BULLETIN DE LA S. M. F.

L. SANCERY

De la répartition des nombres entre les diviseurs de $\varphi(\mu)$ lorsque μ est une puissance d'un nombre premier impair ou le double d'une telle puissance

Bulletin de la S. M. F., tome 4 (1875-1876), p. 17-29

<http://www.numdam.org/item?id=BSMF_1875-1876__4__17_0>

BULLETIN

DE LA

SOCIÉTÉ MATHÉMATIQUE DE FRANCE.

MÉMOIRES ET COMMUNICATIONS.

De la répartition des nombres entre les diviseurs de $\varphi(M)$, *lorsque* M *est une puissance d'un nombre premier impair, ou le double d'une telle puissance;* par M. L. SANCERY.

(Séance du 21 juillet 1875.)

Il n'y a, ce me semble, aucun auteur qui, traitant des racines primitives, expose la théorie de la répartition des nombres entre les divers diviseurs de $\varphi(M)$, lorsque M est un nombre de la forme p^ν ou $2p^\nu$, p étant un nombre premier impair. Pourtant cette théorie ne relève que d'un théorème unique, théorème simple et fort général, qui comprend, comme cas particulier, tout ce que l'on rencontre dans les ouvrages relativement aux racines primitives selon les modules p^ν ou $2p^\nu$, et même ce théorème-ci, dû à M. Arndt, et inséré au *Journal de Crelle,* t. 31, p. 260, année 1846 : « *Quando g ad exponentem* $p-1$ *pertinet sec. mod. p (quo facto g radix primitiva est), ad unum horum pertinere debet* $p-1$, $(p-1)p$, $(p-1)p^2$, ..., $(p-1)p^{\nu-1}$, *sec. mod.* p^ν. » Or cette répartition des nombres entre les divers diviseurs de $\varphi(M)$ n'est pas sans jeter quelque clarté sur la théorie de l'équation binôme $x^m = a + \mathfrak{M}(M)$, M ayant l'une des trois formes p, p^ν, $2p^\nu$. C'est ainsi que, entre autres choses, elle permet d'arriver aux deux théorèmes suivants, dans les énoncés desquels n représente l'exposant auquel appar-

tient a suivant le module M; Δ le plus grand commun diviseur entre m et $\frac{\varphi(M)}{n}$; Δ_1 le produit des puissances qui se trouvent dans Δ des facteurs premiers communs à Δ et n, en sorte que $\Delta = \Delta_1 \Delta_2$; $1, \delta_2, \delta'_2, \delta''_2, \ldots, \Delta_2$ les diviseurs de Δ_2 et Δ'' un quelconque d'entre eux.

THÉORÈME I. — *L'équation* $x^m = a + \mathfrak{M}(M)$ *possède*

$$\frac{\varphi(n\Delta_1)}{\varphi(n)}, \quad \frac{\varphi(n\Delta_1\delta_2)}{\varphi(n)}, \quad \frac{\varphi(n\Delta_1\delta'_2)}{\varphi(n)}, \quad \ldots, \quad \frac{\varphi(n\Delta_1\Delta_2)}{\varphi(n)}$$

solutions prises respectivement parmi les nombres qui, suivant le module M, *appartiennent aux exposants*

$$n\Delta_1, \quad n\Delta_1\delta_2, \quad n\Delta_1\delta'_2, \quad \ldots, \quad n\Delta_1\Delta_2.$$

Ces différents groupes de racines fournissent le résidu a par des puissances de degrés inférieurs à m et égaux respectivement à

$$\alpha\Delta_1, \quad \alpha\Delta_1\delta_2, \quad \alpha\Delta_1\delta'_2, \quad \ldots, \quad \alpha\Delta_1\Delta_2,$$

α ayant dans chaque cas une valeur particulière qu'on peut obtenir directement par la résolution d'une congruence du premier degré.

