JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

TRYGVE NAGEL

Généralisation d'un théorème de Tchebycheff

Journal de mathématiques pures et appliquées 8^e série, tome 4 (1921), p. 343-356.
<http://www.numdam.org/item?id=JMPA_1921_8_4__343_0>

Généralisation d'un théorème de Tchebycheff;

PAR TRYGVE NAGEL,

à Kristiania (Norvège).

INTRODUCTION.

On doit à Tchebycheff le théorème remarquable que voici (1) :

P_x *étant le plus grand nombre premier qui divise le produit*

$$(1+2^2)(1+4^2)(1+6^2)\ldots(1+4x^2),$$

le rapport $\frac{P_x}{x}$ *croît infiniment avec* x.

Après la mort de Tchebycheff, M. A. Markoff a trouvé dans ses manuscrits posthumes une feuille, tout à fait sale et déchirée, où se trouvaient des calculs presque inintelligibles, mais qui l'ont conduit à la démonstration du théorème. Sa démonstration fut publiée dans le *Bulletin de l'Académie Impériale des Sciences de Saint-Pétersbourg*, 1895 (2).

Ce résultat a été généralisé par M. G. Pólya, qui a démontré le théorème suivant (3) :

(1) On le trouve annoncé dans les *Cours lithographiés* (4e édition, p. 197) de Hermite.

(2) Ces renseignements sont tirés du Mémoire de M. C. STÖRMER, *Une application d'un théorème de Tchebycheff* (*Archiv for Mathematik og Naturvidenskab*, t. XXIV, Kristiania, 1902).

(3) G. PÓLYA, *Généralisation d'un théorème de M. Störmer* (*Archiv for Mathematik og Naturvidenskab*, t. XXXV, Kristiania, 1917).

En posant pour $n > 2$

$$F_n(x) = \prod_{\rho} (x - \rho),$$

où ρ *parcourt les* $\varphi(n)$ *racines primitives* $n^{\text{ièmes}}$ *de l'unité, et en désignant par* P_x *le plus grand facteur premier du produit*

$$F_n(1).F_n(2).F_n(3)\ldots F_n(x),$$

on a

$$\lim_{x=\infty} \frac{x}{P_x} = 0.$$

Dans ce qui suit nous allons démontrer que le théorème de Tchebycheff peut être étendu à *toute fonction rationnelle entière* $f(x)$, irréductible, de degré > 1, à coefficients entiers.

Nous allons, en effet, démontrer le théorème :

En désignant par P_x le plus grand facteur premier du produit

$$f(1).f(2).f(3)\ldots f(x),$$

où $f(x)$ est un polynome entier, irréductible, de degré > 1, on a

$$\lim_{x=\infty} \frac{x(\log x)^{\varepsilon}}{P_x} = 0,$$

où ε est une quantité quelconque < 1.

Dans les deux premiers paragraphes, nous démontrons quelques lemmes préliminaires : 1° sur le nombre de racines de la congruence

$$f(x) \equiv 0 \pmod{p^{\alpha}},$$

où $f(x)$ est un polynome entier, et où p est premier; et 2° sur l'ordre de grandeur de la somme

$$\sum_{p \leq x} \nu_p \frac{\log p}{p}$$

qui est étendue à tous les nombres premiers $p \leq x$, et où ν_p désigne le nombre de racines de la congruence

$$f(x) \equiv 0 \pmod{p}.$$

Le troisième paragraphe contient la généralisation du théorème de Tchebycheff.

1. Étant donnée la fonction rationnelle, entière de x de degré n à coefficients entiers

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n,$$

nous allons ici démontrer quelques théorèmes sur la congruence

$$f(x) \equiv 0 \pmod{p^\alpha},$$

où p est un nombre premier quelconque. Pour simplifier, nous supposons : 1° que le plus grand commun diviseur des coefficients $a_0, a_1, \ldots, a_n$ soit égal à 1 ; 2° que l'équation $f(x) = 0$ n'ait aucune racine multiple, c'est-à-dire que le discriminant D de $f(x)$ soit différent de zéro. Alors il est bien connu que le nombre de solutions de la congruence

