A. Gelfond, Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier, *Rec. Math. [Mat. Sbornik] N.S.*, 1940, Volume 7(49), Number 1, 7–25

1940 МАТЕМАТИЧЕСКИЙ СБОРНИК Т. 7 (49), N. 1
RECUEIL MATHÉMATIQUE

Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier

A. Gelfond (Moscou)

§ 1

Dans mon article[1] „Sur l'approximation du rapport des logarithmes de deux nombres algébriques au moyen de nombres algébriques“ j'ai démontré que si α et β sont algébriques, $\alpha \neq 0,\ 1,\ \beta \neq 0,\ 1$ et si $\frac{\ln \alpha}{\ln \beta}$ est irrationnel, l'inégalité

$$\left|\frac{\ln \alpha}{\ln \beta} - \theta\right| < e^{-\ln^{3+\varepsilon} H}, \quad \varepsilon > 0, \tag{1}$$

où H est la hauteur de l'équation dont le nombre algébrique θ est une racine, n'a qu'un nombre fini de solutions algébriques différentes θ.

En particulier, en posant $\theta = \frac{m}{n}$, m et n étant des entiers, $(m, n) = 1$, nous obtenons immédiatement que pour $n \geqslant n_0(\varepsilon)$ on a l'inégalité

$$|n \ln \alpha - m \ln \beta| > e^{-\ln^{3+\varepsilon} m}, \quad \varepsilon > 0,$$

ou bien l'inégalité

$$|\alpha^n - \beta^m| > |\beta|^m e^{-\ln^{3+\varepsilon}|m|}, \quad \varepsilon > 0, \tag{2}$$

quand

$$|\beta|^m \geqslant |\alpha|^n, \quad n > 0, \quad m > 0, \quad |\alpha| \neq 1, \quad |\beta| \neq 1.$$

Cette dernière inégalité permet d'affirmer que deux progressions géométriques à bases algébriques dont les modules ne sont pas égaux à 1 possèdent cette propriété que la différence entre leurs membres est ou bien très grande ou bien pas trop petite pour les grandes valeurs des exposants.

Le but du présent article est d'établir une autre propriété des progressions géométriques à raisons algébriques. La différence de deux membres de progressions géométriques à raisons α et β, $|\alpha| \neq 1$, $|\beta| \neq 1$, α et β étant algébriques et $\frac{\ln \alpha}{\ln \beta}$ irrationnel, $\alpha^n - \beta^m$ n'est pas divisible par $\wp^\gamma$, où $\wp$ est un idéal premier, pourvu que $\gamma > \ln^{3+\varepsilon} n$, $\varepsilon > 0$, $n \geqslant m > 0$, $n > n_0$. Autrement dit, $\alpha^n - \beta^m$ ne peut pas être aussi petit que l'on veut au sens $\wp$-adique, si $|\alpha|_\wp \geqslant 1$, $|\beta|_\wp \geqslant 1$.

Cette dernière affirmation peut être écrite dans la forme de l'inégalité

$$|\alpha^n - \beta^m|_\wp > \wp^{-\ln^{3+\varepsilon} n}, \quad \varepsilon > 0, \tag{3}$$

[1] Bulletin de l'Académie des Sciences de l'U.R.S.S., (1939).

où le module du premier membre est pris au sens $\wp$-adique; on déduit de cette inégalité et de l'inégalité (2) le théorème suivant:

Si α, β, γ *sont des nombres algébriques réels,* $|\alpha| \neq 0, 1$, $|\beta| \neq 0, 1$, $|\gamma| \neq 0, 1$, *dont l'un au moins n'est pas une unité algébrique, l'équation*

$$\alpha^x + \beta^y = \gamma^z \tag{4}$$

n'a qu'un nombre fini de solutions en nombres rationnels entiers x, y, z, *sauf dans le cas où*

$$\alpha = \pm 2^{k_1}, \quad \beta = \pm 2^{k_2}, \quad \gamma = \pm 2^{k_3}, \tag{5}$$

k_1, k_2 *et* k_3 *étant rationnels.*

En particulier, quand α, β et γ sont rationnels et aucun d'eux n'est égal ni à 0, ni à 1, ni à -1, l'équation (4) n'a qu'un nombre fini de solutions sauf le cas de α, β et γ définis par l'égalité (5).

§ 2

Dans toutes les considérations qui suivent les nombres algébriques $\alpha, \alpha_1, \ldots, \alpha_{k_1}, \beta, \beta_1, \ldots, \beta_{k_2}$ appartiendront à un corps algébrique R d'ordre ν, $\wp$ sera un idéal premier du corps R et $R(\wp)$ sera une extension $\wp$-adique du corps R. Nous poserons $N(\wp) = p^\rho$ où $\rho \geqslant 1$, $|p|_\wp = \varphi$, c'est-à-dire $p \equiv 0 \pmod{\wp^\varphi}$ et $p \not\equiv 0 \pmod{\wp^{\varphi+1}}$.

On sait que ρ et φ seront des nombres entiers, $\rho\varphi \leqslant \nu$. Remarquons d'ailleurs que si α est un nombre algébrique entier de R, on a $|\alpha|_\wp \geqslant |N(\alpha)|_\wp$ dans $R(\wp)$. Si A est un nombre entier, nous conviendrons d'écrire $|A|_\wp \geqslant A^{-1}$, cette inégalité étant comprise dans ce sens que $|A|_\wp \geqslant \wp^{-\lambda\varphi}$ où $\lambda = \left[\frac{\ln A}{\ln p}\right]$. La méthode des fonctions $\wp$-adiques que nous suivrons dans la suite a été introduite dans les travaux de K. Mahler et T. Skolem[2].

Démontrons maintenant un théorème concernant les bornes inférieures des polynômes algébriques de nombres algébriques au sens $\wp$-adique.

Lemme I. *Soient* $\alpha_1, \alpha_2, \ldots, \alpha_t$ *des nombres algébriques du corps* R, *dont les numérateurs et les dénominateurs ne sont pas divisibles par un idéal premier* $\wp$ *du corps* R. *Soient d'ailleurs* $A_{h_1, h_2, \ldots, h_t}$ *des nombres entiers rationnels. Alors ou bien*

$$F(\alpha_1, \alpha_2, \ldots, \alpha_t) = \sum_{h_1=0}^{N_1} \cdot \sum_{h_t=0}^{N_t} A_{h_1, \ldots, h_t} \alpha_1^{h_1} \ldots \alpha_t^{h_t} = 0 \tag{6}$$

ou bien

$$|F(\alpha_1, \ldots, \alpha_t)|_\wp \geqslant \{C^{1+\sum_1^t N_i} A^\nu\}^{-1} \tag{7}$$

où C *ne dépend que de* $\alpha_1, \alpha_2, \ldots, \alpha_t$, ν *est l'ordre de* R *et*

$$A = \max |A_{h_1, \ldots, h_t}|. \tag{8}$$

---

[2] K. Mahler, Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen, Acad. Wetensch. Amsterdam Proceed., **38**, (1935), 50; Th. Skolem, Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen, Mathem. Ann., **111**, (1935), 399.

Pour la démonstration on remarque d'abord qu'il existe un entier rationnel B tel que $B\alpha_1$, $B\alpha_2, \ldots, B\alpha_t$ seront des nombres entiers du corps R. Il est facile à voir que

$$|N[B^{1+\sum_1^t N_i} F(\alpha_1, \ldots, \alpha_t)]| < C^{1+\sum_1^t N_i} A^{\nu}, \tag{9}$$

ce qui conduit à notre lemme, puisque

$$|F(\alpha_1, \ldots, \alpha_t)|_{\wp} \geqslant |N(B^{1+\sum_1^t N_i} F(\alpha_1, \ldots, \alpha_t)|_{\wp}. \tag{10}$$

§ 3

Soit $\wp$ un idéal premier du corps algébrique R, p un entier rationnel premier, $N(\wp)=p^{\rho}, p \equiv 0 \pmod{\wp^{\varphi}}$. Soit $R(\wp)$ une extension $\wp$-adique du corps R d'ordre ν. Nous dirons qu'une fonction $f(z)$ d'une variable $\wp$-adique dans le corps $R(\wp)$ est normale[3], si l'on peut représenter $f(z)$, par une série potentielle

$$f(z)=f_0+f_1 z+\ldots+f_n z^n+\ldots \tag{11}$$

où les f_i, $i=0, 1, 2, \ldots, n, \ldots$, sont des nombres $\wp$-adiques et les conditions suivantes sont vérifiées

$$|f_k|_{\wp} \leqslant 1, \quad k=0, 1, 2, \ldots, \quad \lim_{k=\infty} |f_k|_{\wp}=0. \tag{12}$$

Il est évident que dans les conditions (12) la série (11) converge uniformément (au sens $\wp$-adique) si $|z|_{\wp} \leqslant 1$ et que pour $|z|_{\wp} \leqslant 1$ on a $|f(z)|_{\wp} \leqslant 1$. Il est aisé de voir que $F(z)=\frac{1}{k!} f^{(k)}(z+z_0)$, $|z_0|_{\wp} \leqslant 1$, est aussi une fonction normale de z et que la somme et le produit de fonctions normales sont aussi des fonctions normales.

