BULLETIN DE LA S. M. F.

FROLOV

Sur les racines primitives

Bulletin de la S. M. F., tome 21 (1893), p. 113-128

<http://www.numdam.org/item?id=BSMF_1893__21__113_0>

Sur les racines primitives; par M. Frolov.

1. Euler fut amené à la conclusion, qu'il est impossible de saisir entre un nombre premier et ses racines primitives aucune relation, d'où l'on puisse déduire au moins une seule de ces racines, de sorte qu'on ne peut, d'après lui, les découvrir que par tâtonnements, c'est-à-dire en essayant différents nombres. Quoique Gauss ait donné une méthode très ingénieuse pour découvrir sans tâtonnements une racine primitive d'un module premier, cette méthode est tellement compliquée qu'on ne l'emploie guère. La complication de cette méthode apparaît déjà dans l'exemple donné par Gauss lui-même. En effet, pour découvrir que le nombre 5 est une racine primitive du nombre 73, il a dû former les périodes des trois nombres 2, 3 et 54, qui sont tous résidus quadratiques de 73, tandis qu'on serait arrivé au même résultat beaucoup plus vite, en commençant par essayer 5, comme le plus petit parmi les non-résidus quadratiques de 73, ce qui aurait épargné beaucoup de peine.

C'est probablement à cause de la complication de cette méthode que Poinsot, dans ses *Réflexions sur la théorie des nombres,* publiées en 1845, proposa de déterminer les racines primitives d'un module premier m par l'exclusion des résidus des puissances, dont les exposants sont marqués par les facteurs premiers du nombre $(m-1)$. Mais, comme l'a déjà remarqué le très regretté J.-A. Serret, cette méthode devient presque impraticable, dès que le module est un peu considérable.

Ainsi, pour déterminer les racines primitives d'un module premier, on est encore obligé, comme du temps d'Euler, de recourir aux essais de différents nombres. Évidemment, on doit prendre ces derniers parmi les non-résidus quadratiques du module, car il est facile de discerner les nombres qui sont résidus quadratiques de ceux qui ne le sont pas. Les résidus quadratiques sont d'abord les carrés inférieurs à m, savoir 1, 4, 9, 16, ...; puis, pour les modules de la forme $m = 4h-1$, ce sont les nombres h, $h+2$, $h+6$, $h+12$, ... tous compris dans la formule $r \equiv -\frac{m+x^2}{4}$, où x est un nombre indéterminé impair, et pour les modules $m = 4h+1$, ce sont les nombres $-h$, $-h+2$, $-h+6$,

$-h+12, \ldots$; tous compris dans la formule $r \equiv \frac{m-x^2}{4}$, où x est aussi un nombre indéterminé impair. On reconnaît encore facilement si les nombres $\pm 2, \pm 3, \pm 5, \ldots$ sont résidus ou non-résidus quadratiques, d'après les formules déduites par Fermat, Euler et autres grands géomètres. Quant aux non-résidus quadratiques, on ne les détermine directement que pour les modules de la forme $4h-1$, car dans ce cas ce sont les compléments des carrés et des résidus quadratiques. Voici encore une proposition qui permettra de découvrir pour la plupart des modules premiers m quelques résidus et non-résidus quadratiques :

Soient $4p$ celui des deux nombres $(m-1)$ et $(m+1)$ qui est divisible par 4, et $2q$ l'autre qui ne l'est pas; tous les facteurs premiers de p et les facteurs premiers de q de la forme $4k+1$ sont résidus quadratiques de m, tandis que les facteurs premiers de q de la forme $4k-1$, ainsi que 2, si p est impair, sont non-résidus quadratiques.

On obtiendra d'autres résidus, en multipliant deux résidus ou deux non-résidus, et d'autres non-résidus, en multipliant un non-résidu par un résidu.

Par exemple, pour $m=191$, on a $m-1=190=2.5.19$, et $m+1=192=2^6.3$; donc $p=2^4.3$ et $q=5.19$; par conséquent on aura les résidus 2, 3, 5, 6, 10, 15, ... et les non-résidus 19, 38, 57, 95, ... Pour $m=197$, on a $m-1=196=2^2.7^2$ et $m+1=198=2.3^2.11$; donc $p=7^2$ et $q=3^2.11$, et l'on aura les résidus $6.7.22\ldots$ et les non-résidus $2.3.11.14\ldots$. Pour $m=263$, on a $m-1=262=2.131$ et $m+1=264=2^3.3.11$; donc $p=2.3.11$ et $q=131$, et l'on aura les résidus $2.3.6.11\ldots$ et les non-résidus

$$131;\quad 131.3\equiv 130;\quad 130.11\equiv 120;\quad 120.11\equiv 10;\quad \ldots.$$

Il arrive souvent que les non-résidus obtenus de cette manière sont racines primitives. Ainsi, 191 a les racines primitives 19, 57 et 95; 197 a 2, 3 et 11; 263 a 131, 130, 120 et 10. Mais nous allons montrer qu'on n'aura à recourir aux essais de ce genre que dans des cas bien rares.