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

est au plus égal au degré n de $f(x)$, lorsque p est premier. Si x_0 est une racine de la congruence (1), tel que $f'(x_0)$ ne soit pas divisible par p, nous appelons x_0 une *racine simple* de la congruence (1). Si les nombres $f(x_0)$ et $f'(x_0)$ sont tous les deux divisibles par p, nous appelons x_0 une *racine multiple* de la congruence (1). Dans le dernier cas, nous tirons, en effet, de l'identité (1)

$$f(x) = f(x_0) + (x - x_0) f'(x_0) + (x - x_0)^2 \frac{f''(x_0)}{2!} + \ldots + (x - x_0)^n \frac{f^{(n)}(x_0)}{n!} \tag{2}$$

la congruence identique

$$f(x) \equiv (x - x_0)^2 g(x) \pmod{p}, \tag{3}$$

où $g(x)$ est un polynome entier de x de degré $n - 2$. Comme le discriminant D de $f(x)$ est une fonction rationnelle, entière des coefficients de $f(x)$ à coefficients entiers, il resulte de (3) que D est congru au discriminant de $(x - x_0)^2 g(x) \equiv 0 \pmod{p}$; donc :

---

(1) Il est à remarquer que tous les nombres $\frac{1}{r!} f^{(r)}(x_0)$ sont entiers; car

$$\frac{1}{r!} f^{(r)}(x_0) = a_0 \binom{n}{r} x_0^{n-r} + a_1 \binom{n-1}{r} x_0^{n-r-1} + \ldots + a_{n-r}.$$

Lemme I. — Si la congruence (1) possède une racine multiple, le discriminant D de $f(x)$ est divisible par p.

Si l'on connaît toutes les racines de la congruence

$$f(x) \equiv 0 \pmod{p^\alpha}, \tag{4}$$

on en peut déduire toutes les racines de la congruence

$$f(x) \equiv 0 \pmod{p^{\alpha+1}}. \tag{5}$$

Toute racine de (5) est de la forme $x_0 + tp^\alpha$, où x_0 parcourt toutes les racines de (4). Cherchons à déterminer l'entier t tel que le nombre $x_0 + tp^\alpha$ soit une racine de (5), x_0 étant une racine de (4). Nous avons

$$f(x_0 + tp^\alpha) \equiv f(x_0) + tp^\alpha . f'(x_0) + t^2 p^{2\alpha} \frac{f''(x_0)}{2!} + \dots,$$

$$f(x_0 + tp^\alpha) \equiv f(x_0) + tp^\alpha . f'(x_0) \pmod{p^{\alpha+1}}.$$

On aura ainsi à résoudre la congruence

$$f'(x_0)\, t \equiv -\frac{f(x_0)}{p^\alpha} \pmod{p}. \tag{6}$$

Si $f'(x_0)$ n'est pas divisible par p, c'est-à-dire si x_0 est une racine simple de (1), cette congruence a toujours une et une seule racine t. Si $f'(x_0)$ est divisible par p, c'est-à-dire si x_0 est une racine multiple de (1), la congruence (6) a p racines, ou bien elle n'a aucune racine, suivant que $f(x_0)$ est divisible par $p^{\alpha+1}$ ou non. Dans le premier cas, correspondent à toute racine x_0 de (4) les p racines x_0, $x_0 + p^\alpha$, $x_0 + 2p^\alpha$, ..., $x_0 + (p-1)p^\alpha$ de (5).

Nous aurons, par suite, les résultats suivants :

Lemme II. — Soit x_0 une racine simple de la congruence (1). Alors, il y a une et une seule racine de la congruence (4), qui est congrue à $x_0 \pmod{p^\alpha}$.

Lemme III. — Soit x_0 une racine multiple de la congruence (1). Alors, il y a au plus $p^{\alpha-1}$ racines de la congruence (4), qui sont congrues à $x_0 \pmod{p^\alpha}$.

Des lemmes I et II, il résulte :

THÉORÈME I. — *Si p est un nombre premier qui ne divise pas le*

discriminant D *de* $f(x)$, *le nombre de racines incongrues de la congruence*

$$f(x) \equiv 0 \qquad (\mathrm{mod}\, p^{\alpha})$$

est exactement égal à celui de la congruence

$$f(x) \equiv 0 \qquad (\mathrm{mod}\, p).$$

Supposons ensuite que le nombre premier p divise D; et soit p^{μ} la plus haute puissance de p qui divise D. Si la congruence (1) n'a aucune racine multiple, le théorème I est encore vrai.