Soient r_1 et r_2 deux nombres entiers et $x_0, x_1, \ldots, x_{r_2-1}$ des nombres $\wp$-adiques de $R(\wp)$, $|x_i|_{\wp} \leqslant 1$, $i=0, 1, 2, \ldots, r_2-1$. Construisons un polynôme interpolatoire d'ordre $r_1 r_2-1$ défini par les conditions

$$P^{(s)}(x_i)=f^{(s)}(x_i), \quad 0 \leqslant s \leqslant r_2-1, \quad 0 \leqslant i \leqslant r_2-1, \tag{13}$$

où $f(z)$ est une fonction normale de la variable $\wp$-adique z. On sait que les conditions (13) définissent un seul polynôme d'ordre $r_1 r_2-1$. On a pour ce polynôme le lemme suivant:

Lemme II. *Un polynôme d'ordre $r_1 r_2-1$, défini par les conditions* (13), *sera une fonction normale de la variable $\wp$-adique x [conditions* (12)] *pourvu que $f(x)$ soit une fonction normale, les x_i étant quelconques,* $|x_i|_{\wp} \leqslant 1$, $i=0$, $1, 2, \ldots, r_2-1$.

D'ailleurs, si $x=py$ où y est un nombre entier rationnel et p est un nombre premier entier rationnel, si $x_t=pt$, $t=0, 1, \ldots, r_2-1$, on a l'inégalité

$$|P^{(\sigma)}(py)|_{\wp} \leqslant |p^{-\sigma\left[\frac{\ln py}{\ln p}\right]-r_1\left[\frac{\ln pr_2}{\ln p}\right]}|_{\wp} \cdot \max_{\substack{0 \leqslant s \leqslant r_1-1 \\ 0 \leqslant t \leqslant r_2-1}} |f^{(s)}(pt)|_{\wp}. \tag{14}$$

[3] K. Mahler, Über transzendente P-adische Zahlen, Compositio Mathematica, **2**, (1935), 259.

Pour démontrer que le polynôme $P(x)$ est normal il suffit de l'écrire suivant la formule de Newton,

$$P(x)=\sum_{k=0}^{r_2-1}\sum_{s=1}^{r_1} A_{s,k}\,[(x-x_0)\ldots(x-x_{k-1})]^{r_1}(x-x_k)^{s-1}, \tag{15}$$

où l'on a, si $f(x)=\sum\limits_{m=0}^{\infty} f_m x^m$,

$$A_{s,k}=\sum_{m=0}^{\infty} f_m B_{s,k}^{(m)} \tag{16}$$

$B_{s,k}^{(m)}$ étant le coefficient du développement de x^m suivant les polynômes

$$[(x-x_0)\ldots(x-x_{k-1})]^{r_1}(x-x_k)^s,$$

$$x^m=\sum_{k=0}^{\infty}\sum_{s=1}^{r_1} B_{s,k}^{(m)}\,[(x-x_0)\ldots(x-x_{k-1})]^{r_1}(x-x_k)^s. \tag{17}$$

Il suit de l'égalité (17) que tous les $B_{s,k}^{(m)}$ sont des fonctions entières rationnelles des variables $x_0, x_1, \ldots$ ayant des coefficients rationnels entiers. Donc, $|A_{s,k}|_{\wp}\leqslant 1$ parce que $f(x)$ est une fonction normale et $|x_i|_{\wp}\leqslant 1$, $i=0, 1, \ldots, r_2-1$. Il en résulte que $P(x)$ est une fonction normale.

Pour démontrer les inégalités (14) nous représenterons $P(x)$ suivant la formule de Lagrange,

$$P(x)=\sum_{t=0}^{r_2-1}\sum_{s=0}^{r_1-1}\frac{f^{(s)}(x_t)}{s!\,(r_1-s-1)!}\,C_{s,t}(x)\,[(x-x_0)\ldots(x-x_{r_2-1})]^{r_1}, \tag{18}$$

$$C_{s,t}(x)=\left|\frac{d^{r_1-s-1}}{dz^{r_1-s-1}}\,\frac{(z-x_t)^{r_1}}{[(z-x_0)\ldots(z-x_{r_2-1})]^{r_1}(x-z)}\right|_{z=x_t}.$$

Suivant la formule de Leibnitz, nous aurons

$$C_{s,t}(x)=\sum_{h_0+\ldots+h_{r_2-1}=r_1-s-1}\!\!\!\cdots\sum\frac{(-1)^{r_1-s}(r_1-s-1)!\prod\limits_{k=0}^{r_2-1}\dfrac{(r_1+h_k-1)!}{h_k!\,(r_1-1)!}\cdot\dfrac{h_t!\,(r-1)!}{(r_1+h_t-1)!}}{(x_t-x_0)^{r_1+h_0}\ldots(x_t-x_{r_2-1})^{r_2+h_{r_2-1}}(x_t-x)^{h_t+1}}. \tag{19}$$

En posant

$$A_{s,t}^{(h)}=\sum_{\substack{h_0+\ldots+h_{r_2-1}=r_1-s-h-1\\ h_t=0}}\!\!\!\cdots\sum\frac{(-1)^{r_1-s-1}\prod\limits_{k=0}^{r_2-1}\dfrac{(r_1+h_k-1)!}{h_k!\,(r_1-1)!}}{(x_t-x_0)^{h_0}\ldots(x_t-x_{r_2-1})^{h_{r_2-1}}}, \tag{20}$$

nous obtenons

$$C_{s,t}(x)=\frac{(r_1-s-1)!}{[(x_t-x_0)\ldots(x_t-x_{r_2-1})]^{r_1}}\sum_{h=0}^{r_1-s-1}\frac{A_{s,t}^{h}}{(x-x_t)^{h+1}}. \tag{21}$$

Posons maintenant $x=py$, $y>r_2$, y étant entier rationnel et $x_t=pt$. Nous aurons d'abord

$$\left|A_{s,t}^{(h)}\right|_{\wp}\leqslant\left|\frac{1}{p^{r_1-s-h-1}p^{\left[\frac{\ln r_2}{\ln p}\right](r_1-s-h-1)}}\right|_{\wp}, \tag{22}$$

d'où il résulte que

$$\left| C_{s,t}(x) \right|_{\wp} \leqslant \left| \frac{(r_1-s-1)!\, p^{-r_1\left[\frac{\ln r_2}{\ln p}\right]}}{p^{r_1 r_2 - s}[t!\,(r_2-t-1)!]^{r_1}} \right|_{\wp} \left| \frac{1}{(y-t)^{r_1-s}} \right|_{\wp} \tag{23}$$

et que

$$\left| \frac{d^{\sigma}}{dx^{\sigma}} C_{s,t}(x) \right|_{\wp} \leqslant \left| \frac{(r_1-s-1)!\, p^{-r_1\left[\frac{\ln r_2}{\ln p}\right] - r_1 r_2 + s - \sigma}}{[t!\,(r_2-t-1)!]^{r_1}(y-t)^{r_1-s-\sigma}} \right|_{\wp} \tag{24}$$

ou bien, comme $y > r_2$, $t \leqslant r_2 - 1$, $s \leqslant r_1 - 1$,

$$\left| \frac{d^{\sigma_1}}{dx^{\sigma_1}} C_{s,t}(x) \right| \leqslant \left| \frac{(r_1-s-1)!}{[t!\,(r_2-t-1)!]^{r_1}}\, p^{-r_1\left[\frac{\ln r_2}{\ln p}\right] - (r_1+\sigma_1)\left[\frac{\ln y}{\ln p}\right] - r_1 r_2 - \sigma_1} \right|_{\wp} . \tag{25}$$

Ensuite nous aurons

$$\left| \frac{d^{\sigma_2}}{dx^{\sigma_2}} [x(x-p)\ldots(x-pr_2+p)]^{r_1} \right|_{\wp} \leqslant \left| \frac{p^{r_1 r_2}(r_2!)^{r_1}}{p^{\sigma_2} p^{\sigma_2\left[\frac{\ln y}{\ln p}\right]}} \right|_{\wp} . \tag{26}$$

En tenant compte de la formule de Leibnitz et des inégalités (25) et (26), nous obtiendrons immédiatement que

$$\left| \frac{d^{\sigma}}{dx^{\sigma}} C_{s,t}(x)\,[x(x-p)\ldots(x-pr_2+p)]^{r_1} \right|_{\wp} \leqslant$$

$$\leqslant \left| p^{-\sigma\left[\frac{\ln py}{\ln p}\right] - r_1\left[\frac{\ln pr_2}{\ln p}\right]} (r_1-s-1)! \right|_{\wp} . \tag{27}$$

Il en résulte finalement que l'on a l'inégalité

$$|P^{(\sigma)}(py)|_{\wp} \leqslant \left| p^{-\sigma\left[\frac{\ln py}{\ln p}\right] - r_1\left[\frac{\ln pr_2}{\ln p}\right]} \right|_{\wp} \cdot \max_{\substack{0 \leqslant s \leqslant r_1 - 1 \\ 0 \leqslant t \leqslant r_2 - 1}} |f^{(s)}(pt)|_{\wp} \tag{28}$$

pour $y \geqslant 0$ entier positif, puisque

$$|s!|_{\wp} > |r_1!|_{\wp} > |p^{+\frac{r}{p-1}}|_{\wp} .$$

Soit maintenant $F(z)$ une fonction normale de z qui possède aux points $0, p, \ldots, 2p, \ldots, (r_2-1)p$ des zéros multiples d'ordre r_1. Nous aurons alors évidemment [3]

$$F(z) = [z(z-p)\ldots(z-pr_2+p)]^{r_1} \cdot F_1(z), \tag{29}$$

où $F_1(z)$ est aussi une fonction normale de z. En posant $z = py$, nous déduirons immédiatement de la formule (29) l'inégalité

$$|F^{(\sigma)}(py)|_{\wp} \leqslant |p^{r_1 r_2 - \sigma}|_{\wp} = \wp^{-\varphi(r_1 r_2 - \sigma)}, \tag{30}$$

où $y \geqslant 0$ est un entier rationnel et $|p|_{\wp} = \wp^{-\varphi}$.