THÉORÈME II. — *Quand on connaît un nombre appartenant à l'exposant* $n\Delta_1\Delta''$, *on peut déterminer* $\Delta_1\Delta''$ *solutions de l'équation proposée.*

Abordant la théorie en question, je commencerai par énoncer et démontrer ce théorème :

THÉORÈME. — *Dans la suite des nombres entiers donnés par la formule* $a + px$, *où a est un entier inférieur au nombre premier p, appartenant suivant le module p à l'exposant* θ, *on trouve autant de nombres* A *que l'on veut, tels que* $A^\theta - 1$ *soit divisible par une puissance donnée de p,* p^{t+1}, *et ne le soit pas par la puissance immédiatement supérieure; ces nombres ont pour expression générale*

$$a + pz_1 + p^2 z_2 + p^3 z_3 + \ldots + p^t z_t + p^{t+1}\zeta_{t+1} + p^{t+2}Z,$$

$z_1, z_2, \ldots, z_t, z_{t+1}$ *étant des nombres fixes moindres que p, qui,*

lorsqu'ils ne sont pas nuls, peuvent toujours être déterminés successivement par la résolution de congruences du premier degré, $\zeta_{\iota+1}$ *ayant les* $p-1$ *valeurs différentes de* $z_{\iota+1}$ *prises dans la suite* $0, 1, 2, \ldots, p-1$, *et* Z *étant un nombre entier quelconque.*

Soit $p^{1+\mu}$ la plus haute puissance de p qui divise $a^\theta - 1$. Considérons le nombre $a + p^{1+\lambda}z$, z étant un nombre entier non divisible par p, on aura

$$(a+p^{1+\lambda}z)^\theta - 1 = a^\theta - 1 + \theta a^{\theta-1}p^{1+\lambda}z + \frac{\theta(\theta-1)}{1.2}a^{\theta-2}p^{2+2\lambda}z^2 + \ldots,$$

ou, en posant $a^\theta - 1 = p^{1+\mu}Q$,

$$(1) \qquad (a+p^{1+\lambda}z)^\theta - 1 = p^{1+\mu}Q + \theta a^{\theta-1}p^{1+\lambda}z + \mathfrak{M}p^{2+2\lambda}.$$

Si λ est moindre que μ, tous les termes du second membre étant divisibles par $p^{1+\lambda}$, et le deuxième terme n'admettant pas pour diviseur une puissance de p supérieure à $p^{1+\lambda}$, l'expression $(a+p^{1+\lambda}z)^\theta - 1$ est exactement divisible par $p^{1+\lambda}$ et non par une puissance plus élevée. Il résulte de là que les nombres compris dans les formules

$$a+pz, \quad a+p^2z, \quad a+p^3z, \quad \ldots, \quad a+p^\mu z$$

rendent la fonction $X^\theta - 1$ divisible respectivement par

$$p, \quad p^2, \quad p^3, \quad \ldots, \quad p^\mu,$$

et non par une puissance plus élevée. Comme z est un nombre premier avec p, on peut le représenter par $\zeta + p\mathrm{Z}$, ζ *étant l'un des nombres* $1, 2, 3, \ldots, p-1$, et Z un entier quelconque. Les formules ci-dessus deviennent alors

$$a+p\zeta+p^2\mathrm{Z}, \quad a+p^2\zeta+p^3\mathrm{Z}, \quad a+p^3\zeta+p^4\mathrm{Z}, \quad \ldots, \quad a+p^\mu\zeta+p^{1+\mu}\mathrm{Z}.$$

Si λ est égal à μ, tous les termes du second membre de l'identité (1) sont divisibles par $p^{1+\mu}$, et l'on a

$$(a+p^{1+\mu}z)^\theta - 1 = p^{1+\mu}(\mathrm{Q} + \theta a^{\theta-1}z + \mathfrak{M}p^{1+\mu}).$$

Si le nombre $\mathrm{Q} + \theta a^{\theta-1}z$ n'est pas divisible par p, $p^{1+\mu}$ est la plus haute puissance de p qui divise $(a+p^{1+\mu}z)^\theta - 1$; mais, si ce nombre est divisible par p, il n'en est plus ainsi. Soit donc z_1 la

valeur de z moindre que p qui satisfait à la congruence

$$(2) \qquad Q + \theta a^{\theta-1} z \equiv \mathfrak{M} p,$$

et ζ_1 un quelconque des nombres 0, 1, 2, ..., $p-1$, différent de z_1, les nombres compris dans la formule

$$a + p^{1+\mu}\zeta_1 + p^{2+\mu}Z$$

rendront $X^\theta - 1$ divisible par $p^{1+\mu}$ et non par une puissance plus élevée. Au contraire, la formule

$$a + p^{1+\mu} z_1 + p^{2+\mu} Z$$

donnera des nombres rendant $X^\theta - 1$ divisible par une puissance de p supérieure à $p^{1+\mu}$.

