BULLETIN DE LA S. M. F.

V. MYLLER-LEBEDEFF

Sur un théorème de Gauss-Arndt relatif aux congruences binômes

Bulletin de la S. M. F., tome 50 (1922), p. 148-153

<http://www.numdam.org/item?id=BSMF_1922__50__148_0>

SUR UN THÉORÈME DE GAUSS-ARNDT RELATIF AUX CONGRUENCES BINOMES;

PAR VERA MYLLER-LEBEDEFF.

On sait que la congruence binome

$$z^{\delta} \equiv 1 \qquad (\text{mod } n, \text{ ou } n = p^{\alpha} \text{ ou } 2p^{\alpha})$$

(p un nombre premier $\neq 2$), où l'on peut toujours supposer δ diviseur de $\varphi(n)$, a exactement δ racines dont $\varphi(\delta)$ appartiennent à l'exposant δ.

Gauss a démontré (*Disqu. Arithm.*, art. 81) que la somme des racines primitives de p, c'est-à-dire des nombres appartenant à l'exposant $\varphi(p)$ est $\equiv 0 \pmod p$, si $p-1$ est divisible par un carré, ou $\equiv \pm 1 \pmod p$, si $p-1$ est le produit de facteurs premiers inégaux. Arndt a généralisé ce résultat (*Journal de Crelle*, t. 31, p. 326) de la façon suivante : « La somme des nombres appartenant au même exposant $\delta \pmod p$ est $\equiv 0 \pmod p$, si δ est divisible par un carré, et $\equiv \pm 1 \pmod p$, si δ n'est divisible par aucun carré. »

Bachmann (*Niedere Zahlentheorie*, t. I, p. 333) a cru que l'on puisse énoncer le théorème d'Arndt de la même façon pour le module p^{α}, $2p^{\alpha}$, δ étant un diviseur quelconque de

$$\varphi(p^{\alpha}) = \varphi(2p^{\alpha}) = p^{\alpha-1}(p-1).$$

Ensuite il a observé pourtant (*voir* le même Volume, p. 402, Zusätze) que le théorème n'est vrai que si δ est diviseur de $p-1$; en particulier, il ne peut pas être appliqué aux racines primitives de p^{α}, $2p^{\alpha}$, le cas de Gauss excepté.

On peut cependant généraliser le théorème de Gauss-Arndt pour le module p^{α}, $2p^{\alpha}$, et nous nous proposons de le faire dans ce qui suit. Le résultat est le suivant :

Soit

$$\delta = p^{k} q_1^{m} q_2^{n} \dots q_i^{t}$$

un diviseur de

$$\varphi(p^{\alpha}) = \varphi(2p^{\alpha}) = p^{\alpha-1}(p-1) = p^{\alpha-1} q_1^{\beta} q_2^{\gamma} \dots q_i^{\varepsilon} q_{i+1}^{\sigma} \dots q_r^{\tau}.$$

La somme des nombres appartenant à l'exposant δ *est*

$$\equiv 0 \qquad (\mathrm{mod}\, p^\alpha \text{ ou } 2p^\alpha)$$

si $\delta : p^k$ *est divisible par un carré et*

$$\equiv (-1)^i \varphi(p^k) \quad (\mathrm{mod}\, p^\alpha), \qquad \text{resp.} \equiv (p^\alpha - 1)^i \varphi(p^k) \quad (\mathrm{mod}\, 2p^\alpha),$$

si $\delta : p^k$ *est le produit de facteurs premiers inégaux. Pour* $k = 0$, *il est à poser* $\varphi(1) = 1$. *En particulier, la somme des racines primitives de* p^α, $2p^\alpha$ *est*

$$\equiv 0$$

si $p - 1$ *est divisible par un carré et*

$$\equiv (-1)^r \varphi(p^{\alpha-1}) \quad (\mathrm{mod}\, p^\alpha), \qquad \text{resp.} \equiv (p^\alpha - 1)^r \varphi(p^{\alpha-1}) \quad (\mathrm{mod}\, 2p^\alpha),$$