Ensuite, si le polynôme d'ordre $r_1 r_2 - 1$ est défini par les conditions

$$P^{(s)}(pt) = f^{(s)}(pt), \quad 0 \leqslant s \leqslant r_1 - 1, \quad 0 \leqslant t \leqslant r_2 - 1, \tag{31}$$

où $f(z)$ est une fonction normale, il sera aussi une fonction normale. Donc, la fonction $F(z) = f(z) - P(z)$ sera normale et $F^{(s)}(pt) = 0$, $0 \leqslant s \leqslant r_1 - 1$, $0 \leqslant t \leqslant r_2 - 1$. Nous obtenons ainsi l'inégalité

$$|f^{(\sigma)}(pt) - P^{(\sigma)}(pt)|_{\wp} \leqslant \wp^{-\varphi(r_1 r_2 - \sigma)}, \tag{32}$$

où $t \geqslant 0$ est un entier rationnel.

On déduit immédiatement des inégalités (14) et (32) le lemme suivant:

Lemme III. *Soit $f(z)$ une fonction normale, les nombres $\sigma \geqslant 0$, $r_1 > 1$, $r_2 > 1$, $y \geqslant 0$ des entiers rationnels, p un nombre premier rationnel et*

$$|p|_{\wp} = \wp^{-\varphi}.$$

On aura alors l'inégalité

$$|f^{(\sigma)}(py)|_{\wp} \leqslant \max\left[\wp^{-\varphi(r_1 r_2 - \sigma)}, \wp^{\varphi\sigma\left[\frac{\ln py}{\ln p}\right] + \varphi r_1\left[\frac{\ln r_2 p}{\ln p}\right]} \cdot M\right], \tag{33}$$

$$M = \max_{\substack{0 \leqslant s \leqslant r_1 - 1 \\ 0 \leqslant t \leqslant r_2 - 1}} |f^{(s)}(pt)|_{\wp}.$$

Pour les applications ultérieures de ce lemme il est très commode de lui donner une forme un peu différente.

Lemme IV. *Soit $f(z)$ une fonction normale, les nombres $N > p$, $\sigma \geqslant 0$, $r_1 > 1$, $r_2 > 1$, $y \geqslant 0$ des entiers rationnels vérifiant les conditions*

$$\sigma \leqslant r_1,\ r_1 = [N^{1+\delta}] + 1,\ r_2 \leqslant N^3,\ y \leqslant N^3,\ 0 < \delta < 1 \ \text{et}\ |p|_{\wp} = \wp^{-\varphi}. \tag{34}$$

On aura alors l'inégalité

$$|f^{(\sigma)}(py)|_{\wp} \leqslant \max\left[\wp^{-\varphi N^{1+\delta}(r_2 - 1)}, \wp^{16\varphi N^{1+\delta}\ln N} \max_{\substack{0 \leqslant s \leqslant r_1 - 1 \\ 0 \leqslant t \leqslant r_2 - 1}} |f^{(s)}(pt)|_{\wp}\right]. \tag{35}$$

Le lemme IV est une conséquence tout à fait immédiate du lemme III.

§ 4

Soit R un corps algébrique d'ordre ν, $\wp$ un idéal premier du corps R,

$$N(\wp) = p^{\rho},\ p \equiv 0 \pmod{\wp^{\varphi}},\ |p|_{\wp} = \wp^{\varphi}.$$

Soient d'ailleurs α et β deux nombres du corps R vérifiant les conditions

$$\alpha \equiv 1 \pmod{\wp^{k_1}},\ \beta \equiv 1 \pmod{\wp^{k_2}},\ k_2 \geqslant k_1 > \frac{\varphi}{p-1}. \tag{36}$$

Posons $a = \ln\alpha$, $b = \ln\beta$, $a \neq 0$, $b \neq 0$. Les nombres a et b sont complètement déterminés dans $R(\wp)$, l'extension $\wp$-adique du corps R, puisque

$$|\alpha - 1|_{\wp} = \wp^{-k_1},\ |\beta - 1|_{\wp} = \wp^{-k_2},\ k_2 \geqslant k_1 \geqslant 1.$$

D'ailleurs, comme

$$|n!|_{\wp} > \wp^{-n\frac{\varphi}{p-1}},\ \wp^{-k_1} \geqslant |a|_{\wp},$$

les séries

$$\alpha = e^a = \sum_0^{\infty} \frac{a^n}{n!},\ \beta = e^b = \sum_0^{\infty} \frac{b^n}{n!},\ \sqrt[n]{|a^n|_{\wp}} < \sqrt{\left|\frac{1}{n!}\right|_{\wp}} \tag{37}$$

convergeront (au sens $\wp$-adique) et

$$\left|\frac{a^n}{n!}\right|_{\wp} \leqslant 1,\ \left|\frac{b^n}{n!}\right|_{\wp} \leqslant 1,\ n = 0, 1, 2, \ldots$$

Il en résulte que les fonctions

$$\alpha^z = \sum_0^{\infty} \frac{a^n}{n!} z^n \ \text{et}\ \beta^z = \sum_0^{\infty} \frac{b^n}{n!} z^n$$

seront normales dans le corps $R(\wp)$ ainsi que la fonction

$$f(z)=\sum_{n_1=0}^{N}\sum_{n_2=0}^{N} A_{n_1n_2}\alpha^{n_1z}\beta^{n_2z}, \tag{38}$$

où tous les $A_{n_1n_2}$ sont des entiers rationnels.

Supposons encore que $\frac{\ln\alpha}{\ln\beta}$ est un nombre irrationnel au sens ordinaire. Pour les fonctions de cette nature on a le.

Lemme V. *Soit N un nombre entier, $N>N_0$, δ un nombre réel, $0<\delta<1$, On peut alors choisir les entiers rationnels A_{n_1,n_2}, $|A_{n_1,n_2}|\leqslant p^{[N^{2-\delta}]}$, p étant le nombre premier auquel appartient l'idéal premier $\wp$, de telle manière qu'ils ne soient pas nuls simultanément et que la fonction $f(z)$,*

$$f(z)=\sum_{n_1=0}^{N}\sum_{n_2=0}^{N} A_{n_1,n_2}\alpha^{n_1z}\beta^{n_2z}, \tag{39}$$

vérifie les inégalités

$$|f^{(\sigma)}(pt)|_\wp<\wp^{-\varphi[N^{2-\delta}\sqrt{\ln N}]} \tag{40}$$

pous tous les entiers rationnels σ et t,

$$0\leqslant\sigma\leqslant[N^{1+\delta}]+1,\quad 0\leqslant t\leqslant\left[\frac{N^{1-\delta}}{\ln N}\right]+2. \tag{41}$$

Pour démontrer ce lemme posons $r_1=[N^{1+\delta}]+1$, $r_2=\left[\frac{N^{1-\delta}}{\ln N}\right]+2$. Posons d'ailleurs $r_0=[N^{2-\delta}\sqrt{\ln N}]+1$ et

$$a_1=-\sum_{n=1}^{2\varphi N^2}\frac{(1-\alpha)^n}{n},\quad b_1=-\sum_{n=1}^{2\varphi N^2}\frac{(1-\beta)^n}{n},\quad a=\ln\alpha,\quad b=\ln\beta. \tag{42}$$

Il est évident que a_1 et b_1 seront des nombres algébriques du corps R et que d'ailleurs

$$|a-a_1|_\wp<\wp^{-\varphi N^2},\quad |b-b_1|_\wp<\wp^{-\varphi N^2}. \tag{43}$$

Posons

$$F_{s,t}=\sum_{n_1=0}^{N}\sum_{n_2=0}^{N} A_{n_1,n_2}(n_1a_1+n_2b_1)^s\alpha^{n_1pt}\beta^{n_2pt}. \tag{44}$$

Il suit alors des inégalités (42) que $s\geqslant 0$ et t étant des entiers rationnels arbitraires on a l'inégalité

$$|f^{(s)}(pt)-F_{s,t}|_\wp<\wp^{-\varphi N^2}, \tag{45}$$

où

$$f^{(s)}(pt)=\sum_{n_1=0}^{N}\sum_{n_2=0}^{N} A_{n_1,n_2}(n_1a+n_2b)^s\alpha^{n_1pt}\beta^{n_2pt}. \tag{46}$$

Faisons correspondre à chaque fonction $f(z)$, obtenue pour les nombres entiers rationnels A_{n_1,n_2}, $1\leqslant A_{n_1,n_2}\leqslant p^{[N^{2-\delta}]}$, r_1r_2 nombres algébriques $F_{s,t}$, $0\leqslant s\leqslant r_1-1$, $0\leqslant t\leqslant r_2-1$. Comme $1\leqslant A_{n_1,n_2}\leqslant p^{[N^{2-\delta}]}$ et $0\leqslant n_1\leqslant N$, $0\leqslant n_2\leqslant N$, nous aurons $p^{[N^{2-\delta}](N+1)^2}$ fonctions $f(z)$ différentes. Mais comme $N(\wp^{\varphi r_0})=p^{\rho\varphi r_0}$, tous les nombres du corps R, dont les dénominateurs ne se divisent pas par $\wp$, forment

