Propriétés additives. I.

Par

J. G. van der Corput (Groningen).

§ 1. Introduction.

La théorie additive des nombres est la partie de la susdite science dans laquelle l'addition est ou bien la seule ou bien la principale opération figurant dans les problèmes. Le problème le plus important qui se présente dans ce domaine est la question de savoir quels nombres peuvent être écrits comme la somme de deux ou plus de deux termes possédant une propriété donnée; on peut se demander en outre de combien de manières différentes un nombre donné peut être écrit sous cette forme. Par exemple la proposition de Landau que tout entier assez grand est la somme de huit cubes positifs, appartient à la théorie additive des nombres malgré le fait que la notion d'un cube s'appuie sur la multiplication et non sur l'addition. Le théorème de Vinogradow que tout entier suffisamment grand est la somme de trois nombres premiers, montre un phénomène analogue. Ce théorème est également considéré comme appartenant à la théorie additive des nombres, quoique la notion de nombre premier, qui est définie par des propriétés de divisibilité, n'appartienne pas strictement à cette théorie.

Dans le second paragraphe de cette communication je déduirai trois théorèmes qui sont fondamentaux pour la théorie additive des nombres et que j'appellerai respectivement les théorèmes A, B et C. Chacune de ces propositions se rattache à une certaine classe de problèmes que je désignerai par la même lettre; la classe A est formée par les problèmes qu'on peut traiter avec le théorème A, etc. Je diviserai chacune de ces trois classes en trois catégories, que je distinguerai par I, II et III. Par exemple C I est la première catégorie de la classe C. Considérons d'abord les neuf catégories de problèmes, ainsi obtenues.

A I. Soit $\psi(y_1,\dots,y_s)$ un polynome qui prend des valeurs entières pour toutes les valeurs entières des nombres $y_1,\dots,y_s$. Posons d'abord la question quels sont les nombres t qui peuvent être écrits sous la forme

$$\psi(y_1,\dots,y_s)=t, \tag{1}$$

où $(y_1,\dots,y_s)$ désigne un point à coordonnées entières appartenant à un certain domaine Y et vérifiant les congruences

$$y_\sigma \equiv u_\sigma \pmod{U_\sigma} \quad (\sigma=1,\dots,s),$$

u_σ et $U_\sigma>0$ étant des entiers donnés. Considérons encore un problème plus général. Introduisons deux nombres naturels m et n, en outre mn entiers $b_{\mu\nu}$ et n nombres naturels s_ν où μ parcourt le système $1,2,\dots,m$ tandis que ν parcourt le système $1,2,\dots,n$. Introduisons ensuite n polynomes $\psi_\nu(y_{\nu1},\dots,y_{\nu,s_\nu})$ $(\nu=1,\dots,n)$, qui prennent des valeurs entières pour toutes les valeurs entières de $y_{\nu1},\dots,y_{\nu,s_\nu}$. Je considère comme appartenant aussi à la catégorie A I le problème de savoir quels systèmes $t=(t_1,\dots,t_m)$ peuvent être écrits sous la forme

$$\sum_{\nu=1}^{n} b_{\mu\nu}\psi_\nu(y_{\nu1},\dots,y_{\nu,s_\nu})=t_\mu \quad (\mu=1,\dots,m), \tag{2}$$

où $(y_{\nu1},\dots,y_{\nu,s_\nu})$ est un point appartenant à un domaine donné Y_ν et pour lequel on a

$$y_{\nu\sigma}\equiv u_{\nu\sigma} \pmod{U_{\nu\sigma}}, \tag{3}$$

$(\nu=1,\dots,n;\ \sigma=1,\dots,s_\nu)$, $u_{\nu\sigma}$ et $U_{\nu\sigma}>0$ désignant des entiers donnés.

A II. Nous posons les mêmes questions que dans A I, mais maintenant nous imposons aux nombres $y_{\nu1},\dots,y_{\nu,s_\nu}$ la condition d'être des nombres premiers. Le théorème de Vinogradow que tout nombre impair assez grand est la somme de trois nombres premiers, appartient à cette catégorie. De même la proposition que tout nombre impair est la somme de deux nombres premiers diminuée d'un nombre premier. Dans les catégories A II, B II et C II je supposerai que $u_{\nu\sigma}$ soit premier avec $U_{\nu\sigma}$ et que $y_{\nu\sigma}$ soit $\geqslant 2$ pour tout point $(y_{\nu1},\dots,y_{\nu,s_\nu})$ appartenant à Y_ν.

A III. Cette catégorie est une combinaison des deux précédentes. Je partage les $s_1+\ldots+s_n$ couples (ν, σ), où ν parcourt le système $1, \ldots, n$, et σ le système $1, \ldots, s_\nu$ en deux familles et j'exige que pour un couple de la première famille $y_{\nu\sigma}$ soit un nombre premier. Je suppose pour chaque couple (ν, σ) de la première famille que $u_{\nu\sigma}$ soit premier avec $U_{\nu\sigma}$ et que $y_{\nu\sigma}$ soit $\geqq 2$ pour tout point $(y_{\nu 1}, \ldots, y_{\nu s_\nu})$ appartenant à Y_ν.

Si la première famille ne contient aucun couple, on retrouve la catégorie A I, et s'il n'y a aucun couple dans la seconde, on obtient A II. Les propositions que chaque entier assez grand est la somme de deux nombres premiers augmentée d'un carré, et que chaque entier peut être écrit d'une infinité de manières comme la somme de deux nombres premiers diminuée d'un carré, appartient à la catégorie A III.

B I. Considérons encore la relation (1). Introduisons un entier $X \geqq 3$ et cherchons une règle qui nous permette de décider pour beaucoup de nombres naturels $t \leqq X$, s'ils peuvent être écrits sous la forme (1) ou non. Il n'est pas nécessaire que cette règle soit valable pour tous les nombres naturels $t \leqq X$, mais j'exige que le nombre des exceptions soit petit par rapport à X, c'est-à-dire, $N'(X)$ désignant le nombre des nombres naturels $t \leqq X$, auxquels la règle trouvée n'est pas applicable, j'exige que $\frac{N'(X)}{X}$ tend vers zéro, si X croît indéfiniment. Cela étant, je dis que la règle vaut pour presque chaque nombre naturel $t \leqq X$. Mais j'exige plus, à savoir qu'à tout nombre Ω indépendant de X corresponde un nombre c_1 indépendant de X tel que $N'(X)$ soit inférieur à $c_1 X (\log X)^{-\Omega}$. J'exprimerai ce fait en disant que cette règle vaut pour à peu près (dans le sens faible) chaque nombre naturel $\leqq X$.

Parlons plus amplement de cette notion „à peu près" (en allemand: nahezu; en anglais: nearly; en néerlandais: vrijwel). Partout dans cet article je parlerai de certaines quantités que j'appellerai fixes. Quand je dis dans une assertion qu'il existe un nombre fixe avec une certaine propriété, je veux dire qu'il est possible de trouver un nombre qui possède cette propriété et qui est défini univoquement par les nombres fixes déjà nommés. Par exemple pour tout nombre fixe positif ε et pour tout nombre naturel t le nombre des diviseurs de t est inférieur à $c_2 t^\varepsilon$, où c_2 est fixe. Dans ce cas „fixe" veut dire: indépendant de t.

La notation $\beta \prec\prec \gamma$, introduite par M. Vinogradow, veut dire qu'il existe un nombre positif fixe c_3 tel qu'on ait $|\beta| \leqq c_3 |\gamma|$.

Partout dans cet article figurera un entier $X \geqq 3$, qui n'est pas fixe; je désignerai $\log X$ par x. Je dis qu'à peu près (dans le sens faible) chaque élément d'un système possède une certaine propriété si pour tout nombre fixe Ω le nombre des éléments du système qui ne possèdent pas cette propriété, est $\prec\prec N x^{-\Omega}$, où N désigne le nombre total des éléments du système.

Avec cette nouvelle notion nous pouvons énoncer le problème cité ci-dessus de la manière suivante: on demande une règle qui nous permette de décider pour à peu près (dans le sens faible) chaque nombre naturel $t \leqq X$, si un tel nombre peut être écrit sous la forme (1) ou non; dans cette forme $(y_1, \ldots, y_s)$ est un point situé dans un certain domaine et dont les coordonnées satisfont à certaines congruences.

De la même manière on étudie le système (2). On demande une règle qui décide pour à peu près (dans le sens faible) chaque système t, formé par m nombres naturels $t_\mu \leqq X$, si un tel système peut être mis sous la forme (2) ou non.

Je dis qu'à peu près (dans le sens fort) chaque élément d'un système possède une certaine propriété s'il existe un nombre positif fixe ω tel que le nombre des éléments, qui ne possèdent pas cette propriété, soit $\prec\prec N X^{-\omega}$, où N désigne le nombre total des éléments du système. Exemple: à peu près (dans le sens fort) chaque nombre naturel $\leqq X$ est la somme de cinq cubes positifs; à peu près (dans le sens faible) chaque nombre naturel $\leqq X$ est la somme des cubes de cinq nombres premiers.

B II. Nous posons les mêmes questions que dans B I, mais maintenant nous exigeons en outre que les entiers $y_1, \ldots, y_s$, respectivement $y_{\nu\sigma}$ $(\nu = 1, \ldots, n;\ \sigma = 1, \ldots, s_\nu)$ soient des nombres premiers. Le théorème qu'à peu près (dans le sens faible) chaque nombre positif pair $\leqq X$ est la somme de deux nombres premiers, appartient à cette catégorie.

B III. Nous partageons encore les couples (ν, σ) en deux familles et nous exigeons pour un couple de la première famille que $y_{\nu\sigma}$ soit premier et appartienne à une progression arithmétique donnée. Cette catégorie contient par exemple la proposition qu'à peu près (dans le sens faible) chaque nombre naturel $\leqq X$ est égal à un nombre premier, augmenté d'un carré; également le théorème qu'à peu près (dans le sens faible) chaque nombre naturel $\leqq X$ est un nombre premier, diminué d'un cube.

C I. Etudions encore (1). Dans la classe C nous ne considérons pas tous les nombres naturels $t \leqq X$, mais seulement ceux qui appartiennent à une suite donnée. Dans cette classe nous cherchons une règle qui nous permette de décider pour à peu près chaque nombre naturel $t \leqslant X$ appartenant à cette suite, si un tel nombre possède la forme (1) ou non, $(y_1, \ldots, y_s)$ désignant un point du domaine Y, à coordonnées entières satisfaisant à certaines congruences. Le même problème se présente dans l'étude du système (2), si nous considérons seulement les nombres naturels $t_\mu \leqslant X$ appartenant à des suites données.

C II et C III. Ces deux catégories sont analogues à la catégorie précédente, mais maintenant nous exigeons que toutes ou certaines des inconnues soient des nombres premiers. C II par exemple contient la proposition qu'à peu près (dans le sens faible) chaque carré pair $\leqq X$ est la somme de deux nombres premiers; le nombre des carrés pairs $\leqslant X$ qui ne possèdent pas cette forme, est donc par exemple $<< \sqrt{X}\, x^{-100}$. La catégorie C III renferme le théorème qu'à peu près (dans le sens faible) chaque puissance cinquième $\leqq X$ qui n'est pas égale à un multiple de 8 augmenté de 0, 1 ou 5, peut être écrite comme la somme de deux nombres premiers impairs, augmentée de deux carrés impairs; le nombre des exceptions est donc par exemple $<< X^{\frac{1}{5}} x^{-1000}$. Il va sans dire que les nombres qui sont égaux à un multiple de 8 augmenté de 0, 1 ou 5, n'entrent pas en considération.

Notre première tâche sera de chercher un énoncé qui nous permette d'appliquer des méthodes analytiques. Je vais d'abord expliquer par un problème particulier de quelle manière cela peut se faire. Le nombre des manières d'écrire un entier $t \geqslant 4$ comme la somme de deux nombres premiers impairs est égal à

$$L(t) = \sum_{v+v'=t} r(v)\, r'(v'), \tag{4}$$

étendu aux paires d'entiers $v \geqslant 3$ et $v' \geqslant 3$, dont la somme vaut t; dans cette formule $r(v) = r'(v)$ est égal à 1 ou 0, selon que v est premier ou non.

Si $L(t)$ est positif, t est la somme de deux nombres premiers impairs. La question de savoir si t est la somme de deux nombres premiers impairs revient donc à celle de savoir si $L(t)$ est positif ou non. Nous ne savons pas encore, si $L(t)$ est positif pour tout nombre pair $t \geqslant 4$, mais nous avons démontré qu'il en est ainsi pour à peu près (dans le sens faible) tout nombre positif pair $\leqslant X$. Nous savons même plus: ζ désignant un nombre fixe quelconque, on a pour à peu près (dans le sens faible) chaque nombre positif pair $t \leqslant X$

$$L(t) = \left(1 + \frac{\Theta}{(\log t)^{\zeta}}\right) Z(t)\, \Lambda(t), \tag{5}$$

où $|\Theta| < 1$ et

$$\Lambda(t) = \sum_{v+v'=t} \rho(v)\, \rho'(v'), \tag{6}$$

étendu aux paires d'entiers $v \geqslant 3$ et $v' \geqslant 3$ dont la somme égale t; dans cette formule nous avons posé

$$\rho(v) = \rho'(v) = \frac{1}{\log v};$$

$$Z(t) = K \prod_{\substack{p \mid t \\ p>2}} \frac{p-1}{p-2} \quad \text{et} \quad K = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right), \tag{7}$$

où le premier produit est étendu à tous les facteurs premiers impairs p de t, tandis que le second est étendu à tous les nombres premiers $p > 2$. L'ordre de grandeur de $\Lambda(t)$ est celui de $\frac{t}{\log^2 t}$ et est donc défini, dès que l'on connaît l'ordre de grandeur de t, mais l'ordre de grandeur du facteur $Z(t)$ dépend du caractère arithmétique de t et est grand pour un nombre naturel t qui possède beaucoup de petits facteurs premiers impairs. On peut s'attendre à ce qu'un tel nombre puisse être écrit de beaucoup de manières différentes comme la somme de deux nombres premiers. L'expérience fournit le même résultat; par exemple $4996 = 2^2 \cdot 1249$; $4998 = 2 \cdot 3 \cdot 7^2 \cdot 17$ et $5000 = 2^3 5^4$ peuvent être écrits respectivement de 124, 288 et 150 manières comme la somme de deux nombres premiers impairs, de sorte que pour 4998 qui possède les facteurs 3 et 7, le nombre des décompositions est relativement grand.

Il est évident que (5) est aussi valable pour tout nombre impair $t > 1$, si nous posons pour un tel nombre $Z(t) = 0$. Le fait que (5) est vérifié pour à peu près (dans le sens faible) chaque nombre positif $\leqslant X$ découle du fait que

$$\sum_{t=2}^{X} |L(t) - Z(t)\, \Lambda(t)|^2 << X^{3-\Omega}$$

pour tout nombre fixe Ω.

Passons après cette remarque préliminaire aux problèmes généraux.

J'introduis deux nombres naturels fixes m et $n>m$, en outre mn entiers fixes $b_{\mu\nu}$ ($\mu=1,\dots,m$; $\nu=1,\dots,n$) et n fonctions $r_\nu(v)$, définies pour chaque entier v; j'adjoins à chaque système t de m entiers $t_1,\dots,t_m$ la somme

$$L(t)=\Sigma_1\, r_1(v_1)\dots r_n(v_n), \tag{8}$$

où Σ_1 est étendu aux entiers $v_1,\dots,v_n$, vérifiant les m relations

$$\sum_{\nu=1}^{n} b_{\mu\nu}\, v_\nu = t_\mu \quad (\mu=1,\dots,m); \tag{9}$$

je suppose que la série figurant dans le membre de droite de (8) converge absolument. Posons le problème de déduire pour la fonction $L(t)$ une formule approximative. Les théorèmes fondamentaux, qui nous permettent dans beaucoup de cas de trouver une telle formule, sont longs et compliqués, mais je vais donner ici quelques renseignements sur ces trois propositions. Commençons par la condition E qui est commune aux trois théorèmes. J'adjoins à la fonction $r_\nu(v)$ ($\nu=1,\dots,n$) une fonction $\rho_\nu(v)$ telle que les deux sommes

$$\sum_{v=-\infty}^{\infty} r_\nu(v) \quad \text{et} \quad \sum_{v=-\infty}^{\infty} \rho_\nu(v)$$

possèdent approximativement les mêmes valeurs. Mais j'exige plus: je suppose que pour tout nombre naturel q et pour tout entier k la somme

$$\sum_{v\equiv k \pmod q} r_\nu(v)$$

soit approximativement égale à la somme

$$\sum_{v=-\infty}^{\infty} \rho_\nu(v), \tag{10}$$

multipiée par un facteur qui dépend seulement de q et de k.

Je puis énoncer ce qui précède d'une autre manière. Comparons

$$\sum_{v=-\infty}^{\infty} e^{2\pi i\alpha v}\, r_\nu(v) \tag{11}$$

à la somme (10). Tout d'abord nous exigeons donc que ces deux sommes possèdent pour $\alpha=0$ une même valeur approximative. Si α est égal à une fraction irréductible $\frac{a}{q}$, la somme (11) peut être mise sous la forme

$$\sum_{k=0}^{q-1} e^{\frac{2\pi i a k}{q}} \sum_{v\equiv k \pmod q} r_\nu(v)$$

et possède donc, si q n'est pas trop grand, une valeur qui est approximativement égale à la somme (10), multipliée par un facteur qui ne dépend que de la fraction irréductible $\frac{a}{q}$ et que je désignerai par $z_\nu\left(\frac{a}{q}\right)$. Je supposerai en outre que l'expression (11) garde approximativement la même valeur, si α est situé dans le voisinage immédiat de la fraction irréductible $\frac{a}{q}$ à petit dénominateur, et qu'elle est pour $\nu=1,2,\dots,m$ approximativement égale à zéro, si α n'est pas situé dans le voisinage immédiat d'une fraction à petit denominateur.

