Sur l'hypothèse de Goldbach pour presque tous les nombres pairs.

J. G. van der Corput (Groningen).

Goldbach énonça en 1742, dans sa correspondance avec Euler, l'hypothèse que tout nombre pair >4 est la somme de deux nombres premiers. Cette hypothèse n'a pas encore démontrée ni réfutée. En mai de cette année, M. I. M. Vinogradow [1]) a démontré d'une manière ingénieuse et pourtant élémentaire que tout nombre impair suffisamment grand est la somme de trois nombres premiers. Dans cet article je déduirai la proposition que presque tout nombre naturel pair est la somme de deux nombres premiers impairs, c'est à dire, ε désignant un nombre positif quelconque, tout nombre suffisamment grand N a la propriété qu'il y a moins de εN nombres naturels pairs $\leqq N$ qui ne peuvent pas être écrits comme la somme de deux nombres premiers. Il est vrai que M. M. Hardy et Littlewood sont arrivés à ce même résultat, mais seulement en admettant que l'hypothèse de Riemann soit valable [2]); comme on sait, cette hypothèse, de laquelle ils partent, n'a pas encore démontrée.

[1]) I. M. Vinogradow, Representation of an odd number as a sum of three primes, Comptes Rendus de l'Académie des Sciences de l'URRS, 1937, Vol. XV, Nr. 6 — 7, p. 169 — 172.

[2]) Voir par ex. E. Landau, Vorlesungen über Zahlentheorie, Volume 1, p. 185—186, p. 232, S. Hirzel, Leipzig, 1927.

Remarque ajoutée aux épreuves corrigées: dans le periodique „Zentralblatt" 16, p. 292, (1937), M. Heilbronn a déjà fait remarquer que la méthode de Vinogradow fournit le théorème que presque tout nombre naturel pair est la somme de deux nombres premiers.

Ce n'est pas seulement le théorème de Goldbach pour presque tous les nombres pairs que je déduirai, mais je démontrerai même qu'à tout nombre naturel m correspond une constante c_1, ne dépendant que de m, telle que pour toute valeur $\geqq 3$ de N, le nombre des nombres naturels pairs $\leqq N$ qui ne sont pas égaux à la somme de deux nombres premiers impairs, est inférieur à $c_1 N(\log N)^{-m}$.

Cette proposition entraîne celle de M. Vinogradow qui apprend que tout nombre impair suffisamment grand N est la somme de trois nombres premiers; car le nombre des nombres $N-p$, où p parcourt le système des nombres premiers impairs $<N$, a le même ordre de grandeur que $\frac{N}{\log N}$, de sorte qu'au moins un de ces nombres est la somme de deux nombres premiers impairs, si N est suffisamment grand. Pareillement on obtient le résultat que tout nombre impair $s \geqq 0$ peut être écrit, même d'une infinité de manières, sous la forme $p+p'-p''$, où p, p' et p'' designent des nombres premiers impairs; en effet, le nombre des nombres $s+p''$, ou p'' parcourt le système des nombres premiers impairs $<N$, a le même ordre des grandeur que $\frac{N}{\log N}$.

En outre je démontrerai que presque tout nombre naturel pair est la différence de deux nombres premiers impairs; à tout nombre naturel m correspond même une constante c_2, ne dépendant que de m, tel que le nombre des exceptions $\leqq N$ est inférieur à $c_2 N(\log N)^{-m}$, pour toute valeur $\geqq 3$ de N.

Je déduirai ces résultats d'un théorème général qui m'a donné encore beaucoup d'autres corollaires que je traiterai dans un autre article [3]). Dans ce théorème je considère une suite dénombrable de nombres positifs

$$(\gamma) \quad \gamma_1, \gamma_2, \ldots$$

et une suite de nombres naturels

$$(\eta) \quad \eta_1, \eta_2, \ldots .$$

Soient V, V' et T trois intervalles, dont chacun contient au moins un nombre entier. Les sommes $\sum_v$, $\sum_{v'}$ et $\sum_t$ sont étendues à tous

[3]) Voir J. G. van der Corput, Sur le théorème de Goldbach - Vinogradow, Comptes Rendus de Paris 205, (1937) p. 479 — 481; Une nouvelle généralisation du théorème de Goldbach - Vinogradow, Comptes Rendus de Paris 205, (1937), p. 591 — 592.

les nombres entiers, appartenant respectivement à V, V' et T; la somme $\sum_{v+v'=t}$ est étendue à toutes les paires de nombres entiers v et v', telles que v appartienne à V, que v' appartienne à V' et que $v+v'$ soit égale à un nombre donné t. Soient $r(v)$, $\rho(v)$, $r'(v')$, $\rho'(v')$ et $w(t)$ définis pour tout nombre entier v de V, pour tout nombre entier v' de V' et pour tout nombre entier t de T; je suppose toujours $w(t) \geqq 0$.

Je me pose le problème de déduire pour la somme

$$L(t) = \sum_{v+v'=t} r(v)\, r'(v') \tag{1}$$

une valeur approximative, valable pour beaucoup de nombres entiers t de T. A un facteur près, cette valeur approximative sera égale à

$$\Lambda(t) = \sum_{v+v'=t} \rho(v)\, \rho'(v'). \tag{2}$$

Afin d'obtenir ce résultat, j'impose trois conditions:

1. *Soit $N \geqq 3$, et soit $n = \log N$; chacun des deux intervalles V et V' ait une longueur $\leqq N$. Dans l'intervalle V la fonction $\rho(v)$ soit monotone et en valeur absolue $\leqq \Gamma$, où Γ ne dépend pas de v. Dans l'intervalle V' la fonction $\rho'(v')$ soit monotone et en valeur absolue $\leqq \Gamma'$, où Γ' ne depend pas de v'. Supposons en outre*

$$\sum_{v} |r(v)|^2 \leqq \Gamma^2 N; \tag{3}$$

$$\sum_{v'} |r'(v')|^2 \leqq \Gamma'^2 N. \tag{4}$$

2. *A tout nombre naturel q et à tout nombre naturel $k \leqq q$ correspondent deux nombres $\chi(q,k)$ et $\chi'(q,k)$, tels que les inégalités*

$$|\chi(q,k)| \leqq \gamma_1 q^l, \qquad |\chi'(q,k)| \leqq \gamma_1 q^l, \tag{5}$$

$$\left| \sum_{\substack{v \leqq u \\ v \equiv k \pmod q}} r(v) - \chi(q,k) \sum_{v \leqq u} \rho(v) \right| \leqq \gamma_m \Gamma N q^l n^{-m} \tag{6}$$

et

$$\left| \sum_{\substack{v' \leqq u' \\ v' \equiv k \pmod q}} r'(v') - \chi'(q,k) \sum_{v' \leqq u'} \rho'(v') \right| \leqq \gamma_m \Gamma' N q^l n^{-m} \tag{7}$$

soient valables pour tout nombre naturel m, pour tout nombre entier u de V et pour tout nombre entier u' de V'; dans ces inégalités l désigne un nombre $\geqq 0$, indépendant de m, q, k, u et u'.