$p^{\rho\varphi r_0}$ classes d'après le module $\wp^{\varphi r_0}$. Donc, pour des entiers rationnels A_{n_1,n_2} différents on peut obtenir au plus $p^{\rho\varphi r_0 r_1 r_2}$ fonctions $f(z)$, pour lesquelles parmi les $r_1 r_2$ nombres $F_{s,t}$ il y en a au moins un tel que ces nombres appartiennent à des classes différentes suivant le module $\wp^{\varphi r_0}$. Comme pour $N > N_0'(\delta)$ on a $[N^{1-\delta}](N+1)^2 > \rho\varphi r_0 r_1 r_2$, il en résulte que pour $N > N_0'$ il existe au moins deux fonctions $f_1(z)$ et $f_2(z)$ telles que toutes les valeurs $F_{s,t}^{(1)}$ et $F_{s,t}^{(2)}$ correspondantes appartiennent aux mêmes classes suivant le module $\wp^{\varphi r_0}$. Il en suit que pour la fonction $f(z) = f_1(z) - f_2(z)$ les coefficients A_{n_1,n_2} seront inférieurs à $p^{[N^{1-\delta}]}$ en valeur absolue et les valeurs $F_{s,t} = F_{s,t}^{(1)} - F_{s,t}^{(2)}$, $0 \leqslant s \leqslant r_1 - 1, 0 \leqslant t \leqslant$ $\leqslant r_2 - 1$, seront divisibles par $\wp^{\varphi r_0}$. Mais en vertu des inégalités (43) nous pouvons affirmer que $|f^{(s)}(pt)|_\wp < \wp^{-\varphi r_0}$, $N > N_0''$, donc la fonction choisie vérifie les conditions du lemme V.

Voici encore un lemme qui est une modification du lemme I.

L e m m e VI. *Soit $f(z)$ une fonction vérifiant les conditions du lemme* V, *q_1 et q_2 des entiers rationnels, $q = \max[|q_1|, |q_2|]$, $q \leqslant p^{[N^{1-2\delta}]}$, $0 < \delta < \frac{1}{2}$. Alors, quels que soient les entiers rationnels σ et $t \geqslant 0$, $0 \leqslant \sigma \leqslant [N^{1+\delta}]$, il existe des constantes $\lambda_0 > 0$ et $\lambda_1 > 0$ qui ne dépendent pas de N telles que pour $N > N_1$ ou bien*

$$Q_{\sigma,t} = \sum_{n_1=0}^{N} \sum_{n_2=0}^{N} A_{n_1,n_2}(n_1 q_1 + n_2 q_2)^\sigma \alpha^{n_1 pt} \beta^{n_2 pt} = 0 \tag{47}$$

ou bien

$$|Q_{\sigma,t}|_\wp > \wp^{-\lambda_0 N^{2-\delta} - \lambda_1 N t}. \tag{48}$$

Ce lemme est une conséquence immédiate du lemme I.

§ 5

Ces lemmes étant démontrés, nous pouvons démontrer maintenant le théorème fondamental:

T h é o r è m e I. *Soit R un corps algébrique d'ordre ν, $\wp$ son idéal premier appartenant au nombre premier p, $N(\wp) = p^\rho$, $|p|_\wp = \wp^{-\varphi}$, k_1 et k_2, $k_2 \geqslant k_1$, des entiers rationnels, $k_2 \geqslant k_1 > \frac{\varphi}{p-1}$, $\alpha \neq 1$, $\beta \neq 1$ des nombres du corps R, $|\alpha - 1|_\wp = \wp^{-k_1}$, $|\beta - 1|_\wp = \wp^{-k_2}$, q_1 et q_2, $(q_1, q_2) = 1$, des entiers rationnels, $q = \max[|q_1|, |q_2|]$. Alors, quel que soit $\varepsilon > 0$, l'inégalité*

$$\left| \frac{q_2}{q_1} - \frac{\ln\beta}{\ln\alpha} \right|_\wp < \wp^{-\ln^{3+\varepsilon} q}, \tag{49}$$

où $\ln\alpha$ et $\ln\beta$ sont déterminés au sens $\wp$-adique, ne possède qu'un nombre fini de solutions en nombres entiers q_1 et q_2, $(q_1, q_2) = 1$, s'il n'existe pas d'entiers rationnels n, m, $mn \neq 0$, tels que $\alpha^n = \beta^m$.

D é m o n s t r a t i o n. Remarquons d'abord que la condition $\alpha^n \neq \beta^n$, $mn \neq 0$, exclut le cas où α où bien β est une racine de l'unité. D'ailleurs, comme

$$|\ln\alpha|_\wp = \wp^{-k_1}, \quad |\ln\beta|_\wp = \wp^{-k_2}, \quad k_2 \geqslant k_1,$$

on a $|q_1|_\wp = 1$.

Supposons que pour un ε donné, $0 < \varepsilon < \frac{1}{2}$, l'inégalité (49) est vraie pour une infinité de nombres q_1, q_2 premiers entre eux, autrement dit, quelque grand que soit $q = \max[|q_1|, |q_2|]$.

Posons $\delta = \frac{\varepsilon}{12}$, $N = \left[\frac{\ln q}{\ln p}\right]^{\frac{1}{1-2\varepsilon}}$. Alors au lieu de l'inégalité (49) on peut écrire l'inégalité

$$\left|\frac{q_2}{q_1} - \frac{\ln \alpha}{\ln \beta}\right|_{\wp} < \wp^{-\varphi N^{3+\frac{\varepsilon}{2}}}, \quad N > N_2, \tag{50}$$

qui doit par hypothèse avoir lieu quelque grand que soit N.

Soit $N'_0 = \max[N_0, N_1, N_2]$. Alors, d'après le lemme V, on peut choisir des entiers A_{n_1, n_2}, $|A_{n_1, n_2}| \leqslant p^{[N^{2-\delta}]}$, non tous nuls de manière que la fonction $f(z)$ correspondante,

$$f(z) = \sum_{n_1=0}^{N} \sum_{n_2=0}^{N} A_{n_1, n_2} \alpha^{n_1 z} \beta^{n_2 z}, \tag{51}$$

vérifie les $r_1 r_2$ inégalités

$$|f^{(s)}(pt)|_{\wp} < \wp^{-\varphi [N^{2-\delta} \ln^{\frac{1}{2}} N]} \tag{52}$$

où $\delta = \frac{\varepsilon}{12}$ et

$$0 \leqslant s \leqslant r_1 - 1, \quad 0 \leqslant t \leqslant r_2 - 1, \quad r_1 = [N^{1+\delta}] + 1, \quad r_2 = \left[\frac{N^{1-\delta}}{\ln N}\right] + 2.$$

Nous allons considérer maintenant les nombres

$$Q_{s,t} = \sum_{n_1=0}^{N} \sum_{n_2=0}^{N} A_{n_1, n_2} (n_1 q_1 + n_2 q_2)^s \alpha^{n_1 pt} \beta^{n_2 pt}, \tag{53}$$

liés à la fonction $f(z)$ déjà construite. Il suit immédiatement de l'inégalité (50) que

$$|\ln^{-s}\alpha f^{(s)}(pt) - q_1^{-s} Q_{s,t}|_{\wp} < \wp^{-\varphi N^{3+\frac{\varepsilon}{2}}}, \tag{54}$$

quels que soient s et t entiers et non négatifs. Or, en vertu des inégalités (52) et (54) nous aurons pour $0 \leqslant s \leqslant r_1 - 1$ et $0 \leqslant t \leqslant r_2 - 1$ l'inégalité

$$|Q_{s,t}|_{\wp} < \max\left[\wp^{k_1 N^{1+\delta} - \varphi [N^{2-\delta} \sqrt{\ln N}]}, \quad \wp^{-N^{3+\frac{\varepsilon}{2}}}\right]. \tag{55}$$

D'après le lemme VI ou bien $Q_{s,t} = 0$ ou bien

$$|Q_{s,t}|_{\wp} > \wp^{-\lambda_0 N^{2-\delta} - \lambda_1 N^{2-\delta}}, \tag{56}$$

parce que $t \leqslant N^{1-\delta}$. Pour $N > N_3 \geqslant N'_0$ le second membre de l'inégalité (55) est inférieur au second membre de l'inégalité (56), autrement dit $Q_{s,t} = 0$, $0 \leqslant s \leqslant r_1 - 1$, $0 \leqslant t \leqslant r_2 - 1$. Il suit alors de l'inégalité (54) que $|f^{(s)}(pt)| < \wp^{-\varphi N^{3+\frac{\delta}{2}}}$.

En appliquant à la fonction $f(z)$ le lemme IV, nous obtenons immédiatement que pour $N > N'_3 \geqslant N_3$ on a

$$|f^{(\sigma)}(pt)|_{\wp} < \wp^{-\varphi \frac{N^2}{\ln N}}, \quad \sigma \leqslant r_1 - 1, \quad t \leqslant N^3, \tag{57}$$

parce que $\varphi N^2 \ln^{-1} N < N^{3+\frac{\varepsilon}{2}} - 16\varphi N^{1+\delta} \ln N$ pour $N > N'_3 \geqslant N_3$.

