NOUVELLES ANNALES DE MATHÉMATIQUES

G. FONTENÉ

Sur les modules de la forme P^m, P premier (impair ou pair)

Nouvelles annales de mathématiques 4^e série, tome 8 (1908), p. 193-216

<http://www.numdam.org/item?id=NAM_1908_4_8__193_0>

[17a]

SUR LES MODULES DE LA FORME p^m, p PREMIER (IMPAIR OU PAIR);

PAR M. G. FONTENÉ.

1. La première Partie de ce Mémoire est relative aux modules de la forme p^m, p étant un nombre premier autre que 2; la seconde Partie est relative au module 2^m.

Si on laisse de côté le module 4, qui admet 3 comme racine primitive, on sait que, *pour un module composé* M, *il n'existe de racines primitives, c'est-à-dire de nombres appartenant à l'exposant* $\varphi(M)$, *que dans les deux cas suivants :*

$$M = p^m, \quad p \text{ premier et autre que } 2,$$
$$M = 2p^m, \quad \text{» } \quad \text{»}$$

Dans le premier cas, qui est le plus intéressant, on a

$$\varphi(p^m) = p^{m-1}(p-1),$$

et il existe des nombres N appartenant à l'exposant

$$p^{m-k}\delta \qquad (k \geqq 1),$$

δ étant un diviseur de $p-1$; le nombre de ces nombres, supposés inférieurs à p^m, est

$$\varphi(p^{m-k}\delta) \quad \text{ou} \quad \varphi(p^{m-k})\,\varphi(\delta),$$

ou encore

$$k < m, \qquad p^{m-k-1}(p-1)\,\varphi(\delta),$$
$$k = m, \qquad \varphi(\delta):$$

je me propose de donner de ces nombres, pour chaque valeur de k et chaque valeur de δ, *une*

expression plus arithmétique que celle qui résulte de l'emploi d'une racine primitive relative au module p^m.

Je dirai ensuite un mot sur le cas du module $2p^m$, pour lequel on a

$$\varphi(2p^m) = \varphi(p^m).$$

Dans la seconde Partie, je considère le module 2^m, $m \geqq 3$, pour lequel il n'y a pas de racines primitives. Aux exposants 2^{m-2}, 2^{m-3}, ..., 2, appartiennent des nombres dont le nombre est

$$2\varphi(2^{m-2}),\ 2\varphi(2^{m-3}),\ \ldots,\ 2\varphi(2);$$

restent les deux nombres 1 et $2^m - 1$ qui appartiennent respectivement aux exposants 1 et 2.

PREMIÈRE PARTIE.

MODULES DE LA FORME p^m, p ÉTANT IMPAIR.

I.

Nous chercherons d'abord à quel exposant appartient un nombre donné N, relativement au module p^m.

2. Lemme. — *Soit un nombre* H, *pour lequel on a, avec* $h \geqq 1$,

$$\begin{cases} H - 1 = p^h q' & (p \geqq 3) \\ (q' \text{ non multiple de } p); \end{cases}$$

on a aussi

$$\begin{cases} H^{p^{m-h}} - 1 = p^m q \\ (q \text{ non multiple de } p). \end{cases}$$

Ces deux faits (l'un positif, l'autre négatif) ayant lieu par hypothèse pour $m = h$, il suffira de montrer

que, s'ils ont lieu pour une valeur de m, ils ont lieu pour la valeur immédiatement supérieure.

Écrivons

$$H^{p^{m-h}} = p^m q + 1,$$

q ne renfermant pas le facteur p, et élevons les deux membres à la puissance p. Comme les coefficients du binome, pour un exposant premier p, sont multiples de p, sauf le premier et le dernier qui ont la valeur 1 (1), on a

$$\begin{aligned} H^{p^{m+1-h}} = {} & p^{p^m} && q^p \\ & + p^{(p-1)m+1} && q^{p-1} \\ & + p^{(p-2)m+1} && q^{p-2}\,A \\ & + \ldots \\ & + p^{2m+1} && q^2\,L \\ & + p^{m+1} && q \\ & + 1, \end{aligned}$$

et, par suite,

$$H^{p^{m+1-h}} - 1 = p^{m+1}\,Q;$$

ainsi le premier membre est divisible par p^{m+1}.

En outre, Q ne renferme pas le facteur p ; on a en effet le diviseur qui donne le quotient, Q étant p^{m+1},

$$\begin{aligned} Q = {} & p^{(p-1)m-1} && q^p \\ & + p^{(p-2)m} && q^{p-1} \\ & + p^{(p-3)m} && q^{p-2}\,A \\ & + \ldots \\ & + p^m && q^2\,L \\ & + && q, \end{aligned}$$

---

(1) Un fait analogue a lieu pour la formule qui donne la puissance $p^{\text{ième}}$ d'un polynome, et cela donne une démonstration du théorème de Fermat. (*Voir* CAHEN, *Éléments de la Théorie des nombres*, p. 66; nous indiquerons les renvois à cet Ouvrage par la notation C, p. 66.)

et la partie qui précède q est multiple de p, même dans le cas le plus défavorable, $p = 3$, où cette partie est

$$p^{2m-1} q^3 + p^m q^2,$$

m étant au moins 1. Comme l'égalité ci-dessus en H n'est pas autre chose que l'égalité primitive avec $m + 1$ au lieu de m, comme de plus le quotient Q a la propriété du quotient q, le fait annoncé est établi.