3. *Pour tout nombre naturel m et pour tout nombre réel α, tels que l'intervalle fermé $(\alpha - N^{-1} n^{\gamma_m}, \alpha + N^{-1} n^{\gamma_m})$ ne contienne aucune fraction à dénominateur positif $\leqq n^{\gamma_m}$, on ait*

$$\left| \sum_{t} w(t)\, e^{2\pi i \alpha t} \right| \leqq \gamma_m n^{-m} \sum_{t} w(t) \tag{8}$$

et

$$\left| \sum_{v} r(v)\, e^{2\pi i \alpha v} \right| \leqq \gamma_m \Gamma N n^{-m}. \tag{9}$$

Sous ces conditions à tout nombre naturel m correspondent un nombre naturel $\sigma \geqq m$, ne dépendant que de m et de la suite (η), et aussi un nombre positif c_3, ne dépendant que de m, de l et des suites (γ) et (η), tels que

$$\sum_{t} w(t) \left| L(t) - \Lambda(t) \sum_{\frac{a}{q}} E\left(\frac{a}{q}\right) E'\left(\frac{a}{q}\right) e^{-\frac{2\pi i a t}{q}} \right|^2 \leqq c_3 \Gamma^2 \Gamma'^2 N^2 n^{-m} \sum_{t} w(t); \tag{10}$$

la somme $\sum_{\frac{a}{q}}$ est étendue à toutes les fractions $\frac{a}{q}$ irréductibles telles que $0 \leqq a < q \leqq n^\sigma$; en outre on a

$$E\left(\frac{a}{q}\right) = \sum_{k=1}^{q} e^{2\pi i \frac{ak}{q}} \chi(q,k) \qquad \text{et} \qquad E'\left(\frac{a}{q}\right) = \sum_{k=1}^{q} e^{2\pi i \frac{ak}{q}} \chi'(q,k). \tag{11}$$

Avant de donner la démonstration de ce théorème, je traiterai d'abord deux propositions auxiliaires.

Lemme 1: *Si a_h et b_h sont nuls lorsque h est suffisamment grand, on a*

$$\int_0^1 \left| \sum_{h=1}^{\infty} a_h\, e^{2\pi i h \alpha} \right| \left| \sum_{h=1}^{\infty} b_h\, e^{2\pi i h \alpha} \right| d\alpha \leqq \sqrt{\sum_{h=1}^{\infty} |a_h|^2 \cdot \sum_{h=1}^{\infty} |b_h|^2}.$$

Démonstration: On peut admettre

$$A = \sum_{h=1}^{\infty} |a_h|^2 > 0 \quad \text{et} \quad B = \sum_{h=1}^{\infty} |b_h|^2 > 0.$$

Si l'on pose

$$\xi = \frac{1}{\sqrt{A}} \sum_{h=1}^{\infty} a_h e^{2\pi i h\alpha} \quad \text{et} \quad \eta = \frac{1}{\sqrt{B}} \sum_{h=1}^{\infty} b_h e^{2\pi i h\alpha},$$

on a

$$|\xi|^2 = \xi\,\bar{\xi} = \frac{1}{A} \sum_{h=1}^{\infty} \sum_{k=1}^{\infty} a_h \bar{a}_k e^{2\pi i (h-k)\alpha}$$

donc

$$\int_0^1 |\xi|^2 d\alpha = \frac{1}{A} \sum_{h=1}^{\infty} a_h \bar{a}_h = 1$$

et

$$\int_0^1 |\eta|^2 d\alpha = 1,$$

de sorte que le membre de gauche de l'assertion est égal à

$$\sqrt{AB} \int_0^1 |\xi\,\bar{\eta}|\, d\alpha \leqq \frac{1}{2}\sqrt{AB} \int_0^1 (|\xi|^2 + |\eta|^2)\, d\alpha = \sqrt{AB}.$$

Lemme 2: *Si N est $\geqq 3$, si l'intervalle V contient au moins un nombre entier, si V a une longueur $\leqq N$, et si pour tout nombre entier u de V*

$$\left| \sum_{v \leqq u} g(v) \right| \leqq \nu,$$

où ν est indépendant de u, on a pour tout nombre réel β

$$\left| \sum_{v} g(v) e^{2\pi i \beta v} \right| \leqq 3\nu (1 + N |\sin \pi\beta|).$$

Démonstration: Si l'on pose

$$\sum_{v \leqq u} g(v) = G(u),$$

on a

$$\begin{aligned} \sum_{v} g(v) e^{2\pi i \beta v} &= \sum_{v} (G(v) - G(v-1)) e^{2\pi i \beta v} \\ &\leqq 2\nu + \left| \sum_{v} G(v) (e^{2\pi i \beta (v+1)} - e^{2\pi i \beta v}) \right| \\ &\leqq 2\nu + (N+1)\nu\, |e^{2\pi i \beta} - 1| \\ &\leqq 3\nu (1 + N |\sin \pi\beta|). \end{aligned}$$

Maintenant je donnerai la démonstration du théorème que je diviserai en trois parties.

Première partie de la démonstration.

Soit m un nombre naturel arbitraire mais fixe. Dans cette démonstration $c_4, c_5, \ldots, c_{19}$ désigneront des nombres positifs convenablement choisis, ne dépendant que de m, l et des suites (γ) et (η).

Je pose $\zeta = \eta_m$ et $\sigma = \eta_{m+3\zeta}$. Sans troubler la généralité on peut supposer $\sigma \geqq m$. En vertu de (9), appliqué avec $m + 3\zeta$ au lieu de m, on a

$$\left| \sum_{v} r(v) e^{2\pi i \alpha v} \right| \leqq c_4\, \Gamma N \eta^{-m-3\zeta} \tag{12}$$

pour tout nombre naturel m et pour tout nombre réel α tels que l'intervalle fermé $(\alpha - N^{-1}\eta^2,\ \alpha + N^{-1}\eta^2)$ ne contienne aucune fraction à dénominateur positif $\leqq \eta^2$.

Posons $\tau = m + (2l+4)\sigma$,

$$\begin{cases} R(\alpha) = \sum_{v} r(v) e^{2\pi i \alpha v}; & P(\alpha) = \sum_{v} \rho(v) e^{2\pi i \alpha v}; \\ R'(\alpha) = \sum_{v'} r'(v') e^{2\pi i \alpha v'}; & P'(\alpha) = \sum_{v'} \rho'(v') e^{2\pi i \alpha v'}. \end{cases} \tag{13}$$

Dans l'intervalle $0 \leqq \alpha \leqq 1$ je considère les fractions irréductibles $\frac{a}{q}$ à dénominateur positif $\leqq \eta^2$. Ces fractions, ordonnées selon la grandeur, forment la suite de Farey appartenant à η^2. Entre deux fractions consécutives $\frac{a}{q}$ et $\frac{a^*}{q^*}$ de cette suite j'intercale la mediante $\frac{a+a^*}{q+q^*}$. Si $\frac{a}{q}$ est une fraction, appartenant à la suite et située entre

0 et 1, je désignerai par $j\left(\frac{a}{q}\right)$ le plus petit intervalle fermé contenant $\frac{a}{q}$ et borné par deux médiantes; $j(0)$ soit l'intervalle fermé $(1-\mu, \lambda)$, où λ désigne la plus petite, μ la plus grande des médiantes intercalées.