Dans la suite nous supposerons N, donc $f(z)$, fixes et $N > N_\tau$ où $\tau = \left[\frac{24}{\varepsilon}\right] + 16$; N_τ est plus grand que tous les N_t, N'_t, pour $t < \tau$. Pour cette fonction qui restera invariable dans la suite les inégalités (57) seront vérifiées.

Soit maintenant $s \leqslant r_1 - 1$, $0 \leqslant t \leqslant N^{1-\frac{\delta}{2}} + 1$. Alors, comme il résulte de (54) et (57) que $|Q_{s,t}|_{\wp} < \wp^{-\varphi \frac{N^2}{\ln N} + k_1 N^{1+\delta}}$, nous obtiendrons en vertu du lemme VI:

$$Q_{s,t} = 0, \quad 0 \leqslant s \leqslant r_1 - 1, \quad 0 \leqslant t \leqslant N^{1-\frac{\delta}{2}}.$$

En effet, pour $N > N_4$ on a

$$\varphi \frac{N^2}{\ln N} - k_1 N^{1+\delta} > \lambda_1 N (N^{1-\frac{\delta}{2}} + 3) + \lambda_0 N^{2-\delta} \tag{58}$$

et $N_\tau > N_4$. En vertu des inégalités (54) nous aurons donc

$$|f^{(s)}(pt)|_{\wp} < \wp^{-\varphi N^{3+\frac{\varepsilon}{2}}}, \quad 0 \leqslant s \leqslant r_1 - 1, \quad 0 \leqslant t \leqslant N^{1-\frac{\delta}{2}} + 1.$$

En appliquant encore une fois à $f(z)$ le lemme IV, nous aurons

$$|f^{(\sigma)}(pt)|_{\wp} < \wp^{-\varphi N^{2+\frac{\delta}{2}}}, \quad \sigma \leqslant r_1 - 1, \quad |t| < N^3, \tag{59}$$

puisque pour $N > N'_4$ on a

$$\varphi N^{2+\frac{\delta}{2}} < -16\varphi N^{1+\delta} \ln N + N^{3+\frac{\varepsilon}{2}} \tag{60}$$

et $N_\tau > N'_4 \geqslant N_4$.

Donc, en vertu de nos lemmes, nous avons obtenu en partant des inégalités (57) et (50) l'inégalité (59) et d'ailleurs $Q_{s,t} = 0$, $0 \leqslant s \leqslant r_1 - 1$, $0 \leqslant t \leqslant N^{1-\frac{\delta}{2}}$. Supposons maintenant que pour notre fonction $f(z)$ les inégalités suivantes sont vérifiées:

$$|f^{(\sigma)}(pt)|_{\wp} < \wp^{-\varphi N^{2+\frac{m\delta}{2}}}, \quad \sigma \leqslant r_1 - 1, \quad t \leqslant N^3; \tag{61}$$

m étant un entier rationnel, $1 \leqslant m < \frac{2+\varepsilon}{\delta} - 1$. Il suit alors de l'inégalité (54) que l'on a

$$|Q_{s,t}|_{\wp} < \wp^{-\varphi N^{2+\frac{m\delta}{2}} + k_1 N^{1+\delta}}, \tag{62}$$

où

$$0 \leqslant s \leqslant r_1 - 1, \quad 0 \leqslant t \leqslant N^{1+\frac{m-1}{2}\delta} + 2.$$

Mais pour les mêmes valeurs de s, t il suit du lemme VI que ou bien $Q_{s,t}=0$ ou bien

$$|Q_{s,t}|_{\wp}>\wp^{-\lambda_0 N^{2-\delta}-\lambda_1 N^{2+\frac{m-1}{2}\delta}-2\lambda_1}. \tag{63}$$

Comme pour $N>N_{4+m}$ le second membre de l'inégalité (62) est inférieur au second membre de l'inégalité (63) et comme $N>N_\tau>N_{4+m}$, on a $Q_{s,t}=0$, $0\leqslant s\leqslant r_1-1$, $0\leqslant t\leqslant N^{1+\frac{m-1}{2}\delta}$. Donc, en vertu de l'inégalité (54)

$$|f^{(s)}(pt)|_{\wp}<\wp^{-\varphi N^{3+\frac{\varepsilon}{2}}},\quad 0\leqslant s\leqslant r_1-1,\quad 0\leqslant t\leqslant N^{1+\frac{m-1}{2}\delta}+2. \tag{64}$$

Or, en posant $r_2=[N^{1+\frac{m-1}{2}\delta}]+2$ dans le lemme IV, nous aurons

$$|f^{(\sigma)}(pt)|_{\wp}\leqslant\wp^{-\varphi N^{2+\frac{m+1}{2}\delta}},\quad 0\leqslant\sigma\leqslant r_1-1,\quad t\leqslant N^3, \tag{65}$$

puisque pour $N>N'_{4+m}$ on a

$$N^{2+\frac{m+1}{2}\delta}<N^{3+\frac{\varepsilon}{2}}-16N^{1+\delta}\ln N \tag{66}$$

et $N>N_\tau>N'_{4+m}$.

Donc, si l'on suppose que toutes les inégalités (61) sont vérifiées pour $f(z)$, les inégalités (65) seront aussi vérifiées pour ces fonctions et d'ailleurs

$$Q_{s,t}=0,\quad 0\leqslant s\leqslant r_1-1,\quad 0\leqslant t\leqslant N^{1+\frac{m-1}{2}\delta}+2, \tag{67}$$

pour $1\leqslant m\leqslant\frac{2+\varepsilon}{\delta}-1$ et $N>N_\tau>\max[N_{4+m}, N'_{4+m}]$. Or, pour $m=1$ les inégalités (61) sont vraies, parce qu'elles coïncident avec l'inégalité (59), donc les inégalités (65) et les conditions (67) sont vraies pour chaque m, $m\leqslant\frac{2+\varepsilon}{\delta}-1$.

Choisissons maintenant le nombre entier m égal à $m=\left[\frac{24}{\varepsilon}\right]+11$, ce qui est possible puisque $\delta=\frac{\varepsilon}{12}$, donc

$$\left[\frac{24}{\varepsilon}\right]+11\leqslant\frac{12(2+\varepsilon)}{\varepsilon}-1. \tag{68}$$

Alors $1+\frac{m-1}{2}\delta\geqslant 2+\frac{3}{8}\varepsilon$. Donc, pour notre fonction $f(z)$ les conditions (67) sont vérifiées pour $0\leqslant s\leqslant r_1-1$, $0\leqslant t\leqslant N^{2+\frac{3}{8}\varepsilon}+1$, puisque $N>N_\tau$ et $N_\tau>\max[N_0, N'_0, \ldots, N_{m+4}, N'_{m+4}]$.

Mais les conditions (67) donnent un système d'équations homogènes par rapport aux $(N+1)^2-1$ inconnues A_{n_1,n_2}, $0\leqslant n_1\leqslant N$, $0\leqslant n_2\leqslant N$,

$$Q_{s,t}=\sum_{n_1=0}^{N}\sum_{n_2=0}^{N}A_{n_1,n_2}(\alpha^{n_1 p}\beta^{n_2 p})^t=0,\quad 0\leqslant t\leqslant(N+1)^2-2. \tag{69}$$

Le déterminant de ce système est celui de Vandermond, donc il ne peut s'annuler que si pour certaines valeurs de n_1, n_2, n'_1, n'_2, $(n_1-n'_1)^2+(n_2-n'_2)^2\neq 0$, on a

$\alpha^{n_1 p}\beta^{n_2 p}=\alpha^{n'_1 p}\beta^{n'_2 p}$. Cette dernière relation ne peut avoir lieu pour des entiers rationnels n_1, n_2, n'_1, n'_2, $(n_1-n'_1)^2+(n_2-n'_2)^2\neq 0$, puisque $\frac{\ln\alpha}{\ln\beta}$ serait dans ce cas rationnel et il est évident que l'inégalité (50) ne pourrait pas être vérifiée pour des q_1 et q_2 aussi grands que l'on veut. Le cas où α ou bien β est une racine de l'unité a été exclu par les conditions de notre théorème. Donc, le système d'équations linéaires (69) a un déterminant non nul, et par suite tous les A_{n_1, n_2} sont nuls, $0\leqslant n_1\leqslant N$, $0\leqslant n_2\leqslant N$, ce qui contredit à la condition de leur choix (lemme V). Ainsi le théorème I est démontré.

Démontrons maintenant deux théorèmes concernant la divisibilité de la différence des puissances par une puissance d'un idéal premier.

Théorème II. *Soit $\wp$ un idéal premier d'un corps algébrique R, α et β deux nombres de ce corps dont les numérateurs et les dénominateurs ne contiennent pas $\wp$. Supposons d'ailleurs que $\alpha^n\neq\beta^m$ si m et n sont des entiers rationnels et que $mn\neq 0$. Alors pour chaque $\varepsilon>0$ et $q>q_0(\alpha, \beta, \wp)$ la congurence*

$$\alpha^x\pm\beta^y\equiv 0 \pmod{\wp^{[\ln^{3+\varepsilon} q]}}, \tag{70}$$

où x et y sont des entiers rationnels et $q=\max[|x|, |y|]$, $|x|+|y|\neq 0$, est impossible.