Dans les applications les fonctions $r_\nu(v)$ sont données par les problèmes et peuvent être très irrégulières, mais nous choisissons les fonctions $\rho_\nu(v)$, que nous leur adjoignons nous-mêmes, aussi simples que possible.

Dans ce petit résumé de la condition E, commune aux trois théorèmes fondamentaux, j'ai essayé d'énoncer le fond essentiel de cette condition. Comme le lecteur le voit, il ne s'agit ici que de valeurs moyennes des fonctions $e^{2\pi i\alpha v} r_\nu(v)$ et c'est précisément le grand mérite de M. M. Siegel et Vinogradow d'avoir démontré que cette condition est vérifiée pour beaucoup de problèmes dont il est question à présent.

Le but de cet article est d'étudier quels points $t=(t_1,\dots,t_m)$ à m coordonnées entières peuvent être mis sous la forme

(12) $$\sum_{\nu=1}^{n} b_{\mu\nu}\, v_\nu = t_\mu \quad (\mu = 1, \ldots, m),$$

où m, n et $b_{\mu\nu}$ sont des entiers fixes, $n > m > 0$ et où $v_1, \ldots, v_n$ désignent des entiers possédant certaines propriétés. Je suppose que le déterminant

(13) $$\begin{vmatrix} b_{11} & \ldots & b_{1m} \\ \ldots & \ldots & \ldots \\ b_{m1} & \ldots & b_{mm} \end{vmatrix}$$

ne s'annule pas. Désignons par b^{-1} le nombre des points $\tau = (\tau_1, \ldots, \tau_m)$ dont les coordonnées sont $\geqslant 0$ et < 1 et qui possèdent la propriété que les n nombres $\sum_{\mu=1}^{m} b_{\mu\nu}\tau_\mu$ $(\nu = 1, \ldots, n)$ soient entiers.

Comme nous le verrons, dans ce cas il y a un lien étroit entre $L(t)$ et la somme analogue

$$\Lambda(t) = \Sigma_1\, \rho_1(v_1) \ldots \rho_n(v_n).$$

Pour beaucoup de points t la valeur approximative cherchée de $L(t)$ est égale à $b\,\Lambda(t)$, multiplié par un facteur $Z(t)$ qui dépend de la matrice

$$M = \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{m1} & \ldots & b_{mn} \end{pmatrix}$$

et des nombres $z_\nu\left(\frac{a}{q}\right)$ introduits ci-dessus. Comme nous le verrons dans les applications, l'ordre de grandeur de $\Lambda(t)$ est défini par celui des entiers $t_1, \ldots, t_m$, tandis que l'ordre de grandeur du facteur $Z(t)$ dépend du caractère arithmétique de ces nombres. Ce facteur, que M. M. Hardy et Littlewood ont appelé „the singular series", parce qu'ils l'ont écrit comme la somme d'une série et qui est nommé parfois „the singular product", quand il prend la forme d'un produit, sera appelé par

moi le facteur arithmétique. Je parlerai plus amplement de ce facteur arithmétique dans le paragraphe 3 de cet article.

Dans le théorème fondamental A je donnerai une borne supérieure pour

$$|L(t) - bZ(t)\,\Lambda(t)|,$$

dans les deux autres une borne pour la somme $\sum_t w(t)\,|L(t) - bZ(t)\,\Lambda(t)|^2$, étendue aux points $t = (t_1, \ldots, t_m)$ à coordonnées entières; $w(t) = w(t_1, \ldots, t_m)$ est un nombre $\geqq 0$ que nous choisissons arbitrairement avec la seule condition qu'il possède certaines propriétés générales.

Examinons dans les problèmes appartenant aux susdites catégories, comment les fonctions $r_\nu(v)$, $\rho_\nu(v)$ et $z_\nu\left(\frac{a}{q}\right)$ doivent être choisies.

Dans les problèmes des catégories I soit $r_\nu(v)$ le nombre de manières d'écrire l'entier v sous la forme

$$v = \psi_\nu(y_{\nu 1}, \ldots, y_{\nu, s_\nu}),$$

où $(y_{\nu 1}, \ldots, y_{\nu, s_\nu})$ désigne un point du domaine donné Y_ν et vérifie les congruences

(14) $$y_{\nu\sigma} \equiv u_{\nu\sigma} \pmod{U_{\nu\sigma}}.$$

Alors $L(t)$ désigne le nombre de manières d'écrire le système $t = (t_1, \ldots, t_m)$ sous la forme (2), où les entiers $y_{\nu 1}, \ldots, y_{\nu, s_\nu}$ vérifient les conditions nommées. Dans les problèmes des catégories II nous imposons encore aux nombres $y_{\nu\sigma}$ la condition d'être premiers et enfin dans les problèmes des catégories III nous exigeons que $y_{\nu\sigma}$ soit premier pour chaque couple (ν, σ) de la première famille. Etudions la classe III qui renferme les deux autres. Pour plus de simplicité je supprimerai pour l'instant l'indice ν, c'est-à-dire je partage le système $1, 2, \ldots, s$ en deux familles, $r(v)$ est le nombre de manières d'écrire v sous la forme $v = \psi(y_1, \ldots, y_s)$, où $y = (y_1, \ldots, y_s)$ désigne un point appartenant à un certaine domaine Y et vérifiant les congruences

(15) $$y_\sigma \equiv u_\sigma \pmod{U_\sigma} \quad (\sigma = 1, \ldots, s),$$

tandis que y_σ doit être premier pour chaque σ de la première famille;

$\psi(y_1,\dots,y_s)$ désigne un polynome donné à coefficients entiers, u_σ et $U_\sigma>0$ des entiers donnés, tels que u_σ soit premier avec U_σ pour chaque σ de la première famille; je suppose $y_\sigma\geqq 2$ pour chaque σ de la première famille et pour tout point y du domaine Y.

Pour toute fraction irréductible $\frac{a}{q}$ la somme

$$S=\sum_{v=-\infty}^{\infty} e\left(\frac{av}{q}\right) r(v),$$

où $e(\beta)=e^{2\pi i\beta}$, est égale à $\sum_y{}_2\, e\left(\frac{a}{q}\psi(y)\right)$, où $\sum_y{}_2$ est étendu aux points y définis plus haut. Désignons par d_σ le plus grand commun diviseur de q et U_σ. Si $\sum_h{}_3$ est étendu aux systèmes $h=(h_1,\dots,h_s)$ formés par s nombres $h_\sigma\leqq\frac{qU_\sigma}{d_\sigma}$, la somme S est égale à

$$\sum_h{}_3\, e\left(\frac{a}{q}\psi(h)\right)\sum_y{}_4\, 1,$$

où $\sum_y{}_4$ est étendu aux points y qui satisfont en outre aux congruences

$$y_\sigma\equiv h_\sigma\ (\mathrm{mod.}\ \tfrac{qU_\sigma}{d_\sigma})\quad(\sigma=1,\dots,s). \tag{16}$$

Il suit de (15) et (16) que $\sum_y{}_4\, 1$ s'annule si les s congruences

$$h_\sigma\equiv u_\sigma\ (\mathrm{mod.}\ U_\sigma)\quad(\sigma=1,\dots,s) \tag{17}$$

ne sont pas remplies en même temps. Considérons un système $h=(h_1,\dots,h_s)$ qui vérifie ce système de congruences. Si la première famille contient un σ pour lequel le plus grand commun diviseur de q et h_σ est supérieur à 1, le nombre premier correspondant y_σ est en vertu de (16) égal à ce plus grand commun diviseur et on peut s'attendre à ce que pour un tel système h la somme $\sum_y{}_4\, 1$ soit petite. Considérons enfin un système h vérifiant (17) tel que h_σ soit premier avec q pour tout σ de la première famille. Comme u_σ est premier avec U_σ pour tout σ

appartenant à la première famille, la somme $\sum_y{}_4\, 1$ est pour un tel système h dans des conditions très générales approximativement égale à $\frac{\Gamma}{\sum_h{}_5\, 1}$;

$$\Gamma=\left\{\prod_\sigma{}'\frac{1}{\varphi(U_\sigma)}\right\}\left\{\prod_\sigma{}''\frac{1}{U_\sigma}\right\}\sum_y{}_6\prod_\sigma{}'\frac{1}{\log y_\sigma},$$

où $\sum_y{}_6$ est étendu à tous les points $y=(y_1,\dots,y_s)$ du domaine Y, à coordonnées entières; $\prod_\sigma{}'$ et $\prod_\sigma{}''$ sont étendus aux σ de la première, respectivement seconde famille; $\sum_h{}_5$ est étendu aux systèmes $h=(h_1,\dots,h_s)$ formés par s nombres naturels $h_\sigma\leqq\frac{qU_\sigma}{d_\sigma}$ qui vérifient le système (17) et possèdent en outre la propriété que h_σ soit premier avec q pour tout σ de la première famille. On obtient ainsi pour S la valeur approximative $\Gamma\, z(\frac{a}{q})$, si l'on pose

$$z\left(\frac{a}{q}\right)=\frac{\sum_h{}_5\, e\left(\frac{a}{q}\psi(h)\right)}{\sum_h{}_5\, 1}. \tag{18}$$

Afin de donner la valeur de la fonction correspondante $\rho(v)$, je considérerai d'abord le cas particulier $s=1$, de sorte que Y est un domaine linéaire. Je supposerai que Y est un intervalle tel que $\psi'(y_1)=\frac{d\psi(y_1)}{dy_1}$ ne s'annule en aucun point de cet intervalle. Si 1 appartient à la première famille, c'est-à-dire si nous imposons à y_1 la condition d'être premier, je suppose en outre que l'extrémité de gauche de Y est fixe et $\geqq 2$. Dans ces conditions je pose $\rho(v)=0$ pour un entier v auquel ne correspond aucun point η de Y tel qu'on ait $v=\psi(\eta)$. Si à v correspond un nombre η (qui n'est pas nécessairement entier) de Y avec $\psi(\eta)=v$, ce nombre η est défini univoquement et je pose

$$\rho(v)=\frac{1}{\varphi(U_1)|\psi'(\eta)|\log\eta}\quad\text{ou}\quad\rho(v)=\frac{1}{U_1|\psi'(\eta)|}, \tag{19}$$

selon que 1 appartient à la première ou à la seconde famille. Γ est alors approximativement égal à

(20) $$\sum_{v=-\infty}^{\infty} \rho(v).$$

Etudions ensuite le cas général $s \geqq 1$. Dans ce cas nous pouvons poser dans certaines conditions

(21) $$\rho(v) = \left(\prod_{\sigma}' \frac{1}{\varphi(U_\sigma)}\right) \cdot \left(\prod_{\sigma}'' \frac{1}{U_\sigma}\right) I_1(v),$$

où $\prod_{\sigma}'$ et $\prod_{\sigma}''$ sont étendus aux σ appartenant respectivement à la première ou à la seconde famille; $I_1(v)$ est l'intégrale

$$I_1(v) = \int \cdots \int \left(\prod_{\sigma}' \frac{1}{\log \eta_\sigma}\right) d\eta_1 \ldots d\eta_s,$$

étendu au sous-ensemble de Y défini par les inégalités

$$v - \frac{1}{2} < \psi(\eta_1, \ldots, \eta_s) \leqq v + \frac{1}{2}.$$

En effet, si certaines conditions, d'ailleurs très générales, sont remplies, on trouve pour ce choix de la fonction $\rho(v)$, que Γ est encore approximativement égal à (20).

Si dans notre problème appartenant aux catégories III tous les nombres $s_1, \ldots, s_n$ possèdent la valeur 1, on peut définir les fonctions $\rho_\nu(v)$ par (19) et on trouve

$$\Lambda(t) = \left(\prod_{\nu}' \frac{1}{\varphi(U_\nu)}\right) \left(\prod_{\nu}'' \frac{1}{U_\nu}\right) \sum_{\tau} \frac{1}{|\psi_1'(\eta_1) \ldots \psi_n'(\eta_n)|} \prod_{\nu}' \frac{1}{\log \eta_\nu},$$

où $\sum_\tau$ est étendu aux entiers $v_1, \ldots, v_n$ qui satisfont aux relations

$$\sum_{\nu=1}^{n} b_{\mu\nu} v_\nu = t_\mu \qquad (\mu = 1, \ldots, m)$$

et auxquels correspondent n points η_ν appartenant à Y_ν $(\nu = 1, \ldots, n)$ avec

$$v_\nu = \psi_\nu(\eta_\nu) \qquad (\nu = 1, \ldots, n);$$

$\prod_{\nu}'$ et $\prod_{\nu}''$ sont étendus aux nombres ν $(\nu = 1, \ldots, n)$, pour lesquels le couple $(\nu, 1)$ appartient à la première, respectivement à la seconde famille.

Après avoir donné les fonctions $z_\nu\left(\frac{a}{q}\right)$, $\rho_\nu(v)$ et $\Lambda(t)$, je vais m'occuper du facteur arithmétique. Il est possible d'exprimer ce facteur au moyen de sommes exponentielles, mais je préfère l'exprimer à l'aide du nombre des systèmes $h = (h_1, \ldots, h_s)$ formés par s nombres naturels $h_\sigma \leqq U_\sigma p^\beta$ qui satisfont aux systèmes (17),

(22) $$\chi_\mu(h_1, \ldots, h_s) \equiv 0 \pmod{p^\beta} \quad (\mu = 1, \ldots, m)$$

et

(23) $$\prod_{\sigma}' h_\sigma \not\equiv 0 \pmod{p};$$

$\chi_\mu(h_1, \ldots, h_s)$ est un polynome à coefficients entiers, p un nombre premier, β un nombre naturel et le produit $\prod_{\sigma}'$ est étendu aux nombres σ de la première famille. Comme je l'ai déjà dit, pour tout σ de la première famille, u_σ est premier avec U_σ. Désignons par ζ le nombre des σ appartenant à la première famille avec $U_\sigma \not\equiv 0 \pmod{p}$, par $p^{(s-m)\beta-\zeta}(p-1)^\zeta$ $Q_\beta(p,t)$ le nombre des systèmes h formés par s nombres naturels $h_\sigma \leqq U_\sigma p^\beta$ qui satisfont à (17), (22) et (23). Pour étudier le nombre $Q_\beta(p,t)$, on peut considérer la matrice

$$M^* = \begin{pmatrix} U_1 \chi_{11} & \ldots & U_s \chi_{1s} \\ \ldots & \ldots & \ldots \\ U_1 \chi_{m1} & \ldots & U_s \chi_{ms} \end{pmatrix},$$

où $\chi_{\mu\sigma} = \frac{\partial \chi_\mu}{\partial h_\sigma}$. Dans un article que je publie en même temps sous le titre „Sur quelques systèmes de congruences" dans les Proceedings de l'Académie néerlandaise des Sciences à Amsterdam, je trouve le résultat suivant:

Proposition 1: *Supposons qu'il existe un entier $\gamma \geqq 0$ avec la propriété que le système*

$$\chi_\mu(h_1, \ldots, h_s) \equiv 0 \pmod{p^{2\gamma+1}} \quad (\mu = 1, \ldots, m)$$

ne possède aucune solution avec (17), (23) *et $\lambda_m > \lambda_{m-1} + \gamma$, où p^{λ_μ} est la puissance la plus élevée de p qui divise chaque déterminant d'ordre μ de la matrice M^*. Dans ces conditions $Q_\beta(p,t)$ possède pour toutes les valeurs de $\beta \geqq 2\gamma + 1$ la même valeur.*

Supposons que les conditions de cette proposition soient remplies, (avec (26) au lieu de (23)) si nous posons $s = s_1 + \ldots + s_n$ et

$$\chi_\mu(h_1, \ldots, h_s) = \sum_{\nu=1}^{n} b_{\mu\nu}\, \psi_\nu(h_{\nu 1}, \ldots, h_{\nu, s_\nu}) - t_\mu$$

$(\mu = 1, \ldots, m)$. Comme je le démontrerai dans le paragraphe 3, le facteur arithmétique est alors dans beaucoup de cas égal au produit $\prod_p Q(p, t)$, étendu ou bien à tous les nombres premiers p ou bien aux nombres premiers p inférieurs à une certaine borne.

Avant de passer à des cas particuliers, je vais distinguer deux cas différents. Considérons encore les systèmes (2) et (3), où $y_{\nu\sigma}$ est premier pour chaque couple (ν, σ) de la première famille. Supposons qu'il existe une puissance p^τ d'un nombre premier p tel que le système

$$\sum_{\nu=1}^{n} b_{\mu\nu}\, \psi_\nu(h_{\nu 1}, \ldots, h_{\nu, s_\nu}) \equiv t_\mu \pmod{p^\tau} \tag{24}$$

$(\mu = 1, \ldots, m)$ ne possède aucune solution avec

$$h_{\nu\sigma} \equiv u_{\nu\sigma} \pmod{U_{\nu\sigma}} \qquad (\nu = 1, \ldots, n;\ \sigma = 1, \ldots, s_\nu) \tag{25}$$

et

$$\prod'_{(\nu,\sigma)} h_{\nu\sigma} \equiv 0 \pmod{p}. \tag{26}$$

Pour les entiers $y_{\nu\sigma}$ vérifiant (2) et (3) on a donc

$$\prod'_{(\nu,\sigma)} y_{\nu\sigma} \equiv 0 \pmod{p},$$

d'où il suit que pour au moins un couple (ν, σ) de la première famille le nombre premier $y_{\nu\sigma}$ est égal au nombre premier fixe p. Nous pouvons donc réduire le problème posé à un autre problème renfermant une inconnue de moins. J'appellerai ce cas le cas réductible. Dans le cas irréductible à chaque puissance p^τ d'un nombre premier p correspond donc au moins un système d'entiers $h_{\nu\sigma}$ avec (24), (25) et (26).