2. Il y a des cas, où les racines d'un module premier se déter-

minent immédiatement, sans aucun essai. Avant de les signaler, rappelons que l'on dit, avec Euler, que deux nombres sont *associés* entre eux, si leur produit est congru à 1. Ainsi a et b sont associés entre eux, s'il y a la congruence $ab \equiv 1 \pmod{m}$. Leurs complémentaires à m sont aussi associés entre eux, car on a $(m-a)(m-b) \equiv -a-b = ab \equiv 1$. En changeant les signes, on aura $-ab \equiv -1$; donc le produit d'un nombre a par le complément de son associé $-b$ est congru à -1. Pour abréger, nous dirons que deux nombres, dont le produit est congru à -1, sont *contre-associés* entre eux.

Dans un groupe de quatre termes a, b, $-b$, $-a$, chacun d'eux a son associé, son contre-associé et son complémentaire à m. Nous dirons que a et $-a$ sont les *termes extrêmes,* et b et $-b$ sont les *termes moyens* de ce groupe.

On sait que deux nombres complémentaires 1 et $m-1 \equiv -1$ sont associés chacun à lui-même, car $1^2 \equiv 1$ et $(-1)^2 \equiv 1$. Ajoutons qu'ils sont contre-associés l'un de l'autre, car on a $1(-1) \equiv -1$. Donc ces deux nombres forment un groupe complet, qu'on peut écrire de la manière suivante 1, 1, -1, -1.

Pour $m = 4h+1$, il y a encore deux autres nombres complémentaires, que nous désignerons par w et $-w$, qui sont associés entre eux, en satisfaisant à la congruence $-w^2 \equiv 1 \pmod{m}$. En changeant les signes, on aura $w^2 = (\pm w)^2 \equiv -1$, ce qui signifie que chacun de ces deux nombres est contre-associé à lui-même. Ces nombres forment le groupe complet w, $-w$, w, $-w$.

Les nombres w et $-w$, ainsi que 1 et -1, sont résidus de tous les degrés impairs qui sont facteurs de $(m-1)$, pour tous les modules m au-dessus de 5.

En effet, soit g une racine primitive quelconque de $m = 4h+1$. On aura $g^{\frac{m-1}{2}} \equiv -1$, et comme on a $w^2 \equiv -1$, il viendra $w^2 \equiv g^{\frac{m-1}{2}}$, d'où l'on tire

$$\pm w \equiv \pm g^{\frac{m-1}{4}} \equiv \pm g^h.$$

Il en résulte : 1° que si h est impair, w et $-w$ sont résidus de tous les degrés impairs de h et de $(m-1)$, et 2° que si h est pair, ils sont en outre résidus quadratiques de m.

Par exemple, pour $m = 37 = 4.9 + 1$ et $h = 9$, on a $w = 6$ et $-w = 31$, qui sont résidus seulement du troisième degré, car h est impair; tandis que, pour $m = 41 = 4.10 + 1$ et $h = 10$, on a $w = 9$ et $-w = 32$, qui sont résidus du cinquième degré et résidus quadratiques, car h est pair.

3. Nous signalerons trois cas, où les non-résidus quadratiques d'un module sont ses racines primitives.

I. *Tout module premier de la forme* $m = 2^{2^c} + 1$, *où c est un nombre quelconque, a pour racines primitives tous ses non-résidus quadratiques et entre autres les nombres* 3, 5 *et* 10.

C'est évident, car le nombre $m - 1 = 2^{2^c}$ n'ayant qu'un seul facteur premier 2, tous les nombres inférieurs à m sont résidus ou non-résidus quadratiques, et tous ces derniers sont nécessairement racines primitives de m; et comme les nombres premiers de la forme $2^{2^c} + 1$ appartiennent aux formes $8h + 1$, $12h + 5$ et $10h - 3$, il s'ensuit qu'ils ont le résidu quadratique 2 et les non-résidus 3 et 5, qui sont par conséquent leurs racines primitives, ainsi que 10, qui est le produit d'un résidu par un non-résidu. Par exemple, les modules $17 = 2^4 + 1$, $257 = 2^8 + 1$, $65537 = 2^{16} + 1$, ... ont tous les racines primitives 3, 5 et 10 et n'ont pas la racine primitive 2.