Si λ est supérieur à μ, on pourra écrire l'identité (1)

$$(a + p^{1+\lambda} z)^\theta - 1 = p^{1+\mu}(Q + \theta a^{\theta-1} p^{\lambda-\mu} z + \mathfrak{M} p^{1+\mu}).$$

On voit alors que le premier membre n'admettra pas pour diviseur une puissance de p supérieure à $p^{1+\mu}$; d'ailleurs les nombres $a + p^{1+\lambda} z$ sont actuellement compris parmi ceux qui ont pour expression $a + p^{1+\mu}\zeta_1 + p^{2+\mu}Z$ et correspondent au cas où $\zeta_1 = 0$. L'hypothèse $\lambda > \mu$ ne donne donc rien de particulier.

Considérons actuellement les nombres compris dans la formule

$$a + p^{1+\mu} z_1 + p^{2+\mu+\lambda} z,$$

z_1 étant la valeur fournie par la congruence (2). On aura, en posant $(a + p^{1+\mu} z_1)^\theta - 1 = p^{2+\mu+\mu'} Q'$,

$$(3) \quad \begin{cases} (a + p^{1+\mu} z_1 + p^{2+\mu+\lambda} z)^\theta - 1 \\ \quad = p^{2+\mu+\mu'} Q' + \theta (a + p^{1+\mu} z_1)^{\theta-1} p^{2+\mu+\lambda} z + \mathfrak{M} p^{4+\mu+2\lambda}. \end{cases}$$

Tant que λ sera inférieur à μ', la plus haute puissance de p qui divise le premier membre de cette identité sera égale à $p^{2+\mu+\lambda}$, et par conséquent les nombres compris dans les formules

$$a + p^{1+\mu} z_1 + p^{2+\mu} z, \quad a + p^{1+\mu} z_1 + p^{3+\mu} z, \quad \ldots, \quad a + p^{1+\mu} z_1 + p^{1+2\mu+\mu'} z,$$

ou bien dans celles-ci, obtenues en remplaçant, comme plus haut,

z par $\zeta + pZ$,

$$a + p^{1+\mu} z_1 + p^{2+\mu}\zeta + p^{3+\mu} Z,$$
$$a + p^{1+\mu} z_1 + p^{3+\mu}\zeta + p^{4+\mu} Z,$$
$$\dots\dots\dots\dots\dots\dots\dots,$$
$$a + p^{1+\mu} z_1 + p^{1+\mu+\mu'}\zeta + p^{2+\mu+\mu'} Z,$$

rendront la fonction $X^\theta - 1$ respectivement divisible par

$$p^{2+\mu}, \quad p^{3+\mu}, \quad \dots, \quad p^{1+\mu+\mu'}.$$

Si λ est égal à μ', l'identité (3) peut s'écrire

$$(a + p^{1+\mu} z_1 + p^{2+\mu+\mu'} z)^\theta - 1$$
$$= p^{2+\mu+\mu'} [Q' + \theta (a + p^{1+\mu} z_1)^{\theta-1} z + \mathfrak{M} p^{2+\mu+\mu'}].$$

Alors on voit que la plus haute puissance de p qui divise le premier membre est égale à $p^{2+\mu+\mu'}$ lorsque $Q' + \theta (a + p^{1+\mu} z_1)^{\theta-1} z$ n'est pas divisible par p, mais que, quand p divise cette quantité, le premier membre admet pour diviseur une puissance de p supérieure à $p^{2+\mu+\mu'}$. Soit donc z_2 la valeur de z moindre que p qui satisfait à la congruence

$$Q' + \theta (a + p^{1+\mu} z_1)^{\theta-1} z \equiv \mathfrak{M} p, \tag{4}$$

et ζ_2 un quelconque des nombres $0, 1, 2, \dots, p-1$ différent de z_2, les nombres compris dans la formule

$$a + p^{1+\mu} z_1 + p^{2+\mu+\mu'} \zeta_2 + p^{3+\mu+\mu'} Z$$

rendront $X^\theta - 1$ divisible par $p^{2+\mu+\mu'}$ et non par une puissance plus élevée. Au contraire, la formule

$$a + p^{1+\mu} z_1 + p^{2+\mu+\mu'} z_2 + p^{3+\mu+\mu'} Z$$

donnera des nombres rendant $X^\theta - 1$ divisible par une puissance de p supérieure à $p^{2+\mu+\mu'}$.