3. **Théorème.** — *Soit p un nombre premier autre que* 2,

$$p \geqq 3.$$

Le nombre N *étant premier avec p, si* δ *est l'exposant auquel appartient* N *(ou son résidu n par rapport à p) pour le module p, et si la plus haute puissance de p qui divise* $N^\delta - 1$ *est* p^h, *avec* $h \geqq 1$, *l'exposant auquel appartient* N *relativement au module* p^m *est*

$$p^{m-h}\delta,$$

tant qu'on a $h \leqq m$.

On a, par hypothèse, avec $h \geqq 1$,

$$(1) \qquad \begin{cases} N^\delta - 1 = p^h q' \\ (q' \text{ non multiple de } p); \end{cases}$$

on a en outre

$$(2) \qquad N^\delta - 1 = \dot{p} \qquad (\delta \text{ minimum});$$

la conclusion est, avec $m \geqq h$,

$$(3) \quad N^{p^{m-h}\delta} - 1 = p^m q \qquad (\text{exposant minimum pour N}).$$

1° D'après (2), les seules puissances de N qui, divisées par p, donnent 1 pour reste, sont celles dont l'exposant est multiple de δ; l'exposant auquel appartient N, pour le module p^m, est donc d'abord multiple de δ.

2° D'après (1), en appliquant le lemme du n° 2 avec $H = N^{\delta}$, on a

$$\begin{cases} N^{p^{m-h}\delta} - 1 = p^m q \\ (q \text{ non multiple de } p); \end{cases}$$

l'exposant auquel appartient N, pour le module p^m, est donc $p^{m-h}\delta$, ou un diviseur de ce nombre ; comme cet exposant doit être multiple de δ, qui est un diviseur de $p - 1$, il est certainement de la forme $p^{l-h}\delta$, avec $l \leqq m$.

Or, avec l'hypothèse (1), on a

$$\begin{cases} N^{p^{l-h}\delta} - 1 = p^l q \\ (q \text{ non multiple de } p); \end{cases}$$

donc le premier membre n'est divisible par p^m que si l'on a $l = m$. Le nombre N appartient donc bien à l'exposant $p^{m-h}\delta$, comme l'indique l'écriture (3).

On peut observer que le quotient q de l'égalité (3) *ne renferme plus le facteur p.* L'énoncé même du théorème entraîne d'ailleurs cette conséquence ; sans quoi N appartiendrait pour le module p^{m+i} à un exposant diviseur de $p^{m-h}\delta$, ce qui est contraire au théorème.

4. **Remarque.** — Si l'on a $h > m$, l'exposant auquel appartient N est simplement δ, puisqu'on a, d'après (1),

$$N^{\delta} - 1 = p^m \times p^{h-m} q',$$

et que, d'ailleurs, cet exposant doit renfermer le facteur δ ; le quotient $p^{h-m}q'$ renferme alors le facteur p.

(La même chose a déjà lieu pour $h = m$, si ce n'est que le quotient est alors q' non multiple de p.)

II.

Voyons maintenant, ce qui est l'objet principal de ce Mémoire, quels nombres N appartiennent à un exposant donné $p^{m-k}\delta$, k étant au moins 1, et δ étant un diviseur de $p-1$. Pour

$$k = 1, 2, \ldots, h, \ldots, m-1,$$

on doit chercher les nombres qui satisfont à la fois aux conditions (1) et (2), δ et h étant donnés. Pour $k = m$, c'est-à-dire lorsqu'il s'agit des nombres N qui appartiennent simplement à l'exposant δ, on aura à tenir compte de la remarque du n° 4.

Nous commencerons par résoudre, et c'est l'objet de ce paragraphe, un problème plus général que celui que nous avons en vue.

5. **Problème I.** — *Résoudre la congruence*

$$N^s = \mathfrak{N} + \dot{p}^{h+1},$$

l'exposant s n'étant pas multiple de p; le point indique un multiple de p^{h+1}.

