PUBLICATIONS MATHEMATIQUES D'ORSAY

86-01

THÉORIE ANALYTIQUE ET ÉLÉMENTAIRE DES NOMBRES

Actes du Colloque du C.I.R.M.

30 mai au 3 juin 1983

Edité par H. Daboussi, P. Liardet et G. Rauzy

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

Code matière AMS : 10 A - 10 C - 10 F -
10 G - 10 H - 10 K - 10 L

PUBLICATIONS

MATHEMATIQUES

D'ORSAY

86-01

THÉORIE ANALYTIQUE ET ÉLÉMENTAIRE DES NOMBRES

Actes du Colloque du C.I.R.M.

30 mai au 3 juin 1983

Edité par H. Daboussi, P. Liardet et G. Rauzy

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

THEORIE ANALYTIQUE ET ELEMENTAIRE DES NOMBRES

Actes du Colloque du C.I.R.M.
30 mai au 3 juin 1983

INTRODUCTION

Ce volume contient les Actes du Colloque "Théorie analytique et élémentaire des nombres" qui a rassemblé 60 participants dans le site merveilleux du C.I.R.M. à Marseille, du 30 mai au 3 juin 1983.

Nous donnons ici la rédaction de 15 des conférences de ce colloque, ainsi que les résumés des autres conférences ayant donné ou devant donner lieu à des publications par ailleurs.

Qu'il nous soit permis ici de remercier encore une fois l'ensemble des participants de ce colloque, ainsi que les organismes ayant contribué à son financement :

-La S.M.F.

-Les Universités d'Aix-Marseille 1 et 2.

Une mention particulière doit être faite pour le C.I.R.M. qui outre une part du financement, nous a offert son cadre et son accueil si sympatique.

LISTE DES PARTICIPANTS

ALLOUCHE J-P. (E.N.S. Fontenay)
BAKER R.C. (Royal Holloway College, London)
BALOG A. (Acad. Sc., Budapest)
BEJIAN R. (Aix-Marseille 1)
BERTRAND A. (Bordeaux 1)
BLANCHARD A. (Aix-Marseille 1)
BLANCHARD C. (Aix-Marseille 1)
BOREL J-P. (Limoges)
CAR M. (Aix-Marseille 3)
CHAIX H. (Aix-marseille 1)
COQUET J. (Valenciennes)
DABOUSSI H. (Paris-Sud)
DE CLERCK L. (Katholieke Univ., Louvain)
DELANGE H. (Paris-Sud)
DESHOUILLERS J-M. (Bordeaux 1)
DRESS F. (Bordeaux 1)
DUBOIS E. (Caen)
DUMONT J-M. (Aix-Marseille 2)
DUPAIN Y. (Bordeaux 1)
ERDÖS P. (Acad. Sc., Budapest)
FARDOUX G. (Aix-Marseille 1)
FAURE H. (Aix-Marseille 1)
FOUVRY E. (Bordeaux 1)
FURSTENBERG H. (Hebrew Univ., Jérusalem)
HELLEKALEK P. (Uni. Salzbourg)
HEVERTSE J. (Uni. Leiden)
HILDEBRAND A. (Paris-Sud)
LAGRANGE J. (Reims)
LANGEVIN M. (E.N.S. Saint-Cloud)
LIARDET P. (Aix-Marseille 1)
LABORDE (Paris 6)
MASSIAS J-P. (Limoges)
MELA J-F. (Paris-Nord)
MENDES-FRANCE M. (Bordeaux)
MEYER J. (Reims)
NARKIEWICZ W. (Wrocław)
NICOLAS J-L. (Limoges)
NIEDERREITER H. (Acad. Sc., Vienne)
PARREAU F. (Paris-Nord)
PAYSANT-LEROUX R. (Caen)
POUSPOURIKAS E. (Aix-Marseille 2)
QUEFFELEC M. (Paris-Nord)
RAUZY G. (Aix-Marseille 2)
RHIN G. (Metz)
ROBIN G. (Limoges)
SCHWARZ W. (Francfort)
SOUBLIN J-P. (Aix-Marseille 1)
TENENBAUM G. (Nancy 1)
THOMAS A. (Aix-Marseille 1)
TOFFIN Ph. (Caen)
VALLEE B. (Caen)
VAN DEN BOSCH P. (Valenciennes)
VOLKMANN B. (Stuttgart)
MAUDUIT C. (Aix-Marseille 2)

LISTE DES CONFERENCES

ALLOUCHE J.-P.	Propriétés arithmétiques d'un automate cellulaire.
BAKER R.C.	On the Values of Entire Functions at the Positive Integers.
BALOG A.	A Remark on the Distribution of αp Modulo One.
COQUET J.	Pertubations des entiers et répartition des suites.
DELANGE H.	Une remarque sur la fonction de Dickman.
DUBOIS E.	Application des meilleures approximations au calcul d'unités.
DUMONT J.-M.	Discrépance des progressions arithmétiques dans la suite de Morse.
ERDÖS P.	Some Problems on Number Theory.
FAURE H.	Lemme de Bohl pour les suites de Van der Corput.
FOUVRY E.	Sur le théorème de Brun-Titchmarsh.
FURSTENBERG H.	Dynamical Systems and Number Theory.
HELLGOUARCH Y.	Equation de Pell et points d'ordre fini.
HELLEKALEK P.	Ergodicity of a Class of Cylinder Flows.
HEVERTSE J.	On the Number of Solutions of the Thue-Mahler Equation.
HILDEBRAND A.	Sur le "petit crible" de Erdös et Ruzsa.
IWANIEC H.	Prime Geodesics Theorem.
LAGRANGE J.	Sur une quadruple équation.
LANGEVIN M.	Distance d'un entier algébrique au disque unité et problème de Lehrmer.
MAUDUIT C.	Suites reconnaissables par automates finis et équirépartition modulo un.
MENDES-FRANCE M.	Automata and p-adic Numbers.
NARKIEWICZ W.	Propriétés bizarres de $\sigma_k(n)$.
NICOLAS J.-L.	Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers.
NIEDERREITER H.	Exponential Sums over Finite Fields.
QUEFFELEC M.	Etude spectrale des substitutions.
ROBIN G.	Irrégularité dans la distribution des nombres premiers dans les progressions arithmétiques.
SCHWARZ W.	A Correction to "Remarks on Elliott's Theorem on Mean-Values of Multiplicative Functions" and some Remarks on Almost-Even Number-Theoretical Functions.
TENENBAUM G.	Théorèmes taubériens avec restes.
VOLKMANN B.	A propos du théorème de Cassels-Schmidt.

*
* *

TABLE DES MATIERES

ON THE VALUES OF ENTIRE FUNCTIONS AT THE POSITIVE INTEGERS

R.C. BAKER

Let $f(x)$ be an entire function that is real on the real axis and not a polynomial. It is likely that a growth condition

(1) $\qquad \log|f(z)| < (\log|z|)^{\alpha}$

for large z, with $\alpha < 2$, is sufficient to ensure the uniform distribution modulo one of the sequence

(2) $\qquad f(n) \quad (n=1,2,\ldots)$.

Rauzy [4] was able to show that $\alpha < 5/4$ certainly suffices for this uniform distribution. G. Rhin [5] wrote a very long paper inspired by Rauzy's work showing that the sequence

(3) $\qquad f(p) \quad (p \text{ prime})$

is uniformly distributed modulo one for $\alpha < 7/6$.

Recently I was able to show [1] that the condition $\alpha < 4/3$ will suffice for both the Rauzy and Rhin theorems. The proof is modelled on that of Rhin, but I found a number of simplifications. In particular, in looking at $\{f(j)\}$ $(j \leqslant N)$ I was able to confine the discussion to approximations to f of the form

$$(4) \qquad g(x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} x^k$$

in the interval $1 \leqslant x \leqslant N$. Rauzy [4] used 'local' approximations

$$(5) \qquad g_j(x) = \sum_{k=0}^{n} \frac{f^{(k)}(x_j)}{k!} (x - x_j)^j \qquad (x_j \leqslant x < x_{j+1}) \ ,$$

while Rhin used both (1) and (2) according to the value of N. Another gain over [5] was the elimination of the use of the sieve in the mode of Vinogradov (Theorem 2a of [6], Chapter IX). Instead, the estimation of sums

$$S(x,G,q) = \sum_{\substack{x=1 \\ (x,q)=1}}^{q} \chi(x)\, e_q(G(x))$$

with χ a <u>real</u> Dirichlet character, plays a role. Here

$$G(x) = A_h x^h + \ldots + A_1 x$$

with integer A_i satisfying $(A_h,\ldots,A_1,q) = 1$. I showed that

(6) $$| S(\chi,G,q) | < \exp(16h)\, q^{1-1/(4h)} ,$$

but this could probably be improved to a similar contant times $q^{1-1/(2h)}$ by following the details of Chen [2] more closely. For the application to the present problem, (6) is equally good. Roughly speaking, the study of the exponential sum

(7) $$\sum_{p \leqslant N} e(f(p))$$

is reduced to that of certain sums

$$T = \sum_{u < n \leqslant v} \Lambda(n)\, e_q(G(n))$$

where $\frac{G(x)}{q}$ is an approximation to a Taylor polynomial $g(x)$ as in (4). It is not difficult to see that

$$\sum_{u < n \leqslant v} \Lambda(n) e_q(G(n)) = O(\log N \log q) + \sum_{\substack{\ell=1 \\ (\ell,q)=1}}^{q} e_q(G(\ell))(\psi(v,q,\ell) - \psi(u,q,\ell))$$

in the usual notation of primes in arithmetic progressions. If we insert an 'explicit formula' for ψ (as in (2.5) of Prachar [3], Chapter IX) we obtain

(8) $$T = \frac{v-u}{\phi(q)} S(\chi_o,G,q) - \frac{S(\chi_1,G,q)}{\phi(q)} \frac{(v^{\beta_1} - u^{\beta_1})}{\beta_1} + R .$$

Here β_1 is the (perhaps nonexistent) real zero near 1 of the 'exceptional' character $\chi_1 \pmod q$. The terms R derive from the other zeros of the L functions and are manageable, at least if q is not too large. In this case the insertion of (6) into (8) will give a suitable estimate for T. In the case where approximation $G(x)/q$ to $g(x)$ (suitably chosen via Dirichlet's theorem on Diophantine approximation) has

$$q > \exp\left(\frac{10 \log N}{\log \log N}\right) ,$$

a different approach is required, based on the use of Vaughan's identity in (7), and then Vinogradov's mean value theorem (which actually sets the limit of the method).

In the present note we show that no growth condition such as (1) can yield any useful information on the discrepancy of the sequencies (2),(3).

THEOREM. *Let* $F(x)$ $(x=1,2,\ldots)$ *be any positive function* $\geqslant 1$ *tending to infinity with* x. *There is an entire function*

$$f(z) = \sum_{k=1}^{\infty} \frac{z^k}{q_1 \cdots q_k}$$

$(q_1, q_2, \ldots$ *positive integers*$)$ *for which*:

(i) we have

(10) $\log \left| f(R e^{i\theta}) \right| \leqslant F(R) \log R$

for $R \geqslant 1$;

(ii) the discrepancy $D(N)$ of $f(1),\ldots,f(N)$ (modulo one) satisfies

(11) $D(N) \geqslant N F(N)^{-1}$

for infinitely many N .

Proof. Let $q_1=2$. Once $q_1,\ldots,q_{m-1}$ have been defined (where $m \geqslant 2$) we set q_m equal to any positive integer for which we have:

(12) $q_m > q_{m-1}$,

(13) $\log q_m > m^2$,

(14) $F(x) > m$ for all $x \geqslant q_m/2$;

and furthermore, writing $N_m = [(q_m/8)^{1/m}]$

(15) $F(N_m) > 2q_1 \cdots q_{m-1}$.

For any sequence of integers defined in this way, the function f defined by (9) is clearly entire, from (13). We shall prove in addition that (10) holds, and that

(16) $D(N_m) \geqslant N_m F(N_m)^{-1}$ $\quad (m=2,3,\ldots)$.

Let's begin with (10). In view of (12), it will certainly suffice to show that

(17) $$\sum_{k=1}^{\infty} \frac{R^k}{q_1 \cdots q_k} \leqslant R^{F(R)}$$

whenever

(18) $(q_{m-1}/2) \leqslant R < (q_m/2)$

$(m = 2,3,\ldots)$. To prove (17) , we first observe that

(19) $$\frac{R^k}{q_1 \cdots q_k} > \frac{2R^{k+1}}{q_1 \cdots q_{k+1}}$$

for $k \geqslant m-1$; this is a consequence of (18) and (12) . Thus

(20) $$\sum_{k=m}^{\infty} \frac{R^k}{q_1 \cdots q_k} < \frac{R^m}{q_1 \cdots q_m}(1 + (1/2) + (1/4) + \ldots) < \frac{R^{m-1}}{q_1 \cdots q_{m-1}} .$$

On the other hand, if $m > 2$, we have

$$\frac{R^k}{q_1 \cdots q_k} \leqslant \frac{2R^{k+1}}{q_1 \cdots q_{k+1}}$$

for $k \leqslant m-2$. This yields

$$\sum_{k=1}^{m-1} \frac{R^k}{q_1 \cdots q_k} \leqslant \frac{R^{m-1}}{q_1 \cdots q_{m-1}} \left(1 + 2 + \ldots + 2^{m-2} \right) .$$

In fact, this is seen to hold for $m \geqslant 2$. Combining this with (20) , (13) , we obtain

$$(21) \qquad \sum_{k=1}^{\infty} \frac{R^k}{q_1 \cdots q_k} < \frac{2^{m-1} R^{m-1}}{q_1 \cdots q_{m-1}} < R^{m-1}$$

for R in the interval (19) .
What is more,

$$(22) \qquad m - 1 \leqslant F(R) \quad \text{for} \quad R \geqslant q_{m-1}/2 .$$

This is a consequence of (14) if $m \geqslant 3$ and the hypothesis $F(x) \geqslant 1$ if $m = 2$. Now (17) follows from (21) and (22) .

Now for the 'arithmetic condition' (16) : We have only to show that

$$(23) \qquad \sum_{k=m}^{\infty} \frac{N_m^{\,k}}{q_1 \cdots q_k} < \frac{1}{4q_1 \cdots q_{m-1}} .$$

For then

$$\left| f(n) - \sum_{k=1}^{m-1} \frac{n^k}{q_1 \cdots q_k} \right| < \frac{1}{4q_1 \cdots q_{m-1}} \qquad (1 \leqslant n \leqslant N_m)$$

and $\{f(n)\}$ evidently cannot lie in $[\frac{1}{4q_1 \cdots q_{m-1}} , \frac{3}{4q_1 \cdots q_{m-1}}]$ for these values of n . This yields

$$D(N_m) \geqslant \frac{N_m}{2q_1 \cdots q_{m-1}} > N_m F(N_m)^{-1}$$

because of (15) .

It remains to prove (23) . The argument used to prove (20) works with $R = N_m$, because $N_m < q_m/2$. Thus

$$\sum_{k=m}^{\infty} \frac{N_m^{\,k}}{q_1 \cdots q_k} < \frac{2N_m^{\,m}}{q_1 \cdots q_m} \leqslant \frac{1}{4q_1 \cdots q_{m-1}}$$

from the definition of N_m . This yields (23) , and the proof of the theorem is complete.

It is clear from the proof that the inequality analogous to (11) holds for the

subsequence $f(p)$ $(p \leqslant N)$; namely, the discrepancy is $\geqslant \pi(N)\, F(N)^{-1}$.

I would like to thank Professor W.K. Hayman, with whom I had interesting conversations concerning this problem.

REFERENCES

[1] R.C. Baker : Entire functions and uniform distribution modulo one. To appear, Proc. London Math. Soc.

[2] J-R. Chen : On Professor Hua's estimate of exponential sums. Sci. Sinica 20 (1977), 711-719.

[3] K. Prachar : Primzahlverteilung. Springer, Berlin 1957.

[4] G. Rauzy : Fonctions entières et répartition modulo un, II. Bull. Soc. Math. France 101 (1973), 185-192.

[5] G. Rhin : Répartition modulo 1 de $f(p_n)$ quand f est une serie entière. Répartition Modulo I , 176-244. Lecture Notes in Math. N° 475, Springer, Berlin 1975.

[6] I. M. Vinogradov : The Method of Trigonometrical Sums in the Theory of Numbers. Wiley-Interscience, New York 1954.

R. C. Baker
Royal Holloway College
Egham
Surrey TW20 OEX

*

* *

A REMARK ON THE DISTRIBUTION OF αp MODULO ONE.

Antal BALOG

1. The best result concerning the distribution of αp modulo one is due to G. Harman who proved :

THEOREM 1 (Harman (1983)).

Suppose that α is irrational and let $\| x \|$ denote the smallest distance of x from an integer. Then, for any real β, there are infinitely many primes p such that

$$\| \alpha p - \beta \| < p^{-3/10} \tag{1.1}$$

This 3/10 improves the following earlier exponents :

(1.2) I.M. Vinogradov (1954) : $1/5 - \varepsilon$,

(1.3) R.C. Vaughan (1977) : $1/4 - \varepsilon$,

(1.4) D.R. Heath-Brown (1982) : $4/15$.

The papers mentioned above use the following approach : After reducing the problem to the investigation of a sum over primes they relate the sum to bilinear forms and estimate these forms. The different results come from the different methods of relating the sum to bilinear forms but they use exactly the same bounds for bilinear forms.

The main purpose of this remark is to change the method of estimating bilinear forms. This new approach can give Theorem 1 only in the homogenous case (i.e. if $\beta = 0$), and only in a very sophisticated manner : While the main part of Harman's work is an ingenious method of treating sums over primes, and we leave this unchanged, our estimates for bilinear forms are far more complicated than Harman's ones.

Our approach, however, makes a connection between the distribution problem and classical problems of analytic number theory. One can prove :

THEOREM 2 .

Suppose that α is irrational and $\varepsilon > 0$ is any real number. If either the Generalized Riemann Hypothesis (later GRH) or the Large Value Conjecture (later LVC) is true then there are infinitely many primes p such that

$$\| \alpha p \| < p^{-1/3+\varepsilon} \tag{1.5}$$

Moreover our approach is more sensitive to the order of approximation of α by ra-

tionals. One can prove

THEOREM 3

Suppose that α *is irrational and* $\varepsilon > 0$ *is any real number. If*

$$\|\alpha q\| < q^{-43/31 - \varepsilon} \tag{1.6}$$

for infinitely many integers q *then*

$$\|\alpha p\| < p^{-9/28} \tag{1.7}$$

for infinitely many primes p .

One expects that the stronger condition (1.6) we assume, the better result (1.7) can be derived, but this is not the case. The exponent 9/28 is close to the best possible one of our method, even if we require far stronger conditions than that of (1.6).

2. The starting point of the original approach is the following. For a given three-tuplet α,β,δ (α is irrational, β is any real number and $0 < \delta < 1/2$) we define the function

$$f(x) = f_{\alpha,\beta,\delta}(x) = h(\alpha x - \beta) \tag{2.1}$$

where $h(y)$ is the characteristic function of the interval $(-\delta,\delta)$ extended periodically to the real line with period 1 .
Then the sum

$$\sum_{p \leqslant X} f(p) \tag{2.2}$$

is the number of those primes p up to X that satisfy

$$\|\alpha p - \beta\| < \delta \ . \tag{2.3}$$

The fact, that by choosing $\delta = X^{-3/10}$, (2.2) is positive for infinitely many X , proves Theorem 1 . In Harman's work this fact follows from the estimates for bilinear forms . Supposing that α is irrational and

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2} \ , \quad (a,q) = 1 \ , \quad |\theta| < 1 \ , \tag{2.4}$$

$$X = q^{3/2} \ , \quad \delta > X^{-1/3 + 5\varepsilon} \ , \quad \varepsilon > 0 \ , \tag{2.5}$$

$$|a_m| \ll m^{\varepsilon/5} \ , \quad |b_n| \ll n^{\varepsilon/5} \ , \tag{2.6}$$

we have

$$\sum_{\substack{mn \leqslant X \\ M < m \leqslant 2M \\ N < n \leqslant 2N}} a_m b_n f(mn) = 2\delta \sum_{\substack{mn \leqslant X \\ \cdot\cdot < m \leqslant 2M \\ < n \leqslant 2N}} a_m b_n + O(\delta X^{1-\varepsilon}) \tag{2.7}$$

provided

$$\delta^{-1}X^{5\varepsilon} << M << \delta^{2}X^{1-5\varepsilon} \quad \text{or} \quad \delta^{-2}X^{5\varepsilon} << M << \delta X^{1-5\varepsilon} \quad , \tag{2.8}$$

and we also have

$$\sum_{\substack{mn \leqslant X \\ M < m \leqslant 2M \\ N < n \leqslant 2N}} a_m f(mn) = 2\delta \sum_{\substack{mn \leqslant X \\ M < m \leqslant 2M \\ N < n \leqslant 2N}} a_m + O(\delta X^{1-\varepsilon}) \tag{2.9}$$

provided

$$M << \delta X^{1-5\varepsilon} \quad . \tag{2.10}$$

The proof is easy, see Vaughan (1977). All the proofs (1.1) - (1.4) give positive lower bound for (2.2) by using the above estimates for bilinear forms. To illustrate how they achieve this we state here, as the simplest method, the Vaughan's identity (see Vaughan (1977)).

For an arbitrary function $F(n)$ and for the parameters $1 \leqslant u \leqslant X$, $1 \leqslant v \leqslant X$ we have

$$\begin{aligned} \sum_{n \leqslant X} \Lambda(n) F(n) = {} & \sum_{n \leqslant v} \Lambda(n) F(n) + \sum_{\substack{mn \leqslant X \\ m \leqslant u}} \sum \mu(m) \log n \, F(mn) - \\ & - \sum_{\substack{mn \leqslant X \\ m \leqslant uv}} \sum a_m F(mn) + \sum_{\substack{mn \leqslant X \\ u < m \\ v < n}} \sum \mu(m) b_n F(mn) \end{aligned} \tag{2.11}$$

where the coefficients a_m and b_n satisfy

$$|a_m| \leqslant \log m \quad , \quad |b_n| \leqslant \log n \tag{2.12}$$

(The coefficients a_m and b_n depend not only on m and n but on u and v as well; actually

$$a_m = \sum_{\substack{m = dt \\ d \leqslant u \\ t \leqslant v}} \mu(d) \Lambda(t) \quad , \quad b_n = \sum_{\substack{n = dt \\ v < t}} \Lambda(t) \ ) \ . \tag{2.13}$$

The reader can easily verify (1.3) from (2.11) choosing

$$\delta \geqslant X^{-1/4+3\varepsilon} \quad , \quad u = v = X^{1/3} \tag{2.14}$$

and using (2.9) for the second and third terms, and (2.7) for the fourth term in the left hand side of (2.12).

3. The essence of the new argument is surprisingly simple. Suppose that α is irrational and

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2} \quad , \quad (a,q) = 1 \quad , \quad |\theta| < 1 \ . \tag{2.4}$$

If we find primes $p \leqslant X$, $q < X < q^2$ satisfying one of the congruences

(3.1) $$ap \equiv \ell \ (q) \quad , \quad 1 \leqslant \ell \leqslant L < q \quad , \quad (\ell,q) = 1$$

then, for these primes

(3.2) $$\|\alpha p\| < \frac{L}{q} + \frac{X}{q^2} \quad .$$

A well-known conjecture asserts that

(3.3) $$\pi(q^{1+\varepsilon},q,a) > 0$$

for all $(a,q) = 1$, $\varepsilon > 0$, $q > q_0(\varepsilon)$. Choosing $\ell = L = 1$, $X = q^{1+\varepsilon}$ in (3.1) , from (3.2) we get

(3.4) $$\|\alpha p\| < 2q^{-1+\varepsilon} \leqslant 2p^{-\frac{1-\varepsilon}{1+\varepsilon}}$$

for a prime $p \leqslant q^{1+\varepsilon}$. As is well-known from the Dirichlet Approximation Theorem, there are infinitely many rationals $\frac{a}{q}$ satisfying (2.4) for any irrational α . Using (3.4) for these q-s we get

(3.5) $$\|\alpha p\| < p^{-1+\varepsilon}$$

for infinitely many primes p (supposing the truth of (3.3)) .
The proof of (3.3) is hopeless at present, as even the powerful GRH implies only

(3.6) $$\pi(q^{2+\varepsilon},q,a) > 0 \ .$$

(3.6) is too weak to have any consequence for our problem, but using the GRH more efficiently we can get Theorem 2 .
Next we prove Theorem 2 in the case of the GRH . We are interested in the average distribution of primes in arithmetic progressions, i.e. in the sum

(3.7) $$S = \sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \pi(X,q,\ell\bar{a})$$

where $a\bar{a} \equiv 1 \ (q)$. (We can express S another way : Let $g(n)$ be the characteristic function of the residue classes $\ell\bar{a}$ modulo q , $\ell \leqslant L$, $(\ell,q) = 1$. Then

(3.8) $$S = \sum_{p \leqslant X} g(p) \quad .$$

This has the same shape as (2.2) , therefore the methods of Vinogradov, Vaughan and others can be applied. However, the completion of the proof is traditionally based on a Fourier-expansion method, and we repleace this step by a character-sum method). From the orthogonality of the characters

(3.9) $$S = \frac{1}{\varphi(q)} \sum_{\chi} \sum_{\ell \leqslant L} \bar{\chi}(\ell) \sum_{p \leqslant X} \chi(ap)$$

Here and below $\sum_{\chi}$ means that the sum is taken over all characters modulo q . The main term comes from the principal character χ_0 , and it is about

(3.10) $$\frac{LX}{q \log X} \quad .$$

The GRH implies (see Montgomery (1971))

(3.11) $$\Big| \sum_{p \leqslant X} \chi(p) \Big| << X^{1/2} \log X$$

for $\chi \neq \chi_0$, $X \geqslant q$ while the Mean Value Theorem (see next section) implies

(3.12) $$\sum_{\chi} \Big| \sum_{\ell \leqslant L} \chi(\ell) \Big| << qL^{1/2} \log L$$

for $L < q$. Thus the contribution of the non-principal characters is less than

(3.13) $$L^{1/2} X^{1/2} \log^2 X \ .$$

Choosing

(3.14) $$L = q^{1/2} \log^4 q \quad , \quad X = q^{3/2} \log^4 q$$

we get (on the GRH)

(3.15) $$S = \frac{LX}{q \log X} \left(1 + O\left(\frac{1}{\log X}\right)\right)$$

and from (3.2)

(3.16) $$\| \alpha p \| < \frac{2 \log^4 q}{q^{1/2}} < \frac{\log^6 X}{X^{1/3}} \quad .$$

Using this argument for infinitely many q we get Theorem 2 in the case of the GRH.

4. For technical reasons we will use weighted sums lile

(4.1) $$S_1 = \sum_{\substack{\ell = 1 \\ (\ell, q) = 1}}^{\infty} w_\ell \sum_{\substack{p \leqslant X \\ ap \equiv \ell (q)}} \log \frac{X}{p}$$

where

(4.2) $$w_\ell = e^{-(2\ell/L)^h} \quad , \quad h = \log^2 q$$

and

(4.3) $$S_2 = \sum_{\substack{\ell \leqslant L \\ (\ell, q) = 1}} \ell^{-1/2} \sum_{\substack{p \leqslant X \\ ap \equiv \ell (q)}} \log \frac{X}{p} \ .$$

In this section we will prove the following estimates for bilinear forms.

LEMMA 1

Supposing $\varepsilon > 0$, $MN \leqslant X$ and

(4.4) $$q^{1/2 + 5\varepsilon} << L < q < X < q^2 \quad , \quad q^{2 + 5\varepsilon} << LX \quad ,$$

(2.6) $$|a_m| << m^{\varepsilon/5} \quad , \quad |b_n| << n^{\varepsilon/5}$$

we have

(4.5)
$$\sum_{\substack{\ell=1 \\ (\ell,q)=1}}^{\infty} w_\ell \sum_{\substack{mn \leq X \\ M<m\leq 2M \\ N<n\leq 2N \\ amn \equiv \ell(q)}} a_m b_n \log \frac{X}{mn} =$$

$$= \frac{1}{\varphi(q)} \sum_{\substack{\ell=1 \\ (\ell,q)=1}}^{\infty} w_\ell \sum_{\substack{mn \leq X \\ M<m\leq 2M \\ N<n\leq 2N \\ (mn,q)=1}} a_m b_n \log \frac{X}{mn} + O\left(\frac{LX^{1-\varepsilon}}{q}\right)$$

provided

(4.6) $$\frac{q}{L} X^{5\varepsilon} << M << \frac{L^2}{q^2} X^{1-5\varepsilon} \quad \text{or} \quad \frac{q^2}{L^2} X^{5\varepsilon} << M << \frac{L}{q} X^{1-5\varepsilon}$$

and supposing in addition that $b_n = 1$ for all n we also have (4.5) provided

(4.7) $$M << \frac{L}{q} X^{1-5\varepsilon} .$$

LEMMA 2 .

Supposing $\varepsilon > 0$, $MN \leq X$ and

(4.8) $$q^{3/8+3\varepsilon} << L < q \, , \, q^{1+3\varepsilon} << X < q^2 \, , \, q^{1+3\varepsilon} << L^{1/2} X^{7/16} ,$$

(2.6) $$|a_m| << m^{\varepsilon/5} \quad , \quad |b_n| << n^{\varepsilon/5}$$

we have

(4.9)
$$\sum_{\substack{\ell \leq L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{mn \leq X \\ M<m\leq 2M \\ N<n\leq 2N \\ amn \equiv \ell(q)}} a_m b_n \log \frac{X}{mn} =$$

$$= \frac{1}{\varphi(q)} \sum_{\substack{\ell \leq L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{mn \leq X \\ M<m\leq 2M \\ N<n\leq 2N \\ (mn,q)=1}} a_m b_n \log \frac{X}{mn} + O\left(\frac{L^{1/2} X^{1-\varepsilon}}{q}\right)$$

provided

(4.10) $$\left(\frac{q}{L}\right)^{4/3} X^{5\varepsilon} << M << \left(\frac{L}{q}\right)^{4/3} X^{1-5\varepsilon} .$$

LEMMA 3 .

Supposing $\varepsilon > 0$, $MN_1 \ldots N_j \leq X$ and

$$1 \leqslant L < q < X < q^2 \ , \ q^{2+3\varepsilon} << LX \ , \tag{4.11}$$

$$|a_m| << m^{\varepsilon/5} \tag{4.12}$$

we have

$$\sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{mn_1 \dots n_j \leqslant X \\ M < m \leqslant 2M \\ N_i < n_i \leqslant 2N_i \\ amn_1 \dots n_j \equiv \ell(q)}} \dots \sum a_m \log \frac{X}{mn_1 \dots n_j} =$$

$$= \frac{1}{\varphi(q)} \sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{mn_1 \dots n_j \leqslant X \\ M < m \leqslant 2M \\ N_i < n_i \leqslant 2N_i \\ (mn_1 \dots n_j, q)=1}} \dots \sum a_m \log \frac{X}{mn_1 \dots n_j} + O\left(\frac{L^{1/2} X^{1-\varepsilon}}{q}\right) \tag{4.13}$$

provided

$$M << \frac{L}{q} X^{1-5\varepsilon} \qquad \text{if} \quad j = 1 \ , \tag{4.14}$$

$$M << \frac{X^{1-5\varepsilon}}{q} \qquad \text{if} \quad j = 2 \ . \tag{4.15}$$

LEMMA 4.

Supposing $\varepsilon > 0$, $MN \leqslant X$ and

$$q^{3/8+3\varepsilon} << L < q < X < q^2 \ , \ q^{2+3\varepsilon} << LX \tag{4.16}$$

$$|a_m| << m^{\varepsilon/5} \ , \ |b_n| << n^{\varepsilon/5} \tag{2.6}$$

we have - under the LVC -

$$\sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{mn \leqslant X \\ M < m \leqslant 2M \\ N < n \leqslant 2N \\ amn \equiv \ell(q)}} \sum a_m b_n \log \frac{X}{mn} =$$

$$= \frac{1}{\varphi(q)} \sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{mn \leqslant X \\ M < m \leqslant 2M \\ N < n \leqslant 2N \\ (mn,q)=1}} \sum a_m b_n \log \frac{X}{mn} + O\left(\frac{L^{1/2} X^{1-\varepsilon}}{q}\right) \tag{4.17}$$

provided

$$\frac{q}{L} X^{5\varepsilon} << M << \frac{L}{q} X^{1-5\varepsilon} \ . \tag{4.18}$$

The proofs need some more lemmas.

LEMMA 5 , (Reflexion Argument, Jutila (1977)) .

If $\chi \neq \chi_0$, $1 \leq L \leq q$, $h = \log^2 q$ and

$$L^* = \frac{qh^3}{L} = \frac{q \log^6 q}{L} \tag{4.19}$$

then

$$\Big| \sum_{\substack{\ell = 1 \\ (\ell,q)=1}}^{\infty} e^{-(2\ell/L)^h} \chi(\ell) \Big| << 1 + L^{1/2} d(q) \int_{-h^2}^{h^2} \Big| \sum_{\ell \leq L^*} \frac{\chi(\ell)}{\ell^{1/2 + i\tau}} \Big| \, d\tau \ . \tag{4.20}$$

LEMMA 6 , (Mean Value Theorem, Montgomery (1971)) .

For an arbitrary collection of complex numbers a_m we have

$$\sum_{\chi} \Big| \sum_{m \leq M} a_m \chi(m) \Big|^2 \leq (M+q) \sum_{m \leq M} |a_m|^2 \ . \tag{4.21}$$

LEMMA 7 , (Fourth Power Moment, Montgomery (1971)) .

$$\sum_{\chi \neq \chi_0} \Big| \sum_{\ell \leq L} \frac{\chi(\ell)}{\ell^{1/2 + it}} \Big|^4 << q(|t|+1) \log^6 qL(|t|+1) \ . \tag{4.22}$$

LEMMA 8 , (Large Value Theorem, Jutila (1977)) .

For an arbitrary collection of complex numbers a_m and for a positive V we have

$$\#\{\chi : \Big| \sum_{m \leq M} a_m \chi(m) \Big| > V\} << \frac{MG}{V^2} + \frac{q^{1+\eta} MG^3}{V^6} \tag{4.23}$$

where $G = \sum_{m \leq M} |a_m|^2$ and $\eta > 0$.

LEMMA 9 , (Burgess (1963)) .

If $\chi \neq \chi_0$ and $\eta > 0$, $L \geqslant 1$ then

$$\Big| \sum_{\ell \leq L} \frac{\chi(\ell)}{\ell^{1/2}} \Big| << q^{3/16 + \eta} \tag{4.24}$$

We are going to prove Lemma 1 . Using the orthogonality of the characters it is enough to show that under the given conditions

$$\Big| \sum_{\chi \neq \chi_0} \chi(a) L(\chi) C(\chi) \Big| << L \chi^{1-\varepsilon} \tag{4.25}$$

where

$$L(\chi) = \sum_{\ell=1}^{\infty} w_\ell \chi(\ell) \ , \tag{4.26}$$

$$(4.27)\qquad C(\chi) = \sum_{\substack{mn \leq X \\ M< m \leq 2M \\ N < n \leq 2N}} a_m b_n \chi(mn) \log \frac{X}{mn} \quad .$$

Taking

$$(4.28)\qquad A(s,\chi) = \sum_{M < m \leq 2M} \frac{a_m \chi(m)}{m^s} \quad , \quad B(s,\chi) = \sum_{N < n \leq 2N} \frac{b_n \chi(n)}{n^s}$$

We can express $C(\chi)$ as a Perron integral

$$(4.29)\qquad C(\chi) = \frac{1}{2\pi i} \int_{(1/2)} A(s,\chi)\, B(s,\chi)\, \frac{X^s}{s^2}\, ds$$

and, by taking absolute value

$$(4.30)\qquad |C(\chi)| << X^{1/2} \int_0^\infty |A(\tfrac{1}{2}+it,\chi)\, B(\tfrac{1}{2}+it,\chi)|\, \frac{dt}{t^2+1} \quad .$$

Writing (4.30) and (4.20) into the left hand side of (4.25) we arrive at

$$(4.31)\qquad \begin{aligned} &\Big|\sum_{\chi \neq \chi_0} \chi(a)\, L(\bar{\chi})\, C(\chi)\Big| << X^{1/2} \int_0^\infty \sum_{\chi \neq \chi_0} |A(\tfrac{1}{2}+it,\chi) B(\tfrac{1}{2}+it,\chi)|\, \frac{dt}{t^2+1} + \\ &+ L^{1/2} X^{1/2} d(q) \int_0^\infty \int_0^{h^2} \sum_{\chi \neq \chi_0} |L^*(\tfrac{1}{2}+i\tau,\chi) A(\tfrac{1}{2}+it,\chi) B(\tfrac{1}{2}+it,\chi)|\, \frac{d\tau dt}{t^2+1} \end{aligned}$$

where

$$(4.32)\qquad L^*(s,\chi) = \sum_{\ell \leq L^*} \frac{\chi(\ell)}{\ell^s}$$

and $L^* = \dfrac{q \log^6 q}{L}$ is defined in Lemma 5 .

From the Cauchy-Schwarz inequality

$$(4.33)\qquad \sum_{\chi \neq \chi_0} |AB| \leq \Big(\sum_\chi |A|^2\Big)^{1/2} \Big(\sum_\chi |B|^2\Big)^{1/2} ,$$

$$(4.34)\qquad \sum_{\chi \neq \chi_0} |AB| \leq q^{1/4} \Big(\sum_\chi |A|^2\Big)^{1/2} \Big(\sum_{\chi \neq \chi_0} |B|^4\Big)^{1/4} ,$$

$$(4.35)\qquad \sum_{\chi \neq \chi_0} |L^* AB| \leq \Big(\sum_\chi |L^* A|^2\Big)^{1/2} \Big(\sum_\chi |B|^2\Big)^{1/2} ,$$

$$(4.36)\qquad \sum_{\chi \neq \chi_0} |L^* AB| \leq \Big(\sum_\chi |A|^2\Big)^{1/2} \Big(\sum_\chi |L^* B|^2\Big)^{1/2} ,$$

$$(4.37)\qquad \sum_{\chi \neq \chi_0} |L^* AB| \leq \Big(\sum_{\chi \neq \chi_0} |L^*|^4\Big)^{1/4} \Big(\sum_{\chi \neq \chi_0} |B|^4\Big)^{1/4} \Big(\sum_\chi |A|^2\Big)^{1/2} .$$

Suppose that $b_n = 1$ for all n . By using (4.34) , (4.37) , Lemma 6 and Lemma 7

we get

$$(4.38)\qquad \Big|\sum_{\chi\neq\chi_0}\chi(a)L(\bar{\chi})C(\chi)\Big| << X^{1/2+\varepsilon}q^{1/2}(q+M)^{1/2}+L^{1/2}X^{1/2+\varepsilon}q^{1/2}(q+M)^{1/2} \ll LX^{1-\varepsilon}$$

provided

$$(4.39)\qquad q^{2+3\varepsilon} << LX \quad , \quad M << \frac{L}{q}X^{1-5\varepsilon} \quad .$$

In the general case, we use (4.33) , (4.34) or (4.35) and Lemma 6

$$(4.40)\qquad \begin{aligned}&\Big|\sum_{\chi\neq\chi_0}\chi(a)L(\bar{\chi})C(\chi)\Big| << X^{1/2+\varepsilon}(q+M)^{1/2}(q+N)^{1/2} + \\ &+ L^{1/2}X^{1/2+\varepsilon}\min((q+L^*M)(q+N)\ ,\ (q+M)(q+L^*N))^{1/2} << \\ &<< qL^{1/2}X^{1/2+\varepsilon}+q^{1/2}X^{1+\varepsilon}+L^{1/2}X^{1/2+\varepsilon}\min\Big(\frac{qX}{M}+\frac{q^2M}{L}\ ,\ qM+\frac{q^2X}{LM}\Big)^{1/2}\end{aligned}$$

and this has the required size provided

$$(4.41)\qquad \begin{aligned}&q^{2+3\varepsilon} << LX \quad , \quad q^{1+3\varepsilon} << L \quad , \\ &\frac{q}{L}X^{5\varepsilon} \ll M \ll \frac{L^2}{q^2}X^{1-5\varepsilon} \quad \text{or} \quad \frac{q^2}{L^2}X^{5\varepsilon} \ll M \ll \frac{L}{q}X^{1-\varepsilon} \quad .\end{aligned}$$

The proof of Lemma 1 is complete.