Si λ est supérieur à μ', l'identité (3) devient

$$(a + p^{1+\mu} z_1 + p^{2+\mu+\lambda} z)^\theta - 1$$
$$= p^{2+\mu+\mu'} [Q' + \theta (a + p^{1+\mu} z_1)^{\theta-1} z^{\lambda-\mu'} + \mathfrak{M} p^{2+\mu+\mu'}];$$

la plus haute puissance de p qui divise le premier membre est donc égale à $p^{2+\mu+\mu'}$; d'ailleurs les nombres $a + p^{1+\mu} z_1 + p^{3+\mu+\lambda} z$

sont actuellement compris parmi ceux qui ont pour expression $a + p^{1+\mu} z_1 + p^{2+\mu+\mu'} \zeta_2 + p^{3+\mu+\mu'} Z$ et correspondent au cas où $\zeta_2 = 0$; l'hypothèse $\lambda > \mu'$ n'apprend donc rien de nouveau.

On pourrait considérer de même les nombres compris dans la formule

$$a + p^{1+\mu} z_1 + p^{2+\mu+\mu'} z_2 + p^{3+\mu+\mu'+\lambda} z,$$

et refaire les raisonnements précédents. Ces raisonnements peuvent donc être reproduits indéfiniment; par conséquent on peut trouver parmi les valeurs de $a + px$ autant de nombres que l'on voudra, rendant la fonction $X^0 - 1$ divisible par une puissance quelconque de p, $p^{\varepsilon+1}$, et non par la suivante, et obtenir l'expression générale de ces nombres par la résolution de congruences du premier degré.

Si l'on suppose $\mu = \mu' = \ldots = 0$, on trouve que les nombres rendant la fonction $X^0 - 1$ uniquement divisible par p sont donnés par la formule

$$a + p\zeta_1 + p^2 Z,$$

que ceux qui rendent $X^0 - 1$ divisible par p^2 et non par p^3 sont compris dans la formule

$$a + pz_1 + p^2 \zeta_2 + p^3 Z,$$

et qu'en général les nombres rendant $X^0 - 1$ divisible par $p^{1+\varepsilon}$ et non par $p^{2+\varepsilon}$ ont pour expression

$$a + pz_1 + p^2 z_2 + p^3 z_3 + \ldots + p^\varepsilon z_\varepsilon + p^{\varepsilon+1} \zeta_{\varepsilon+1} + p^{\varepsilon+2} Z,$$

$z_1, z_2, z_3, \ldots, z_\varepsilon, z_{\varepsilon+1}$ étant des nombres fixes moindres que p, que l'on peut toujours déterminer successivement par la résolution de congruences du premier degré à une inconnue, $\zeta_{\varepsilon+1}$ ayant les $p - 1$ valeurs différentes de $z_{\varepsilon+1}$ prises dans la suite $0, 1, 2, \ldots, p-1$, et Z étant un nombre entier quelconque. La formule de tous les nombres rendant $X^0 - 1$ divisible par $p^{\varepsilon+1}$ est

$$a + pz_1 + p^2 z_2 + \ldots + p^\varepsilon z_\varepsilon + p^{\varepsilon+1} Z.$$

Il est à remarquer que les deux expressions précédentes renferment comme cas particuliers toutes celles que nous avons antérieurement établies, pourvu, ce qui n'avait pas lieu précédemment,

qu'on admette que z_1, z_2, ..., $z_{\varepsilon+1}$ puissent être des quantités nulles.

Applications. — I. Le nombre 1 appartient à l'exposant 1, et la fonction $X^0 - 1$, devenant nulle pour $X = 1$, $\theta = 1$, est divisible par une puissance quelconque de p; le nombre μ peut donc être regardé comme infini, et par suite

$$1 + p\zeta + p^2 Z, \quad 1 + p^2\zeta + p^3 Z, \quad 1 + p^3\zeta + p^4 Z, \quad \ldots,$$

représentent les nombres qui, appartenant à l'exposant 1, rendent $X - 1$ divisible respectivement par p, p^2, p^3, ..., et non par les puissances immédiatement supérieures.