II. *Tout module premier de la forme* $m = 2n + 1$, *où n est un nombre premier impair, a pour racines primitives également tous ses non-résidus quadratiques, sauf* $m - 1 \equiv -1$.

En effet, dans ce cas, il n'y a que deux résidus du degré impair n, et comme ce sont les nombres 1 et -1, tous les autres nombres sont résidus ou non-résidus quadratiques, et ces derniers sont nécessairement racines primitives de m. Par exemple, $m = 26003 = 2.13001 + 1$, étant de la forme $8h + 3$, a le non-résidu quadratique 2; par conséquent ce nombre est une racine primitive de 26003.

III. *Tout module premier* $m = 4n + 1$, *où n est un nombre premier impair, a de même pour racines primitives tous ses non-résidus quadratiques.*

En effet, dans ce cas, il y a quatre résidus du degré n, qui sont les nombres 1, -1, w et $-w$, tandis que tous les autres nombres sont résidus ou non-résidus quadratiques, et ces derniers sont nécessairement racines primitives de m. Par exemple, pour $m = 32069 = 4.8017 + 1$, qui appartient aux formes $8h - 3$ et $12h - 3$, les nombres 2 et 3 sont non-résidus quadratiques, et par conséquent ils sont racines primitives de 32069.

4. Nous allons exposer brièvement, en omettant les démonstrations peu essentielles, un procédé qui permettra de découvrir rapidement les racines primitives de la plupart des nombres, sans aucun essai.

Il consiste dans le déploiement des $(m - 1)$ nombres, inférieurs au module m, en chaînes de groupes de quatre termes, associés, contre-associés et complémentaires, que nous avons considérés dans le n° 2; ces chaînes sont très faciles à construire, car il est permis de faire l'échange des facteurs entre deux nombres associés ou contre-associés, et comme l'un des deux termes extrêmes ou moyens est toujours pair, on peut le diviser par 2, en multipliant par 2 son associé ou contre-associé, le plus petit des deux.

Il en résultera deux nouveaux termes associés ou contre-associés et l'on n'aura qu'à y adjoindre leurs complémentaires à m, pour obtenir un groupe nouveau.

Par exemple, on a, pour $m = 281$, le groupe

24, 82, 199, 257.

En multipliant par 2 le terme 24 et en divisant par 2 le terme 82, on obtiendra le groupe

48, 41, 240, 233.

Si, au contraire, on multiplie par 2 le terme 82, en divisant par 2 le terme 24, on aura le groupe

12, 164, 117, 269.

Ces trois groupes formeront une portion d'une chaîne

... 12, 164, 117, 269; 24, 82, 199, 257; 48, 41, 240, 233: ...,

qu'on pourra prolonger des deux côtés, en répétant la même opération, jusqu'à ce qu'on arrive à des groupes qui ne puissent plus en produire de nouveaux, ou bien jusqu'à ce qu'on arrive des deux côtés au même groupe.

Dans le premier cas on aura une *chaîne ouverte,* terminée par deux groupes, que nous appellerons *groupes d'arrêt.* Il y a quatre espèces de groupes d'arrêt :

$$1^\circ \quad 1, \quad 1, \quad -1, \quad -1; \qquad 2^\circ \quad w, \quad -w, \quad w, \quad -w,$$
$$3^\circ \quad u, \quad -2u, \quad 2u, \quad -u; \qquad 4^\circ \quad v, \quad 2v, \quad -2v, \quad -v,$$

que nous désignerons respectivement par les notations abrégées $[1]$, $[w]$, $[u]$, $[v]$.

Dans le dernier cas, la chaîne rentre en elle-même et nous dirons qu'elle est *circulaire* ou *fermée.*

Pour m de la forme $4h-1$, il n'y a pas de groupe w; donc il n'y aura qu'une seule chaîne ouverte, terminée par $[1]$ et $[u]$, si h est impair, ou par $[1]$ et $[v]$, si h est pair.

Pour m de la forme $4h+1$, il y a aussi une seule chaîne ouverte, terminée par $[1]$ et $[w]$, si h est impair. Au contraire, si h est pair, on a deux chaînes ouvertes, terminées par quatre groupes d'arrêt : $[1]$, $[w]$, $[u]$, $[v]$.