Next we turn to the proof of Lemma 2 and Lemma 4 . We retain the former notations $C(\chi)$, $A(s,\chi)$ and $B(s,\chi)$ but in the sequel we take

$$(4.42)\qquad L(\chi) = \sum_{\ell\leq L}\frac{\chi(\ell)}{\ell^{1/2}} \quad .$$

Using (4.30) it is enough to show that under the given conditions

$$(4.43)\qquad \sum_{\chi\neq\chi_0}|L(\chi)A(\tfrac{1}{2}+it,\chi)B(\tfrac{1}{2}+it,\chi)| << L^{1/2}X^{1/2-\varepsilon}$$

uniformly in t . We have the trivial bounds

$$(4.44)\qquad |A(s,\chi)| << M^{1/2+\varepsilon/5} \ , \ |B(s,\chi)| << N^{1/2+\varepsilon/5}$$

and from Lemma 9

$$(4.45)\qquad |L(\chi)| << q^{3/16+\eta} \quad , \quad \eta > 0 \quad .$$

It follows easily from (4.44) that the characters $\chi\neq\chi_0$ for which

$$(4.46)\qquad |L(\chi)| < q^{-1}$$

can be neglected. By the Mean Value Theorem (Lemma 6) the contribution of those characters $\chi\neq\chi_0$ for which one of the two bounds in (4.44) is less than $q^{\varepsilon/2}$ is at most

$$(4.47)\qquad q^{1/2+\varepsilon}(q+M)^{1/2}+q^{1/2+\varepsilon}(q+N)^{1/2}$$

which has the required size provided

$$(4.48) \qquad q^{2+3\varepsilon} << LX \quad , \quad \frac{q}{L} X^{5\varepsilon} << M << \frac{L}{q} X^{1-5\varepsilon} \quad .$$

The set of the remaining characters can be classified into at most $\log^3 X$ subsets $S(U,V,W)$ of characters satisfying simultanously the conditions

$$(4.49) \qquad V < |A(\tfrac{1}{2}+it,\chi)| \leqslant 2V \ , \ W < |B(\tfrac{1}{2}+it,\chi)| \leqslant 2W \ , \ U < |L(\chi)| \leqslant 2U$$

where

$$(4.50) \qquad q^{-1} \leqslant U << q^{3/16+\eta} \ , \ q^{\varepsilon/2} \leqslant V,W << q \ ,$$

and we will show

$$(4.51) \qquad UVW\,|S(U,V,W)| << L^{1/2} X^{1/2-\varepsilon} \quad .$$

We can derive some bounds for $S(U,V,W)$ from Lemma 6 , Lemma 7 and Lemma 8 . For simplicity we omit some q^{ε} factors from the left hand side of the formulas .

$$(4.52) \qquad \begin{aligned} |S(U,V,W)| &<< \frac{M+q}{V^2} \ , \\ |S(U,V,W)| &<< \frac{N+q}{W^2} \ , \\ |S(U,V,W)| &<< \frac{q}{U^4} \ , \\ |S(U,V,W)| &<< \frac{M}{V^2} + \frac{qM}{V^6} \ , \\ |S(U,V,W)| &<< \frac{N}{W^2} + \frac{qN}{W^6} \ . \end{aligned}$$

We apply an argument of Heath-Brown (see Iwaniec (1982) where he uses it in a similar context) . We take

$$(4.53) \qquad F = \min\left(\frac{M+q}{V^2}, \frac{N+q}{W^2}, \frac{M}{V^2} + \frac{qM}{V^6}, \frac{N}{W^2} + \frac{qN}{W^6}, \frac{q}{U^4} \right)$$

and we show

$$(4.54) \qquad UVWF << L^{1/2} X^{1/2-2\varepsilon} \quad .$$

We consider four cases.

Case 1 $F \leqslant 2M/V^2 \ , \ 2N/W^2$. From (4.50)

$$(4.55) \qquad UVWF \leqslant 2\,UVW \min\left(\frac{M}{V^2} , \frac{N}{W^2} \right) \leqslant 2U(MN)^{1/2} << q^{3/16+\eta} X^{1/2} << L^{1/2} X^{1/2-2\varepsilon} .$$

Case 2 $F > 2M/V^2 \ , \ 2N/W^2$. From (4.52)

$$(4.56) \qquad UVWF \leqslant 2\,UVW \min\left(\frac{q}{V^2} , \frac{q}{W^2} , \frac{qM}{V^6} , \frac{qN}{W^6} , \frac{q}{U^4} \right) \leqslant$$

$$(4.56)\quad \leqslant 2\,UVW\left(\frac{q^2}{V^2W^2}\right)^{5/16}\left(\frac{q^2MN}{V^6W^6}\right)^{1/16}\left(\frac{q}{V^4}\right)^{1/4} \leqslant q\,\chi^{1/16} << L^{1/2}\chi^{1/2-2\varepsilon}\ .$$

Case 3 $F > 2M/V^2$, $F \leqslant 2N/W^2$. From (4.52)

$$UVWF \leqslant 2\,UVW \min\left(\frac{q}{V^2}, \frac{N}{W^2}, \frac{qM}{V^6}, \frac{q}{U^4}\right) \leqslant$$

$$\leqslant 2\,UVW\left(\frac{q}{V^2}\right)^{1/8}\left(\frac{N}{W^2}\right)^{1/2}\left(\frac{qM}{V^6}\right)^{1/8}\left(\frac{q}{U^4}\right)^{1/4} \leqslant 2q^{1/2}N^{1/2}M^{1/8} \leqslant$$

$$\leqslant 2q^{1/2}\chi^{1/2}M^{-3/8} << L^{1/2}\chi^{1/2-2\varepsilon}\ .$$

Case 4 $F \leqslant 2M/V^2$, $F > 2N/W^2$. By interchanging the roles of M and N , V and W from (4.57) we get

$$(4.58)\qquad UVWF \leqslant 2q^{1/2}M^{1/2}N^{1/8} \leqslant 2q^{1/2}\chi^{1/8}M^{3/8} << L^{1/2}\chi^{1/2-2\varepsilon}\ .$$

The proof of Lemma 2 is finished. For the proof of Lemma 4 we note that the LVC (see Heath-Brown (1979)) implies that for an arbitrary collection of complex numbers a_m , a real number $\eta > 0$ and $V > q^{\eta}$ we have

$$(4.59)\qquad \#\{\chi : |\sum_{m \leqslant M} a_m \chi(m)| > V\} << \frac{M}{V^2}\max_{m \leqslant M}|a_m|^2\ .$$

This shows that under the LVC we have to consider only the Case 1 , and Lemma 4 follows from the above argument.

Finally we prove Lemma 3 . As it is familiar by now

$$(4.60)\qquad \sum_{\chi \neq \chi_0} |L(\chi)\,A(\tfrac{1}{2}+it,\chi)\,B_1(\tfrac{1}{2}+it,\chi)\ldots B_j(\tfrac{1}{2}+it,\chi)| << (|t|+1)^{1/2+\varepsilon}L^{1/2}\chi^{1/2-\varepsilon}$$

gives the required result. This follows easily from the Mean Value Theorem and from the Fourth Power Moment via Cauchy-Schwarz inequality

$$(4.61)\qquad \sum |LAB_1| \leqslant \left(\sum |L|^4\right)^{1/4}\left(\sum |B_1|^4\right)^{1/4}\left(\sum |A|^2\right)^{1/2},$$

$$\sum |LAB_1B_2| \leqslant \left(\sum |LA|^2\right)^{1/2}\left(\sum |B_1|^4\right)^{1/4}\left(\sum |B_2|^4\right)^{1/4}$$

We omit the details.

5. In this section we discuss the consequences of the estimates in the previous section.

With the notations (3.7) and (4.1) we have

$$(5.1)\qquad S > \frac{1}{\log\chi}S_1 + O(e^{-q})\ .$$

Choosing

$$X = qL \tag{5.2}$$

in our arguments, we can see from (3.2) that L/q has the same role that δ had originally. As the critical conditions (2.8) and (2.10) are exactly the same as (4.6) and (4.7) we can derive all the results (1.1) - (1.4) from Lemma 1 by using the appropriate methods of relating a sum over primes to bilinear forms. In particular, combining Lemma 1 with Harman's method we can cover Theorem 1 (in the homogenous case) but there is no room here to give details.

Next we prove Theorem 2 on the LVC. We choose

$$L = q^{1/2+6\varepsilon} \quad , \quad X = q^{3/2+6\varepsilon} \tag{5.3}$$

and we use Vaughan's identity (2.11) with

$$F(n) = \begin{cases} \ell^{-1/2} \log \frac{X}{n} & \text{if } an \equiv \ell(q) \ , \ \ell \leqslant L \text{ and } (\ell,q) = 1 \ , \\ 0 & \text{otherwise .} \end{cases} \tag{5.4}$$

Choosing

$$u = v = X^{1/3} \ , \tag{5.5}$$

Lemma 3 with $j=1$ covers the second and third terms while Lemma 4 covers the fourth term and we get

$$\sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{n \leqslant X \\ an \equiv \ell(q)}} \Lambda(n) \log \frac{X}{n} =$$

$$= \frac{1}{\varphi(q)} \sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{n \leqslant X \\ (n,q)=1}} \Lambda(n) \log \frac{X}{n} + O\left(\frac{L^{1/2} X^{1-\varepsilon/2}}{q}\right) \tag{5.6}$$

From the trivial inequality

$$S > \frac{1}{\log X} S_2 \tag{5.7}$$

we can easily derive

$$S >> \frac{L^{1/2} X}{q \log X} \tag{5.8}$$

supposing (5.3) and the LVC . This implies Theorem 2 .

Lemma 2 and Lemma 3 ($j=1$) combined with Vaughan's identity give only the result (1.3) but it is interesting to note that the limit 1/4 comes not from the use of the Vaughan's identity but from the use of the Large Value Theorem. Any improvement on the Large Value Theorem leads to better exponents than 1/4 without applying deeper methods than Vaughan's identity. The limit is 1/3 .

Finally we prove Theorem 3 . This requires the use of Heath-Brown's argument, because Vaughan's identity is not sufficient. We will be brief, the details can be found in

Heath-Brown (198?) . Let

$$(5.9) \qquad X^{1/10} \leqslant z \leqslant X^{1/5} \ , \ z_0 = \exp\left(\frac{\log X}{(\log\log X)^2}\right) \ , \ K = [\,(\log\log X)^2\,]$$

b real numbers where X is sufficiently large, and define the coefficients A_n , B_n , $A_n(j)$, $A_n^*(j)$ as follows . For $\operatorname{Re} s > 1$

$$(5.10) \qquad \Pi(s) = \prod_{p \leqslant z} \left(1 - \frac{1}{p^s}\right) \ , \ \Pi_0(s) = \prod_{p \leqslant z_0} \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)\, B_n}{n^s} \ ,$$

$$(5.11) \qquad \sum_{n=1}^{\infty} \frac{A_n}{n^s} = \log \zeta(s)\, \Pi(s) = \sum_{\alpha=1}^{\infty} \sum_{p > z} \frac{1}{\alpha p^{\alpha s}} \ ,$$

$$(5.12) \qquad \sum_{n=1}^{\infty} \frac{A_n(j)}{n^s} = (\zeta(s)\, \Pi(s) - 1)^j \ ,$$

$$(5.13) \qquad \sum_{n=1}^{\infty} \frac{A_n^*(j)}{n^s} = \left(\zeta(s) \sum_{n \leqslant z} \frac{\mu(n)\, B_n}{n^s} \sum_{k=0}^{K} \frac{(-1)^k}{k!} \left(\sum_{z_0 < p \leqslant z} \frac{1}{p^s} \right)^k - 1 \right)^j \ .$$

In other words,

$$(5.14) \qquad A_n = \begin{cases} 1/\alpha & \text{if } n = p^\alpha \ , \ p > z \ , \\ 0 & \text{otherwise} \ , \end{cases}$$

B_n is the characteristic function of the numbers having no prime factors $> z_0$, and $A_n(j)$ is the representations of n as a product of j factors composed by primes $> z_0$. The definition of $A_n^*(j)$ is rather complicated but it is clear that $A_n^*(j)$ approximates $A_n(j)$ in a certain sense.

We can formulate this connection the following way, see Heath-Brown (198?) § 2 . For any function $F(n)$ we have

$$\left| \sum_{n \leqslant X} A_n(j) F(n) - \sum_{n \leqslant X} A_n^*(j) F(n) \right| <<$$

$$(5.15) \qquad << \sum_{z < d \leqslant z_0} \mu^2(d)\, B_d \sum_{m \leqslant \frac{X}{d}} d_{2j}(m) F(dm) +$$

$$+ \sum_{z_0 < p \leqslant z} \sum_{m \leqslant \frac{X}{p^2}} d_{2j}(m) F(p^2 m)$$

where $d_j(m)$ denotes the number of representations of m as a product of j factors. Using the well-known bound of Linnik (1963)

$$(5.16) \qquad \sum_{\substack{m \leqslant Y \\ m \equiv a(q)}} d_j(m) << \frac{Y}{q} \log^{C_j} Y \quad \text{if } (a,q) = 1 \ , \ q < Y^{1-\varepsilon} \ ,$$

we get in the case of $F(n)$ is defined by (5.4) that the right hand side of (5.15) is

$$(5.17) \qquad << \frac{L^{1/2} X}{q} e^{-(\log\log X)^2}$$

provided

$$(5.18) \qquad z^2 q < X^{1-\varepsilon} .$$

When $F(n) = \log \frac{X}{n}$, 0 according as $(n,q) = 1$ or not than the right hand side of (5.15) is

$$(5.19) \qquad << X e^{-(\log\log X)^2} .$$

The connection between A_n and $A_n(j)$ follows from the identity

$$(5.20) \qquad \log \zeta(s)\Pi(s) = \sum_{j=1}^{\infty} \frac{(-1)^{j-1}}{j} (\zeta(s)\Pi(s)-1)^j ,$$

thus by comparing the coefficients:

$$(5.21) \qquad A_n = \sum_{j=1}^{\infty} \frac{(-1)^{j-1}}{j} A_n(j) .$$

The large j-s cause a little trouble so we use a sieve argument similar to the simplest Brun's sieve

$$(5.22) \qquad A_n \begin{matrix} \geq \\ = \\ < \end{matrix} \sum_{j=1}^{J} \frac{(-1)^{j-1}}{j} A_n(j)$$

and $\geqslant$ ($\leqslant$) holds for even (odd) J-s .
We are interested in

$$(4.3) \qquad S_2 = \sum_{p \leqslant X} F(p)$$

(c.f. (5.4)). We can connect this sum to

$$(5.23) \qquad S_2' = \sum_{n \leqslant X} A_n F(n)$$

(c.f. (4.14)) and using (5.21) or (5.22) we can transfer this to the investigation of

$$(5.24) \qquad S(j) = \sum_{n \leqslant X} A_n(j) F(n) .$$

We will show that under some conditions on L, X, z, j we have

$$(5.25) \qquad S^*(j) = \sum_{n \leqslant X} A_n^*(j) F(n) = \frac{1}{\varphi(q)} \sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{\substack{n \leqslant X \\ (n,q)=1}} A_n^*(j) \log \frac{X}{n} + O\left(\frac{L^{1/2} X^{1-\varepsilon}}{q}\right) .$$

(5.15), (5.17), (5.19 and (5.25) lead to

$$(5.26)\qquad S(j) = \frac{1}{\varphi(q)} \sum_{\substack{\ell \leqslant L \\ (\ell,q)=1}} \ell^{-1/2} \sum_{n \leqslant X} A_n(j) \log \frac{X}{n} + O\left(\frac{L^{1/2} X}{q} e^{-(\log\log X)^2}\right)$$

and we get from (5.21) and (5.22) that for even J

$$(5.27)\qquad S_2 >> \frac{L^{1/2}}{q} R(J) + O\left(\frac{L^{1/2} X}{q} e^{-(\log\log X)^2}\right)$$

where

$$(5.28)\qquad R(J) = \sum_{n \leqslant X} A_n \log \frac{X}{n} + \sum_{J < j} \frac{(-1)^j}{j} \sum_{n \leqslant X} A_n(j) \log \frac{X}{n} .$$

First we investigate the expression $R(4)$, (for $j=5$ we are not able to prove (5.25)). Note that $R(J)$ is independent of L and q. We will show that

$$(5.29)\qquad R(4) >> \frac{X}{\log X}$$

if

$$(5.30)\qquad z = X^{1/7 - 10\varepsilon}$$

with a sufficiently small ε. (5.30) implies that the terms $j \geqslant 8$ vanish. The contribution of the n-s having seven prime factors can be neglected because all these primes must satisfy

$$(5.31)\qquad X^{1/7 - 10\varepsilon} < p \leqslant X^{1/7 + 60\varepsilon} .$$

The n-s having six prime factors contribute to the term $j=6$ with

$$(5.32)\qquad \frac{1}{6} \sum_{\substack{p_1 \cdots p_6 \leqslant X \\ p_i > z}} \log \frac{X}{p_1 \cdots p_6}$$

and to the term $j=5$ with at most

$$(5.33)\qquad 5 \cdot \frac{1}{5} \sum_{\substack{p_1 \cdots p_6 \leqslant X \\ P_i > z}} \log \frac{X}{p_1 \cdots p_6} .$$

The contribution of the n-s having five prime factors is similar to (5.32) with 5 in place of 6. There are no other contributions. By the prime number theorem

$$(5.34)\qquad \begin{aligned} R(4) \geqslant & \sum_{p \leqslant X} \log \frac{X}{p} - \frac{1}{5} \sum_{\substack{p_1 \cdots p_5 \leqslant X \\ p_i > z}} \log \frac{X}{p_1 \cdots p_6} - \\ & - \frac{5}{6} \sum_{\substack{p_1 \cdots p_6 \leqslant X \\ p_i > z}} \log \frac{X}{p_1 \cdots p_6} - 10^7 \cdot \varepsilon \cdot \frac{X}{\log X} \geqslant \\ \geqslant & \frac{X}{\log X} \left(1 - \frac{1}{5} \int\cdots\int \frac{dt_1 \cdots dt_4}{t_1 \cdots t_4 (1 - t_1 - \cdots - t_n)} - \frac{5}{6} \int\cdots\int \frac{dt_1 \cdots dt_5}{t_1 \cdots t_5 (1 - t_1 - \cdots - t_5)} - 10^8 \varepsilon \right. \frac{X}{\log X} \end{aligned}$$

where the integrals are taken over the four and five dimensional domains

$$(5.35)\qquad \begin{aligned} D_4 &= \left(\tfrac{1}{7} - 10\varepsilon \leqslant t_i\ ,\ t_1+\ldots+ t_4 \leqslant \tfrac{6}{7} + 10\varepsilon\right)\ , \\ D_5 &= \left(\tfrac{1}{7} - 10\varepsilon \leqslant t_i\ ,\ t_1+\ldots+ t_5 \leqslant \tfrac{6}{7} + 10\varepsilon\right) \end{aligned}$$

respectively. Numerical integration shows that (5.29) is true whenever ε is small enough.

We will be ready if we prove (5.25) with (5.30) , $j \leqslant 4$ and

$$(5.36)\qquad X = q^{56/31 + 11\varepsilon}\ ,\ L = qX^{-9/28}$$

because in this case

$$(5.37)\qquad \|\alpha p\| < \frac{L}{q} + \frac{X}{q^{74/31 + 15\varepsilon}} << X^{-9/28}$$

for a great many primes p up to X .

Note that (5.36) implies (4.8) , (4.11) and (5.18) .

The structure of $A_n^*(j)$ (c.f. (5.13)) shows that $S^*(j)$ can be rewritten as a sum of at most

$$(K+1)^j << (\log\log X)^8$$

multilinear forms of type

$$(5.38)\qquad \sum_{\substack{m_1\ldots m_r n_1\ldots n_j \leqslant X \\ m_i \leqslant z\ \ i=1,\ldots,r}} \ldots \sum a_{m_1}^{(1)}\ldots a_{m_r}^{(r)} F(m_1\ldots m_r n_1\ldots n_j)$$

with

$$(5.39)\qquad r \leqslant j(K+1) << (\log\log X)^2\ .$$

Further splitting up and rearranging arguments lead to the representation of $S^*(j)$ as a sum of at most

$$(5.40)\qquad (K+1)^j 2^{j(K+1)} (\log X)^{24} << e^{(\log\log X)^3}$$

multilinear forms of type

$$(5.41)\qquad \sum_{\substack{m_1\ldots m_r n_1\ldots n_j \leqslant X \\ M_i < m_i \leqslant 2M_i \\ N_i < n_i \leqslant 2N_i}} \ldots \sum a_{m_1}^{(1)}\ldots a_{m_r}^{(r)} F(m_1\ldots m_r n_1\ldots n_j)$$

where $r \leqslant 20$ and

$$(5.42)\qquad M_i \leqslant z \qquad i = 1,\ldots,r\ ,$$

$$(5.43)\qquad M_1\ldots M_r N_1\ldots N_j \leqslant X\ ,\ \ N_1 \geqslant \ldots \geqslant N_j\ ,$$

$$(5.44)\qquad |a_m^{(i)}| << m^{\varepsilon/10} \qquad i = 1,\ldots,r\ .$$

we can assume

$$M_1 \ldots M_r N_1 \ldots N_j > X^{1-4\varepsilon} \tag{5.45}$$

otherwise both (5.41) and its expected value are trivially less than the required error term.

We can use Lemma 2 if there is a subproduct M of $M_1 \ldots M_r N_1 \ldots N_j$ satisfying

$$X^{3/7-5\varepsilon} << M << X^{4/7+5\varepsilon}, \tag{5.46}$$

and we can use Lemma 3 if either

$$N_1 \geqslant X^{4/7+5\varepsilon} \tag{5.47}$$

or $j \geqslant 2$ and

$$N_1 N_2 \geqslant X^{4/7+5\varepsilon}. \tag{5.48}$$

z was chosen to equal the quotient of the two sides of (5.46). This ensures that if N is any number less than $X^{3/7-5\varepsilon}$ and $NM_1 \ldots M_r$ is greater than $X^{3/7-5\varepsilon}$ then there is a subproduct M of $NM_1 \ldots M_r$ between $X^{3/7-5\varepsilon}$ and $X^{4/7+5\varepsilon}$.

Suppose that there is no subproduct M of $M_1 \ldots M_r N_1 \ldots N_j$ satisfying (5.46), $N_1 < X^{4/7+5\varepsilon}$ and for $j \geqslant 2$, $N_1 N_2 < X^{4/7+5\varepsilon}$. Then $N_1 < X^{3/7-5\varepsilon}$ and for $j \geqslant 2$, $N_1 N_2 < X^{3/7-5\varepsilon}$ and therefore $M_1 \ldots M_r N_1 < X^{3/7-5\varepsilon}$ and for $j \geqslant 2$, $M_1 \ldots M_r N_1 N_2 < X^{3/7-5\varepsilon}$. On the other hand for $j = 3$, $N_3 < N_1$ and for $j = 4$, $N_3 N_4 < N_1 N_2$. These inequalities imply $M_1 \ldots M_r N_1 \ldots N_j < X^{6/7-10\varepsilon}$ which contradicts (5.45).

The proof of Theorem 3 is completed.

6. ACKNOLEDGEMENT.

The author would like to express his thanks to Prof. P. Liardet and to Prof. G. Rauzy for their kind invitation to the "COLLOQUE THEORIE ANALYTIQUE ET ELEMENTAIRE DES NOMBRES" and for the opportunity of giving a talk on this subject.

REFERENCES

D. BURGESS (1963): On character sums and L series,II.,Proc. Lond. Math. Soc.,13 (1963),524-536.

G. HARMAN (1983): On the distribution of αp modulo one, J. London Math. Soc.,27 (1983),9-18.

D. R. HEATH-BROWN(1979): A large value estimate for Dirichlet polynomials, J. London Math. Soc.,20(1979),8-18.

D. R. HEATH-BROWN(1982): unpublished.

D. R. HEATH-BROWN(198?): The number of primes in a short interval,I.,to appear.

H. IVANIEC(1982): On the Brun-Titchmarsh theorem. J. Math. Soc. Japan,34(1982),95-123.

M. JUTILA(1977): Zero density estimates for L functions, Acta Arith.,32(1977), 55-62.

Yu. V. LINNIK(1963): The dispersion method in binary additive problems. American Math. Soc., Providence,1963.

H. L. MONTGOMERY(1971): Topics in multiplicative number theory. Springer, Berlin.

R. C. VAUGHAN(1977): On the distribution of αp modulo 1 , Mathematika,24(1977), 135-141.

I. M. VINIGRADOV(1954): The method of trigonometric sums in the theory of numbers, Whiley- Interscience, London,1954.

*

* *

Antal BALOG
MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST 1395 , PF 428

PERMUTATIONS DES ENTIERS
ET REPARTITION DES SUITES

Jean COQUET

Summary: *The permutations* h *of* $\mathbb{N}$ *which transform every* μ*-distributed (resp.* μ*-well distributed) sequence* u *with values in a compact metric space* X *into a sequence* $u \circ h$ *which is* μ*-distributed (resp.* μ*-well distributed) too, are studied.*

I. INTRODUCTION

I.1. Définitions.

. Une partie A de $\mathbb{N}$ a pour densité d (resp. pour densité uniforme d) si

$$d = \lim_{N\to\infty} \frac{1}{N} \text{Card } (A \cap [0\,,\ N[\,)$$

(resp. si $d = \lim_{N\to\infty} \frac{1}{N} \text{Card } (A \cap [\tau\,,\ N+\tau[\,)$ uniformément par rapport à $\tau \in \mathbb{N}$).

. X étant un espace métrique compact muni d'une mesure de probabilité μ , une partie Y de X , μ-mesurable et de frontière μ-négligeable, est appelée une partie de μ-continuité.

. Une suite $u:\mathbb{N} \to X$ est dite μ-répartie [4] (resp. uniformément μ-répartie) si pour toute partie Y de X , de μ-continuité, $u^{-1}(Y)$ a une densité (resp. une densité uniforme) égale à $\mu(Y)$.

I.2. Rappels.

De nombreuses études ont été faites de transformations qui, à toute suite μ-répartie, associent une suite μ-répartie. On peut citer notamment le travail de G. RAUZY [5] (voir aussi [7]) sur la stabilité de l'équirépartition d'une suite dans un groupe compact par addition d'une autre suite et le lien remarquable avec l'indépendance statistique.

Dans le livre de G. RAUZY [6], on trouve des résultats et des références sur la répartition des suites extraites.

H. RINDLER [8] a étudier la génération des classes d'équivalence de suites μ-réparties à partir de l'une d'elles au moyen des permutations h de $\mathbb{N}$ qui vérifient la condition de stabilité:

$$\text{Card } \{n \in \mathbb{N}\ ;\ n < N\ ,\ h(n) \geqslant N\} = o(N)\ .$$

On trouve des préoccupations semblables dans un travail de J. COUOT [3]. Enfin, l'auteur a montré dans [2] que si $s(n)$ est la somme des chiffres de n dans une base et si u est uniformément μ-répartie, $u \circ s$ l'est aussi. Par contre, s ne conserve pas la μ-répartition ordinaire.

Dans cet article, on étudie les permutations de $\mathbb{N}$ qui conservent la répartition ou la répartition uniforme et on donne quelques exemples.

I.3. Conservation de la répartition.

Définition. 1) Une permutation h de $\mathbb{N}$ conserve la répartition (resp. la répartition uniforme) dans l'espace métrique probabilisé (X,μ) si, pour toute suite $u:\mathbb{N} \to X$, μ-répartie (resp. uniformément μ-répartie), $u \circ h$ est μ-répartie (resp. uniformément μ-répartie).
Si h conserve la répartition (resp. la répartition uniforme) dans tout espace métrique compact probabilisé, h est appelée une permutation c.r.s.(resp. c.r.u.s.).

2) Une partie A de $\mathbb{N}$ est connexe si $A + [0,1[$ est un intervalle. Une composante connexe d'une partie B de $\mathbb{N}$ est une partie connexe maximale de B. Par commodité, la longueur $\ell(A)$ d'une partie connexe bornée A de $\mathbb{N}$ désigne la longueur de $A + [0,1[$.

Notations. 1) On note $[a,b[$ l'ensemble $\{a,\ldots,b-1\}$.

2) Pour tout entier N , on pose $H(N) = h([0,N[)$ et on note $\bar{H}(N)$ le plus petit intervalle contenant $H(N)$.

On caractérise les permutations c.r.u.s. et on donne une condition suffisante pour qu'une permutation ne soit pas c.r.s. . Au paragraphe V , on étudie des permutations liées à la représentation binaire des entiers.

THEOREME 1. h *désigne une permutation de* $\mathbb{N}$. *Il y a équivalence entre les cinq assertions suivantes :*
(i) h *est c.r.u.s. ;*
(i bis) pour toute partie A *de* $\mathbb{N}$ *ayant une densité uniforme,* $h^{-1}(A)$ *a une densité uniforme égale à celle de* A *;*
(ii) il existe un espace métrique compact X *muni d'une probabilité* μ *non concentrée en un point dans lequel* h *conserve la répartition uniforme ;*
(ii bis) il existe un réel d , $0 < d < 1$, *tel que pour toute partie* A *de* $\mathbb{N}$ *de densité uniforme* d , $h^{-1}(A)$ *ait une densité uniforme égale à* d *;*
(iii) le nombre maximal par rapport à $t \in \mathbb{N}$ *de composantes connexes de* $h([t,N+t[)$ *est un* $o(N)$ *lorsque* N *tend vers l'infini.*

THEOREME 2. h *désigne une permutation de* $\mathbb{N}$. *S'il existe* $\beta > 0$ *tel que pour tout* $\alpha > 0$, *il existe une infinité d'entiers* N *pour lesquels il existe une*

partie $P(N)$ *de* $\bar{H}(N) \setminus H(N)$ *et une injection* $\phi_N : P(N) \to H(N)$ *vérifiant :*

$$\text{Card } P(N) \geqslant \beta N \text{ et pour tout } n \in P(N),\ |n - \phi_N(n)| \leqslant \alpha n \quad ,$$

h *n'est pas une permutation c.r.s..*

La condition précédente est peut-être nécessaire et suffisante pour que h ne soit pas c.r.s.. En tout cas, il est nécessaire pour que h ne soit pas c.r.s. qu'il existe $\beta > 0$ et une infinité d'entiers N pour lesquels

$$\text{Card}(\bar{H}(N) \setminus H(N) \geqslant \beta N \ .$$

II. PREUVE DU THEOREME 1

Le schéma de démonstration est (iii) => (i bis) => (i) => (ii) => (ii bis) => (iii). L'implication (i) => (ii) est évidente.

II.1. Preuve de (i bis) => (i)

$u : \mathbb{N} \to X$ désigne une suite μ-répartie. Etant donnée une partie Y de X de μ-continuité, $\mu(Y)$ est la densité uniforme de $u^{-1}(Y)$ donc de $h^{-1}(u^{-1}(Y)) = \{n \in \mathbb{N} \ ; \ u(h(n)) \in Y\}$. Ainsi, uoh est uniformément μ-répartie. ∎

II.2. Preuve de (ii) => (ii bis)

D'après l'hypothèse sur μ, il existe ([4], p 201) une partie Y de X, de μ-continuité, telle que $0 < \mu(Y) < 1$. On peut évidemment supposer Y compacte. On note $d = \mu(Y)$.

Soit A une partie de $\mathbb{N}$ de densité uniforme d. On va construire une suite $u : \mathbb{N} \to X$ uniformément μ-répartie et telle que $A = u^{-1}(Y)$, ce qui permettra de conclure car, uoh étant aussi uniformément μ-répartie, $h^{-1}(A)$ aura aussi pour densité uniforme d.

D'après un résultat de BAAYEN et HEDRLIN [1], il existe une suite $u_1 : \mathbb{N} \to Y$ uniformément μ_1-répartie où μ_1 est la restriction à Y de $\frac{\mu}{d}$. De même il existe une suite $u_2 : \mathbb{N} \to X \setminus \overset{\circ}{Y}$ uniformément μ_2-répartie où μ_2 est la restriction à $X \setminus \overset{\circ}{Y}$ de $\frac{\mu}{1-d}$.

Comme la frontière de $X \setminus Y$ est μ-négligeable, on peut quitte à remplacer les termes $u_2(n)$ appartenant à la frontière par des éléments arbitraires de $X \setminus \overline{Y}$, supposer que u_2 est à valeurs dans $X \setminus \overline{Y} = X \setminus Y$.

On note $(a_k)_{k\in\mathbb{N}}$ la suite croissante des éléments de A et $(b_j)_{j\in\mathbb{N}}$ la suite croissante des éléments de $\mathbb{N} \setminus A$ et on pose :

$$u(n) = \begin{cases} u_1(k) \text{ si } n = a_k \\ \\ u_2(j) \text{ si } n = b_j \end{cases}$$

Soit alors Z une partie de X de μ-continuité. On pose $Z_1 = Z \cap Y$, $Z_2 = Z \cap (X \setminus Y)$, $\alpha_1 = \mu(Z_1)$, $\mu_2 = \alpha(Z_2)$.

$$u^{-1}(Z) \cap [t,N+t[= \{a_k \in [t,N+t[\ ; \ k \in u_1^{-1}(Z_1)\} \cup \{b_j \in [t,N+t[\ ; \ j \in u_2^{-1}(Z_2)\}$$

On pose $r = \text{Inf } \{k \ ; \ a_k \in [t, N+t[\}$ si $A \cap [t,N+t[\neq \emptyset$ et $s = \text{Inf } \{k \ ; \ a_k \geq N + t\}$.

Comme la densité uniforme de A est d, pour tout $\varepsilon > 0$, il existe $K_1 \in \mathbb{N}$ tel que $N \geq K_1 \Rightarrow |s - r - dN| = |\text{Card } (A \cap [t, N+t[) - dN| \leq \varepsilon N$.

En particulier $s - r \geq \frac{d}{2} N$ si $\varepsilon \leq \frac{d}{2}$.

D'autre part, $\text{Card } \{a_k \in [t, N+t[\ ; \ k \in u_1^{-1}(Z_1)\} = \text{Card } [r, s[\cap u_1^{-1}(Z_1)$.

Comme $u_1^{-1}(Z_1)$ a pour densité uniforme $\frac{\alpha_1}{d} = \mu_1(Z_1)$, pour $N \geq K_2$, $|\text{Card } ([r,s[\cap u_1^{-1}(Z_1)) - \frac{\alpha_1}{d} (s-r)| \leq \varepsilon(s-r) \leq \varepsilon N$. Pour $N \geq \text{Max } (K_1, K_2)$

$$|\text{Card } \{a_k \in [t, N+t[\ ; \ k \in u_1^{-1}(Z_1)\} - \alpha_1 N| \leq 2 \ \varepsilon N.$$

A l'aide d'une inégalité analogue pour $\{b_j \in [t, N+t[\ ; \ j \in u_2^{-1}(Z_2)\}$, on conclut que $\mu(Z) = \alpha_1 + \alpha_2$ est la densité uniforme de $u^{-1}(Z)$. ∎

II.3. Preuve de (iii) => (i bis)

A désigne une partie de $\mathbb{N}$ de densité uniforme d. On a :

$$\text{Card } (h^{-1}(A) \cap [t, n+t[) = \text{Card } (A \cap h([t, N+t[)).$$

Etant donné $\varepsilon > 0$, il existe $K \in \mathbb{N}^*$ tel que, pour tout intervalle I de longueur > K,

$$|\text{Card } (A \cap I) - d\ell(I)| \leq \varepsilon\ell(I).$$

On en déduit en distinguant les composantes connexes de $h([t, n+t[)$ de longueur > K et les autres :

$$|\text{Card } (A \cap h([t, N+t[)) - dN| \leq \varepsilon N + o(N)$$

Ainsi $h^{-1}(A)$ a une densité uniforme égale à d.

II.4. Preuve de (i bis) => (iii)

On suppose que h ne vérifie pas (iii).

Lemme 1. *Il existe un entier* L *tel que le nombre maximal par rapport à* t *de composantes connexes de longueur* L *de* $h([t,N+t[)$ *ne soit pas un* $o(N)$.

preuve : par l'absurde. Soit $\varepsilon > 0$, on choisit K tel que $K^{-1} < \varepsilon$. Le nombre maximal de composantes de longueur > K de $h([t, N+t[)$ est inférieur à $\frac{N}{K} < \varepsilon N$. Si le lemme était faux, le nombre maximal de composantes de longueur $\leq$ K serait majoré par εN pour N assez grand donc h vérifierait (iii). ■

Du lemme 1, on déduit qu'il existe $L \in \mathbb{N}^*$, $\delta \in]0, 1[$ et une suite d'intervalles $I_r = [t_r, N_r + t_r[$ vérifiant :

$$\begin{cases} \ell(I_r) \xrightarrow[r\to\infty]{} \infty \\ h(I_r) \text{ a au moins } \delta N_r \text{ composantes connexes de longueur L.} \end{cases}$$

Lemme 2. *Il existe* $\alpha \in]0,1[$ *et une suite d'intervalles* J_k *tels que*

$\ell(J_k) \underset{k\to\infty}{\to} \infty$, $\text{Sup } J_k < \text{Inf } J_{k+1}$, $\text{Sup } h(J_k) < \text{Inf } h(J_{k+1})$ *et* $h(J_k)$ *ait au moins* $\alpha\ell(J_k)$ *composantes connexes de longueur* L.

preuve : on choisit $\alpha = \frac{\delta}{2}$ et on construit $J_k = [a_k, b_k[$ par récurrence en commençant par $J_1 = I_1$. On suppose $J_1, \ldots, J_k$ construits. Il existe un intervalle I_r tel que :

$\frac{\delta}{2} N_r \geq m_k = \text{Max } (1 + b_k ; \inf \{m ; \forall n \geq m, h(n) > \text{Sup } h(J_k)\})$

On pose alors $a_{k+1} = \text{Sup } (t_r, m_k)$ et $b_{k+1} = N_r + t_r$. Par construction,

$\text{Sup } J_k < \text{Inf } J_{k+1}$, $\text{Sup } h(J_k) < \text{Inf } h(J_{k+1})$, $\ell(J_{k+1}) \geq N_r (1 - \frac{\delta}{2})$

donc $\ell(J_k) \underset{k\to\infty}{\longrightarrow} +\infty$. Enfin, le nombre de composantes connexes de longueur L de $h(J_{k+1})$ est au moins $\delta N_r - m_k \geq \alpha N_r \geq \alpha\ell(J_{k+1})$. ∎

On se donne maintenant un réel $d \in]0,1[$. Il s'agit de construire $A \subset \mathbb{N}$ de densité uniforme d et telle que $h^{-1}(A)$ n'ait pas pour densité uniforme d. Par complémentarité, on peut supposer $d \geq \frac{1}{2}$.