Soit maintenant x_0 une racine de la congruence

$$f(x) \equiv 0 \qquad (\mathrm{mod}\, p^{\mu+1}),$$

et de plus une racine multiple de (1). Dans ce cas, le nombre $f'(x_0)$ est au plus divisible par p^{μ}. Car, si $f'(x_0)$ était divisible par $p^{\mu+1}$, l'identité (2) donnerait la congruence identique

$$f(x) \equiv (x - x_0)^2 g(x) \qquad (\mathrm{mod}\, p^{\mu+1}),$$

d'où résulterait $D \equiv 0 \pmod{p^{\mu+1}}$, contre l'hypothèse. [D est une fonction rationnelle, entière des coefficients de $f(x)$ à coefficients entiers.]

Si $f'(x_0)$ est divisible par p^{β} et non par $p^{\beta+1}$, on a donc $\beta \leq \mu$. Il résulte de plus que les nombres $f'(x_0 + tp^{\mu+1})$, pour t entier quelconque, sont divisibles par p^{β} et non par $p^{\beta+1}$.

Si x_1 est une racine congrue à $x_0 \pmod{p^{\mu+1}}$ de la congruence

$$f(x) \equiv 0 \qquad (\mathrm{mod}\, p^{\alpha+\beta}), \tag{7}$$

où $\alpha \geq \mu + 1$, tous les nombres

$$x_1 + up^{\alpha} \qquad (u = 0, 1, 2, \ldots, p^{\beta} - 1) \tag{8}$$

le sont aussi. Car le nombre

$$f(x_1 + up^{\alpha}) = f(x_1) + up^{\alpha} f'(x_1) + \frac{1}{2} u^2 p^{2\alpha} f''(x_1) + \ldots$$

est divisible par $p^{\alpha+\beta}$, puisque $f'(x_1) \equiv 0 \pmod{p^{\beta}}$ et $2\alpha > \alpha + \beta$.

Cherchons les racines de la congruence

$$f(x) \equiv 0 \pmod{p^{\alpha+\beta+1}}, \tag{9}$$

qu'on peut déduire des p^β racines (8) de la congruence (7).

Ces racines sont de la forme $x_1 + up^\alpha + vp^{\alpha+\beta}$. Nous avons

$$f(x_1 + up^\alpha + vp^{\alpha+\beta}) = f(x_1 + up^\alpha) + vp^{\alpha+\beta} \cdot f'(x_1 + up^\alpha) + \ldots \equiv f(x_1 + up^\alpha) \pmod{p^{\alpha+\beta+1}},$$

vu que

$$f'(x_1 + up^\alpha) \equiv 0 \pmod{p}.$$

Comme $2\alpha \geqq \alpha + \beta + 1$, nous aurons

$$f(x_1 + up^\alpha) \equiv f(x_1) + up^\alpha \cdot f'(x_1) \pmod{p^{\alpha+\beta+1}}.$$

Nous aurons donc à résoudre la congruence

$$f(x_1) + up^\alpha \cdot f'(x_1) \equiv 0 \pmod{p^{\alpha+\beta+1}}.$$

La congruence

$$\frac{f(x_1)}{p^{\alpha+\beta}} \equiv -u\frac{f'(x_1)}{p^\beta} \pmod{p}$$

possède toujours une et une seule racine, soit u_0, puisque $f'(x_1)$ n'est pas divisible par $p^{\beta+1}$. Nous obtenons ainsi en partant des p^β racines (8) de la congruence (7), les p^β racines suivantes de la congruence (9) :

$$x_1 + (u_0 + hp)p^\alpha + vp^{\alpha+\beta}, \tag{10}$$

où $h = 0, 1, 2, \ldots, p^{\beta-1} - 1$, et où $v = 0, 1, 2, \ldots, p-1$, et *pas d'autres racines.*

En posant $x_1 + u_0 p^\alpha = x_1'$, le système (10) est équivalent à

$$x_1' + tp^{\alpha+1}, \tag{10'}$$

où $t = 0, 1, 2, \ldots, p^\beta - 1$.

