas une racine primitive. Au contraire, si t n'est résidu d'aucun degré autre que celui qui est marqué par l'exposant j, il est une racine primitive.

12. Éclaircissons l'application de cette méthode par quelques exemples :

1° Soit proposé le module $m = 89 = 2^3 . 11 + 1$.

On construit la chaîne principale

	N° 1.	N° 2.
1, 1, 88, 88;	2, 45, 44, 87;	4, 67, 22, 85;
N° 3.	**N° 4.**	**N° 5.**
8, 78, 11, 81;	16, 39, 50, 73;	32, 64, 25, 57;

qui contient 22 termes. Donc $s = 22$, et $j = \frac{88}{22} = 4$. Ce dernier n'a qu'un seul diviseur $d = 2$.

La chaîne ne contient pas les termes 3, 5, 6, 7, 10, ...

Le résidu partiel de 3 est $3^2 = 9$; il ne se trouve pas dans la chaîne. Le résidu principal $3^4 = 81$ y figure dans le groupe n° 3 et il n'est pas résidu de 11e degré, car 3 n'est pas divisible par 11. Donc 3 est une racine primitive de 89.

Le résidu partiel de 5 est $5^2 = 25$; on le trouve dans la chaîne; donc 5 n'est pas une racine primitive.

Le résidu partiel de 6 est $6^2 = 36$; il ne se trouve pas dans la chaîne. Le résidu principal $6^4 \equiv 50$ y figure dans le n° 4, et comme 4 n'est pas divisible par 11, 6 est une racine primitive.

2° Soit proposé le module $m = 601 = 2^3 . 3 . 5^2 + 1$.

La chaîne principale est

	N° 1.	N° 2.
1, 1, 600, 600;	2, 301, 300, 599;	4, 451, 150, 597;
N° 3.	**N° 4.**	**N° 5.**
8, 526, 75, 593;	16, 263, 338, 585;	32, 432, 169, 569;
N° 6.	**N° 7.**	**N° 8.**
64, 216, 385, 537;	128, 108, 493, 473;	256, 54, 547, 345;
N° 9.	**N° 10.**	**N° 11.**
512, 27, 574, 89;	423, 314, 287, 178;	245, 157, 444, 356;
N° 12.		
490, 379, 222, 111.		

Elle contient 50 termes. Donc $s = 50$, et $j = \frac{600}{50} = 12$. Il a quatre diviseurs 2, 3, 4 et 6.

On ne voit pas dans la chaîne les termes 3, 5, 6, 7, ...

Les quatre résidus partiels de 3 sont $3^2 = 9$; $3^3 = 27$; $3^4 = 81$; $3^6 \equiv 128$; les résidus 27 et 128 figurent dans la chaîne, donc 3 n'est pas une racine primitive.

Les quatre résidus partiels de 5 sont $5^2 = 25$; $5^3 = 125$; $5^4 \equiv 24$; $5^6 \equiv 600$. On trouve dans la chaîne le résidu 600, donc 5 n'est pas une racine primitive.

Les quatre résidus partiels de 7 sont $7^2 = 49$; $7^3 = 343$; $7^4 \equiv 598$; $7^6 = 454$; aucun d'eux ne figure dans la chaîne. Le résidu principal $7^{12} \equiv 574$ se trouve dans le groupe n° 9 de la chaîne; 9 n'est pas divisible par 5, donc 7 est une racine primitive.

3° Prenons le module $m = 683 = 2 . 11 . 31 + 1$.

On a la chaîne principale

	N° 1.	N° 2.
1, 1, 682, 682;	2, 342, 341, 681;	4, 171, 512, 679;

N° 3.	N° 4.	N° 5.
8, 427, 256, 675;	16, 555, 128, 667;	32, 619, 64, 651;

qui contient 22 termes. Donc $s = 22$ et $j = \frac{682}{22} = 31$, nombre premier.

La chaîne ne renferme pas 3, 5, 6, 7, ...

Le résidu principal de 3 est $3^{31} \equiv 1$, donc il est résidu des degrés 2 et 11, et 3 n'est pas une racine primitive.

Le résidu principal de 5 est $5^{31} \equiv 427$; il se trouve dans le groupe n° 3 et n'est pas résidu des degrés 2 et 11, donc 5 est une racine primitive de 683.

Ces exemples éclaircissent sufisamment l'application de la nouvelle méthode et nous espérons que l'on reconnaîtra qu'elle est plus simple et moins laborieuse que les autres méthodes connues.

ERRATA

du Mémoire *Sur les racines primitives,* inséré dans le tome XXI du *Bulletin de la Société mathématique de France,* année 1893.

1° Page 113, ligne 3 en remontant, *au lieu de :* $r \equiv -\frac{m+x^2}{4}$, *lisez :* $r \equiv \frac{m+x^2}{4}$.

2° Page 123, lignes 6-8, *au lieu de :* car le groupe central de ces chaînes est composé de résidus de tous les degrés impairs, et les groupes composés ..., *lisez :* car le groupe central de ces chaînes, qui existe si h n'est pas divisible par 4, est composés de résidus de tous les degrés impairs; s'il n'existe pas, les deux groupes du milieu sont composés de racines primitives; les deux groupes extrêmes le sont dans les deux cas, et parce que les groupes composés ....

3° Page 124, ligne 3 en remontant, *au lieu de :* Pour les modules de la forme $m = 6N + 1$, où N est ..., *lisez :* Pour les modules des formes $m = 6N + 1$ et $m = 12N + 1$, où N est ....

FIN DU TOME XXII.