E_1 désigne la réunion des composantes connexes de longueur L de tous les ensembles $h(J_k)$, chacune étant complétée par l'entier suivant immédiatement.

E_2 désigne la réunion des composantes connexes de longueur différente de L de tous les ensembles $h(J_k)$.

Enfin, $E_3 = \mathbb{N} \setminus (E_1 \cup E_2)$.

Dans la suite, on suppose E_2 et E_3 infinis, les autres cas se traitant de la même façon.

On désigne par B une partie arbitraire de $\mathbb{N}$ de densité uniforme d et B' une partie de $\mathbb{N}$ de densité uniforme $\frac{(L+1)d-1}{L}$ (≥ 0 card $\geq \frac{1}{2}$)

ϕ_1 désigne la bijection croissante de B' sur l'ensemble E_1, réunion des composantes de longueur L de tous les $h(J_k)$.

On pose alors $A = (E_1 \setminus E_1^*) \cup \phi_1(B') \cup \phi_2(B) \cup \phi_3(B)$.

D'une part, $\text{Card}\,(h^{-1}(A) \cap J_k) = \text{Card}\, A \cap h(J_k)$

$= \text{Card}\,(A \cap h(J_k) \cap E_1^*) + \text{Card}\,(A \cap h(J_k) \cap E_2)$.

$\text{Card}\,(A \cap h(J_k) \cap E_2) \underset{k\to\infty}{\sim} d\ \text{Card}\, E_2 \cap h(J_k)$ et

$\text{Card}\,(A \cap h(J_k) \cap E_1^*) \underset{k\to\infty}{\sim} \frac{d(L+1)-1}{L}\ \text{Card}\,(h(J_k) \cap E_1^*)$

donc $\limsup_k \frac{\text{Card}\,(A \cap h(J_k))}{\ell(J_k)} \leqslant d(1-\alpha) + \alpha\,\frac{(L+1)d-1}{L} < d$.

D'autre part, A a pour densité uniforme d. En effet :

$\text{Card}\,(A \cap [t, N+t[) = \text{Card}(\phi_2(B) \cap [t, n+t[) + \text{Card}\,(\phi_3(B) \cap [t, N+t[)$.

$+ \text{Card}\,(((E_1 \setminus E_1^*) \cup \phi_1(B')) \cap [t, N+t[)$

Etant donné $\varepsilon > 0$, il existe $M \in \mathbb{N}$ tel que, pour tout intervalle I, $\ell(I) > M \Rightarrow |\text{Card}\,(B \cap I) - d\ell(I)| \leqslant \varepsilon\ell(I)$.

Ainsi, pour tout intervalle I, $|\text{Card}\,(B \cap I) - d\ell(I)| \leqslant \varepsilon\ell(I) + M$; ce qui donne, pour r = 2 ou 3,

$|\text{Card}\,(\phi_r(B) \cap [t, N+t[) - d\ \text{Card}\,(E_r \cap [t, N+t[)|$

$= |\text{Card}\,(B \cap \phi_r^{-1}([t, N+t[)) - d\ \text{Card}\,\phi_r^{-1}([t, N+t[)|$

$M + \varepsilon\ \text{Card}\,\phi_r^{-1}([t, N+t[) = M + \varepsilon\ \text{Card}\,(E_r \cap [t, N+t[)$.

De même, il existe $M' \in \mathbb{N}$ tel que

$|\text{Card}\,(\phi_1(B') \cap [t, N+t[) - \frac{(L+1)d-1}{L}\ \text{Card}\,(E_1 \cap [t, N+t[)|$

$\leqslant M' + \varepsilon\ \text{Card}\,(E_1^* \cap [t, N+t[)$ de sorte que :

$\left|\text{Card}\,(\phi_1(B') \cap [t, N+t[) - \frac{(L+1)d-1}{L+1}\ \text{Card}\,(E_1 \cap [t, N+t[)\right|$

$\leqslant M' + \varepsilon\ \text{Card}\,(E^* \cap [t, N+t[) + \left|\text{Card}\,(E_1^* \cap [t, N+t[) - \frac{L}{L+1}\ \text{Card}\,(E_1 \cap [t, N+t[)\right|$

$\leqslant M' + 2 + \varepsilon\ \text{Card}\,(E_1^* \cap [t, N+t[)$.

Comme $|\text{Card}\,((E_1 \setminus E_1) \cap [t, N+t[) - \frac{1}{L+1}\ \text{Card}\,(E_1 \cap [t, N+t[)| \leqslant 2$,

on obtient finalement :

$$|\mathrm{Card}(A \cap [t\ ,\ N+t[) - dN\ | \leqslant\ 2M + M' + 4\varepsilon N$$

pour N assez grand de sorte que A a bien pour densité uniforme d .

III. PREUVE DU THEOREME 2.

Par des arguments semblables à ceux du II, on se ramène à construire une partie A de $\mathbb{N}$ de densité $\frac{1}{2}$ telle que $h^{-1}(A)$ n'ait pas pour densité $\frac{1}{2}$.

III.1. Lemme 3. *Il existe* $\beta > 0$ *et une suite croissante d'entiers* (N_k) *tels que pour tout* $k \in \mathbb{N}^*$, *il existe une partie* Q_k *de* $\bar{H}(N_{k+1}) \setminus (H(N_{k+1}) \cup \bar{H}(N_k))$ *et une injection* $\psi_k : Q_k \to H(N_{k+1}) \setminus \bar{H}(N_k)$ *vérifiant :* $\mathrm{Card}\ Q_k \geq \frac{1}{2}\ \beta N_{k+1}$ *et, pour tout entier* $t \geq \mathrm{Sup}\ \bar{H}(N_k)$, $|\mathrm{Card}(Q_k \cap [0,t[) - \mathrm{Card}(\psi_k(Q_k) \cap [0,t[)| \leqslant \frac{2t}{k}$

Preuve : on suppose que $N_1, \ldots N_k$ ont été déterminés, N_1 arbitraire. On pose $M_k = \mathrm{Sup}\ H(N_k) = \mathrm{Sup}\ \bar{H}(N_k)$. D'après l'hypothèse du théorème 2, il existe un entier N_{k+1} vérifiant les conditions :

- $M_k \leqslant \frac{\beta}{4} N_{k+1}$
- il existe une partie $P(N_{k+1})$ de $\bar{H}(N_{k+1}) \setminus H(N_{k+1})$ et une injection $\phi'_k : P(N_{k+1}) \to H(N_{k+1})$ telles que :

$$\mathrm{Card}\ P(N_{k+1}) \geq \beta N_{k+1} \text{ et pour tout } n \in P(N_{k+1}),\ |n - \phi'_k(n)| \leqslant \frac{n}{k+1}$$

On choisit alors $Q_k = P(N_{k+1}) \setminus [0,2\ M_k[$ et ψ_k désigne la restriction de ϕ'_k à Q_k.

D'une part, $\mathrm{Card}\ Q_k \geq \mathrm{Card}\ P(N_{k+1}) - 2M_k \geq \frac{\beta}{2} N_{k+1}$.

D'autre part, $Q_k \cap \bar{H}(N_k) = \emptyset$ et $\psi_k(Q_k) \cap \bar{H}(N_k) = \emptyset$, la dernière condition résultant du fait que si $n \in Q_k$, $\phi'_k(n) \geq (1 - \frac{1}{k+1})\ n \geq M_k$.

Enfin, on a la majoration suivante :

$$|\mathrm{Card}\ (Q_k \cap [0,t[) - \mathrm{Card}(\psi_k(Q_k) \cap [0,t[|$$

$$\leqslant \mathrm{Card}\ \{n \in Q_k\ ;\ n < t,\ \phi'_k(n) \geq t\} + \mathrm{Card}\ \{n \in Q_k\ ;\ n \geq t,\ \phi'_k(n) < t\}$$

$$\leqslant \frac{t}{k+2} + \frac{t}{k} < \frac{2t}{k}\ .$$ Le lemme 3 est démontré.

III.2. Fin de la preuve du théorème 2

Avec les notations du lemme 3, on pose $\mathcal{C} = \bigcup_{k=1}^{\infty} Q_k$ et $\mathcal{S} = \bigcup_{k=1}^{\infty} \psi_k(Q_k)$

D'après le lemme 3,

$$|\mathrm{Card}(\mathcal{C} \cap [0,N[) - \mathrm{Card}(\mathcal{S} \cap [0,N[| = o(N) \text{ lorsque } N \text{ tend vers l'infini.}$$

D'autre part,

$$\mathrm{Card}(\mathcal{S} \cap H(N_{k+1})) - \mathrm{Card}(\mathcal{C} \cap H(N_{k+1}))$$

$$\geq \mathrm{Card}\ \psi_k(Q_k) - \mathrm{Card}\ \bar{H}(N_k) \geq \mathrm{Card}\ Q_k - M_k \geq \frac{\beta}{4} N_{k+1},$$

de sorte que :

$$\mathrm{Card}([0, N_{k+1}[\cap h^{-1}(\mathcal{S})) - \mathrm{Card}([0,N_{k+1}[\cap h^{-1}(\mathcal{C})) \geq \frac{\beta}{4} N_{k+1}.$$

$\mathcal{C}$ et $\mathcal{S}$ étant disjoints, $\mathrm{Card}(\mathcal{C} \cap [0,N[) + \mathrm{Card}(\mathcal{S} \cap [0,N[) \leq N$.

Ainsi $\mathrm{Card}\ \mathcal{C} \cap [0,N[\leq \frac{N}{2} + o(N)$ et

$$\mathrm{Card}\ \mathcal{S} \cap [0,N[\leq \frac{N}{2} + o(N).$$

Donc il existe une partie B de $\mathbb{N}$ de densité $\frac{1}{2}$ vérifiant :

$$B \supset \mathcal{C} \qquad \text{et} \qquad B \cap \mathcal{S} = \emptyset$$

Si $h^{-1}(B)$ n'a pas pour densité $\frac{1}{2}$, on pose A = B.

Si $h^{-1}(B)$ a pour densité $\frac{1}{2}$, on pose $A = (B \setminus \mathcal{C}) \cup \mathcal{S}$, de sorte que A a pour densité $\frac{1}{2}$ comme B et que :

$$\mathrm{Card}(h^{-1}(A) \cap [0,N_{k+1}[) - \mathrm{Card}(h^{-1}(B) \cap [0,N_{k+1}[) \geq \frac{\beta}{4} N_{k+1}.$$

IV. REMARQUES

IV.1. *Les permutations c.r.s. ne forment pas un groupe, les permutations c.r.u.s. non plus.*

Par exemple, on pose h(0) = 0, h(1) = 1 et pour $K \geq 1$,

$$h(n) = \begin{cases} 2^K + \dfrac{n-2^K}{2} & \text{si } n \text{ pair, } n \in [2^K,\ 2^{K+1}[\\ 2^K + 2^{K-1} + \dfrac{n-1-2^K}{2} & \text{si } n \text{ impair, } n \in [2^K,\ 2^{K+1}[\end{cases}$$

h est c.r.s. et c.r.u.s. alors que h^{-1} n'est ni c.r.s. ni c.r.u.s.

IV.2. *Il n'existe aucune permutation* h *de* $\mathbb{N}$ *transformant toute suite équirépartie* u *dans* $\mathbb{R}/\mathbb{Z}$ *en une suite* uoh *uniformément équirépartie.*

D'après ce qu'on a vu au II, h serait telle que pour toute A de $\mathbb{N}$ de densité d, $h^{-1}(A)$ ait pour densité uniforme d.

Soit A une partie de densité d, on suppose que $h^{-1}(A)$ a pour densité uniforme d. Comme $h(n) \xrightarrow[n\to\infty]{} \infty$, on peut construire par récurrence une suite d'intervalles disjoints $F_k = [N_k,\ N_k + k[$ tels que $\bigcup_{k=1}^{\infty} h(F_k)$ ait pour densité 0. Il suffit de choisir F_{k+1} tel que :

$$N_{k+1} > kN_k \quad \text{et} \quad \operatorname{Inf} h(F_{k+1}) > k \operatorname{Sup} h(F_k).$$

Alors $B = A \bigcup_{k=1}^{\infty} h(F_k)$ a pour densité d alors que $h^{-1}(B) \cap F_k$ est vide.

IV.3. *Les permutations* h *transformant la* μ*-répartition uniforme en* μ*-répartition sont celles pour lesquelles le nombre de composantes connexes de* $h([0,N[)$ *est un* $o(N)$.

Il existe de telles permutations h qui ne sont pas c.r.u.s.. On peut choisir par exemple $h(n) = n$ si $n < 16$ et pour $K \geq 2$,

$$h(n) = \begin{cases} n \text{ si } n \in [4^K + 2^{K+1},\ 4^{K+1}[\\ 4^K + 2(n-4^K) \text{ si } n \in [4^K,\ 4^K + 2^K[\\ 4^K + 2(n-4^K-2^K) + 1 \text{ si } n \in [4^K+2^K,\ 4^K+2^{K+1}[\end{cases}$$

Il en existe également qui ne sont pas c.r.s.. On peut choisir par $h(n) = n$ si $n < 2$ et pour $K \geq 2$

$$h(n) = \begin{cases} n + (K+1)! - 2K! & \text{si } n \in \left[K!\ 2K!\right[\\ n - K! & \text{si } n \in \left[2K!,\ (K+1)!\right[\end{cases}$$

En combinant ces idées, on peut construire une permutation h qui n'est ni c.r.s. ni c.r.u.s. mais qui transforme toute suite uniformément μ-répartie en une suite μ-répartie.

IV.4 *Les permutations envisagées par RINDLER dans [8] sont c.r.s. mais pas forcément c.r.u.s.*

IV.5. Soit $u : \mathbb{N} \to X$ complètement μ-répartie ([6], [8]), la suite $u^* : n \rightsquigarrow (u(n), u(n+1), \ldots, u(n+k), \ldots)$ à termes dans $X^{\mathbb{N}}$ est répartie selon la mesure-produit $\hat{\mu}_\infty$ induite par μ. Si h est une permutation c.r.s., $u^* oh$ est μ-répartie également donc uoh est complètement μ-répartie.

Ainsi toute permutation c.r.s. conserve la complète répartition des suites.

V. PERMUTATIONS BINAIRES

V.1. On envisage les permutations h_θ définies de la manière suivante : si θ est une permutation de $\mathbb{N}$ et si $n = \sum_{r=o}^{\infty} e_r(n)2^r$, $e_r(n) \in \{0,1\}$, est le développement binaire de n, on pose :

$$h_\theta(n) = \sum_{r=o}^{\infty} e_r(n)2^{\theta(r)}$$

THEOREME 3. *1) Toute permutation* h_θ *est c.r.u.s.*

2) h_θ *est c.r.s. si et seulement si* θ *-id est bornée (id désigne bien sûr l'identité de* $\mathbb{N}$*).*

Remarque : *les permutations* h_θ *qui sont c.r.s. forment un groupe.*

V.2. Preuve du 1)

Etant donné $\varepsilon > 0$, on choisit un entier K tel que $2^{-K} \leqslant \varepsilon$ puis un entier L tel que $[0, K[\subset \theta([0,L[)$ et enfin un entier N tel que $2^L \leqslant \varepsilon N$.

On pose $a = \inf \{i \in \mathbb{N} ; t \leqslant i2^L\}$ et $b = \operatorname{Max} \{i \in \mathbb{N} ; i2^L \leqslant N+t\}$.

$$h_\theta([t, N+t[) = h_\theta([t, a2^L[) \cup h_\theta([b2^L, N+t[) \cup \left(\bigcup_{a \leqslant i < b} h_\theta([i2^L, (i+1)2^L[) \right)$$

Par construction, chaque composante de $h_\theta([i2^L, (i+1)2^L[)$ a une longueur au moins égale à 2^K. Donc le nombre total de composantes connexes de $h_\theta([t,N+t[)$ est majoré par $N.2^{-K} + 2^{L+1} \leqslant 3\varepsilon N$. On conclut par le théorème 1.

V.3. Preuve du 2) ; condition nécessaire

On choisit K assez grand pour que $0 \in \theta([0,K[)$ et on écrit

$\theta([0,K[) = [a_1, a_1 + \ell_1[\cup [a_1, a_2 + \ell_2[\cup \ldots \cup [a_q, a_q + \ell_q[$ avec $a_1 = 0$, $\ell_j > 0$ et $a_{j+1} > a_j + \ell_j$

Si θ - id n'est pas majorée, $a_q + \ell_q - K$ n'est pas majorée.

Si θ - id n'est pas minorée, $K - \ell_1$ n'est pas majorée.

Donc si θ - id n'est pas bornée, $a_q + \ell_q - \ell_1$ n'est pas majorée.

Les composantes connexes de $h_\theta([0,2^K[)$ sont de la forme

$C = C(k_q, \ldots, k_2) = \left[\sum_{j=2}^{q} k_j 2^{a_j}, \sum_{j=2}^{q} k_j 2^{a_j} + 2^{\ell_1} \right[$ où pour tout $j \in \{2,..,q\}$, $k_j < 2^{\ell_j}$. Leur longueur commune est 2^{ℓ_j}.

Dans l'énoncé du théorème 2, on choisit $\beta = \frac{1}{2}$. Etant donné $\alpha > 0$ arbitraire, on choisit m entier assez grand pour que $\alpha(2^m - 1) > 1$.

On choisit ensuite K de manière que $a_q + \ell_q > \ell_1 + m$ (il existe une infinité de telles valeurs de K). Conformément aux notations du théorème 2, on choisit la partie $P([0,2^K[)$ de $\bar{H}([0,2^K[) \setminus H([0,2^K[)$ de la manière suivante :

$$P([0,2^K[) = \bigcup_{k_2,\ldots k_{q-1}} \left(\bigcup_{2^{\ell_q - 1} \leq k_q < 2^{\ell_q}} \left[\sum_{j=2}^{q} k_j 2^{a_j} - 2^{\ell_1}, \sum_{j=2}^{q} k_j 2^{a_j} \right[\right)$$

où $k_j < 2^{\ell_j}$ pour $j < q$ et on pose $\phi(n) = n + 2^{\ell_1}$.

ϕ est une injection dont l'image est la réunion des composantes $C(k_q,\ldots, k_2)$ avec $2^{\ell_q - 1} \leq k_q < 2^{\ell_q}$. La somme des longueurs de ces composantes est 2^{K-1} car la moitié des valeurs possibles de k_q sont permises. On a bien $\beta = \frac{1}{2}$. D'autre part :

$$\phi(n) - n = 2^{\ell_1} < \alpha(2^{\ell_1 + m} - 2^{\ell_1})$$
$$\leq \alpha(2^{a_q} 2^{\ell_q - 1} - 2^{\ell_1}) \leq \alpha(2^{a_q} k_q - 2^{\ell_1}) \leq \alpha n.$$

La condition du théorème 2 est remplie, h_θ n'est pas c.r.s.

V.4. Preuve du 2) ; condition suffisante

On suppose θ-id bornée. Il existe $B > 0$ tel que

$$t - B \leq \theta(t) \leq t + B \quad \text{pour tout } t \in \mathbb{N}$$

A désigne un ensemble de densité d. On écrit tout entier N sous la forme $N = 2^{s_o} + 2^{s_1} + \ldots + 2^{s_k}$ avec $s_o > s_1 > \ldots > s_k$.

On pose $\ell_r = \text{Max}\,\{j \in \mathbb{N} ;\ [0, j[\cap \theta([0, s_r[) \text{ de sorte que } \ell_r \geq s_r - B$.

D'une part $h_\theta([0,N[) \subset h_\theta([0,2^{s_o+1}[) \subset [0,2^{s_o+B+1}[$

D'autre part, les composantes connexes de $h_\theta([0,2^{s_o}[)$ ont pour longueur 2^{ℓ_o} et celles de $h_\theta([2^{s_o}+\ldots+2^{s_{r-1}}, 2^{s_o}+\ldots+2^{s_{r-1}}+2^{s_r}[)$ ont pour longueur 2^{ℓ_r}.

Etant donné $\varepsilon > 0$, on choisit un entier ω tel que $2^{-\omega} \leqslant \varepsilon$, puis un entier M tel que, pour tout $m \geqslant 2^M$,

$$|\mathrm{Card}(A \cap [0,m[) - dm| \leqslant \varepsilon 2^{-\omega} m .$$

On pose enfin $\rho = \mathrm{Max}\{r;\ s_o - s_r \leqslant \omega\}$. Alors,

$$\mathrm{Card}(A \cap h_\theta([2^{s_o}+\ldots+2^{s_\rho}, N[)) \leqslant 2^{1+s_{\rho+1}} \leqslant N.2^{-\omega} \leqslant \varepsilon N .$$

Et toute composante connexe C de $h_\theta([0\ ,\ 2^{s_o}+\ldots+2^{s_\rho}[)$ a une longueur minorée par $2^{\ell_\rho} \geqslant 2^{s_\rho - B} \geqslant 2^{s_o - B - \omega}$. Si on choisit N assez grand pour que $s_o - B - \omega \geqslant M$,

$$|\mathrm{Card}(A \cap C) - d\,\mathrm{Card}\,C| \leqslant \varepsilon 2^{-\omega}(\mathrm{Inf}\,C + \mathrm{Sup}\,C) \leqslant \varepsilon 2^{-\omega}\, 2^{s_o + B + 2} \leqslant \varepsilon 4^{B+1}\, \ell(C) .$$

On obtient finalement

$$|\mathrm{Card}(A \cap h_\theta([0,N[)) - dN| \leqslant (4^{B+1} + 2)\varepsilon N .$$

$h_\theta^{-1}(A)$ a pour densité d , donc h_θ est c.r.s..

VI. LIEN AVEC L'INDEPENDANCE STATISTIQUE

Deux suites $u_1 : \mathbb{N} \to X_1$ et $u_2 : \mathbb{N} \to X_2$ à valeurs dans des espaces métriques compacts sont dites <u>statistiquement indépendantes</u> [6] (on note $u_1 \perp u_2$) si pour toutes $f_1 : X_1 \to \mathbb{C}$ et $f_2 : X_2 \to \mathbb{C}$ continues,

$$0 = \lim_{N\to\infty} \left(\frac{1}{N} \sum_{n<N} f_1(u_1(n))\, f_2(u_2(n)) - \left(\frac{1}{N} \sum_{n<N} f_1(u_1(n))\right) \left(\frac{1}{N} \sum_{n<N} f_2(u_2(n))\right)\right).$$

On dit qu'une permutation h de $\mathbb{N}$ <u>conserve l'indépendance statistique</u> (h est c.i.s.) si quelles que soient les suites u_1 et u_2 à valeurs dans des espaces métriques compacts :

$$u_1 \perp u_2 \Rightarrow u_1 \circ h \perp u_2 \circ h .$$

Est-il vrai que les permutations c.r.s. et c.i.s. coïncident ?

BIBLIOGRAPHIE

[1] BAAYEN P.C. - HEDRLIN Z.:The existence of well-distributed sequences in compact spaces. Indag. Math. 27 (1965),221-228 .

[2] COQUET J.: Sur certaines suites uniformément équiréparties modulo 1. Acta Arithmetica 36 (1980),157-162 .

Conservation de l'équirépartition. Primaths 4,Marseille, 1981 .

[3] COUOT J.: Théorie ergodique de l'équirépartition. Lecture Notes in Math.475 (1974), 26-88 .

[4] KUIPERS L. - NIEDERREITER H.: Uniform distribution of sequences. Wiley Interscience, New York, 1974 .

[5] RAUZY G.: Equirépartition et entropie. Lecture Notes in Math. 475 (1974),155-175 .

[6] RAUZY G.: Propriétés statistiques de suites arithmétiques. P.U.F., Collection Sup le Mathématicien, 1976 .

[7] RINDLER H.: Fast Konstante Folgen. Acta Arithmetica 35 (1979),189-193 .

[8] RINDLER H.: Eine Charakterisierung gleichverteilter Folgen. Archiv der Math. 32 (1979), 185-188 .

*

* *

Jean COQUET
Département de Mathématique
Université de Valenciennes
Le Mont-Houy
59326 Valenciennes Cedex

APPLICATION DES MEILLEURES APPROXIMATIONS AU CALCUL D'UNITÉS

par

E. DUBOIS (Caen)

Les meilleures approximations (M.A.) ontsurtout été étudiées pour leurs propriétés d'approximations diophantiennes. Depuis quelques années, avec le développement de l'informatique, des méthodes de calcul de certaines M.A. ont été mises au point. A cette fin on a le plus souvent modifié la définition usuelle de M.A. Ceci conduit à diverses notions. Nous considérerons ici le cas de M.A. de zéro par une forme linéaire à trois variables, relativement à deux autres formes linéaires. Nous en déduirons, en utilisant quelques résultats de Voronoi [4 et 8], une méthode de calcul d'un système fondamental d'unités d'un corps cubique totalement réel.

I. Rappel des cas connus

I.1 - Si θ est un nombre réel on dit que (p,q) est une M.A. de θ si

$$|q'\theta-p'| < |q\theta-p| \Rightarrow |q'| > q > 0$$

On sait que les M.A. de θ sont les réduites (sauf peut être la première) du développement en fraction continue de θ. Si on remplace la condition $|q'| > q$ par $F(p',q') > F(p,q)$ où F est une fonction distance "raisonnable" on sait [5b] que cette propriété reste vraie au moins à partir d'un certain rang.

L'application au calcul d'unité est bien connue. On a :

Théorème I.1 - Le développement de θ en fraction continue conduit à l'unité fondamentale de l'anneau $\mathbb{Z}[\theta]$.

Pour tout corps quadratique réel il suffit alors de considérer θ tel que $1,\theta$ soit une base d'entiers pour obtenir l'unité fondamentale du corps.

I.2 - Dans le cas de 2 nombres réels v,w tels que $1,v,w$ soit une base d'entiers d'un corps cubique à conjugués complexes on définit la notion de M.A. suivante :

Définition .- $P = (p_o, p_1, p_2)$ dans $\mathbb{Z}^3$ est une F_c-M.A. de zéro par la forme linéaire $L(P) = p_o + p_1 v + p_2 w$, relativement à la forme quadratique $F_c(P) = N(L(P)) / L(P) = |L'(P)|^2$ (en notant $L'(P)$ un conjugué de $L(P)$) si et seulement si

$$\forall Q \in \mathbb{Z}^3, \qquad 0 < L(Q) < L(P) \leqslant 1 \Rightarrow F_c(Q) > F_c(P).$$

On sait calculer la suite des F_c-M.A. et on a :

Théorème [5] .- Soit $(P_n)_{n\geqslant 0}$ la suite des F_c-M.A. d'une base d'entiers d'un corps cubique à conjugués complexes. La première unité rencontrée dans la suite $(L(P_n))_{n>0}$ est l'unité fondamentale du corps.

II. Cas d'un corps cubique totalement réel

II.1 - Soient $1, v, w$ une base d'entiers d'un tel corps ; v', v'' (resp. w', w'') les conjugués de v (resp. w). Pour $P = (p_o, p_1, p_2)$ dans $\mathbb{Z}^3$ notons

$$L(P) = p_o + p_1 v + p_2 w$$

et $L_1(P)$, $L_2(P)$ les conjugués de $L(P)$.

Définition .- Nous dirons que le point P est extremal si et seulement si la région

$$\{Q \in \mathbb{Z}^3 / \ 0 < |L(Q)| < L(P) , \quad |L_1(Q)| < |L_1(P)|, \quad |L_2(Q)| < |L_2(P)|\}$$

est vide.

Il est évident que toute unité $L(P)$ correspond à un point P extremal. On doit donc rechercher un système fondamental d'unités (le groupe est ici de rang 2) parmi ces points extremaux.

Nous allons donner un méthode de calcul de certaines suites de points extremaux et en utilisant des résultats de Voronoi nous en déduirons une méthode pour déterminer un système fondamental d'unités.

Indépendamment J. BUCHMANN [3] a aussi mis un point des méthodes de calculs donnant des résultats similaires.

II.2 - Suite de MA_i

Définition .- Nous dirons que (T_n) est une suite de MA_i de zéro pour la forme linéaire L_i relativement à L_j, L_k ($\{i,j,k\} = \{0,1,2\}$) si et seulement si

$$T_o \text{ est un point extrémal, } L_i(T_o) > 0$$

et si pour tout $n \geqslant 0$

$$L_i(T_{n+1}) = \text{Min } \{|L_i(Q)| \ ; \ Q \in \mathbb{Z}^3, \ |L_j(Q)| < |L_j(T_n)|, \ |L_k(Q)| < |L_k(T_n)|\}$$

Il est clair que T_o étant donné, la suite $(T_n)_{n\geqslant 0}$ est bien définie et que pout tout n, T_n est un point extremal. Sans restreindre la généralité nous supposerons que $(i,j,k) = (0,1,2)$ et que $T_o = (1,0,0)$. On a :

Théorème .- Si $(T_n)_{n\geqslant 0}$ est une suite de MA_o alors pour tout $n \geqslant 0$ il existe un point auxiliaire R_n tel que (T_n, R_n, T_{n+1}) soit une base de $\mathbb{Z}^3$.

Preuve : Toute MA_o est un point extremal et donc deux MA_o consécutives T_n, T_{n+1}, sont linéairement indépendantes. (On trouve facilement des exemples où trois MA_o consécutives T_{n-1}, T_n, T_{n+1} sont linéairement dépendantes).

Pour tout point entier Q', notons $d(Q') = \det(T_n, Q', T_{n+1})$. Soit Q un point tel que

$$d(Q) = \text{Min } \{d(Q') \ ; \ Q' \text{ entier}, \ d(Q') > 0\}$$

Nous voulons montrer que $d(Q) = 1$. Sinon soit d un diviseur premier de $d(Q)$ et considérons les points

$$P = \frac{1}{d}(\ell_o T_n + \ell_1 Q + \ell_2 T_{n+1})$$

P est entier si et seulement si (ℓ_o, ℓ_1, ℓ_2) satisfont un système linéaire de congruences modulo d. Or le déterminant $d(Q)$ de ce système est divisible par d. Il admet donc une solution entière non triviale (ℓ_o, ℓ_1, ℓ_2) vérifiant $|\ell_i| \leqslant \frac{d}{2}$.

Si $\ell_1 = 0$ on a $|L_o(P)| < L_o(T_{n+1})$ et pour $j = 1,2$ $|L_j(P)| < |L_j(T_n)|$ car $L_o(T) < L_o(T_{n+1})$ et $|L_j(T_{n+1})| < |L_j(T_n)|$. Ceci est contradictoire avec la définition de T_{n+1}.

Si $\ell_1 \neq 0$ on a $0 < |d(P)| < d(Q)$ ce qui contradictoire avec le choix de Q et termine la preuve.

II.3 - Méthode de calcul d'une suite de MA_o

Nous notons (Q,R,T) la base (T_{n-1},R_{n-1},T_n). Au départ on prend

$$T_{-1} = (0,0,1), \quad R_{-1} = (0,1,0), \quad T_o = (1,0,0)$$

II.3.1 - La première étape consiste à trouver un point entier S dans la région

$$|L_\ell(S)| < |L_\ell(T)| \qquad \ell = 1,2$$

En cherchant S sous la forme $iQ + jR + kT$ ceci revient à déterminer une solution entière (i,j,k) du système

$$|ia_\ell + jb_\ell + k| < 1 \quad (\ell = 1,2)$$

où $a_\ell = L_\ell(Q) / L_\ell(T)$, $b_\ell = L_\ell(R) / L_\ell(T)$.

Notons $A = (a_1,a_2)$, $B = (b_1,b_2)$, $D = (-1,1)$ et $X.Y$ le produit scalaire dans $\mathbb{R}^2$. On remplace (A,B) par $(A_1,B_1) = (\lambda A+B, A)$, λ étant l'entier le plus proche de $-(B.D) / (A.D)$. On a alors $|A_1.D| < \frac{1}{2} |A.D|$. Et on continue le procédé jusqu'à $|A_n.D| < 1$. Si $A_n = (x,y) = iA + jB$ on a $|x-y| < 1$. On choisit alors pour k un entier tel que $|x+k| < 1$ et $|y+k| < 1$. (i,j,k) est alors une solution du système.

II.3.2 - La deuxième étape consiste à décrire l'ensemble des points entiers P, que l'on exprime sous la forme $iQ + jR + kT$, vérifiant :

$$0 < L_o(P) < |L_o(S)|$$

$$|L_\ell(P)| < |L_\ell(T)| \quad (\ell = 1,2)$$

Chaque point P considéré en cours de calcul est rangé dans S. La borne $L_o(S)$ s'améliore donc à chaque fois. Le dernier point S sera la MA_o suivante (T_{n+1}).

Ce système s'écrit en utilisant les notations de II.3.1 pour a_ℓ et b_ℓ :

$$|ia_o + jb_o + k| < c_o$$

$$|ia_\ell + jb_\ell + k| < 1 \qquad \ell = 1,2$$

où $(a_o,b_o,c_o) = \frac{1}{L_o(T)} (L_o(Q), L_o(R), |L_o(S)|)$.

Plusieurs méthodes sont possibles. La plus simple à programmer consiste à calculer les composantes des sommets du parallélépipède. On obtient des bornes pour i,j,k. Précisément on a :

$$|i| \leqslant i_M = \left[\frac{c_o|b_1-b_2| + |b_2-b_o| + |b_o-b_1|}{|a_o(b_1-b_2)+a_1(b_2-b_o)+a_2(b_o-b_1|} \right]$$

et des expressions similaires pour les majorants j_M, k_M de (j) et (k). Chaque amélioration de S, donc de c_o, a une influence simple sur i_M, j_M, k_M. Pour chaque triplet (i,j,k) vérifiant $|i| \leqslant i_M$, $|j| \leqslant j_M$, $|k| \leqslant k_M$ on doit tester si le système est satisfait. On conserve dans S le meilleur point.

II.3.3 - La troisième étape consiste à compléter $T = T_n$, $S = T_{n+1}$ en une base.

En écrivant :

$$\begin{pmatrix} T \\ \cdot \\ S \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ \cdot & \cdot & \cdot \\ i & j & k \end{pmatrix} \begin{pmatrix} Q \\ R \\ T \end{pmatrix}$$

il suffit de déterminer i', j' tels que $(i'j - ij') = 1$. Le point $R' = i'Q + j'R$ convient.

II.3.4 - Précision des calculs

Le passage d'un rang n au suivant nécessite le calcul de

$$L_\ell(R'), L_\ell(S) \qquad \ell = 0,1,2.$$

Il est dangereux de les calculer en fonction de l'étape précédente (i.e $L_\ell(S) = iL_\ell(Q) + jL_\ell(R) + kL_\ell(T)$) car les erreurs d'arrondi risquent de se cumuler. Il est préférable de les calculer directement en fonction des données (i.e $L_o(S) = s_o + s_1v + s_2w$ si $s = (s_o,s_1,s_2)$ ...).

Lorsque $n \to \infty$, Max $|s_i| \to \infty$, $L_1(S) \to 0$ et $L_2(S) \to 0$. Pour calculer $L_1(S)$ et $L_2(S)$ il est donc nécessaire d'avoir v', w', v'', w'' avec une grande précision. Ce sont ces conditions qui assurent la validité des calculs.

Si on avait besoin de pousser un calcul on peut tourner cette difficulté en déterminant, par un calcul en entier et en multiprécision, l'équation vérifiée par $L_\ell(S)$ ($\ell = 0,1$ ou 2 donne la même équation).

III. Système fondamental

III.1 - L'idée de chercher un système fondamental d'unités parmi les suites MA_o, MA_1 ou MA_2 vient de l'espoir que la suite MA_o partant de 1 contienne la plus petite unité ε_o, positive vérifiant $|\varepsilon_o'| < 1$ et $|\varepsilon_o''| < 1$, ce qui est faux, et du résultat suivant.

Théorème .- Soit K un corps cubique totalement réel. Soient $\varepsilon_o, \varepsilon_1, \varepsilon_2$ les unités vérifiant :

$$\varepsilon_o > 0, \quad |\varepsilon_o'| < 1, \quad |\varepsilon_o''| < 1 \quad \text{et} \quad \varepsilon_o \quad \text{minimal}$$

$$|\varepsilon_1| < 1, \quad \varepsilon_1' > 0, \quad |\varepsilon_1''| < 1 \quad \text{et} \quad \varepsilon_1' \quad \text{minimal}$$

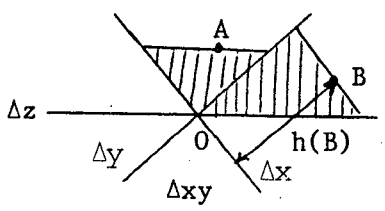
$$|\varepsilon_2| < 1, \quad |\varepsilon_2'| < 1 \quad \varepsilon_2'' > 0 \quad \text{et} \quad \varepsilon_2'' \quad \text{minimal}$$

Alors tout couple $(\varepsilon_i, \varepsilon_j)$ est un système fondamental d'unités.

Ce résultat est dû à Berwick [1]. Il est tombé dans l'oubli et a été redémontré, en autre, par Smadja [7, chap. 6]. Ma démonstration est basée sur le lemme suivant :

Lemme 1 .- Soit un réseau du plan $\mathbb{R}^2$. Considérons trois droites Δx, Δy, Δz concourantes en 0 et formant 2 à 2 des angles de 60 degrés. Pour toute permuation de x,y,z notons Δxy la région limitée par Δx et Δy et si $A \in \Delta xy$ notons $h(A)$ la distance à Δz.

Alors si $A \in \Delta xy$ avec $h(A)$ minimal, $B \in \Delta yz$ avec $h(B)$ minimal alors (A,B) est une base du réseau



L'hypothèse signifie que les régions hachurées ne contiennent aucun point du réseau. Pour montrer que (A,B) est une base du réseau il suffit de montrer que le parallélogramme construit sur OA et OB ne contient aucun point du réseau. Ce que l'on obtient en translatant de OA, OB ou de $OA + OB$ les régions hachurées ou leurs symétriques par rapport à O.

Le lien avec le théorème est la bijection

$$\varepsilon \longrightarrow (\log|\varepsilon|, \log|\varepsilon'|, \log|\varepsilon''|)$$

entre le groupe des unités et un réseau contenu dans un plan (car $|\varepsilon\varepsilon'\varepsilon''| = 1$).

Dans le même ordre d'idée on peut montrer avec les notations précédentes :

Lemme .- Si A et $C \in \Delta xy$ avec $h(A)$ minimal et C non multiple de A avec $h(C)$ minimal alors (A,C) est une base du réseau.

Théorème .- Soit K un corps cubique totalement réel ; ε,η des unités multiplicativement indépendantes vérifiant

$$|\varepsilon'| < 1, \quad |\varepsilon''| < 1, \quad \varepsilon > 0, \quad \varepsilon \text{ minimal}$$

$$|\eta'| < 1, \quad |\eta''| < 1, \quad \eta > \varepsilon, \quad \eta \text{ minimal}$$

alors (ε,η) est un système fondamental d'unités de K.

Pour pouvoir utiliser ce résultat il faudrait trouver une méthode de calcul de la suite des points extrémaux vérifiant $|L_\ell(P)| < 1$ pour $\ell = 1,2$ rangés par $L_o(P)$ croissant. Ce que nous ne savons pas encore faire de manière simple. La suite des MA_o peut oublier des points extrémaux. De même le théorème de Berwick ne peut s'appliquer car la suite des MA_o de 1 ne conduit pas nécessairement à ε_o. Nous avons des exemples où elle passe à côté. Il est peut être possible que la suite MA_o de 1 ne contienne aucune unité. Nous n'avons pas rencontré d'exemple.

III.2 - Périodicité des suites de MA

Soient P et une unité ε, notons $\varepsilon*P$ le point entier tel que $L(\varepsilon*P) = \varepsilon L(P)$.