si $p - 1$ *ne l'est pas.*

Démonstration. — Soit g une racine primitive de p^α, $2p^\alpha$; pour $2p^\alpha$, on doit toujours supposer g impair. On a le théorème connu : g^h appartient à l'exposant

$$\delta = \varphi(p^\alpha) : d \qquad (\mathrm{mod}\, p^\alpha \text{ ou } 2p^\alpha),$$

alors, et seulement alors, quand d est le plus grand commun diviseur de h et $\varphi(p^\alpha)$. Par conséquent,

$$g^{x_i \mathrm{M}_i}, \qquad \text{où} \qquad \mathrm{M}_i = p^{\alpha-1} \frac{p-1}{q_i^t},$$

et x_i parcourt les $\varphi(q_i^t)$ nombres premiers avec q_i, et $< q_i^t$ représente tous les $\varphi(q_i^t)$ nombres appartenant à l'exposant q_i^t. Notons que

$$g^{\mathrm{M}_i} - 1 \not\equiv 0 \qquad (\mathrm{mod}\, p),$$

car M_i n'est pas divisible par $p - 1$. De même

$$g^{y_i \mathrm{N}}, \qquad \text{où} \qquad \mathrm{N} = p^{\alpha-1-k}(p-1)$$

et y_i sont les $\varphi(p^k)$ nombres premiers avec p, et $< p^k$ donne tous les nombres appartenant à p^k.

Un nombre appartenant à δ peut être représenté par le produit de nombres appartenant respectivement aux facteurs de δ premiers entre eux. Ce théorème, connu pour le module p, est encore vrai

pour le module p^α, $2p^\alpha$. En effet, l'exposant h d'un tel produit,

$$g^{x_1 M_1 + x_2 M_2 + \ldots x_i M_i + y_i N} = g^h,$$

a le plus grand commun diviseur avec $\varphi(p^\alpha)$ égal à

$$p^{\alpha-1-k} q_1^{\beta-m} q_2^{\gamma-n} \ldots q_i^{\varepsilon-t} q_{i+1}^{\sigma} \ldots q_r^{\tau};$$

donc g^h appartient bien à l'exposant δ.

Il s'ensuit que, désignant par S la somme cherchée des nombres appartenant à δ, et par $P_1, P_2, \ldots, R$ les sommes des nombres appartenant respectivement à $q_1^m, q_2^n, \ldots, p^k$, on a

$$S \equiv P_1 P_2 \ldots R \qquad (\mathrm{mod}\, p^\alpha \text{ ou } 2p^\alpha).$$

Soit d'abord $m > 1$. Les $\varphi(q_1^m)$ nombres x_1 se partagent en systèmes de q_1 nombres

$$\begin{aligned} &x_1,\ x_1 + \frac{\delta}{q_1},\ x_1 + \frac{2\delta}{q_1},\ \ldots,\ x_1 + \frac{(q_1-1)\delta}{q_1}, \\ &x'_1,\ x'_1 + \frac{\delta}{q_1},\ x'_1 + \frac{2\delta}{q_1},\ \ldots,\ x'_1 + \frac{(q_1-1)\delta}{q_1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned}$$

et la somme des nombres provenant de chaque système est $\equiv 0$. En effet,

$$g^{x_1 M_1} + g^{\left(x_1 + \frac{\delta}{q_1}\right) M_1} + \ldots + g^{\left(x_1 + \frac{(q_1-1)\delta}{q_1}\right) M_1} = g^{x_1 M_1} \frac{g^{\delta M_1} - 1}{g^{\frac{\delta}{q_1} M_1} - 1}.$$

Mais $\delta M_1 : q_1$ n'est pas divisible par $p - 1$, tandis que δM_1 est divisible par $p^{\alpha-1}(p-1)$; donc

$$g^{\delta M_1} - 1 \equiv 0 \qquad (\mathrm{mod}\, p^\alpha \text{ ou } 2p^\alpha),$$

tandis que

$$g^{\frac{\delta}{q_1} M_1} - 1 \not\equiv 0 \qquad (\mathrm{mod}\, p).$$

Ainsi

$$P_1 \equiv 0 \qquad (\mathrm{mod}\, p^\alpha \text{ ou } 2p^\alpha);$$

donc

$$S \equiv 0 \qquad (\mathrm{mod}\, p^\alpha \text{ ou } 2p^\alpha). \qquad \text{C. Q. F. I}$$