Chacune des fractions de la suite ayant un dénominateur positif $\leqq n^{\sigma}$, chaque médiante intercalée a un dénominateur positif $\leqq 2n^{\sigma}$. Par consequent on a pour toute fraction $\frac{a}{q}$ de la suite de Farey et pour toute médiante intercalée $\frac{A}{Q}$

$$\left|\frac{a}{q}-\frac{A}{Q}\right| \geqq \frac{1}{qQ} \geqq \frac{1}{2n^{2\sigma}}. \tag{14}$$

La fonction $L(t)$, definie dans (1) satisfait aux inégalités

$$|L(t)|^2 \leqq \sum_{v} |r(v)|^2 . \sum_{v'} |r'(v')|^2 \left(\sum_{v} 1\right)^2 \leqq 4\Gamma^2\Gamma'^2 N^4 \tag{15}$$

en vertu de (3) et (4). Les fonctions $\rho(v)$ et $\rho'(v')$ étant en valeurs absolues inférieures respectivement à Γ et Γ', et l'intervalle V contenant tout au plus $N+1$ nombres entiers, la fonction $\Lambda(t)$, definie par (2), jouit de la propriété

$$|\Lambda(t)| \leqq \sum_{v} \Gamma\Gamma' \leqq \Gamma\Gamma'(N+1) < \Gamma\Gamma' N^2. \tag{16}$$

Les relations (11) et (5) impliquent pour toute fraction $\frac{a}{q}$ de la suite de Farey les inégalités

$$\left|E\left(\frac{a}{q}\right)\right| \leqq \gamma_1 q^{l+1} \leqq \gamma_1 n^{(l+1)\sigma} \quad \text{et} \quad \left|E'\left(\frac{a}{q}\right)\right| \leqq \gamma_1 n^{(l+1)\sigma}.$$

La somme $\sum_{\frac{a}{q}}$ contient tout au plus $n^{2\sigma}$ termes, donc

$$\sum_{\frac{a}{q}} \left|E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)\right| \leqq \gamma_1^2 n^{(2l+4)\sigma}. \tag{17}$$

Il suit de (15), (16) et (17) que le membre de gauche de (10) est tout au plus

$$\Gamma^2\Gamma'^2 N^4 (2+\gamma_1^2 n^{(2l+4)\sigma})^2 \sum_{t} w(t). \tag{18}$$

Par conséquent on peut admettre

$$\frac{1}{2n^{2\sigma}} > N^{-1} n^{\tau}, \tag{19}$$

car sinon, on a $N < c_5$ et alors l'expression (18) est inférieure ou égale à $c_6 \Gamma^2\Gamma'^2 N^2 n^{-m} \sum_{t} w(t)$.

Il résulte de (14) et (19) que l'intervalle $j\left(\frac{a}{q}\right)$ contient l'intervalle $\left(\frac{a}{q}-N^{-1}n^{\tau}, \frac{a}{q}+N^{-1}n^{\tau}\right)$; je désignerai par $j^*\left(\frac{a}{q}\right)$ la partie de l'intervalle $j\left(\frac{a}{q}\right)$ n'appartenant pas à l'intervalle fermé $\left(\frac{a}{q}-N^{-1}n^{\tau}, \frac{a}{q}+N^{-1}n^{\tau}\right)$, et je poserai

$$U(t) = \sum_{\frac{a}{q}} \int_{j^*\left(\frac{a}{q}\right)} R(\alpha) R'(\alpha) e^{-2\pi i \alpha t} d\alpha.$$

Deuxième partie da la démonstration.

Dans cette partie de la démonstration je déduirai pour tout nombre entier t de T la relation

$$\left|L(t) - \Lambda(t) \sum_{\frac{a}{q}} E\left(\frac{a}{q}\right) E'\left(\frac{a}{q}\right) e^{-\frac{2\pi i a t}{q}}\right|^2 = |U(t)|^2 + \tag{20}$$

$$+ \Theta c_7 \Gamma^2\Gamma'^2 N^2 n^{-m},$$

où $|\Theta| < 1$.

Démonstration: On a

$$(21)\quad \left\{\begin{aligned} &L(t)-\Lambda(t)\sum_{\frac{a}{q}} E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)e^{-\frac{2\pi i a t}{q}} \\ &=\sum_{\frac{a}{q}}\int_{i\left(\frac{a}{q}\right)} R(\alpha)R'(\alpha)e^{-2\pi i t\alpha}\,d\alpha- \\ &\sum_{\frac{a}{q}} E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)\int_0^1 \mathrm{P}(\alpha)\mathrm{P}'(\alpha)\,e^{-2\pi i\left(\alpha+\frac{a}{q}\right)t}\,d\alpha=U(t)-U_1(t)+U_2(t). \end{aligned}\right.$$

où

$$U_1(t)=\sum_{\frac{a}{q}} E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)\int_{N^{-1}n^{\tau}}^{1-N^{-1}n^{\tau}} \mathrm{P}(\alpha)\mathrm{P}'(\alpha)\,e^{-2\pi i\left(\alpha+\frac{a}{q}\right)t}\,d\alpha$$

et

$$U_2(t)=\sum_{\frac{a}{q}}\int_{-N^{-1}n^{\tau}}^{N^{-1}n^{\tau}}\left(R\left(\frac{a}{q}+\alpha\right)R'\left(\frac{a}{q}+\alpha\right)-E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)\mathrm{P}(\alpha)\mathrm{P}'(\alpha)\right)e^{-2\pi i\left(\alpha+\frac{a}{q}\right)}d\alpha.$$

Les fonctions $\rho(v)$ et $\rho'(v')$ étant monotones et en valeurs absolues inférieures respectivement à Γ et Γ', on obtient moyennant la sommation partielle les inégalités

$$|\mathrm{P}(\alpha)|\leqq\frac{c_8\Gamma}{|\sin\pi\alpha|}\qquad\text{et}\qquad|\mathrm{P}'(\alpha)|\leqq\frac{c_9\Gamma'}{|\sin\pi\alpha|},$$

donc

$$\int_{N^{-1}n^{\tau}}^{1-N^{-1}n^{\tau}}|\mathrm{P}(\alpha)\mathrm{P}'(\alpha)|\,d\alpha\leqq c_{10}\Gamma\Gamma'\int_{N^{-1}n^{\tau}}^{1-N^{-1}n^{\tau}}\frac{d\alpha}{\sin^2\pi\alpha}$$

$$=\frac{2}{\pi}c_{10}\Gamma\Gamma'\operatorname{ctg}\pi N^{-1}n^{\tau}\leqq 2c_{10}\Gamma\Gamma' N n^{-\tau}.$$

Par conséquent il résulte de (17)

$$(22)\qquad |U_1(t)|\leqq 2c_{10}\gamma_1{}^2\Gamma\Gamma' N n^{-\tau+(2l+4)\sigma}=2c_{10}\gamma_1{}^2\Gamma\Gamma' N n^{-m}.$$

La relation (11) entraîne pour tout nombre entier u de V

$$\left|\sum_{v\leqq u}e^{2\pi i\frac{av}{q}}r(v)-E\left(\frac{a}{q}\right)\sum_{v\leqq u}\rho(v)\right|=\left|\sum_{k=1}^{q}e^{2\pi i\frac{ak}{q}}\left(\sum_{\substack{v\leqq u\\ v\equiv k\,(\mathrm{mod}\,q)}}r(v)-\chi(q,k)\sum_{v\leqq u}\rho(v)\right)\right|$$
$$\leqq c_{11}\Gamma N q^{l+1}n^{-m-2\tau-(l+3)\sigma},$$

en vertu de (6), appliqué avec $m+2\tau+(l+3)\sigma$ au lieu de m. Le lemme 2 nous apprend donc pour les fonctions $R(\alpha)$ et $\mathrm{P}(\alpha)$, definies par (13),

$$\left|R(\alpha)-E\left(\frac{a}{q}\right)\mathrm{P}\left(\alpha-\frac{a}{q}\right)\right|\leqq c_{12}\Gamma N q^{l+1}n^{-m-2\tau-(l+3)\sigma}\left(1+N\left|\alpha-\frac{a}{q}\right|\right).$$

Dans l'intervalle $(\alpha-N^{-1}n^{\tau},\ \alpha+N^{-1}n^{\tau})$ et pour toute fraction $\frac{a}{q}$ appartenant à la suite de Farey, on a donc

$$\left|R(\alpha)-E\left(\frac{a}{q}\right)\mathrm{P}\left(\alpha-\frac{a}{q}\right)\right|\leqq c_{13}\Gamma N q^{l+1}n^{-m-\tau-(l+3)\sigma}$$
$$\leqq c_{13}\Gamma N n^{-m-\tau-2\sigma}.$$