Démonstration. Soit p le nombre entier rationnel premier auquel appartient l'idéal $\wp$, $N(\wp)=p^\rho$, $|p|_\wp=\wp^{-\theta}$ et ν le degré du corps R. Alors

$$\varphi(\wp^\lambda)=N(\wp^\lambda)\left[1-\frac{1}{N(\wp)}\right].$$

Sans restreindre la généralité de la démonstration nous pouvons supposer que la congruence (70) est vraie pour une infinité de x, y positifs, car dans le cas contraire on pourrait remplacer l'un des deux nombres α et β ou bien tous les deux par α^{-1} et β^{-1} et réduire notre théorème à ce cas. Soit $u=\varphi(\wp^\lambda)$ où $\lambda>\frac{2\rho\theta}{p-1}$ et λ est un entier. Alors, comme $|\alpha|_\wp=1$, $|\beta|_\wp=1$, on aura les égalités

$$|\alpha^u-1|_\wp=\wp^{-k_1},\quad |\beta^u-1|_\wp=\wp^{-k_2},\quad k_1\geqslant\lambda,\quad k_2\geqslant\lambda. \tag{71}$$

Supposons pour fixer les idées que $k_2\geqslant k_1$, parce que dans le cas contraire on pourrait changer le rôle de α et β. Soit $\alpha^u=\alpha_1$, $\beta^{-u}=\beta_1$ et $a=\ln\alpha_1$, $b=\ln\beta_1$, où les logarithmes sont définis au sens $\wp$-adique dans le corps $R(\wp)$, c'est-à-dire

$$a=\ln\alpha_1=-\sum_1^\infty\frac{(1-\alpha_1)^n}{n},\quad b=\ln\beta_1=-\sum_1^\infty\frac{(1-\beta_1)^n}{n}. \tag{72}$$

De l'égalité (72) et de la condition $k_2\geqslant k_1\geqslant\lambda>\frac{2\rho\theta}{p-1}$ nous obtenons immédiatement que $|a|_\wp=\wp^{-k_1}$, $|b|_\wp=\wp^{-k_2}$. En développant α_1^x et β_1^y en séries d'interpolation de Newton où les points d'interpolation sont 0, 1, 2, ..., nous aurons

$$\left.\begin{aligned} \alpha_1^x&=\sum_{n=0}^\infty\frac{(\alpha_1-1)^n}{n!}x(x-1)\dots(x-n+1),\\ \beta_1^y&=\sum_{n=0}^\infty\frac{(\beta_1-1)^n}{n!}y(y-1)\dots(y-n+1),\end{aligned}\right\} \tag{73}$$

où les séries convergent au sens $\wp$-adique pour $|x|_\wp \leqslant 1$, $|y|_\wp \leqslant 1$, puisque

$$|\beta_1 - 1|_\wp \leqslant |\alpha_1 - 1|_\wp \leqslant \wp^{-\lambda} < \wp^{-\frac{2\rho\theta}{p-1}} < \sqrt[n]{|n!|_\wp}, \tag{74}$$

et les fonctions qui se trouvent aux seconds membres des égalités (73) ont des valeurs algébriques ordinaires α_1^x et β_1^y quand x et y sont des entiers rationnels non négatifs.

En réunissant dans les seconds membres des égalités (73) les coefficients d'une même puissance de x et de y, nous verrons, après avoir fait des transformations faciles et tenu compte de la convergence uniforme et absolue des séries (73) au sens $\wp$-adique, que

$$\alpha_1^x = \sum_{n=0}^{\infty} \frac{(\ln \alpha_1)^n}{n!} x^n, \quad \beta_1^y = \sum_{n=0}^{\infty} \frac{(\ln \beta_1)^n}{n!} y^n, \tag{75}$$

où $\ln \alpha_1$ et $\ln \beta_1$ ont des valeurs que l'on prend des égalités (72), et que les seconds membres des égalités (75) ont des valeurs algébriques ordinaires α_1^x et β_1^y pour $x \geqslant 0$, $y \geqslant 0$, x et y étant des entiers rationnels. Mais comme

$$\alpha_1^x \beta_1^y - 1 = \sum_{n=1}^{\infty} \frac{(x \ln \alpha_1 + y \ln \beta_1)^n}{n!} \tag{76}$$

on a

$$\alpha_1^x \beta_1^y = 1 = (x \ln \alpha_1 + y \ln \beta_1) \left[1 + \sum_{n=2}^{\infty} \frac{(x \ln \alpha_1 + y \ln \beta_1)^{n-1}}{n!}\right], \tag{77}$$

où, puisque $\lambda > \frac{2\rho\theta}{p-1}$,

$$\left|1 + \sum_{n=2}^{\infty} \frac{(x \ln \alpha_1 + y \ln \beta_1)^{n-1}}{n!}\right|_\wp = 1 \tag{78}$$

pour $|x|_\wp \leqslant 1$, $|y|_\wp \leqslant 1$. Donc, x et y étant des entiers rationnels, $x \geqslant 0$, $y \geqslant 0$, on a

$$|\alpha_1^x \beta_1^y - 1|_\wp = |x \ln \alpha_1 + y \ln \beta_1|_\wp. \tag{79}$$

Supposons maintenant que la congruence (70) a lieu quelque grand que soit q. Nous verrons alors que pour des valeurs de q aussi grandes que l'on veut, u étant un nombre pair, on aura l'inégalité

$$|\alpha_1^x \beta_1^y - 1|_\wp = |x \ln \alpha_1 + y \ln \beta_1|_\wp < \wp^{-[\ln^{3+\varepsilon} q]} \tag{80}$$

pour $\varepsilon > 0$, $|x| > 0$, $|y| > 0$.

Il suit de cette dernière inégalité que

$$\left|\frac{x}{y} + \frac{\ln \beta_1}{\ln \alpha_1}\right| < \wp^{-[\ln^{3+\varepsilon} q] + 2k_1 + 2 \ln q} \tag{81}$$

où $\varepsilon > 0$ ne dépend pas de q et $q = \max[|x|, |y|]$. Ainsi pour $q > q_0(\alpha, \beta, \wp)$ nous aboutissons à une contradiction avec le théorème I, ce qui démontre le théorème II.

Remarquons que q_0 peut être calculé effectivement à partir de α, β et $\wp$.

Théorème II'. *Soit R un corps algébrique, $\wp$ son idéal premier, α et β deux nombres du corps R, dont les numérateurs et les dénominateurs ne sont* *pas divisibles par* $\wp$. *Supposons d'ailleurs que pour certains* m_1 *et* m_2 *entiers rationnels on a* $\alpha^{m_1}=\beta^{m_2}$.

Alors la congruence

$$\alpha^x \pm \beta^y \equiv 0 \ (\mathrm{mod}\ \wp^{+[\tau \ln q]}), \tag{82}$$

où $\tau > \tau_0(\alpha, \beta, \wp) > 0$, *x et y étant des entiers rationnels,* $\alpha^x - \beta^y \neq 0$ *et* $q = \max[|x|, |y|] > 1$, *ne peut avoir lieu quels que soient x et y.*

Remarquons d'abord que notre théorème est évident quand α et β sont des racines de l'unité. Considérons le cas où l'un de ces nombres est une racine de l'unité et l'autre ne l'est pas. Soit par exemple $\beta = e^{2\pi i \frac{k}{m}}$, α n'étant pas une racine de l'unité. Soit p le nombre premier auquel appartient l'idéal premier $\wp$, $N(\wp)=p^\rho$, $u = \varphi(\wp^\lambda) = N(\wp^\lambda)\left[1 - \frac{1}{N(\wp)}\right]$, $\lambda > \frac{2\varphi}{p-1}$ et $|p|_\wp = \wp^{-\varphi}$.

Il suit alors de la congruence (82) que nous supposerons vérifiée que l'on a

$$|\alpha^{mux} - 1|_\wp = \wp^{-[\tau \ln q]}. \tag{83}$$

Mais comme $\lambda > \frac{2\varphi}{p-1}$ et $|n!|_\wp > \wp^{-\frac{\varphi n}{p-1}}$, on a

$$|\alpha^{mux} - 1|_\wp = |x(\alpha^{mu} - 1)|_\wp \geqslant \wp^{-[\tau_0 \ln q]}, \quad q > 1,$$

où il est facile de déterminer τ_0. Donc, pour $\tau > \tau_0$ l'inégalité (83) ne peut avoir lieu.

Passons maintenant au cas où α et β ne sont pas des racines de l'unité, mais pour certaines valeurs des entiers m_1 et m_2 on a la relation $\alpha^{m_1} = \beta^{m_2}$ où $m_1 > 0$ a la plus petite valeur possible.

Alors $\alpha^{ux} - \beta^{uy} \neq 0$, où $u = \varphi(\wp^\lambda)$, $\lambda > \frac{2\varphi}{p-1}$, car dans le cas contraire le théorème serait déjà démontré.