Nous éclairerons les considérations précédentes par quelques exemples. Considérons le système

$$\sum_{\nu=1}^{n} b_{\mu\nu}\, p_\nu = t_\mu \qquad (\mu = 1, \ldots, m), \tag{27}$$

où les p_ν désignent des nombres premiers avec

$$p_\nu \equiv u_\nu \pmod{U_\nu} \quad (\nu = 1, \ldots, n); \tag{28}$$

supposons que $m > 0$, $n > m$, $U_\nu > 0$, u_ν et $b_{\mu\nu}$ soient des entiers fixes tels que u_ν soit premier avec U_ν $(\nu = 1, \ldots, n)$ et que le déterminant (13) formé par les m^2 nombres $b_{11}, \ldots, b_{mm}$ ne s'annule pas. Si nous posons $r_\nu(v) = 1$ pour tout nombre premier $v \leqq X$ avec $v \equiv u_\nu \pmod{U_\nu}$, et $r_\nu(v) = 0$ pour les autres entiers, $L(t)$ est le nombre de manières d'écrire le système t sous la forme (27), où p_ν désignent des nombres premiers $\leqq X$ avec (28). Comme je l'ai indiqué, $\rho_\nu(v)$ est dans ce cas $\frac{1}{\varphi(U_\nu)\log v}$ pour les entiers $v \geqslant 2$ et $\leqslant X$, tandis que $\rho_\nu(v) = 0$ pour les autres entiers. Par conséquent on a

$$\Lambda(t) = \left\{\prod_{\nu=1}^{n} \frac{1}{\varphi_\nu(U_\nu)}\right\} \Sigma_8 \frac{1}{(\log v_1)(\log v_2)\ldots(\log v_n)}, \tag{29}$$

où Σ_8 est étendu aux entiers $v_\nu \geqslant 2$ et $\leqslant X$ qui satisfont au système

$$\sum_{\nu=1}^{n} b_{\mu\nu}\, v_\nu = t_\mu \qquad (\mu = 1, \ldots, m).$$

Grâce aux recherches de M. M. Siegel et Vinogradow nous savons maintenant que la condition E, qui est commune aux trois théorèmes fondamentaux, est remplie, si la notion „à peu près" est prise dans le sens faible [1]).

Le théorème A nous apprend immédiatement pour chaque nombre fixe Ω

$$L(t) - b\,Z(t)\,\Lambda(t) << x^{-\Omega}\left\{X^{n-m} + X\sum_{\lambda=1}^{m}\sqrt{N_\lambda}\right\}, \tag{30}$$

où $Z(t)$ désigne le facteur arithmétique, tandis que N_λ peut être défini de la manière suivante: associons à tout nombre naturel $\lambda \leqslant m$ un nombre naturel $l \leqslant n-1$ et une permutation $\lambda, \lambda_1, \ldots, \lambda_{n-1}$ du système $1, 2, \ldots, n$; désignons [2]) par N_λ le nombre des systèmes formés par $2n-2$ entiers v_ν, v_ν' $(\nu \neq \lambda)$ qui sont tous $\geqslant 2$ et $\leqslant X$ et qui vérifient les relations

[1]) Dans ces théorèmes nous prenons $g_\nu = X$ et $r_\nu\left(\frac{a}{q}\right) = \frac{\mu(q)}{\varphi(q)}$, où $\mu(q)$ désigne la fonction de Möbius.

[2]) Les nombres R_λ et P_λ figurant dans le théorème A sont $<< N_\lambda$.

(31) $$\sum_{\nu=\lambda_1,\ldots,\lambda_l} b_{\mu\nu}(v_\nu - v_\nu') = 0; \quad \sum_{\nu=\lambda_{l+1},\ldots,\lambda_{n-1}} b_{\mu\nu}(v_\nu - v_\nu') = 0.$$

Il est clair que le résultat (30) n'a d'intérêt que si les nombres $N_1,\ldots,N_m$ ne sont pas trop grands. Pour cela j'introduirai l'hypothèse suivante: si λ est un nombre naturel quelconque $\leqq m$ et si l'on supprime dans la matrice

$$M=\begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{m1} & \ldots & b_{mn} \end{pmatrix}$$

la $\lambda^{ième}$ colonne, la matrice restante peut être partagée en deux matrices, chacune de rang m. En effet, dans ce cas nous pouvons choisir le nombre l et la permutation $\lambda, \lambda_1, \ldots, \lambda_{n-1}$ de telle façon que chacune des deux matrices

$$\begin{pmatrix} b_{1,\lambda_1} \ldots b_{1,\lambda_l} \\ \ldots \\ b_{m,\lambda_1} \ldots b_{m,\lambda_l} \end{pmatrix} \text{ et } \begin{pmatrix} b_{1,\lambda_{l+1}} \ldots b_{1,\lambda_{n-1}} \\ \ldots \\ b_{m,\lambda_{l+1}} \ldots b_{m,\lambda_{n-1}} \end{pmatrix}$$

soit de rang m. Le nombre des systèmes formés par $2l$ entiers $v_{\lambda_1}, \ldots, v_{\lambda_l}$, $v'_{\lambda_1}, \ldots, v'_{\lambda_l}$, tous $\geqq 2$ et $\leqq X$, pour lesquels la première des relations (31) est remplie, est donc $<< X^{2l-m}$ et on obtient un résultat analogue (avec $n-1-l$ au lieu de l) pour la seconde des relations (31). Par conséquent $N_\lambda << X^{2n-2-2m}$, de sorte que (30) prend la forme $L(t) - b\,Z(t)\,\Lambda(t) << x^{-\Omega} X^{n-m}$ pour tout nombre fixe Ω.

Afin d'obtenir le facteur arithmétique $Z(t)$, il est utile, comme il suit des remarques précédentes, d'étudier le système de congruences

(32) $$\begin{cases} \sum_{\nu=1}^{n} b_{\mu\nu} y_\nu \equiv t_\mu \pmod{p^\beta} & (\mu = 1,\ldots,m), \\ y_\nu \equiv u_\nu \pmod{U_\nu} & (\nu = 1,\ldots,n), \end{cases}$$

où p est un nombre premier, β un nombre naturel. Dans ce cas particulier on a $s=n$,

$$\chi_\mu(h_1,\ldots,h_n) = \sum_{\nu=1}^{n} b_{\mu\nu} h_\nu - t_\mu$$

et la matrice M^*, qui figure dans le raisonnement précédent, est égale à

$$\begin{pmatrix} U_1 b_{11} & \ldots & U_n b_{1n} \\ \ldots & \ldots & \ldots \\ U_1 b_{m1} & \ldots & U_n b_{mn} \end{pmatrix}.$$

Comme le déterminant (13) formé par les m^2 nombres $b_{11},\ldots,b_{mm}$ est différent de zéro, il existe un entier $\gamma \geqslant 0$ tel qu'au moins un déterminant d'ordre m de cette matrice ne soit pas divisible par $p^{\gamma+1}$. La proposition 1 nous donne ainsi le résultat suivant: si $p^{(n-m)\beta-n}(p-1)^n Q_\beta(p,t)$ désigne le nombre des solutions $y_1,\ldots,y_n$ de (32) telles que $y_1 y_2 \ldots y_n$ ne soit pas divisible par p, le nombre $Q_\beta(p,t)$ possède pour chaque $\beta \geqslant 2\gamma+1$ la même valeur. Je désigne cette valeur par $Q(p,t)$.

Le paragraphe 3 nous apprendra que le facteur arithmétique $Z(t)$ peut être écrit sous la forme

$$Z(t) = \prod_p Q(p,t),$$

où le produit, étendu à tous les nombres premiers p, converge absolument. De cette manière nous trouvons le résultat suivant:

Proposition 2: *Supposons que $m>0$, $n \geqslant 2m+1$, $U_\nu > 0$, u_ν et $b_{\mu\nu}$ $(\mu=1,\ldots,m;\ \nu=1,\ldots,n)$ désignent des entiers fixes tels que u_ν soit premier avec U_ν $(\nu=1,\ldots,n)$ et que le déterminant formé par les m premières colonnes de la matrice*

$$M=\begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{m1} & \ldots & b_{mn} \end{pmatrix}$$

ne s'annule pas. Si λ est un nombre naturel quelconque $\leqslant m$ et si l'on supprime dans M la $\lambda^{ième}$ colonne, je supposerai que la matrice restante puisse être divisée en deux matrices, chacune de rang m. Dans ces conditions on a pour tout nombre fixe Ω

$$L(t) - b\,\Lambda(t) \prod_p Q(p,t) << x^{-\Omega} X^{n-m},$$

où $L(t)$, b, $\Lambda(t)$ et $Q(p,t)$ possèdent les valeurs indiquées ci-dessus.

Pour un point t pour lequel se présente le cas réductible, au moins un des facteurs $Q(p,t)$ s'annule, donc aussi le facteur arithmétique $Z(t)$;

le résultat, obtenu pour un tel point, est évident, puisque l'inégalité plus forte

$$L(t) << X^{n-m-1}$$

est alors immédiate. Pour un point t pour lequel se présente le cas irréductible, aucun des facteurs $Q(p, t)$ ne s'annule. Il n'est pas nécessaire de soumettre ces facteurs à un examen rigoureux, parce qu'il suit des résultats généraux, trouvés dans le paragraphe 3 de cet article, que dans le cas irréductible $Q(p, t)$ est supérieur à un nombre positif indépendant de p et de t; dans le cas irréductible le facteur arithmétique est donc supérieur à un nombre positif indépendant de t. Si c_4 et c_5 désignent des nombres positifs fixes, on trouve donc que pour tout point t donnant lieu au cas irréductible et vérifiant l'inégalité

$$\Lambda(t) > c_4 x^{-c_5} X^{n-m}, \tag{33}$$

$L(t)$ est positif, si X est suffisamment grand. Nous avons ainsi trouvé:

Proposition 3: *Si c_4 et c_5 désignent des nombres positifs fixes et si X est assez grand, tout point t pour lequel se présente le cas irréductible et qui vérifie l'inégalité* (33), *peut être mis, dans les conditions de la proposition précédente, sous la forme* (27), *où les nombres premiers $p_1, \dots, p_n$ satisfont aux congruences* (28).

Dans le cas particulier où le système

$$\sum_{\nu=1}^{n} b_{\mu\nu}\zeta_\nu > 0 \quad (\mu = 1, \dots, m); \quad \zeta_\nu > 0 \quad (\nu = 1, \dots, n) \tag{34}$$

possède $n-m$ solutions linéairement indépendantes, l'ordre de grandeur du nombre des systèmes formés par n entiers $v_\nu \geqslant 2$ et $\leqslant X$ tels qu'on ait

$$\sum_{\nu=1}^{n} b_{\mu\nu} v_\nu = t_\mu \quad (\mu = 1, \dots, m)$$

est égal à X^{n-m}, si X est suffisamment grand et si le point fixe t donne lieu au cas irréductible; $\Lambda(t)$ est donc d'ordre de grandeur $x^{-n}X^{n-m}$. La proposition précédente fournit donc comme corollaire le résultat suivant:

Proposition 4: *Si les conditions de la proposition 2 sont remplies et si le système* (34) *possède $n-m$ solutions linéairement indépendantes,*

chaque point t pour lequel se présente le cas irréductible, peut être mis d'une infinité de manières différentes sous la forme (27), *où les nombres premiers p_ν satisfont aux congruences* (28).

Considérons le cas particulier $m = 1$. Si $b_1, \dots, b_n$, où n est $\geqq 3$, désignent des entiers fixes $\neq 0$, qui n'ont pas tous le même signe, et si u_ν est premier avec U_ν $(\nu = 1, \dots, n)$, chaque entier t, donnant lieu au cas irréductible, peut être mis, d'après la proposition précédente, d'une infinité de manières différentes sous la forme

$$t = b_1 p_1 + \dots + b_n p_n, \tag{35}$$

où les nombres premiers p_ν vérifient les congruences (28).

Si par contre $b_1, \dots, b_n$ sont tous positifs, et si t est un entier assez grand pour lequel se présente le cas irréductible, $\Lambda(t)$ possède, si l'on choisit X convenablement, l'ordre de grandeur $X^{n-1}x^{-n}$ et la proposition 3 nous apprend:

Si n est $\geqslant 3$, si $b_1, \dots, b_n$ désignent des nombres naturels, u_ν un entier qui est premier avec le nombre naturel U_ν $(\nu = 1, \dots, n)$, chaque entier t assez grand, pour lequel se présente le cas irréductible, peut être mis sous la forme (35), *où les nombres premiers p_ν satisfont à* (28).

Passons à l'application du théorème fondamental B. Si $L(t)$ désigne encore le nombre de manières d'écrire $t = (t_1, \dots, t_m)$ sous la forme (27), où les nombres premiers p_ν sont $\leqslant X$ et vérifient les congruences (28), si $\Lambda(t)$ est encore défini par (29) et si le déterminant (13), formé par les m^2 nombres $b_{11}, \dots, b_{mm}$, ne s'annule pas, le théorème B nous donne pour chaque nombre fixe Ω l'inégalité

$$\sum_t |L(t) - bZ(t)\Lambda(t)|^2 << x^{-\Omega}\{X^{2n-m} + X^2 \sum_{\lambda=1}^{m} N_\lambda'\}, \tag{36}$$

où N_λ' est le nombre des systèmes formés par $2n-2$ entiers v_ν, v_ν' $(\nu \neq \lambda)$ tels qu'on ait

$$\sum_{\substack{\nu=1 \\ \nu\neq\lambda}}^{n} b_{\mu\nu}(v_\nu - v_\nu') = 0 \quad (\mu = 1, \dots, m);$$

$\sum_t$ est étendu aux points $t = (t_1, \dots, t_m)$ à m coordonnées entières.

Si l'on supprime la $\lambda^{ième}$ colonne de la matrice M, je supposerai que le rang de la matrice restante vaut m. Alors on a $N_\lambda' << X^{2n-2-m}$, de sorte

que le membre de droite de (36) est $<< x^{-Q}X^{2n-m}$. Comme nous le verrons, le facteur arithmétique $Z(t)$ peut être écrit comme un produit $\prod_p Q(p,t)$, étendu aux nombres premiers inférieurs à une certaine borne; $Q(p,t)$ possède la valeur indiquée ci-dessus. Cependant dans ce problème il est parfois possible d'écrire le facteur arithmétique comme le produit analogue, étendu à tous les nombres premiers. Ce cas se présente par exemple dans le problème suivant, étudié par M. M. Hardy et Littlewood[3]).

Posons la question de savoir, $t_1<t_2<\ldots<t_m$ désignant des nombres naturels, combien de nombres premiers $p\leqslant X-t_m$ possèdent la propriété que les $m+1$ nombres p, $p+t_1,\ldots,p+t_m$ soient premiers en même temps. Ce problème conduit au système

$$-y_1+y_{\mu+1}=t_\mu \quad (\mu=1,\ldots,m). \tag{37}$$

Dans ce cas particulier on a $n=m+1$ et $U_1=\ldots=U_n=1$ et $b=1$. Le plus grand commun diviseur des déterminants d'ordre m de la matrice

$$\begin{pmatrix} -1 & 1 & 0 & \ldots & 0\\ -1 & 0 & 1 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ -1 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

est 1, de sorte que $p^{1-n}(p-1)^n Q(p,t)$ désigne le nombre des solutions $y_1,\ldots,y_{m+1}$ avec $y_1\ldots y_{m+1}\not\equiv 0 \pmod p$ du système

$$-y_1+y_{\mu+1}\equiv t_\mu \pmod p \quad (\mu=1,\ldots,m).$$

Si ζ_p désigne le nombre des restes modulo p distincts qui figurent dans le système $0, t_1,\ldots,t_m$, l'entier y_1 peut prendre exactement $p-\zeta_p$ valeurs différentes modulo p, d'où il suit

$$Q(p,t)=(p-1)^{-m-1}p^m(p-\zeta_p). \tag{38}$$

Pour chaque nombre premier $p>t_m$ on a $\zeta_p=m+1$ et

$$Q(p,t)=\frac{p^{m+1}-(m+1)p^m}{(p-1)^{m+1}},$$

[3]) G. H. Hardy and J. E. Littlewood, Some problemes of „Partitio Numerorum" III. On the expression of a number as a sum of primes, Acta Mathematica **44** (1922). 1—70; voir p. 52—62.

de sorte que le produit $\prod_p Q(p,t)$, étendu à tous les nombres premiers p, est un produit convergent. Comme nous le verrons, ce produit peut être pris comme facteur arithmétique $Z(t)$.