On obtient d'une manière analogue

$$\left|R'(\alpha)-E'\left(\frac{a}{q}\right)\mathrm{P}'\left(\alpha-\frac{a}{q}\right)\right|\leqq c_{14}\Gamma' N n^{-m-\tau-2\sigma}.$$

Les relations (3) et (4) entraînent

$$|R(\alpha)|^2\leqq\sum_v 1.\sum_v|r(v)|^2\leqq 2\Gamma^2N^2\qquad\text{et}\qquad|R'(\alpha)|\leqq\sqrt{2}\,\Gamma' N,$$

par conséquent

$$\left|R(\alpha)R'(\alpha)-E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)\mathrm{P}\left(\alpha-\frac{a}{q}\right)\mathrm{P}'\left(\alpha-\frac{a}{q}\right)\right|$$
$$\leqq\left|R(\alpha)\right|\left|R'(\alpha)-E'\left(\frac{a}{q}\right)\mathrm{P}'\left(\alpha-\frac{a}{q}\right)\right|+$$
$$\left|R'(\alpha)\right|\left|R(\alpha)-E\left(\frac{a}{q}\right)\mathrm{P}\left(\alpha-\frac{a}{q}\right)\right|+$$
$$\left|R(\alpha)-E\left(\frac{a}{q}\right)\mathrm{P}\left(\alpha-\frac{a}{q}\right)\right|\cdot\left|R'(\alpha)-E'\left(\frac{a}{q}\right)\mathrm{P}'\left(\alpha-\frac{a}{q}\right)\right|$$
$$<c_{15}\Gamma\Gamma' N^2 n^{-m-\tau-2\sigma}$$

donc

$$|U_2(t)| \leqq \sum_{\frac{a}{q}} 2N^{-1}n^{\tau}\cdot c_{15}\Gamma\Gamma' N^2 n^{-m-\tau-2\tau} \leqq 2c_{15}\Gamma\Gamma' N n^{-m}. \tag{23}$$

Il résulte de (21), (22) et (23)

$$L(t) - \Lambda(t)\sum_{\frac{a}{q}} E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)e^{-\frac{2\pi i a t}{q}} = U(t) + \Theta_1 c_{16}\Gamma\Gamma' N n^{-m}, \tag{24}$$

où $|\Theta_1|<1$. Le lemme 1 nous apprend

$$|U(t)| \leqq \int_0^1 |R(\alpha)R'(\alpha)|\,d\alpha \leqq \sqrt{\sum_{v}|r(v)|^2\cdot\sum_{v'}|r'(v')|^2} \tag{25}$$

$$\leqq \Gamma\Gamma' N$$

en vertu de (3) et (4). Si nous remplaçons dans (24) t par $-t$ et si nous multiplions les deux relations, ainsi obtenues, nous obtenons

$$\left|L(t) - \Lambda(t)\sum_{\frac{a}{q}} E\left(\frac{a}{q}\right)E'\left(\frac{a}{q}\right)e^{-\frac{2\pi i a t}{q}}\right|^2$$

$$= (U(t) + \Theta_1 c_{16}\Gamma\Gamma' N n^{-m})\,(\overline{U}(t) + \overline{\Theta}_1 c_{16}\Gamma\Gamma' N n^{-m})$$

$$= U(t)\overline{U}(t) + \Theta\, c_{17}\Gamma^2\Gamma'^2 N^2 n^{-m}.$$

d'où suit l'assertion de la deuxième partie de la démonstration.

Troisième partie de la démonstration.

L'assertion de la deuxième partie de la démonstration nous apprend, qu'il suffit de deduire l'inégalité

$$\sum_t w(t)\,|U(t)|^2 \leqq c_{18}\Gamma^2\Gamma'^2 N^2 n^{-m}\sum_t w(t). \tag{26}$$

Le membre de gauche est égal à

$$\sum_t w(t)\,U(t)\,\overline{U}(t) = \tag{27}$$

$$\sum_{\frac{a}{q}}\sum_{\frac{a'}{q'}}\int_{j^*\left(\frac{a}{q}\right)}\int_{j^*\left(\frac{a'}{q'}\right)} R(\alpha)R'(\alpha)\,\overline{R}(\beta)\overline{R}'(\beta)\sum_t w(t)\,e^{2\pi i(\beta-\alpha)t}\,d\alpha\,d\beta,$$

la somme $\sum_{\frac{a'}{q'}}$ étant étendue à toutes les fractions irreductibles $\frac{a'}{q'}$ elles que $0 \leqq a' < q' \leqq n^{\tau}$.

Je considère d'abord les paires des nombres α, β telles que l'intervalle fermé $(\beta-\alpha-N^{-1}n^{\tau},\ \beta-\alpha+N^{-1}n^{\tau})$ ne contient aucune fraction à dénominateur positif $\leqq n^{\tau}$. Le nombre τ étant égal à τ_{1m}, la relation (8) appliquée avec $\beta-\alpha$ au lieu de α, apprend que la contribution de ces paires α, β au membre de droite de (27) est en valeur absolue tout au plus égale à

$$c_{19}n^{-m}\left(\sum_t w(t)\right)\left(\int_0^1 |R(\alpha)R'(\alpha)|\,d\alpha\right)^2 \leqq c_{19}n^{-m}\Gamma^2\Gamma'^2 N^2\sum_t w(t)$$

en vertu de (25).

Finalement je considère les paires des nombres α, β telles que l'intervalle $(\beta-\alpha-N^{-1}n^{\tau},\ \beta-\alpha+N^{-1}n^{\tau})$ contient au moins une fraction à dénominateur positif $\leqq n^{\tau}$. La contribution de ces paires au membre de droite de (27) est en valeur absolue tout au plus égale à

$$\left(\sum_t w(t)\right)\int_0^1 |R(\alpha)R'(\alpha)|\,d\alpha\,\int^* |R(\beta)R'(\beta)|\,d\beta;$$

le nombre α étant donné, la somme $\int^*$ est étendue aux nombres β, situés à l'intérieur d'un intervalle $j^*\left(\frac{a'}{q'}\right)$ et jouissant de la propriété que l'intervalle fermé $(\beta-\alpha-N^{-1}n^{\tau},\ \beta-\alpha+N^{-1}n^{\tau})$ contient au moins une fraction à dénominateur positif $\leqq n^{\tau}$.