On obtient de la condition $\alpha^{m_1} = \beta^{m_2}$ et de la congruence (82)

$$\left.\begin{aligned} |\alpha^{ux} - \beta^{uy}|_\wp = |x \ln \alpha^u - y \ln \beta^u|_\wp \leqslant \wp^{-[\tau \ln q]}, \\ m_1 \ln \alpha^u - m_2 \ln \beta^u = 0. \end{aligned}\right\} \tag{84}$$

Mais comme $xm_2 - ym_1 \neq 0$, $y > m_2$, car dans le cas contraire on aurait $\alpha^x - \beta^y = 0$, on obtient immédiatement des relations (84) que l'on a

$$|(xm_2 - ym_1) \ln \alpha^u|_\wp < \wp^{-[\tau \ln q]} \tag{85}$$

pour $\tau > \tau_0(\alpha, \beta, \wp)$, ce qui est impossible.

Théorème III. *Si* α *et* β *sont des nombres algébriques, x et y des entiers rationnels,* $q = \max[x \ln |\alpha|, |y \ln |\beta|]$, *on a pour* $q_1 = q_0(\alpha, \beta, \varepsilon)$ *l'inégalité*

$$|\alpha^x \pm \beta^y| > e^{q - \ln^{3+\varepsilon} q_1}, \quad q_1 = \max[|x|, |y|], \tag{86}$$

où l'on a supposé $\alpha^x \pm \beta^y \neq 0$ *et* $\varepsilon > 0$ *est arbitraire. On exclut le cas où* $\alpha = e^{i\varphi_1}$, $\beta = e^{i\varphi_2}$ *et il n'existe aucune relation linéaire à coefficients entiers entre les nombres* φ_1, φ_2 *et* π.

La démonstration de cette proposition est basée sur l'inégalité [4]

$$|x \ln \alpha - y \ln \beta| > e^{-\ln^{3+\varepsilon} q_1} \tag{87}$$

---

[4] Voir note [1].

où x et y sont des entiers rationnels, $q_1 = \max[|x|, |y|]$, α et β sont des nombres algébriques et d'ailleurs $\frac{\ln \alpha}{\ln \beta}$ est irrationnel. On démontre cette inégalité presque par la même méthode que l'inégalité (49). Une démonstration détaillée se trouve dans l'article déjà cité.

Supposons que $\frac{\ln|\alpha|}{\ln|\beta|}$ est irrationnel. Nous aurons donc, en supposant pour fixer les idées que $|\alpha^x| > |\beta^y|$, l'inégalité

$$|\alpha^x \pm \beta^y| = |\alpha^x| \cdot |e^{y \ln \beta - x \ln \alpha} \pm 1| \geqslant$$
$$\geqslant |\alpha^x| [1 - e^{-|x \ln|\alpha| - y \ln|\beta||}] \geqslant |\alpha^x| \min \left[\frac{1}{3}, |x \ln|\alpha| - y \ln|\beta||\right] \quad (88)$$

d'où résulte l'inégalité (86).

Supposons maintenant que $\frac{\ln|\alpha|}{\ln|\beta|}$ est rationnel. Alors $\alpha = \rho^m e^{i\varphi_1}$, $\beta = \rho^n e^{i\varphi_2}$, $m = m_1 d$, $n = n_1 d$, $\rho \neq 1$. Si $mx \neq ny$, ce cas se réduit évidemment au précédent, parce que les inégalités (88) restent vraies et $|x|\ln\alpha| - y|\ln\beta|| > |\ln\rho|$. C'est pourquoi nous allons considérer le cas où $mx = ny$, c'est-à-dire $x = n_1 z$, $y = m_1 z$, où z est un entier. Alors, en posant $\alpha^{n_1}\beta^{-m_1} = e^{i\varphi}$, on a

$$|\alpha^x \pm \beta^y| = |\beta^y| \left|1 \pm \left(\frac{\alpha^{n_1}}{\beta^{m_1}}\right)^z\right| > |\beta^y| \min\left[\frac{1}{4}, \left|\frac{z \ln e^{i\varphi} - k \ln e^{\pi i}}{i}\right|\right]. \quad (89)$$

Notre théorème en résulte en vertu de l'inégalité (87) si $\frac{\varphi}{\pi}$ est irrationnel et immédiatement si $\frac{\varphi}{\pi}$ est rationnel. Le cas où $|\alpha| = 1$ et $|\beta| \neq 1$ ou inversement est évident quand $y \neq 0$ et se réduit au précédent [inégalité (89)] quand $y = 0$.

Il reste à considérer un seul cas, celui où $\alpha = e^{i\varphi_1}$, $\beta = e^{i\varphi_2}$, et pour certaines valeurs des entiers n_1, n_2, n_3 non tous nuls, on a la relation $\varphi_1 n_1 + \varphi_2 n_2 + \pi n_3 = 0$. Alors, en supposant par exemple que $n_3 \neq 0$, on obtient

$$|\alpha^x - \beta^y| > \min\left[\frac{1}{4}, |x\varphi_1 + y\varphi_2 + k\pi|\right] =$$
$$= \min\left[\frac{1}{4}, \frac{1}{n_3} |(n_3 x - n_1 k)\varphi_1 - (n_3 y + n_2 k)\varphi_2|\right], \quad (90)$$

où $|k| < |x\varphi_1 - y\varphi_2|$. En vertu de l'inégalité (87) on en déduit le théorème que nous voulions démontrer.

§ 6

Le trois théorèmes obtenus peuvent être appliqués à l'étude de l'équation $\alpha^x + \beta^y = \gamma^z$, où α, β et γ sont algébriques, x, y et z sont des entiers rationnels.

Théorème IV. *Soient α, β et γ des nombres algébriques du corps R, dont aucun n'est égal à* 0, 1 *ou* —1, *ils sont tous réels et au moins l'un d'eux n'est pas une unité algébrique. Alors l'équation*

$$\alpha^x + \beta^y = \gamma^z \quad (91)$$

n'a qu'un nombre fini de solutions en entiers rationnels x, y et z sauf le cas où

$$\alpha = \pm 2^{n_1}, \quad \beta = \pm 2^{n_2}, \quad \gamma = \pm 2^{n_3}, \quad (92)$$

où n_1, n_2 et n_3 sont des nombres rationnels.

Démonstration. Supposons que l'équation (91) a une infinité de solutions en entiers rationnels x, y et z. Sans restreindre la généralité de la démonstration on peut supposer que l'équation (91) a une infinité de solutions en x, y, z non négatifs, car pour réduire à ce cas il aurait suffi de remplacer dans l'équation (91) possédant une infinité de solutions l'un ou plusieurs des nombres α, β et γ par α^{-1}, β^{-1}, γ^{-1}. Donc, nous allons supposer que l'équation (91) a une infinité de solutions en x, y et z entiers et non négatifs. Quelles que soient ces solutions (x, y, z) de l'équation (91), pour chacune de ces solutions l'une des six relations suivantes doit être vérifiée:

$$\left.\begin{array}{lll} |\alpha|^x \geqslant |\beta|^y \geqslant |\gamma|^z, & |\beta|^y \geqslant |\alpha|^x \geqslant |\gamma|^z, & |\gamma|^z \geqslant |\alpha|^x \geqslant |\beta|^y, \\ |\alpha|^x \geqslant |\gamma|^z \geqslant |\beta|^y, & |\beta|^y \geqslant |\gamma|^z \geqslant |\alpha|^x, & |\gamma|^z \geqslant |\beta|^y \geqslant |\alpha|^x. \end{array}\right\} \tag{93}$$

Comme il existe une infinité de solutions (x, y, z), l'une au moins des inégalités (93) a lieu pour une infinité de solutions (x, y, z) de l'équation (91). Supposons par exemple que ce soit

$$|\beta|^y \geqslant |\gamma|^z \geqslant |\alpha|^x. \tag{94}$$

En vertu des conditions de notre théorème $|\alpha| \neq 1$, $|\beta| \neq 1$ et $|\gamma| \neq 1$, parce que α, β et γ sont réels. Remarquons d'abord qu'en vertu de $|\alpha| \neq 1$, $|\beta| \neq 1$ et $|\gamma| \neq 1$ et de l'équation (91) le cas où, dans la suite infinie des solutions (x, y, z), l'une des variables croît indéfiniment et les deux autres sont bornées est exclu. Donc, deux des trois variables x, y et z croissent indéfiniment. Mais il suit immédiatement du théorème III que la troisième variable doit aussi croître indéfiniment, parce que, $u \neq \pm 1$ et $v \neq \pm 1$ étant réels, algébriques et $m > 0$, $n > 0$ croissant indéfiniment, la différence $u^n \pm v^n$ doit croître ou décroître indéfiniment en vertu de l'inégalité (86). Donc, notre suite infinie de solutions (x, y, z) jouit de cette propriété que, $A > 0$ étant quelconque, il n'existe qu'un nombre fini de solutions pour lesquelles au moins l'une des inégalités $x < A$, $y < A$ ou bien $z < A$ est vérifiée. Soit donc $\{(x, y, z)\}$ une suite infinie de solutions de l'équation (91) pour lesquelles l'inégalité (94) est vérifiée et supposons d'ailleurs que pour toutes ces solutions on a $x > A$, $y > A$, $z > A$, A étant assez grand pour qu'en vertu du théorème III on ait les inégalités

$$|\beta^y + \alpha^x| > |\beta|^y e^{-\ln^{\frac{13}{4}} y}, \quad |\beta^y - \gamma^z| > |\beta|^y e^{-\ln^{\frac{13}{4}} y}. \tag{95}$$

Ces inégalités suivent immédiatement de l'inégalité (86) du théorème III.