Remarquons ici qu'il est indifférent de multiplier ou de diviser par 2 l'un ou l'autre terme complémentaire, car le résultat reste le même. En effet, soit g une racine primitive de m et $a \equiv g^l$. Alors un groupe quelconque $a, b, -b, -a$ peut être représenté de la manière suivante :

$$g^l, \quad g^{m-1-l}, \quad g^{\frac{m-1}{2}-l}, \quad g^{\frac{m-1}{2}+l},$$

car on a

$$g^l . g^{m-1-l} \equiv g^{m-1} \equiv 1, \quad g^{\frac{m-1}{2}-l} . g^{\frac{m-1}{2}+l} \equiv g^{m-1} \equiv 1.$$

Soit $2 \equiv g^k$. En multipliant par 2 le premier terme g^l, on aura

$$g^{l+k}, \quad g^{m-1-l-k}, \quad g^{\frac{m-1}{2}-l-k}, \quad g^{\frac{m-1}{2}+l+k}$$

et, si l'on multiplie par 2 le dernier terme $g^{\frac{m-1}{2}+l}$, on aura également

$$g^{l+k}, \quad g^{m-1-l-k}, \quad g^{\frac{m-1}{2}-l-k}, \quad g^{\frac{m-1}{2}+l+k}$$

Donc le résultat est le même dans les deux cas.

5. *Si, en commençant une chaîne par le groupe* [1], *on parvient à englober dans cette chaîne ouverte tous les* $(m-1)$ *nombres inférieurs à* m, *on en conclura que* m, *s'il est de la forme* $4h+1$, *a les racines primitives* 2 *et* -2, *ou l'une de ces racines primitives, s'il est de la forme* $4h-1$.

C'est évident, car dans ce cas ce procédé n'est autre chose que la formation de la période du nombre 2 ou -2. Comme on a

$$g^{m-1} \equiv 1, \quad g^{\frac{m-1}{2}} \equiv -1 \pmod{m},$$

un groupe quelconque peut être représenté de la manière suivante :

$$g^l, \quad g^{-l}, \quad -g^{-l}, \quad -g^l.$$

Si $g = 2$ ou -2, et l est un nombre indéterminé, on aura

$$2^l, \quad 2^{-l}, \quad -2^{-l}, \quad -2^l;$$

donc tous les termes sont compris dans la formule $\pm 2^{\pm l}$, et il est clair que si une chaîne englobe tous les $(m-1)$ nombres, 2 et -2 ou l'un de ces nombres est racine primitive, selon que m est de la forme $4h+1$ ou $4h-1$.

Pour m *de la forme* $4h-1$, *si la chaîne est terminée par* $[u]$, *c'est* 2 *qui est la racine primitive, et si elle est terminée par* $[v]$, *c'est* -2.

En effet, si 2 est racine primitive, le dernier groupe sera

$$2^{\frac{m-3}{4}}, \quad 2^{m-1-\frac{m-3}{4}}, \quad 2^{\frac{m-1}{2}-\frac{m-3}{4}}, \quad 2^{\frac{m-1}{2}+\frac{m-3}{4}}$$

ou

$$2^{\frac{m-3}{4}}, \quad 2^{\frac{3m-1}{4}}, \qquad 2^{\frac{m+1}{4}}, \qquad 2^{\frac{3m-5}{4}}.$$

En le ramenant à la forme

$$2^{\frac{m-3}{4}}, \quad 2.2^{\frac{3m-5}{4}}, \quad 2.2^{\frac{m-3}{4}}, \quad 2^{\frac{3m-5}{4}},$$

on voit que le troisième terme est le double du premier, et le deuxième terme est le double du quatrième, de sorte que ce groupe appartient à la forme $[u]$. Au contraire, si la chaîne est terminée par le groupe $[v]$, cela indiquera que 2 n'est pas une ra-

cine primitive de m, et par conséquent c'est -2 qui l'est nécessairement.

Ainsi le déploiement des nombres en chaîne permet de déterminer rapidement, si le module proposé a les racines primitives 2 et -2 ou l'une de ces racines.

Éclaircissons ceci par quelques exemples :

1° Soit $m = 61 = 2^2.3.5+1$, de la forme $4h+1$. En commençant par le groupe (1), on formera la chaîne

1,	1,	60,	60;	2,	31,	30,	59;	4,	46,	15,	57;
8,	23,	38,	53;	16,	42,	19,	45;	32,	21,	40,	29;
3,	41,	20,	58;	6,	51,	10,	55;	12,	56,	5,	49;
24,	28,	33,	37;	48,	14,	47,	13;	35,	7,	54,	26;
9,	34,	27,	52;	18,	17,	44,	43;	36,	39,	22,	25;
11,	50,	11,	50,								

qui est terminée par le groupe $[w]$ et contient tous les soixante nombres inférieurs au module 61. Donc, comme ce module est de la forme $4h+1$, il a les racines primitives 2 et $-2 \equiv 59$.