Supposons en second lieu $m = 1, n = 1, \ldots, t = 1$. On a

$$P_1 = g^{M_1} + g^{2M_1} + \ldots + g^{(q_1-1)M_1} = \frac{g^{q_1 M_1} - 1 - (g^{M_1} - 1)}{g^{M_1} - 1} \equiv -1 \qquad (\mathrm{mod}\, p^\alpha),$$

car

$$g^{q_1 M_1} - 1 = g^{\delta} - 1 = M p^{\alpha} \qquad \text{et} \qquad g^{M_1} - 1 \not\equiv 0 \pmod{p}.$$

Dans le cas du module $2p^{\alpha}$, on voit que P_1 est pair; donc

$$P_1 = (2M + 1) p^{\alpha} - 1$$

ou

$$P_1 \equiv p^{\alpha} - 1 \pmod{2p^{\alpha}}.$$

Il reste à calculer la somme R des nombres appartenant à p^k $(0 < k \leq \alpha - 1)$. Pour cela on pourrait encore employer la représentation par les puissances d'une racine primitive; mais on arrive plus simplement au résultat en développant les nombres appartenant à l'exposant $p^k \pmod{p^{\alpha}}$, d'après les puissances de p (¹).

Observons d'abord qu'un nombre appartenant à $p^k \pmod{p^{\alpha}}$ appartient aux exposants p^{k-1}, p^{k-2}, ..., 1 par rapport aux modules $p^{\alpha-1}$, $p^{\alpha-2}$, ..., $p^{\alpha-k}$. On le voit tout de suite en représentant ce nombre sous la forme $g^{y_i N}$, $N = p^{\alpha-1-k}(p-1)$ de ci-dessus. Ce nombre (nommons-le m_k) doit donc être de la forme

$$m_k = 1 + M p^{\alpha-k}, \qquad \text{où} \qquad M \not\equiv 0 \pmod{p},$$

car autrement m_k appartiendrait à 1 et non à $p \pmod{p^{\alpha-k+1}}$. Si M satisfait cette condition, m_k appartient bien à $p^k \pmod{p^{\alpha}}$.

Démontrons-le par l'induction. D'abord on voit que m_k appartient à $p \pmod{p^{\alpha-k+1}}$; en effet, si t était l'exposant de $m_k \pmod{p^{\alpha-k+1}}$, on aurait

$$m_k^t \equiv 1 \pmod{p^{\alpha-k+1}}$$

ou

$$(1 + M p^{\alpha-k})^t = 1 + M t p^{\alpha-k} + M' p^{\alpha-k+1} \equiv 1 \pmod{p^{\alpha-k+1}};$$

donc $Mt \equiv 0 \pmod{p}$ et, par suite, $t = p$.

Supposons maintenant que m_k appartient à $p^{n-1} \pmod{p^{\alpha-k+n-1}}$, et soit t l'exposant de m_k par rapport au mod $p^{\alpha-k+n}$

$$m_k^t \equiv 1 \pmod{p^{\alpha-k+n}},$$

donc

$$\equiv 1 \pmod{p^{\alpha-k+n-1}} \qquad \text{et} \qquad t = p^{n-1} t_1.$$

Mais, d'après un théorème de Gauss (*Disqu. Arithm.*, art. 86),

(¹) Pour cette méthode, *voir* aussi M. FONTENÉ, *Sur les modules de la forme* p^m (*Nouvelles Annales*, 4ᵉ série, t. VIII, p. 193).

si t est divisible par p^{n-1} et non par p^n, on a

$$(1 + \mathrm{M} p^{\alpha-k})^t - 1 \equiv \mathrm{M} t p^{\alpha-k} \pmod{p^{\alpha-k+n}};$$

donc $\mathrm{M} t p^{\alpha-k}$ est divisible par $p^{\alpha-k+n}$ et $t = p^n$. C. Q. F. D.