On obtient immédiatement des inégalités (94) et (95) les inégalités

$$\left.\begin{array}{l} y \ln|\beta| \geqslant z \ln|\gamma| \geqslant x \ln|\alpha|, \\ z \ln|\gamma| > y \ln|\beta| - \ln^{\frac{13}{4}} y, \\ x \ln|\alpha| > y \ln|\beta| - \ln^{\frac{13}{4}} y, \end{array}\right\} \tag{96}$$

d'où il résulte immédiatement que

$$z = \frac{\ln|\beta|}{\ln|\gamma|}\,y + \frac{\theta_1}{\ln|\gamma|}\ln^{3+\frac{1}{4}} y,\quad x = \frac{\ln|\beta|}{\ln|\alpha|}\,y + \frac{\theta_2}{\ln|\alpha|}\ln^{3+\frac{1}{4}} y, \tag{97}$$

où $|\theta_1| \leqslant 1$, $|\theta_2| \leqslant 1$.

D'après les conditions de notre théorème l'un au moins des nombres, α, β ou γ n'est pas une unité algébrique. Soit γ, par exemple, ce nombre. Donc, il existe au moins un idéal premier du corps R qui appartient ou bien au numérateur, ou bien au dénominateur de γ, autrement dit $|\gamma|_{\wp} = \wp^{k_3}$ où k_3 n'est pas nul. Supposons k_3 négatif, c'est-à-dire supposons que γ soit divisible par $\wp^{-k_3}$. Alors l'hypothèse que $|\alpha|_{\wp} = 1$ et $|\beta|_{\wp} = 1$ nous conduit à une contradiction avec le théorème II ou II', parce que dans ce cas d'une part

$$|\alpha^x + \beta^y|_{\wp} > \wp^{-\ln^{3+\frac{1}{4}} x},\quad x > x_0,\quad y > y_0, \tag{98}$$

et d'autre part, en vertu de l'équation (91) et des relations (97),

$$|\alpha^x + \beta^y|_{\wp} = \wp^{k_3 z} \leqslant \wp^{-\lambda x},\quad x > x_0, \tag{99}$$

où $\lambda > 0$.

Dans le cas où $k_3 > 0$ il est tout à fait évident que $\wp$ doit entrer en puissance négative en l'un des nombres α ou β. Donc, si $|\gamma|_{\wp} = \wp^{-k_3}$, on a $|\alpha|_{\wp} = \wp^{-k_1}$, $|\beta|_{\wp} = \wp^{-k_2}$ et l'un au moins des nombres k_1 ou k_2 est non nul. Ainsi nous pouvons poser $|\alpha|_{\wp} = \wp^{-k_1}$, $|\beta|_{\wp} = \wp^{-k_2}$ et $|\gamma|_{\wp} = \wp^{-k_3}$ et d'ailleurs affirmer que parmi les trois nombres k_1, k_2 et k_3 deux nécessairement diffèrent de zéro. Il suit alors de l'équation (91) que

$$\left.\begin{aligned} \wp^{-k_3 z} &\leqslant \max[\wp^{-k_1 x},\ \wp^{-k_2 y}], \\ \wp^{-k_2 y} &\leqslant \max[\wp^{-k_3 z},\ \wp^{-k_1 x}], \\ \wp^{-k_1 x} &\leqslant \max[\wp^{-k_2 y},\ \wp^{-k_3 z}], \end{aligned}\right\} \tag{100}$$

d'où il résulte que pour chaque solution (x, y, z) l'une au moins des trois relations

$$k_3 z \geqslant k_2 y = k_1 x,\quad k_2 y \geqslant k_3 z = k_1 x,\quad k_1 x \geqslant k_2 y = k_3 z \tag{101}$$

doit être vérifiée. Comme pour chacune des solutions vérifiant les relations (97) l'une au moins des inégalités (101) est vérifiée, il est évident que l'une de ces relations doit être vérifiée pour une infinité de solutions.

Supposons que ce soit $k_1 x \geqslant k_3 z = k_2 y$. En posant $k_3 = dn_3$, $k_2 = dn_2$ et en remarquant que d a le même signe que k_2 et $(n_3, n_2) = 1$, nous voyons que $y = n_3 t$, $z = n_2 t$. En comparant ces relations avec les égalités (97), nous obtenons

$$n_2 t \ln|\gamma| = n_3 t \ln|\beta| + \theta \ln^{3+\frac{1}{4}} n_3 t,\quad |\theta| \leqslant 1, \tag{102}$$

et cette relation doit être vraie pour des valeurs de t aussi grandes que l'on veut. Cela n'est possible que dans le cas où $n_2 \ln|\gamma| = n_3 \ln|\beta|$ ou bien $\gamma^{n_2} = \pm\beta^{n_3}$. En posant $\gamma^{n_2} = \delta$ nous obtenons de l'équation (91) l'égalité

$$\alpha^x = 2\delta^t \tag{103}$$

et cette relation doit avoir lieu pour une infinité de x et t positifs.

Si l'on suppose que δ est une unité algébrique il en résulte que α ne peut pas être une unité algébrique. Mais ceci est impossible parce que 2 ne peut contenir une puissance aussi grande que l'on veut d'un idéal premier. Soit donc $\wp$ un idéal premier qui entre dans δ et $|\delta|_{\wp}=\wp^{-m_1}$. Alors en posant $|2|_{\wp}=\wp^{-a}$ et $|\alpha|_{\wp}=\wp^{-m_2}$, nous obtenons $xm_2=a+tm_1$ et cette équation doit avoir des solutions pour des valeurs de x et t aussi grandes que l'on veut.

Alors $t=t_0+m'_1v$, $x=x_0+m'_2v$ où l'on a posé $(a, m_1, m_2)=d$, $m_1=m'_1d$, $m_2=m'_2d$ et $a=a'd$. En substituant les valeurs de t et x dans l'équation (103), nous obtenons

$$2\delta^{t_0}\alpha^{-x_0}=[\alpha^{m'_2}\delta^{-m'_1}]^v \tag{104}$$

et cette égalité doit avoir lieu pour des valeurs de v aussi grandes que l'on veut. Il en resulte que

$$\alpha^{m'_2}=\pm\delta^{m'_1},\quad 2\delta^{t_0}=\pm\alpha^{x_0}, \tag{105}$$

parce que α et δ sont réels. Mais on peut obtenir immédiatement de ces deux relations que

$$\alpha=\pm 2^{\frac{m'_1}{x_0m'_1-t_0m'_2}},\quad \delta=\pm 2^{\frac{m'_2}{x_0m'_1-t_0m'_2}}. \tag{106}$$

Ceci démontre notre théorème. La borne pour $|x|$, $|y|$ et $|z|$ peut être trouvée effectivement, ce qui suit des raisonnements précédents.

Corollaire. *Si* β, α *et* γ *sont des nombres rationnels*, $\alpha\beta\gamma\neq 0$, $|\alpha|\neq 1$, $|\beta|\neq 1$, $|\gamma|\neq 1$, *l'équation*

$$\alpha^x+\beta^y=\gamma^z \tag{107}$$

ne peut avoir une infinité de solutions en entiers rationnels (x, y, z) *que dans le cas où*

$$\alpha=\pm 2^{n_1},\quad \beta=\pm 2^{n_2},\quad \gamma=\pm 2^{n_3}, \tag{108}$$

n_1, n_2, n_3 *étant des entiers rationnels.*

De même que le théorème IV on peut démontrer un théorème plus général:

Théorème V. *Soient* α, β *et* γ *des nombres algébriques dont aucun n'est égal ni à zéro, ni à une racine de l'unité et dont l'un au moins n'est pas une unité algebrique. Alors l'équation*

$$\alpha^x+\beta^y=\gamma^z \tag{109}$$

ne peut avoir une infinité de solutions en entiers rationnels x, y *et* z *que dans le cas où*

$$\beta=(\eta_1\alpha)^{k_1},\quad \gamma=(\eta_2\alpha)^{k_2}, \tag{110}$$

η_1 *et* η_2 *étant des unités algébriques*, k_1 *et* k_2 — *des nombres rationnels.*

(Поступило в редакцию 3/XI 1939 г.)

О делимости разности степеней целых чисел на степень простого идеала

А. О. Гельфонд (Москва)

(Резюме)

Пользуясь нормальными функциями $\wp$-адического переменного, я доказываю, что, каково бы ни было $\varepsilon > 0$, сравнение

$$\alpha^n \pm \beta^m \equiv 0 \ (\mathrm{mod}\, \wp^{\ln^{3+\varepsilon} q}),$$
$$q = \max[|x|, |y|],$$

где m и n — целые числа, α и β — алгебраические числа тела R, $\wp$ — простой идеал тела R, не входящий в числители и знаменатели α и β, невозможно при $q > q_0(\varepsilon)$.

Пользуясь этим утверждением, а также одним неравенством, показывающим, что отношение логарифмов алгебраических чисел в том случае, когда оно иррационально, плохо приближается рациональными дробями, я доказываю следующую теорему:

Уравнение

$$\alpha^x + \beta^y = \gamma^z,$$

где α, β и γ — алгебраические действительные числа, отличные от нуля и ± 1, и по крайней мере одно из них не есть алгебраическая единица, может иметь только конечное число решений в целых числах x, y и z за исключением того случая, когда

$$\alpha = \pm 2^{n_1}, \quad \beta = \pm 2^{n_2}, \quad \gamma = \pm 2^{n_3},$$

где n_1, n_2 и n_3 — рациональные числа.