2° Soit $m = 67 = 2.3.11+1$, de la forme $4h-1$. En commençant par le groupe (1), on formera la chaîne :

1,	1,	66,	66;	2,	34,	33,	65;	4,	17,	50,	63;
8,	42,	25,	59;	16,	21,	46,	51;	32,	44,	23,	35;
64,	22,	45,	3;	61,	11,	56,	6;	55,	39,	28,	12;
43,	53,	14,	24;	19,	60,	7,	48;	38,	30,	37,	29;
9,	15,	52,	58;	18,	41,	26,	49;	36,	54,	13,	31;
5,	27,	40,	62;	10,	47,	20,	57,				

qui est terminée par le groupe $[u]$; donc 67 a la racine primitive 2.

3° Soit $m = 71 = 2.5.7+1$, de la forme $4h-1$. On aura la chaîne

1,	1,	70,	70;	2,	36,	35,	69;	4,	18,	53,	67;
8,	9,	62,	63;	16,	40,	31,	55;	32,	20,	51,	39;
64,	10,	61,	7;	57,	5,	66,	14;	43,	38,	33,	28;
15,	19,	52,	56;	30,	45,	26,	41;	60,	58,	13,	11;
49,	29,	42,	22;	27,	50,	21,	44;	54,	25,	46,	17;
37,	48,	23,	34;	3,	24,	47,	68;	6,	12,	59,	65,

qui est terminée par le groupe $[\nu]$; donc 71 a la racine primitive $-2 \equiv 69$.

6. Le déploiement en chaîne des groupes de nombres associés et contre-associés permet en même temps de reconnaître les résidus de tous les degrés et toutes les racines primitives.

Pour $m = 4h + 1$, les termes 1 et -1 du groupe initial [1] étant résidus de tous les degrés, il s'ensuit que les groupes des rangs impairs 1, 3, 5, 7, ... seront composés de résidus quadratiques. Tels sont, pour $m = 61$, les groupes

1,	1,	60,	60;	4,	46,	15,	57;	16,	42,	19,	45;
3,	41,	20,	58;	12,	56,	5,	49;	48,	14,	47,	13;
9,	34,	27,	52;	36,	39,	22,	25.				

Comme pour ce module on a $m - 1 = 60 = 2^2 . 3 . 5$, il y aura encore les résidus de degrés impairs 3 et 5. Les groupes composés de résidus du troisième degré occupent les rangs 1, 4, 7, 10, ... Tels sont les groupes

1,	1,	60,	60;	8,	23,	38,	53;	3,	41,	20,	58;
24,	28,	33,	37;	9,	34,	27,	52;	11,	50,	11,	50.

Les groupes composés des résidus du cinquième degré occupent les rangs 1, 6, 11, 16. Tels sont les groupes

1,	1,	60,	60;	32,	21,	40,	29;
48,	14,	47,	13;	11,	50,	11,	50.

Tous les autres groupes

2,	37,	30,	59;	6,	51,	10,	55;
35,	7,	54,	26;	18,	17,	44,	43,

sont composés de racines primitives.

Pour $m = 4h - 1$, les termes 1 et -1 du groupe initial, étant aussi résidus de tous les degrés impairs, on déterminera ces derniers comme dans le cas précédent. Quant aux résidus quadratiques, il y a à considérer deux cas : 1° Si la racine primitive est -2, les deux premiers termes de tous les groupes sont résidus quadratiques, et les deux derniers termes, tant qu'ils ne sont pas résidus d'aucun degré impair, sont racines primitives. Ainsi, pour

$m = 71$, les termes 2,36; 4,18; 8,9; 16,40; 32,20; ... sont résidus quadratiques, tandis que les termes 35,69; 53,67; 62,63; 31,55; 61,7; 33,28; 52,56; 31,11; 42,22; 21,44; 47,68; 59,65 sont racines primitives. 2° Si la racine primitive est 2, les deux premiers et les deux derniers termes des groupes consécutifs sont à tour de rôle résidus quadratiques ou racines primitives, tant qu'ils ne sont pas résidus de degrés impairs. Ainsi, pour $m = 67$, les termes 33,65; 4,17; 25,59; 16,21; ... sont résidus quadratiques, tandis que les termes 2,34; 50,63; 46,51; 32,44; 61,11; 28,12; 7,48; 18,41; 13,31; 20,57 sont racines primitives.