Le théorème B nous donne ainsi la

Proposition 5: *Associons à tout point t dont les coordonnées entières vérifient les inégalités $0<t_1<\ldots<t_m$, le nombre $L(t)$ de nombres premiers $p\leqslant X-t_m$, tels que p, $p+t_1,\ldots,p+t_m$ soient premiers; posons en outre*

$$\Lambda(t)=\sum_{v=2}^{X-t_m}\prod_{\mu=0}^{m}\frac{1}{\log(v+t_\mu)},$$

où $t_0=0$. Définissons $Q(p,t)$ par (38). Dans ces conditions la somme

$$\sum_t |L(t)-\Lambda(t)\prod_p Q(p,t)|^2,$$

étendue aux points $t=(t_1,\ldots,t_m)$ avec

$$0<t_1<t_2<\ldots t_m\leqslant X, \tag{39}$$

est pour chaque nombre fixe c_6 certainement $<< X^{m+2}x^{-c_6}$.

De ce résultat il découle immédiatement qu'à peu près (dans le sens faible) chaque point t avec (39) vérifie la relation

$$L(t)=(1+\frac{\Theta}{x^{c_7}})\Lambda(t)\prod_p Q(p,t), \tag{40}$$

où c_7 est un nombre fixe quelconque et Θ est en valeur absolue inférieur à 1. A peu près (dans le sens faible) chaque point t avec (39) pour lequel se présente le cas irréductible possède donc la propriété qu'on peut trouver un nombre premier p tel que les $m+1$ nombres p, $p+t_1,\ldots,p+t_m$ soient premiers.

M. M. Hardy et Littlewood ont énoncé l'hypothèse que (40) est vérifié pour chaque point fixe t avec (39) donnant lieu au cas irréductible, sous la seule supposition que X soit suffisamment grand. Le raisonnement précédent nous apprend que cette hypothèse est certainement vraie pour à peu près (dans le sens faible) chaque point t avec (39).

Sans plus tarder je passe maintenant aux théorèmes fondamentaux, dont d'autres applications suivront plus tard.

§ 2. Les trois théorèmes fondamentaux.

Afin de simplifier l'énoncé des théorèmes fondamentaux, j'introduis deux conditions.

Condition D: Je dirai que les fonctions $r(v), \rho(v)$ et $z(\frac{a}{q})$ et le nombre positif g satisfont à la condition D, quand ils possèdent les propriétés suivantes:

$r(v)$ et $\rho(v)$ sont définis pour tout entier v et $z(\frac{a}{q})$ est une fonction de période 1 de la fraction[4]) irréductible $\frac{a}{q}$; il existe un nombre fixe c_8 tel que l'inégalité

$$z(\tfrac{a}{q}) << q^{c_8} \tag{41}$$

soit vérifiée pour toute fraction irréductible $\frac{a}{q}$. Supposons

$$\sum_{v=-\infty}^{\infty} |r(v)| \text{ et } \sum_{v=-\infty}^{\infty} |\rho(v)| << g. \tag{42}$$

Supposons dans le cas faible, pour tout choix des nombres fixes c_9, c_{10} et c_{11}, que l'expression

$$\sum_{v=-\infty}^{\infty} e^{2\pi i \alpha v} r(v) - z(\tfrac{a}{q}) \sum_{v=-\infty}^{\infty} e^{2\pi i (\alpha - \frac{a}{q}) v} \rho(v) \tag{43}$$

soit $<< g x^{-c_9}$ pour chaque fraction irréductible $\frac{a}{q}$ à dénominateur $\leqq x^{c_{10}}$ et pour chaque nombre réel α avec $|\alpha - \frac{a}{q}| \leqq X^{-1} x^{c_{11}}$.

Supposons enfin dans le cas fort qu'il existe trois nombres fixes positifs c_{12}, c_{13} et c_{14} tels que l'expression (43) soit $<< g X^{-c_{12}}$ pour chaque fraction irréductible $\frac{a}{q}$ à dénominateur $\leqq X^{c_{13}}$ et pour tout nombre réel α avec $|\alpha - \frac{a}{q}| \leqq X^{-1+c_{14}}$.

[4]) Dans cet article fraction veut toujours dire une fraction dont le numérateur et le dénominateur sont entiers et dont le dénominateur est positif.

Condition E: Introduisons deux entiers fixes $m>0$ et $n>m$, en outre mn entiers fixes $b_{\mu\nu}$ $(\mu=1,\ldots,m;\ \nu=1,\ldots,n)$ avec

$$\begin{vmatrix} b_{11} & \ldots & b_{1m} \\ \ldots & \ldots & \ldots \\ b_{m1} & \ldots & b_{mm} \end{vmatrix} \neq 0. \tag{44}$$

Supposons que la condition D soit satisfaite par les fonctions $r_\nu(v)$, $\rho_\nu(v)$ et $z_\nu(\frac{a}{q})$ et les nombres g_ν $(\nu=1,\ldots,n)$ et que nous ayons

$$\sum_{v=-\infty}^{\infty} |\rho_\mu(v+1) - \rho_\mu(v)| << g_\mu X^{-1} \quad (\mu=1,\ldots,m). \tag{45}$$

Supposons[5]) dans le cas faible pour chaque nombre fixe c_{15}

$$\sum_{v=-\infty}^{\infty} |\rho_\nu(v+1) - \rho_\nu(v)| << g_\nu x^{-c_{15}} \quad (\nu=m+1,\ldots,n) \tag{46}$$

et dans le cas fort pour un nombre fixe positif convenable c_{16}

$$\sum_{v=-\infty}^{\infty} |\rho_\nu(v+1) - \rho_\nu(v)| << g_\nu X^{-c_{16}} \quad (\nu=m+1,\ldots,n). \tag{47}$$

Dans le cas faible nous supposerons qu'à tout nombre fixe c_{17} corresponde un nombre positif c_{18} tel que les m inégalités

$$\sum_{v=-\infty}^{\infty} e^{2\pi i \alpha v} r_\mu(v) << g_\mu x^{-c_{17}} \tag{48}$$

$(\mu=1,\ldots,m)$ soient vérifiées pour chaque nombre réel α jouissant de

[5]) Les inégalités (46) et (47) sont superflues, si chacun des $m(n-m)$ entiers $b_{\mu\nu}$, où $\nu>m$, est divisible par le déterminant figurant dans (44).

la propriété [6]) que l'intervalle $(\alpha \mp X^{-1} x^{c_{18}})$ ne contienne aucune fraction à dénominateur $\leqq x^{c_{18}}$.

Dans le cas fort nous supposerons qu'à tout nombre positif c_{19} correspond un nombre positif c_{20} tel que les m inégalités

$$\sum_{v=-\infty}^{\infty} e^{2\pi i \alpha v} r_\mu(v) << g_\mu X^{-c_{20}} \tag{49}$$

$(\mu = 1, \ldots, m)$ soient vérifiées pour chaque valeur réelle de α jouissant de la propriété que l'intervalle $(\alpha \mp X^{-1+c_{19}})$ ne contienne aucune fraction à dénominateur $\leqq X^{c_{19}}$.

Partout dans cet article je poserai pour tout point $t = (t_1, \ldots, t_m)$ à m coordonnées entières

$$L(t) = \Sigma_1 \prod_{\nu=1}^{n} r_\nu(v_\nu) \text{ et } \Lambda(t) = \Sigma_1 \prod_{\nu=1}^{n} \rho_\nu(v_\nu);$$

Σ_1 est toujours étendu aux entiers $v_1, \ldots, v_n$ tels qu'on ait

$$\sum_{\nu=1}^{n} b_{\mu\nu} v_\nu = t_\mu \quad (\mu = 1, \ldots, m). \tag{50}$$

Soit b^{-1} le nombre des points $\tau = (\tau_1, \ldots, \tau_m)$ dont les coordonnées sont $\geqq 0$ et < 1 et possèdent la propriété que les n nombres $\sum_{\mu=1}^{m} b_{\mu\nu} \tau_\mu$ $(\nu = 1, \ldots, n)$ soient entiers. Pour chaque système $\gamma = (\gamma_1, \ldots, \gamma_m)$ formé par m fractions irréductibles γ_μ, je pose

$$\eta(\gamma) = \prod_{\nu=1}^{n} z_\nu \Big(\sum_{\mu=1}^{m} b_{\mu\nu} \gamma_\mu \Big).$$

Par $x(\Omega_1, \Omega_2)$, où Ω_2 est $\geqq \Omega_1$, je désignerai un ensemble quelconque formé par des systèmes $\gamma = (\gamma_1, \ldots, \gamma_m)$, où $\gamma_1, \ldots, \gamma_m$ sont des fractions irréductibles $\geqq 0$ et < 1 avec les deux propriétés suivantes:

[6]) $(\alpha \mp \xi)$ désigne toujours l'intervalle fermé $(\alpha - \xi, \alpha + \xi)$.

1. L'ensemble $x(\Omega_1, \Omega_2)$ contient chaque système γ dont chacune des m fractions irréductibles $\gamma_\mu \geqq 0$ et < 1 possède un dénominateur $\leqq x^{\Omega_1}$.

2. Chaque fraction γ_μ figurant dans un système quelconque γ de $x(\Omega_1, \Omega_2)$ possède un dénominateur $\leqq x^{\Omega_2}$.

Par $X(\omega_1, \omega_2)$, où ω_2 est $\geqq \omega_1$, je désignerai un ensemble quelconque formé par des systèmes $\gamma = (\gamma_1, \ldots, \gamma_m)$, où $\gamma_1, \ldots, \gamma_m$ sont des fractions irréductibles $\geqq 0$ et < 1 avec les deux propriétés suivantes:

1. L'ensemble $X(\omega_1, \omega_2)$ contient chaque système γ dont chacune des m fractions irréductibles $\gamma_\mu \geqq 0$ et < 1 possède un dénominateur $\leqq X^{\omega_1}$.

2. Chaque fraction γ_μ figurant dans un système quelconque γ de $X(\omega_1, \omega_2)$ possède un dénominateur $\leqq X^{\omega_2}$.

Les sommes $\sum_{\gamma \text{ dans } x(\Omega_1, \Omega_2)}$ et $\sum_{\gamma \text{ dans } X(\omega_1, \omega_2)}$ sont étendues aux systèmes γ appartenant à un ensemble quelconque $x(\Omega_1, \Omega_2)$, respectivement $X(\omega_1, \omega_2)$.

Théorème fondamental A.

Conditions: *Supposons la condition* E *vérifiée. A tout nombre naturel* $\lambda \leqq m$ *j'associe un nombre naturel* $l \leqq n-1$, *une permutation* $(\lambda, \lambda_1, \ldots, \lambda_{n-1})$ *du système* $(1, 2, \ldots, n)$ *et je pose, pour tout point* $t = (t_1, \ldots, t_m)$ *à* m *coordonnées entières,*

$$R_\lambda = \Sigma_9 \prod_{\substack{\nu=1 \\ \nu \neq \lambda}}^{n} r_\nu(v_\nu) \overline{r}_\nu(v_\nu'); \quad P_\lambda = \Sigma_9 \prod_{\substack{\nu=1 \\ \nu \neq \lambda}}^{n} \rho_\nu(v_\nu) \overline{\rho}_\nu(v_\nu'), \tag{51}$$

où Σ_9 *est étendu aux points à* $2n-2$ *coordonnées entières* v_ν, v_ν' $(\nu \neq \lambda)$ *tels qu'on ait*

$$\sum_{\nu=\lambda_1, \ldots, \lambda_l} b_{\mu\nu}(v_\nu - v_\nu') = 0 \text{ et } \sum_{\nu=\lambda_{l+1}, \ldots, \lambda_{n-1}} b_{\mu\nu}(v_\nu - v_\nu') = 0$$

$(\mu = 1, \ldots, m)$. *Posons finalement*

$$T = X^{-m} g_1 \ldots g_n + \sum_{\lambda=1}^{m} g_\lambda (\sqrt{R_\lambda} + \sqrt{P_\lambda}).$$

Assertion: *Dans le cas faible à tout nombre fixe* Ω *correspond*

un nombre fixe Ω_1 tel qu'on ait pour tout nombre fixe $\Omega_2 \geqq \Omega_1$ et pour tout point $t=(t_1,\dots,t_m)$ à m coordonnées entières

$$L(t)-b\Lambda(t)\sum_{\gamma \text{ dans } x(\Omega_1,\Omega_2)} e^{-2\pi i\sum_{\mu=1}^{m}\gamma_\mu t_\mu}\eta_l(\gamma)<<x^{-\Omega}T.$$

Dans le cas fort, il existe un nombre positif fixe ω_2 tel qu'à chaque nombre positif fixe $\omega_1 \leqq \omega_2$ corresponde un nombre positif fixe ω avec la propriété

$$L(t)-b\Lambda(t)\sum_{\gamma \text{ dans } X(\omega_1,\omega_2)} e^{-2\pi i\sum_{\mu=1}^{m}\gamma_\mu t_\mu}\eta_l(\gamma)<<X^{-\omega}T.$$

Théorème fondamental B.

Conditions : *Supposons la condition* E *vérifiée. A tout nombre $\lambda \leqq m$ j'adjoins*

$$R_\lambda=\Sigma_{10}\prod_{\substack{\nu=1\\ \nu\neq\lambda}}^{n} r_\nu(v_\nu)\overline{r}_\nu(v_\nu');\quad P_\lambda=\Sigma_{10}\prod_{\substack{\nu=1\\ \nu\neq\lambda}}^{n}\rho_\nu(v_\nu)\overline{\rho}_\nu(v_\nu'), \tag{52}$$

où Σ_{10} est étendu aux points à $2n-2$ coordonnées entières v_ν, v_ν' $(\nu\neq\lambda)$ tels qu'on ait

$$\sum_{\substack{\nu=1\\ \nu\neq\lambda}}^{n} b_{\mu\nu}(v_\nu-v_\nu')=0 \quad (\mu=1,\dots,m).$$

Pour tout point $t=(t_1,\dots,t_m)$ à m coordonnées entières je pose

$$w(t)=\prod_{\mu=1}^{m} w_\mu(t_\mu),$$

où $w_\mu(h)$ est, pour $\mu=1,\dots,m$, une fonction $\geqq 0$ de h vérifiant l'inégalité

$$\sum_{h=-\infty}^{\infty}|w_\mu(h+1)-w_\mu(h)|\leqq X^{-1}\sum_{h=-\infty}^{\infty}w_\mu(h), \tag{53}$$

où la série, figurant dans le membre de droite, converge. Posons

$$T=X^{-2m}g_1^2\dots g_n^2+X^{-m}\sum_{\lambda=1}^{m}g_\lambda^2(R_\lambda+P_\lambda).$$

Assertion : *Dans le cas faible, à tout nombre fixe Ω correspond un nombre fixe Ω_1 tel qu'on ait pour tout nombre fixe $\Omega_2 \geqq \Omega_1$*

$$\sum_t w(t)\,|L(t)-b\Lambda(t)\sum_{\gamma \text{ dans } x(\Omega_1,\Omega_2)} e^{-2\pi i\sum_{\mu=1}^{m}\gamma_\mu t_\mu}\eta_l(\gamma)|^2<<x^{-\Omega}T\sum_t w(t),$$

où $\sum_t$ est étendu à tous les points $t=(t_1,\dots,t_m)$ à m coordonnées entières.

Dans le cas fort, il existe un nombre positif fixe ω_2 tel qu'à chaque nombre positif fixe $\omega_1 \leqq \omega_2$ corresponde un nombre positif fixe ω avec la propriété

$$\sum_t w(t)\,|L(t)-b\Lambda(t)\sum_{\gamma \text{ dans } X(\omega_1,\omega_2)} e^{-2\pi i\sum_{\mu=1}^{m}\gamma_\mu t_\mu}\eta_l(\gamma)|^2<<X^{-\omega}T\sum_t w(t).$$

Théorème fondamental C.

Conditions: *Supposons la condition* E *vérifiée. Soit l un nombre naturel $\leqq n-1$. Posons*

$$R=\Sigma_{11}\prod_{\nu=1}^{n} r_\nu(v_\nu)\overline{r}_\nu(v_\nu');\qquad P=\Sigma_{11}\prod_{\nu=1}^{n}\rho_\nu(v_\nu)\overline{\rho}_\nu(v_\nu'), \tag{54}$$

où Σ_{11} est étendu aux points à $2n$ coordonnées entières v_ν, v_ν' tels qu'on ait

$$\sum_{\nu=1}^{l} b_{\mu\nu}(v_\nu-v_\nu')=0 \text{ et } \sum_{\nu=l+1}^{n} b_{\mu\nu}(v_\nu-v_\nu')=0$$

$(\mu=1,\dots,m)$ et posons en outre

$$T=X^{-2m}g_1^2\dots g_n^2+R+P \text{ et } w(t)=w(t_1,\dots t_m)\geqq 0.$$

Supposons dans le cas faible qu'à tout nombre fixe c_{21} corresponde un nombre fixe c_{22} tel que l'inégalité

(55) $$\sum_t w(t)\, e^{2\pi i \sum_{\mu=1}^{m} \alpha_\mu t_\mu} << x^{-c_{21}} \sum_t w(t)$$

soit remplie pour tous les points $\alpha = (\alpha_1, \ldots, \alpha_m)$, *excepté ceux pour lesquels chacun des* m *intervalles* $(\alpha_\mu \mp X^{-1} x^{c_{22}})$ *contient au moins une fraction à dénominateur* $\leqq x^{c_{22}}$.

Supposons dans le cas fort qu'à tout nombre positif fixe c_{23} *corresponde un nombre positif fixe* c_{24} *avec la propriété*

$$\sum_t w(t)\, e^{2\pi i \sum_{\mu=1}^{m} \alpha_\mu t_\mu} << X^{-c_{24}} \sum_t w(t),$$

sauf si chacun des m *intervalles* $(\alpha \mp X^{-1+c_{23}})$ *contient au moins une fraction à dénominateur* $\leqq X^{c_{23}}$.

L'assertion est précisément la même que celle du théorème B.