Supposons connus les $h+1$ derniers chiffres de $\mathfrak{N}$ écrit en base p, et cherchons les $h+1$ derniers chiffres de N écrit de même (1); on veut avoir

$$\begin{aligned}(n + ap + bp^2 + \ldots + ep^{h-1} + fp^h + \dot{p}^{h+1})^s \\ = \nu + \alpha p + \beta p^2 + \ldots + \varepsilon p^{h-1} + \varphi p^h + \dot{p}^{h+1};\end{aligned}$$

(1) Dans le traitement des questions où le module est une puissance de p, on procède de proche en proche à partir du module premier p, en faisant croître d'une unité à chaque fois l'exposant de la puissance (C, p. 99); on comprend dès lors que l'emploi du système de numération à base p doit donner aux démonstrations un tour aisé.

nous supposerons $\mathfrak{N}$ non multiple de p, c'est-à-dire

$$\nu \not\equiv 0, \qquad \text{d'où} \qquad n \not\equiv 0.$$

On doit avoir d'abord

$$n^s = \nu + \dot{p} \qquad (n < p);$$

ν *doit donc être un reste de puissance* $s^{ième}$ *par rapport au module* p, et la condition pour qu'il en soit ainsi est celle-ci : δ désignant le plus grand commun diviseur entre s et $p-1$, ν doit être l'une des $\frac{p-1}{\delta}$ solutions de la congruence

$$\nu^{\frac{p-1}{\delta}} = 1 + \dot{p};$$

cette condition remplie, la congruence ci-dessus en n a δ solutions distinctes (C, p. 99). Dans le cas particulier

$$\nu = 1,$$

que nous aurons à considérer, ces δ solutions sont, comme on sait, celles de la congruence

$$n^\delta = 1 + \dot{p} \qquad (n < p).$$

La valeur de n étant choisie, on doit avoir en second lieu

$$(n + ap)^s = \nu + \alpha p + \dot{p}^2,$$

ou

$$(n^s - \nu) + s n^{s-1} ap - \alpha p = \dot{p}^2,$$

ou

$$\frac{n^s - \nu}{p} + s n^{s-1} a - \alpha = \dot{p} \qquad (\alpha < p);$$

on a supposé s non multiple de p pour que le coefficient de l'inconnue a soit premier avec le module p,

et la congruence a alors une solution, soit a (¹).

On doit avoir ensuite

$$(n + ap + bp^2)^s = \nu + \alpha p + \beta p^2 + \dot{p}^3,$$

ou

$$[(n + ap)^s - (\nu + \alpha p)] + s(n + ap)^{s-1} bp^2 - \beta p^2 = \dot{p}^3,$$

on divise par p^2, etc. (²).

On continue ainsi de proche en proche.

6. **Problème II.** — *L'exposant s n'étant pas multiple de p, trouver* N *d'après les conditions*

$$\begin{cases} N^s - \nu = p^h q' \\ (q' \text{ non multiple de } p), \end{cases}$$

où ν *est un reste de puissance* $s^{ième}$ *par rapport au module p.*

Il faut, dans ce qui précède, faire

$$\begin{cases} \alpha = 0, \quad \beta = 0, \quad \ldots, \quad \varepsilon = 0 \\ (\varphi \neq 0). \end{cases}$$

La valeur de n étant choisie, si l'on désigne par a_0,

(¹) Si s est multiple de p, on a

$$(n + \dot{p})^s = n^s + \dot{p}^2;$$

la congruence à résoudre est impossible ou indéterminée selon qu'on n'a pas ou qu'on a

$$n^s = \nu + \alpha p + \dot{p}^2.$$

(²) Si s est multiple de p, on a

$$(n + ap + \dot{p}^2)^s = (n + ap)^s + \dot{p}^3;$$

la congruence à résoudre est impossible ou indéterminée selon qu'on n'a pas ou qu'on a

$$(n + ap)^s = \nu + \alpha p + \beta p^2 + \dot{p}^3.$$

$b_0, \ldots, e_0, f_0$ les valeurs de $a, b, \ldots, e, f$, pour $\alpha, \beta, \ldots, \varepsilon, \varphi$ égaux à zéro, il faut prendre (puisque φ ne doit pas être nul)

$$\left\{ \begin{array}{c} N = n + a_0 p + b_0 p^2 + \ldots + e_0 p^{h-1} + f p^h + \dot{p}^{h+1} \\ (f \neq f_0). \end{array} \right.$$

Le nombre des valeurs de n est δ, le nombre des valeurs de f est $p - 1$; à chacune de ces valeurs de f correspond pour φ l'une des valeurs $1, 2, 3, \ldots, p - 1$, dans l'égalité

$$N^s - 1 = p^h(\dot{p} + \varphi).$$

Pour une même valeur de n, les nombres N forment $p - 1$ progressions arithmétiques de raison p^{h+1}.