m_k est donc de la forme

$$m_k = 1 + i_1 p^{\alpha-k} + i_2 p^{\alpha-k+1} + \ldots + i_k p^{\alpha-1},$$

où i_1 peut prendre les valeurs $1, 2, \ldots, p-1$ et $i_2, \ldots, i_k$ les valeurs $0, 1, 2, \ldots, p-1$. Tous ces nombres sont incongrus entre eux $(\mathrm{mod}\, p^\alpha)$, car en posant

$$m'_k = 1 + i'_1 p^{\alpha-k} + i'_2 p^{\alpha-k+1} + \ldots + i'_k p^{\alpha-1},$$

on tirerait de la congruence

$$m_k - m'_k \equiv 0 \pmod{p^\alpha}$$

ou

$$i_1 - i'_1 + (i_2 - i'_2) p + \ldots + (i_k - i'_k) p^{k-1} \equiv 0 \pmod{p^k},$$

que les différences $i_1 - i'_1$, $i_2 - i'_2$, $\ldots$, $i_k - i'_k$ sont nulles à la fois.

Nous avons donc à calculer

$$\mathrm{R} = \sum_{i_1, i_2, \ldots, i_k} m_k,$$

où $i_1, i_2, \ldots, i_k$ varient dans les limites indiquées. Employons encore l'induction. Désignons par $m_1, m_2, \ldots$ les nombres appartenant à $p, p^2, \ldots (\mathrm{mod}\, p^{\alpha-k+1}, p^{\alpha-k+2}, \ldots)$. On a

$$\sum m_1 = \sum_{i_1=1}^{p-1} (1 + i_1 p^{\alpha-k}) = p - 1 + p^{\alpha-k}(1 + 2 + \ldots + p - 1) \equiv p - 1 \pmod{p^{\alpha-k+1}}$$

et

$$\sum m_2 = \sum_{i_1} \sum_{i_2=0}^{p-1} (m_1 + i_2 p^{\alpha-k+1}) = \sum_{i_1} p m_1 + \mathrm{M} p^{\alpha-k+2} \equiv p(p-1) \pmod{p^{\alpha-k+2}}.$$

Supposons que

$$\sum_{i_1, \ldots, i_{k-1}} m_{k-1} \equiv p^{k-2}(p-1) \pmod{p^{\alpha-1}}.$$

Il s'ensuivra

$$R = \sum m_k = \sum_{i_1, \ldots, i_{k-1}} \sum_{i_k=0}^{p-1} (m_{k-1} + i_k p^{\alpha-1}) = \sum p m_{k-1} + M p^{\alpha},$$

$$R \equiv p^{k-1}(p-1) \equiv \varphi(p^k) \pmod{p^{\alpha}}. \qquad \text{C. Q. F. D.}$$

D'ailleurs, on a aussi

$$R \equiv \varphi(p^k) \pmod{2p^{\alpha}},$$

parce qu'on doit supposer les $\varphi(p^k)$ nombres appartenant à $p^k \pmod{2p^{\alpha}}$ impairs; donc R est pair.

Maintenant les congruences

$$S \equiv P_1 P_2 \ldots P_i R \pmod{p^{\alpha} \text{ ou } 2p^{\alpha}},$$
$$P_1 \equiv -1 \pmod{p^{\alpha}} \quad \text{ou} \quad \equiv p^{\alpha} - 1 \pmod{2p^{\alpha}},$$
$$R \equiv \varphi(p^k) \pmod{p^{\alpha} \text{ ou } 2p^{\alpha}},$$

établies, on conclut dans le cas que $\delta : p^k$ a tous ses facteurs premiers inégaux :

$$S \equiv (-1)^i \varphi(p^k) \pmod{p^{\alpha}}$$

et

$$S \equiv (p^{\alpha} - 1)^i \varphi(p^k) \pmod{2p^{\alpha}}. \qquad \text{C. Q. F. D.}$$