Lemme .- Si T_n et T_{n+1} sont deux MA_o consécutives alors pour toute unité ε, $\varepsilon*T_n$ et $\varepsilon*T_{n+1}$ sont deux MA_o consécutives.

Il est clair que si T_n est un point extremal, $\varepsilon * T_n$ l'est aussi. D'autre part, s'il existe un point Q tel que

$$0 < L(Q) < \varepsilon L(T_{n+1}),\ |L_1(Q)| < |L_1(T_n)|,\ |L_2(Q)| < L_2(T_n)$$

alors le point $\varepsilon^{-1} * Q$ contredirait la définition de T_{n+1}.

Théorème .- Soit $(T_n)_{n \geqslant 0}$ une suite de MA_o (T_o quelconque). Notons $\alpha_n = L(T_n)$. Il existe k, n_o et une unité ε vérifiant $|\varepsilon'| < 1$, $|\varepsilon''| < 1$ tels que

$$T_{n+k} = \varepsilon * T_n \qquad n \geqslant n_o$$

On dira que la suite est périodique et que $T_{n+1}, \ldots, T_{n+k}$ est une période (n quelconque $\geqslant n_o$) modulo le facteur de multiplicité ε.

Preuve : D'après le théorème de Minkowski, il existe une constante C ne dépendant que du corps (si D est le discriminant du corps on peut prendre $C = \sqrt{D}$) telle que la région

$$\{P \mid |L_\ell(P)| < |L_\ell(T_n)| \quad \ell = 1,2, \quad |L(P)| < c / (L_1(T_n)\, L_2(T_n))\}$$

contienne au moins un point entier non nul. La norme des $L(P_n)$ est donc bornée par C. Or modulo les unités il n'y a qu'un nombre fini de classes d'entiers algébriques ayant la même norme. Il existe donc n_o, k et une unité ε tels que

$$T_{n_o+k} = \varepsilon * T_{n_o}$$

Le lemme montre par récurrence que cette relation reste vraie pour tout $n \geqslant n_o$.

Les éléments de la suite sont donc à partir d'un certain rang

$$\varepsilon^i * T_{n_o+1}, \ldots, \varepsilon^i * T_{n_o+k} \qquad i = 0,1,2\ldots$$

Ceci nous conduit à considérer la double suite "purement périodique"

$$\ldots \varepsilon^{-i} * T_{n_o+1}, \ldots, \varepsilon^{-i} * T_{n_o+k}, \ldots T_{n_o+1} \ldots T_{n_o+k} \ldots \varepsilon^i * T_{n_o+1}, \ldots, \varepsilon^i * T_{n_o+k} \ldots$$

Définition .- Une telle double suite est appelée 0-chaine (ou chaine de direction 0).

Toute suite extraite de cette double suite (donc tronquée à gauche) est une suite de MA_o.
On définit de même des 1-chaines et des 2-chaines à partir d'une période d'une suite de MA_1 ou de MA_2.

III.3 - Propriétés des chaines

- Lemme 1 : Deux chaines de même direction sont ou bien confondues ou bien n'ont aucun point en commun (c'est évident).

- Lemme 2 : Deux chaines de direction différente ont un point commun

- Lemme 3 : Si on multiplie (*) les éléments d'une chaine par une même unité, on obtient une chaine de même direction ayant le même facteur périodique.

- Lemme 4 : Si pour deux chaines (T_n) et (P_n) de même direction, il existe m et n et une unité η tel que $T_m = \eta * P_n$ alors elles se déduisent l'une de l'autre par multiplication (*) par η.

Les lemmes 3 et 4 sont évidents à partir du lemme de III.2.

Les chaines se comportent comme des droites parallèles de trois directions différentes. Comme Voronoi, on va en déduire un système fondamental d'unités.

III.4 - Méthode de détermination d'un système fondamental d'unités

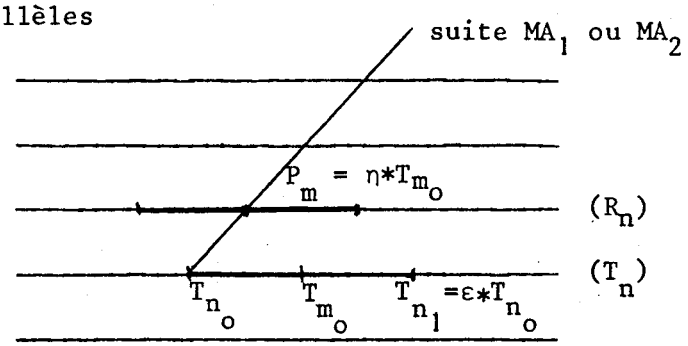
- On détermine une base d'entiers $1,v,w$ du corps considéré.

- On part de $T_o = (1,0,0)$. On calcule les termes T_n de la suite des MA_o jusqu'à ce qu'il existe n_o, n_1 $(1 \leqslant n_o \leqslant n_1)$ tels que $L(T_{n_1}) / L(T_{n_o})$ soit une unité disons ε. On prend n_1 minimal.

- Puis à partir de T_{n_o} on calcule les termes P_m de la suite de MA_1 (ou MA_2) jusqu'à ce qu'il existe m_o, $n_o \leqslant m_o < n_1$ tel que $L(P_m) / L(T_{m_o})$ soit une unité disons η.

Théorème .- ε,η ainsi construit est un système fondamental d'unités du corps.

On considère la O-chaine $\varepsilon^i * T_{n_o}, \ldots, \varepsilon^i * T_{n_1-1}$ et les O-chaines obtenues par multiplication par une unité δ quelconque. On obtient des O-chaines parallèles



Ces chaines sont ordonnées par l'intersection avec une 1-chaine quelconque, certaines sont au "dessus" de la O-chaine (T_n), d'autres sont au dessous. Si δ est une unité, les O-chaines obtenues par multiplication par δ et par δ^{-1} sont de part et d'autre de (T_n). Il suffit alors de considérer les O-chaines qui sont au-"dessus". Considérons la O-chaine (R_n) la plus proche de (T_n). Il existe η tel que (R_n) et (T_n) se déduisent par multiplication par η. Alors toutes les chaines considérées sont de la forme $(\eta^i * T_n)$ $i = 1,2,\ldots$ et toutes les unités sont de la forme $\delta = \eta^i \varepsilon^j$ $j \in \mathbb{Z}$, $i \geqslant 0$ (ou $\delta = \eta^{-i} \varepsilon^j$ correspondant aux O-chaines qui sont au-dessous de (T_n)). η ou $\eta\varepsilon^{j_o}$ pour un certain j_o, est caractérisé par le fait que m est le premier indice pour lequel P_m est congru modulo une unité, η ou $\eta\varepsilon^{j_o}$ à un élément de $T_{n_o}, \ldots, T_{n_1-1}$. $(L(P_m) / L(T_{m_o}) = \eta)$.

IV - Quelques exemples

Nous donnons l'équation définissant le corps sous la forme $X^3 - eX - d = 0$, le discriminant D. Nous notons θ la plus grande racine positive de l'équation et $\alpha = (\alpha_n)$ (resp. $\beta = (\beta_n)$, $\gamma = (\gamma_n)$) les suites MA_o (resp. MA_1, MA_2) de 1. Nous avons calculé ces trois suites et nous en déduisons des systèmes fondamentaux d'unités que nous exprimons en fonction de θ.
Nous donnons également les équations vérifiées par ces unités et les relations permettant de relier les différentes bases entre-elles.

IV.1 - Le corps défini par $X^3-7X-7 = 0$, de discriminant 49 est abélien (cela n'a aucune influence sur la méthode utilisée) et admet $1,\theta,\theta^2$ pour base d'entiers.

Les trois suites α,β,γ sont périodiques de longueur 1. $\alpha_1 = -4+2\theta+\theta^2$, $\beta_1 = -10+3\theta+2\theta^2$, $\gamma_1 = -4+\theta+\theta^2$. Ils sont conjugués et vérifient l'équation $X^3-2X^2-X+1 = 0$ et la relation $\alpha_1\beta_1\gamma_1 = 1$.

Les couples (α_1,β_1), (β_1,γ_1), (γ_1,α_1) sont des systèmes fondamentaux d'unités.

IV.2 - Le corps défini par $X^3-4X+2 = 0$, de discriminant 148 est non abélien et admet pour base d'entiers $1,\theta,\theta^2$. Les trois suites α,β,γ sont périodiques de longueur 1

$$\alpha_1 = 1-2\theta-\theta^2 \qquad \beta_1 = -7+\theta+2\theta^2 \qquad \gamma_1 = -1+\theta$$

vérifient les équations respectives

$$X^3+5X^2-X-1 = 0 \qquad X^3+5X^2-5X+1 = 0 \qquad X^3+3X^2-X-1 = 0$$

Les couples (α_1,β_1), (β_1,γ_1), (α_1,γ_1) sont des systèmes fondamentaux d'unités.

IV.3 - Le corps défini par $X^3-7X+4 = 0$, de discriminant 940 admet $1,\theta,\theta^2$ pour base d'entiers. Les suites α,β,γ sont périodiques de longueur respective $\ell_1 = 2$, $\ell_2 = 2$, $\ell_3 = 3$ et contiennent les unités

$$\alpha_2 = -5+7\theta+3\theta^2 \qquad \beta_2 = -33+3\theta+5\theta^2 \qquad \gamma_3 = -3+6\theta-2\theta^2$$

vérifiant les équations respectives

$$X^3-27X^2+5X+1 = 0 \quad X^3+29X^2-11X+1 = 0 \quad X^3+37X^2-5X-1 = 0$$

et la relation $\alpha_2\beta_2\gamma_3 = 1$.

Les couples (α_2,β_2), (β_2,γ_3), (γ_3,α_2) sont des bases.

IV.4 - Le corps défini par $X^3-20X+34 = 0$, de discriminant 788 admet $1,\theta,\theta^2$ pour base d'entiers. Les suites α et β sont périodiques de longueur $\ell_1 = 3$, $\ell_2 = 2$ et contiennent les unités

$$\alpha_3 = -133+31\theta+11\theta^2 \qquad \beta_2 = 87-14\theta-6\theta^2$$

vérifiant les équations respectives

$$X^3-41X^2+11X+1 = 0 \qquad X^3-21X^2-5X+1 = 0$$

Mais la suite γ périodique de longueur 2 a une prépériode. Elle ne contient pas d'unité. On a les situations suivantes :

γ_1/α_1 est une unité vérifiant $X^3-9X^2+7X-1 = 0$

γ_2/β_1 est une unité vérifiant $X^3+21X^2-33X+1 = 0$

$\gamma_3/\gamma_1 = \gamma_1/\alpha_1$

On en déduit que les couples

$$(\alpha_3,\beta_2),\ (\alpha_3,\gamma_1/\alpha_1),\ (\beta_2,\gamma_3/\gamma_1),\ (\gamma_3/\gamma_1,\alpha_3)$$

sont des systèmes fondamentaux d'unités. On a les relations

$$\alpha_3\beta_2(\gamma_1/\alpha_1) = 1, \qquad \alpha_3(\beta_2^{-2})\ (\gamma_2/\gamma_1) = 1,$$

cet exemple montre qu'une suite de MA_i ne contient pas toujours une unité.

Pour obtenir un système fondamental d'unités il suffit de calculer 2 suites. Nous avons donc fait trop de calculs. Nous n'avons pas d'argument pour, étant donné un corps, choisir les deux directions les mieux appropriées.

Nous n'avons pas dressé de table, il en existe dans la littérature. Notre but était de montrer que le calcul de certaines M.A permet de calculer un système fondamental d'unités d'un corps cubique totalement réel.

La méthode exposée ici est plus rapide que celle de [7] et semble équivalente à celle de [3]. La précision des calculs est très facile à cerner. La méthode peut donc s'appliquer à des cas ponctuels difficiles (unités avec de grandes composantes dans la base d'entiers).

Références

[1] W.E.H. BERWICK .- Algebraic number fields with two independant units. Proc. London Math. Soc. (2) 34 (1932), p. 360-378.

[2] A.J. BRENTJES .- Multidimensional continued fraction algorithm (Thèse 1981, Amsterdam)

[3] J. BUCHMANN .- Zahlengeometrische Kettenbruchalgorithmen Zur Einheitenberechnung - (Thèse 1982, Köln).

[4] DELONE, FADDEEV .- The theory of irrationalities of the third degree Am. Math. Soc. Trans. of Math. Monographs 10 (1964).

[5a] E. DUBOIS .- Best approximation of zero by a cubic linear form. Calculation of the fundamental unit of a not totally real cubic field. Proc. Queen's Number Theory Conf. Kingston (1979) p. 205-221.

[5b] E. DUBOIS .- Approximations diophantiennes simultanées de nombres algébriques. (Thèse 1980, Paris).

[6] E. DUBOIS et G. RHIN .- Meilleure approximation d'une forme linéaire cubique. Acta Arithm. XL (1982), p. 197-208.

[7] R. SMADJA .- Calculs effectifs sur les idéaux des corps de nombres algébriques - Publication de l'Université d'Aix-Marseille 1976.

[8] VORONOI .- Sur la généralisation de l'algorithme des fractions continues (en Russe) - (Thèse 1896, Warsaw).

*

* *

Eugène DUBOIS
Université de Caen
Département de Mathématiques
et de Mecanique
F-14032 Caen Cedex

SOME PROBLEMS ON NUMBER THEORY

P. ERDÖS

In this little note I discuss mainly problems on prime numbers some of which occupied me for a long time, but I mention also some new questions. The quality of the problems considered will be very uneven, some are more exercises, some certainly serious problems, unfortunately I am not always sure into which category the problems belong.

First I discuss some problem which arose during our meeting. An old and very difficult conjecture of mine states that ($d(n)$ denotes the number of divisors of n) $d(n) = d(n+1)$ has infinitely many solutions. It is probably presumptions to call this "my conjecture" it probably was asked long ago. I only call it my conjecture since it is mentioned in one of my papers. Brun's method easily gives that for infinitely many n, $c_1 < d(n)/d(n+1) < c_2$ and in fact the set of limit points of $d(n)/d(n+1)$ contains intervals [1] [2]. No doubt the sequence $d(n)/d(n+1)$ is everywhere dense in $(0,\infty)$, but the only limit points know are 0 and ∞. My original conjecture on $d(n) = d(n+1)$ may very well be unattackable and it was a great surprise to me when Claudia Spiro (unpublished) proved that $d(n) = d(n+5040)$ has infinitely many solutions. It is based on the fact that there are 8 primes p_i, $i = 1,\ldots,8$ so that the least common multiple of the differences $p_j - p_i$ $1 \leqslant i \leqslant 8$ is 5040. This lead Narkiewicz and me to consider the following problem : Denote by $D(p_1,\ldots,p_n)$ the least common multiple of the $\binom{n}{2}$ numbers $p_j - p_i$. Put

$$f(n) = \min_{p_1,\ldots,p_n} D(p_1,\ldots,p_n)$$

and $F(n)$ is the smallest value of $D(p_1,\ldots,p_n)$ assumed for infinitely many $p_1,p_2,\ldots,p_n$. We of course can not even prove that $F(2)$ is finite since this would imply that $p_{k+1} - p_k < C$ has infinitely many solutions for some C, but we will assume the prime k-tuple conjecture of Hardy and Littlewood which of course implies $F(n) < \infty$. Put

$$g(n) = \prod_{q < m} q^{\alpha_q}$$

where α_q is the largest integer for which $\phi(q^{\alpha_q}) = (q-1)q^{\alpha_q - 1} < n$.

A simple argument shows that $F(n) \geqslant g(n)$ since if q is not one of the p's then $q^{\alpha_q} \mid D(p_1,\ldots,p_n)$. If q is one of the p's then $q^{\alpha_q} \mid D(p_1,\ldots,p_n)$ if $(q-1-q^{\alpha_q - 1} < n-1$. We conjectured that $f(n)/g(n) \to \infty$ and that $f(n) = g(n)$

is possible only for every small values of n . Very likely $f(n) = F(n)$ for $n > n_0$. We could not even show that $f(8) = 5040$.
It could be 2520 if all the 8 p's are incongruent mod 16 . We only could exclude this by long computations which we did not carry out. It follows from the prime number theorem that $\log g(n) = (n + o(1))$. We think that perhaps

$$(1) \qquad \lim \frac{\log f(n)}{n} < \infty \ , \ \lim \frac{\log F(n)}{n} < \infty \ .$$

It might be of some interest to obtain an asymptotic formula for $\log D(2,3,\ldots,p_n)$ probably

$$(2) \qquad \log D(2,3,\ldots,p_n) / n \log n = c \ , \text{for some } 0 < c < 1 \ .$$

In a recent letter Claudia Spiro deduced from the prime k-tuple conjecture that

$$(3) \qquad F(n) \qquad (g(n))^{1+c\frac{\log\log n}{\log n}} \ .$$

The conjecture $f(n)/g(n) \to \infty$ remains open. In view of her result (3) it would perhaps be of interest to study

$$\max_{p_1,\ldots,p_n} \{(\max_{1\leq i\leq n} p_i) D(p_1,\ldots,p_n)\} = A_n \ .$$

Is it true that $A_n^{1/n} \to \infty$? or at least $A_n > (1+\varepsilon)^n$ i.e.
A related function is

$$\min_{p_1,\ldots,p_n} \prod_{i=1}^{n} p_i D(p_1,\ldots,p_n) = B_n \ .$$

$B_n > (n!)^{1+c}$ or $B_n > n!^c$ for every c if $n > n_0(c)$ would perhaps be of some interest.
These problems can be considered for other sequences than the primes $a_1,a_2,\ldots,a_n$ are n square-free numbers what can be said about $\min D(a_1,\ldots,a_n)$? At the moment I can say nothing non-trivial about this problem.

Some questions which Nicolas and I considered lead to the following question : let $p_1,p_2,\ldots,p_n$ be an arbitrary set of n primes. Is it true that

$$(4) \qquad \sum_{1\leq i<j\leq k} \frac{1}{p_j - p_i} < Cn \ ?$$

(4) is still open. It follows from the prime k-tuple conjecture that (4) if true is best possible i.e. there are infinitely many n-tuples of primes $p_{i_1},\ldots,p_{i_k}$ for which

$$\sum_{1\leq j<j'\leq n} \frac{1}{p_{i_j} - p_{i_{j'}}} > Cn \ .$$

I thought for a while that instead of (4) the following stronger result may hold : Let $a_1 < a_2 < \ldots < a_n$ be a sequence of integers for which every interval of length t contain for every t fewer than $c_1 t/\log t$ a's . Is it then true that

$$(5) \qquad \sum_{1 \leqslant i < j \leqslant n} \frac{1}{a_j - a_i} < Cn \ ?$$

Unfortunately, Ruzsa gave a simple counterexample to (5) . Let the a's be the integers of the form $\sum_{i=1}^{s} \varepsilon_i 2^i$, where $\varepsilon_i = 0$ or 1 but $\varepsilon_i = 0$ if i is a power of 2 and s is chosen so that $s - \frac{\log s}{\log 2} = \frac{\log n}{\log 2} + O(1)$.

It is easy to see that the a's satisfy our condition but

$$(6) \qquad \sum_{1 \leqslant i < j \leqslant n} \frac{1}{a_j - a_i} > c\, n \log\log n$$

(6) contradicts (5) and is easily seen to be best possible. Probably a counterexample to (4) can also be found (i.e. the a 's can be chosen to be primes). Put $d_k = p_{k+1} - p_k$; d_k seems to behave very irregularly. Put

$$D(x) = \max_{p_k < x} (p_{k+1} - p_k) .$$

Cramer [3] conjectured that $\overline{\lim} \frac{d_k}{(\log k)^2} = 1$. A slight strengthening of Cramer conjecture states

$$(7) \qquad \lim \frac{D(x)}{(\log x)^2} = 1 .$$

It is quite possible though that Cramer's conjecture holds but (7) il false. (7) in particular would imply that

$$\frac{D(2x)}{D(x)} \to 1$$

and there certainly is no real evidence that this holds. In fact I suspect that it fails. There is no doubt that every even d is of the form $p_{k+1} - p_k$ but the smallest k for which $p_{k+1} - p_k = d$ probably tends to infinity exponentially in d but I can not prove that it tends to infinity faster than polynomially, perhaps this is not hopeless and I overlook a simple argument.

Denote by $U(x)$ the number of even integers of the form $p_j - p_i$, $3 \leqslant p_i < p_j \leqslant x$. $U(x) > cx$ follows immediately by Bruns method, but perhaps, $U(x) > \frac{x}{2} - (\log x)^{\alpha}$, for some α and all $x > x_0(\alpha)$ and perhaps for infinitely many x : $U(x) > \frac{x}{2} - C$ for some absolute constant C . Both of these conjectures are of course unattackable in the foreseeable future (the second one can perhaps be disproved).

Denote by $V(x)$ the number of integers of the form $a_j - a_i$ where $1 < a_i < a_j \leqslant x$ are squarefree numbers. $V(x) > x - x^{\alpha}$ is easy to prove for some $\alpha < 1$, also

$V(x) > x - C$ holds for infinitely many x and it seems to be easy to prove that for every t the density of the integers, for which $V(x) = x - t$, exists and the density of integers for which $V(x) < x - t$ tends to 0 as $t \to \infty$. The reason for the vagueness of my statement is that I did not think the proof over in all details.

Rankin [4] proved in 1938 that

$$(8) \qquad D(x) > c \log x \log\log x \log\log\log\log x \, (\log\log\log x)^{-2} = L(x) .$$

Since then the only improvement of (8) was that the original value of c has been replaced by a larger one by Schönhage and Rankin. This fact lead me to offer a reward of 10^4 dollars for a proof that (8) holds for every c and infinitely many x (in fact it no doubt holds for all x). I am so sure that this conjecture is true that I offer 25 000 dollars for a disproof. I really feel like offering 10^6 dollars, but contrary to rumours [5], I never offer a prize if I could not pay it.

Let $H(x)/D(x) \to \infty$. Is it true that ($\pi(y)$ is the number of primes not exceeding y)

$$(9) \qquad \pi(x+H(x)) - \pi(x) = (1+o(1))\, H(x)/\log x \ ?$$

(9) if true, is no doubt unattackable at present. Let $H_1(x)/L(x) \to \infty$. I noticed that I could not disprove that

$$(10) \qquad \pi(x+H_1(x)) - \pi(x) = (1+o(1))\, H_1(x)/\log x .$$

H.Meier wrote me that he proved that if (10) holds then $H_1(x) > (\log x)^{1+\varepsilon}$. I hope Meier will soon publish the proof of his interesting result. In the mean time Maier in fact proved that $H_1(x)$ must tend to infinity faster than any fixed power of $\log x$. His proof will be published soon. Denote by $A(x)$ the number of distinct integers of the form $p_{k+1} - p_k < x$. Is it true that

$$(11) \qquad A(x)/D(x) \to 0 \ ?$$

I have no intuition about (11) and it is quite possible that the limit in (11) does not exist. I expect that

$$(12) \qquad \max_{p_k < x} \min (p_{k+1} - p_k , p_k - p_{k-1}) \Big/ \max_{p_k < x} (p_{k+1} - p_k) \to 0$$

(12) is certainly true, but is probably very deep. All these questions can be formulated for the sequence $q_1 < q_2 < \ldots$ of square-free numbers, unfortunately these questions seem to me nearly as difficult as the questions about primes, with a few exception. It is a simple exercise in the use of the siefe of Eratosthenes that for every d there are infinitely many indices k for which $q_{k+1} - q_k = d$. k probably increases exponentially in d, we can at least show that it does not increases faster. Let $p_1 < p_2 < \ldots$ be an infinite sequence of primes, $a_1 < a_2 < \ldots$ is the sequence of integers not divisible by any of the p's.

We can ask the same question about $a_{i+1} - a_i$ but can answer them only if the p's tend to infinity very fast.

Perhaps we have more chance for success if we consider the integers relatively prime to n . Let $1 = a_1 < \ldots < a_{\phi(n)} = n-1$ be the integers relatively prime to n and put ($J(n)$ after Jacobstahl) [6] :

$$J(n) = \max_{a_i < n} (a_{i+1} - a_i) .$$

Jacobstahl conjectured $J(n) < c(\log n)^2$ and this was proved by Iwaniec [7] , but perhaps $J(n) < (\log n)^{1+\varepsilon}$, this would require very much better sieve methods than the ones at our disposal at present.

Let n_k be the product of the first k primes ,Jacobstahl conjectured that for $m \leqslant n_k$, $J(m) < J(n_k)$. Perhaps $J(m) < J(n_k)$ for all $m < n_{k+1}$, with possibly a finite number of exceptions. Clearly $J(n_{k+1}) > J(n_k)$ and probably

(13) $$J(n_{k+1}) - J(n_k) \to \infty \qquad \text{but} \qquad J(n_{k+1})/J(n_k) \to 1 .$$

The second conjecture of (13) seems certain to be true. The following conjecture seems important to me . Let $n_k < x < n_{k+1}$, then

(14) $$J(n_k)/D(x) \to 0 .$$

(14) seems important to me, all our information on large values of $p_{k+1} - p_k$ comes from our information on $J(n_k)$. I feel confident that (14) is true but see no way of an attack. I offer a record of 1000 dollars for any relevant information on (14) and 3000 dollars for a proof or disproof.

I expect that

(15) $$\max_{1 \leqslant i < \phi(n_k)} \min(a_{i+1} - a_i , a_i - a_{i-1})/J(n_k) \to 0 .$$

Perhaps (15) will not be very difficult in any case it should be much easier than (12) . (15) certainly is false for almost all integers, but may remain true for the sequence of integers satisfying $\phi(n_k')/n_k' \to 0$ i.e. $\prod_{p \mid n_k'} (1 - \frac{1}{p}) \to 0$.

It is true that if $H(n)/J(n) \to \infty$ then

(16) $$\phi_n(x, x+H(n)) = (1+o(1)) \frac{\phi(n)}{n} H(n)$$

where $\phi_n(u,v)$ is the number of integers $u < m < v$ $(m,n) = 1$. (16) is related to (9) but is probably much easier. (16) certainly holds for almost all n but I can not prove it for the n_k 's , but in any case I am sure it is much easier that (9) .

An old (more than 40 years) and striking conjecture of mine asserts that there is an absolute constant C so that for every n

$$(17) \qquad \sum_{k=1}^{\phi(n)-1} (a_{k+1} - a_k)^2 = C \frac{n^2}{\phi(n)} .$$

Hooley [8] has many nice results on the conjecture (17), but (17) is still open even if we assume that $\phi(n) < cn$.

Now let me state some more conjectures on the integers relatively prime to n. Many of these conjectures become trivial for the integers n which have few prime factors. Therefore we will usually restrict ourselves to state the problems for the integers n_k. Let $r = r(k)$ be the smallest index for which

$$(18) \qquad a_{r+1} = J(n_k)$$

i.e. r is smallest index for which $a_{\ell+1} - a_\ell$ assumes its maximum. I am sure that r increases exponentially in k but can not even prove that increases faster than polynomially. I would like to get an estimation for the number of solution of (18), also it is not clear to me that

$$(9) \qquad a_{t+1} - a_t = s$$

is solvable for every even $s < J(n_k)$. Perhaps the proof of this will be easy. A formula for the number of solutions and an estimation for the smallest solution would perhaps be of some interest. I just thought of these questions and have to ask for the indulgence of the reader if some of these problems are trivial or false. I conjectured some time ago that if $(a,b) = 1$, $a < b < x$ then

$$(20) \qquad \min(J(a), J(b)) < c \log x .$$

(20) is certainly a "serious" conjecture and if true, might give some insight into the mysterious behaviour of $p_{k+1} - p_k$.

A related old conjecture of mine states that if we consider the congruences

$$(21) \qquad n \equiv a_p \pmod{p}, \quad p < x ,$$

then for every choise of the a_p there always is an integer $n < x$ which satisfies at most one of the congruences (21).

Unfortunately I can make no contribution to the solution of these problems. During our meeting Hildebrandt and I proved that for every $\varepsilon > 0$ il $x > x_0(\varepsilon)$ one can find congruences

$$(22) \qquad n \equiv a_p ,$$

$$\exp(1-\varepsilon) \log x \log\log\log x / \log\log x < p < x$$

so that every integer $n < x$ satisfies at least one of the congruences (22), and that this becomes false if in (22) $1-\varepsilon$ is replaced by $1+\varepsilon$. One could try to make the result more precise by asking for the largest p_1 for which there are con-

gruences (22) for $p_1 \leqslant p \leqslant x$ so that every integer $n \leqslant x$ satisfies at least one of them. The exact determination of p_1 is of course hopeless but no doubt (22) could be made more precise.

Denote by $a_1^{(r)} < a_2^{(r)} < \ldots$ the set of integers which have at most r prime factors. It is a simple exercice to prove that for $r = 2$ [9]

$$\overline{\lim}\ (a_{i+1}^{(r)} - a_i^{(r)}) / \log(a_i^{(r)}) > 0 \quad . \tag{23}$$

I could never prove that the limit in (23) is ∞, also I could get no satisfactory result for $r > 2$. The limit could very well be 0 for $r > 2$.
Now I would like to restate some old problems of Selfridge and myself [10] which seem interesting to us but which have been completely neglected partly because our paper has been made to some extent obsolete by the results of Hensley and Richards [11]. Let

$$n < a_1 < a_2 < \ldots < a_t \leqslant n+k \quad , \quad (a_i, a_j) = 1 \quad , \quad 1 \leqslant i < j \leqslant t \ . \tag{24}$$

The sequence (24) is called complete if for every $n < s \leqslant n+k$, $(s, a_i) > 1$ for some $1 \leqslant i \leqslant t$. Put $\max t = F(n;k)$ and $\min t = f(n;k)$ where the maximum and minimum is to be taken for all complete sequences (24). Consider the four functions

$$\max_n F(n;k) \ , \ \min_n F(n;k) \ , \ \max_n f(n;k) \ , \ \min_n f(n;k) \ .$$

Our results on $\max F(n;k)$ have been made obsolete by Hensley and Richards, but perhaps it is remarkable that we could only prove

$$25\, k^{\frac{1}{2} - \varepsilon} < \min F(n;k) < c\, k (\log\log k)^2 (\log k)^{-2} (\log\log\log k)^{-1} \ . \tag{25}$$

The upper bound in (25) is clearly related to Rankin's result (8) and will be hard to improve but the lower bound should surely be improved to $k^{1-\varepsilon}$ or at least to $k^{1/2+\varepsilon}$ perhaps even $\min F(n;k)/k^{1/2} \to \infty$ would be of some interest.
Both $\max_n F(n;k)$ and $\min_n F(n;k)$ are clearly monotonic but $\max_n f(n;k)$ is not monotonic since $\max_n f(n;6) = 3$ and $\max_n f(n;5) = 4$, this is the only such case we found, but we only computed $\max_n f(n;k)$ for $k \leqslant 45$. Put

$$\min_n (F(n;k) - f(n;k)) = g(k) \ . \tag{26}$$

We conjectured that $g(k) \to \infty$ as $k \to \infty$. Perhaps (26) can be proved algorithmically and will not be difficult. Clearly all the integers all whose prime factors are $\geqslant k$ must occur in every complete sequence. Perhaps

$$\lim_{k\to\infty} \max_n \frac{F(n;k)}{k/\log k} > 1 \tag{27}$$

but as far as I know (27) is still open, we only can prove that the lim sup is finite and the lim inf $\geqslant 1$.

It is trivial that $\min f(n;k) = 2$. Denote by n_k the smallest integer for which $f(n_k;k) = 2$. Trivially $n_k \leqslant \prod_{p_i \leqslant k} p_i - k$. We have a non-trivial proof that for some k there is strict inequality.

Denote further by n_k' the smallest integer for which there are two integers a and b , $n_k' < a < b < n_k' + k$ so that $(n+j, ab) > 1$ for $1 \leqslant j \leqslant k$. The difference between n_k' and n_k is that in the definition of n_k' we do not require $(a,b) = 1$. We show that for all sufficiently large $k < n_k' < \frac{1}{2} \prod_{p < k} p$ and probably $n_k' = O\left(\prod_{p<k} p\right)$.

For which k is it true that if $(a,b) = 1$, $1 < b-a = k$, then there always is a c , $a < c < b$ such that $(a,b,c) = 1$? Perhaps for $k > k_0$ there is no such k . If such a k exists then for this k , $n_k = \prod_{p<k} p - k$.

Is there a k so that for some set of k consecutive integers $n+1, \ldots, n+k$

$$\left(n+i \ , \prod_{\substack{j=1 \\ j \neq i}}^{k} (n+j)\right) = A(n;i)$$

is complete for every i , $1 \leqslant i \leqslant k$? Is there a k so that every $A(n;i)$ has more than r distinct prime factors ? For $r = 0$ every sufficiently large k has this property. This is a well known result of Brauer, Pillai and Szekeres [12] . For $r > 0$ we do not know the answer which may very well by yes for $r = 1$ and no for $r > 1$. This problem is related to (23).

In another paper Selfridge and I [13] prove the following surprising theorem : For every $\varepsilon > 0$ and k there is a set of k^2 primes $p_1 > \ldots > p_{k^2}$ and an interval $I = \{x, x + (3-\varepsilon)p_1\}$ so that the number of distinct integers m in I which are multiples of any the p 's is $2k$. This theorem is surprising since one would expect that the number of these integers is $> ck^2$. Since our proof is not easily accessible I give it here in full detail. First we prove that our result is best possible. In fact we show that any interval I' of length $> 2p_1$ contains at least $2k$ distinct multiples of the p 's . This is essentially best possible. The interval $\left\{ \prod_{i=1}^{k^2} p_i - p_{k^2} + 1 \ , \ \prod_{i=1}^{k^2} p_i + p_{k^2} - 1 \right\}$ has length $2p_{k^2} - 2$ and contains only one multiple of the p 's . Let I' be the interval $\{a,b\}$, $b - a > 2p_1$. I_1' is the interval $\{a, a + \frac{1}{2}(b-a)\}$ and I_2' the interval

$\{a + \frac{1}{2}(b-a), b\}$ both of these intervals contains at least

$$\sum_{i=1}^{k^2} \left[\frac{b-a}{2p_i} \right] \geqslant k^2$$

multiples of the p's (counted by multiplicity). If no m in I is a multiple of more than k of the p's then clearly there are at least $2k$ distinct multiples of the p's in I. Thus assume say that there is an m in I_1' which is a multiple of $r > k$, p's, where r is the largest such integer.
Let $p_{i_1},\ldots,p_{i_r}$, $r > k$ be the prime factors of m. This in I_1' there are at least $\frac{k^2}{r}$ distinct multiples of the p's. For every P_{i_j} let s_j be the smallest integer for which $m + 2^{s_j}.p_{i_j}$ is in I_2', such an s_j clearly exists, and the numbers $m + 2^{s_j}.p_{i_j}$ are clearly distinct for $j = 1,2,\ldots,r$. Thus I' contains at least $r + \frac{k^2}{r} > 2k$ distinct multiples of the p's which completes the proof.
Now we prove the more difficult statement that there is an I of length $(3-\varepsilon)p_1$ which contains no more than $2k$ distinct multiples of the p's. First we prove a

Lemma.- For every k and arbitrary large N there are k^2 primes

$$N < q_0 < q_1 < \ldots < q_{k^2-1} < N + (\log N)^{k+3}$$

satisfying for every $1 \leqslant i \leqslant k-1$, $1 \leqslant j \leqslant k-1$

$$q_i - q_0 = q_{i+tk} - q_{tk} .$$

In others words there are k sets of k primes whose internal structure is the same. Probably very much more is true : there is an $f(k)$ and infinitely many primes p so that all the numbers $p + t\,f(k)$, $0 \leqslant t < k^2$, are primes - in fact consecutive primes. Needless to say it is quite hopeless at present to prove this conjecture and fortunately we do not need it.
The proof of the Lemma is by a simple counting argument. It followq from the prime number theorem (or a more elementary theorem) that for every large x there is an interval of length $L > (4k \log x)^{k+2}$ between $\frac{x}{2}$ and x which contains more than $\frac{L}{2 \log x}$ primes. Denote these primes by

$$y < r_1 < r_2 < \ldots < r_w < y + L , \quad w > \frac{L}{2 \log x} .$$

Consider the $[\frac{w-1}{k}]$ intervals $[r_{(u-1)k+1}, r_{uk+1}]$, $uk+1 < w$. We only retain those intervals which are shorter than $4k \log x$. Clearly there are at least

$L(4k \log x)^{-1}$ such intervals. The number of patterns for the k primes $r_{(u-1)k+1}, r_{(u-1)k+2}, \dots, r_{uk}$ in these intervals is clearly less than $(4k \log x)^{k+1}$. Thus for sufficiently large x there are more than k k-tuples of primes giving the same pattern, which completes the proof of our Lemma.

Now using the Chinese remainder theorem we are ready to complete the proof of our theorem. Put

$$\alpha_i = \prod_{j=0}^{k-1} q_{ik+j} , \quad \beta_j = \prod_{i=0}^{k-1} q_{ik+j} , \quad 1 \leqslant i , j \leqslant k-1 .$$

Clearly

$$\prod_{i=0}^{k-1} \alpha_i = \prod_{j=0}^{k-1} \beta_j = \prod_{\ell=0}^{k^2-1} q_\ell .$$

Now we determine $x \bmod \prod_{\ell=0}^{k^2-1} q_\ell$ as follows :

$$x+q_j \equiv 0 \pmod{\beta_j} , \quad x+q_0 \equiv q_{jk} \pmod{\alpha_j} , \quad 0 \leqslant j \leqslant k-1 .$$

A simple argument shows that the interval $\{x-q_0+1 , x+2q_0-1\}$ of length $3q_0 - 2 > (3-\varepsilon) q_{k^2-1}$ contains only $2k$ multiples of the q's namely the unique multiples of $\alpha_0, \alpha_1, \dots, \alpha_{k-1} ; \beta_0, \beta_1, \dots, \beta_{k-1}$.

Let now again $p_1 > p_2 > \dots > p_{k^2}$, and I an interval of length $\geqslant 3p_1$. Unfortunately here so to speak "all hell breaks loose" and we completely loose control over the distinct multiples of the p's. It is quite possible that in this case I contains more than $c\, k^2$ distinct multiples of the p's. I can only prove the following much weaker theorem.

Let $p_1 > \dots > p_{k^2}$, and I an interval of length $\geqslant 3p_1$. Then I contains at least $6^{1/2} k$ distinct multiples of the p's.

Clearly the interval I contains at least $3k^2$ multiples or the p's, counted by multiplicity. Let r be the largest integer so that there is an m in I which is the multiple of r p's say $m \equiv 0 \pmod{p_{\ell_1}, \dots, p_{\ell_r}}$.

Each p_{ℓ_j}, $j = 1, \dots, r$ has at least two other multiples in I (namely $m \pm p_{\ell_j}$ or $m+p_{\ell_j}$, $m+2p_{\ell_j}$ or $m-p_{\ell_j}$, $m-2p_{\ell_j}$). These $2r+1$ multiples of the p's are clearly all distinct. Thus I contains at least

$$\min \left(\frac{3k^2}{r} , 2r+1 \right) > 6^{1/2} k$$

distinct multiples of the p's, which completes our proof of our theorem.

I am sure that this result is not best possible. Perhaps the following related pro-

blem is also interesting : Determine the smallest $f(u)$ so that if $p_1 > \ldots > p_u$ are primes, every interval of length $f(u)p_1$ contains an integer divisible by precisely one of the p's . Clearly many related questions can be asked.