7. Si la chaîne, commencée par le groupe [1], s'arrête sans avoir englobé tous les $(m - 1)$ nombres, il faut déployer en d'autres chaînes les nombres qui ne sont pas entrés dans la première chaîne. Pour cela, on n'a pas besoin de faire de longs calculs pour déterminer deux nombres associés, car on trouvera toujours dans la première chaîne deux termes associés ou contre-associés qui, par l'échange de leurs facteurs, donneront deux nouveaux termes associés ou contre-associés, qui serviront à la formation d'une chaîne nouvelle. Par exemple, pour $m = 151$, la chaîne, commencée par le groupe [1], contient le groupe

32, 118, 33, 119,

sans contenir le terme 3. On trouvera le groupe contenant ce dernier, en divisant par 11 le terme 33 et en multipliant par le même facteur son contre-associé 32; on aura ainsi le groupe

3, 101, 50, 148,

qui servira à la formation d'une seconde chaîne.

Après avoir déployé en chaînes tous les $(m - 1)$ nombres, on écartera celles qui sont composées entièrement de résidus.

On n'aura en général que deux ou trois chaînes et rarement plus de six. Pour $m = 4h - 1$ on n'aura qu'une seule chaîne ouverte et quelques chaînes fermées, et ce ne sont que ces dernières qui peuvent contenir des racines primitives. Pour $m = 4h + 1$ et h impair, comme nous l'avons déjà dit au n° 4, il y aura aussi une seule chaîne ouverte et quelques chaînes fermées; et si h est pair,

on aura deux chaînes ouvertes, et dans ce cas, s'il n'y a pas de chaînes fermées, c'est la chaîne ouverte, terminée par les groupes $[u]$ et $[v]$, qui contiendra toutes les racines primitives; autrement ces dernières se trouveront dans des chaînes fermées.

Il est très aisé de reconnaître et d'exclure les résidus dans une chaîne ouverte, terminée par $[u]$ et $[v]$, car le groupe central de ces chaînes est composé de résidus de tous les degrés impairs, et les groupes composés de résidus d'un degré impair quelconque sont disposés à des distances égales, marquées par l'exposant de ce degré. Après cette exclusion, les groupes qui resteront contiendront les racines primitives.

Quant aux chaînes fermées, qui n'ont pas de groupe central, on reconnaîtra les groupes composés de résidus d'après de certains caractères que nous allons signaler. Remarquons d'abord que, si le nombre de termes d'une chaîne fermée n'est pas divisible par un des facteurs de $(m-1)$, cette chaîne ne contiendra pas un seul résidu du degré dont l'exposant est marqué par ce facteur, ou bien tous ses termes seront résidus de ce degré.

Par exemple, pour $m = 127 = 2.3^2.7 + 1$, on a quatre chaînes fermées, chacune de 28 termes; ce nombre n'étant pas divisible par le facteur 3, et comme il y a $\frac{126}{3} = 42$ résidus de troisième degré, une de ces chaînes, ainsi que la chaîne ouverte qui a 14 termes, est composée entièrement de résidus du troisième degré. On reconnaîtra facilement cette chaîne fermée, car on y trouve le cube 27.

Il y a des cas, pour les modules de la forme $4h+1$, où une chaîne fermée est composée entièrement de racines primitives. Cela arrive quand 2 et -2 sont résidus de tous les degrés dont les exposants sont facteurs de $(m-1)$.

Par exemple, pour $m = 433 = 2^4.3^3 + 1$, il y a une chaîne fermée de 144 termes qui sont tous racines primitives de 433.

8. Les exemples suivants, pris parmi les cas les plus simples, suffiront à éclaircir l'application de notre procédé à la recherche des racines primitives :

I. *Si m est de la forme* $2n^c+1$, *où n est un nombre premier impair et c est un nombre entier quelconque, tous les résidus*

du degré impair n seront contenus dans la chaîne ouverte, commencée par le groupe [1], *de sorte que, pour trouver les racines primitives, on n'aura qu'à séparer les non-résidus quadratiques, qui seront tous racines primitives.*

En effet, dans ce cas, 2 et — 2, ne pouvant pas être simultanément résidus quadratiques, car m est de la forme $4h - 1$, sont nécessairement résidus du degré impair n.

Prenons une racine primitive quelconque g et posons $2 \equiv g^k$. L'exposant k doit contenir le facteur n, et comme tous les termes de la chaîne, commencée par [1], sont de la forme $\pm 2^{\pm l}$, cette forme deviendra $\pm (g^k)^{\pm l} \equiv \pm g^{\pm kl}$, et, l'exposant kl contenant le facteur n, tous les termes de la chaîne seront résidus du degré n.

Par exemple, pour $m = 251 = 2 \cdot 5^3 + 1$, la chaîne ouverte, commencée par [1], contient tous les 50 résidus du cinquième degré, de sorte que tous les autres nombres, en dehors de cette chaîne, sont résidus ou non-résidus quadratiques, et ces derniers sont nécessairement racines primitives. Ainsi le non-résidu $251 - 15^2 = 26$ est racine primitive de 251.