Si l'intervalle fermé $(\beta-N^{-1}n^{\tau},\ \beta+N^{-1}n^{\tau})$ contiendrait une fraction $\frac{A}{Q}$ à dénominateur positif $\leqq n^{\tau}$, le nombre β serait situé sur le segment $\left(\frac{A}{Q}-N^{-1}n^{\tau},\ \frac{A}{Q}+N^{-1}n^{\tau}\right)$, et d'après la conclusion à la fin de la première partie de cette démonstration, ce segment appartient à $j\left(\frac{A}{Q}\right)$; alors β serait situé à l'intérieur de $j\left(\frac{A}{Q}\right)$; mais β appartient

à $j^*\left(\frac{a'}{q'}\right)$, donc à $j\left(\frac{a'}{q'}\right)$, d'où il suivrait $\frac{A}{Q}=\frac{a'}{q'}$, ce qui est impossible, parce que β n'appartient pas à l'intervalle fermé $\left(\frac{a'}{q'}-N^{-1}n^{\zeta}, \frac{a'}{q'}+N^{-1}n^{\zeta}\right)$. Par conséquent l'intervalle $(\beta-N^{-1}n^{\zeta}, \beta+N^{-1}n^{\zeta})$, et à plus forte raison, l'intervalle $(\beta-N^{-1}n^{\zeta}, \beta+N^{-1}n^{\zeta})$ ne contient aucune fraction à dénominateur positif $\leqq n^{\zeta}$. La relation (12), appliquée avec β au lieu de α, nous apprend donc

$$|R(\beta)|\leqq c_4\,\Gamma\,N n^{-m-3\zeta}.$$

La formule (4) fournit

$$|R'(\beta)|\leqq\sqrt{2}\,\Gamma' N.$$

Par conséquent la contribution au membre de droite de (27) des paires α, β dont il est question maintenant, est en valeur absolue tout au plus égale à

$$\sqrt{2}\,c_4\Gamma\Gamma' N^2 n^{-m-3\zeta}\left(\sum_t w(t)\right)\int_0^1 |R(\alpha)R'(\alpha)|\,d\alpha\int^* d\beta.$$

Le nombre α étant donné, seules les valeurs de β entrent en considération, pour lesquelles l'intervalle fermé $(\beta-\alpha-N^{-1}n^{\zeta}, \beta-\alpha+N^{-1}n^{\zeta})$ contient au moins une fraction irréductible $\frac{a'}{q'}$ telle que $0\leqq a'<q'\leqq n^{\zeta}$. Le nombre de ces fractions est $\leqq n^{2\zeta}$, de sorte que l'on a pour tout α

$$\int^* d\beta\leqq n^{2\zeta}\cdot 2N^{-1}n^{\zeta}=2N^{-1}n^{3\zeta},$$

et la contribution des paires nommées α, β au membre de droite de (27) est en valeur absolue tout au plus

$$2\sqrt{2}\,c_4\Gamma\Gamma' N n^{-m}\left(\sum_t w(t)\right)\int_0^1 |R(\alpha)R'(\alpha)|\,d\alpha$$

$$\leqq 2\sqrt{2}\,c_4\Gamma^2\Gamma'^2 N^2 n^{-m}\sum_t w(t)$$

en vertu de (25).

Ainsi le théorème est complètement démontré.

Afin de pouvoir appliquer ce théorème j'ai besoin de quelques remarques préliminaires.

Dans une suite arithmétique

$$k,\quad k+q,\quad k+2q,\ \ldots\ ,$$

dont le premier terme k (que nous supposons positif et inférieur ou égal à q) est premier avec la raison q, figurent, comme l'avait déjà démontré Dirichlet, une infinité de nombres premiers. Pour tout nombre entier $\geqq 2$, je désignerai par

$$\frac{1}{\varphi(q)}\sum_{y=2}^{x}\frac{1}{\log y}+F_{q,k}(x),$$

où $\varphi(q)$ désigne la fonction d'Euler, le nombre de nombres premiers $\leqq x$, compris dans la progression en question. Le théorème fondamental de la théorie des nombres premiers dit qu'à tout nombre positif m correspond un nombre c_{20}, dépendant seulement de m et q, tel qu'on ait, pour tout nombre entier $x\geqq 2$,

$$|F_{q,k}(x)|\leqq c_{20}\,x(\log x)^{-m}; \tag{28}$$

ceci vaut pour tout nombre naturel q et pour nombre naturel $k\leqq q$, qui est premier avec q. Le théorème de Siegel-Walfisz [4]), dont la démonstration est encore très compliquée, nous apprend que le nombre c_{20}, qui figure dans (28), peut même être choisi indépendant de q, c'est-à dire dépendant uniquement de m.

---

[4]) Le théorème de Siegel-Walfisz s'énonce comme suit: Si q et $k\leqq q$ sont des nombres naturels, premiers entre eux, on a, quelque soit le nombre positif ε,

$$|F_{q,k}(x)|<c_{21}\,x\,e^{-c_{21}\sqrt{\log x}}+c_{21}\,\frac{x^{1-c_{22}q^{\varepsilon}}}{\varphi(q)\log x};$$

c_{21} est une constante absolue, et c_{22} un nombre dépendant uniquement de ε. Pour déduire de ce théorème que la constante c_{20} de (28) peut être choisie indépendante de q, je considère deux cas:

1. Soit $q\leqq(\log x)^{2m}$. Choisissons $\varepsilon=\frac{1}{2m}$. Le nombre c_{22} dépend uniquement de m, et on a

$$x^{c_{22}q^{-\varepsilon}}=e^{c_{22}q^{-\varepsilon}\log x}\geqq e^{c_{22}\sqrt{\log x}}.$$

L'inégalité de Siegel-Walfisz se transforme donc, en vertu de ce qu'on a

$$\varphi(q)\log x\geqq\log 2,$$

Je ferai usage, non seulement de ce théorème de Siegel-Walfisz, mais aussi du théorème suivant, que M. Vinogradow démontre dans l'article cité en note 1.

Lemme 3: *Soient N entier $\geqq 2$, $m>1$, $\tau=N(\log N)^{-3m-6}$ et*

$$\left|\beta-\frac{a}{q}\right| \leqq \frac{1}{q\tau},$$

où $\frac{a}{q}$ est une fraction irréductible, telle qu'on ait

$$(\log N)^{3m+6} \leqq q \leqq \tau.$$

On a alors

$$\left|\sum_{p\leqq N} e^{2\pi i\beta p}\right| \leqq c_{24} N(\log N)^{-m}, \tag{29}$$

où la somme est étendue à tous les nombres premiers $p\leqq N$, tandis que c_{24} est un nombre dépendant uniquement de m.

---

en l'inégalité

$$|F_{q,h}(x)| < c_{21} x e^{-c_{22}\sqrt{\log x}} + \frac{c_{21}}{\log 2} x e^{-c_{22}\sqrt{\log x}}$$

$$< c_{23} x (\log x)^{-m},$$

où c_{23} désigne un nombre, qui dépend uniquement de m.

2. Soit $q>(\log x)^{2m}$. Le nombre de nombres premiers $\leqq x$, qui figurent dans la série arithmétique considérée, est tout au plus

$$\frac{x}{q} < \frac{x}{(\log x)^{2m}} \leqq \frac{x}{(\log 2)^m (\log x)^m}.$$

Considérons alors la formule connue

$$\varphi(q) = q \prod_{p/q}\left(1-\frac{1}{p}\right),$$

où le produit est étendu à tous les facteurs premiers de q. Pour $p\geqq 3$, on a $1-\frac{1}{p}>\frac{1}{\sqrt{p}}$ et pour $p=2$, on a $1-\frac{1}{p}>\frac{1}{2\sqrt{p}}$. On a donc

$$\varphi(q) \geqq \frac{1}{2} q \prod_{p/q}\frac{1}{\sqrt{p}} \geqq \frac{1}{2}\sqrt{q} > \frac{1}{2}(\log x)^m.$$

Il en résulte qu'on a

$$\frac{1}{\varphi(q)}\sum_{y=2}^{x}\frac{1}{\log y} < \frac{2x}{(\log x)^m \log 2}.$$

Il ressort de ceci que le nombre c_{20} de (28) peut être choisi dépendant uniquement de m.

Je mettrai ce théorème de Vinogradow sous une autre forme, moyennant le théorème suivant de Dirichlet.