Dans les théorèmes fondamentaux le facteur arithmétique est écrit comme une somme. Dans le paragraphe suivant ce facteur sera mis sous la forme d'un produit.

On peut mettre les assertions des trois théorèmes fondamentaux sous une autre forme. Pour cela je pose, pour tout point t à m coordonnées entières et pour tout système $\gamma' = (\gamma_1', \ldots, \gamma_n')$, formé par n fractions irréductibles,

$$\Lambda(t, \gamma') = \Sigma_1 \prod_{\nu=1}^{n} e^{-2\pi i \gamma_\nu' v_\nu} \rho_\nu(v_\nu)\, z_\nu(\gamma_\nu').$$

Par $x'(\Omega_1, \Omega_2)$, où Ω_2 est $\geqslant \Omega_1$, je désigne un ensemble quelconque formé par des systèmes $\gamma' = (\gamma_1', \ldots, \gamma_n')$, où $\gamma_1', \ldots, \gamma_n'$ sont des fractions irréductibles $\geqslant 0$ et < 1 avec les deux propriétés suivantes:

1. L'ensemble $x'(\Omega_1, \Omega_2)$ contient chaque système γ' dont chacune des n factions irréductibles $\gamma_\nu' \geqslant 0$ et < 1 possède un dénominateur $\leqslant x^{\Omega_1}$.

2. Chaque fraction γ_ν' figurant dans un système γ' de $x'(\Omega_1, \Omega_2)$ possède un dénominateur $\leqslant x^{\Omega_2}$.

Par $X'(\omega_1, \omega_2)$, où ω_2 est $\geqslant \omega_1$, je désignerai un ensemble quelconque formé par des systèmes $\gamma' = (\gamma_1', \ldots, \gamma_n')$, où $\gamma_1', \ldots, \gamma_n'$ sont des fractions irréductibles $\geqslant 0$ et < 1 avec les deux propriétés suivantes:

1. L'ensemble $X'(\omega_1, \omega_2)$ contient chaque système γ' dont chacune des n fractions irréductibles $\gamma_\nu' \geqslant 0$ et < 1 possède un dénominateur $\leqslant X^{\omega_1}$.

2. Chaque fraction γ_ν' figurant dans un système γ' de $X'(\omega_1, \omega_2)$ possède un dénominateur $\leqslant X^{\omega_2}$.

Comme je le démontrerai, l'assertion du théorème A est équivalente à la suivante:

Supposons les conditions du théorème A *remplies. Dans le cas faible, à tout nombre fixe* Ω *correspond un nombre fixe* Ω_1' *tel qu'on ait pour tout nombre fixe* $\Omega_2' \geqslant \Omega_1'$ *et pour tout point* t *à* m *coordonnées entières,*

$$L(t) - \sum_{\gamma' \text{ dans } x'(\Omega_1', \Omega_2')} \Lambda(t, \gamma') << x^{-\Omega} T$$

et dans le cas fort, il existe un nombre positif fixe ω_2' *tel qu'à chaque nombre positif fixe* $\omega_1' \leqslant \omega_2'$ *corresponde un nombre positif fixe* ω *avec la propriété*

$$L(t) - \sum_{\gamma' \text{ dans } X'(\omega_1', \omega_2')} \Lambda(t, \gamma') << X^{-\omega} T.$$

En effet, il suffit de considérer le cas faible; le cas fort peut être traité de la même manière. Supposons que la deuxième assertion soit déjà démontrée. Choisissons $\Omega_1' = \frac{1}{2m} \Omega_1$ et $\Omega_2' = m \Omega_2$. On a

(56) $$b \Lambda(t) \sum_{\gamma \text{ dans } x(\Omega_1, \Omega_2)} e\left(-\sum_\mu \gamma_\mu t_\mu\right) \eta(\gamma)$$

$$= b \sum_{\gamma \text{ dans } x(\Omega_1, \Omega_2)} \Sigma_1 \prod_{\nu=1}^{n} \rho_\nu(v_\nu)\, e(-\gamma_\nu' v_\nu)\, z_\nu(\gamma_\nu')$$

où $e(\beta) = e^{2\pi i \beta}$,

$$\gamma_\nu' \equiv \sum_{\mu=1}^{m} b_{\mu\nu} \gamma_\mu \pmod 1 \text{ et } 0 \leqslant \gamma_\nu' < 1 \quad (\nu = 1, \ldots, n).$$

Dans chaque terme le système $\gamma' = (\gamma_1', \dots, \gamma_n')$ est formé par n fractions irréductibles γ_ν' dont le dénominateur est $\leqq x^{m\Omega_2} = x^{\Omega_2'}$. Réciproquement à tout système γ' formé par n fractions irréductibles $\gamma_\nu' \geqq 0$ et < 1 à dénominateur $\leqq x^{\Omega_1'}$ correspondent zéro ou b^{-1} systèmes $\gamma = (\gamma_1, \dots, \gamma_m)$ dans lesquels γ_μ est $\geqq 0$ et < 1; si γ existe, le dénominateur de chaque fraction irréductible γ_μ est $<< x^{m\Omega_1'}$, donc $\leqq x^{\Omega_1}$, si X est assez grand (sinon les assertions des théorèmes fondamentaux sont évidentes). L'expression (56) est donc égale à une somme de la forme

$$\sum_{\gamma' \text{ dans } x'(\Omega_1', \Omega_2')}' \Lambda(t, \gamma'),$$

où la somme Σ' est étendue aux systèmes γ' appartenant à un certain ensemble $x'(\Omega_1', \Omega_2')$ tels que le système de congruences cité soit résoluble. Je puis supposer que cet ensemble $x'(\Omega_1', \Omega_2')$ soit tel que pour chacun de ses systèmes γ', pous lesquels le système de congruences cité n'est pas résoluble, les dénominateurs q_ν de γ_ν' $(\nu = 1, \dots, n)$ soient $\leqq x^{\Omega_1'}$.

Si pour tout système d'entiers $\chi_1, \dots, \chi_n$ avec

$$\sum_{\nu=1}^{n} b_{\mu\nu}\chi_\nu = 0 \qquad (\mu = 1, \dots m)$$

les n nombres $\gamma_\nu'\chi_\nu$ sont entiers, le système de congruences cité est résoluble; en effet, par des transformations élémentaires on peut réduire le cas général au cas particulier où les $m(n-m)$ nombres $b_{\mu\nu}$ $(\mu = 1, \dots m;\ \nu = m+1, \dots, n)$ sont nuls et alors $\gamma_{m+1}', \dots, \gamma_n'$ sont entiers et la remarque est évidente. Pour un système γ' de $x'(\Omega_1', \Omega_2')$, pour lequel le système de congruences cité n'est pas résoluble, correspondent donc n entiers $\chi_1, \dots, \chi_n$ avec

$$\sum_{\nu=1}^{n} b_{\mu\nu}\chi_\nu = 0 \qquad (\mu = 1, \dots, m),$$

tels qu'au moins un des n nombres $\gamma_\nu'\chi_\nu$ ne soit pas entier. On peut choisir ces entiers χ_ν en valeur absolue $<< x^{n\Omega_1'}$. On a pour un tel système

$$\sum_{h_1=1}^{q_1} \dots \sum_{h_n=1}^{q_n} e\Big(-\sum_{\nu=1}^{n} h_\nu\gamma_\nu'\chi_\nu\Big) = \prod_{\nu=1}^{n}\sum_{h=1}^{q_\nu} e(-h\gamma_\nu'\chi_\nu) = 0.$$

Pour chaque système v avec

$$\sum_{\nu=1}^{n} b_{\mu\nu}v_\nu = t_\mu \qquad (\mu = 1, \dots, m)$$

on a de même

$$\sum_{\nu=1}^{n} b_{\mu\nu}(v_\nu + h_\nu\chi_\nu) = t_\mu \quad (\mu = 1, \dots, m).$$

Pour un système γ' de $x'(\Omega_1', \Omega_2')$, pour lequel le système de congruences cité n'est pas résoluble, on a donc

$$\Sigma_1 \sum_{\nu=1}^{n} \rho_\nu(v_\nu) e(-\gamma_\nu' v_\nu) = q_1^{-1} \dots q_n^{-1} \Sigma_1 S(v),$$

où

$$S(v) = \sum_{h_1=1}^{q_1} \dots \sum_{h_n=1}^{q_n} \prod_{\nu=1}^{n} \rho_\nu(v_\nu + h_\nu\chi_\nu)\, e(-\gamma_\nu' v_\nu - h_\nu\gamma_\nu'\chi_\nu)$$

$$= \sum_{h_1=1}^{q_1} \dots \sum_{h_n=1}^{q_n} \Big\{ \prod_{\nu=1}^{n} \rho_\nu(v_\nu + h_\nu\chi_\nu) - \prod_{\nu=1}^{n} \rho_\nu(v_\nu) \Big\} \prod_{\nu=1}^{n} e(-\gamma_\nu' v_\nu - h_\nu\gamma_\nu'\chi_\nu).$$

En vertu de (45) et (46) on trouve donc

$$\Sigma_1 \prod_{\nu=1}^{n} \rho_\nu(v_\nu)\, e(-\gamma_\nu' v_\nu) << g_1 \dots g_n X^{-m} x^{-\zeta} < T x^{-\zeta},$$

où ζ désigne un nombre fixe quelconque. Il en résulte que

$$\sum_{\gamma' \text{ dans } x'(\Omega_1', \Omega_2')}'' \Lambda(t, \gamma') << T x^{-\Omega},$$

où Σ'' est étendu aux systèmes γ' de $x'(\Omega_1', \Omega_2')$ pour lesquels le système de congruences cité n'est pas résoluble, de sorte que la première assertion découle de la seconde. D'une manière analogue on démontre qu'inversement la deuxième assertion résulte de la première.

Le même raisonnement nous apprend que les assertions des théorèmes B et C sont équivalentes aux suivantes:

Supposons les conditions du théorème B *ou* C *remplies. Dans le cas*

faible, à tout nombre fixe Ω *correspond un nombre fixe* Ω_1' *tel qu'on ait pour tout nombre fixe* $\Omega_2' \geqq \Omega_1'$

$$\sum_t w(t)\,|L(t) - \sum_{\gamma' \text{ dans } x'(\Omega_1', \Omega_2')} \Lambda(t,\gamma')|^2 << x^{-\Omega} T \sum_t w(t)$$

et dans le cas fort, il existe un nombre positif fixe ω_2' *tel qu'à chaque nombre positif fixe* $\omega_1' \leqq \omega_2'$ *corresponde un nombre positif fixe* ω *avec la propriété*

$$\sum_t w(t)\,|L(t) - \sum_{\gamma' \text{ dans } X'(\omega_1', \omega_2')} \Lambda(t,\gamma')|^2 << X^{-\omega} T \sum_t w(t).$$

Passons à la démonstration des trois théorèmes fondamentaux.

Démonstration. I. Introduction.

Nous pouvons supposer que X soit supérieur à tout nombre fixe donné d'avance; en effet sinon les assertions des théorèmes fondamentaux sont évidentes. Introduisons n nombres naturels fixes quelconques $k_1, \ldots, k_n$. Comme je vais le montrer maintenant, on peut supposer, sans nuire à la généralité, que les nombres $b_{1\nu}, \ldots, b_{m\nu}$ soient divisibles par k_ν $(\nu = 1, \ldots, n)$. Je le démontrerai seulement pour le cas faible du théorème A; les autres cas peuvent être traités de la même manière. Supposons que le théorème A, pris dans le sens faible, soit déjà démontré dans le cas particulier, où $b_{1\nu}, \ldots, b_{m\nu}$ sont divisibles par k_ν $(\nu = 1, \ldots, n)$. Introduisons n nombres naturels $h_\nu \leqq k_\nu$ $(\nu = 1, \ldots, n)$ et posons

$$r_\nu'(v) = \rho_\nu'(v) = 0, \qquad \text{si } v \equiv h_\nu \pmod{k_\nu}$$

$$r_\nu'(v) = r_\nu\left(\frac{v-h_\nu}{k_\nu}\right); \quad \rho_\nu'(v) = \rho_\nu\left(\frac{v-h_\nu}{k_\nu}\right) \text{ si } v \equiv h_\nu \pmod{k_\nu},$$

$$z_\nu'(\gamma_\nu') = \sum_{\varkappa=1}^{k_\nu} e\left(-\frac{h_\nu}{k_\nu}(\gamma_\nu' + \varkappa)\right) z_\nu\left(\frac{\gamma_\nu' + \varkappa}{k_\nu}\right).$$

Je dis que ces fonctions $r_\nu'(v)$, $\rho_\nu'(v)$, $z_\nu'(\gamma_\nu')$ et le nombre g_ν satisfont à la condition D. Pour obtenir ce résultat, il suffit de montrer que

$$(57) \qquad \sum_{v'=-\infty}^{\infty} e(\alpha' v')\, r_\nu'(v') - z_\nu'(\gamma_\nu') \sum_{v'=-\infty}^{\infty} e((\alpha' - \gamma_\nu')v')\, \rho_\nu'(v')$$

est $<< g_\nu x^{-c_9}$ pour chaque fraction irréductible γ_ν' à dénominateur $\leqq x^{\frac{1}{2}c_{10}}$ et pour tout nombre réel α' avec

$$(58) \qquad |\alpha' - \gamma_\nu'| \leqq X^{-1} x^{c_{11}}.$$

Si l'on pose

$$r = r_\nu, \quad \rho = \rho_\nu, \quad z = z_\nu, \quad g = g_\nu, \quad \alpha = \frac{\alpha' + \varkappa}{k_\nu}, \quad \frac{a}{q} = \frac{\gamma_\nu' + \varkappa}{k_\nu},$$

où $\varkappa$ désigne un nombre naturel $\leqq k_\nu$, on a

$|\alpha - \frac{a}{q}| = \frac{1}{k_\nu}\,|\alpha' - \gamma_\nu'| \leqq X^{-1} x^{c_{11}}$ et le dénominateur de $\frac{\gamma_\nu' + \varkappa}{k_\nu}$ est $\leqq k_\nu x^{\frac{1}{2}c_{10}} \leqq x^{c_{10}}$, si X est assez grand. On trouve ainsi, d'après la condition D, que la différence entre

$$(59) \qquad \sum_{v=-\infty}^{\infty} e\left(\frac{(\alpha' + \varkappa)(v - h_\nu)}{k_\nu}\right) r_\nu(v)$$

et

$$e\left(-\frac{h_\nu(\gamma_\nu' + \varkappa)}{k_\nu}\right) z_\nu\left(\frac{\gamma_\nu' + \varkappa}{k_\nu}\right) \sum_{v=-\infty}^{\infty} e\left(\frac{(\alpha' - \gamma_\nu')(v - h_\nu)}{k_\nu}\right) \rho_\nu(v)$$

est $<< g_\nu x^{-c_9}$.

Tout d'abord remarquons que la seconde expression ne change pas beaucoup, si l'on y remplace $\rho_\nu(v)$ par $\rho_\nu(v^*)$ et

$$e\left(\frac{(\alpha' - \gamma_\nu')(v - h_\nu)}{k_\nu}\right) \quad \text{par} \quad e\left(\frac{(\alpha' - \gamma_\nu')(v^* - h_\nu)}{k_\nu}\right),$$

où v^* désigne le plus petit nombre $\geqq v$ qui est congru à $h_\nu \pmod{k_\nu}$. En effet, l'erreur introduite par le premier changement est d'après (41), (45) et (46) certainement $<< g_\nu x^{-c_9}$ et l'erreur provenant du second changement, possède en vertu de (41), (58) et (42) également une valeur $<< g_\nu x^{-c_9}$. De cette manière nous trouvons que la différence entre (59) et

$$k_\nu\, e\left(-\frac{h_\nu(\gamma_\nu'+\varkappa)}{k_\nu}\right) z_\nu\left(\frac{\gamma_\nu'+\varkappa}{k_\nu}\right) \sum_{v\equiv h_\nu \pmod{k_\nu}} e\left(\frac{(\alpha'-\gamma_\nu')(v-h_\nu)}{k_\nu}\right) \rho_\nu(v)$$

est $<< g_\nu x^{-c_9}$. En sommant pour $\varkappa = 1, \ldots, k_\nu$, on trouve que l'expression (57), qui est égale à la différence entre

$$\sum_{v\equiv h_\nu \pmod{k_\nu}} e\left(\frac{\alpha'(v-h_\nu)}{k_\nu}\right) r_\nu(v),$$

et

$$z_\nu'(\gamma_\nu') \sum_{v\equiv h_\nu \pmod{k_\nu}} e\left(\frac{(\alpha'-\gamma_\nu')(v-h_\nu)}{k_\nu}\right) \rho_\nu(v)$$

est $<< g_\nu x^{-c_9}$.