II. Le nombre $p - 1$ appartient à l'exposant 2 suivant le module p, car $(p-1)^2 - 1 = p(p-2)$; de plus il est le seul nombre moindre que p qui appartienne à cet exposant. On peut donc obtenir immédiatement les formules des nombres qui, appartenant à l'exposant 2, rendent la fonction $X^2 - 1$ uniquement divisible par p, p^2, p^3, ... Ainsi les nombres $-1 + p\zeta + p^2 Z$ rendent $X^2 - 1$ divisible par p et non par p^2, et les nombres $-1 + p^2\zeta + p^3 Z$ rendent $X^2 - 1$ divisible par p^2 et non par p^3, ...

Je vais montrer maintenant que, lorsqu'on prend pour module une puissance p^ν d'un nombre premier p, la suite des nombres premiers avec le module peut être distribuée en autant de classes qu'il y a de diviseurs pour $\varphi(p^\nu)$, les nombres d'une classe appartenant à un même exposant diviseur de $\varphi(p^\nu)$.

Théorème fondamental. — *Un nombre* A *appartenant à l'exposant* θ, *suivant le module premier impair* p, *appartient, suivant le module* p^ν, *à l'exposant* θ, *si la plus haute puissance de* p *qui divise* $A^\theta - 1$ *est égale ou supérieure à* p^ν, *et, lorsque cette plus haute puissance est inférieure à* p^ν, *en la désignant par* p^μ, *le nombre* A *appartient à l'exposant* $\theta p^{\nu-\mu}$.

I. Soit a un des nombres moindres que p appartenant à l'exposant θ, suivant le module p, tous les nombres congrus à a donnés par la formule $A = a + px$ appartiennent au même exposant et satisfont à la relation $A^\theta = (a + px)^\theta = 1 + \mathfrak{M}p$. De plus, les puissances de A ayant pour exposant un multiple de θ sont les seules qui, divisées par p, donnent le résidu 1. Si maintenant, suivant le module p^ν, le nombre A appartient à l'exposant t, on aura

$A^t = 1 + \mathfrak{M} p^\nu$, et, par conséquent, aussi $A^t = 1 + \mathfrak{M} p$; d'où il suit que t est égal à θ ou à un de ses multiples.

II. Désignons par p^μ la plus haute puissance de p, qui divise $A^\theta - 1$, en sorte que $A^\theta - 1 = Q p^\mu$, Q n'étant pas divisible par p.

1° Soit $\mu \geq \nu$. Il est clair que A appartient à l'exposant θ suivant le module p^ν, puisque A^θ, divisé par p^ν, donne le résidu 1, et que toute puissance de A, d'un degré inférieur à θ, diminuée d'une unité, n'étant pas divisible par p, ne peut l'être par p^ν. Ainsi la première partie du théorème se trouve démontrée.

2° Soit $\mu < \nu$. Si l'on élève les deux membres de l'égalité $A^\theta = 1 + Q p^\mu$ à la puissance λ, il vient

$$A^{\theta\lambda} = (1 + Q p^\mu)^\lambda = 1 + \lambda Q p^\mu + \frac{\lambda(\lambda-1)}{1.2} Q^2 p^{2\mu} + \frac{\lambda(\lambda-1)(\lambda-2)}{1.2.3} Q^3 p^{3\mu} + \ldots,$$

d'où

$$A^{\theta\lambda} - 1 = p^\mu (\lambda Q + \mathfrak{M} p^\mu).$$

Par là on voit que, si λ ne renferme en facteur aucune puissance de p, la quantité $A^{\theta\lambda} - 1$ ne peut être divisible par une puissance de p supérieure à la $\mu^{\text{ième}}$. Donc $A^{\theta\lambda} - 1$ ne sera divisible par p^ν que si $\lambda = \lambda_1 p^\rho$, λ_1 étant premier avec p. Si l'on remplace λ par cette valeur, le développement précédent devient

$$A^{\theta\lambda_1 p^\rho} = 1 + \lambda_1 p^\rho Q p^\mu + \frac{\lambda_1 p^\rho (\lambda_1 p^\rho - 1)}{1.2} Q^2 p^{2\mu} + \frac{\lambda_1 p^\rho (\lambda_1 p^\rho - 1)(\lambda_1 p^\rho - 2)}{1.2.3} Q^3 p^{3\mu} + \ldots.$$