Lemme 4: *Si γ est un nombre réel quelconque et si τ est un nombre $\geqq 1$, il existe au moins une fraction $\frac{a}{q}$ telle qu'on ait*

$$0<q\leqq\tau \qquad \text{et} \qquad \left|\gamma-\frac{a}{q}\right| < \frac{1}{q\tau}. \tag{30}$$

Démonstration: (empruntée à M. L. Törnquist). Considérons, pour tout point $\gamma\lambda$, où λ est un nombre entier $\geqq 0$ et $\leqq\tau$, l'ensemble j_λ des points β, qui appartiennent à l'intervalle $0<\beta<1$, et auxquels correspond un nombre entier g tel qu'on ait $|\gamma\lambda-g-\beta|<\frac{1}{2\tau}$; l'ensemble j_λ est composé de un ou deux intervalles ouverts, de longueur totale $\frac{1}{\tau}$. Ces ensembles j_λ sont tous compris dans l'intervalle $0<\beta<1$ et leur nombre est supérieur à τ. Leur longueur totale est donc supérieure à 1, et il existe au moins un β qui appartient à deux ensembles distincts j_λ et j_μ; nous pouvons supposer d'ailleurs $0\leqq\mu<\lambda\leqq\tau$. Il existe des nombres g et h tels qu'on ait

$$|\gamma\lambda-g-\beta|<\frac{1}{2\tau} \qquad \text{et} \qquad |\gamma\mu-h-\beta|<\frac{1}{2\tau},$$

donc

$$|\gamma(\lambda-\mu)-(g-h)|<\frac{1}{\tau}.$$

On obtient maintenant la deuxième relation (30) en posant $q=\lambda-\mu$ et $a=g-h$; on a de plus $0<q\leqq\lambda\leqq\tau$ et le lemme est donc démontré.

Je mettrai maintenant le lemme 3 sous la forme suivante.

Lemme 5: *Si N est un nombre entier $\geqq 3$, si m est un nombre naturel, si $\tau=N(\log N)^{-3m-6}$ et si le nombre réel α est choisi de telle sorte que l'intervalle fermé $\left(\alpha-\frac{1}{\tau}, \alpha+\frac{1}{\tau}\right)$ ne contienne aucune fraction à dénominateur positif $\leqq(\log N)^{3m+6}$, on a*

$$\left|\sum_{p\leqq N} e^{2\pi i\alpha p}\right| < c_{25} N(\log N)^{-m}.$$

où c_{25} est un nombre positif convenablement choisi, dépendant uniquement de m.

Démonstration: L'inégalité est évidente, si $m=1$. Posons donc $m>1$. Puisque l'intervalle $\left(\alpha-\frac{1}{\tau},\ \alpha+\frac{1}{\tau}\right)$ ne contient aucun nombre entier, τ est $\geqq 1$. En vertu du lemme précédent, il existe une fraction $\frac{a}{q}$ satisfaisant aux inégalites (30) avec $\gamma=\alpha$. Nous pouvons supposer que cette fraction soit irréductible. Elle est certainement située dans l'intervalle $\left(\alpha-\frac{1}{\tau},\ \alpha+\frac{1}{\tau}\right)$ et possède donc, en vertu des conditions du lemme à démontrer, un dénominateur $>(\log N)^{3m+6}$. Le lemme 3 donne maintenant la proposition continue dans le lemme 5.

Lemme 6. *Si q_1 et q_2 sont deux nombres naturels donnés, premiers entre eux, à tout nombre entier a, ayant les propriétés*

$$0\leqq a<q_1q_2 \qquad \text{et} \qquad (a, q_1q_2)=1, \tag{31}$$

est associé d'une façon biunivoque un couple de nombres entiers a_1 et a_2, tels qu'on ait

$$0\leqq a_1<q_1, \quad (a_1, q_1)=1, \quad 0\leqq a_2<q_2, \quad (a_2, q_2)=1, \tag{32}$$

$$a\equiv q_1a_2+q_2a_1. \pmod{q_1q_2}. \tag{33}$$

Démonstration. q_1 et q_2 étant premiers entre eux, il en résulte que la congruence

$$a\equiv q_1x \pmod{q_2}$$

a une et une seule solution $x=a_2$ dans l'intervalle $0\leqq a_2<q_2$. La congruence

$$a\equiv q_2y \pmod{q_1}$$

a également une et une seule solution $y=a_1$ dans l'intervalle $0\leqq a_1<q_1$. Le nombre $a-q_1a_2-q_2a_1$ est divisible par q_1 et q_2, donc aussi par leur produit. Si a_1 et q_1 avaient un facteur commun, ce facteur apparaîtrait dans a. Or, a et q_1 sont premiers entre eux. Les nombres a_1 et q_1 sont donc également premiers entre eux, et il en est de même de a_2 et q_2.

S'il y avait une seconde solution b_1, b_2 de

$$a\equiv q_1b_2+q_2b_1, \qquad 0\leqq b_1<q_1 \qquad \text{et} \qquad 0\leqq b_2<q_2,$$

alors, en vertu de (33), le produit $q_1(a_2-b_2)$, donc aussi (a_2-b_2) serait divisible par q_2. Il en résulte donc qu'on a $a_2=b_2$, de même que $a_1=b_1$.

Voyons maintenant la réciproque. Soient a_1 et a_2 deux nombres satisfaisant aux relations (32), et soit a le nombre défini par (33) et $0\leqq a<q_1q_2$. Les nombres a et q_1q_2 sont premiers entre eux. Un facteur commun de a et q_1 serait en effet un facteur commun de a_1 et q_1, de même qu'un facteur commun de a et q_2 serait un facteur commun de a_2 et q_2. Or, a_1, q_1 et a_2, q_2 sont deux couples de nombres premiers entre eux. A deux nombres donnés a_1 et a_2, tels qu'on ait (32) correspond donc un et un seul nombre a, tel qu'on ait (31) et (33). Le lemme est donc démontré.

L'expression $\mu(q)$ désignera partout dans cet article la fonction de Möbius, c'est-à-dire que $\mu(q)$ vaut 0, lorsque q est divisible par un carré supérieur à 1, et que sinon $\mu(q)$ vaut 1 ou -1 selon que le nombre de facteurs premiers de q est pair ou impair. On a donc, par exemple, $\mu(1)=1$, $\mu(2)=\mu(3)=-1$, $\mu(4)=0$, $\mu(5)=-1$, $\mu(6)=1$, $\mu(7)=-1$, $\mu(8)=0$.

Lemme 7. *Si q_1 et q_2 sont des nombres premiers entre eux, on a*

$$\mu(q_1q_2)=\mu(q_1)\mu(q_2) \qquad \text{et} \qquad \varphi(q_1q_2)=\varphi(q_1)\varphi(q_2).$$

Démonstration. Si l'un au moins des nombres q_1 et q_2 est divisible par un carré supérieur à 1, c'est aussi le cas pour q_1q_2, et les deux membres de la première relation qu'il faut démontrer sont alors égaux à 0. Sinon, chacun de ces deux membres est égal à $(-1)^{l_1+l_2}$, où l_1 représente le nombre de facteurs premiers de q_1 et l_2 le nombre de facteurs premiers de q_2. Finalement on a

$$\varphi(q_1q_2)=q_1q_2\prod_{p/q_1q_2}\left(1-\frac{1}{p}\right)=\left\{q_1\prod_{p/q_1}\left(1-\frac{1}{p}\right)\right\}\left\{q_2\prod_{p/q_2}\left(1-\frac{1}{p}\right)\right\}=\varphi(q_1)\varphi(q_2).$$

Nous aurons partout, dans cet article,

$$e(\beta)=e^{2\pi i\beta} \qquad \text{et} \qquad Z(q, m)=\sum_{\substack{a=0\\(a,q)=1}}^{q-1}e\left(\frac{am}{q}\right),$$

où q désigne un nombre naturel et m un nombre entier; (a, q) désigne e plus grand commun diviseur de a et q.