Il est clair que la condition E reste valable, si l'on y remplace r_ν, ρ_ν et z_ν par r_ν', ρ_ν' et z_ν'. Posons $b'_{\mu\nu} = k_\nu b_{\mu\nu}$. Comme ces coefficients $b'_{\mu\nu}$ sont divisibles par k_ν, nous pouvons appliquer le théorème A. En remplaçant t_μ par

$$t_\mu' = t_\mu - \sum_{\nu=1}^{n} b_{\mu\nu} h_\nu \quad (\mu = 1, \ldots, m),$$

le cas particulier cité du théorème A nous apprend qu'à tout nombre fixe Ω correspond un nombre fixe Ω_1' tel qu'on ait pour tout nombre fixe $\Omega_2' \geqq \Omega_1'$

$$L(t,h) - \sum_{\gamma' \text{ dans } x'(\Omega_1', \Omega_2')} \Lambda(t,\gamma',h) << x^{-\Omega} T. \tag{60}$$

Dans cette formule on a

$$L(t,h) = \Sigma_{12} \prod_{\nu=1}^{n} r_\nu'(v_\nu') = \Sigma_{13} \prod_{\nu=1}^{n} r_\nu(v_\nu),$$

où Σ_{12} est étendu aux entiers $v_1', \ldots, v_n'$ avec

$$\sum_{\nu=1}^{n} b'_{\mu\nu} v_\nu' = t_\mu' \qquad (\mu = 1, \ldots, m),$$

et où Σ_{13} est donc étendu aux entiers $v_1, \ldots, v_n$, vérifiant les relations

$$\sum_{\nu=1}^{n} b_{\mu\nu} v_\nu = t_\mu \quad (\mu = 1, \ldots, m); \; v_\nu \equiv h_\nu \pmod{k_\nu} \quad (\nu = 1, \ldots, n).$$

En outre on a

$$\Lambda(t,\gamma',h) = \Sigma_{12} \prod_{\nu=1}^{n} e(-\gamma_\nu' v_\nu')\, \rho_\nu'(v_\nu')\, z_\nu'(\gamma_\nu')$$

$$= \sum_{\varkappa} \Sigma_{14} \Sigma_{12} \prod_{\nu=1}^{n} e\left(-\gamma_\nu' v_\nu' - \frac{h_\nu}{k_\nu}(\gamma_\nu'+\varkappa_\nu)\right) \rho_\nu(k_\nu v_\nu' + h_\nu)\, z_\nu\left(\frac{\gamma_\nu'+\varkappa_\nu}{k_\nu}\right),$$

où $\sum_{\varkappa} \Sigma_{14}$ est étendu aux systèmes $\varkappa$ formés par n nombres naturels $\varkappa_\nu \leqq k_\nu$. En posant $k_\nu v_\nu' + h_\nu = v_\nu$, on trouve donc

$$\sum_{h} \Sigma_{14} \Lambda(t,\gamma',h) = \sum_{\varkappa} \Sigma_{14} \Sigma_1\, e\left(-\frac{(\gamma_\nu'+\varkappa_\nu)v_\nu}{k_\nu}\right) \rho_\nu(v_\nu)\, z_\nu\left(\frac{\gamma_\nu'+\varkappa_\nu}{k_\nu}\right).$$

A chaque couple $\varkappa_\nu, \gamma_\nu'$, où $\varkappa_\nu$ est un nombre naturel $\leqq k_\nu$ et γ_ν' une fraction irréductible $\geqq 0$ et < 1, correspond une seule fraction γ_ν'' avec

$$\gamma_\nu'' \equiv \frac{\gamma_\nu'+\varkappa_\nu}{k_\nu} \pmod 1 \text{ et } 0 \leqq \gamma_\nu'' < 1;$$

réciproquement, à chaque fraction γ_ν'' correspond un seul couple $\varkappa_\nu, \gamma_\nu'$. Si le dénominateur de γ_ν' est $\leqq x^{\Omega_1'}$, celui de γ_ν'' est $\leqq k_\nu x^{\Omega_1'} \leqq x^{2\Omega_1'}$, quand X est assez grand; si le dénominateur de γ_ν'' est $\leqq x^{\frac{1}{2}\Omega_2'}$, celui de γ_ν' est $\leqq k_\nu x^{\frac{1}{2}\Omega_2'} \leqq x^{\Omega_2'}$, lorsque X est suffisamment grand. La somme

$$\sum_{\gamma'' \text{ dans } x'(2\Omega_1', \frac{1}{2}\Omega_2')} \Lambda(t,\gamma''),$$

où Ω_2' est $\geqq 4\Omega_1'$, peut donc être mise sous la forme

$$\sum_{h} \Sigma_{14} \sum_{\gamma' \text{ dans } x'(\Omega_1', \Omega_2')} \Lambda(t,\gamma',h).$$

La relation

$$\sum_{h} \Sigma_{14} L(t,h) = L(t)$$

est immédiate, de sorte que (60) nous apprend

$$L(t) - \sum_{\gamma'' \text{ dans } x'(2\Omega_1', \frac{1}{2}\Omega_2')} L(t, \gamma'') << x^{-\Omega} T.$$

Il suit de ce résultat qu'on peut, sans nuire à la généralité, supposer les nombres $b_{\mu\nu}$ divisibles par k_ν $(\nu = 1, \ldots, n)$. Dans le reste de la démonstration je supposerai que les $m(n-m)$ nombres $b_{\mu\nu}$, où ν est $> m$, soient divisibles par la valeur absolue du déterminant figurant dans (44).

Dans la démonstration des cas faibles j'introduis un nombre fixe quelconque Ω, ensuite un nombre fixe convenable Ω_1 (dépendant de Ω), en outre un nombre fixe quelconque $\Omega_2 \geqq \Omega_1$ et finalement un nombre fixe convenable Ω_3 (dépendant de Ω et Ω_2). Dans la démonstration des cas forts j'introduis un nombre positif fixe convenable $\omega_2 < \frac{1}{4}$, un nombre positif fixe quelconque $\omega_1 \leqq \omega_2$ et deux nombres positifs fixes convenables $\omega_3 < \frac{1}{4}$ et ω (dépendants de ω_1). Plus loin je fixerai le choix des nombres Ω_1, Ω_3, ω_2, ω_3, et ω.

Dans les cas faibles j'adjoins à chaque système γ de $x(\Omega_1, \Omega_2)$ le cube $j(\gamma)$ à m dimensions dont le centre coïncide avec le point γ et dont les arêtes sont parallèles aux axes de coordonnées et possèdent la longueur $2X^{-1}x^{\Omega_3}$. Dans les cas forts j'associe à chaque système γ de $X(\omega_1, \omega_2)$ le cube $j(\gamma)$ à m dimensions dont le centre coïncide avec γ et dont les arêtes sont parallèles aux axes de coordonnées et possèdent la longueur $2X^{-1+\omega_3}$.

En tenant compte dans les cas forts de ce que ω_2 et ω_3 sont inférieurs à $\frac{1}{4}$, on voit pour des valeurs assez grandes de X, qu'il est impossible de trouver deux points $\alpha = (\alpha_1, \ldots, \alpha_m)$ et $\alpha' = (\alpha_1', \ldots, \alpha_m')$ appartenant à deux cubes $j(\gamma)$ différents, tels qu'on ait

$$\alpha_\mu \equiv \alpha_\mu' \pmod 1 \quad (\mu = 1, \ldots, m). \tag{61}$$

Désignons par j' la partie du cube $0 \leqq \alpha_\mu < 1$ $(\mu = 1, \ldots, m)$, formée par les points α, auxquels ne correspond aucun point α' situé dans un des cubes $j(\gamma)$ et vérifiant les congruences (61). Si $\chi(\alpha) = \chi(\alpha_1, \ldots, \alpha_m)$ est une fonction continue quelconque de période 1 des variables $\alpha_1, \ldots, \alpha_m$ on a

$$\int_0^1 d\alpha\, \chi(\alpha) = \sum_\gamma{}_{15} \int_{j(\gamma)} d\alpha\, \chi(\alpha) + \int_{j'} d\alpha\, \chi(\alpha); \tag{62}$$

$\sum_\gamma{}_{15}$ est étendu dans les cas faibles aux systèmes γ de $x(\Omega_1, \Omega_2)$, dans les cas forts aux systèmes γ de $X(\omega_1, \omega_2)$; le membre de gauche de (62) est une abréviation pour

$$\int_0^1 \cdots \int_0^1 \chi(\alpha_1, \ldots, \alpha_m)\, d\alpha_1, \ldots, d\alpha_m,$$

de même que la dernière intégrale, figurant dans (62) est une abréviation pour

$$\int_{j'} \cdots \int \chi(\alpha_1, \ldots, \alpha_m)\, d\alpha_1 \ldots d\alpha_m.$$

Si X est suffisamment grand, le cube $j(\gamma)$ est une partie du parallélépipède $J(\gamma)$, défini par les inégalités

$$-\tfrac{1}{2} \leqq \sum_{\mu=1}^{m} b_{\mu\nu}(\alpha_\mu - \gamma_\mu) < \tfrac{1}{2} \quad (\nu = 1, \ldots, m).$$

Posons pour $\nu = 1, \ldots, n$

$$F_\nu(\alpha) = \sum_{v=-\infty}^{\infty} r_\nu(v)\, e(v \sum_\mu \alpha_\mu b_{\mu\nu})$$

et

$$\Phi_\nu(\alpha) = \sum_{v=-\infty}^{\infty} \rho_\nu(v)\, e(v \sum_\mu \alpha_\mu b_{\mu\nu}); \tag{63}$$

$\sum_\mu$ est étendu aux nombres naturels $\mu \leqq m$. Posons en outre

$$W(\alpha, \gamma) = (\prod_\nu F_\nu(\alpha)) - \gamma_1(\gamma) \prod_\nu \Phi_\nu(\alpha - \gamma); \tag{64}$$

$\prod_\nu$ est étendu aux nombres naturels $\nu \leqq n$; il va sans dire qu'on obtient $\Phi_\nu(\alpha - \gamma)$ en remplaçant dans (63) α_μ par $\alpha_\mu - \gamma_\mu$. Nous avons

$$L(t) = \sum_1 \prod_\nu r_\nu(v_\nu) = \int_0^1 d\alpha \sum_{v_1=-\infty}^{\infty} \cdots \sum_{v_n=-\infty}^{\infty} \prod_\nu r_\nu(v_\nu)\, e(\sum_\mu \alpha_\mu(-t_\mu + \sum_\nu b_{\mu\nu} v_\nu))$$

$$= \sum_\gamma{}_{15} \int_{j(\gamma)} d\alpha\, (\prod_\nu F_\nu(\alpha))\, e(-\sum_\mu \alpha_\mu t_\mu) + U_1(t), \tag{65}$$

où

$$U_1(t) = \int_{j'} d\alpha \,(\prod_\nu F_\nu(\alpha))\, e(-\sum_\mu \alpha_\mu t_\mu).$$

Le premier terme figurant dans (65) est égal à

$$U_2(t) = \sum_\gamma{}_{15} \int_{j(\gamma)} d\alpha\, W(\alpha,\gamma)\, e(-\sum_\mu \alpha_\mu t_\mu),$$

augmenté de

$$\sum_\gamma{}_{15}\, \eta(\gamma) \int_{j(\gamma)} d\alpha\, (\prod_\nu \Phi_\nu(\alpha-\gamma))\, e(-\sum_\mu \alpha_\mu t_\mu).$$

On obtient ainsi

$$(66)\quad L(t) - \sum_\gamma{}_{15}\eta(\gamma) \int_{J(\gamma)} d\alpha\, (\prod_\nu \Phi_\nu(\alpha-\gamma))\, e(-\sum_\mu \alpha_\mu t_\mu) = U_1(t) + U_2(t) - U_3(t),$$

où

$$U_3(t) = \sum_\gamma{}_{15}\,\eta(\gamma) \int_{J(\gamma)-j(\gamma)} d\alpha\, (\prod_\nu \Phi_\nu(\alpha-\gamma))\, e(-\sum_\mu \alpha_\mu t_\mu).$$

L'intégrale figurant dans (66) possède la valeur

$$e(-\sum_\mu \gamma_\mu t_\mu) \int_{J(0)} d\alpha\, (\prod_\nu \Phi_\nu(\alpha))\, e(-\sum_\mu \alpha_\mu t_\mu)$$

$$= e(-\sum_\mu \gamma_\mu t_\mu) \sum_{v_1=-\infty}^{\infty} \cdots \sum_{v_n=-\infty}^{\infty} (\prod_{\nu=1}^{n} \rho_\nu(v_\nu))\, I_3,$$

où

$$I_3 = \int_{J(0)} d\alpha\, e(\sum_\mu \alpha_\mu (\sum_\nu b_{\mu\nu} v_\nu - t_\mu)).$$

Considérons les points $\tau = (\tau_1, \ldots, \tau_m)$ tels que les nombres

$$\tau_\nu' = \sum_\mu b_{\mu\nu}\tau_\mu \quad (\nu = 1, \ldots, n)$$

possèdent la propriété que $\tau_1', \ldots, \tau_m'$ soient entiers. Comme chacun des m $(n-m)$ coefficients $b_{\mu\nu}$, où ν est $> m$, est divisible par la valeur absolue du déterminant (44), les nombres $\tau'_{m+1}, \ldots, \tau_n'$ sont également entiers. Le nombre b^{-1} de ces points τ avec la condition supplémentaire $0 \leqq \tau_\mu < 1$ est donc égal à la valeur absolue du déterminant (44) nommé et l'intégrale I_3 possède la valeur b pour chaque système d'entiers $v_1, \ldots, v_n$ avec la propriété

$$\sum_\nu b_{\mu\nu} v_\nu = t_\mu \quad (\mu = 1, \ldots, m).$$

Considérons maintenant un système d'entiers $v_1, \ldots, v_n$ pour lesquels ces m relations ne sont pas remplies en même temps. Comme $\tau_1', \ldots, \tau_n'$ sont entiers pour chaque point τ cité, on a

$$e(\sum_\mu (\alpha_\mu + \tau_\mu)(\sum_\nu b_{\mu\nu} v_\nu - t_\mu)) = e(-\sum_\mu \tau_\mu t_\mu + \sum_\mu \alpha_\mu (\sum_\nu b_{\mu\nu} v_\nu - t_\mu)),$$

par conséquent

$$e(-\sum_\mu \tau_\mu t_\mu) \int_{J(\tau)} d\alpha\, e(\sum_\mu \alpha_\mu (\sum_\nu b_{\mu\nu} v_\nu - t_\mu)) = I_3.$$

La somme de ces intégrales, étendue à tous les points τ avec $|\tau_\mu| \leqq \xi$ $(\mu = 1, \ldots, m)$ est pour les très grandes valeurs de ξ d'une part approximativement égale à

$$e(-\sum_\mu \tau_\mu t_\mu) \int_{|\alpha_\mu| \leqq \xi} d\alpha\, e(\sum_\mu \alpha_\mu (\sum_\nu b_{\mu\nu} v_\nu - t_\mu)) =$$

$$e(-\sum_\mu \tau_\mu t_\mu) \prod_\mu \int_{-\xi}^{\xi} e(u(\sum_\nu b_{\mu\nu} v_\nu - t_\mu))\, du,$$

donc approximativement égale à zéro, d'autre part égale à I_3, multiplié par le nombre des points τ, situés dans le cube $|\tau_\mu| \leqq \xi$. On trouve donc $I_3 = 0$ et l'intégrale, figurant dans (66) possède la valeur

$$b\, e(-\sum_\mu \gamma_\mu t_\mu) \sum_1 \prod_{\nu=1}^{n} \rho_\nu(v_\nu) = b\, \Lambda(t)\, e(-\sum_\mu \gamma_\mu t_\mu),$$

d'où

$$L(t) - b\,\Lambda(t) \sum_{\gamma} {}_{15}\eta(\gamma)\, e\Big(-\sum_{\mu} \gamma_\mu t_\mu\Big) = U_1(t) + U_2(t) - U_3(t).$$

Nous avons maintenant besoin de bornes supérieures convenables pour les contributions de $U_1(t)$, $U_2(t)$ et $U_3(t)$.

Dans les cas faibles je déduirai des conditions du théorème A les inégalités

$$U_1(t) << x^{-\Omega} \sum_{\lambda=1}^{m} g_\lambda \sqrt{R_\lambda} \tag{67}$$

et

$$U_3(t) << x^{-\Omega} \sum_{\lambda=1}^{m} g_\lambda \sqrt{P_\lambda}, \tag{68}$$

des conditions du théorème B

$$\sum_t w(t)\,|U_1(t)|^2 << x^{-\Omega} X^{-m} \sum_{\lambda=1}^{m} g_\lambda^2 R_\lambda \cdot \sum_t w(t) \tag{69}$$

et

$$\sum_t w(t)\,|U_3(t)|^2 << x^{-\Omega} X^{-m} \sum_{\lambda=1}^{m} g_\lambda^2 P_\lambda \cdot \sum_t w(t) \tag{70}$$

et finalement des conditions du théorème C

$$\sum_t w(t)\,|U_1(t)|^2 << x^{-\Omega}(X^{-2m} g_1^2 \dots g_n^2 + R) \sum_t w(t) \tag{71}$$

et

$$\sum_t w(t)\,|U_3(t)|^2 << x^{-\Omega}(X^{-2m} g_1^2 \dots g_n^2 + P) \sum_t w(t). \tag{72}$$

En outre on a dans les cas faibles dans les conditions de A, B et C

$$U_2(t) << x^{-\Omega_4} X^{-m} g_1 \dots g_n, \tag{73}$$

où $\Omega_4 = \Omega$ dans le théorème A, et $\Omega_4 = \frac{1}{2}\Omega$ dans les deux autres théorèmes. Dans les cas forts on peut remplacer dans les résultats précédents $x^{-\Omega}$ par $X^{-\omega}$.

Dans les cas faibles je trouverai les résultats concernant $U_1(t)$ dans la deuxième partie de cette démonstration, ceux concernant $U_3(t)$ dans la troisième et ceux concernant $U_2(t)$ dans la quatrième; les cinquième, sixième et septième parties contiendront pour les cas forts les formules analogues, respectivement pour $U_2(t)$, $U_3(t)$ et $U_1(t)$; donc en sens inverse.