II. *Pour $m = 4n^c + 1$, où n est un nombre premier impair et c un nombre entier quelconque, la chaîne ouverte contiendra également tous les résidus du degré n.*

En effet, dans ce cas m n'étant pas de la forme $8h + 1$, les nombres 2 et — 2 ne sont pas résidus quadratiques, et par conséquent ils sont résidus du degré n.

Par exemple, pour $m = 109 = 2^2 \cdot 3^3 + 1$, la chaîne ouverte, commencée par [1], englobe tous les 36 résidus du troisième degré, et tous les non-résidus quadratiques qui n'entrent pas dans cette chaîne sont racines primitives. A l'aide de la proposition que nous avons donnée au numéro 1, on trouve que 11 est non-résidu quadratique de 109; par conséquent ce nombre et son associé 10 sont racines primitives de ce module.

III. *Pour les modules de la forme $m = 6N + 1$, où N est un nombre quelconque, premier ou composé, pair ou impair, il y a un groupe dont deux termes associés diffèrent d'une unité*

avec deux autres termes associés, et tous ces termes sont résidus de tous les degrés marqués par les facteurs du nombre N.

Cette proposition permettra de reconnaître facilement les résidus et les racines primitives dans les chaînes fermées, si l'on y trouve un groupe de cette espèce.

En représentant ce groupe par

$$a,\quad b,\quad a+1,\quad b+1$$

et en appelant *termes mineurs* les termes a et b et *termes majeurs* les termes $(a+1)$ et $(b+1)$, on démontrera sans peine :

1° Que le carré d'un terme mineur est congru à son associé et celui d'un terme majeur est congru à son contre-associé, de sorte qu'on aura

$$a^2 \equiv b,\quad b^2 \equiv a,\quad (a+1)^2 \equiv a,\quad (b+1)^2 \equiv b,\quad \ldots \quad (\text{mod. } m);$$

2° Que le cube d'un terme mineur est congru à 1, et celui d'un terme majeur est congru à -1. Ainsi l'on aura

$$a^3 \equiv 1,\quad b^3 \equiv 1,\quad (a+1)^3 \equiv -1,\quad (b+1)^3 \equiv -1,\quad \ldots \quad (\text{mod. } m);$$

3° Que si g est une racine primitive quelconque, le groupe de cette espèce sera représenté de la manière suivante

$$g^{N},\quad g^{5N},\quad g^{2N},\quad g^{4N}.$$

Par exemple, pour $m = 223 \equiv 6.37 + 1$ et $N = 37$, on a le groupe

$$184,\quad 40,\quad 183,\quad 39$$

qui peut être représenté ainsi

$$g^{37},\quad g^{185},\quad g^{74},\quad g^{148};$$

4° Que si N est un nombre premier, on aura deux chaînes : la chaîne ouverte englobera tous les résidus du troisième degré, tandis que la chaîne circulaire contiendra un groupe a, b, $a+1$, $b+1$, composé de quatre résidus du degré N, les deux autres résidus de ce degré étant les termes 1 et -1 de la chaîne ouverte.

Par exemple, pour $m = 31 = 6.5 + 1$, on a deux chaînes :

A. 1, 1, 30, 30; 2, 16, 15, 29; 4, 8, 23, 27.

B. 3, 21, 10, 28; 6, 26, 5, 25;
12, 13, 18, 19; 24, 22, 9, 7; 17, 11, 20, 14.

Les dix termes de la chaîne A sont résidus du troisième degré, et les termes 6, 26, 5, 25 de la chaîne B sont résidus du cinquième degré, et comme le module 31 est de la forme $12h - 5$, le nombre 3 est non-résidu quadratique, et par conséquent il est racine primitive, ainsi que son associé 21 et les deux premiers termes de tous les groupes de la chaîne B, excepté 6 et 26, qui sont résidus du cinquième degré.

Généralement, pour $m = 4h - 1$, si h est pair, comme cela a lieu pour $m = 31 = 4.8 - 1$, ce sont tous les premiers ou tous les derniers termes des groupes qui sont racines primitives, sauf ceux qui sont résidus de degrés impairs, et au contraire, si h est impair, ce sont, à tour de rôle, les premiers et les derniers termes des groupes consécutifs qui sont racines primitives, comme cela a lieu pour $m = 43 = 4.11 + 1$.