Or on peut reconnaître que tous les termes, à partir du troisième inclusivement, sont divisibles par $p^{\rho+2\mu}$. Prenons, en effet, l'un de ces termes

$$\frac{\lambda_1 p^\rho (\lambda_1 p^\rho - 1)(\lambda_1 p^\rho - 2) \ldots (\lambda_1 p^\rho - h + 1)}{1.2.3 \ldots h} Q^h p^{h\mu},$$

et écrivons-le comme il suit :

$$p^\rho \lambda_1 \frac{(\lambda_1 p^\rho - 1)(\lambda_1 p^\rho - 2) \ldots (\lambda_1 p^\rho - h + 1)}{1.2 \ldots (h-1)} \frac{1}{h} Q^h p^{h\mu}.$$

L'expression

$$\frac{(\lambda_1 p^\rho - 1)(\lambda_1 p^\rho - 2) \ldots (\lambda_1 p^\rho - h + 1)}{1.2 \ldots (h-1)} = F,$$

dont les deux termes renferment le même nombre de facteurs formés de nombres entiers consécutifs, se réduit, comme on le sait, à un nombre entier. Il suit de là, puisque les coefficients binomiaux sont aussi entiers, que, lorsque h est premier avec p, $\frac{\lambda_1 F}{h}$ doit être un nombre entier. Le terme considéré est donc divisible par $p^{\rho+h\mu}$, et, par conséquent, par $p^{\rho+2\mu}$, puisque $h \geq 2$.

Lorsque h n'est pas premier avec p, mais est égal à $h_1 p^s$, on ne voit pas aussi aisément que le terme considéré soit divisible par $p^{\rho+2\mu}$; mais, si on l'écrit de la manière suivante :

$$p^{\rho}\lambda_1 \frac{(\lambda_1 p^{\rho}-1)(\lambda_1 p^{\rho}-2)\ldots(\lambda_1 p^{\rho}-h+1)}{1.2\ldots(h-1)} \frac{1}{h_1} Q^h \frac{p^{h_1 p^s \mu}}{p^s},$$

on reconnaît encore, h_1 étant premier avec p, que

$$\lambda_1 \frac{(\lambda_1 p^{\rho}-1)(\lambda_1 p^{\rho}-2)\ldots(\lambda_1 p^{\rho}-h+1)}{1.2\ldots(h-1)} \frac{1}{h_1}$$

est un nombre entier. Par conséquent, pour que ce terme soit divisible par $p^{\rho+2\mu}$, il suffit que

$$\frac{p^{h_1 p^s \mu - 2\mu}}{p^s}$$

soit entier. Or il en sera toujours ainsi, si la condition

$$\mu(h_1 p^s - 2) \geq s$$

est d'elle-même vérifiée. On voit immédiatement, p étant un nombre premier impair et s un entier quelconque, que la condition

$$p^s - 2 \geq s,$$

qui revient à $\log p \geq \frac{\log(s+2)}{s+2} \frac{s+2}{s}$, est satisfaite. En effet, les deux rapports

$$\frac{\log(s+2)}{s+2}, \quad \frac{s+2}{s}$$

diminuent quand s augmente, et sont moindres que $\frac{\log(1+2)}{1+2}$, $\frac{1+2}{1}$; donc $\frac{\log(s+2)}{s}$ est égal ou inférieur à $\log 3$; d'ailleurs $\log p$

est égal ou supérieur à log3 : donc la condition

$$p^s - 2 \geq s$$

est toujours vérifiée. On en déduit successivement

$$h_1 p^s - 2 \geq s, \quad \mu(h_1 p^s - 2) \geq s,$$

et ce dernier résultat constitue justement l'inégalité qu'il importait d'établir; par conséquent, tous les termes du développement ci-dessus sont, à partir du troisième inclusivement, divisibles par $p^{\rho+2\mu}$. Il en résulte que l'on a

$$A^{\theta\lambda_1 p^\rho} - 1 = p^{\rho+\mu}(\lambda_1 Q + \mathfrak{M} p^\mu);$$

cette égalité montre que $A^{\theta\lambda_1 p^\rho} - 1$ n'est divisible par p^ν que sous la condition

$$\rho + \mu \geq \nu.$$

Par conséquent, en prenant $\lambda_1 = 1$, $\rho + \mu = \nu$ ou $\rho = \nu - \mu$, on aura dans $\theta p^{\nu-\mu}$ l'exposant de la plus petite puissance de A qui, divisée par p^ν, donne le résidu 1, et A appartient à l'exposant $\theta p^{\nu-\mu}$. La seconde partie du théorème est donc démontrée.