II. Sur $U_1(t)$ dans les cas faibles.

Dans les conditions du théorème C il existe un nombre fixe c_{25} tel que l'inégalité

$$\sum_t w(t)\, e\Big(\sum_\mu \alpha_\mu t_\mu\Big) << x^{-\Omega} \sum_t w(t) \tag{74}$$

soit remplie pour tous les points $\alpha = (\alpha_1, \dots, \alpha_m)$, excepté ceux pour lesquels chacun des m intervalles $(\alpha_\mu \mp X^{-1} x^{c_{25}})$ contient au moins une fraction à dénominateur $\leqslant x^{c_{25}}$. Dans la démonstration des théorèmes A et B je poserai $c_{25} = 0$. Les inégalités (48) nous fournissent un nombre positif fixe c_{26} tel que nous ayons

$$\sum_{v=-\infty}^{\infty} r_\mu(v)\, e(\alpha v) << g_\mu x^{-\Omega-m-3m c_{25}} \quad (\mu = 1, \dots, m) \tag{75}$$

pour tout nombre réel α avec la propriété que l'intervalle $(\alpha \mp X^{-1} x^{c_{26}})$ ne contienne aucune fraction à dénominateur $\leqslant x^{c_{26}}$. Posons $\Omega_1 = m c_{26} + 1$, $\Omega_2 \geqslant \Omega_1$ et $\Omega_3 \geqslant \Omega_1$ et démontrons (67), (69) et (71).

Supposons pour l'instant qu'à au moins un point $\alpha = (\alpha_1, \dots, \alpha_m)$ de j' correspondent m fractions Γ_λ $(\lambda = 1, \dots, m)$ dont les dénominateurs sont $\leqslant x^{c_{26}}$ et qui vérifient les m inégalités

$$\Big|\sum_\mu \alpha_\mu b_{\mu\lambda} - \Gamma_\lambda\Big| \leqslant X^{-1} x^{c_{26}} \quad (\lambda = 1, \dots, m). \tag{76}$$

En vertu de (44) on peut trouver m fractions irréductibles γ_μ' qui satisfont aux système

$$\sum_\mu b_{\mu\lambda} \gamma_\mu' = \Gamma_\lambda \quad (\lambda = 1, \dots, m). \tag{77}$$

Les dénominateurs de ces fractions sont $<< x^{m c_{26}}$ et les relations (76) et (77) nous apprennent

$$\alpha_\mu - \gamma_\mu' << X^{-1} x^{c_{26}} \quad (\mu = 1, \dots, m),$$

de sorte que l'on a $0 \leqslant \gamma_\mu' \leqslant 1$, si X est assez grand. Posons

$$\alpha_\mu' = \alpha_\mu; \quad \gamma_\mu = \gamma_\mu' \quad \text{si} \quad \gamma_\mu' < 1,$$

$$\alpha_\mu' = \alpha_\mu - 1; \quad \gamma_\mu = 0, \quad \text{si} \quad \gamma_\mu' = 1.$$

Alors nous trouvons

$$\alpha_\mu' - \gamma_\mu << X^{-1} x^{c_{26}} \quad (\mu = 1, \ldots, m).$$

Pour les valeurs assez grandes de X on obtient donc en vertu de $\Omega_3 \geqslant \Omega_1 = mc_{26} + 1$, que $\alpha_\mu' - \gamma_\mu$ est en valeur absolue $< X^{-1} x^{\Omega_3}$ et que le dénominateur de γ_μ est $< x^{\Omega_3}$. Il suivrait de ce résultat que α' serait situé dans $j(\gamma)$, ce qui est impossible, puisque α appartient à j'.

De cette manière nous avons trouvé qu'à tout point α de j' correspond au moins un nombre naturel $\lambda \leqslant m$ tel qu'on ait pour chaque fraction Γ_λ à dénominateur $\leqslant x^{c_{26}}$

$$|\sum_\mu \alpha_\mu b_{\mu\lambda} - \Gamma_\lambda| > X^{-1} x^{c_{26}}.$$

La formule (75), appliquée avec $\sum_\mu \alpha_\mu b_{\mu\lambda}$ au lieu de α nous apprend donc

$$F_\lambda(\alpha) << g_\lambda x^{-\Omega - m - 3mc_{25}}. \tag{78}$$

Considérons maintenant séparément les trois théorèmes fondamentaux.

II A. Dans les conditions du théorème A il résulte de (78) que

$$U_1(t) << x^{-\Omega} \sum_{\lambda=1}^{m} g_\lambda I_4,$$

où

$$I_4 = \int_0^1 d\alpha \, |\prod_{\nu \neq \lambda} F_\nu(\alpha)|.$$

On a

$$\prod_{\nu \neq \lambda} F_\nu(\alpha) = \Pi_1 F_\nu(\alpha) . \Pi_2 F_\nu(\alpha);$$

Π_1 est étendu aux nombres $\nu = \lambda_1, \ldots, \lambda_l$ et Π_2 aux nombres $\nu = \lambda_{l+1}, \ldots, \lambda_{n-1}$. Le carré de I_4 est en vertu de l'inégalité de Schwarz tout au plus égal au produit des deux intégrales

$$I_5 = \int_0^1 d\alpha \, \Pi_1 |F_\nu(\alpha)|^2 \quad \text{et} \quad I_6 = \int_0^1 d\alpha \, \Pi_2 |F_\nu(\alpha)|^2.$$

L'intégrale I_5 possède la valeur

$$\int_0^1 d\alpha \, \Pi_1 F_\nu(\alpha) \overline{F}_\nu(\alpha) = \Sigma_{16} \Pi_1 r_\nu(v_\nu) \overline{r}_\nu(v_\nu') I_7,$$

où Σ_{16} est étendu aux entiers $v_{\lambda_1}, \ldots, v_{\lambda_l}, v'_{\lambda_1}, \ldots, v'_{\lambda_l}$ et où

$$I_7 = \int_0^1 d\alpha e\Big(\sum_\mu \alpha_\mu \sum_{\nu = \lambda_1, \ldots, \lambda_l} b_{\mu\nu}(v_\nu - v_\nu')\Big)$$

possède d'après le raisonnement donné dans la partie I de cette démonstration, la valeur 1 ou zéro, selon que le système

$$\sum_{\nu = \lambda_1, \ldots, \lambda_l} b_{\mu\nu}(v_\nu - v_\nu') = 0 \quad (\mu = 1, \ldots, m) \tag{79}$$

est vérifié ou non. On a donc

$$I_5 = \Sigma_{17} \Pi_1 \rho_\nu(v_\nu) \overline{\rho}_\nu(v_\nu'),$$

étendu aux systèmes v_ν, v_ν' $(\nu = \lambda_1, \ldots, \lambda_l)$ vérifiant (79). De la même manière on trouve un résultat analogue pour I_6, de sorte que $I_5 I_6$ est égal au nombre R_λ défini dans (51) et que I_4 est $\leqslant \sqrt{R_\lambda}$. Nous avons trouvé ainsi (67).

II B. Dans les conditions du théorème B on a

$$\sum_t w(t) |U_1(t)|^2 =$$

$$\left\{ \int_{j'} \int_{j'} d\alpha \, d\beta \, (\prod_\nu F_\nu(\alpha) \overline{F}_\nu(\beta)) \sum_t w(t) e\Big(\sum_\mu (\beta_\mu - \alpha_\mu) t_\mu\Big). \right. \tag{80}$$

Une sommation par parties nous apprend en vertu de (53) que pour tout nombre réel u et pour $\mu = 1, \ldots, m$,

$$\sum_{h=-\infty}^{\infty} w_\mu(h) e(uh) << \sigma(u) \sum_{h=-\infty}^{\infty} w_\mu(h),$$

où $\sigma(u)$ désigne le plus petit des nombres 1 et $X^{-1} |\sin \pi u|^{-1}$. Le membre

de gauche de (80) est donc en vertu de (78) et de $F_\lambda(\beta) << g_\lambda$ (cette inégalité suit de (42)) certainement

$$<< \sum_t w(t). \int_{j'}^{} \int_{j'}^{} d\alpha\, d\beta \,|\prod_\nu F_\nu(\alpha) F_\nu(\beta)|. \prod_\mu \sigma(\beta_\mu - \alpha_\mu)$$

$$<< x^{-\Omega-m} \sum_t w(t) \sum_{\lambda=1}^{m} g_\lambda^2 I_8,$$

où

$$I_8 = \int_0^1 \int_0^1 d\alpha\, d\beta \,|\prod_{\nu \neq \lambda} F_\nu(\alpha) F_\nu(\beta)|. \prod_\mu \sigma(\beta_\mu - \alpha_\mu).$$

On a donc $I_8 \leqslant \frac{1}{2}(I_9 + I_{10})$, où

$$I_9 = \int_0^1 \int_0^1 d\alpha\, d\beta \,|\prod_{\nu \neq \lambda} F_\nu(\alpha)|^2 \prod_\mu \sigma(\beta_\mu - \alpha_\mu);$$

si l'on remplace $F_\nu(\alpha)$ par $F_\nu(\beta)$, on obtient I_{10}, de sorte que I_9 et I_{10} possèdent la même valeur.

$\sigma(u)$ étant une fonction de u de période 1, la substitution $\beta_\mu = \alpha_\mu + u_\mu$ transforme I_9 en I_{11} I_{12}, où

$$I_{11} = \prod_\mu \int_{-\frac{1}{2}}^{\frac{1}{2}} \sigma(u)\, du << X^{-m} x^m$$

et

$$I_{12} = \Sigma_{18} \left(\prod_{\nu \neq \lambda} r_\nu(v_\nu) \overline{r}_\nu(v_\nu')\right) \int_0^1 d\alpha\, e\left(\sum_\mu \alpha_\mu \sum_{\nu \neq \lambda} b_{\mu\nu}(v_\nu - v_\nu')\right)$$

$$= \Sigma_{19} \prod_{\nu \neq \lambda} r_\nu(v_\nu) \overline{r}_\nu(v_\nu');$$

Σ_{18} est étendu aux points à $2n-2$ coordonnées entières v_ν, v_ν' $(\nu \neq \lambda)$, et Σ_{19} à ceux de ces points qui satisfont aux m relations

$$\sum_{\nu \neq \lambda} b_{\mu\nu}(v_\nu - v_\nu') = 0 \quad (\mu = 1, \ldots, m),$$

de sorte que I_{12} est égal au nombre R_λ défini dans (52). I_8 est donc $<< X^{-m} x^m R_\lambda$ et on obtient (69).

II C. La relation (80) est vérifiée aussi dans les conditions du théorème C. Considérons d'abord la contribution au membre de droite de (80) des points α et β tels que chaque fraction située dans au moins un des m intervalles $(\beta_\mu - \alpha_\mu \mp X^{-1} x^{c_{25}})$ possède un dénominateur $> x^{c_{25}}$. Dans ce cas nous pouvons utiliser (74) avec $\beta_\mu - \alpha_\mu$ au lieu de α_μ, de sorte que la susdite contribution est

$$<< x^{-\Omega} I_{13}^2 \sum_t w(t),$$

où

$$I_{13} = \int_0^1 d\alpha \,|\prod_\nu F_\nu(\alpha)|.$$

On a donc

$$I_{13}^2 \leqslant \int_0^1 d\alpha. \,|\prod_{\nu=1}^{l} F_\nu(\alpha)|^2. \,|\prod_{\nu=l+1}^{n} F_\nu(\alpha)|^2$$

et le raisonnement de II B nous montre que le membre de droite est égal au nombre R défini par (54). Pour obtenir (71) il suffit donc de considérer la contribution au membre de droite de (80) des points α et β tels que chacun des m intervalles $(\beta_\mu - \alpha_\mu \mp X^{-1} x^{c_{25}})$ contienne au moins une fraction à dénominateur $\leqq x^{c_{25}}$.

En vertu de (75) et $F_\nu(\alpha) << g_\nu$, cette dernière contribution est

$$<< x^{-\Omega-3mc_{25}} g_1 \ldots g_n \sum_t w(t). \int_0^1 d\beta \,|\prod_\nu F_\nu(\beta)| \int^{*} d\alpha,$$

où $\int^{*} d\alpha$ est étendu aux points $\alpha = (\alpha_1, \ldots, \alpha_m)$ tels qu'on ait $0 \leqslant \alpha_\mu \leqq 1$ et que chacun des m intervalles $(\beta_\mu - \alpha_\mu \mp X^{-1} x^{c_{25}})$ contienne au moins une fraction γ_μ à dénominateur $\leqslant x^{c_{25}}$. Le nombre des systèmes $\gamma = (\gamma_1, \ldots, \gamma_m)$ qui entrent en considération est $<< x^{2mc_{25}}$ et on a donc

$$\int^{*} d\alpha << X^{-m} x^{3mc_{25}}.$$

Par conséquent la contribution nommée est

$$<< X^{-m} x^{-\Omega} g_1 \dots g_n I_{14} \sum_t w(t),$$

où

$$I_{14} = \int_0^1 d\beta \left| \prod_\nu F_\nu(\beta) \right|$$

possède un carré qui est tout au plus égal à

$$\int_0^1 d\beta \left| \prod_{\nu=1}^{l} F_\nu(\beta) \right|^2 . \int_0^1 d\beta \left| \prod_{\nu=l+1}^{n} F_\nu(\beta) \right|^2 = R.$$

La contribution en question est donc

$$<< x^{-\Omega} X^{-m} g_1 \dots g_n \sqrt{R} \sum_t w(t)$$

$$< x^{-\Omega} (X^{-2m} g_1^2 \dots g_n^2 + R) \sum_t w(t).$$

III. Sur $U_3(t)$ dans les cas faibles.

Supposons fixé $\Omega_1 = m c_{26} + 1$. Désignons par Ω_2 un nombre fixe quelconque $\geqq \Omega_1$. Dans les conditions du théorème C il existe un nombre positif fixe c_{27} tel que l'inégalité

$$\sum_t w(t)\, e(\alpha_\mu t_\mu) << x^{-\Omega-4m\Omega_2} \sum_t w(t), \tag{81}$$

soit vérifiée pour tous les points $\alpha = (\alpha_1, \dots, \alpha_m)$, excepté ceux pour lesquels chacun des m intervalles $(\alpha_\mu \mp X^{-1} x^{c_{27}})$ contient au moins une fraction à dénominateur $\leqq x^{c_{27}}$. Posons dans les démonstrations des théorèmes A, B et C respectivement

$$\Omega_3 = \Omega + 1 + mn\Omega_2 c_8 + 2m\Omega_2;$$

$$\Omega_3 = \Omega + 1 + m + 2mn\Omega_2 c_8 + 4m\Omega_2;$$

$$\Omega_3 = \Omega + 1 + 2mn\Omega_2 c_8 + 3m c_{27};$$

dans ces formules c_8 est la constante figurant dans (41).

Supposons pour l'instant qu'à au moins un point $\alpha = (\alpha_1, \dots, \alpha_m)$ de $J(\gamma) - j(\gamma)$ correspondent m entiers $y_1, \dots, y_m$ tels que nous ayons pour $\lambda = 1, \dots, m$

$$\left| \sum_\mu b_{\mu\lambda} (\alpha_\mu - \gamma_\mu) - y_\lambda \right| \leqq X^{-1} x^{\Omega_3 - 1}. \tag{82}$$

Il suivrait de la définition de $J(\gamma)$ que les entiers $y_1 \dots, y_m$ s'annulent, si X est assez grand. Comme le déterminant (44), formé par les m^2 coefficients $b_{11}, \dots, b_{mm}$ ne s'annule pas, on trouverait pour $\mu = 1, \dots, m$

$$|\alpha_\mu - \gamma_\mu| << X^{-1} x^{\Omega_3 - 1}, \text{ donc } < X^{-1} x^{\Omega_3}$$

pour les valeurs assez grandes de X. On trouve ainsi une contradiction, puisque α n'appartient pas à $j(\gamma)$. De cette manière nous avons trouvé qu'à tout point α de $J(\gamma) - j(\gamma)$ correspond au moins un nombre naturel $\lambda \leqq m$ tel que nous ayons pour tout entier y

$$\left| \sum_\mu b_{\mu\lambda} (\alpha_\mu - \gamma_\mu) - y \right| > X^{-1} x^{\Omega_3 - 1},$$

par conséquent

$$\left| \sin \left(\pi \sum_\mu b_{\mu\nu} (\alpha_\mu - \gamma_\mu) \right) \right| > \left| \sin \pi X^{-1} x^{\Omega_3 - 1} \right| \geqslant X^{-1} x^{\Omega_3 - 1}$$

et (45) nous fournit grâce à la sommation par parties

$$\Phi_\lambda(\alpha - \gamma) << g_\lambda x^{-\Omega_3 + 1}. \tag{83}$$

Cette inégalité est analogue à (78), mais $F_\lambda(\alpha)$ est remplacé par $\Phi_\lambda(\alpha - \gamma)$.

Le nombre des systèmes γ formés par m fractions irréductibles γ_μ à dénominateur $\leqq x^{\Omega_2}$ est au plus $x^{2m\Omega_2}$. Comme $\sum_\mu b_{\mu\nu} \gamma_\mu$ est égal à une fraction à dénominateur $<< x^{m\Omega_2}$, il suit de (41) qu'on a

$$\eta(\gamma) = \prod_\nu z_\nu \left(\sum_\mu b_{\mu\nu} \gamma_\mu \right) << x^{mn\Omega_2 c_8}. \tag{84}$$

Séparons maintenant les raisonnements relatifs aux trois théorèmes différents.