Il résulte de là, lorsque x_1 parcourt toutes les racines de (7), qui sont congrues à $x_0 \pmod{p^{\mu+1}}$: Le nombre de racines congrues à $x_0 \pmod{p^{\mu+1}}$ de la congruence (7) est indépendant de α, lorsque $\alpha \geqq \mu + 1$.

A toute valeur de x_0 correspond une valeur déterminée de β, qui est $\leqq \mu$. Par conséquent, nous pouvons tirer la conclusion :

La congruence

$$f(x) \equiv 0 \pmod{p^{\alpha+\mu}} \tag{11}$$

possède exactement autant de racines que la congruence

$$f(x) \equiv 0 \pmod{p^{2\mu+1}}, \tag{12}$$

quel que soit $\alpha > \mu$.

[Car, de toute racine de (12), qui est une racine simple de (1), se déduit, d'après le lemme II, une et une seule racine de (11).]

Si la congruence (1) possède exactement m racines simples et m_1 racines multiples, le nombre de racines de la congruence (12) est au plus égal à (d'après les lemmes II et III)

$$m + m_1 p^{2\mu} \leq n\mathrm{D}^2.$$

Nous avons ainsi démontré :

THÉORÈME II. — *La congruence*

$$f(x) \equiv 0 \pmod{p^{\alpha}},$$

où p est un facteur premier du discriminant D *de* $f(x)$, *possède au plus* $n\mathrm{D}^2$ *racines incongrues* (1).

2. Supposons que le corps algébrique $k(\alpha)$ de degré n soit engendré par le nombre α, racine de l'équation $f(x) = 0$, où

$$f(x) \equiv x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$

est une fonction entière, irréductible de x à coefficients entiers.

En prenant pour point de départ la formule connue (2)

$$\sum_{\mathrm{N}(\mathfrak{p}) \leq x} \log \mathrm{N}(\mathfrak{p}) = x + \mathrm{O}\left(x e^{-c\sqrt{\log x}}\right), \tag{1}$$

(1) Notre démonstration de cette proposition se date du 6 février 1921. M. Ore nous a communiqué qu'il a démontré ce théorème déjà au mois de janvier. Sa démonstration va paraître dans *Norsk Matematisk Tidsskrift*, t. 3 (Kristiania, 1921).

(2) *Voir* M. E. LANDAU, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale* (Leipzig, 1918, p. 109).

où la somme est étendue à tous les idéaux premiers $\mathfrak{p}$ du corps $k(\alpha)$ dont la norme ne surpasse pas x, et où c est une constante positive, nous allons d'abord démontrer la formule suivante :

$$\sum_{N(\mathfrak{p})\leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} = \log x + O(1). \tag{2}$$

Posons, pour abréger,

$$\vartheta(x) = \sum_{N(\mathfrak{p})\leq x} \log N(\mathfrak{p}), \qquad \psi(x) = \sum_{N(\mathfrak{p})\leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}$$

et

$$\eta(x) = \vartheta(x) - x = O\left(x e^{-c\sqrt{\log x}}\right).$$

Alors nous avons

$$\begin{aligned}\psi(x) &= \sum_{m=2}^{x} \frac{\vartheta(m) - \vartheta(m-1)}{m} \\ &= \sum_{2}^{x} \frac{1}{m} + \sum_{2}^{x} \frac{1}{m}[\eta(m) - \eta(m-1)] \\ &= \log x + O(1) + \sum_{2}^{x} \eta(m)\left[\frac{1}{m} - \frac{1}{m+1}\right] - \frac{1}{2}\eta(1) + \frac{\eta(x)}{x+1},\end{aligned}$$

vu que

$$\sum_{2}^{x} \frac{1}{m} = \log x + O(1).$$

En y introduisant

$$\eta(x) = O\left(x e^{-c\sqrt{\log x}}\right),$$

on aura

$$\psi(x) = \log x + O(1) + O\left(\sum_{2}^{x} \frac{e^{-c\sqrt{\log m}}}{m+1}\right) + O\left(e^{-c\sqrt{\log x}}\right).$$