Corollaire I. — *Les nombres fournis par la formule* $a + px$, *a étant moindre que p et appartenant à l'exposant* θ *suivant le module p, appartiennent, suivant le module* p^ν, *aux divers exposants*

$$\theta, \quad \theta p, \quad \theta p^2, \quad \ldots, \quad \theta p^{\nu-1}.$$

Un nombre appartient

à l'exposant	θ	*lorsque*	$\mu \geq \nu$,
»	θp	»	$\mu = \nu - 1$,
»	θp^2	»	$\mu = \nu - 2$,
»	.. ,		.....,
»	$\theta p^{\nu-1}$	»	$\mu = \nu - (\nu - 1) = 1$.

Réciproquement,

Si un nombre appartient, suivant le module p^ν, *à un exposant* θp^i, *i n'étant pas nul, ce nombre rend la fonction* $X^\theta - 1$ *divisible par* $p^{\nu-i}$, *et non par une puissance plus élevée.*

COROLLAIRE II. — *Puisque un diviseur quelconque de* $\varphi(p^\nu)$ *est de la forme* θp^σ, θ *étant l'un des diviseurs de* $p-1$, *l'unité et* $p-1$ *compris, et* σ *pouvant prendre toutes les valeurs depuis zéro jusqu'à* $\nu-1$ *inclusivement, il existe des nombres appartenant à un diviseur quelconque de* $\varphi(p^\nu)$ *pris pour exposant.*

COROLLAIRE III. — *Un nombre* A *appartient à l'exposant* $p^{\nu-1}(p-1)$, *c'est-à-dire est racine primitive pour le module* p^ν, *quand il est racine primitive pour le module* p, *et qu'en outre* $A^{p-1}-1$ *n'est divisible que par la première puissance de* p.

COROLLAIRE IV. — *On peut, en se servant de la formule donnée par le premier théorème, répartir entre les diviseurs* $\theta, \theta p, \theta p^2, \ldots, \theta p^{\nu-1}$ *les nombres appartenant, suivant le module* p, *à l'exposant* θ.

En effet, cette formule, donnant les nombres qui rendent $X^\theta - 1$ divisible par $p^{\varepsilon+1}$ et non par $p^{\varepsilon+2}$, fournit par cela même les nombres appartenant à l'exposant $\theta p^{\nu-\varepsilon-1}$; mais, pour opérer la répartition, il sera plus simple dans la pratique de procéder par exclusion. Il faudra prendre les nombres $a, b, c, \ldots$, moindres que p, appartenant à l'exposant θ pour le module p, former les suites des nombres moindres que p^ν qui leur sont congrus suivant le même module, puis chercher pour chaque suite les nombres qui rendent la fonction $X^\theta - 1$ divisible par p^2 et les supprimer : tous les nombres restants appartiendront à l'exposant $\theta p^{\nu-1}$; chercher dans les suites des nombres rendant $X^\theta - 1$ divisible par p^2 ceux pour lesquels cette fonction est divisible par p^3, et les supprimer : tous les nombres restants appartiendront à l'exposant $\theta p^{\nu-2}$, et ainsi de suite.

Remarque I. — On peut reconnaître que ce corollaire renferme comme cas particulier la proposition donnée par M. Lebesgue dans le *Journal de Liouville,* 1re série, t. XIX, p. 334, année 1854.

Remarque II. — Les applications ci-dessus I et II donnent les nombres appartenant aux exposants

$$1, \quad p, \quad p^2, \quad \ldots, \quad p^{\nu-1};$$
$$2, \quad 2p, \quad 2p^2, \quad \ldots, \quad 2p^{\nu-1}.$$

COROLLAIRE V. — *Il existe, suivant le module* p^ν, $\varphi(\theta p^{\nu-i})$ *nombres appartenant à l'exposant* $\theta p^{\nu-i}$.