III A. Dans les conditions du théorème A on trouve en vertu de (83) et (84)

$$U_3(t) << x^{-\Omega_3+1+mn\Omega_2 c_8} \sum_{\gamma 15} \sum_{\lambda=1}^{m} g_\lambda I_{15},$$

où

$$I_{15} = \int_{J(\gamma)} d\alpha \,|\, \prod_{\nu\neq\lambda} \Phi_\nu(\alpha-\gamma)\,| = \int_{J(0)} d\alpha \,|\, \prod_{\nu\neq\lambda} \Phi_\nu(\alpha)\,|,$$

par conséquent $I_{15}^2 \leqq I_{16} I_{17}$, où

$$I_{16} = \int_{J(0)} d\alpha \,|\, \Pi_1 \Phi_\nu(\alpha)\,|^2 \quad \text{et} \quad I_{17} = \int_{J(0)} d\alpha \,|\, \Pi_2 \Phi_\nu(\alpha)\,|^2.$$

Un raisonnement analogue à celui de II A nous apprend que $I_{16}\, I_{17}$ est égal à P_λ. Comme le nombre de termes de la somme Σ_{15} est $\leqq x^{2m\Omega_2}$, on obtient

$$U_3(t) << x^{-\Omega_3+1+mn\Omega_2 c_8+2m\Omega_2} \sum_{\lambda=1}^{m} g_\lambda \sqrt{P_\lambda}.$$

d'où résulte (68).

III B. Dans les conditions du théorème B les inégalités (83) et (84) nous donnent

$$\sum_t w(t)\,|\,U_3(t)\,|^2 << x^{-\Omega_3+1+2mn\Omega_2 c_8} \sum_t w(t) \sum_{\lambda=1}^{m} g_\lambda^2 \sum_{\gamma 15} \sum_{\gamma' 15} I_{18},$$

où

$$I_{18} = \int_{J(\gamma)} \int_{J(\gamma')} d\alpha\, d\beta \,|\, \prod_{\nu\neq\lambda} \Phi_\nu(\alpha-\gamma)\, \overline{\Phi}_\nu(\beta-\gamma')\,|\, \prod_\mu \sigma(\beta_\mu-\alpha_\mu)$$

possède d'après le raisonnement tenu dans II B une valeur $<< X^{-m} x^m P_\lambda$. Nous obtenons donc

$$\sum_t w(t)\,|\,U_3(t)\,|^2 << x^{-\Omega_3+1+m+2mn\Omega_2 c_8+4m\Omega_2} X^{-m} \sum_{\lambda=1}^{m} g_\lambda^2 P_\lambda \sum_t w(t),$$

d'où suit (70).

III C. Dans les conditions du théorème C les points α et β tels que chaque fraction située dans au moins un des m intervalles $(\beta_\mu - \alpha_\mu \mp X^{-1} x^{c_{27}})$ possède un dénominateur $> x^{c_{27}}$, fournissent à la somme

$$\sum_t w(t)\,|\,U_3(t)\,|^2$$

une contribution, qui est d'après (81)

$$<< x^{-\Omega-4m\Omega_2} \sum_t w(t) \sum_{\gamma 15} \sum_{\gamma' 15} I_{19} I_{20},$$

où

$$I_{19} = \int_{J(\gamma)} d\alpha \,|\, \prod_\nu \Phi_\nu(\alpha-\gamma)\,|$$

et où I_{20} est l'intégrale analogue avec γ' au lieu de γ. On trouve donc que I_{19}^2 et I_{20}^2 sont $\leqslant P$, de sorte que la contribution des points cités α et β est $<< x^{-\Omega} P \Sigma w(t)$. La contribution des autres points α et β est d'après (83) et (84)

$$<< x^{-\Omega_3+1+2mn\Omega_2 c_8} g_1 \dots g_n \sum_t w(t) \sum_{\gamma 15} \sum_{\gamma' 15} I_{21},$$

où

$$I_{21} = \int_{J(\gamma')} d\beta \,|\, \prod_\nu \Phi_\nu(\beta-\gamma')\,| \int^{*} d\alpha$$

possède une valeur

$$<< X^{-m} x^{3mc_{27}} \int_{J(\gamma')} d\beta \,|\, \prod_\nu \Phi_\nu(\beta-\gamma')\,| \leqq X^{-m} x^{3mc_{27}} \sqrt{P}.$$

La contribution des points α et β en question est donc

$$<< x^{-\Omega_3+1+2mn\Omega_2 c_8+3mc_{27}} (X^{-2m} g_1^2 \dots g_n^2 + P) \sum_t w(t),$$

d'où suit (72).

IV. Sur $U_2(t)$ dans les cas faibles.

Maintenant Ω_1, Ω_2 et Ω_3 sont déjà choisis. Il suit de la condition D que pour tout point α de $j(\gamma)$ la différence entre $F_\nu(\alpha)$ et $z_\nu(\sum_\mu b_{\mu\nu}\gamma_\mu)\,\Phi_\nu(\alpha-\gamma)$

est $<< g_\nu x^{-\Omega_4 - 2m\Omega_2 - m\Omega_3}$. D'après (42) le nombre $F_\nu(\alpha)$ est $<<g_\nu$, de sorte que la fonction $W(\alpha, \gamma)$, définie par (64), est $<<g_1 \dots g_n x^{-\Omega_4 - 2m\Omega_2 - m\Omega_3}$. Comme le volume de $j(\gamma)$ est $2^m X^{-m} x^{m\Omega_3}$, le nombre $U_2(t)$ satisfait à (73).

V. Sur $U_2(t)$ dans les cas forts.

Démontrons dans cette partie qu'il existe un nombre positif fixe c_{28} tel qu'on ait

$$U_2(t) << X^{-m-c_{28}} g_1 \dots g_n,$$

lorsque les nombres positifs fixes ω_2 et ω_3 sont choisis assez petits.

Si les nombres positifs fixes ω_2 et ω_3 sont assez petits, la différence entre $F_\nu(\alpha)$ et $z_\nu(\sum_\mu b_{\mu\nu}\gamma_\mu)\,\Phi_\nu(\alpha-\gamma)$ est d'après la condition D, certainement $<< g_\nu X^{-c_{12}}$, pour tout point α de $j(\gamma)$, de sorte que $W(\alpha, \gamma)$, figurant dans (64), est $<<g_1 \dots g_n X^{-c_{12}}$, d'où

$$U_2(t) << X^{2n\omega_2 - m + m\omega_3} g_1 \dots g_n X^{-c_{12}} \leqq g_1 \dots g_n X^{-m-\frac{1}{2}c_{12}},$$

si ω_2 et ω_3 sont assez petits.

VI. Sur $U_3(t)$ dans les cas forts.

Supposons choisi le nombre positif fixe ω_3. Démontrons qu'il existe un nombre positif fixe c_{29} tel qu'on ait, si ω_2 est assez petit,

$$U_3(t) << X^{-c_{29}} \sum_{\lambda=1}^{m} g_\lambda \sqrt{P_\lambda}, \tag{85}$$

$$\sum_t w(t)\,|U_3(t)|^2 << X^{-c_{29}-m} \sum_{\lambda=1}^{m} g_\lambda^2 P_\lambda \sum_t w(t) \tag{86}$$

et

$$\sum_t w(t)\,|U_3(t)|^2 << X^{-c_{29}} (X^{-2m} g_1^2 \dots g_n^2 + P) \sum_t w(t) \tag{87}$$

dans les conditions respectivement des théorèmes A, B et C.

Remarquons, comme dans la troisième partie de cette démonstration, qu'à aucun point α de $J(\gamma) - j(\gamma)$ ne correspondent n entiers $y_1, \dots, y_n$ tels qu'on ait

$$|\sum_\mu b_{\mu\lambda}(\alpha_\mu - \gamma_\mu) - y_\lambda| \leqq X^{-1+\frac{1}{2}\omega_3} \quad (\lambda = 1, \dots, m),$$

quand X est assez grand. Par conséquent à tout point α de $J(\gamma) - j(\gamma)$ correspond au moins un nombre naturel $\lambda \leqq m$ vérifiant l'inégalité

$$\Phi_\lambda(\alpha - \gamma) << g_\lambda X^{-\frac{1}{2}\omega_3}. \tag{88}$$

Le nombre des systèmes $\gamma = (\gamma_1, \dots, \gamma_m)$, qui entrent en considération, est $<<X^{2m\omega_2}$ et comme $\sum_\mu b_{\mu\nu}\gamma_\mu$ est une fraction à dénominateur $<< X^{m\omega_2}$, on a en vertu de (41)

$$\eta(\gamma) = \prod_\nu z_\nu(\sum_\mu b_{\mu\nu}\gamma_\mu) << X^{mnc_8\omega_2}. \tag{89}$$

Distinguons les trois théorèmes.

VI A. Dans les conditions du théorème A les relations (88) et (89) nous apprennent

$$U_3(t) << \sum_{\lambda=1}^{m} g_\lambda X^{-\frac{1}{2}\omega_3 + mn\,c_8\,\omega_2} \sum_\gamma{}_{15} \int_{J(\gamma)} d\alpha\, |\prod_{\nu \neq \lambda} \Phi_\nu(\alpha - \gamma)|$$

$$<< X^{-\frac{1}{2}\omega_3 + mn\,c_8\,\omega_2 + 2m\omega_2} \sum_{\lambda=1}^{m} g_\lambda \sqrt{P_\lambda},$$

d'où suit (85), si ω_2 est assez petit.

VI B. Dans les conditions du théorème B nous savons en vertu de (88) et (89) que le membre de gauche de (86) est

$$<< X^{-\frac{1}{2}\omega_3 + 2\,mn\,c_8\,\omega_2} \sum_t w(t) \sum_{\lambda=1}^{m} g_\lambda{}^2 \sum_\gamma{}_{15} \sum_{\gamma'}{}_{15} I_{18},$$

où I_{18} désigne l'intégrale qui figure dans la partie III B et qui est $\leqq X^{-m} x^m P_\lambda$. De cette manière on obtient (86).

VI C. Posons $c_{30} = \frac{\omega_3}{12m}$. La contribution au membre de gauche de (87) des points α et β tels que chacun des m intervalles $(\beta_\mu - \alpha_\mu \mp X^{-1+c_{30}})$ contienne au moins une fraction à dénominateur $\leqq X^{c_{30}}$ est, en vertu de (88) et (89),

$$X^{-\frac{1}{2}\omega_3 + 2\,m\,n\,c_8\,\omega_2} g_1 \dots g_n \sum_t w(t) \sum_\gamma{}_{15} \sum_{\gamma'}{}_{15} I_{21},$$

où I_{21} désigne l'intégrale, figurant dans la partie III C; l'astérisque indique maintenant que chacun des m intervalles $(\beta_\mu - \alpha_\mu \mp X^{-1+c_{30}})$ contient au moins une fraction à dénominateur $\leqq X^{c_{30}}$. On a donc

$$\int^{*} d\alpha << X^{-m+3mc_{30}},$$

par conséquent

$$g_1 \dots g_n I_{21} << g_1 \dots g_n X^{-m+3mc_{30}} \sqrt{P} < X^{3mc_{30}} \left(X^{-2m} g_1^2 \dots g_n^2 + P\right),$$

de sorte que la contribution des points α et β considérés possède au plus le même ordre que le membre de droite de (87), si ω_2 est assez petit. Pour les autres points α et β on a d'après les conditions du théorème C

$$\sum_t w(t)\, e\left(\sum_\mu (\beta_\mu - \alpha_\mu) t_\mu\right) << X^{-c_{31}} \sum_t w(t),$$

où c_{31} est fixe (indépendant de ω_2). La contribution de ces points α et β est donc, en vertu de (89),

$$<< X^{-c_{31}+2mnc_8\omega_2} \sum_t w(t) \sum_\gamma \sum_{\gamma'} I_{19} I_{20},$$

où les intégrales I_{19} et I_{20}, qui figurent déjà dans le raisonnement III C, sont $\leqq \sqrt{P}$, de sorte que la contribution de ces points α et β est

$$<< X^{-c_{31}+2mnc_8\omega_2+4m\omega_2} P \sum_t w(t).$$

On trouve ainsi (87) pour les valeurs assez petites de ω_2.

VII. Sur $U_1(t)$ dans les cas forts.

Supposons choisis les nombres positifs fixes ω_3 et ω_2. Désignons par ω_1 un nombre positif fixe quelconque $\leqslant \omega_2$ et démontrons dans les conditions des théorèmes A, B et C respectivement

$$U_1(t) << X^{-c_{32}} \sum_{\lambda=1}^{m} g_\lambda \sqrt{R_\lambda}, \tag{90}$$

$$\sum_t w(t) |U_1(t)|^2 << X^{-c_{32}-m} \sum_{\lambda=1}^{m} g_\lambda^2 R_\lambda \sum_t w(t) \tag{91}$$

et

$$\sum_t w(t) |U_1(t)|^2 << X^{-c_{32}} (X^{-2m} g_1^2 \dots g_n^2 + R) \sum_t w(t) \tag{92}$$

où c_{32} est un nombre positif fixe convenable. Exactement comme dans la partie II de cette démonstration nous trouvons, pour X assez grand, qu'à chaque point α de j' correspond au moins un nombre naturel $\lambda \leqq m$ tel que l'intervalle $(\sum_\mu b_{\mu\nu} \alpha_\mu \mp X^{-1+\frac{1}{2}\omega_1})$ ne contienne aucune fraction à dénominateur $\leqq X^{\frac{1}{2}\omega_1}$. D'après la condition E on a donc

$$F_\lambda(\alpha) << g_\lambda X^{-c_{33}}, \tag{93}$$

où c_{33} est positif et fixe. Distinguons les trois théorèmes.

VII A. Dans les conditions du théorème A nous avons

$$U_1(t) << X^{-c_{33}} \sum_{\lambda=1}^{m} g_\lambda \int_0^1 d\alpha \prod_{\nu \neq \lambda} F_\nu(\alpha) \leqq X^{-c_{33}} \sum_{\lambda=1}^{m} g_\lambda \sqrt{R_\lambda}.$$

VII B. Si les conditions du théorème B sont remplies, nous avons

$$\sum_t w(t) |U_1(t)|^2 << X^{-c_{33}} \sum_t w(t) \sum_{\lambda=1}^{m} g_\lambda^2 I_8,$$

où l'intégrale I_8, figurant dans II B, est $<< X^{-m} x^m R_\lambda$.

VII C. Posons $c_{34} = \frac{c_{33}}{6m}$. La contribution au membre de gauche de (92) des points α et β tels qu'aucun des m intervalles $(\beta_\mu - \alpha_\mu - X^{-1+c_{34}})$ ne contienne de fraction à dénominateur $\leqslant X^{c_{34}}$, est en vertu de (93)

$$<< X^{-c_{33}} g_1 \dots g_n \sum_t w(t) \int_0^1 d\beta \prod_\nu |F_\nu(\beta)| \int^{*} d\alpha,$$

où

$$\int^{*} d\alpha << X^{-m+3mc_{34}}.$$

Cette contribution est donc

$$<< X^{-m-\frac{1}{2}c_{33}} g_1 \dots g_n \sqrt{R} \sum_t w(t)$$

$$<< X^{-\frac{1}{2}c_{33}} (X^{-2m} g_1^2 \dots g_n^2 + R) \sum_t w(t).$$

Pour les autres points α et β il découle des conditions du théorème C, qu'on a

$$\sum_t w(t)\, e\Big(\sum_\mu (\beta_\mu - \alpha_\mu) t_\mu\Big) << X^{-c_{35}} \sum_t w(t),$$

où c_{35} est positif et fixe; la contribution de ces points est donc

$$<< X^{-c_{35}} I_{13} \sum_t w(t),$$

où I_{13} désigne l'intégrale qui est $\leqslant R$. Cette dernière contribution est donc $<< X^{-c_{35}} R \sum_t w(t)$.

De cette manière les trois théorèmes fondamentaux sont complètement démontrés.

(Reçu le 18 janvier 1939.)

Zur Arithmetisierung des Beweises des Minkowskischen Diskriminanten und Kronecker-Weberschen Einbettungssatzes.

Von

S. Lubelski (Warszawa).

E. Noether hat das Problem gestellt, einen arithmetischen Beweis für den Minkowskischen Diskriminantensatz (d. h. ohne Zuhilfenahme des Begriffes der reellen Zahl) zu finden*). In dieser Arbeit zeigen wir, wie sich der genannte Beweis für algebraisch auflösbare Polynome arithmetisieren lässt (vgl. Satz 5). Dieser Beweis ist von wesentlicher Bedeutung bei der Arithmetisierung des Beweises des Kronecker-Weberschen Einbettungssatzes,

die ebenfalls hier durchgeführt wird (vgl. Satz 9).

Als Anwendung hiervon geben wir einen arithmetischen Beweis des folgenden, auf algebraisch auflösbare Polynome beschränkten, Radosschen Satzes:

Ist $f(x)$ ein irreduzibles ganzzahliges algebraisch auflösbares Polynom vom Grade $n \geqq 2$, so gibt es unendlich viele Primzahlen p, für die $f(x)$ nicht in Linearfaktoren mod p *zerlegbar ist* (vgl. Satz 10).

§ 1. Arithmetischer Beweis des Minkowskischen Diskriminantensatzes für algebraisch auflösbare Polynome.

Wir benutzen oft die folgenden wohlbenkannten Sätze:

Hilfssatz 1. *Damit das Quadrat eines Ideals des algebraischen Körpers*

*) Auf diese Noethersche Fragestellung hat mich in liebenswürdiger Weise Herr N. Tschebotarëw aufmerksam gemacht.

[1]) G. Rados: Über Kongruenzbedingungen der rationalen Lösbarkeit von algebraischen Gleichungen. Math. Annalen 87 (1922), S. 78—81.