Lemme 8: 1. *On a, si q_1 et q_2 sont des nombres premiers entre eux,*

$$Z(q_1q_2, m)=Z(q_1, m).Z_1(q_2, m).$$

2. *On a, si q et m sont des nombres premiers entre eux,*

$$Z(q, m) = \mu(q).$$

3. *Si q n'est pas divisible par un carré supérieur à 1, on a*

$$Z(q, m) = \mu(q)\,\mu(d)\,\varphi(d),$$

où d représente le plus grand commun diviseur de q et m ($d = q$ si $m = 0$).

Démonstration: 1. On a, en vertu du lemme 6, si q_1 et q_2 sont premiers entre eux,

$$Z(q_1 q_2, m) = \sum_{\substack{a=0 \\ (a, q_1 q_2)=1}}^{q_1 q_2 - 1} e\left(\frac{a m}{q_1 q_2}\right)$$

$$= \sum_{\substack{a_1=0 \\ (a_1, q_1)=1}}^{q_1-1} \sum_{\substack{a_2=0 \\ (a_2, q_2)=1}}^{q_2-1} e\left(\frac{a_1 m}{q_1} + \frac{a_2 m}{q_2}\right)$$

$$= Z(q_1, m)\, Z(q_2, m).$$

Il suit de là qu'on a, si

$$q = p_1^{\beta_1} \ldots p_s^{\beta_s}$$

est la représentation canonique de q en facteurs premiers,

$$Z(q, m) = Z(p_1^{\beta_1}, m)\, Z(p_2^{\beta_2}, m) \ldots Z(p_s^{\beta_s}, m). \tag{34}$$

2. Soient q et m des nombres premiers entre eux. Si p est un facteur premier de q, alors p n'est pas un diviseur de m, et on a donc, pour tout nombre entier $\beta \geqq 2$,

$$Z(p^\beta, m) = \sum_{a=0}^{p^\beta - 1} e\left(\frac{a m}{p^\beta}\right) - \sum_{b=0}^{p^{\beta-1}-1} e\left(\frac{b m}{p^{\beta-1}}\right) = 0 - 0 = 0.$$

Lorsque q est divisible par un carré supérieur à 1, on a donc, en vertu de (34),

$$Z(q, m) = 0 = \mu(q).$$

Supposons alors que q ne soit pas divisible par un carré supérieur à 1. On a, pour tout facteur premier p de q,

$$Z(p, m) = \sum_{a=1}^{p-1} e\left(\frac{a m}{p}\right) = -1,$$

parce que p n'est pas un diviseur de m. Le nombre $Z(q, m)$ a donc, en vertu de (34), la valeur $+1$ ou -1, selon que q possède un nombre pair ou impair de facteurs premiers. On a donc toujours, lorsque q et m désignent des nombres premiers entre eux,

$$Z(q, m) = \mu(q).$$

3. Soit q un nombre non divisible par un carré supérieur à 1, et soit p un nombre premier.

$Z(p, m) = \sum_{a=1}^{p-1} e\left(\frac{a m}{p}\right)$ est égal à $p-1$ ou -1 selon que p est ou n'est pas un diviseur de m. $Z(q, m)$ est donc égal, en vertu de (34), à $(-1)^l \Pi (p-1)$, où l représente le nombre de facteurs premiers de q, qui ne figurent pas dans m, et où le produit $\Pi(p-1)$ est étendu à tous les facteurs premiers de q, qui figurent dans m. Le nombre l est le nombre de facteurs premiers de q, qui ne figurent pas dans le plus grand commun diviseur d de q et m; ce nombre l est donc égal à $h-k$, où h représente le nombre de facteurs premiers de q, et k le nombre de facteurs premiers de d. On a donc

$$(-1)^l = (-1)^{h-k} = (-1)^{h+k} = \mu(q)\,\mu(d).$$

Le produit $\Pi(p-1)$ étant étendu à tous les facteurs premiers de d, est égal à $\varphi(d)$, parce que d n'est pas divisible par un carré >1.

Il est ainsi démontré qu'on a

$$Z(q, m) = \mu(q)\,\mu(d)\,\varphi(d).$$

Lemme 9: *On a*

$$\sum_{\substack{q>1 \\ q \text{ impair}}} \frac{\mu^2(q)}{\varphi^2(q)} < \frac{3}{5};$$

le membre de gauche est la série $\sum \frac{1}{\varphi^2(q)}$, étendue à tous les nombres impairs $q>1$, qui ne sont multiples d'aucun carré >1.

Démonstration: En vertu de $\frac{95}{168} < \frac{3}{5}$ il suffit de démontrer pour tout nombrer naturel N

$$\sum_{\substack{1<q\leqq N \\ q \text{ impair}}} \frac{\mu^2(q)}{\varphi^2(q)} < \frac{95}{168}.$$

Le produit

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

étendu à tous les nombres premiers >2 et $\leqq N$, se transforme par développement en

$$1+\sum_1 \frac{1}{(p_1-1)^2(p_2-1)^2\ldots(p_s-1)^2},$$

où la somme $\sum_1$ est étendue à tous les nombres impairs $q>1$ qui ne sont divisibles par aucun carré >1 et dont chaque facteur premier est $\leqq N$; dans cette somme $p_1, p_2, \ldots p_s$ désignent les facteurs premiers de q. On a $\sum_1 \geqq \sum_2$, la somme $\sum_2$ étant étendue à tous les nombres impairs $q>1$ et $\leqq N$ qui ne sont divisibles par aucun carré >1. Pour un pareil nombre on a

$$(p_1-1)(p_2-1)\ldots(p_s-1)=\prod_{p/q}(p-1)=q\prod_{p/q}\left(1-\frac{1}{p}\right)=\varphi(q),$$

donc

$$\prod_{2<p\leqq N}\left(1+\frac{1}{(p-1)^2}\right)\geqq 1+\sum_2\frac{1}{\varphi^2(q)}=1+\sum_{\substack{1<q\leqq N\\ q\text{ impair}}}\frac{\mu^2(q)}{\varphi^2(q)}$$

d'après la définition de la fonction de Möbius. En outre on a

$$\prod_{2<p\leqq N}\left(1+\frac{1}{(p-1)^2}\right)\leqq \prod_{2<p\leqq N} e^{\frac{1}{(p-1)^2}}$$

$$=e^{\sum\limits_{2<p\leqq N}\frac{1}{(p-1)^2}}<e^{\sum\limits_{h=1}^{\infty}\frac{1}{(2h)^2}}$$

$$=e^{\frac{\pi^2}{24}}<e^{\frac{5}{12}}<1+\frac{5}{12}+\frac{1}{2}\cdot\frac{5^2}{12^2}\sum_{h=0}^{\infty}\left(\frac{5}{12}\right)^h$$

$$=1+\frac{5}{12}+\frac{5^2}{2.12.7}=1+\frac{95}{168},$$

d'où résulte l'inégalité qu'il faut démontrer.

Maintenant je démontrerai qu'à tout nombre naturel m correspond un nombre c_1, dépendant uniquement de m, tel que le nombre des

nombres pairs $\leqq N$, qui ne sont pas égaux à la somme de deux nombres premiers impairs, soit inférieur à $c_1 N n^{-m}$; ceci vaut pour tout nombre $N\geqq 3$. J'applique le théorème principal de cet article en choisissant pour V, V' et T l'intervalle $(3, N)$; je pose $r(v)=r'(v)=1$ ou 0, selon que v est un nombre premier impair ou non, et en outre je pose

$$\rho(v)=\rho'(v)=\frac{1}{\log v};\qquad \eta_{|m}=3m+6;\qquad \Gamma=\Gamma'=1,\qquad l=0;$$

$w(t)=1$ ou 0, selon que t est pair ou impair. Je démontrerai d'abord que les conditions du théorème sont valables, si l'on choisit la suite (η) convenablement.