Or, nous avons pour m_0 suffisamment grand

$$e^{-c\sqrt{\log m}} < \frac{1}{[\log(m+1)]^2}$$

pour tous les $m \geq m_0$. Comme la série $\sum_{2}^{\infty} \frac{1}{m(\log m)^2}$ est convergente,

nous aurons, par suite,

$$\psi(x) = \log x + O(1). \qquad \text{C. Q. F. D.}$$

Désignons maintenant par $\nu_p^{(r)}$ le nombre d'idéaux premiers (différents) de degré r divisant l'idéal principal $[p]$, où p est un nombre premier (rationnel). Si $\mathfrak{p}_r$ désigne un idéal premier de degré r, nous aurons les équations :

$$(3)\qquad \begin{cases} \displaystyle\sum_{\mathfrak{p}_1}^{N(\mathfrak{p}_1)\leq x} \frac{\log N(\mathfrak{p}_1)}{N(\mathfrak{p}_1)} = \sum_{p}^{p\leq x} \nu_p^{(1)} \frac{\log p}{p}, \\ \displaystyle\sum_{\mathfrak{p}_2}^{N(\mathfrak{p}_2)\leq x} \frac{\log N(\mathfrak{p}_2)}{N(\mathfrak{p}_2)} = \sum_{p}^{p^2\leq x} 2\nu_p^{(2)} \frac{\log p}{p^2}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots, \\ \displaystyle\sum_{\mathfrak{p}_n}^{N(\mathfrak{p}_n)\leq x} \frac{\log N(\mathfrak{p}_n)}{N(\mathfrak{p}_n)} = \sum_{p}^{p^n\leq x} n\nu_p^{(n)} \frac{\log p}{p^n}, \end{cases}$$

où les sommes à droite sont étendues à tous les nombres premiers $p \leq x$ (dans la première), $\leq x^{\frac{1}{2}}$ (dans la seconde), etc.

Or, nous avons, pour $r \geq 2$,

$$\sum_{p}^{p^r\leq x} r\nu_p^{(r)} \frac{\log p}{p^r} < rn \sum_{p}^{p^r\leq x} \frac{\log p}{p^2} = O(1),$$

puisque la série $\displaystyle\sum_{k=1}^{\infty} \frac{\log k}{k^2}$ est convergente.

Par addition, il résulte donc de (3),

$$(3')\qquad \sum_{N(\mathfrak{p})\leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} = \sum_{p\leq x} \nu_p^{(1)} \frac{\log p}{p} + O(1).$$

Or, si nous désignons par ν_p le nombre de racines incongrues de la congruence

$$f(x) \equiv 0 \pmod{p},$$

nous avons d'après Dedekind $\nu_p^{(1)} = \nu_p$, pourvu que p ne soit pas un diviseur « non essentiel » de « l'index » du nombre entier α du corps

$k(\alpha)$ (1). Comme il n'y a qu'un nombre fini de tels diviseurs « non essentiels », nous pouvons dans la formule (3') remplacer $\nu_p^{(1)}$ par ν_p. En appliquant la formule (2), on aura, par suite, la formule suivante :

$$\sum_{p}^{p \leq x} \nu_p \frac{\log p}{p} = \log x + O(1), \tag{4}$$

où la somme est étendue à tous les nombres premiers $p \leq x$.

Cette formule est encore valable pour le polynome irréductible

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \qquad (a_0 \neq 0).$$

Car, si nous y posons

$$a_0 x = z$$

et

$$g(z) = a_0^{n-1} f(x) = z^n + a_1 z^{n-1} + \ldots + a_{n-1} a_0^{n-2} z + a_n a_0^{n-1},$$

la formule (4) est valable pour le polynome $g(z)$. Or, le nombre de racines de la congruence

$$f(x) \equiv 0 \pmod{p}$$

est exactement égal à celui de la congruence

$$g(z) \equiv 0 \pmod{p},$$

sauf pour a_0 divisible par p. La formule (4) est donc valable pour tous les polynomes irréductibles.

Lorsque $f(x)$ est réductible, la formule (4) subsiste encore, si l'on y remplace le membre $\log x$ par $m \log x$, où m désigne le nombre de facteurs irréductibles différents contenus dans $f(x)$.

3. Soit donnée la fonction rationnelle, entière de degré n à coefficients entiers

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n. \tag{1}$$

---

(1) *Voir* R. DEDEKIND, *Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen* (*Abh. der K. Ges. der Wiss. zu Göttingen*, 1878).