7. **Cas particulier.** — *L'exposant s n'étant pas multiple de p, trouver* N *d'après les conditions*

$$\left\{ \begin{array}{c} N^s - 1 = p^h q' \\ (q' \text{ non multiple de } p). \end{array} \right.$$

Si l'on désigne toujours par δ le plus grand commun diviseur entre s et $p - 1$, les valeurs de N sont celles qui vérifient les conditions plus simples :

$$(1) \qquad \left\{ \begin{array}{c} N^\delta - 1 = p^h q' \\ (q' \text{ non multiple de } p); \end{array} \right.$$

cela donne

$$(1') \left\{ \begin{array}{c} N = n + a_0 p + b_0 p^2 + \ldots + e_0 p^{h-1} + f p^h + \dot{p}^{h+1} \\ (f \neq f_0); \end{array} \right.$$

n est l'une des δ solutions de la congruence

$$n^\delta - 1 = \dot{p},$$

et, lorsque la valeur de n a été choisie, les coeffi-

cients a_0, b_0, ..., e_0 sont absolument déterminés, le nombre des valeurs de f est $p-1$. En effet, d'une part les valeurs de N qui satisfont aux conditions (1) satisfont aux conditions proposées, et, d'autre part, la réponse au problème primitif est également de la forme (1') avec δ valeurs pour n et $p-1$ valeurs pour f; d'ailleurs, en ce qui concerne n, on a déjà rappelé que les congruences

$$n^s - 1 = \dot{p}, \qquad n^\delta - 1 = \dot{p}$$

ont les mêmes solutions (congruences à modules premiers).

III.

8. **Des nombres qui appartiennent à un exposant donné pour un module donné** p^m, $p \geqq 3$. — Pour avoir les nombres N qui appartiennent à l'exposant $p^{m-h}\delta$ relativement au module p^m, δ étant un diviseur de $p-1$, et h ayant l'une des valeurs $1, 2, \ldots, m-1$ (mais non la valeur m que nous écartons pour le moment), il faut prendre les nombres N qui vérifient les conditions suivantes :

$$(1) \qquad \begin{cases} N^\delta - 1 = p^h q' \\ (q' \text{ non multiple de } p) \end{cases}$$

et

$$(2) \qquad N^\delta - 1 = \dot{p} \qquad (\delta \text{ minimum});$$

on supposera d'ailleurs

$$N < p^m.$$

Le nombre N devant ici appartenir à l'exposant δ pour le module p, il doit en être de même de son résidu n par rapport à p, et l'on doit avoir

$$(2') \qquad n^\delta - 1 = \dot{p} \qquad (\delta \text{ minimum}).$$

Le nombre des valeurs de n pour la formule (1') est alors seulement $\varphi(\delta)$; comme, dans cette formule,

$$(1')\quad \begin{cases} N = n + a_0 p + b_0 p^2 + \ldots + e_0 p^{h-1} + f p^h + \dot{p}^{h+1} \\ (f \neq f_0), \end{cases}$$

le coefficient f a $p-1$ valeurs, les nombres demandés N forment $(p-1)\varphi(\delta)$ progressions arithmétiques de raison p^{h+1}, et chacune de ces progressions doit être limitée par la condition $N < p^m$. On peut écrire

$$N = N' + p^{h+1} \times (0, 1, 2, \ldots, p^{m-1-h} - 1),$$

avec $N' < p^{h+1}$. Comme on a pour n des valeurs en nombre $\varphi(\delta)$, pour f des valeurs en nombre $p-1$, pour le multiplicateur de p^{h+1} des valeurs en nombre p^{m-h-1}, le nombre des valeurs de N qu'on obtient est

$$\varphi(\delta) \times (p-1) \times p^{m-h-1} \qquad \text{ou} \qquad \varphi(p^{m-h}\delta),$$

comme on le sait par ailleurs.

Pour $h = m-1$, on arrive à prendre

$$\begin{cases} N = n + a_0 p + b_0 p^2 + \ldots + r_0 p^{m-2} + s p^{m-1} \\ (s \neq s_0). \end{cases}$$

Si l'on prend enfin

$$N = n + a_0 p + b_0 p^2 + \ldots + r_0 p^{m-2} + s_0 p^{m-1},$$

on a

$$N^\delta - 1 = \dot{p}^m,$$

le quotient pouvant renfermer le facteur p, et N appartient à l'exposant δ pour le module p^m. On a pour N des valeurs en nombre $\varphi(\delta)$. On peut dire qu'on a ici $h \geqq m$; le quotient de $N^\delta - 1$ par p^m renferme le facteur p à la puissance $h-m$, si h est plus grand que m.

Dans tous les cas, les nombres N (plus petits que p^m) qui appartiennent à l'exposant $p^{m-k}\delta$ pour le module p^m sont en nombre

$$\varphi(p^{m-k}\delta).$$

9. Prenons, par exemple, $p = 7$. Pour des valeurs données de δ et de h, les nombres N qui satisfont aux conditions (1) et (2) forment $6\varphi(\delta)$ progressions arithmétiques illimitées (*voir* le Tableau de la page 205).