Denote by I_n the interval $(\frac{n}{3}, \frac{n}{2})$ and by $f(x,n)$ the number of integers m, $x < m < x+n$ which have at least one prime factor in I_n . An old conjecture of mine states

$$f(x,n) > cn/\log n . \tag{28}$$

It seems ridiculous that I have not been able to make any progress with (28) and I am not sure if I am just being silly and overlook an obvious point or whether (28) is really difficult or at least requires a clever idea. It is easy to see that the number of integers having at least two prime factors in $\{x,x+n\}$ is at most

$$\frac{1}{2}(\pi(\tfrac{n}{2}) - \pi(\tfrac{n}{3})) = (1+o(1))\frac{n}{12 \log n}$$

and that equality is possible here, also $f(x,n) \leqslant 2(\pi(\frac{n}{2}) - \pi(\frac{n}{3}))$ for suitable values of x and equality is again possible, but I would only prove $f(x,n) > c\left(\frac{n}{\log n}\right)^{1/2}$. It is not difficult to show that there is an absolute constant C so that if $n \to \infty$ then for almost all x

$$f(x,n) = (C+ (1))\frac{n}{\log n}$$

and with a little more trouble one could obtain results on the distribution function of the error $f(x,n) - C\frac{n}{\log n}$. None of this seems to help with (28) .

To finish the paper let me just state a few older problem. Denote by $p_1, p_2, \ldots$ the sequence of primes. Prachar and I [14] conjectured that the number of indices k for which for every $i < k < j$

$$p_i/i < p_k/k < p_j/j \tag{29}$$

is finite.

(29) seems very plausible and it probably holds for many other sequences e.g. for the primes $p \equiv a \pmod b$ or for the set of integers not divisible by a set of primes $\sum 1/p_i = \infty$ where the complementary set q_i also satisfies $\sum 1/q_i = \infty$. In fact (29) should hold if $a_k/k \to \infty$ but not too fast and a_k is not too regular. These rather vague statements of course do not really help and it must be left open whether any non-trivial statement related to (29) can be made and proved.

More than 25 years ago I made the following (foolish) conjecture. Let $a_1 < a_2 < \ldots < a_k \leqslant n$, $\prod_{i=1}^{k} 1/a \leqslant 1$. Is it then true that the number of integers not exceeding n which are not divisible by any of the a's is $> cn$. This was disproved by Schinzel and Szekeres [15] and more recently Ruzsa and Tenenbaum proved that the number of these integers is $> c_1 \frac{n}{\log n}$, but can be less than $c_2 n/\log n$.

Let $p_1 < p_2 < \ldots < n$ be a sequence of primes for which $\sum 1/p_i \leqslant 1$. Then it is easy to see that there are cn integers no one of which is a multiple of any of the p's $\leqslant n$. It will perhaps not be difficult to determine the smallest possible value of c.

One of the most interesting unconventional problems of primes is due to Ostman: Prove that one can not find two sequences $a_1 < a_2 < \ldots, b_1 < b_2 \ldots$ of at least two elements so that all but a finite number of primes are of the form $a_i + b_j$ and only a finite number of composite numbers are of the form $a_i + b_j$, in other words the symmetric difference of the primes and the integers of the form $a_i + b_j$ must be infinite. This striking conjecture is still open. Hornfeck [16] proved it in the case that one of the sequence $a_1 < a_2 < \ldots$ or $b_1 < b_2 < \ldots$ is finite.

It follows from the prime k-tuple conjecture that there are two infinite sequences $a_1 < a_2 < \ldots, b_1 < b_2 < \ldots$ so that all the sums $a_i + b_j$ are primes. It seems certain that at least one of these sequences must tend to infinity at least exponentially. By the way it seems certain that if there are only a finite number of composite numbers among the $a_i + b_j$ then there are only $(\frac{x}{\log x})$ primes $p < x$ of the form $a_i + b_j$ which would be much stronger than Ostmans conjecture. Since the analog of the prime k-tuple conjecture clearly holds for the squarefree numbers it is easy to see that there are infinite sequences $a_1 < a_2 < \ldots, b_1 < b_2 < \ldots$ so that all the integers $a_i + b_j$ are squarefree. Perhaps it is true that if all but a finite number of the $a_i + b_j$ are squarefree and both sequences a_i and b_j are infinite then the number of squarefree integers of the form $a_i + b_j$ is $o(x)$, or even slightly stronger $A(x)\, B(x) = o(x)$ where $A(x) = \sum_{a_i < x} 1$, $B(x) = \sum_{b_i < x} 1$.

Pomerance once asked: Is there a subsequence of the primes $p_{i_1} < p_{i_2} < \ldots$ whose second difference $p_{i_r} - 2p_{i_{r+1}} + p_{i_{r+2}}$ is bounded from above (or bounded in absolute value). Probably such a sequence does not exist, not even if the primes are replaced by the squarefree numbers, but I do not see how to attack these questions.

About 30 years ago, Ricci and I [17] proved that the set of limit points of $(p_{k+1} - p_k)/\log k$ is of positive Lebesgue measure. Unfortunately ∞ is the only limit point of this set known to us. Can one prove that this set has a finite limit point $\geqslant 1$?

Perhaps the following somewhat vague conjecture is not hopeless : Let $H(x)/\log x \to \infty$ smoothly but $H(x) < L(x)$ (see (8)) . Is it then true that the set of limit points of $(p_{k+1} - p_k)/H(k)$ have positive measure ? Is there for every C an index k for which

$$C \log x < p_k - p_{k-1} < p_{k+1} - p_k \ , \ p_k < x \ ?$$

Finally I state a somewhat unconventional problem which was considered by Pomerance and myself. Straus and I once conjectured that if $k > k_0$ then there always is an i for which

$$p_k^2 < p_{k+i}\, p_{k-i} \tag{30}$$

Pomerance [18] disproved this, in fact he disproved this for much more general sequences. We tried unsuccessfully to prove that in fact for almost k (30) in fact holds. It would suffice to show that for almost all k there is an i for which

$$2p_k > p_{k+i} + p_{k-i} \ , \ p_{k+i} < p_k + p_k^{1/2} \tag{31}$$

but we could not prove (31). Is it true that the number of distinct integers of the form $p_{n+i} + p_{n-i}$, $i = 1,2,\ldots$ is $> cn/\log n^2$? It easily follows from the sharper form of the prime number theorem that the number of solutions of $A = p_{n+i} + p_{n-i}$ in i is bounded if $n \to \infty$, but we can show this only for the A's in the neighborhood of $2p_n$.

Pomerance and I further considered the following problems : Is it true that for $n > n_0$ there always is an i for which $2p_n = p_{n+i} + p_{n-i}$? The answer is almost certainly affirmative. Is it true that there is a c so that infinitely many i and every $i < n$

$$p_{n+i} + p_{n-i} - 2p_n > -C \ ?$$

Put

$$M(n) = \max_i p_{n+i}\, p_{n-i} \ .$$

Is it true that there is an $\alpha > 0$ so that for infinitely many n

$$M_n > p_{n+i}\, p_{n-i} + n^{\alpha} \ , \tag{32}$$

and if the answer is affirmative try to determine the largest α for which (32) holds for infinitely many n .

Finally I would like to remark that (17) leads to interesting and deep problems for other sequences e.g. let $q_1 < q_2 < \ldots$ be the sequence of consecutive squarefree numbers. Is it true that for every α

$$\sum_{q_n < x} (q_{n+1} - q_n)^{\alpha} < c_{\alpha} x \ ? \tag{33}$$

I proved (33) for every $\alpha \leqslant 2$ and Hooley [16] proved it for every $\alpha \leqslant 3$ (Hooley just informed me that he can prove it for every $\alpha \leqslant 3+\varepsilon$ for some small positive ε . If (33) holds for every α then for every $\varepsilon > 0$ and $n > n_0(\varepsilon)$, $q_{n+1}-q_n < q_n^{\varepsilon}$. Thus (33) if true is probably very deep. I could not disprove the following much stronger conjecture

$$(34) \qquad \sum_{q_n < x} \exp C(q_{n+1} - q_n) < \alpha_C x .$$

(34) if true is completely beyond our reach, but perhaps (34) can be disproved.

Recently Heath-Brown (by using and further developing the method of Claudia Spiro) proved that the number of solutions of $d(n) = d(n+1)$, $n < x$, is greater than $c\,x(\log x)^{-?}$ The problem on $d(n) = d(n+1)$ is in fact a joint problem of mine with L. Missky (see P. Erdös and L. Missky, On the distribution of values of the divisor fonction d(n), Proc. London Math. Sco. 3(1952),257-271).

*
* *

REFERENCES.

[1] P. Erdös, Some remarks on Euler's ϕ-function, Acta Arith. 4 (1958) , 10-19.

[2] For a more detailed proof of these statements see a forthcoming paper of Pomerance, Sárközy and myself.

[3] H. Cramer, On the order of magnitude of the difference between consecutive prime numbers, Acta Arith. 2 (1937) , 23-46.

[4] R.A. Rankin, The difference between consecutive prime numbers, J. London Math. Soc. 13 (1938) , 242-247.

[5] See P.D.T. A. Elliott, Probabilistic Number Theory , Springer Verlag 1980, Vol. 1, p. 254.

[6] P. Erdös, On the integers relatively prime to n and on a number theoretic function considered by Jacobstahl, Math. Scand. 10 (1962) , 163-170.

[7] Iwaniec, On the problem of Jacobstahl, Demonstratio Mathematica 11 (1978), 1-7.

[8] C. Hooley, On the differences of consecutives numbers relatively prime to n , I , II and III , Acta Arith. 8 (1963/6) ; Publ. Math. Debrecen 12 (1969) , 39-49; Math. Zeitschrift 90 (1965) , 355-369.

[9] P. Erdős , Problem 237 in Elemente der Mathematik 10 (1955).

[10] P. Erdős and T. Selfridge, Complete prime subsets of consecutive integers, Proc. Manitoba Conf. 1971, 1-14.

[11] Hensley and I. Richards, Primes in intervals, Acta Arithmetica 25 (1973), 375-391, see also P. Erdös and I. Richards, Density functions for prime and relatively prime numbers, Monatshefte Math. 83 (1977) , 99-112.

[12] R.I. Evans, On blocks of consecutive integers, Amer. Math. Monthly 76 (1969), 48-49.

[13] P. Erdös, Problems and results in combinatorial analysis and combinatorial number theory, Proceedings of the Ninth Southeastern Conference on Combinatorics Graph Theory and Computing 1978, 29-40.-
See also a related problem of Suranyi and myself : P. Erdös and J. Suranyi, Remarks on a problem of a mathematical competition (in Hungarian) Math. Lapok, X (1959), 39-47.

[14] P. Erdös and K. Prachar, Sätze und Probleme über $p_{h/k}$. Abhandlungen Math.Sem. Hamburg, 25 (1961-62), 251-256.

[15] A. Schinzel and Szekeres, Sur un problème de Paul Erdös, Acta Sci. Math. Szeged 20 (1959), 221-229.

[16] C. Hooley, On the distribution of squarefree numbers, Canada J. Math. 25 (1973), 1216-1223.

[17] G. Ricci, Recherches sur l'allure de la suite $p_{n+1}-p_n/\log p_n$,Colloque sur la théorie des nombres, Bruxelles (1955), 93-106. Liège and Paris. My paper appeared in the lectures notes of a conference held in 1955 at Lake Como, Italy, this paper has not been reviewed and is not easily accessible.

[18] C. Pomeranie, The prime number graph, Math. Comp. 33 (1979), 399-408.

*

* *

P. ERDÖS
Mathematical Institute of the
Hungarian Academy of Sciences
BUDAPEST 1395, PF 428

SUR LE THEOREME DE BRUN - TITCHMARSCH

par E. FOUVRY

I.- RESULTATS.

Un des problèmes classiques de la théorie analytique des nombres est l'évaluation, pour a et q entiers premiers entre eux, de la fonction $\pi(x;q,a)$, cardinal de l'ensemble des nombres premiers inférieurs à x, congrus à a modulo q. Ici, on ne s'intéresse qu'à une majoration *en moyenne* de cette fonction, plus précisément, on étudie le problème suivant :

Problème : Soient $\varepsilon > 0$, $A > 0$, $\frac{1}{2} \leqslant \theta \leqslant 1 - \varepsilon$, $Q = x^{\theta}$, a *un entier fixé. Quelle fonction* $C(\theta)$ *peut-on prendre pour que l'inégalité*

$$\pi(x;q,a) \leqslant \frac{x}{\varphi(q) \log x} (C(\theta) + \varepsilon)$$

soit vraie pour $x \geqslant x_0(a,A,\varepsilon)$, *pour presque tout* q *de l'intervalle* $[Q,2Q]$ *premier avec* a , *le nombre d'exceptions ne dépassant pas* $Q(\log x)^{-A}$?

La formule conjecturée par Montgomery

$$\pi(x;q,a) = \frac{\mathrm{Li}\, x}{\varphi(q)} + O_{\varepsilon}\left(\left(\frac{x}{q}\right)^{\frac{1}{2}+\varepsilon}\right) \qquad \left((q,a)=1 \ , \ q \leqslant x^{1-\varepsilon}\right)$$

entraîne que le bon ordre de grandeur serait $C(\theta) = 1$.
En 1981, J.M. DESHOUILLERS et H. IWANIEC, partant de leurs estimations en moyenne de sommes de Kloosterman ([1]) sont parvenus à la fonction $C(\theta) = 4/(3(1-\theta))$, d'où ils ont déduit que, pour une infinité de nombres premiers p , le plus grand facteur premier de $p+a$ vaut au moins $p^{\delta-\varepsilon}$ avec $\delta = 0{,}65635 \ldots$ ([2]) .

On améliore leur résultat de la façon suivante :

THEOREME ([5]) : *Pour* $\frac{1}{2} \leqslant \theta \leqslant \frac{11}{20}$, *le problème proposé admet pour solution la fonction* $C(\theta) = C_1(\theta) - C_2(\theta)$, *avec*

$$C_1(\theta) = \begin{cases} \dfrac{12}{25 - 40\theta} & \left(\frac{1}{2} \leqslant \theta \leqslant \frac{53}{104}\right) \\ \dfrac{48}{47 - 56\theta} & \left(\frac{53}{104} \leqslant \theta \leqslant \frac{11}{20}\right) \end{cases}$$

et

$$C_2(\theta) = \begin{cases} \log\left(\frac{10(1-\theta)}{9\theta}\right) & \left(\frac{1}{2} \leqslant \theta \leqslant \frac{10}{19}\right) \\ 0 & \left(\frac{10}{19} \leqslant \theta \leqslant \frac{11}{20}\right) \end{cases}$$

Le gain est sensible en $\theta = \frac{1}{2}$, puisque $C(\frac{1}{2})$ passe de la valeur 2,6666 ... à la valeur 2,2946 ... Par contre, la constante δ ne voit sa valeur augmenter que de 15.10^{-4}.

II.- QUELQUES IDEES SUR LA DEMONSTRATION.

La démonstration de Deshouillers et Iwaniec débute par la formule du crible de Rosser - Iwaniec, appliquée à la suite

$$\mathcal{A}(q) = \{n \leqslant x \ ; \ n \equiv a[q]\}$$

conduisant à l'inégalité

$$(1) \qquad \pi(x;q,a) \leqslant \frac{(2+\varepsilon)x}{\varphi(q)\log D} + R_q^+(D)$$

avec

$$R_q^+(D) = \sum_{\substack{d \leqslant D \\ (d,q)=1}} \lambda(d) \sum_{\substack{n \in \mathcal{A}(q) \\ d \mid n}} 1 - \frac{x}{dq}$$

Le coefficient $\lambda(d)$ est "bien factorisable", c'est-à-dire que pour toute décomposition $D = MN$ avec $M > 1$ et $N > 1$, on peut écrire λ comme produit de convolution arithmétique

$$(2) \qquad \lambda(\,.\,) = \alpha(\,.\,) * \beta(\,.\,)$$

où $\alpha(\,.\,)$ et $\beta(\,.\,)$ sont nuls hors des intervalles $[1,M]$ et $[1,N]$ respectivement, et sont "petits en moyenne".

Utilisant un développement en série de Fourier et des majorations de sommes de Kloosterman, et en choisissant au mieux les nombres M et N, on montre, dans [2], que $R_q^+(D)$ est petit en moyenne, pour $D = (xQ^{-1})^{3/2 - 2\varepsilon}$, ce qui conduit au résultat.

La première amélioration est fondée sur l'idendité de Buchstab, on est ramené ainsi à remplacer l'inégalité (1) par la suivante :

$$\pi(x;q,a) \leqslant \frac{(2+\varepsilon)x}{\varphi(q)\log D} - E(q) + R_q^+(D)$$

où on a posé

$$E(q) = \#\{n \in \mathcal{A}(q) \ ; \ D^{1/3} \leqslant \inf\{p;p\mid n\} < x^{1/2}\} .$$

Il est facile de minorer $E(q)$ par $E'(q)$, avec

$$E'(q) = \#\{n \in \mathcal{A}(q) \ ; \ n = p_1p_2 \ , \ Qx^{\varepsilon} \leqslant p_2 \leqslant x^{\frac{10}{19} - \varepsilon}\} .$$

Le théorème 3 de [3] permet alors de remplacer, pour presque tout q de $[Q,2Q]$, la quantité $E'(q)$ par

$$\frac{1}{\varphi(q)} \#\{ n \leqslant x ; n = p_1 p_2 , Qx^{\varepsilon} \leqslant p_2 \leqslant x^{\frac{10}{19} - \varepsilon} \}$$

On retrouve ainsi la fonction $C_2(\theta)$ du théorème.

Pour obtenir la seconde amélioration, on revient à la construction du coefficient $\lambda(d)$ ([6]).

Notons D_i un nombre de la forme $D^{\varepsilon^2(1+\varepsilon^7)^k}$ $(k \geqslant 0)$ et (D) une suite $(D_1,\ldots,D_r)$ vérifiant les inégalités $D_1 \geqslant D_2 \geqslant D_3 \ldots$

$$(3) \qquad D_1^3 \leqslant D , \quad D_1 D_2 D_3^3 \leqslant D \ldots,$$

Il apparaît alors que $R_q^+(D)$ est la somme

$$R_q^+(D) = \sum_{(D)} R_q^+((D))$$

avec

$$R_q^+((D)) = \sum_{\nu < D^{\varepsilon}} c_\nu(D,\varepsilon) \sum_{D_i \leqslant p_i < D_i^{1+\varepsilon^7}} \left(\sum_{\substack{\nu p_1 \ldots p_r \ell \leqslant x \\ \nu p_1 \ldots p_r \ell \equiv a\,[q]}} 1 - \frac{x}{\nu p_1 \ldots p_2 q} \right)$$

$$(|c_\nu(D,\varepsilon)| \leqslant 1) .$$

On dispose ainsi d'un grand nombre de variables p_i, qui seront réarrangées par un argument combinatoire. Evoquons deux cas extrêmes :

Quand (D) possède beaucoup de D_i "petits", on peut regrouper certains p_i (notés $p'_1 \ldots p'_k$) en une variable $m = p'_1 \ldots p'_k$, comprise dans l'intervalle $[x^{-1+\varepsilon} Q^2 , x^{5/6-\varepsilon} Q^{-4/3}]$. Le théorème 1 de [4] donne alors la majoration

$$\sum_{\substack{Q < q \leqslant 2Q \\ (q,a)=1}} |R_q^+((D))| << x(\log x)^{-A}$$

soit encore $|R_q^+((D))| < \dfrac{\varepsilon x}{\varphi(q) \log x}$

pour presque tout q de $[Q,2Q]$ premier avec a.

Par contre, lorsque D ne contient pas de D_i "petit", les inégalités (3) entraînent que $D_1 \ldots D_r \leqslant D D_r^{-1}$, autrement dit, on écrira λ sous la forme (2) avec le produit MN beaucoup plus petit que D, ce qui permet alors de prendre pour ce dernier une valeur supérieure à $(xQ^{-1})^{-2\varepsilon+3/2}$.

En conclusion, le théorème repose essentiellement sur les articles [3] et [4], dont la motivation est de franchir la valeur $\frac{1}{2}$ de l'exposant de répartition d'un certain type de suites d'entiers, obtenues par convolution de suites de supports particuliers. Dans ces travaux, on calcule une dispersion grâce à un développement en série de Fourier et des majorations de sommes de Kloosterman.

BIBLIOGRAPHIE.

[1] J.M. DESHOUILLERS and H. IWANIEC, *Kloosterman sums and the Fourier coefficients of cusp forms*, Invent. Math. 70 (1982), 219-288.

[2] J.M. DESHOUILLERS and H. IWANIEC, *On the Brun-Titchmarsch theorem*, Proc. Janos Bolyai Soc. Conf (à paraître).

[3] E. FOUVRY, *Répartition des suites dans les progressions arithmétiques*, Acta Arith XLI (1982), 359-382.

[4] E. FOUVRY, *Autour du théorème de Bombieri-Vinogradov*, Acta Math. (à paraître).

[5] E. FOUVRY, *Sur le théorème de Brun Titchmarsch*, Acta Arith. (à paraître).

[6] H. IWANIEC, *A new form of the error term in the linear sieve*, Acta Arith. 37 (1980), 307-320.

Etienne FOUVRY

U.E.R. de Mathématiques et d'Informatique
Université de Bordeaux I
351, Cours de la Libération
33405 TALENCE CEDEX

EQUATION DE PELL ET POINTS D'ORDRE FINI

Yves HELLEGOUARCH et Mireille LOZACH (Caen)

L'idée de ce travail remonte à la visite d'A. SCHINZEL à Caen en 1981 et le résultat principal en est la construction de familles de variétés abéliennes admettant des points prescrits d'ordre fini.
De nombreux membres de l'équipe d'Algèbre et de Théorie des Nombres de Caen y retrouveront leurs suggestions et critiques; en particulier E. Dubois, R. Paysant-Le Roux, P. Satgé et B. Vallée.

I. PARTIE GÉOMÉTRIQUE

1) La courbe $\mathcal{C}$ et sa jacobienne

On se donne un entier $p > 0$, un corps k dont la caractéristique ne divise pas p et un polynôme unitaire de degré pn, avec $n > 0$, $D(X) \in k[X]$. $\overline{k}$ désignant une clôture algébrique de k (fixée dans la suite) on suppose que $D(X)$ n'a que des racines simples dans $\overline{k}$.

On considère la courbe $\mathcal{C}$ d'équation :

$$Y^p = D(X)$$

et on désigne par K le corps des fonctions de $\mathcal{C}$ sur k : $K = k(X,Y)$, $\overline{K}$ le corps des fonctions de $\mathcal{C}$ sur $\overline{k}$: $\overline{K} = \overline{k}(X,Y)$.

Les extensions $K/k(x)$ et $\overline{K}/\overline{k}(X)$ sont de degré p, et la seconde est galoisienne de groupe de Galois $G \cong \mathbf{Z}/p\mathbf{Z}$.

La première n'est pas nécessairement galoisienne comme l'on voit en prenant $k = \mathbf{Q}$.

On désignera par σ un générateur de G, il sera déterminé par :

$$\begin{cases} \sigma(X) = X \\ \sigma(Y) = \zeta Y \end{cases}$$

où ζ est une certaine racine primitive $p^{\text{ième}}$ de 1. Il est clair que G est un groupe d'automorphismes de la courbe $\mathcal{C}$.

Une place $\mathfrak{p}$ de $\overline{k}(x)$ se prolonge en général en p places $P_1, P_2, P_3, \ldots$ de $\overline{K}$, sauf lorsque $D(X)$ est annulé par $\mathfrak{p}$ (on écrira $D(X) \in \mathfrak{p}$). Les prolongements des places à distance finie de $\overline{k}(X)$ seront appelées les "points à distance finie" de $\mathcal{C}$.

Pour prolonger la place à l'infini ($\frac{1}{X} \in \mathfrak{p}$), on considère la transformation birationnelle :

$$\begin{cases} X \longmapsto X' = \dfrac{1}{X} \\ Y \longmapsto Y' = \dfrac{Y}{X^n} \end{cases}$$

qui transforme $\mathcal{C}$ en $\mathcal{C}^*$ d'équation :

$$Y'^p = D^*(X')$$

où D^* désigne le polynôme réciproque de D. Puisque D est unitaire, $D^*(0) = 1$, donc la place à l'infini se prolonge en p places de $\overline{K}$, que l'on notera ∞_0 (lorsque $Y \longmapsto 1$), ∞_1 (lorsque $Y \longmapsto \zeta$),..., ∞_{p-1} (lorsque $Y \longmapsto \zeta^{p-1}$) (Voir [Deuring]).

Le groupe abélien libre $\mathcal{A}$ engendré par les places de $\overline{K}$ est appelé le groupe des diviseurs de $\mathcal{C}$. Les éléments de $\mathcal{A}$ qui sont invariants par $\mathrm{Gal}\,(\overline{k}/k)$ sont appelés les diviseurs rationnels de $\mathcal{C}$ lorsque k est de caractéristique zéro [1].

La jacobienne J de $\mathcal{C}$ est le groupe quotient du groupe $\mathcal{A}_o$ des diviseurs de degré zéro par le sous-groupe des diviseurs des éléments de $\overline{K}$. Un point de J est rationnel lorsqu'il est l'image d'un diviseur rationnel par la projection cononique : $\mathcal{A}_o \longrightarrow J$.

2) Equation de Pell généralisée

On considère un élément quelconque $\varphi \in K$:

$$\varphi = U_o(X) + U_1(X)Y + \ldots + U_{p-1}(X)Y^{p-1}$$

avec $U_i(X) \in \overline{k}(X)$.

On appelle norme de φ, la fraction rationnelle :

$$N(\varphi) = \varphi \cdot \sigma(\varphi) \cdot \ldots \cdot \sigma^{p-1}(\varphi) \in \overline{k}(X)$$

---

(1) Dans le cas général, il faut tenir compte des questions de séparabilité.

Lorsque $\varphi \in k(X)$, il est clair que $N(\varphi) \in k(X)$. On appellera "équation de Pell" l'équation :

$$(E_p) \qquad N(\varphi) = C^{te}, \text{ avec } C^{te} \in \overline{k}^*$$

ou encore :

$$\begin{vmatrix} U_o(X), & U_1(X)D^{1/p}, \ldots & U_{p-1}(X)D^{p-1/p} \\ U_1(X)D^{1/p}, & U_2(X)D^{2/p}, \ldots & U_o(X) \\ \\ U_{p-1}(X)D^{p-1/p}, & U_o(X) \quad , \ldots & U_{p-2}(X)D^{p-2/p} \end{vmatrix} = C^{te}$$

Exemples :

1) $p = 2$, (E_2) : $U_o^2 - DU_1^2 = C^{te}$

2) $p = 3$, (E_3) : $U_o^3 + U_1^3 D + U_2^3 D^2 - 3U_o U_1 U_2 D = C^{te}$

Définition :

On dira que la solution $(U_o(X),\ldots,U_{p-1}(X))$ de (E_p) est triviale ssi $U_o(X) \in \overline{k}^*$ et $U_1(X) = \ldots = U_{p-1}(X) = 0$.

3) Solutions polynômiales dans $\overline{k}[X]$

Puisque le groupe de Galois G agit sur le groupe des diviseurs $\mathcal{A}$ de $\mathcal{C}$, il est clair que J est un $\mathbb{Z}[G]$-module.

Théorème 1.- L'équation (E_p) admet une solution non triviale $(U_o,U_1,\ldots,U_{p-1}) \in (\overline{k}[X])^p$ ssi le point $(\sigma-e)\infty_o$ est annulé sur J par un élément de $\mathbb{Z}[G]$ non nul et du type :

$$\mu_o e + \mu_1 \sigma + \ldots + \mu_{p-2}\sigma^{p-2}$$

avec $(\mu_o,\mu_1,\ldots,\mu_{p-2}) \in \mathbb{Z}^{p-1}$.

Démonstration :

1) Pour toute solution $(U_o, U_1, \ldots, U_{p-1})$ de (E_p) on pose :

$$\varphi = U_o + U_1 Y + \ldots + U_{p-1}Y^{p-1} \in \overline{K}$$

Dire que la solution $(U_o,\ldots,U_{p-1})$ est polynomiale, revient à dire que $\sigma^i(\varphi)$, pour $i = 0,\ldots,p-1$, n'admet pas de pôles à distance finie.

Puisque $\varphi \cdot \sigma(\varphi)\ldots\sigma^{p-1}(\varphi) = C^{te}$, ces fonctions n'admettent pas non plus de zéros à distance finie.

2) On a donc :

$$\text{Div}\ (\varphi) = \nu_o \infty_o + \ldots + \nu_{p-1}\infty_{p-1}$$

avec $\nu_o + \ldots + \nu_{p-1} = 0$, donc :

$$\begin{aligned}\text{Div}\ (\varphi) &= \nu_1(\infty_1 - \infty_o) + \ldots + \nu_{p-1}(\infty_{p-1} - \infty_o)\\ &= \nu_1(\sigma - e)\infty_o + \ldots + \nu_{p-1}(\sigma^{p-1} - e)\infty_o\\ &= [\nu_1 e + \nu_2(\sigma+e) + \ldots + \nu_{p-1}(\sigma^{p-2} + \ldots + e)](\sigma - e)\infty_o\\ &= [\mu_o e + \mu_1\sigma + \ldots + \mu_{p-2}\sigma^{p-2}](\sigma - e)\infty_o\end{aligned}$$

Comme la matrice de passage des ν_i aux μ_i est unimodulaire, la première partie du théorème est prouvée.

3) $\mu_o = \mu_1 = \ldots = \mu_{p-2} = 0$ équivaut à :

$$\nu_o = \nu_1 = \ldots = \nu_{p-1} = 0$$

donc à $\text{Div}\ (\varphi) = 0$, donc à $\varphi \in \overline{k}^*$

4) Solutions polynomiales dans $k[X]$

Dans ce paragraphe, on suppose que la caractéristique de k est nulle.

4.1) Il est clair que le diviseur :

$$R = \infty_1 + \ldots + \infty_{p-1} - (p-1)\infty_o$$

est rationnel sur k, sa classe est donc un point de J rationnel sur k.

Théorème 2.- On suppose que p est premier et que $[k(\xi) : k] = p-1$.

Dans ces conditions l'équation (E_p) admet une solution non triviale $(U_o, U_1, \ldots, U_{p-1}) \in (k[X])^p$ ssi le point R est d'ordre fini sur J.

Démonstration : On désigne par k' le corps $k(\zeta)$ et par $\zeta \overset{\tau}{\longmapsto} \zeta^i$ un générateur de $\mathrm{Gal}\,({}^{k'}/_{k})$. τ se prolonge à $k'(X,Y)$ en posant $\tau(X) = X$ et $\tau(Y) = Y$. En reprenant les notations de la démonstration du théorème 1, on a :

$$\tau(\mathrm{Div}\ \varphi) = \mathrm{Div}\ (\tau\varphi) = \nu_o \infty_o + \nu_1 \infty_i + \nu_2 \infty_{2i} + \ldots + \nu_{p-1} \infty_{(p-1)i}$$

Puisque le diviseur de φ est rationnel, on a :

$$\nu_1 = \nu_i = \nu_{i^2} = \ldots = \nu_{i^{p-2}}$$

et comme i engendre $({}^{\mathbb{Z}}/_{p\mathbb{Z}})^*$ on a en fait :

$$\nu_1 = \nu_2 = \ldots = \nu_{p-1}$$

Finalement :

$$\mathrm{Div}\ (\varphi) = \nu_1 [\infty_1 + \ldots + \infty_{p-1} - (p-1)\infty_o]$$

d'où :

$$\nu_1 R = 0$$

sur la jacobienne J (c'est une condition nécessaire et suffisante).

D'autre part, on a déjà vu que $\nu_1 = 0$ équivaut à $\varphi \in k^*$.

4.2) Le théorème suivant est intermédiaire entre les théorèmes 1 et 2.

Définition : On désigne par Ω l'ensemble $\{\infty_o, \infty_1, \ldots, \infty_p\}$ et par ω_i, $i = 0, \ldots, s$, les orbites de Ω pour l'action de $\mathrm{Gal}\,(k(\zeta)/_k)$, en convenant de poser $\omega_o = \{\infty_o\}$. On désignera par $|\omega_i|$ le cardinal de ω_i.

Alors pour $i \in \{0,1,\ldots,s\}$ les diviseurs $R_i = \sum_{\infty_m \in \omega_i} \infty_m$ sont rationnels sur k.

Théorème 3.- L'équation (E_p) admet une solution non triviale $(U_o,U_1,\ldots,U_{p-1}) \in (k[X])^p$ ssi il existe $(n_o,\ldots,n_s) \in \mathbb{Z}^{s+1}$, non tous nuls, tels que :

$$n_1(R_1 - |\omega_1|R_o) + \ldots\ n_s(R_s - |\omega_s|R_o) = 0$$

sur la jacobienne J.

La démonstration se base sur des remarques analogues à celles qui ont été utilisées dans la démonstration du théorème 2.

Exemples :

1) Supposons $p = 2$, alors on voit que $\infty_1 - \infty_o$ doit être un point d'ordre fini (Schinzel).

2) Supposons que $p = 2q$, avec q premier impair et $k = \mathbb{Q}$. Les racines $p^{\text{ième}}$ de l'unité dans $\bar{k}$ sont

$$1,\ \zeta,\ldots,\ \zeta^{q-1},\ -1,\ -\zeta,\ldots,\ -\zeta^{q-1}$$

$\mathrm{Gal}\,(k(\zeta)/k) \cong (\mathbb{Z}/q\mathbb{Z})^*$, c'est un groupe cyclique dont on désignera par i un générateur. Les orbites ω_m sont :

$$\omega_o = \{\infty_o\}, \qquad \omega_q = \{\infty_q\}$$

$$\omega_1 = \{\infty_1,\infty_i,\infty_{i^2},\ldots\}$$

$$\omega_{q+1} = \{\infty_{q+1},\omega_{i(q+1)},\infty_{i^2(q+1)},\ldots\}$$

(∞_{q+1} ne peut pas appartenir à ω_1 car i est impair et $q+1$ est pair).

On a donc :

$$R_o = \infty_o$$

$$R_q = \infty_\infty$$

$$R_1 = \infty_1+\infty_i+\infty_{i^2}+\ldots$$

$$R_{q+1} = \infty_{q+1}+\infty_{i(q+1)}+\infty_{i^2(q+1)}+\ldots$$

La condition géométrique est donc :

$$\ell_1(R_q-R_o) + \ell_2(R_1 - (q-1)R_o) + \ell_3(R_{q+1} - (q-1)R_o) = 0 \quad \text{avec } (\ell_1,\ell_2,\ell_3) \in \mathbb{Z}^3 .$$

5) Exemples

Dans tout ce paragraphe $k = \mathbb{Q}$.

5.1) Le cas $p = 2$ a été traité par Schinzel (voir aussi II,3)

5.2) Dans le cas $p = 3$, l'équation de Pell est :

$$(E_3) \qquad U_o^3 + U_1^3 D + U_2^3 D^2 - 3U_o U_1 U_2 D = C^{te}$$

Eugène Dubois a trouvé deux familles de polynômes D pour lesquelles (E_3) admet une solution non triviale.

Première famille :

$$D_1 = P(P^2Q^6 + 3PQ^3 + 3)$$

avec P et Q unitaires, de degrés p et q, tels que $p+2q>0$. Une solution non triviale est :

$$(1 + PQ^3, -Q, 0)$$

Deuxième famille :

$$D_2 = P(P^2Q^3 + 3)$$

avec P et Q unitaires, de degrés p et q, tels que $p+q > 0$. Une solution non triviale est :

$$(1, PQ^2, -Q)$$

Lemme : Lorsque P et Q sont dans $\mathbb{Z}[X]$ et lorsque $P \equiv X^p$, $Q \equiv X^q$ (modulo 3), alors le polynôme D n'a pas de racines multiples lorsque P n'en a pas.

Démonstration : Dans les deux cas on peut écrire $D = PR$, avec $R = P^2Q^6 + 3PQ^3 + 3$ (resp. $P^2Q^3 + 3$).

Il est clair que P et R sont premiers entre eux, il suffit donc de montrer que R n'a pas de racines multiples. En fait, on voit facilement, en appliquant le critère d'Eisenstein à R et au nombre 3, que R est irréductible.

Théorème 4.- On suppose que P et Q sont choisis de telle sorte que D_1 et D_2 n'admettent pas de racines multiples. Si on désigne par J_1 (resp. J_2) la jacobienne de la courbe associée à D_1 (resp. D_2) le point $\infty_1 + \infty_2 - 2\infty_o$ est annulé par $p + 3q$ (resp. $2p + 3q$) sur J_1 (resp. J_2).

Démonstration :

Les deux cas étant analogues, nous nous limiterons au premier cas. Posons :

$$\varphi = 1 + PQ^3(X) - YQ(X) = \frac{X'^{p+3q} + P^*Q^{*3}(X') - Y'Q^*(X')}{X'^{p+3q}}$$

où P^* et Q^* désignent les polynômes réciproques de P et Q, et :

$$\tilde{\varphi} = X'^{p+3q}\,\varphi$$

Alors on voit qu'il existe $m > 0$ tel que [1]

$$\mathrm{Div}^+(\tilde{\varphi}) = m\infty_o,\ \mathrm{Div}^+(\sigma(\tilde{\varphi})) = m\infty_2,\ \mathrm{Div}^+(\sigma^2(\tilde{\varphi})) = m\infty_1$$

Comme : $\tilde{\varphi} \cdot \sigma(\tilde{\varphi}) \cdot \sigma^2(\tilde{\varphi}) = \lambda X'^{3(p+3q)}$ et :

$$\mathrm{Div}^+(X') = \infty_o + \infty_1 + \infty_2$$

on voit que $m = 3(p+3q)$.

Comme $\mathrm{Div}\,(\varphi)$ ne dépend que des places à l'infini, on a :

$$\begin{aligned}\mathrm{Div}\,(\varphi) &= \mathrm{Div}\,(\tilde{\varphi}) - (p+3q)\,\mathrm{Div}\,(X') \\ &= (p+3q)(2\infty_o - \infty_1 - \infty_2)\end{aligned}$$

(1) Div^+ désigne $\sup(0, \mathrm{Div})$.

II. PARTIE ANALYTIQUE

1) Calcul de $D^{1/p}$

Dans tout ce qui suit, on désignera par $k((\frac{1}{X}))$ le corps des séries formelles en $\frac{1}{X}$; c'est-à-dire des expressions $F(X)$ du type :

$$F(X) = \sum_{m \geqslant m_o} a_m X^{-m}$$

Lorsque $F(X) \neq 0$, on suppose $a_{m_o} \neq 0$ et on dit que $-m_o$ est le degré de F. Lorsque $F = 0$, on pose degré $F = -\infty$.

Dans ces conditions, il est clair que l'on a :

$$\begin{cases} \deg(F_1 F_2) = \deg F_1 + \deg F_2 \\ \deg(F_1 + F_2) \leqslant \deg F_1 + \deg F_2 \end{cases}$$

Lorsque $a_{m_o} = 1$, on dit que F est unitaire.

On suppose toujours que la caractéristique de k ne divise pas p.

Proposition.- L'équation :

$$Y^p = D(X)$$

admet une solution unitaire de degré n dans $k((\frac{1}{X}))$.

Démonstration : Posons $D(X) = X^{pn}[1 + \frac{1}{X} R(\frac{1}{X})]$ où $R(\frac{1}{X})$ est un polynôme en $\frac{1}{X}$ de degré $pn-2$. Alors la formule du binôme de Newton permet de définir (parce que la caractéristique de k ne divise pas p) un élément Δ de $k((\frac{1}{X}))$ dont la puissance $p^{\text{ième}}$ est bien D, à savoir :

$$\Delta(X) = X^n \left[\sum_{i=0}^{\infty} \binom{\frac{1}{p}}{i} X^{-i} R^i(\frac{1}{X}) \right]$$

2) Groupe des solutions polynomiales de l'équation de Pell

On cherche des éléments :

$$\varphi = U_o(X) + U_1(X)Y + \ldots + U_{p-1}(X) Y^{p-1}$$

avec $U_i(X) \in \overline{k}[X]$ satisfaisant à :

$$(E_p) \qquad N(\varphi) = \varphi.\sigma(\varphi) \ \ldots \ \sigma^{p-1}(\varphi) = \mu$$

avec $\mu \in \bar{k}^*$.