Désignons par P_x le plus grand facteur premier du produit

$$f(1).f(2).f(3)\ldots f(x). \tag{2}$$

[Cette définition exige que $f(x)$ ne s'annule pour aucune valeur entière, positive de x.]

Le but de ce paragraphe est de montrer qu'on a

$$\lim_{x\to\infty} \frac{x(\log x)^{\varepsilon}}{P_x} = 0, \qquad \text{où } \varepsilon < 1, \tag{3}$$

pour toute fonction irréductible $f(x)$ de degré > 1.

Cherchons d'abord une limite supérieure de l'exposant L de la plus haute puisance p^L du nombre premier p, qui divise le produit

$$f(1).f(2).f(3)\ldots f(N). \tag{4}$$

Si p ne divise pas le discriminant D de $f(x)$, la congruence

$$f(x) \equiv 0 \pmod{p^m}$$

possède exactement ν_p racines incongrues (*cf.* § **1**, théorème I, et pour la définition de ν_p, § **2**). L'exposant L de la plus haute puissance de p qui divise (4) ne peut donc surpasser la quantité

$$\nu_p\left[\mathrm{E}\left(\frac{N}{p}\right)+1+\mathrm{E}\left(\frac{N}{p^2}\right)+1+\ldots+\mathrm{E}\left(\frac{N}{p^l}\right)+1\right], \tag{5}$$

où p^{l+1} est plus grand que tous les nombres $|f(1)|, |f(2)|, \ldots, |f(N)|$. [$\mathrm{E}(x)$ désigne le plus grand nombre entier contenu dans x.]

Si p divise le discriminant D, le nombre des racines de la congruence

$$f(x) \equiv 0 \pmod{p^m}$$

est au plus égal à $n\mathrm{D}^2$ (*cf.* § **1**, théorème II). L'exposant cherché L ne peut donc être supérieur à

$$n\mathrm{D}^2\left[\mathrm{E}\left(\frac{N}{p}\right)+1+\mathrm{E}\left(\frac{N}{p^2}\right)+1+\ldots+\mathrm{E}\left(\frac{N}{p^l}\right)+1\right]. \tag{5'}$$

Nous pouvons toujours déterminer un nombre positif x_0 tel que (1)

$$|f(x)| = |a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n| < a_0(x+x_0)^n$$

(1) Pour simplifier, nous supposons a_0 positif.

pour toute valeur positive de x. Car nous avons, pour $x > 0$,

$$|f(x)| \leqq a_0 x^n + |a_1| x^{n-1} + \ldots + |a_k| x^{n-k} + \ldots + |a_n|$$

et

$$a_0(x + x_0)^n = a_0 x^n + a_0 \binom{n}{1} x_0 x^{n-1} + \ldots + a_0 \binom{n}{k} x_0^k x^{n-k} + \ldots + a_0 x_0^n.$$

Il suffit donc de choisir le nombre x_0 plus grand que tous les nombres

$$\left| \sqrt[k]{\frac{a_k}{a_0 \binom{n}{k}}} \right| \qquad (k = 1, 2, 3, \ldots, n).$$

Il résulte de là qu'on peut choisir l'exposant l de manière qu'on ait

$$p^l \leqq a_0 (N + x_0)^n < p^{l+1}$$

ou

$$l \leqq \frac{\log a_0}{\log p} + n \frac{\log(N + x_0)}{\log p} < l + 1. \tag{6}$$

Comme

$$E\left(\frac{N}{p}\right) + E\left(\frac{N}{p^2}\right) + \ldots + E\left(\frac{N}{p^l}\right) \leqq N\left(\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^l}\right) < \frac{N}{p-1},$$

nous pouvons remplacer les limites (5) et (5′) par les suivantes :

$$\nu_p \frac{N}{p-1} + \nu_p \frac{\log a_0}{\log p} + n \nu_p \frac{\log(N + x_0)}{\log p}$$

et

$$n D^2 \frac{N}{p-1} + n D^2 \frac{\log a_0}{\log p} + n^2 D^2 \frac{\log(N + x_0)}{\log p}.$$

Par conséquent, nous aurons

$$\begin{aligned} &\sum_{x=1}^{x=N} \log |f(x)| \\ &< \sum_{p}^{p \leqq p_N} \log p \left[\nu_p \frac{N}{p-1} + \nu_p \frac{\log a_0}{\log p} + n \nu_p \frac{\log(N + x_0)}{\log p} \right] \\ &+ \sum_{D \equiv 0 \pmod p} \log p \left[n D^2 \frac{N}{p-1} + n D^2 \frac{\log a_0}{\log p} + n^2 D^2 \frac{\log(N + x_0)}{\log p} \right]. \end{aligned}$$

Il est évident que l'ordre de grandeur de la dernière somme est $O(N)$.