Cela étant, si le module est, par exemple, 7^4, les nombres de la double colonne qui a pour titre $\delta = 3$ appartiennent successivement aux exposants $7^3 \times 3$, $7^2 \times 3$, 7×3, et la suite de la colonne ($h \geq 4$) donne une progression unique de nombres appartenant à l'exposant 3. Si l'on se borne aux nombres plus petits que 7^4, les progressions renferment successivement 7^2 termes, 7 termes, 1 terme, et encore 1 terme; de sorte que, dans la colonne qui correspond à $\delta = 3$, $n = 2$, par exemple, le nombre des éléments est

$$(7^2 + 7 + 1) \times (7 - 1) + 1 \quad \text{ou} \quad 7^3;$$

le nombre total des colonnes étant $7 - 1$, le nombre total des éléments est

$$7^3 \times (7 - 1) \quad \text{ou} \quad \varphi(7^4).$$

10. Pour $\delta = 1$, on veut avoir

$$\begin{cases} N - 1 = p^h q' & (N - 1 = \dot{p}) \\ (q' \text{ non multiple de } p), \end{cases}$$

c'est-à-dire *a priori*

$$N = p^h \times (1, 2, 3, \ldots, p - 1) + 1 + \dot{p}^{h+1},$$

avec $f \not\equiv 0$.

	$\delta = 1.$	$\delta = 2.$	$\delta = 3.$		$\delta = 6.$	
	$n = 1.$	$n = 6.$	$n = 2.$	$n = 4.$	$n = 5.$	$n = 3.$
$h = 1.$		$N = 6 + \dot{7}^2$	$N = 2 + \dot{7}^2$	$N = 4 + 7^2$	$N = 5 + \dot{7}^2$	$N = 3 + 7^2$
	$N = 8 + 7^2$	13	9	11	12	10
	15	20	16			17
	22	27	23	25	26	24
	29	34		32	33	
	36	41	37	39	40	38
	43		44	46	47	45
$h = 2.$		$N = 48 + \dot{7}^3$	$N = 30 + \dot{7}^3$		$N = 31 + \dot{7}^3$	
	$N = 50 + \dot{7}^3$	...	...	$N = 67 + \dot{7}^3$	...	$N = 68 + \dot{7}^3$
	...	...	...	...	...	...
...	...	...	...	...	...	...

Pour $\delta = 2$, on veut avoir

$$\begin{cases} N^2 - 1 = p^h q' \qquad (N + 1 = \dot{p}) \\ (q' \text{ non multiple de } p), \end{cases}$$

c'est-à-dire *a priori*

$$N = p^h \times (1, 2, 3, \ldots, p-1) - 1 + \dot{p}^{h+1},$$

avec $f \neq 0$; cette écriture correspond à $n = -1$, et, si l'on veut conserver $n = p - 1$, il faut écrire

$$N = (p-1) + (p-1)p + (p-1)p^2 + \ldots + (p-1)p^{h-1} + p^h \times (0, 1, 2, \ldots, p-2) + \dot{p}^{h+1},$$

avec $f \neq p - 1$.

Si l'on suppose, par exemple, $p = 3$, c'est-à-dire

$$\begin{cases} N^\delta - 1 = 3^h q' \\ (q' \text{ non multiple de } 3), \end{cases}$$

on peut avoir seulement $\delta = 1$, ou $\delta = 2$, ce qui donne d'abord

$$N = \dot{3} + 1$$

ou

$$N = \dot{3} - 1.$$

Pour $h = 1$, on a donc (avec $n = \pm 1$)

$$N = \pm 1 + 3(1, 2) + \dot{9}.$$

Restent les nombres N des deux formes $9\lambda \pm 1$; prenant d'abord λ non multiple de 3, on a

$$N = \pm 1 + 9(1, 2) + \dot{27},$$

et ces nombres correspondent à $h = 2$. Restent les nombres N des deux formes $27\lambda \pm 1$, etc.

11. Remarque générale pour le cas où δ est pair. — Si δ est pair, $\delta = 2d$, les conditions (1) et (2) du n° 8 sont équivalentes à celles-ci :

$$[1] \qquad \begin{cases} N^d + 1 = p^h q' \\ (q' \text{ non multiple de } p), \end{cases}$$

$$[2] \qquad N^d + 1 = \dot{p} \qquad (d \text{ minimum});$$

en effet, $N^d - 1$ n'est pas divisible par p, de sorte que $N^d + 1$ doit être divisible par p^h.