1. La longueur des intervalles V et V' est inférieure à N; la fonction $\frac{1}{\log v}$ est monotone, positive et inférieure à 1; on a

$$\sum_{p\leqq N}1\leqq N.$$

2. D'après le théorème de Siegel-Walfisz les relations (6) et (7) sont valables, si $\chi(q,k)=\chi'(q,k)$ est égal à $\frac{1}{\varphi(q)}$ ou 0, selon que k est premier avec q ou non.

3. Le lemme 5 nous fournit (9). En outre on a

$$\left|\sum_t w(t)e^{2\pi i\alpha t}\right|\leqq\frac{1}{|\sin 2\pi\alpha|}\leqq\frac{1}{4N^{-1}n^{3m+6}}\leqq\frac{1}{4}Nn^{-m},$$

si l'intervalle fermé $(2\alpha-2N^{-1}n^{3m+6},\ 2\alpha+2N^{-1}n^{3m+6})$ ne contient aucun nombre entier.

Les conditions du théorème étant valables, on a

$$\sum_t w(t)\left|L(t)-\Lambda(t)\sum_{\frac{a}{q}}E^2\left(\frac{a}{q}\right)e^{-\frac{2\pi i\alpha t}{q}}\right|^2\leqq c_{26}N^3n^{-m}, \tag{35}$$

où c_{26} dépend uniquement de m. Dans cette formule $L(t)$ est le nombre de manières d'écrire t comme la somme de deux nombres premiers impairs, et

$$\Lambda(t)=\sum_{v=3}^{t-3}\frac{1}{(\log v)\log(t-v)}. \tag{36}$$

Les nombres a et q étant premiers entre eux, on a

$$E\left(\frac{a}{q}\right)=\frac{1}{\varphi(q)}\sum_{\substack{k=1\\(k,\,q)=1}}^{q} e^{2\pi i\frac{a\,k}{q}}=\frac{\mu(q)}{\varphi(q)}$$

d'après le lemme 8; donc $E^2\left(\frac{a}{q}\right)$ est égal à 0 ou $\frac{1}{\varphi^2(q)}$, selon que q est divisible par un carré >1 ou non. Pour les nombres q qui ne sont multiples d'aucun carré >1, on a, d'après le lemme 8,

$$\sum_{\substack{a=1\\(a,\,q)=1}}^{q} E^2\left(\frac{a}{q}\right)e^{-2\pi i\frac{at}{q}}=\frac{1}{\varphi^2(q)}\sum_{\substack{a=1\\(a,\,q)=1}}^{q} e^{-\frac{2\pi i a t}{q}}$$

$$=\frac{\mu(q)\,\mu(d)\,\varphi(d)}{\varphi^2(q)},$$

où d désigne le plus grand commun diviseur de q et t. On a donc

$$\sum_{\frac{a}{q}} E^2\left(\frac{a}{q}\right)e^{-\frac{2\pi i a t}{q}}=\sum_{q\leqq n^c}{}' \frac{\mu(q)\,\mu(d)\,\varphi(d)}{\varphi^2(q)},$$

le prime indiquant que seuls figurent les nombres naturels q qui ne sont divisibles par aucun carré >1.

Si l'on pose $q=dh$, ni le nombre d, ni le nombre h est multiple d'un carré >1; le nombre h est premier avec d et avec $\frac{t}{d}$, donc avec t. Inversément, si d est un diviseur de t, si aucun des nombres d et h n'est multiple d'un carré >1, et si h est premier avec t, le nombre $q=dh$ n'est divisible par aucun carré >1, et d est le plus grand commun diviseur de q et t. Par consequent

$$\sum_{\frac{a}{q}} E^2\left(\frac{a}{q}\right)e^{-\frac{2\pi i a t}{q}}=\sum_{d}\frac{1}{\varphi(d)}\sum_{h}\frac{\mu(h)}{\varphi^2(h)};$$

la somme $\sum_d$ est étendue à tous les diviseurs $d\leqq n^c$ de t, qui ne sont divisibles par aucun carré >1; la somme $\sum_h$ est étendue à tous les nombres naturels $h\leqq\frac{n^c}{d}$, qui ne sont multiples d'aucun carré >1 et

qui sont premiers avec t. Si t est pair, h est impair, et le lemme 9 nous apprend

$$\sum_{h}\frac{\mu(h)}{\varphi^2(h)}=1+\sum_{h>1}\frac{\mu(h)}{\varphi^2(h)}\geqq 1-\sum_{\substack{k>1\\ k\text{ impair}}}^{\infty}\frac{\mu^2(k)}{\varphi^2(k)}\geqq\frac{2}{5},$$

donc

$$\sum_{\frac{a}{q}} E^2\left(\frac{a}{q}\right)e^{-\frac{2\pi i a t}{q}}\geqq\frac{2}{5}\sum_{d}\frac{1}{\varphi(d)}\geqq\frac{2}{5}. \tag{37}$$

Pour les nombres t qui sont $\geqq N n^{-\frac{1}{3}m}$ et $\geqq 6$, il suit de (36)

$$\Lambda(t)\geqq\frac{1}{n^2}\sum_{v=3}^{t-3}1\geqq\frac{t}{6\,n^2}\geqq\frac{1}{6}N n^{-\frac{1}{3}m-2}. \tag{38}$$

Si A désigne le nombre des nombres pairs t qui sont $\geqq N n^{-\frac{1}{3}m}$, $\geqq 6$ et $\leqq N$ et pour lesquels $L(t)=0$, il résulte de (35), (37) et (38)

$$\frac{1}{225}A N^2 n^{-\frac{2}{3}m-4}\leqq c_{26}N^3 n^{-m},$$

donc

$$A\leqq 225\,c_{26}N n^{-\frac{1}{3}m+4}.$$

Le nombre des nombres naturels pairs $\leqq N$, pour lesquels $L(t)=0$, est donc tout au plus égale à

$$225\,c_{26}N n^{-\frac{1}{3}m+4}+3+\frac{1}{2}N n^{-\frac{1}{3}m}.$$

Ceci vaut pour tout nombre naturel m, de sorte que le nombre des nombres naturels pairs $\leqq N$, pour lesquels $L(t)=0$, est tout au plus égal à $c_1 N n^{-m}$, où c_1 dépend uniquement de m.

Je finirai cet article par la démonstration qu'à tout nombre naturel m correspond une constante c_2, dépendant uniquement de m, telle que pour tout $N\geqq 3$ il y a moins de $c_2 N n^{-m}$ nombres naturels pairs $\leqq N$, qui ne sont pas égaux à la différence de deux nombres premiers impairs. Je choisis pour V et T l'intervalle $(3, N)$, pour V' l'intervalle $(-N, -3)$; je pose $r(v)=r'(-v)$ égal à 1 ou 0, selon que v est un nombre premier impair ou non; en outre je pose

$$\rho(v) = \rho'(-v) = \frac{1}{\log v}; \qquad \eta_m = 3m + 6; \qquad \Gamma = \Gamma' = 1; \qquad l = 0;$$

$w_t = 1$ ou 0, selon que t est pair ou impair.

Ainsi on trouve encore la formule (35) mais maintenant $L(t)$ désigne le nombre de manières d'écrire t comme la différence des deux nombres premiers impairs $\leqq N$, et le raisonnement donné ci-dessus nous fournit le résultat cherché.

(Reçu le 17 novembre 1937.)