Nous avons, de plus,

$$\sum_{p\leq P_N} \nu_p \frac{\log p}{p-1} = \sum_{p\leq P_N} \nu_p \frac{\log p}{p} + O(1).$$

Car la série

$$\sum_{p}^{\infty} \nu_p \frac{\log p}{p(p-1)}$$

est convergente, puisque l'est la série

$$\sum_{k=2}^{\infty} \frac{\log k}{k(k-1)}.$$

Nous arrivons donc à la relation

$$(7) \quad \sum_{x=1}^{x=N} \log|f(x)| < \sum_{p\leq P_N} N\nu_p \frac{\log p}{p} + \sum_{p\leq P_N} \nu_p[\log a_0 + n\log(N+x_0)] + O(N).$$

Supposons qu'il existe une grandeur g telle qu'on ait pour une infinité de valeurs de N l'inégalité

$$(8) \qquad P_N \leq gN(\log N)^{\varepsilon} \qquad \text{pour } \varepsilon < 1.$$

Dans ce cas, nous aurons, d'après la formule (4), paragraphe **2** :

$$\sum_{p\leq P_N} \nu_p \frac{\log p}{p} = \log P_N + O(1) \leq \log N + \varepsilon \log\log N + O(1),$$

et, en outre, d'après la théorie de la distribution des nombres premiers,

$$\sum_{p\leq P_N} \nu_p \leq \sum_{p\leq P_N} n = O\left(\frac{P_N}{\log P_N}\right) = O[N(\log N)^{\varepsilon-1}].$$

En introduisant ces valeurs dans (7), il vient

$$(9) \qquad \sum_{x=1}^{x=N} \log|f(x)| < N\log N + O[N(\log N)^{\varepsilon'}],$$

où $\varepsilon' < 1$.

D'autre part, nous avons

$$\sum_{x=1}^{x=N} \log|f(x)| - n\sum_{x=1}^{x=N} \log x = \sum_{x=1}^{x=N} \log|a_0 + a_1 x^{-1} + \ldots + a_n x^{-n}| = O(N).$$

La formule de Stirling,

$$\sum_{x=1}^{x=N} \log x = N\log N - N + \frac{1}{2}\log N + O(1),$$

donne, par suite,

$$\sum_{x=1}^{x=N} \log|f(x)| = nN\log N + O(N).$$

Or, cette formule est contradictoire avec l'inégalité (9), n étant > 1.

L'inégalité (8) n'a donc lieu que pour un nombre fini de valeurs de N. Par conséquent, le théorème (3) se trouve démontré pour toute fonction irréductible $f(x)$ de degré > 1. Nous le pouvons évidemment énoncer sous la forme suivante :

« Soit $f(x)$ une fonction rationnelle, entière, irréductible, de degré > 1 à coefficients entiers. Alors il y a au moins un nombre parmi les nombres

$$f(1),\quad f(2),\quad f(3),\quad \ldots,\quad f(x)$$

qui est divisible par un nombre premier $p > x(\log x)^{\varepsilon}$, ε étant un quantité quelconque < 1, pour tous les $x > x_0$, où le nombre x_0 dépend de ε. »

Plus généralement, nous tirons de là le résultat suivant :

Soit $f(x)$ une fonction rationnelle, entière, à coefficients entiers, possédant au moins un zéro irrationnel. Alors, il y a au moins un nombre, différent de zéro, parmi les nombres

$$f(1),\quad f(2),\quad f(3),\quad \ldots,\quad f(x),$$

qui est divisible par un nombre premier $p > x(\log x)^{\varepsilon}$, ε étant une quantité quelconque < 1, pour tous les $x > x_0$, où le nombre x_0 dépend de ε.