On a ici $\nu = -1$, et la condition

$$(-1)^{\frac{p-1}{d}} = 1 + \dot{p},$$

qui exprime que -1 est un reste de puissance $d^{\text{ième}}$ par rapport au module p, est naturellement satisfaite, $p - 1$ étant multiple de $2d$. La congruence

$$n^d + 1 = \dot{p}$$

donne d valeurs de n, et, parmi ces valeurs, celles pour lesquelles l'exposant d est minimum sont en nombre $\varphi(\delta)$, ou $\varphi(2d)$, c'est-à-dire $2\varphi(d)$ ou $\varphi(d)$ selon que d est pair ou impair. Dans ce dernier cas, par exemple, les solutions de la congruence considérée sont les compléments à p des solutions de la congruence

$$n^d - 1 = \dot{p},$$

et la valeur $\varphi(d)$ est intuitive (*voir* $\delta = 6$ dans le Tableau relatif à $p = 7$); voici un exemple du premier cas :

$$p = 5, \qquad \delta = 4, \qquad d = 2$$

donnent, avec $\varphi(d) = 1$, $2\varphi(d) = 2$,

$$2^2 + 1 = 5, \qquad 3^2 + 1 = 10.$$

On a un lemme analogue à celui qui a été démontré au n° 2, avec $+1$ au lieu de -1.

Pour le théorème, il faut mettre $+1$ au lieu de -1 dans les hypothèses (1) et (2) et dans la conclusion (3).

Les nombres qui appartiennent à l'exposant $p^{m-h}\delta$ pour le module p^m, lorsque δ est pair, $\delta = 2d$, sont ceux pour lesquels on a

$$N^{p^{m-h}d} + 1 = \dot{p}^m \quad \text{(exposant minimum pour N)};$$

ils sont en nombre

$$\varphi(2d) \times \varphi(p^{m-h}) \qquad \text{ou} \qquad \varphi(p^{m-h}\delta).$$

12. **Restes des puissances des nombres** N. — Soit N un nombre qui vérifie les conditions (1) et (2); il appartient, pour le module p^m, à l'exposant $p^{m-h}\delta$, et, dans la suite des restes fournis par la progression

$$1, \quad N, \quad N^2, \quad \ldots, \quad N^{\delta-1}, \quad \ldots,$$

le diviseur étant p^m, les $p^{m-h}\delta$ premiers restes sont distincts. Soit R un des δ premiers restes. On a

$$R \times N^{\delta} = R \times (1 + p^h q') = R + \dot{p}^h;$$

il en résulte que *les restes, pris de δ en δ à partir de* R, *sont les résidus par rapport à p^m des nombres*

$$R + p^h \times (0, 1, 2, 3, \ldots, p^{m-h} - 1),$$

en nombre p^{m-h}.

Si δ est pair, $\delta = 2d$, on a

$$R \times N^d = R \times (-1 + p^h q') = -R + \dot{p}^h;$$

les restes, pris de d en d, sont alternativement les résidus par rapport à p^m des nombres des deux groupes

$$\pm R + p^h \times (0, 1, 2, 3. \ldots, p^{m-h} - 1).$$

Pour $\delta = 1$, $\delta = 2$, les choses sont particulièrement simples.

IV.

13. **Module** $2p^m (p \gtrless 3)$. — Pour le problème I :

$$N^s = \mathfrak{N} + 2\dot{p}^{h+1},$$

il suffira qu'on ait

$$N^s = \mathfrak{N} + \dot{p}^{h+1},$$

N *étant de même parité que* $\mathfrak{N}$. Comme on a alors

$$N = (n + ap + bp^2 + \ldots + ep^{n-1} + fp^h) + kp^{h+1},$$

on prendra k pair ou impair selon les circonstances.

Pour le problème II :

$$\begin{cases} N^s - \nu = 2p^h q' \\ (q' \text{ non multiple de } p), \end{cases}$$

on procédera d'une manière analogue.

Relativement aux nombres qui appartiennent à un exposant donné $p^{m-h}\delta$ pour le module $2p^m$, tant que h n'est pas m, on doit prendre

$$N = N' + p^{h+1} \times (1, 3, 5, \ldots, 2p^{m-1-h} - 1),$$

si N′ est de parité contraire à $\mathfrak{N}$, et

$$N = N' + p^{h+1} \times (0, 2, 4, \ldots, 2p^{m-1-h} - 2),$$

si N′ est de même parité que $\mathfrak{N}$; le nombre de ces nombres est, dans les deux cas,

$$\varphi(\delta) \times (p - 1) \times p^{m-h-1}$$

ou

$$\varphi(p^{m-h}\delta).$$

Pour un exposant δ on prendra

$$N = n + a_0 p + b_0 p^2 + \ldots + s_0 p^{m-1} + p^m \times (0 \text{ ou } 1),$$

de façon que N soit de même parité que $\mathfrak{N}$.

DEUXIÈME PARTIE.

MODULE 2^m, $m \geqq 3$.