Définition.- On dira que deux solutions φ_1 et φ_2 de (E_p) sont équivalentes ssi il existe $\lambda \in k^*$ tel que $\varphi_1 = \lambda\varphi_2$.

On supposera seulement que le polynôme unitaire $D(X)$ est tel que $Y^p - D(X)$ est irréductible dans $k[X,Y]$, ce que l'on désignera sous le nom d'hypothèse faible.

Dans la suite μ_p désignera le groupe des racines $p^{\text{ièmes}}$ de l'unité dans $\bar{k}$.

Théorème 4.- On suppose que l'hypothèse faible est vérifiée.

1) Si φ_1 et φ_2 sont deux solutions de (E_p) alors $\varphi_1\varphi_2^{-1}$ est encore une solution de (E_p).

2) La loi de multiplication des solutions de l'équation de Pell est compatible avec la relation d'équivalence ci-dessus.

3) Le groupe $\mathcal{G}$ des classes d'équivalence est un groupe abélien libre de rang $\leqslant d(k)$ où $d(k)+1$ désigne le nombre d'orbites de μ_p sous l'action de $Gal(k(\zeta)/k)$.

Remarque : avec les notation du théorème 3, on a $d(k) = s$.

Démonstration : Nous nous limiterons à le dernière assertion car les deux premières sont évidentes.

Posons $$h(\varphi) = U_o(X)+U_1(X)\Delta(X) +\ldots+ U_{p-1}(X)\Delta^{p-1}(X)$$

et $$L(\varphi) = (\deg h(\varphi), \deg h\circ\sigma(\varphi) , \ldots, \deg h\circ\sigma^{p-1}(\varphi)).$$

L est un homomorphisme $\mathcal{G} \longrightarrow \mathbb{Z}^p$ dont l'image est contenue dans l'hyperplan d'équation :

$$X_o + X_1 +\ldots+ X_{p-1} = 0$$

Supposons que $\varphi \in \operatorname{Ker} L$, alors pour tout $i = 0,1,\ldots,p-1$ on a :

$$\deg(U_o+\zeta^i U_1\Delta +\ldots+ \zeta^{i(p-1)} U_{p-1}\Delta^{p-1}) = 0$$

En multipliant ces relations par ζ^{ij} et en additionnant, on a :

$$\deg(U_j\ \Delta^j) \leqslant 0$$

pour $j = 0,1,\ldots\ p-1$.

Puisque les U_i sont des polynômes et puisque $n > 0$, on en déduit que :

$$(U_o,U_1,\ldots,U_{p-1}) = (\lambda,0,\ldots\ 0)$$

avec $\lambda \in \bar{k}^*$, donc Ker L est la classe d'équivalence des solutions triviales.

Si d'autre part on désigne par ζ^{n_i}, $i \in \{0,1,\ldots,s\}$, un système de représentants des orbites de μ_p sous l'action de $Gal(k(\zeta)/k)$, l'image de L se trouve dans l'intersection des hyperplans dont les équations sont

$$X_\nu = X_{n_i}, \qquad i \in \{0,1,\ldots,s\}$$

avec $\nu \neq n_i$.

Le nombre d'équations linéairement indépendantes que l'on obtient est ainsi :

$$\sum_{i=0}^{s} (|\omega_i|-1) = p - [d(k)+1]$$

Donc l'image de $\mathcal{G}$ (qui lui est isomorphe) est un groupe libre de rang $\leqslant p - [p-d(k)] = d(k)$.

Corollaire 1.- On désigne par $\mathcal{R}$ le groupe libre engendré par $R_1 - |\omega_1|R_o,\ldots,R_s - |\omega_s|R_o$ et par $\mathcal{P}_o$ le groupe engendré par les diviseurs des éléments de $k[X,Y]$, alors $\mathcal{G}$ est isomorphe à $\mathcal{R} \cap \mathcal{P}_o$.

Démonstration : En effet, on a :

$$\text{degré}[h\circ\sigma^i(\varphi)] = -v_{\infty_{-i}}(\varphi)$$

où $v_{\infty_{-i}}(\varphi)$ désigne la valuation de φ au point ∞_{p-i}.

Comme l'application :

$$(X_o,\ldots,X_i,\ldots,X_{p-1}) \longmapsto (-X_o,\ldots,-X_{-i},\ldots,-X_{-(p-1)})$$

est un isomorphisme de $\mathbb{Z}$-modules, on en déduit que l'image de $\mathcal{G}$ par L dans $\mathbb{Z}^p$ est isomorphe à l'image de $\mathcal{G}$ par l'application $\varphi \longmapsto \text{div}(\varphi)$ dans $\mathcal{R} \cap \mathcal{P}_o$.

Corollaire 2 (théorème de dualité).- Soit $R = {}^{\mathcal{R}}/_{\mathcal{R} \cap \mathcal{P}_o}$ et T le sous-groupe de torsion de R, alors on a :

$$\text{rang}({}^{R}/_{T}) + \text{rang}(\mathcal{Q}) = d(k)$$

Démonstration :

En effet $\mathcal{R} \cong \mathbb{Z}^{d(k)}$.

En appliquant le théorème des diviseurs élémentaires, on a :

$$\mathcal{R} \cap \mathcal{P}_o = \mathbb{Z}a_1 e_1 \oplus \ldots \oplus \mathbb{Z}a_{d(k)}\, e_{d(k)}$$

où $e_1, \ldots, e_{d(k)}$ est une certaine base de $\mathcal{R}$ et où $a_1 | a_2 | \ldots | a_{d(k)}$.

Supposons que a_t soit le dernier diviseur élémentaire non nul, alors :

$$R \cong {}^{\mathbb{Z}}/_{a_1\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}/_{a_t\mathbb{Z}} \times \mathbf{Z}^{d(k)-t}$$

donc $$T \cong {}^{\mathbb{Z}}/_{a_1\mathbf{Z}} \times \ldots \times {}^{\mathbb{Z}}/_{a_t\mathbf{Z}}$$

et $${}^{R}/_{T} \cong \mathbf{Z}^{d(k)-t}$$

Par suite :

$$\text{rang}({}^{R}/_{T}) + \text{rang}(\mathcal{R} \cap \mathcal{P}_o) = d(k)$$

et comme $\mathcal{R} \cap \mathcal{P}_o \cong \mathcal{Q}$, le théorème est démontré.

Remarque : Sous l'hypothèse forte de la première partie (D n'a pas de racines multiples), $\mathcal{P}_o$ est le groupe des diviseurs principaux de K.

3) Le cas $p = 2$

Tout ce qui suit est une reformulation de Shockley "Continued fractions and Pell's equation" ch. 12.

3.1) Nous allons refaire d'abord la théorie des fractions continues dans $k((\frac{1}{X}))$.

Dans toute la suite α sera un élément de $k((\frac{1}{X})) \setminus k(X)$ de degré $\geqslant 0$. Si $\alpha = \sum_{m \geqslant m_o} a_m X^{-m}$, nous appellerons partie entière de α, et nous noterons $[\alpha]$, le polynôme :

$$[\alpha] = \sum_{m_o \leqslant m \leqslant 0} a_m X^{-m}$$

Nous appellerons partie fractionnaire de α le nombre $\alpha - [\alpha]$ et nous le noterons $\{\alpha\}$. Il est clair que :

$$\text{degré } \{\alpha\} < 0$$

En posant $a_i = [\alpha_{i-1}]$ et $\alpha_i = \frac{1}{\{\alpha_i\}}$ on construit la chaîne :

$$(1) \qquad \alpha = \langle a_1, \alpha_1 \rangle = \langle a_1, a_2, \alpha_2 \rangle = \ldots$$

et nous poserons :

$$\langle a_1 \rangle = \frac{P_1}{Q_1}, \quad \langle a_1, a_2 \rangle = \frac{P_2}{Q_2}, \text{ etc...}$$

P_n et Q_n étant les habituels polynômes en a_1, a_2,... déterminés par les relations :

$$(2) \qquad \begin{cases} P_o = 1, \quad Q_o = 0 \\ P_1 = a_1, \quad Q_1 = 1 \\ \text{----------} \\ P_i = a_i P_{i-1} + P_{i-2}, \quad Q_i = a_i Q_{i-1} + Q_{i-2} \end{cases}$$

qui entraînent :

$$(3) \qquad Q_{i+1} P_i - Q_i P_{i+1} = (-1)^i$$

Dans la suite nous prendrons $\alpha = \Delta$, on a donc : $\deg(\alpha) = \deg(a_1) = n \geq 0$.

Proposition 1.- On suppose que degré $(\alpha) \geqslant 0$. Alors pour tout $i \geqslant 2$ on a :

1) $\deg(a_i) > 0$

2) $\begin{cases} \deg(Q_i) = \deg(a_2) + \ldots + \deg(a_i) \\ \deg(P_i) = \deg(a_1) + \ldots + \deg(a_i) \end{cases}$

3) $\deg\left(\alpha - \dfrac{P_i}{Q_i}\right) = \deg\left(\dfrac{1}{Q_i Q_{i+1}}\right)$

4) $\deg(Q_i\alpha - P_i) - \deg(Q_{i+1}\alpha - P_{i+1}) = \deg(a_{i+2})$

Démonstration :

1) $\deg(a_i) = -\deg(\alpha_{i-1}) > 0$

2) résulte des formules de récurrence (2)

3) D'après (1) on a :

$$\alpha = \langle a_1, \ldots, a_i, \alpha_i \rangle = \frac{P_i(a_1, \ldots, a_i + \alpha_i^{-1})}{Q_i(a_1, \ldots, a_i + \alpha_i^{-1})}$$

D'après (2) cela s'écrit :

$$\alpha = \frac{(a_i + \alpha_i^{-1})P_{i-1} + P_{i-2}}{(a_i + \alpha_i^{-1})Q_{i-1} + Q_{i-2}} = \frac{P_i + \alpha_i^{-1} P_{i-1}}{Q_i + \alpha_i^{-1} Q_{i-1}}$$

D'où :

$$\alpha - \frac{P_i}{Q_i} = \frac{P_i + \alpha_i^{-1} P_{i-1}}{Q_i + \alpha_i^{-1} Q_{i-1}} - \frac{P_i}{Q_i} = \frac{\alpha_i^{-1}(P_{i-1}Q_i - P_i Q_{i-1})}{Q_i(Q_i + \alpha_i^{-1} Q_{i-1})}$$

et compte-tenu de (3) :

$$\alpha - \frac{P_i}{Q_i} = \frac{(-1)^{i-1}}{Q_i (Q_{i-1} + \alpha_i Q_i)}$$

d'où :

$$\deg\ (\alpha - \frac{P_i}{Q_i}) = -\deg\ Q_i - \deg\ (Q_{i-1} + \alpha_i Q_i)$$

Comme $\deg\ (Q_{i-1}) < \deg\ Q_i$ et $\deg\ (\alpha_i) = \deg\ (a_{i+1}) > 0$, on a :

$$\deg\ (Q_{i-1} + \alpha_i Q_i) = \deg\ (\alpha_i Q_i) = \deg\ (a_{i+1} Q_i) = \deg\ (a_{i+1} Q_i + Q_{i-1})$$
$$= \deg\ (Q_{i+1})$$

d'où le résultat.

4) Il résulte de 3) que :

$$\deg(Q_i\alpha - P_i) - \deg(Q_{i+1}\alpha - P_{i+1}) = \deg\ (\frac{1}{Q_{i+1}}) - \deg\ (\frac{1}{Q_{i+2}})$$
$$= \deg\ (Q_{i+2}) - \deg\ (Q_{i+1}) = \deg\ (a_{i+2})$$

et ceci termine la démonstration.

Nous laisserons au lecteur le soin de démontrer que le développement en fraction continue de α, avec $\deg\ (a_i) > 0$ pour $i \geqslant 2$, est unique. Et nous le renvoyons à la thèse de Bernard de Mathan pour la démonstration du fait que les convergentes de α sont les meilleures approximations de α, la notion de meilleure approximation étant définie comme suit :

Définition : Soient deux polynômes A et B ($\neq 0$) de k[X]. On dira que $\frac{A}{B}$ est une meilleure approximation de α ssi pour tous A' et B' ($\neq 0$) de k[X], avec $\deg B' \leqslant \deg B$, la condition : $\deg (B'\alpha - A') \leqslant \deg (B\alpha - A)$ entraîne $\frac{A'}{B'} = \frac{A}{B}$.

Nous terminerons les généralités par une dernière proposition :

Proposition 2.- On suppose toujours que $\deg\ (\alpha) \geqslant 0$.
Soient deux polynômes A et B ($\neq 0$) de k[X], alors la condition $\deg\ (B\alpha - A) < \deg\ (\frac{1}{B})$ entraîne que $\frac{A}{B}$ est une convergente de α.

Démonstration :

Supposons que $\deg (B\alpha - A) < \deg (\frac{1}{B})$. Développons $\frac{A}{B}$ (supposée irréductible) en fraction continue :

$$\frac{A}{B} = <a'_1, \ldots, a'_m>$$

et on peut supposer que $A = P_m$ et $B = Q_m$. Définissons β par :

$$\alpha = <a'_1, \ldots, a'_m + \beta^{-1}> = \frac{\beta P_m + P_{m-1}}{\beta Q_m + Q_{m-1}}$$

alors, on a :

$$\alpha - \frac{A}{B} = \frac{\beta P_m + P_{m-1}}{\beta Q_m + Q_{m-1}} - \frac{P_m}{Q_m} = \frac{(-1)^m}{Q_m (\beta Q_m + Q_{m-1})}$$

d'où (compte-tenu de l'hypothèse) :

$$\deg (B\alpha - A) = -\deg (\beta Q_m + Q_{m-1}) < -\deg Q_m$$

soit :

$$\deg (\beta Q_m + Q_{m-1}) > \deg Q_m$$

ce qui entraîne que :

$$\deg \beta > 0$$

on peut donc développer β en fraction continue :

$$\beta = <b_1, b_2 \ldots>$$

Si l'on pose $\gamma = <a'_1, \ldots, a'_m, b_1, b_2, \ldots>$ alors $\gamma = <a'_1, \ldots, a'_m + \beta^{-1}> = \alpha$ et l'unicité du développement en fraction continue montre que $a'_i = a_i$ pour $1 \leqslant i \leqslant m$. Ainsi $\frac{A}{B}$ est bien la $m^{\text{ième}}$ convergente de α.

Corollaire.- Si l'équation de Pell :

$$U_o^2 - U_1^2 D = \lambda$$

admet une solution polynomiale (U_o, U_1) telle que $\deg (U_o - U_1 \Delta) < 0$, alors $\frac{U_o}{U_1}$ est une convergente de Δ.

Démonstration :

Puisque $\deg (U_o - U_1\Delta) < 0$, on a :

$$\deg U_o = \deg (U_1\Delta)$$

d'où :

$$\deg (U_o - U_1\Delta) = -\deg (U_o + U_1\Delta) = -\deg (U_1\Delta) < \deg \left(\frac{1}{U_1}\right)$$

on peut donc appliquer la proposition 2.

3.2) Irrationnelles quadratiques

On travaillera dans le corps $k((\frac{1}{X}))$ et on notera $\alpha \longmapsto \alpha'$ le prolongement de l'automorphisme $\sigma : K \to K$.

Pour ne pas s'écarter du but, on considérera le développement de $\alpha = \Delta$. On a donc :

$$\alpha_o = \alpha, \qquad \alpha'_o = \alpha' = -\Delta$$

d'où : $\deg (\alpha_o) = \deg (\alpha'_o) = n$

et α et α' sont racines d'un polynôme $A_oX^2 + B_oX + C_o$ avec :

$$\begin{cases} A_o = 1 \\ B_o = 0 \\ C_o = -D \end{cases}$$

Pour $i \geqslant 1$, nous poserons :

$$(4) \qquad \begin{cases} A_i = P_i^2 - DQ_i^2 \\ B_i = 2P_iP_{i-1} - 2DQ_iQ_{i-1} \\ C_i = P_{i-1}^2 - DQ_{i-1}^2 \end{cases}$$

on a alors :

Proposition 3

1) α_i et α'_i sont racines de $A_iX^2 + B_iX + X_i$.

2) Pour tout $i \geqslant 1$ on a :

$$B_i^2 - 4A_iC_i = 4D$$

$$\begin{cases} \deg(A_i) = n - \deg(a_{i+1}) \\ \deg(B_i) = n \\ \deg(C_i) = n - \deg(a_i) \end{cases}$$

Démonstration : Nous nous bornerons à démontrer les assertions concernant le degré car le reste est classique.

a) Puisque :

$$\deg\left(\alpha - \frac{P_i}{Q_i}\right) = \deg\left(\frac{1}{Q_iQ_{i+1}}\right) < 0$$

on voit que :

$$\deg\left(\alpha + \frac{P_i}{Q_i}\right) = n$$

On déduit de (4) que :

$$A_i = Q_i^2\left(\frac{P_i}{Q_i} + \alpha\right)\left(\frac{P_i}{Q_i} - \alpha\right)$$

d'où :

$$\deg(A_i) = 2\deg Q_i + \deg\Delta + \deg\left(\frac{1}{Q_iQ_{i+1}}\right)$$

et la proposition 1 donne le résultat.

On calcule de même le degré de C_i.

b) Pour B_i, on a :

$$B_i^2 = 4A_iC_i + 4D$$

et comme $\deg(A_iC_i) = 2n - \deg(a_i) - \deg(a_{i+1}) < 2n$

on en déduit que :

$$2\deg B_i = \deg D = 2n$$

Corollaire.- $\deg (A_i) = 0 \iff \deg (a_{i+1}) = n$

Définition : On dira que le développement de Δ est pseudo-périodique ssi l'un des α_i est entier pour $i > 0$, et on appellera pseudo-période de Δ le plus petit $i > 0$ tel que α_i soit entier.

Proposition 4.- Pour $i \geqslant 1$, on a :

1)
$$\alpha_i = \frac{b_i \pm \Delta}{c_i}$$

avec $b_i = -\frac{1}{2} B_i$, $c_i = A_i$

2)
$$\begin{cases} \deg (\alpha_i) = \deg (a_{i+1}) > 0 \\ \deg (\alpha_i') = -\deg (a_i) < 0 \end{cases}$$

Démonstration :

a) D'après la proposition 3 on sait que α_i et α_i' sont racines de $A_i X^2 + B_i X + C_i$, d'où :

$$\begin{cases} \alpha_i = \dfrac{-B_i \pm 2\Delta}{2A_i} = \dfrac{b_i \pm \Delta}{c_i} \\ \alpha_i' = \dfrac{b_i \mp \Delta}{c_i} \end{cases}$$

b) Comme $[\alpha_i] = a_{i+1}$, on a $\deg \alpha_i = \deg a_{i+1} > 0$, comme $\alpha_i \alpha_i' = \dfrac{C_i}{A_i}$ on a :

$$\deg \alpha_i' = \deg \frac{C_i}{A_i} - \deg a_{i+1} = -\deg a_i$$

Théorème.- L'équation de Pell :

$$(E_2) \qquad U_o^2 - U_1^2 D = \lambda$$

a des solutions non triviales ssi Δ admet un développement pseudo-périodique.

Démonstration :

1) Supposons que (U_o, U_1) soit une solution non triviale de (E_2), alors il existe $i > 0$ tel que

$$\frac{U_o}{U_1} = \frac{P_i}{Q_i}$$

d'après le corollaire à la proposition 2.

D'après les relations (4) on voit que α_i est entier.

2) La réciproque est immédiate.

Corollaire 1.- La solution fondamentale de (E_2) est (P_π, Q_π) où π désigne la pseudo-période de Δ.

Corollaire 2.- Si ℓ désigne l'ordre de $\infty_1 - \infty_o$ sur J et π la pseudo période de Δ, on a :

$$\pi + n - 1 \leqslant \ell \leqslant 1 + \pi(n-1)$$

Démonstration :

Nous avons :

$$P_\pi^2 - Q_\pi^2 D = \lambda$$

Si nous posons :

$$\varphi = P_\pi - Q_\pi Y$$

on trouve avec la méthode de I, 5 :

$$\text{Div}(\varphi) = (\deg P_\pi)(\infty_o - \infty_1)$$

or, d'après la proposition 1 :

$$\deg P_\pi = \deg a_1 + \ldots + \deg a_\pi$$

Comme $\deg a_1 = n$ et $\deg a_i < n$ pour $1 < i \leqslant \pi$, on a :

$$n + \pi - 1 \leqslant \deg P_\pi \leqslant n + (\pi-1)(n-1)$$

et, puisque $\deg P_\pi$ est minimal, $\deg P_\pi = \ell$, d'où :

$$n+\pi-1 \leqslant \ell \leqslant 1+\pi(n-1)$$

Corollaire 3 .- Si $n = 2$, $\ell = \pi+1$

Références

M. DEURING .- Lectures on the Theory of Algebraic.
Functions of one Variable.
Springer, Lecture Notes 314.

B. de MATHAN .- "Approximations diophantiennes dans un corps local"
1968 (Thèse), Université de Caen.

A. SCHINZEL .- "On some problems of the arithmetical theory of
continued fractions"
Acta Arith. 6 (1961) S. 393-413
" " II ibid 7 (1962) S. 287-298.

J.E. SHOCKLEY .- Introduction to number theory.
Holt, Rinehart & Wilson.

(Signalons aussi un travail récent sur un sujet voisin) :

N. NEUBRAND .- "Sharen quadratischen Zahlkörper mit gleichgebauten
Einheiten".
Acta Arithmetica XXXIX (1981) S. 125-132.

APPENDICE À "ÉQUATION DE PELL ET POINTS D'ORDRE FINI"

Mireille LOZACH

Dans le cas $p=2$, on peut démontrer quelques autres propriétés :

Proposition 1.- Pour $i\geqslant 0$, on a $\alpha_i = \dfrac{b_i+(-1)^i\Delta}{c_i}$, et les couples (b_i,c_i) peuvent être déterminés à partir de $(b_o,c_o) = (0,1)$ grâce aux relations $b_{i+1} = b_i - a_{i+1}c_i$ et $c_ic_{i+1} = b_{i+1}^2 - D$, valables pour tout $i\geqslant 0$.

Démonstration : Pour $i=0$, $\alpha_o = \Delta = \dfrac{0+(-1)^o\Delta}{1}$ est bien vérifié.

Pour $i\geqslant 1$, on sait que $\Delta = \dfrac{P_i\alpha_i+P_{i-1}}{Q_i\alpha_i+Q_{i-1}}$, et que $\alpha_i = \dfrac{b_i+\varepsilon_i\Delta}{c_i}$, où $\varepsilon_i = \pm 1$.

On en déduit les relations $\begin{cases} P_ib_i+P_{i-1}c_i = Q_i\,\varepsilon_iD \\ Q_ib_i+Q_{i-1}c_i = P_i\,\varepsilon_iD \end{cases}$, dont on déduit la relation

$c_i = \varepsilon_i(P_i^2-D\,Q_i^2)(-1)^i$, et donc $\varepsilon_i = (-1)^i$, car on sait que $c_i = A_i = P_i^2-D\,Q_i^2$.

Pour $i\geqslant 1$, les relations $b_{i+1} = b_i-a_{i-1}c_i$ et $c_ic_{i+1} = b_{i+1}^2-D$ se déduisent alors immédiatement de $\alpha_i = a_{i+1}+\alpha_{i+1}^{-1}$.

Proposition 2.- Si le développement de Δ est pseudo-périodique (au sens défini plus haut), il est également périodique (au sens habituel du terme), la vraie période de α étant égale à une ou deux fois la pseudo-période définie plus haut.

Démonstration : Si Δ est de pseudo période k, k est le plus petit indice strictement positif tel que c_k soit de degré 0.

1er cas $(-1)^kc_k=1$. On a alors $\alpha_k = \Delta+(-1)^kb_k = a_1+(-1)^kb_k+\alpha_1^{-1}$, soit donc $\Delta = \langle a_1,a_2,\ldots,a_k,a_1+(-1)^kb_k\rangle$

Δ est bien vraiment périodique, de période k.

2ème cas $(-1)^kc_k\neq 1$. Les $(k+1)$ égalités $\alpha_i = a_{i+1}+\alpha_{i+1}^{-1}$ pour $0\leqslant i\leqslant k$, donnent par l'automorphisme $\sigma : \alpha_i' = a_{i+1}+(\alpha_{i+1}')^{-1}$, pour $0\leqslant i\leqslant k$, soit encore : $(-\alpha_{i+1}')^{-1} = a_{i+1}-\alpha_i'$, pour $0\leqslant i\leqslant k$.

Or $\alpha'_o = -\Delta$ et $\deg((-\alpha'_{i+1})^{-1}) = \deg a_{i+1} > 0$, pour $0 \leqslant i \leqslant k$.

On en déduit que le début du développement de $(-\alpha'_{k+1})^{-1}$ est $-\alpha'_{k+1} = <a_{k+1}, a_k, \ldots, a_2, a_1+\Delta>$ où $\deg(a_i+\Delta) = \deg(2a_i) > 0$.

Or $(-\alpha'_{k+1})^{-1} = \dfrac{c_{k+1}}{-b_{k+1}+(-1)^{k+1}\Delta} = \dfrac{-b_{k+1}+(-1)^k\Delta}{c_k}$, où c_k est de degré 0, et $\alpha_k = \dfrac{b_k+b_{k+1}}{c_k} + (-\alpha'_{k+1})^{-1}$ a donc pour début de développement :

$$\alpha_k = < \frac{b_k+b_{k+1}}{c_k} + a_{k+1}, a_k, \ldots, a_1+\Delta >.$$

Le début du développement de α_k étant également $\alpha_k = < a_{k+1}, \alpha_{k+1} >$, on doit avoir $b_k = -b_{k+1} = \dfrac{a_{k+1}c_k}{2}$. Alors :

$$\Delta = < a_1, a_2, \ldots, a_k, \alpha_k > = < a_1, \overline{a_2, \ldots, a_{k+1}, \ldots, a_2, 2a_1} >$$

et Δ est bien <u>vraiment</u> périodique, de période $2k$.

(Cette dernière démonstration peut également s'appliquer au premier cas, mais on trouve alors deux fois la période : si $(-1)^k c_k = 1$, on a donc les relations $a_2 = a_k$, $a_3 = a_{k-1}, \ldots$, et $a_{k+1} = 2a_1$).

<u>Proposition 3</u>.- Si Δ est pseudo périodique, de pseudo période k de <u>vraie</u> période $2k$, k est nécessairement impair.

<u>Démonstration</u> : Dans le deuxième cas de la proposition 2, on peut déduire le développement de $\alpha_k = \dfrac{b_k+(-1)^k\Delta}{c_k}$ de celui de Δ :

$$\alpha_k = < \frac{b_k}{c_k} + \frac{a_1}{(-1)^k c_k}, \overline{(-1)^k c_k a_2, \ldots, \frac{2a_1}{(-1)^k c_k}} > = < \frac{a_1}{(-1)^k c_k}, \overline{(-1)^k c_k a_2, \ldots, \frac{2a_1}{(-1)^k c_k}} >.$$

On a également $\alpha_k = < a_{k+1}, a_k, \ldots, a_1+\Delta >$, soit

$$\alpha_k = < \overline{a_{k+1}, a_k, \ldots, 2a_1, \ldots, a_k} >.$$

Donc $\dfrac{a_1}{(-1)^k c_k} = \dfrac{a_{k+1}}{2}$, et $b_k = (-1)^k a_1$, $\alpha_k = \dfrac{a_1+\Delta}{(-1)^k c_k}$.

Si k était pair, on aurait aussi $\dfrac{2a_1}{c_k^2} = \dfrac{a_{k+1}}{(-1)^k c_k} = [\alpha_{2k}] = 2a_1$, et donc $c_k^2 = 1$.

Puisque $(-1)^k c_k \neq 1$, on aurait alors $(-1)^k c_k = c_k = -1$. On en déduirait que $a_{\frac{k}{2}+1} = -a_{\frac{k}{2}+1}$, ce qui est impossible : k est bien impair.

Exemples 1) $\sqrt{x^2+1} = \langle x, \overline{2x} \rangle$ $\quad \alpha_1 = x+\Delta$, $\quad k=1$

2) $\sqrt{x^4+2x} = \langle x^2, \overline{x, 2x^2} \rangle$ $\quad \alpha_1 = \frac{x^2+\Delta}{2x}$, $\quad \alpha_2 = x^2+\Delta$, $\quad k=2$

3) $\sqrt{x^2+2} = \langle x, \overline{x, 2x} \rangle$ $\quad \alpha_1 = \frac{x+\Delta}{2}$, $\quad \alpha_2 = x+\Delta$, $\quad k=1$.

Dans les exemples 1) et 2), la "période" et la vraie période sont égales, k pouvant être pair ou impair.

Dans l'exemple 3), la vraie période est le double de la "période", et k est impair.

*

* *

Yves HELLEGOUARCH
et
Mireille LOZACH

Université de Caen
Département de Mathématiques
et de Mécanique
F-14032 Caen Cedex

ERGODICITY OF A CLASS OF CYLINDER FLOWS

P. Hellekalek

U.E.R. de Mathematiques
Université de Provence
3, place Victor Hugo
F-13331 Marseille Cedex 3
and
Institut für Mathematik
Universität Salzburg
Petersbrunnstraße 19
A-5020 Salzburg/Austria

Summary : Let $U = \mathbb{R}/\mathbb{Z}$ with Lebesgue measure and $\varphi(x) = 1_{[0,\beta[}(x) - \beta$, $0<\beta<1$. Let G denote the closed subgroup of $\mathbb{R}$ generated by $-\beta$ and $1-\beta$, either with Lebesgue measure in the case $G=\mathbb{R}$ or with Haar measure (counting measure) in the other cases.

Define $T_\varphi : UxG \to UxG$ by $T_\varphi(x,t)=(Tx,t+\varphi(x))$, where $T : U\to U$ is an element of a class of ergodic transformations arising from representations of real numbers to general bases (including the dyadic and p-adic representations).

In this paper the set of numbers β such that T_φ is ergodic on the product space UxG with respect to product measure is determined.

Introduction

Let $q = (q_i)_{i=1}^{\infty}$ be a sequence of integers $q_i \geq 2$. Let $\mathbb{A}(q)$ denote the compact Abelian group of q-adic integers (see [3] for details). The transformation $S: z \to z+1$ on $\mathbb{A}(q)$ is uniquely ergodic with respect to normalized Haar measure.

Let $U = \mathbb{R}/\mathbb{Z}$ and let m denote Lebesgue measure on U. Define $p(k) = q_1 \cdot \ldots \cdot q_k$ for $k = 1,2,\ldots$ and $p(0) = 1$. If

$$z = \sum_{i=0}^{\infty} z_i\, p(i) , \quad z_i \in \{0,1,\ldots,q_{i+1}-1\} ,$$

is an element of $\mathbb{A}(q)$, then $\phi: \mathbb{A}(q) \to U$,

$$\phi(z) = \sum_{i=0}^{\infty} z_i/p(i+1) \mod 1$$

is a measure preserving map from $\mathbb{A}(q)$ onto U. With the exception of a subset of Haar measure zero, ϕ is injective on $\mathbb{A}(q)$.

The q-adic representation of an element x of U,

$$x = \sum_{i=0}^{\infty} x_i/p(i+1) , \quad x_i \in \{0,1,\ldots,q_{i+1}-1\} ,$$

is unique under the condition that $x_i \neq q_{i+1}-1$ for infinitely many i. Therefore the following transformation $T: U \to U$ is well-defined:

$$T(x) = \phi(z+1) , \quad \text{where} \quad z = \sum_{i=0}^{\infty} x_i p(i).$$

T is ergodic with respect to m and $\phi \circ S = T \circ \phi$ a.e. on $\mathbb{A}(q)$. Further properties of T and a relation to irregularities of the distribution of generalized Halton sequences are established in [2].

For the following let

$$\varphi(x) = 1_{[0,\beta[}(x) - \beta,$$

where $0<\beta<1$. Let G denote the closed subgroup of $\mathbb{R}$ generated by $-\beta$ and $1-\beta$. For irrational β G is equal to $\mathbb{R}$, for rational β G is a group isomorphic to the group $\mathbb{Z}$ of integers. In the first case let h denote Lebesgue measure on $\mathbb{R}$, in the second case Haar measure (counting measure) on G.

The transformation $T_\varphi : U \times G \to U \times G$,

$$T_\varphi(x,t) = (Tx, t+\varphi(x))$$

preserves the product measure $m \times h$ on the product space $U \times G$.

We shall call a rational number $\beta = r/s$, $(r,s)=1$, <u>strictly</u> non-q-adic if every number k/s, $1 \leq k \leq s-1$, has infinitely many nonzero digits in its q-adic representation.

<u>Theorem :</u> Suppose the sequence $(q_i)_{i=1}^{\infty}$ is bounded. T_φ is ergodic with respect to $m \times h$ if and only if either β is irrational or β is strictly non-q-adic.

In the case where $T : U \to U$ is an irrational rotation $Tx = x+\theta \mod 1$ with θ irrational, ergodicity of T_φ in dependence of β is known, due to I. Oren [4]. Partial results had been obtained before by J.-P. Conze [1], K. Schmidt [5] and M. Stewart [6] (see also W.A. Veech [7]).

The Proof.

In the following X will denote the direct product of the two measure spaces (U,m) and (G,h) and $\mu = m \times h$ will stand for the product measure. Let $\varphi_k = \varphi + \varphi \circ T + \ldots + \varphi \circ T^{k-1}$, $k = 1,2,\ldots$.

Definition : An element c of G with the property $f(x,t+c)=f(x,t)$ μ-a.e. for any function f in $\{1_B : 1_B \circ T_\varphi = 1_B$, B a measurable subset of X$\}$ will be called a period of T_φ.

Remark : The set of periods of T_φ is a closed subgroup of G.

The following lemma shows how to obtain periods. It has an equivalent in Oren's proposition 1 (see [4]).

Lemma : Suppose there exist a sequence $(k_n)_{n=1}^{\infty}$ of positive integers and a sequence $(A_{k_n})_{n=1}^{\infty}$ of subsets of U such that

(i) $\varphi_{p(k_n)}$ is constant on A_{k_n}

(ii) $\lim_{n\to\infty} \varphi_{p(k_n)}(A_{k_n})$ exists

(iii) $\inf_n m(A_{k_n}) > 0$.

Then for any f in $\{1_B$: B a measurable subset of X$\}$ with $f \circ T_\varphi = f$ μ-a.e. it follows that $f(x,t+c) = f(x,t)$ μ-a.e. where $c = \lim_{n\to\infty} \varphi_{p(k_n)}(A_{k_n})$.

Proof : Comparison of the q-adic representations of x and Tx shows that

$| T^{p(k)}x - x | < 1/p(k)$

for all x in U and all k. Put $a_{k_n} = \varphi_{p(k_n)}(A_{k_n})$.

For any $f = 1_B$, B a measurable subset of X,

$$\lim_{n\to\infty} \int_{U\times G_N} | f(T^{p(k_n)}x,\ t+a_{k_n}) - f(x,t+c) | \, d\mu = 0, \quad G_N = G\cap[-N,N] \qquad (*)$$

for all $N > 0$. If

$$g_{k_n}(x,t) = \left| f(T^{p(k_n)}x,\ t+a_{k_n}) - f(x,t+c) \right| ,$$

then L^1-convergence of the sequence of functions $(g_{k_n})_{n=1}^{\infty}$ in (*) implies convergence a.e. for subsequences. By diagonalization one can find a subsequence $(k_n')_{n=1}^{\infty}$ such that

$$\lim_{n\to\infty} g_{k_n'}(x,t) = 0 \quad \mu\text{-a.e. on } X.$$

The very same arguments as those of Oren in his proposition 1 finish the proof.

Proof of the theorem : The q-adic representation of β, $0<\beta<1$, is given by

$$\beta = \sum_{i=0}^{\infty} \beta_i/p(i+1) , \quad \beta_i \in \{0,1,\ldots,q_{i+1}-1\} ,$$

infinitely many $\beta_i \neq q_{i+1}-1$, the latter being a uniqueness condition. Define

$$\beta(k) = \sum_{i=0}^{k-1} \beta_i/p(i+1) , \quad k = 1,2,\ldots .$$

Then $0 \leq \beta-\beta(k) < 1/p(k)$.

Let β have finite q-adic representation (i.e. $\beta_i \neq 0$ for finitely many i only). Then there exists a function g in the space $L^2(U,m)$ such that $\varphi = g - g\circ T$ m-a.e. (see [2]). If T_φ were ergodic on UxG then the transformation $(x,t) \to (Tx,\ t-\beta) = (Tx,\ t+\varphi(x) \bmod 1)$ on UxG/$\mathbb{Z}$ were a factor of T_φ and therefore ergodic. This contradicts the fact that the functional equation $h(Tx) = \chi(\varphi(x))\ h(x)$, χ a nontrivial character in the dual group of G/$\mathbb{Z}$, has a nontrivial measurable solution h, as follows from $\chi(\varphi(x)) = \chi(g(x))\ \chi(-g(Tx))$.

Hence T_φ is not ergodic if β has finite representation.

Assume from now on that β has infinite q-adic representation, that is, $\beta_i \neq 0$ for infinitely many i. Thus $0<(\beta-\beta(k))\ p(k)<1$. It will be shown that 1 is a period of T_φ.

For any x in U, exactly one of the points $T^j x$, $0\leq j\leq p(k)-1$, belongs to a given elementary q-adic interval $[a/p(k),\ (a+1)/p(k)[$, $0\leq a\leq p(k)-1$, of length $1/p(k)$. Hence the function $\varphi_{p(k)}$ takes only two values on U, $\varphi_{p(k)}(x) \in \{\beta(k)p(k) - \beta p(k),\ \beta(k)p(k)+1 - \beta p(k)\}$.

If

$A_k = \{x \in U: \varphi_{p(k)}(x) = (\beta(k)-\beta)p(k)\}$ and $B_k = \{x \in U: \varphi_{p(k)}(x) = 1+(\beta(k)-\beta)p(k)\}$,

then $\int_U \varphi_{p(k)}(x)\, dm = 0$ implies $m(A_k) = 1 - (\beta - \beta(k))p(k)$ and

$m(B_k) = (\beta - \beta(k))p(k)$.

If one can find a sequence $(k_n)_{n=1}^{\infty}$ such that

$\lim_{n\to\infty} (\beta - \beta(k_n))p(k_n) = c$

with $0<c<1$, then the foregoing lemma implies that $-c$, $1-c$ and, therefore, 1 are periods of T_φ.

Infinitely many digits β_i are nonzero. Let $(i_n)_{n=1}^{\infty}$ be the sequence of those indices i such that $\beta_i \neq 0$. Let K be such that $q_j \leq K$ for all j. Then $(\beta - \beta(i_n))p(i_n) > 1/q_{i_n+1} \geq 1/K$ for all i_n. Let $(i'_n)_{n=1}^{\infty}$ be the subsequence of $(i_n)_{n=1}^{\infty}$ such that

$\beta_{i'_n+1} < q_{i'_n+2} - 1$

Then

$1/k < (\beta - \beta(i'_n))p(i'_n) \leq 1-1/K^2$

for all i'_n. Hence there exists a subsequence $(k_n)_{n=1}^{\infty}$ of $(i'_n)_{n=1}^{\infty}$ such that $\lim_{n\to\infty} (\beta - \beta(k_n))p(k_n)$ lies in $]0,1[$, as desired.