C'est d'après les caractères que nous venons de signaler et quelques autres moins saillants, que l'on reconnaîtra dans des chaînes fermées les résidus de tous les degrés. Après les avoir éliminés, on aura les racines primitives. Il est facile d'appliquer ce procédé aux modules de toutes les formes, telles que $m = 8n + 1$, $12n + 1$, ... et à d'autres, où le nombre $(m - 1)$ contient plusieurs facteurs différents, mais nous ne le ferons pas pour ne pas sortir des limites assignées à ce Mémoire. Il nous semble que ce procédé permettra de découvrir les racines primitives, ainsi que les résidus de tous les degrés, beaucoup plus rapidement que les méthodes dont nous avons parlé au n° 1.

9. Pour compléter ce Mémoire, disons quelques mots d'un autre procédé, mentionné par quelques auteurs, qui permet de découvrir sans essais les racines primitives des modules de la forme $4h - 1$. Ce procédé est fondé sur le théorème suivant :

Pour tout module $m = 4h - 1$, *si l'on multiplie deux nombres complémentaires à* m, *tels que* a *et* $m - a \equiv -a$, *le produit* $a(m - a) \equiv -a^2$ *sera racine primitive, dans le cas où l'un de ces nombres est racine primitive.*

En effet, soit g une racine primitive de m et $a \equiv g^k$; en changeant les signes on aura $-a \equiv -g^k \equiv g^{\frac{m-1}{2}+k}$, et en multi-

pliant ces deux congruences on trouvera $-a^2 \equiv g^{\frac{m-1}{2}+gk}$

Si a est racine primitive, l'exposant k est premier avec $m-1$, et comme $\frac{m-1}{2} = 2h-1$ n'a pas de facteur 2, l'exposant $\frac{m-1}{2} + 2k$ sera aussi premier avec $(m-1)$, et par conséquent le produit $a(m-a) \equiv -a^2$, que nous désignerons par a_1, sera également racine primitive de m.

En répétant cette opération jusqu'à ce qu'on retrouve l'un des nombres initiaux a ou $(m-a) \equiv -a$, on aura une suite de produits

$$-a^2 \equiv a_1, \qquad -a_1^2 \equiv a_2, \qquad -a_2^2 \equiv a_3, \qquad \ldots, \qquad -a_t^2 \equiv \pm a.$$

Dans ce cas, aucun des nombres $a_1, a_2, a_3, \ldots$ ne sera associé d'aucun autre nombre de cette suite. C'est évident, car en prenant deux termes quelconques de cette suite

$$a_i \equiv -g^{2ik}, \qquad a_j \equiv -g^{2jk},$$

et en les multipliant, on aura

$$a_i a_j \equiv g^{(2i+2j)k}.$$

Comme k est premier avec $(m-1)$, le produit $(2^i + 2^j)k$ ne peut pas être égal à $m-1 \equiv 0$, et par conséquent la congruence a_i et $a_j \equiv g^{m-1} \equiv 1$ est impossible. Donc, les termes a_i et a_j ne peuvent pas être associés entre eux. Soit b l'associé de a. Formons sa suite

$$-b^2 \equiv b_1, \qquad -b_1^2 \equiv b_2, \qquad -b_2^2 \equiv b_3, \qquad \ldots, \qquad -b_t^2 \equiv \pm b.$$

Ces nombres $b_1, b_2, b_3, \ldots$ seront respectivement associés de $a_1, a_2, a_3, \ldots$. Donc les racines primitives sont toujours réparties entre une ou plusieurs paires de suites.

Éclaircissons ceci par un exemple. Soit $m = 43 = 2.3.7 + 1$.

En commençant par n'importe quels nombres, on aura cinq suites :

A. $2.41 \equiv 39, \quad 39.4 \equiv 27, \quad 27.16 \equiv 2.$

B. $22.21 \equiv 32, \quad 32.11 \equiv 8, \quad 8.35 \equiv 22.$

C. $\begin{cases} 3.40 \equiv 34, & 34.9 \equiv 5, & 5.38 \equiv 18, \\ 18.25 \equiv 20, & 20.23 \equiv 30, & 30.13 \equiv 3. \end{cases}$

D. $\begin{cases} 29.14 \equiv 19, & 19.24 \equiv 26, & 26.17 \equiv 12, \\ 12.31 \equiv 28, & 28.15 \equiv 33, & 33.10 \equiv 29. \end{cases}$

E. $6.37 \equiv 8, \quad 7.36 \equiv 37.$

Comme 43 a 12 racines primitives, il est clair qu'elles forment les suites C et D et sont

34, 5, 18, 20, 30, 3; 19, 26, 12, 28, 33, 39.

Pour $m = 211 = 2.3.5.7 + 1$, il y a 48 racines primitives, qui se répartissent entre quatre suites de 12 produits. Mais ce procédé est moins expéditif que le procédé général exposé plus haut.