14. Lemme. — *Soit* N *un nombre impair pour lequel on a*

$$(4) \quad \begin{cases} N - 1 = 2^h q' \quad \text{ou} \quad N + 1 = 2^h q' \quad (h \geqq 2) \\ (q' \text{ impair}); \end{cases}$$

on a alors

$$(5) \quad \begin{cases} N^{2^{m-h}} - 1 = 2^m q \quad (m > h) \\ (q \text{ impair}). \end{cases}$$

Pour $m = h + 1$, on doit avoir d'abord

$$N^2 - 1 = 2^{h+1} q \quad (q \text{ impair});$$

or, on a, par hypothèse,

$$N = 2^h q' \pm 1 \quad (q' \text{ impair}),$$

d'où

$$N^2 = 2^{2h} q'^2 \pm 2^{h+1} q' + 1,$$

ou

$$N^2 - 1 = 2^{h+1} q' (2^{h-1} q' \pm 1);$$

pour $h \geqq 2$, on a bien ce qu'on cherche.

D'autre part, supposons qu'on ait obtenu pour une certaine valeur de m

$$(a) \quad N^{2^{m-h}} = 2^m q + 1 \quad (q \text{ impair});$$

on a, par élévation au carré,

$$N^{2^{m+1-h}} = 2^{2m} q^2 + 2^{m+1} q + 1$$

ou

$$(b) \qquad N^{2^{m+1-h}} - 1 = 2^{m+1} q (2^{m-1} q + 1);$$

avec $m > 1$, (b) n'est autre chose que (a) où l'on remplace m par $m + 1$.

Le fait énoncé est donc exact.

15. **Théorème.** — *Un nombre impair étant mis sous la forme* (4), *ou encore sous la forme*

$$(6) \qquad N = (2^h \pm 1) + \dot{2}^{h+1} \qquad (h \geqq 2),$$

ce qui est toujours possible d'une seule façon, l'exposant auquel appartient ce nombre pour le module 2^m *est* 2^{m-h}, *tant qu'on a* $h < m$.

Même démonstration que pour le théorème analogue de la première Partie. *On peut observer que le quotient q de l'égalité* (5) *est impair.*

Je réunis ici les conditions d'inégalité

$$2 \leqq h \leqq m - 1.$$

16. **Remarque.** — Lorsqu'on a $h \geqq m$, le nombre N appartient à l'exposant 1 ou à l'exposant 2 selon qu'on a

$$N = 2^h q' + 1 \qquad \text{ou} \qquad N = 2^h q' - 1.$$

17. **Des nombres qui appartiennent à un exposant donné pour le module** 2^m, $m \geqq 3$. — Le module 2^m étant donné, les nombres de la forme (6), avec $h \leqq m - 1$, appartiennent à l'exposant 2^{m-h}, qui prend les valeurs

$$2^{m-2} \quad 2^{m-3}, \quad \ldots, \quad 2^2, \quad 2;$$

pour chaque exposant, ces nombres forment *deux* pro-

gressions arithmétiques. *Les nombres des deux formes*

$$\dot{2}^m + 1, \quad 2^m - 1$$

appartiennent respectivement aux exposants 1 *et* 2. Si l'on se borne aux nombres inférieurs à 2^m, les nombres considérés sont en nombre

$$2[\varphi(2^{m-2}) + \varphi(2^{m-3}) + \ldots + \varphi(2) + 1],$$
$$\text{ou} \quad 2^{m-1}, \qquad \text{ou} \quad \varphi(2^m).$$

Le module étant 16, par exemple, on a pour l'exposant 4 les nombres 3, 11 et 5, 13; pour l'exposant 2 les nombres 7 et 9, et en outre le nombre 15; pour l'exposant 1, le nombre 1.

18. Prenons la formule (6).

1° Pour $h = 2$, on a les nombres des deux formes

$$N = \dot{8} + 5 \qquad \text{ou} \qquad \dot{8} + 3$$

qui appartiennent à l'exposant 2^{m-2} (quotient du module par 4, ou moitié de l'indicateur du module; pas de racines primitives).

2° Restent les nombres des deux formes $8\lambda \pm 1$. Prenant d'abord λ impair, on a

$$N = \dot{16} + 9 \qquad \text{ou} \qquad \dot{16} + 7.$$

Or, en faisant $h = 3$ (ce qui suppose $m \geqq 4$), on voit que tout nombre de l'une de ces formes appartient à l'exposant 2^{m-3} (quotient du module par 8).

3° Restent les nombres des deux formes $16\lambda \pm 1$. Prenant d'abord λ impair, on a

$$N = \dot{32} + 17 \qquad \text{ou} \qquad \dot{32} + 15.$$

Or, en faisant $h = 4$ (ce qui suppose $m \geqq 5$), on voit

que tout nombre de l'une de ces formes appartient à l'exposant 2^{m-4}.

En continuant ainsi, après avoir fait $h = m - 1$, ce qui donne des nombres appartenant à l'exposant 2, il restera les nombres des deux formes $2^m\lambda \pm 1$, qui appartiennent respectivement aux exposants 1 et 2.