As 1 is a period of T_φ, ergodicity of T_φ on UxG is equivalent to ergodicity of the transformation $(x,t) \to (Tx,t-\beta)$ on $UxG/\mathbb{Z}$. The latter is ergodic if and only if the functional equation $h(Tx) = \chi(-\beta)\, h(x)$, χ an arbitrary nontrivial character in the dual group of $G/\mathbb{Z}$, has the only measurable solution $h(x) = 0$ m-a.e. . $\chi(-\beta)$ is a number of the form $\exp(-2\pi i m\beta)$ with m in $\{1,2,\ldots,s-1\}$ if β is rational, $\beta=r/s$, $(r,s)=1$, and m a nonzero integer if β is irrational. Neither in the case of irrational nor in the case of strictly non-q-adic β will $\chi(-\beta)$ be an eigenvalue of the transformation T (see [2]), hence the functional equation above will only have the trivial measurable solution $h(x)=0$ a.e. .

Remark : The condition that $(q_i)_{i=1}^{\infty}$ is bounded guarantees the existence of limit points of the sequence $((\beta - \beta(k))p(k))_{k=1}^{\infty}$ in the open interval $]0,1[$.

References

[1] Conze, J.-P. : Ergodicité d'une transformation cylindrique. Bull.Soc.Math. France 108 (4), 441-456 (1980).

[2] Hellekalek, P. : Regularities in the distribution of special sequences. J. of Number Theory (to appear).

[3] Hewitt, E. and K.A. Ross : Abstract Harmonic Analysis, Vol.I. Springer-Verlag, Heidelberg-New York-Berlin, 1963.

[4] Oren, I. : Ergodicity of cylinder flows arising from irregularities of distribution. Israel J.Math. 44 (2), 127-138 (1983).

[5] Schmidt, K. : A cylinder flow arising from irregularity of distribution. Comp. Math. 36 (3), 225-232 (1978).

[6] Stewart, M. : Irregularities of uniform distribution. Acta Math. Acad. Scient. Hung. 37 (1-3), 185-221 (1981).

[7] Veech, W.A. : Topological dynamics. Bull. Amer.Math.Soc. 83 (5), 775-830 (1977).

Sur le "petit crible" d'Erdös et Ruzsa

A. HILDEBRAND

Le problème fondamental d'un crible est le suivant : Etant donné une suite finie $(a_n)_{n \leq x}$ d'entiers et un ensemble $\mathcal{P}$ de nombres premiers, on cherche à estimer le nombre des éléments a_n de cette suite qui n'ont pas de facteurs premiers appartenant à $\mathcal{P}$.

Nous considérons ici le cas le plus simple, celui de la suite $a_n = n$, et nous posons, pour tout $x \geq 1$ et tout ensemble $\mathcal{P}$ de nombres premiers $\leq x$,

$$S(x, \mathcal{P}) := \sum_{\substack{n \leq x \\ (n, \mathcal{P}) = 1}} 1 ,$$

où la condition "$(n, \mathcal{P}) = 1$" signifie que n n'a pas de diviseurs premiers appartenant à $\mathcal{P}$. Comme la probabilité qu'un entier positif $n \leq x$ soit divisible par un premier p (fixé) $\leq x$, est approximativement égale à $\frac{1}{p}$, on s'attend (en supposant une certaine "indépendance des premiers") à ce que $S(x, \mathcal{P})$ soit proche de

$$x \prod_{p \in \mathcal{P}} (1 - \frac{1}{p}) .$$

Dans un sens, cet argument heuristique est confirmé par la majoration

$$(1) \qquad S(x, \mathcal{P}) \leq c\, x \prod_{p \in \mathcal{P}} (1 - \frac{1}{p})(1 + \mathcal{O}(\frac{1}{\log x})) ,$$

valable uniformément pour tout $x \geq 2$ et tout ensemble $\mathcal{P}$ de nombres premiers $\leq x$. Le crible classique de Selberg (voir [4], chapitres 5 et 6) permet d'obtenir (1) avec $c = 2e^{\gamma}$, où γ est la constante d'Euler, mais R.R. Hall [5] a montré par une méthode différente qu'on peut prendre $c = e^{\gamma}$, ce qui constitue la valeur optimale de c.

La minoration de $S(x, \mathcal{P})$ est beaucoup plus délicate. Les méthodes classiques du crible mènent à une minoration du type

$$(2) \qquad S(x, \mathcal{P}) \geq c'\, x \prod_{p \in \mathcal{P}} (1 - \frac{1}{p}) ,$$

si l'ensemble $\mathcal{P}$ ne contient pas de "grands" nombres premiers (plus précisément, on obtient (2) avec $c' = c'(\varepsilon)$ si $\mathcal{P} \subset [1, x^{1/2 - \varepsilon}]$, l'exposant $1/2$ étant ici la "limite" du crible). Sans une telle condition sur l'ensemble $\mathcal{P}$, les

cribles classiques ne donnent pas de minoration pour $S(x,\mathcal{P})$. Ceci est dû au fait que dans ces cribles on compare $S(x,\mathcal{P})$ avec sa valeur heuristique $x \prod_{p\in\mathcal{P}}(1-\frac{1}{p})$ et estime la différence entre ces deux quantités. Cette méthode devient ineffective, lorsque l'ordre de $S(x,\mathcal{P})$ est inférieur à l'ordre de $x \prod_{p\in\mathcal{P}}(1-\frac{1}{p})$. Or, $S(x,\mathcal{P})$ peut être beaucoup plus petite que sa valeur heuristique. Il suffit de prendre pour $\mathcal{P}$ des ensembles du type

$$\mathcal{P}(x^{\alpha},x) := \{p \text{ premier} : x^{\alpha} \leqslant p \leqslant x\} \qquad (x \geqslant 1 \ , \ 0 < \alpha \leqslant 1) \ .$$

$S(x,\mathcal{P}(x^{\alpha},x))$ est alors égale au nombre des entiers positifs $n \leqslant x$, n'ayant pas de facteurs premiers dans l'intervalle $[x^{\alpha},x]$, et il est bien connu [2] que

$$\lim_{x\to\infty} \frac{1}{x} S(x,\mathcal{P}(x^{\alpha},x)) = \rho(\frac{1}{\alpha})$$

où ρ est la fonction de Dickmann définie comme fonction continue sur l'intervalle $[0,\infty[$ par

$$\rho(t) = 1 \qquad (0 \leqslant t \leqslant 1) \ ,$$
$$-t\rho'(t) = \rho(t-1) \qquad (t > 1) \ .$$

On a, pour $\alpha \to 0+$, (voir [1])

$$\rho(\frac{1}{\alpha}) = \exp\left(-\frac{1}{\alpha}\log\frac{1}{\alpha}(1+o(1))\right) \ ,$$

de sorte que $\rho(\frac{1}{\alpha})$ décroît beaucoup plus vite que

$$\prod_{p\in\mathcal{P}(x^{\alpha},x)}(1-\frac{1}{p}) = \alpha + o(1)$$

Le problème se pose alors de donner une minoration non triviale pour $S(x,\mathcal{P})$, qui est valable sans restrictions sur l'ensemble $\mathcal{P}$. Une telle minoration a été donnée récemment par Erdös et Ruzsa [3] dans un article intitulé "On the small sieve" : Il existe une constante $c''>0$ telle que, pour tout $x \geqslant 2$ et tout ensemble $\mathcal{P}$ de nombres premiers $\leqslant x$, on a

$$S(x,\mathcal{P}) \geqslant x \exp\left(-\exp(c'' \sum_{p\in\mathcal{P}} \frac{1}{p})\right) \ .$$

En posant

$$G(x,K) := \min_{\mathcal{P}}\left\{ \frac{S(x,\mathcal{P})}{x} : \sum_{p\in\mathcal{P}} \frac{1}{p} \leqslant K \right\} \ ,$$

où $x \geqslant 2$, $K > 0$ et le minimum est étendu sur tous les ensembles $\mathcal{P}$ de nombres premiers $\leqslant x$ satisfaisant à $\sum_{p\in\mathcal{P}} \frac{1}{p} \leqslant K$, le résultat d'Erdös et Ruzsa prend la forme

$$G(x,K) \geqslant e^{-e^{c''K}} \ .$$

Erdös et Ruzsa ont posé le problème de donner une formule asymptotique pour $G(x,K)$ lorsque $x \to \infty$, et ont conjecturé [3, Problème 1], que le minimum dans la défini-

tion de $G(x,K)$ est "asymptotiquement" atteint, lorsque $\mathcal{P}$ est de la forme $\mathcal{P}(x^{\alpha},x)$ avec $\alpha = e^{-K}+o(1)$. Autrement dit, la conjecture d'Erdös et Ruzsa affirme que, pour tout $K > 0$,

$$\lim_{x\to\infty} G(x,K) = \lim_{x\to\infty} \frac{1}{x} S(x,\mathcal{P}(x^{e^{-K}},x)) = \rho(e^{K}) .$$

Nous pouvons démontrer cette conjecture sous une forme plus précise :

THEOREME : Il existe des constantes positives c_1 et c_2 telles que, uniformément pour $x \geqslant 3$ et $0 < K \leqslant c_1 \log\log x$, on a

$$(3) \qquad G(x,K) = \rho(e^{K}) \left(1 + \mathcal{O}\left(\frac{1}{(\log x)^{c_2}}\right)\right) .$$

Le principe de la démonstration est le suivant : la majoration pour $G(x,K)$ se déduit des estimations connues pour $S(x,\mathcal{P}(x^{\alpha},x))$. La minoration triviale

$$S(x,\mathcal{P}) \geqslant [x] - \sum_{p\in\mathcal{P}} [\frac{x}{p}]$$

entraîne

$$G(x,K) \geqslant 1 - K + \mathcal{O}(\frac{1}{x}) ,$$

et comme

$$\rho(u) = 1 - \log u \qquad (1 \leqslant u \leqslant 2) ,$$

ceci donne la minoration souhaitée pour $G(x,K)$, lorsque $0 < K \leqslant \log 2$. On en déduit la minoration dans le cas $K > \log 2$ par un argument inductif assez compliqué dont l'idée sous-jacente est la suivante : Il faut montrer que la fonction

$$\rho(x,u) := G(x,\log u) \qquad (x \geqslant 2 , u \geqslant 1)$$

est proche de $\rho(u)$. Or, la fonction ρ est définie de façon unique comme fonction continue pour les deux conditions

$$\rho(u) = 1 - \log u \qquad (1 \leqslant u \leqslant 2) ,$$
$$-u\,\rho'(u) = \rho(u-1) \qquad (u > 1) .$$

Comme on l'a vu, $\rho(x,u)$ vérifie aussi, à un terme d'erreur près, la première des deux conditions. De plus, on peut établir une inégalité fonctionnelle pour $\rho(x,u)$, qui constitue une forme approximative de la deuxième condition, avec la dérivée remplacée par des différences finies et une inégalité au lieu d'une équation. Il se montre alors que cette inégalité est déjà suffisante pour obtenir la minoration souhaitée de $\rho(x,u)$ par $\rho(u)$.
Une démonstration détaillée sera publiée ailleurs.

Discutons brièvement quelques possibilités de généraliser ce résultat.
Comme $S(x,\mathcal{P})$ s'écrit sous la forme

$$S(x,\mathcal{P}) = \sum_{n\leqslant x} f(n) ,$$

où f est la fonction multiplicative définie par

$$f(p^m) = \begin{cases} 1 & \text{si } p \notin \mathcal{P} , \\ 0 & \text{si } p \in \mathcal{P} , \end{cases}$$

on est tenté d'essayer d'étendre une estimation de $S(x,\mathcal{P})$ à une estimation pour des sommes de fonctions multiplicatives plus générales. Ceci est possible dans le cas de la majoration (1), comme l'a montré Hall [4] : On a uniformément pour tout $x \geqslant 3$ et toute fonction multiplicative f satisfaisant à $0 \leqslant f \leqslant 1$

$$\frac{1}{x} \sum_{n \leqslant x} f(n) \leqslant e^{\gamma} \prod_{p \leqslant x} (1 - \frac{1}{p})(1 + \sum_{m \geqslant 1} \frac{f(p^m)}{p^m}) \left(1 + \mathcal{O}\left(\frac{1}{\log x}\right)\right) .$$

La minoration de $S(x,\mathcal{P})$ donnée par le théorème peut être généralisée de façon similaire : Soit, pour $x \geqslant 2$ et $K > 0$,

$$G_1(x,K) := \min \left\{ \frac{1}{x} \sum_{n \leqslant x} f(n) : \sum_{p \leqslant x} \frac{1 - f(p)}{p} \leqslant K \right\} ,$$

où le minimum est étendu sour toutes les fonctions multiplicatives f vérifiant $0 \leqslant f \leqslant 1$ et $\sum_{p \leqslant x} \frac{1 - f(p)}{p} \leqslant K$. En utilisant la méthode de démonstration esquissée ci-dessus, on peut montrer l'estimation (3) avec $G_1(x,K)$ au lieu de $G(x,K)$. Ceci entraîne

$$\frac{1}{x} \sum_{n \leqslant x} f(n) \geqslant \rho(\exp(\sum_{p \leqslant x} \frac{1 - f(p)}{p})) \left(1 + \mathcal{O}\left(\frac{1}{(\log x)^{c_2}}\right)\right)$$

uniformément pour tout $x \geqslant 3$ et toute fonction multiplicative f vérifiant $0 \leqslant f \leqslant 1$ et

$$\sum_{p \leqslant x} \frac{1 - f(p)}{p} \leqslant c_1 \log\log x .$$

Il serait intéressant d'avoir des minorations analogues pour des suites $(a_n)_{n \leqslant x}$ autres que $a_n = n$. Cependant, notre méthode est étroitement liée aux propriétés arithmétiques de la suite $a_n = n$, et il semble difficile d'étendre ce résultat à d'autres suites. Le seul cas où l'on pourrait espérer obtenir des résultats analogues est celui d'une progression arithmétique.

Une autre possibilité de généralisation, déjà suggérée par Erdös et Ruzsa [3, Problème 2] , est de considérer la quantité $S(x,\mathcal{P},\mathcal{U})$ égale au nombre des entiers positifs $n \leqslant x$, qui vérifient

$$n \not\equiv a_p \bmod p \quad (p \in \mathcal{P}) ,$$

où $\mathcal{P}$ est un ensemble de nombres premiers $\leqslant x$ et $\mathcal{U} = (a_p)_{p \in \mathcal{P}}$ une suite d'entiers positifs. Nous n'avons obtenu une minoration de $S(x,\mathcal{P},\mathcal{U})$ que pour certains ensembles $\mathcal{P}$ particuliers. Ces résultats ainsi que des arguments heuristiques semblent indiquer que la conjecture suivante est vraie :

Conjecture : Soit

$$G_2(x,K) := \min \left\{ \frac{S(x,\mathcal{P},\mathcal{U})}{x} : \sum_{p\in\mathcal{P}} \frac{1}{p} \leqslant K \right\} .$$

Alors, on a uniformément pour $x \geqslant 2$ et $K > 0$

$$G_2(x,K) = \rho(e^K) + \mathcal{O}\left(\frac{1}{\log x}\right) .$$

Le terme reste ne peut être amélioré ici comme P. Erdös nous l'a fait remarquer.

Signalons enfin que Ruzsa [6] a étudié la quantité $S(x,\mathcal{U})$ égale au nombre des entiers positifs $\leqslant x$ qui ne sont divisibles par aucun élément de $\mathcal{U}$, où $\mathcal{U}$ est un ensemble d'entiers positifs. Si on définit

$$G_3(x,K) := \min \left\{ \frac{S(x,\mathcal{U})}{x} : \sum_{a\in\mathcal{U}} \frac{1}{a} \leqslant K \right\} ,$$

où $\mathcal{U}$ parcourt tous les ensembles d'entiers positifs, alors le comportement de $G_3(x,K)$ est complétement différent de celui de $G(x,K)$: Ruzsa a montré que l'on a pour tout $K > 1$

$$\log G_3(x,K) \sim (e^{1-K} - 1) \log x \qquad (x \to \infty) .$$

BIBLIOGRAPHIE.

[1] N.G. de BRUIJN - The asymptotic behaviour of a function occuring in the theory of primes. J. Indian Math. Soc. 15 (A) (1951), 25 - 32.

[2] N.G. de BRUIJN - On the number of positive integers x and free from prime factors y . Indag. Math. 13 (1951) , 50 - 60.

[3] P. ERDÖS et I.Z. RUZSA - On the small sieve I. J. Number Theory 12 (1980), 385 - 394.

[4] H. HALBERSTAM et H.E. RICHERT - Sieve Methods. Academic Press, London 1974.

[5] R.R. HALL - Halving an estimate obtained from Selberg's upper bound method. Acta Arith. 25 (1974) , 347 - 351.

[6] I.Z. RUZSA - On the small sieve II . J. Number Theory 14 (1980), 260 - 268.

SUR UNE QUADRUPLE EQUATION

par J. LAGRANGE

1. Dans [1] J. Leech montre que le système diophantien

$$(1)\quad \begin{aligned} x^2 + y^2 &= \square \\ x^2 + z^2 &= \square \\ x^2 + (y-z)^2 &= \square \\ x^2 + (y+z)^2 &= \square \end{aligned}$$

a une infinité de solutions.

Sa méthode consiste à partir du système

$$(2)\quad \begin{aligned} x'^2 - 3y'^2 &= \square \\ x'^2 - 3z'^2 &= \square \\ x'^2 - 3(y'+z')^2 &= \square \\ x'^2 - 3(y'-z')^2 &= \square \end{aligned}$$

dont il est plus facile de montrer qu'il a une infinité de solutions ; puis à partir d'une solution de ce système (2) Leech construit une solution du système (1). Il ajoute qu'il ne voit aucune méthode pour résoudre directement le système (1). C'est une telle méthode qu'on va donner ici.

Plus généralement on va montrer que quels que soient les entiers p et q le système

$$(3)\quad \begin{aligned} x^2 + y^2 &= \square \\ x^2 + z^2 &= \square \\ p^2x^2 + q^2(y+z)^2 &= \square \\ p^2x^2 + q^2(y-z)^2 &= \square \end{aligned}$$

a une infinité de solutions.

Une solution particulière est

$$(4)\quad \begin{aligned} x &= 4pq^2(p+q)(p+2q)(p^2-2q^2)(p^2+2pq+2q^2)\\ y &= q(p^4+6p^3q+8p^2q^2-4q^4)(p^4+2p^3q+4p^2q^2+8pq^3+4q^4)\\ z &= (p+q)(p^4+2p^3q+4q^4)(p^4+2p^3q-4p^2q^2-8pq^3-4q^4) \end{aligned}$$

On notera que un changement du signe de q ne change pas le système (3) mais que les formules (4) donnent, à une exception près, une autre solution.

L'exception a lieu pour $p = q = 1$ (ou ce qui revient au même pour $p = 2$, $q = 1$) c'est-à-dire pour le système (1) car les formules (4) donnent pour $p = 1$, $q = -1$ la solution triviale $x = 0$. On montrera que dans ce cas la méthode de Leech et notre méthode sont équivalentes.

2. Dans ce paragraphe les lettres désignent des nombres rationnels. Nous allons donner une famille de solutions du système (3). Posons $\frac{p}{q} = \lambda - 1$; ce système s'écrit

$$(5)\quad \begin{aligned} x^2 + y^2 &= \square\\ x^2 + z^2 &= \square \end{aligned}$$

$$(6)\quad \begin{aligned} (\lambda-1)^2x^2 + (y+z)^2 &= (A+B)^2\\ (\lambda-1)^2x^2 + (y-z)^2 &= (A-B)^2 \end{aligned}$$

Le coefficient $\lambda-1$ n'est peut-être pas naturel mais il est nécessaire dans la suite des calculs. On notera que le changement de signe de q donne une valeur de λ différente ce qui donnera deux familles de solutions, à part l'exception déjà signalée.

Le système (5) a la solution générale

$$(7)\quad \begin{aligned} x &= 2\lambda\, u\, v\\ y &= \lambda^2 u^2 v^2 - 1\\ z &= \lambda(u^2-v^2) \end{aligned}$$

Le paramètre λ peut sembler inutile, la valeur $\lambda = 1$ donnant déjà la solution générale. Il a été introduit arbitrairement mais bien entendu coincide avec le λ du système (6).

On écrit ensuite ce système (6) sous la forme

$$(8)\qquad \begin{aligned} yz &= AB \\ (\lambda-1)^2\, x^2+y^2+z^2 &= A^2+B^2 \end{aligned}$$

et on introduit les polynômes

$$P = (\lambda u^2-1)(\lambda v^2-1) + 2\lambda(\lambda-1)\, u\, v$$

$$Q = (u+v)\ (\lambda\, u\, v - 1)$$

$$R = (u-v)\ (\lambda\, u\, v + 1)$$

On vérifie ensuite que les premiers membres du système (8) s'écrivent en fonction de P, Q, R.

On a immédiatement

$$y\, z = \lambda Q\, R$$

un calcul un peu plus délicat donne

$$(\lambda-1)^2\, x^2 + y^2 + z^2 = P^2 + \lambda^2 R^2 - \lambda(\lambda-2)\, Q^2$$

On écrit cette expression sous la forme

$$(\lambda-1)^2\, x^2 + y^2 + z^2 = P^2 + Q^2 + \lambda^2 R^2 - (\lambda-1)^2\, Q^2$$

Si on prend

$$P = (\lambda-1)\, Q$$

on aura

$$A = Q \qquad B = \lambda R\ .$$

C'est-à-dire une solution du système (8).

L'équation $P = (\lambda-1)\, Q$ s'écrit

$$(9)\qquad (\lambda\, u+1)\ (u-1)\ (\lambda\, v+1)\ (v-1) + (\lambda^2-1)\, u\, v = 0\ .$$

C'est une équation du second degré en u et v, les méthodes classiques permettent d'obtenir des solutions.

En résumé on a la construction suivante d'une solution du système (3).

On pose $\frac{p}{q} = \lambda - 1$ (ou $\frac{p}{q} = 1 - \lambda$) ; les formules (7) donnent une solution lorsque u et v sont solutions de l'équation (9). La première solution de cette équation est

$$u = \frac{2}{1-\lambda^2} \quad , \quad v = \frac{1-2\lambda-\lambda^2}{1+\lambda^2}$$

on obtient ainsi la solution (4) citée plus haut.

3. Dans ce paragraphe, à l'exception de u et v, les lettres désignent des nombres entiers.

Montrons maintenant l'équivalence de cette méthode pour $\lambda = 2$ avec celle de Leech.

Soit (u,v) une solution de l'équation (9) ; posons

$$u = \frac{a}{b} \quad , \quad v = \frac{c}{d}$$

on a alors

$$(2a + b)(a-b)(2c + d)(c-d) + 3abcd = 0$$

Par le remplacement éventuel de u par $-\frac{1}{2u}$ on peut toujours supposer b et d impairs ; on voit alors que l'un des nombres a ou c est impair, l'autre pair. Comme $(2a + b)(a-b)$ et ab d'une part, $(2c + d)(c-d)$ et cd d'autre part sont premiers entre eux on a, après un échange éventuel des couples (a,b) et (c,d)

$$(2a + b)(a-b) = 3\varepsilon cd \qquad \varepsilon = \pm 1$$
$$(2c + d)(c-d) = -\varepsilon ab$$

on introduit ensuite les nombres h, k, m, n [1] par :

---

(1) Les lettres h, k, m, n ont la même signification que dans [1], sauf peut-être pour le signe de h.

$$h = 2a^2 - b^2 = ab + 3\varepsilon\, cd$$
$$k = 2c^2 - d^2 = cd - \varepsilon\, ab$$
(10)
$$3(m+n) = 2a^2 + b^2$$
$$m-n = 2c^2 + d^2$$

Un calcul montre que

$$4(m^2 + mn + n^2) = h^2 + 3k^2$$
(11)
$$m^2 + 4mn + n^2 = -\varepsilon\, hk$$

La solution du système (2) est alors donnée par les identités

$$4(m^2 + mn + n^2)^2 - 3(m^2 + 2mn)^2 = (m^2 - 2mn - 2n^2)^2$$
$$4(m^2 + mn + n^2)^2 - 3(2mn + n^2)^2 = (2m^2 + 2mn - n^2)^2$$
$$4(m^2 + mn + n^2)^2 - 3(m^2 - n^2)^2 = (m^2 + 4mn + n^2)^2$$
$$(h^2 + 3k^2)^2/4 - 3h^2 k^2 = (h^2 - 3k^2)^2/4$$

On peut ensuite vérifier l'observation de Leech que les deux premiers $\square$ du système (1) coincident avec les deux premiers $\square$ du système (2).

Réciproquement : si m, n, h, k est une solution du système (11) on en déduit

$$2(m-n)^2 = (h+\varepsilon k)^2 + 2k^2$$
$$18(m+n)^2 = (h - 3\varepsilon\, h)^2 + 2h^2$$

d'où l'existence de a, b, c, d tels que

$$m-n = 2c^2 + d^2 \qquad h+\varepsilon\, k = 4\,\varepsilon\, cd \qquad k = 2c^2 - d^2$$
$$3(m+n) = 2a^2 + b^2 \qquad h - 3\varepsilon\, k = 4\, ab \qquad h = 2a^2 - b^2$$

On en déduit une solution du système (10) c'est-à-dire une solution de l'équation (9).

Exemple numérique :

$a, b, c, d = -1, 5, -2, 3 \qquad h, k = -23, -1 \qquad m, n = -4, 13 \qquad \varepsilon = 1$

d'où la solution

$120^2 + 182^2 = 218^2$ $\qquad$ $266^2 - 3.88^2 = 218^2$

$120^2 + 209^2 = 241^2$ $\qquad$ $266^2 - 3.65^2 = 241^2$

$120^2 + 391^2 = 409^2$ $\qquad$ $266^2 - 3.153^2 = 23^2$

$120^2 + 27^2 = 123^2$ $\qquad$ $266^2 - 3.23^2 = 263^2$

4. Pour $\lambda = -2$ on peut faire un raisonnement analogue à celui qui a été fait au début du paragraphe précédent.

Posant $u = \frac{a}{b}$ $\qquad$ $v = \frac{c}{d}$ $\qquad$ on a

$$(2a - b)(a-b)(2c - d)(c-d) + 3\,a\,b\,c\,b = 0$$

d'où

$$(2a - b)(a-b) = 3\varepsilon\, cd$$
$$(2c - d)(c-d) = -\varepsilon\, ab \qquad \varepsilon = \pm 1$$

On a ensuite après avoir rendu entier

$$A = Q = (ad + bc)(2ac + bd)$$

$$B = -2R = 2(ad - bc)(2ac - bd)$$

on en déduit

$$A + B = 3\varepsilon\,(ab - \varepsilon\, cd)^2$$

$$A - B = -\varepsilon\,(ab + 3\varepsilon\, cd)^2$$

On a ainsi une infinité de solutions pour le système

$$x^2 + y^2 = \square$$
$$x^2 + z^2 = \square$$
$$9x^2 + (y+z)^2 = r^4$$
$$9x^2 + (y-z)^2 = 9\,s^4$$

Exemple numérique :

$a, b, c, d = 7, 5, -2, 3 \qquad \varepsilon = -1$

d'où la solution :

$$840^2 + 559^2 = 1009^2$$
$$840^2 + 682^2 = 1082^2$$
$$9.840^2 + 1241^2 = 53^4$$
$$9.840^2 + 123^2 = 9.29^4$$

Si on prend $\lambda = -4$, on obtient le même système (3) mais les bicarrés n'apparaissent plus.

Exemple numérique :

a, b, c, d = 7, 17, -2, 15

d'où la solution :

$$28560^2 + 39476^2 = 48724^2$$
$$28560^2 + 61889^2 = 68161^2$$
$$9.28560^2 + 101365^2 = 132725^2$$
$$9.28560^2 + 22413^2 = 88563^2$$

132725 et 29521 ne sont pas des carrés.

Il est probable qu'on pourrait obtenir des résultats du même type avec d'autres valeurs de λ .

Référence

[1] J. LEECH - Two Diophantine Birds with One Stone.
Bull. London Math. Soc. 13 (1981), 561-563.

Jean LAGRANGE
Département de Mathématiques
U.E.R. Sciences de Reims
B.P. 347
51062 Reims Cedex

AUTOMATA AND p-ADIC NUMBERS.

M. MENDES FRANCE and A.J. VAN DER POORTEN

We propose two conjectures relating on the one hand to the representation of an irrational algebraic p-adic number and on the other hand to the transcendence of α^{β} in the ring of formal power series over a finite field $\mathbb{F}_p$. These ideas arose in discussion during the second author's recent stay in Bordeaux.

1.- The field $\mathbb{F}_p((X))$ and the ring $\mathbb{F}_p[[X]]$.

Let p be prime and denote by $\mathbb{F}_p$ the field of p elements. Then $\mathbb{F}_p((X))$ is the field of formal Laurent series

$$f = f(X) = \sum_{h=m}^{\infty} f_h X^h \qquad \text{with} \quad f_h \in \mathbb{F}_p \ , \ m \in \mathbb{Z} \ .$$

The element f is said to be algebraic over the field $\mathbb{F}_p(X)$ of rational functions over $\mathbb{F}_p$ if for some $s \in \mathbb{N}$ there are polynomials $a_0, a_1, \ldots, a_s$ of $\mathbb{F}_p[X]$ not all zero so that

$$a_0 f^s + a_1 f^{s-1} + \ldots + a_s = 0 \ .$$

In the sequel we will be concerned with the subring $\mathbb{F}_p[[X]]$ of formal power series; that is, those elements of $\mathbb{F}_p((X))$ with $m \geqslant 0$. The units of this ring are the series with $f_0 \neq 0$ and below we deal with units so that $f_0 = f(0) = 1$.

As usual, though in this context a trifle confusingly, $\mathbb{Z}_p$ denotes the ring of p-adic integers. For $\lambda \in \mathbb{Z}_p$, we write

$$\lambda = \sum_{n=0}^{\infty} \lambda_n p^n \qquad , \ 0 \leqslant \lambda_n < p \ .$$

We may define

$$f^{\lambda} = (f(X))^{\lambda} = \prod_{n=0}^{\infty} (f(X))^{\lambda_n p^n}$$

$$= \prod_{n=0}^{\infty} (f(X^{p^n}))^{\lambda_n}$$

Presuming that f, g are elements of $\mathbb{F}_p[[X]]$ with $f_0 = 1$, $g_0 = 1$ we see that the notation does not delude : for λ, μ in $\mathbb{Z}_p$ we have $f^{\lambda} f^{\mu} = f^{\lambda+\mu}$, $(f^{\lambda})^{\mu} = f^{\lambda\mu}$,

$(fg)^\lambda = f^\lambda g^\lambda$ and so on, whilst f^λ is indeed again an element of $\mathbb{F}_p[[\,X\,]]$. Thus we have a proper exponentiation.

Example 1 The following example amply illustrates the interest of the notion introduced above :

Denote by C the 'Cantor set' of all natural numbers which in their base 3 representation require only the digits 0 and 1. Then in $\mathbb{F}_3[[\,X\,]]$ we have

$$\sum_{m \in C} X^m = \prod_{n=0}^{\infty} (1 + X^{3^n}) = (1+X)^\lambda$$

where in $\mathbb{Z}_3$:

$$\lambda = 1 + 3 + 3^2 + 3^3 + \ldots = -1/2$$

Hence

$$\left(\sum_{m \in C} X^m \right)^2 = (1+X)^{-1} = \sum_{h=0}^{\infty} X^h ,$$

yielding a witty identity in $\mathbb{F}_3[[\,X\,]]$.

Example 2 In the same spirit we see that in $\mathbb{F}_2[[\,X\,]]$ we may find f so that

$$f^3 = (1+X)^{-1} .$$

Indeed, in $\mathbb{Z}_2$ we have

$$-1/3 = 1 + 4 + 4^2 + 4^3 + \ldots$$

so

$$f(X) = \prod_{k=0}^{\infty} (1 + X^{4^k}) = \sum_{m \in L} X^m$$

where m is the set of natural numbers representable as a sum of distinct powers of 4.

Example 3 An inversion formula. Again let $p = 2$ and for $\lambda \in \mathbb{Z}_2$ set

$$sp(\lambda) = \{n : \lambda_n \neq 0\}$$

Suppose, for convenience, that $\lambda_0 = 1$. If g is an element of $\mathbb{F}_2[[\,X\,]]$ such that $g_0 = 1$ and if

$$f(X) = \prod_{k \in sp(\lambda)} g(X^{2^k}) ,$$

then

$$g(X) = \prod_{k \in sp(\lambda^{-1})} f(X^{2^k})$$

At first glance this is a startling claim. In fact we have only reformulated the triviality :

$$f = g^\lambda \quad \text{implies} \quad g = f^{1/\lambda}$$

We conclude this section with the following remark : In characteristic zero we have the Gelfond-Schneider theorem : if $\alpha \in \overline{\mathbb{Q}} \setminus \{0,1\}$ and $\beta \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ then α^β is transcendental. Motivated largely by vague analogy we are moved to suggest that

Conjecture 1 *If* f *is an algebraic element of* $\mathbb{F}_p[[X]]$ *with* $f_0 = 1$ *and* λ *is an algebraic irrational element of* $\mathbb{Z}_p$ *then* f^λ *is a transcendental element of* $\mathbb{F}_p[[X]]$.

The most striking special case has $f(X) = 1+X$ and $p=2$. Given

$$\lambda = \sum_{n=0}^{\infty} \lambda_n 2^n$$

in $\mathbb{Z}_2$, thus with the $\lambda_n \in \{0,1\}$, we have the set of natural numbers

$$\mu = \sum_{n=0}^{\infty} \mu_n 2^n \qquad 0 \leqslant \mu_n \leqslant \lambda_n$$

(with $\mu_n = 0$ for all sufficiently large n). Viewing λ as an infinite sequence $\lambda_0\lambda_1\lambda_2\ldots$ the language $L(\lambda)$ of admissible words $\mu = \mu_0\mu_1\ldots\mu_s$ may be said to consist of all words "under" λ . The conjecture now purports that if λ is an algebraic irrational element of $\mathbb{Z}_2$ then

$$(1+X)^\lambda = \sum_{n \in L(\lambda)} X^n$$

is transcendental over $\mathbb{F}_2(X)$.

2.- Automata.

Formally, a m-automaton consists of a finite set S of states containing a distinguished element i , the initial state, and a subset F of acceptance or final states, related by a map σ

$$\{0,1,2,\ldots,m-1\} \times S \to S$$

known as the transition function. A word $\mu \in \bigcup_{n=0}^{\infty} \{0,1,\ldots,m-1\}^n$ is said to be read or accepted by the automaton if μ sends the state i to a state in F. This is to say, set $i = x_0$, $\mu = \mu_0\mu_1\ldots\mu_s$ $(\mu_j \in \{0,1,\ldots,m-1\})$ and define $x_{k+1} = \sigma(\mu_k, x_k)$. Then μ is accepted by the automaton if $x_{s+1} \in F$. The language L of all words accepted by the automaton is said to be generated by the automaton. We interpret the words of L as natural numbers presented in base m . It is a result of Cobham, but see [4], that L is generated by a finite m-automaton only if the series

$$f(X) = \sum_{n \in L} X^n \in \mathbb{C}[[X]]$$

satisfies a Mahler functional equation

$$a_0(X)f(X^{m^s}) + a_1(X)f(X^{m^{s-1}}) + \ldots + a_{s-1}(X)f(X^m) + a_s(X)f(X) = 0$$

with the a_i in $\mathbb{Z}[X]$. When $m = q$ is a power of a prime p we know [1] that

$$\sum_{n \in L} X^n \in \mathbb{F}_p[[X]]$$

is algebraic over $\mathbb{F}_p(X)$ if *and only if* L is generated by a finite p^k-automaton, for some $k \geqslant 1$. For an informal discussion of these matters see FOLDS ! [2] , 2.4-5.

For $p = 2$ and $f(X) = 1 + X$ our earlier conjecture can now be stated in the following way :

Conjecture 2 *If* λ *is an irrational algebraic 2-adic integer then the language* $L(\lambda)$ *is not generated by a finite 2-automaton.*

Thus the conjecture may be said to assert that the digits of an irrational algebraic 2-adic integer form a relatively 'complicated' sequence. In fact an analogous result is known in the complex case [3] ; a gap in that result has now been closed and the proof can be reconstructed to show that it applies in all metrics. However that result implies only that $\Sigma \lambda_n X^n$ cannot be an algebraic element of $\mathbb{F}_2[[X]]$ if λ is an irrational algebraic element of $\mathbb{Z}_2$; it is silent on the status of the language $L(\lambda)$.

So as to have at least the outline of a proof we close with an explanation of this last remark : Since $\lambda = \Sigma \lambda_n 2^n$ is irrational there are infinitely many k for which both $\lambda_k = 0$ and $\lambda_{k+1} = 0$; if not, this is true of $-\lambda$ and we lose no generality in assuming it true for λ . Consider the derived 2-adic integer

$$\lambda' = \sum_{n \in L(\lambda)} 2^n$$

and its 'truncations'

$$\lambda'_k = \sum_{\substack{n \in L(\lambda) \\ n < 2^k}} 2^n$$

noting that these truncations can be viewed as elements of $\mathbb{Z}$, with $|\lambda'_k| < 2^{2^k}$. But it is easy to see that

$$|\lambda' - \lambda'_k|_2 \leqslant 2^{-2^{k+2}}$$

if $\lambda_k = \lambda_{k+1} = 0$, so λ' is transcendental because it is a 2-adic Roth number. Had we commenced with $-\lambda$ we would have shown λ'^{-1} to be transcendental. Unfortunately, even were $L(\lambda)$ generated by a finite automaton it would follow that λ' is transcendental; though in general by a somewhat more complicated argument.

We conclude, a little reluctantly,with the following remark. The alleged analogy with the Gelfond-Schneider theorem leading to conjecture 1 is somewhat stretched. It seems quite as probable that it suffices for λ to be irrational and that the suggestion that λ should be algebraic simply constitutes a distraction.

This last remark has been vindicated by recent work of the authors. In 'Automata and the arithmetic of formal power series' (à paraître) we prove conjecture 1, requiring only that λ be irrational.

REFERENCES.

[1] G. CHRISTOL, T. KAMAE, M. MENDES-FRANCE, G. RAUZY Suites algébriques, automates et substitutions *Bull. Soc. Math. France* 108 , 401 - 419.

[2] Michel DEKKING, Michel MENDES-FRANCE, Alf VAN DER POORTEN FOLDS ! *The Mathematical Intelligencer* 4 (1982) 130 - 138 ; II 173 - 181 , III 190 - 195.

[3] J. H. LOXTON, A.J. VAN DER POORTEN Arithmetic properties of the solutions of a class of functional equations J. reine angew. Math (Crelle) 330 (1982) 159 - 172 ; II (in preparation).

[4] A.J. VAN DER POORTEN Substitition automata, functional equations and "functions algebraic over a finite field" Contemporary Math. 9 (1982) 307 - 312.

M. MENDES-FRANCE

UER de Mathématiques et Informatique
Université de Bordeaux I

A.J. VAN DER POORTEN

School of Mathematics and Physics
Macquarie University, NSW .

SUR LA DISTRIBUTION DES NOMBRES ENTIERS AYANT UNE QUANTITE FIXEE DE FACTEURS PREMIERS

Jean Louis NICOLAS

Désignons par $\Omega(n) = \sum_{p^a \| n} a$ le nombre de diviseurs de n comptés avec leur multiplicité. On définit :

$$\mathcal{N}(x,k) = \{n \leq x \mid \Omega(n) = k\}$$
$$N(x,k) = \text{Card}\, \mathcal{N}(x,k)$$
$$\mathcal{S}(x,k) = \{n \leq x \mid \Omega(n) \geq k\}$$
$$S(x,k) = \text{Card}\, S(x,k).$$

Dans tout cet article on écrira ℓ à la place de $\log\log x$.