En effet, les nombres appartenant à l'exposant $\theta p^{\nu-t}$ sont fournis par la formule

$$a + pz_1 + p^2 z_2 + \ldots + p^{i-1} z_{i-1} + p^i \zeta_i + p^{i+1} Z ;$$

or, pour une valeur donnée de a et une de ζ_i, cette expression fournit $p^{\nu-i-1}$ valeurs moindres que p^ν, puisque Z peut prendre les valeurs 0, 1, 2, ..., $p^{i+1} - 1$; par conséquent, en tenant compte des $\varphi(\theta)$ valeurs de a et des $p-1$ valeurs de ζ_i, l'expression précédente donne $\varphi(\theta)(p-1)p^{\nu-i-1}$ valeurs moindres que p^ν appartenant à l'exposant $\theta p^{\nu-i}$; mais $\varphi(\theta)(p-1)p^{\nu-i-1} = \varphi(\theta p^{\nu-i})$: la proposition est donc établie.

En particulier, il existe $\varphi[(p-1)p^{\nu-1}]$ ou $\varphi.\varphi(p^\nu)$ nombres appartenant à l'exposant $(p-1)p^{\nu-1}$, c'est-à-dire $\varphi.\varphi(p^\nu)$ racines primitives pour le module p^ν.

On passe des résultats obtenus pour le module p^ν à ceux qui sont propres au module $2p^\nu$ à l'aide du théorème suivant :

Théorème. — *Tout nombre impair qui appartient, selon le module p^ν, à l'exposant θ_1, appartient au même exposant suivant le module $2p^\nu$.*

Nous observerons d'abord que les nombres premiers avec le module $2p^\nu$ se trouvent dans la suite des nombres impairs, puisque l'égalité $\varphi(2p^\nu) = \varphi(p^\nu)$ montre que les diviseurs de $\varphi(p^\nu)$ sont ceux de $\varphi(2p^\nu)$. Cela posé, soit A un nombre impair appartenant à l'exposant θ_1, suivant le module p^ν, on aura $A^{\theta_1} - 1 = \mathfrak{M} p^\nu$, et, puisque $A^{\theta_1} - 1$ est pair, on a aussi $A^{\theta_1} - 1 = \mathfrak{M} 2p^\nu$. Ainsi A ne peut, suivant le module $2p^\nu$, appartenir à un exposant supérieur à θ_1. Si maintenant, suivant le module $2p^\nu$, A appartenait à un exposant θ'_1, moindre que θ_1, on aurait $A^{\theta'_1} - 1 = \mathfrak{M} 2p^\nu$, et par conséquent $A^{\theta'_1} - 1 = \mathfrak{M} p^\nu$, ce qui n'est pas. Le nombre A appartient donc au même exposant selon les deux modules.

Corollaire I. — *Il existe des nombres appartenant, suivant le module $2p^\nu$, à tous les diviseurs de $\varphi(2p^\nu)$.*

Corollaire II. — *La totalité des nombres appartenant, suivant le module $2p^\nu$, à l'exposant $\theta p^{\nu-i}$, est égale à $\varphi(2\theta p^{\nu-i})$.*

En effet, si l'on veut avoir la totalité des nombres impairs moindres que $2p^\nu$, appartenant à l'exposant $\theta p^{\nu-i}$, il suffit d'observer que, si a, b, c, ... sont des nombres moindres que p^ν appartenant à

l'exposant $\theta p^{\nu-i}$, suivant le module p^ν, les nombres appartenant au même exposant et moindres que $2p^\nu$ sont

$$a, \quad b, \quad c, \quad \ldots, \quad a+p^\nu, \quad b+p^\nu, \quad c+p^\nu, \quad \ldots.$$

Or, p^ν étant impair, les deux nombres a, $a+p^\nu$ sont de parités différentes; par conséquent il n'y en a qu'un des deux qui appartienne, selon le module $2p^\nu$, à l'exposant $\varphi(\theta p^{\nu-i})$; la suite précédente offre donc autant de nombres appartenant à l'exposant $\theta p^{\nu-i}$, pour le module $2p^\nu$, qu'il y en a dans la première suite $a, b, c, \ldots$, c'est-à-dire $\varphi(\theta p^{\nu-i})$, ou bien $\varphi(2\theta p^{\nu-i})$. En particulier, il existe $\varphi.\ \varphi(2p^\nu)$ racines primitives pour le module $2p^\nu$.