19. Nous donnerons encore, en commençant par les exposants les plus faibles et en nous bornant aux nombres inférieurs à 2^m, le Tableau suivant :

Exposant.	Nombres.
$\left\{\begin{matrix}1\\2\end{matrix}\right.$	$\left\{\begin{matrix}1\\2^{m-1}\end{matrix}\right.$
2	$(2^{m-1} \pm 1)$
2^2	$(2^{m-2} \pm 1) + 2^{m-1} \times (0, 1)$
2^3	$(2^{m-3} \pm 1) + 2^{m-2} \times (0, 1, 2, 3)$
..	.....
2^{m-h}	$(2^h \pm 1) + 2^{h+1} \times (0, 1, 2, \ldots, 2^{m-h-1} - 1)$
.....	.....
2^{m-2}	$(2^2 \pm 1) + 2^3 \times (0, 1, 2, \ldots, 2^{m-3} - 1)$

Par exemple, avec le module 2^6 ou 64, on peut former comme il suit le Tableau des nombres autres que 1 et 63, avec l'exposant en indice :

$$\begin{array}{ccccccc} & & & (31,33)_2 & & & \\ & (15,17)_4 & & (31,33)_2 & & (47,49)_4 & \\ (7,9)_8 & (15,17)_4 & (23,25)_8 & (31,33)_2 & (39,41)_8 & (47,49)_4 & (55,57)_8 \end{array}$$

une dernière ligne, non écrite faute de place, commencerait par $(3,5)_{16}$ et finirait par $(59,61)_{16}$.

20. **Restes des puissances des nombres N.** — *Pour les nombres de la forme*

$$N = (2^h + 1) + \dot{2}^{h+1},$$

lesquels appartiennent à l'exposant 2^{m-h}, *les restes des puissances par rapport au module* 2^m *sont*

$$2^h \times (0, 1, 2, \ldots 2^{m-h} - 1) + 1.$$

Soit

$$N^t = 2^m Q + R,$$

$$N^t - 1 = 2^m Q + (R - 1);$$

le premier membre est divisible par $N - 1$, donc par 2^h, ...

Pour les nombres de la forme

$$N = (2^h - 1) + 2^{h+1},$$

lesquels appartiennent aussi à l'exposant 2^{m-h}, *les restes des puissances par rapport au module* 2^m *sont, pour les puissances paires de* N,

$$2^{h+1} \times (0, 1, 2, \ldots, 2^{m-h-1} - 1) + 1,$$

et pour les puissances impaires

$$2^{h+1} \times (0, 1, 2, \ldots, 2^{m-h-1} - 1) + (2^h - 1).$$

Soit

$$N^t = 2^m Q + R,$$

$$N^t - 1 = 2^m Q + (R - 1), \qquad N^t + 1 = 2^m Q + (R + 1).$$

Si t est pair, $N^t - 1$ est divisible par $(N + 1)(N - 1)$, donc par 2^{h+1}, ...

Si t est impair, $N^t + 1$ est divisible par $N + 1$, donc par 2^h; le quotient

$$(N^{t-1} - N^{t-2}) + \ldots + (N^2 - N) + 1$$

est impair, et l'on a

$$R = 2^h(2q + 1) - 1 = 2^{h+1}q + (2^h - 1);$$

etc.

21. Les derniers chiffres des puissances de 5 écrites en base 10. — Je terminerai par une remarque pour laquelle je me bornerai à un exemple. On a

$$5 - 1 = 2^2 q'$$

et, par suite,

$$5^{2^{m-2}} - 1 = \dot{2}^m q;$$

on a donc

$$5^m (5^{2^{m-2}} - 1) = \dot{10}^m$$

ou

$$5^{m+2^{m-2}} - 5^m = \dot{10}^m.$$

Donc, *si l'on écrit les puissances de* 5 *dans le système de numération dont la base est* 10, *à partir de* $5^m (m \geqq 2)$, *les m derniers chiffres se reproduisent périodiquement, le nombre des termes de la période étant* 2^{m-2}.

Si l'on fait le calcul des puissances successives de 5, on trouve ceci :

1° Ces puissances, à partir de 5^2, se terminent toutes par 25;

2° A partir de 5^3, elles se terminent alternativement par 125 et 625;

3° A partir de 5^4, elles se terminent périodiquement par 0625, 3125, 5625, 8125;

Etc.

22. Modules 4 et 2. — Relativement au module 2, on a supposé $m \geqq 3$. Pour le module 2^2, les impairs étant de l'une des deux formes $4\lambda \pm 1$, ceux qui correspondent au signe + appartiennent à l'exposant 1, ceux qui correspondent au signe — appartiennent à l'exposant 2; on observera que le module composé 4 admet

la racine primitive 3 :

Puissances.....	1	3	9	...
Restes.....	1	3	1	...

Pour le module 2, tous les impairs appartiennent à l'exposant 1.