En 1900, E. LANDAU a démontré comme corollaire du théorème des nombres premiers que, pour k fixé,

$$N(x,k) \sim \frac{x}{\log x} \frac{(\log\log x)^{k-1}}{(k-1)!} = \frac{x}{\log x} \frac{\ell^{k-1}}{(k-1)!}$$

(cf. [Lan], §56). Cette formule avait été conjecturée par Gauss (cf. [Ell], Introduction). En 1917, Hardy et Ramanujan dans leur célèbre mémoire "The normal number of prime factors of a number n" ont donné une majoration de $N(x,k)$ (cf. [Ram]).

Soit F la fonction définie pour $|z| < 2$, par

$$F(z) = \frac{1}{\Gamma(z+1)} \prod_p (1-1/p)^z (1-z/p)^{-1}$$

où p parcourt l'ensemble des nombres premiers. En 1953, L.G. Sathe (cf. [Sat]) démontrait que, pour $k \leq (2-\varepsilon)\ell$, on a :

$$N(x,k) \sim F(k/\ell) \frac{\ell^{k-1} x}{(k-1)! \log x}$$

étendant ainsi un résultat de P. Erdös qui avait considéré le cas $k - \ell = O(\sqrt{\ell})$; (cf. [Erd 1]).

A la suite de l'article de L.G. Sathe, A. Selberg démontrait la formule (cf. [Sel]) :

$$(1) \qquad \sum_{n\le x} z^{\Omega(n)} = xzF(z)(\log x)^{z-1} + O(x(\log x)^{\mathrm{Re}\, z-2}) \qquad \text{où } x \ge 2,$$

et où le "O" est uniforme dans tout disque $|z| \le R$ avec $R < 2$.

La formule (1) permettait à A. Selberg de retrouver le résultat de L.G. Sathe, et de préciser le comportement de $N(x,k)$ lorsque $(2-\varepsilon)\ell \le k \le B\ell$. Il signale notamment que :

$$N(x,k) \sim C(x \log x)/2^k$$

pour $(2+\varepsilon)\ell \le k \le B\ell$, où B est un nombre réel arbitraire.

La formule (1) a été généralisée de plusieurs façons par H. Delange (cf. [Del]).

En 1978, G. Kolesnik et E.G. Strauss, ont donné (cf. [Kol]) une estimation asymptotique de $N(x,k)$ sous la forme d'une somme double, mais dont les termes sont difficilement comparables. P. Erdös et Sarközy ont démontré dans [Sar] :

$$S(x,k) = O((x \log x)k^4/2^k)$$

uniformément pour tout x et k. Et K. Norton (cf. [Nor 3]) a démontré :

$$S(x,k) = O((x \log x)\sqrt{\ell}/2^k)$$

et annoncé que l'ordre de grandeur de $S(x,k)$ était $x(\log x)2^{-k}$ pour $\ell \le k \le (1-\varepsilon)(\log x)/\log 2$ et x assez grand.

Nous démontrerons :

THEOREME. - *Soit $B > 2$. Il existe b, $0 < b < 1$ tel que l'on ait uniformément pour $x \ge 3$ et $B\ell \le k \le (\log x)/\log 2$:*

$$(2) \qquad N(x,k) = C(x/2^k)\log(x/2^k) + O((x/2^k)\log^b(3x/2^k))$$

avec

$$C = (1/4)\prod_{p>2}(1+1/(p(p-2))) = 0{,}378694.$$

Dans un exposé au colloque d'Orsay (juin 1982) en l'honneur de H. Delange (cf. [Nic]), une estimation de $N(x,k)$ donnant le même terme principal que (2), mais avec un reste moins bon, avait été présentée. La démonstration reposait sur la formule :

$$(3) \qquad N(x,k) = \sum_{m=0}^{k} N'(x/2^{k-m},m)$$

où $N'(y,m) = \mathrm{Card}\{n \le y,\ n \text{ impair},\ \Omega(n) = m\}$.

La formule (3) s'obtient en regroupant les $n \in \mathcal{N}(x,k)$ qui sont divisibles exactement par la même puissance de 2.

On évalue ensuite $N'(y,m)$ grâce à une extension de la formule de Selberg (cf. [Del]), qui permet d'évaluer $\sum_{\substack{n\leq x \\ n\equiv 1 \bmod 2}} z^{\Omega(n)}$. On remarque enfin que dans la sommation de la formule (3) les termes les plus importants sont ceux pour lesquels m est voisin de 2ℓ ; en quelque sorte, l'élément normal de $\mathcal{N}(x,k)$, lorsque $k \geq (2+\varepsilon)\ell$, s'écrit $n = 2^a n'$ avec n' impair et $\Omega(n') \sim 2\ell$.

La démonstration que nous allons donner de la formule (2) est due à G. Halàsz. Cette démonstration est plus simple, elle est élémentaire, c'est-à-dire qu'elle n'utilise pas de variables complexes, et surtout elle donne un meilleur reste. Je remercie très vivement G. Halàsz de me permettre de la reproduire ici.

L'idée de base est d'écrire $n = 2^\alpha m$, m impair. On a alors $\Omega(n) = \alpha + \Omega(m)$ et on en déduit :

$$(4) \qquad N(x,k) = \sum_{\substack{m \text{ impair} \\ m\, 2^{k-\Omega(m)} \leq x \\ \Omega(m)\leq k}} 1 = T_1 - T_2$$

avec

$$T_1 = Q_1(x/2^k) \quad \text{et} \quad Q_1(y) = \sum_{\substack{m \text{ impair} \\ \psi(m) \leq y}} 1 \ ,$$

$$T_2 = Q_2(x/2^k) \quad \text{et} \quad Q_2(y,k) = \sum_{\substack{m \text{ impair} \\ \psi(m) \leq y \\ \Omega(m) > k}} 1 \ ,$$

où on a posé, pour simplifier l'écriture $\psi(m) = m\, 2^{-\Omega(m)}$.

La fonction ψ est complètement multiplicative, et tend vers $+\infty$ sur les nombres impairs. Le théorème résultera de (4), d'une estimation de $Q_1(y)$ et d'une majoration de $Q_2(y,k)$

La démonstration complète apparaitra dans un article des Acta Arithmetica.

Remarques : Il est possible par des méthodes analytiques d'obtenir pour T_1 un développement asymptotique plus long que (10), et de même d'obtenir un équivalent de T_2. Mais malheureusement la méthode ci-dessus, qui convient pour la fonction $\Omega(n)$ complètement additive, ne s'adapte pas par exemple à la fonction $\omega(n) = \sum_{p|n} 1$. Pour cette fonction, les meilleurs résultats actuellement connus sont [Erd 2], [Nor 3] et [Pom].

REFERENCES

[Del] H. DELANGE. *Sur des formules de Atle Selberg.* Acta Arithmetica, XIX, 1971, p. 105-146.

[Ell] P.D.T.A. ELLIOTT. *Probabilistic number theory I et II.* Springer Verlag 1980, Grundlehren der mathematischen Wissenschaften, n° 239-240.

[Erd 1] P. ERDÖS. *On the integers having exactly K prime factors.* Ann. of Math. (2), 49, 1948, p. 53-66.

[Erd 2] P. ERDÖS et J.L. NICOLAS. *Sur la fonction : nombre de facteurs premiers de n.* L'Enseignement Mathématique, t. 27, 1981, p. 3-27.

[Kol] G. KOLESNIK and E.G. STRAUSS. *On the distribution of integers with a given number of prime factors.* Acta Arithmetica, 37, 1980, p. 181-199.

[Lan] E. LANDAU. *Handbuch der Lehre von der Verteilung der Primzahlen.* Chelsea Publishing Company, 1953.

[Nic] J.L. NICOLAS. *Autour de formules dues à A. Selberg.* Colloque en l'honneur de H. Delange, juin 1982, Publication de l'Université Paris Sud - Orsay.

[Nor 1] K.K. NORTON. *On the number of restricted prime factors of an integer,* I. Illinois J. Math. 20, 1976, p. 681-705.

[Nor 3] K.K. NORTON. *On the number of restricted prime factors of an integer*, III. l'Enseignement Mathématique, t. 28, 1982, p. 31-52.

[Pom] C. POMERANCE. *On the distribution of round numbers.* Abstracts A.M.S. 3, 1982, p. 414.

[Ram] S. RAMANUJAN. *Collected Papers.* Chelsea publishing Company, 1962.

[Sar] P. ERDÖS and A. SARKÖZY. *On the number of prime factors of integers.* Acta Sci. Math. 42, 1980, p. 237-246.

[Sat] L.G. SATHE. *On a problem of Hardy on the distribution of integers having a given number of prime factors.* J. Indian Math. Soc. 17, 1953, p. 63-141 ; 18, 1954 ; p. 27-81.

[Sel] A. SELBERG. *Note on a paper by L.G. SATHE.* J. Indian Math. Soc. 18, 1954, p. 83-87.

J.L. NICOLAS

Département de Mathématiques
Université de Limoges
123 Avenue Albert Thomas
F-87060 LIMOGES Cédex
France

EXPONENTIAL SUMS OVER FINITE FIELDS

Harald NIEDERREITER

Let $\mathbb{F}_q$ be the finite field of order q. For $f \in \mathbb{F}_q[x_1,\ldots,x_r]$ and a nontrivial additive character χ of $\mathbb{F}_q$ define the character sum

$$C_1 = \sum_{a_1,\ldots,a_r \in \mathbb{F}_q} \chi(f(a_1,\ldots,a_r)).$$

Together with C_1 we consider lifted character sums corresponding to the various finite extensions $\mathbb{F}_{q^s}$ of $\mathbb{F}_q$ contained in a fixed algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. First, χ is lifted via the trace to a nontrivial additive character $\chi^{(s)}$ of $\mathbb{F}_{q^s}$; in detail, if Tr_s denotes the trace function from $\mathbb{F}_{q^s}$ onto $\mathbb{F}_q$, then set

$$\chi^{(s)}(a) = \chi(\mathrm{Tr}_s(a)) \quad \text{for} \quad a \in \mathbb{F}_{q^s}. \tag{1}$$

Now define

$$C_s = \sum_{a_1,\ldots,a_r \in \mathbb{F}_{q^s}} \chi^{(s)}(f(a_1,\ldots,a_r)).$$

With these lifted character sums one sets up the L-function

$$L(z) = \exp\Big(\sum_{s=1}^{\infty} \frac{C_s}{s} z^s\Big)$$

in the complex variable z. For $r = 1$ one has the classical results of A. Weil on these L-functions (see [5, Ch. 5]). For general r, Grothendieck [4] proved by methods of ℓ-adic cohomology that $L(z)$ is always a rational function. Bombieri [1] conjectured that $L(z)$ has the special form

$$L(z) = P(z)^{(-1)^{r-1}} \tag{2}$$

with a polynomial P, provided that f satisfies some kind of nonsingularity condition. In his famous paper on the Weil conjectures, Deligne [3] proved among other results that Bombieri's conjecture is true if $\deg(f)$ is not a multiple of the characteristic of $\mathbb{F}_q$ and the leading homogeneous part f_0 of f is nonsingular in the standard sense (i.e., there is no point over $\bar{\mathbb{F}}_q$ at which f_0 and all its first-order partial derivatives vanish simultaneously).

In a lecture given at the Oberwolfach Conference on Analytic Number Theory in 1982, S. A. Stepanov announced an elementary proof of the result of Deligne quoted above for the case where $\deg(f)$ is less than the characteristic of $\mathbb{F}_q$ (see [12]). According to the outline given by Stepanov, his method depends, first of all, on an explicit expansion of $L(z)$, where we assume for simplicity that r is odd (otherwise consider $L(z)^{-1}$):

$$L(z) = \exp\Big(\sum_{s=1}^{\infty} \frac{C_s}{s} z^s\Big) = \prod_{s=1}^{\infty} \exp\Big(\frac{C_s}{s} z^s\Big) = \prod_{j=1}^{\infty} \Big(\sum_{i_j=0}^{\infty} \frac{1}{i_j!} \cdot \frac{C_j^{i_j}}{j^{i_j}} z^{ji_j}\Big)$$

(3)

$$= 1 + \sum_{s=1}^{\infty} \Big(\sum_{i_1+2i_2+\ldots+si_s=s} \frac{C_1^{i_1} \ldots C_s^{i_s}}{i_1! \ldots i_s!\, 2^{i_2} \ldots s^{i_s}}\Big) z^s = : 1 + \sum_{s=1}^{\infty} \sigma_s z^s .$$

Now one has to show $\sigma_s = 0$ for all sufficiently large s. Stepanov claimed that he can do this by inserting the explicit form of the sums C_i, then fully expanding the resulting expression for σ_s and combining terms in a suitable way. In a brief note [13] summarizing the method, this point is brushed over. Since I could not get any further details from Stepanov, I tried to reconstruct his argument and I looked first for a simple test case.

It turns out that Stepanov had already used this method in his paper [11] to give an elementary proof of the Davenport-Hasse theorem for Gaussian

sums over finite fields. A closer inspection of this proof reveals, however, that it breaks down at a crucial step of the argument. This raises some doubts about the validity of Stepanov's claim at the Oberwolfach conference. But, obviously, a final verdict can only be given when Stepanov publishes his proof in full detail.

In order to elaborate on the error in [11], it is necessary to first describe the Davenport-Hasse theorem. Let ψ be a multiplicative and χ an additive character of $\mathbb{F}_q$, not both being trivial, and use the convention $\psi(0) = 0$. The corresponding Gaussian sum is defined by

$$G_1 = G(\psi,\chi) = \sum_{a\in\mathbb{F}_q} \psi(a)\,\chi(a).$$

The character ψ is lifted by means of the formula

$$\psi^{(s)}(a) = \psi(N_s(a)) \quad \text{for} \quad a\in\mathbb{F}_{q^s},$$

where N_s is the norm function from $\mathbb{F}_{q^s}$ onto $\mathbb{F}_q$. With $\chi^{(s)}$ being given by (1), we consider the lifted Gaussian sum

$$G_s = G(\psi^{(s)}, \chi^{(s)}) = \sum_{a\in\mathbb{F}_{q^s}} \psi^{(s)}(a)\,\chi^{(s)}(a).$$

The Davenport-Hasse theorem expresses the following simple relation between G_s and G_1.

<u>Davenport-Hasse Theorem.</u> $G_s = (-1)^{s-1} G_1^s$.

In the paper of Davenport and Hasse [2] this relation arose from the study of L-functions of an algebraic function field defined by an Artin-Schreier curve over $\mathbb{F}_q$. The paper contains also a proof of the formula based on the results of Stickelberger [14] concerning the factorization of Gaussian sums in cyclotomic fields. Schmid [10] has given an elementary proof of the Davenport-Hasse theorem by induction on s.

Although this is not made explicit, the method in Stepanov [11] for

proving the Davenport-Hasse theorem amounts to considering an L-function corresponding to Gaussian sums and expanding it as in (3):

$$L(z) = \exp\Big(\sum_{s=1}^{\infty} \frac{G_s}{s} z^s\Big) = 1 + \sum_{s=1}^{\infty} \gamma_s z^s$$

with

$$\gamma_s = \sum_{i_1+2i_2+\ldots+si_s=s} \frac{G_1^{i_1} \ldots G_s^{i_s}}{i_1! \ldots i_s!\, 2^{i_2} \ldots s^{i_s}}.$$

Then one tries to show $\gamma_s = 0$ for $s > 1$. In one of the key steps it is claimed in [11] that for a given solution of $i_1 + 2i_2 + \ldots + si_s = s$ in nonnegative integers $i_1,\ldots,i_s$ the number $N(t_1,\ldots,t_s)$ of tuples

$$(a_1^{(1)},\ldots,a_{i_1}^{(1)},\ldots,a_1^{(s)},\ldots,a_{i_s}^{(s)}),$$

with the first i_1 entries being in $\mathbb{F}_q$, the next i_2 entries being in $\mathbb{F}_{q^2}$,..., the last i_s entries being in $\mathbb{F}_{q^s}$, and with the elementary symmetric polynomials in the $a_i^{(j)}$ and their conjugates over $\mathbb{F}_q$ having prescribed values $t_1,\ldots,t_s \in \mathbb{F}_q$, is independent of $t_1,\ldots,t_s$. This statement is, however, incorrect. For instance, if $i_s = 0$ and

$$t(x) = x^s - t_1 x^{s-1} + t_2 x^{s-2} \mp \ldots + (-1)^s t_s$$

is irreducible over $\mathbb{F}_q$, then $N(t_1,\ldots,t_s) = 0$, whereas $N(0,\ldots,0) = 1$, as can be seen immediately from the factorization of $t(x)$ in its splitting field over $\mathbb{F}_q$. To provide another counterexample, we note that if $i_1 = s$, $i_2 = \ldots = i_s = 0$, then $N(t_1,\ldots,t_s) = 0$ whenever $t(x)$ does not split completely over $\mathbb{F}_q$, whereas $N(0,\ldots,0) = 1$ and $N(1,0,\ldots,0) = s$. The proof of the Davenport-Hasse theorem in [11] is therefore fallacious. Any attempt to repair it would have to be based on a correct formula for $N(t_1,\ldots,t_s)$. Such a formula will, however, be very complicated and lead to a rather involved proof of the Davenport-Hasse theorem.

We present now a short proof of the Davenport-Hasse theorem using a

technique in [5, Ch. 5]. Let $M = \{g \in \mathbb{F}_q[x] : g \text{ monic}\}$, $M_r = \{g \in M : \deg(g) = r\}$, $I = \{g \in M : g \text{ irreducible over } \mathbb{F}_q\}$, $I_d = \{g \in I : \deg(g) = d\}$. Define $\lambda : M \to \mathbb{C}$ by $\lambda(1) = 1$ and

$$\lambda(x^r - c_1 x^{r-1} + \ldots + (-1)^r c_r) = \psi(c_r)\chi(c_1) \quad \text{for } r \geq 1.$$

Then λ is multiplicative in the sense that $\lambda(gh) = \lambda(g)\lambda(h)$ for all $g, h \in M$. Splitting up G_s according to the degree of $a \in \mathbb{F}_{q^s}$ over $\mathbb{F}_q$, writing g_a for the minimal polynomial of a over $\mathbb{F}_q$, and using simple properties of Tr_s and N_s (see [5, Ch. 2]), we get for $|z| < q^{-1}$:

$$\sum_{s=1}^{\infty} \frac{G_s}{s} z^s = \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{d|s} \sum_{\deg(a)=d} (\psi^{(d)}(a)\chi^{(d)}(a))^{s/d}$$

$$= \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{d|s} \sum_{\deg(a)=d} \lambda(g_a)^{s/d} = \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{d|s} d \sum_{g \in I_d} \lambda(g)^{s/d}$$

$$= \sum_{d=1}^{\infty} \sum_{g \in I_d} \sum_{s=1}^{\infty} \frac{1}{s}(\lambda(g)z^d)^s = \sum_{d=1}^{\infty} \sum_{g \in I_d} \log \frac{1}{1-\lambda(g)z^d} = \log \prod_{g \in I} \frac{1}{1-\lambda(g)z^{\deg(g)}}.$$

In this Euler product $\lambda(g)z^{\deg(g)}$ is multiplicative as a function of g, hence

$$\sum_{s=1}^{\infty} \frac{G_s}{s} z^s = \log\Big(\sum_{g \in M} \lambda(g) z^{\deg(g)}\Big) = \log\Big(\sum_{r=0}^{\infty} \Big(\sum_{g \in M_r} \lambda(g)\Big) z^r\Big)$$

$$= \log(1 + G_1 z) = \sum_{s=1}^{\infty} \frac{1}{s} (-1)^{s-1} G_1^s z^s,$$

and comparison of coefficients yields the Davenport-Hasse theorem.

The same method can be applied to other exponential sums. For instance, if ψ_1 and ψ_2 are two multiplicative characters of $\mathbb{F}_q$, not both of them trivial, and if we fix a nonzero $b \in \mathbb{F}_q$, then we can consider the lifted Jacobi sums

$$J_s = \sum_{a \in \mathbb{F}_{q^s}} \psi_1^{(s)}(a)\psi_2^{(s)}(b-a).$$

With

$$\lambda(g) = \psi_1((-1)^{\deg(g)} g(0))\psi_2(g(b)) \quad \text{for } g \in M$$

we get then as above:

$$\sum_{s=1}^{\infty} \frac{J_s}{s} z^s = \log\Big(\sum_{r=0}^{\infty} \Big(\sum_{g \in M_r} \lambda(g)\Big) z^r\Big) = \log(1 + J_1 z) = \sum_{s=1}^{\infty} \frac{1}{s} (-1)^{s-1} J_1^s z^s,$$

and comparison of coefficients yields $J_s = (-1)^{s-1} J_1^s$, a formula first shown by Mitchell [6].

The Davenport-Hasse theorem can be used to establish a formula of the type (2) for L-functions corresponding to a general class of multiple exponential sums. For $1 \leq i \leq r$ let F_i be a finite field, let χ_i be a nontrivial additive character of F_i, and let ψ_i be an arbitrary multiplicative character of F_i. Let H_1 be a subgroup of the direct product $F_1^* \times \ldots \times F_r^*$ of index m, where F^* denotes the multiplicative group of a finite field F. If $F_{i,s}$ is the extension of F_i of degree s contained in a fixed algebraic closure of F_i, let

$$\overline{N}_s : F_{1,s}^* \times \ldots \times F_{r,s}^* \to F_1^* \times \ldots \times F_r^*$$

be the componentwise norm function and set $H_s = \overline{N}_s^{-1}(H_1)$.

For fixed $u \in F_1^* \times \ldots \times F_r^*$ define

$$(4) \quad E_s = m \sum_{(a_1,\ldots,a_r) \in u H_s} \chi_1^{(s)}(a_1) \ldots \chi_r^{(s)}(a_r)\, \psi_1^{(s)}(a_1) \ldots \psi_r^{(s)}(a_r).$$

Then set up the corresponding L-function

$$(5) \qquad L(z) = \exp\Big(\sum_{s=1}^{\infty} \frac{E_s}{s} z^s\Big).$$

Theorem 1. The L-function in (5) is of the form

$$L(z) = P(z)^{(-1)^{r-1}}$$

with a polynomial P of degree m satisfying $P(0) = 1$.

Proof. If $u = (u_1,\ldots,u_r) \in F_1^* \times \ldots \times F_r^*$, we can write

$$(6) \quad E_s = m \sum_{(a_1,\ldots,a_r) \in H_s} \chi_1^{(s)}(u_1 a_1) \ldots \chi_r^{(s)}(u_r a_r)\, \psi_1^{(s)}(u_1 a_1) \ldots \psi_r^{(s)}(u_r a_r).$$

For fixed s we use the Fourier expansion of the restriction of $\chi_i^{(s)}$ to $F_{i,s}^*$ with respect to the characters λ_i of that group:

$$(7)\quad \chi_i^{(s)}(c) = \frac{1}{q_i^s-1}\sum_{\lambda_i} G(\bar{\lambda}_i, \chi_i^{(s)})\,\lambda_i(c) \quad \text{for all } c \in F_{i,s}^*,$$

where q_i denotes the order of F_i, the Fourier coefficients are Gaussian sums, and $\bar{\lambda}_i$ is the conjugate character of λ_i. Inserting (7) in (6) we get

$$E_s = \frac{m}{(q_1^s-1)\dots(q_r^s-1)} \sum^{\sim}_{(a_1,\dots,a_r)\in H_s} \psi_1^{(s)}(u_1a_1)\dots\psi_r^{(s)}(u_ra_r)\cdot$$

$$\cdot \sum^{\sim}_{\lambda_1,\dots,\lambda_r} G(\bar{\lambda}_1, \chi_1^{(s)})\dots G(\bar{\lambda}_r, \chi_r^{(s)})\,\lambda_1(u_1a_1)\dots\lambda_r(u_ra_r)$$

$$= \frac{m}{(q_1^s-1)\dots(q_r^s-1)} \sum^{\sim}_{\lambda_1,\dots,\lambda_r} G(\bar{\lambda}_1, \chi_1^{(s)})\dots G(\bar{\lambda}_r, \chi_r^{(s)})(\psi_1^{(s)}\lambda_1)(u_1)\dots$$

$$(\psi_r^{(s)}\lambda_r)(u_r) \sum^{\sim}_{(a_1,\dots,a_r)\in H_s} (\psi_1^{(s)}\lambda_1)(a_1)\dots(\psi_r^{(s)}\lambda_r)(a_r).$$

Let A_s be the annihilator of H_s in the dual group of $F_{1,s}^*\times\dots\times F_{r,s}^*$. Then the inner sum has the value $|H_s|$ if $(\psi_1^{(s)}\lambda_1,\dots,\psi_r^{(s)}\lambda_r)\in A_s$ and 0 otherwise. Therefore,

$$(8)\quad E_s = \frac{m|H_s|}{(q_1^s-1)\dots(q_r^s-1)} \sum^{\sim}_{(\lambda_1,\dots,\lambda_r)\in A_s} G(\bar{\lambda}_1\psi_1^{(s)}, \chi_1^{(s)})\dots G(\bar{\lambda}_r\psi_r^{(s)}, \chi_r^{(s)})\,\lambda_1(u_1)$$

$$\dots\lambda_r(u_r).$$

Since $\bar{N}_s$ is surjective, we have

$$|\ker \bar{N}_s| = \frac{(q_1^s-1)\dots(q_r^s-1)}{(q_1-1)\dots(q_r-1)},$$

and from $H_1 \simeq H_s/\ker \bar{N}_s$ we get

$$(9)\qquad |H_s| = |H_1|\,\frac{(q_1^s-1)\dots(q_r^s-1)}{(q_1-1)\dots(q_r-1)}.$$

This implies

$$(10)\qquad |A_s| = \frac{(q_1^s-1)\dots(q_r^s-1)}{|H_s|} = \frac{(q_1-1)\dots(q_r-1)}{|H_1|} = |A_1|.$$

Since it is immediate that $(\lambda_1^{(s)},\dots,\lambda_r^{(s)})\in A_s$ whenever $(\lambda_1,\dots,\lambda_r)\in A_1$, it follows from (10) that A_s consists exactly of all $(\lambda_1^{(s)},\dots,\lambda_r^{(s)})$ with $(\lambda_1,\dots,\lambda_r)\in A_1$. Using this fact as well as (9) and the definition of m, the identity (8) attains the form

$$E_s = \sum_{(\lambda_1,\dots,\lambda_r)\in A_1} G(\bar{\lambda}_1^{(s)}\psi_1^{(s)},\chi_1^{(s)})\dots G(\bar{\lambda}_r^{(s)}\psi_r^{(s)},\chi_r^{(s)})\lambda_1^{(s)}(u_1)\dots\lambda_r^{(s)}(u_r).$$

Now we can apply the Davenport-Hasse theorem, and taking into account that $\lambda_i^{(s)}(u_i) = (\lambda_i(u_i))^s$, we get

$$E_s = (-1)^r \sum_{(\lambda_1,\dots,\lambda_r)\in A_1} ((-1)^r G(\bar{\lambda}_1\psi_1,\chi_1)\dots G(\bar{\lambda}_r\psi_r,\chi_r)\lambda_1(u_1)\dots\lambda_r(u_r))^s.$$

Since $|A_1| = m$, we can label the numbers

$$(11)\qquad (-1)^r G(\bar{\lambda}_1\psi_1,\chi_1)\dots G(\bar{\lambda}_r\psi_r,\chi_r)\lambda_1(u_1)\dots\lambda_r(u_r)$$

by $\omega_1,\dots,\omega_m$, so that

$$(12)\qquad E_s = (-1)^r \sum_{j=1}^{m} \omega_j^s.$$

For the L-function in (5) we obtain then

$$L(z) = \exp((-1)^r \sum_{s=1}^{\infty} \frac{z^s}{s} \sum_{j=1}^{m} \omega_j^s) = \exp((-1)^r \sum_{j=1}^{m} \sum_{s=1}^{\infty} \frac{1}{s} (\omega_j z)^s)$$

$$= \exp((-1)^{r-1} \sum_{j=1}^{m} \log(1-\omega_j z)) = P(z)^{(-1)^{r-1}}$$

with

$$P(z) = (1-\omega_1 z)\dots(1-\omega_m z).$$

Since the characters χ_i are nontrivial, we have $\omega_j \neq 0$ for $1 \leq j \leq m$, and the proof of Theorem 1 is complete.

The exponential sums in (4) include various classical exponential sums as special cases, such as Gaussian sums, Kummer cyclotomic periods, and products of such sums. They also include a class of character sums studied by the author in a number of papers (see [7], [8], [9]). This will be explained in the sequel.

Let (y_n), $n = 0,1,\ldots,$ be a linear recurring sequence in $\mathbb{F}_q$ satisfying the linear recurrence relation

(13) $$y_{n+k} = b_{k-1}\, y_{n+k-1} + \ldots + b_0 y_n, \qquad n = 0,1,\ldots,$$

with constant coefficients $b_{k-1},\ldots,b_0 \in \mathbb{F}_q$, $b_0 \neq 0$. To exclude a trivial case, we assume $(y_0,\ldots,y_{k-1}) \neq (0,\ldots,0)$. We can also assume that (13) is the linear recurrence relation of least order satisfied by (y_n), i.e., that

$$f(x) = x^k - b_{k-1}\, x^{k-1} - \ldots - b_0 \in \mathbb{F}_q[x]$$

is the minimal polynomial of (y_n) (compare with [5, Ch. 8]). Then the least period τ of (y_n) is equal to the least positive integer e such that $f(x)$ divides $x^e - 1$. We consider now the case where f has no multiple roots. Then

$$f = f_1 \ldots f_r$$

with distinct monic irreducible polynomials f_i over $K = \mathbb{F}_q$. Let v_i be a fixed root of f_i in its splitting field F_i over K, and let $\mathrm{Tr}_{F_i/K}$ denote the trace function from F_i onto K.

Lemma. Under the conditions above, there exist elements $u_i \in F_i$, $1 \leq i \leq r$, such that

$$y_n = \sum_{i=1}^{r} \mathrm{Tr}_{F_i/K}(u_i v_i^n) \quad \text{for} \quad n = 0,1,\ldots .$$

Proof. Let

(14) $$G(x) = \sum_{n=0}^{\infty} y_n\, x^n$$

be the generating function of (y_n). On account of the linear recurrence relation, it is of the form

$$G(x) = \frac{g(x)}{f^*(x)}$$

with $g \in \mathbb{F}_q[x]$, $\deg(g) < k$, and $f^*(x) = x^k f(1/x)$ being the reciprocal polynomial of f (compare with [5, Ch. 8]). By partial fraction decomposition,

$$G(x) = \sum_{i=1}^{r} \sum_{j=0}^{d_i-1} \frac{a_{ij}}{1-v_i q^j x},$$

where $d_i = \deg(f_i)$, and the elements $a_{ij} \in F_i$ are conjugate over K, i.e., $a_{ij} = a_{i0}^{q^j}$ for $0 \leq j \leq d_i - 1$. Expanding into formal power series, we get

$$G(x) = \sum_{i=1}^{r} \sum_{j=0}^{d_i-1} a_{ij} \sum_{n=0}^{\infty} v_i^{nq^j} x^n = \sum_{n=0}^{\infty} \Big(\sum_{i=1}^{r} \sum_{j=0}^{d_i-1} (a_{i0} v_i^n)^{q^j} \Big) x^n$$

$$= \sum_{n=0}^{\infty} \Big(\sum_{i=1}^{r} \mathrm{Tr}_{F_i/K}(a_{i0} v_i^n) \Big) x^n,$$

and comparison of coefficients with (14) yields the result of the lemma, with $u_i = a_{i0}$.

Since $f(0) = -b_0 \neq 0$, we have $v_i \neq 0$ for $1 \leq i \leq r$, and since f is the minimal polynomial of (y_n), we have $u_i \neq 0$ for $1 \leq i \leq r$. Now let χ be a nontrivial additive character of $K = \mathbb{F}_q$ and consider the character sum

$$\sum_{n=0}^{\tau-1} \chi(y_n) \tag{15}$$

extended over the period of (y_n). Then writing again $d_i = \deg(f_i)$ and using the lemma,

$$\sum_{n=0}^{\tau-1} \chi(y_n) = \sum_{n=0}^{\tau-1} \chi(\mathrm{Tr}_{F_1/K}(u_1 v_1^n)) \cdots \chi(\mathrm{Tr}_{F_r/K}(u_r v_r^n))$$

$$= \sum_{n=0}^{\tau-1} \chi^{(d_1)}(u_1 v_1^n) \cdots \chi^{(d_r)}(u_r v_r^n)$$

$$= \sum_{(a_1,\ldots,a_r) \in uH_1} \chi^{(d_1)}(a_1) \cdots \chi^{(d_r)}(a_r),$$

where $u = (u_1,\dots,u_r) \in F_1^* \times \dots \times F_r^*$ and H_1 is the cyclic subgroup of $F_1^* \times \dots \times F_r^*$ generated by $(v_1,\dots,v_r)$. Consequently, the character sum (15) is, apart from the factor m, a sum of the form E_1 in (4), with $\chi_i = \chi^{(d_i)}$ and trivial ψ_i for $1 \leq i \leq r$.

The identity (12), together with the form of the ω_j given by (11), immediately yields the estimate

$$|E_s| \leq m\,(q_1 \dots q_r)^{s/2}$$

for the sums E_s in (4), where q_i denotes the order of F_i. If all q_i are identical, then we can establish an estimate that is in a sense best possible.

Theorem 2. Let $F_i = \mathbb{F}_q$ for $1 \leq i \leq r$. Then there exist integers C and H with $0 < C \leq m$, $0 \leq H \leq r$, such that

$$|E_s| \leq C\, q^{sH/2} + (m - C)\, q^{s(H-1)/2} \quad \text{for all } s \geq 1.$$

Furthermore, for every $\varepsilon > 0$ there exist infinitely many s with

$$|E_s| \geq (C - \varepsilon)\, q^{sH/2}.$$

Proof. By (12) we have

$$|E_s| = \Big|\sum_{j=1}^{m} \omega_j^s\Big|,$$

where the ω_j are given by (11). For $0 \leq h \leq r$ let m_h be the number of $(\lambda_1,\dots,\lambda_r) \in A_1$ such that $\lambda_i = \psi_i$ holds for exactly h values of i. Then

$$\sum_{h=0}^{r} m_h = m. \tag{16}$$

We note the fact that for a multiplicative character ψ and a nontrivial additive character χ of $\mathbb{F}_q$ we have

$$|G(\psi,\chi)| = \begin{cases} 1 & \text{for } \psi \text{ trivial,} \\ q^{1/2} & \text{otherwise.} \end{cases}$$

Therefore,

$$|E_s| \leq \sum_{h=0}^{r} m_h \, q^{s(r-h)/2}. \tag{17}$$

Let H be the largest value of h with $m_{r-h} \neq 0$. Putting $C = m_{r-H}$, we get

$$|E_s| \leq C \, q^{sH/2} + (m-C) \, q^{s(H-1)/2} \quad \text{for all } s \geq 1,$$

where we used (16).

To prove the second part of Theorem 2, let $\epsilon > 0$ be given and let J be the set of those j, $1 \leq j \leq m$, for which $|\omega_j| = q^{H/2}$. For $j \in J$ we have

$$\omega_j = q^{H/2} \, e^{2\pi i \theta_j} \quad \text{with } \theta_j \text{ real.}$$

We note that the set J has C elements. Therefore, by Dirichlet's theorem on simultaneous diophantine approximations, there exist infinitely many s for which

$$\Big| \sum_{j \in J} e^{2\pi i s \theta_j} \Big| \geq C - \frac{\epsilon}{2}.$$

Consequently,

$$|E_s| \geq \Big|\sum_{j \in J} \omega_j^s\Big| - \Big|\sum_{j \notin J} \omega_j^s\Big| = q^{sH/2} \Big|\sum_{j \in J} e^{2\pi i s \theta_j}\Big| - \Big|\sum_{j \notin J} \omega_j^s\Big|$$

$$\geq (C - \tfrac{\epsilon}{2}) \, q^{sH/2} - (m - C) \, q^{s(H-1)/2} \geq (C - \epsilon) \, q^{sH/2}$$

for infinitely many s.

An interesting special case for applications is that of the character sums in (15), with the minimal polynomial f of (y_n) being irreducible over $\mathbb{F}_q$. In this case $r = 1$, $F_1 = \mathbb{F}_{q^k}$, and H_1 is the subgroup of F_1^* generated by a root v of f, so that $m = (q^k - 1)/\tau$. By the earlier discussion,

$$\sum_{n=0}^{\tau-1} \chi(y_n) = \frac{1}{m} E_1$$

for a sum E_1 of the form (4) with ψ_1 trivial. The lifted sum E_s, $s \geq 2$, corresponds to a subgroup H_s of $F_{1,s}^*$ of the same index m. Now H_s is

cyclic of order $\tau_s = (q^{ks} - 1)/m$, so we can choose a generator $v^{(s)}$ of H_s. Let $f^{(s)}$ be the minimal polynomial of $v^{(s)}$ over $\mathbb{F}_{q^s}$. It is clear that $d = \deg(f^{(s)})$ divides k. Suppose d were a proper divisor of k. Then it follows that

$$\tau_s = \frac{(q^{ks}-1)\tau}{q^k-1} = (q^{k(s-1)} + q^{k(s-2)} + \ldots + 1)\tau > q^{ks/2} > q^{sd} - 1.$$

On the other hand, $v^{(s)}$ is a nonzero element of the finite field of order q^{sd}, hence

$$(v^{(s)})^{q^{sd}-1} = 1,$$

which implies $\tau_s \leq q^{sd} - 1$, a contradiction. Thus we have $\deg(f^{(s)}) = k$. From the earlier discussion we see that there exists a linear recurring sequence $(y_n^{(s)})$ in $\mathbb{F}_{q^s}$ with minimal polynomial $f^{(s)}$ and least period τ_s such that

$$\sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) = \frac{1}{m} E_s.$$

For $s = 1$ we write $y_n^{(1)} = y_n$, $f^{(1)} = f$, and $\tau_1 = \tau$. From (17) and the second part of Theorem 2 we obtain then the following result.

Corollary. For all $s \geq 1$ we have

$$(18) \qquad \left| \sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) \right| \leq \left(1 - \frac{\tau_s}{q^{ks}-1}\right) q^{ks/2} + \frac{\tau_s}{q^{ks}-1}.$$

Furthermore, for every $\varepsilon > 0$ there exist infinitely many s with

$$\left| \sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) \right| \geq \left(1 - \frac{\tau_s}{q^{ks}-1} - \varepsilon\right) q^{ks/2}.$$

In case $\tau_s = q^{ks} - 1$ (i.e., $m = 1$), the second part of the corollary provides no information. But in this case it is easy to see directly that

$$\sum_{n=0}^{\tau_s-1} \chi^{(s)}(y_n^{(s)}) = -1,$$

and so (18) is again best possible.

REFERENCES

[1] E. BOMBIERI, On exponential sums in finite fields, Amer. J. Math. 88, 71-105(1966).

[2] H. DAVENPORT and H. HASSE, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. reine angew. Math. 172, 151-182(1935).

[3] P. DELIGNE, La conjecture de Weil. I, Inst. Hautes Etudes Sci. Publ. Math. 43, 273-307(1974).

[4] A. GROTHENDIECK, Formule de Lefschetz et rationalité des fonctions L, Sém. Bourbaki 1964/65, Exp. 279, Benjamin, New York, 1966.

[5] R. LIDL and H. NIEDERREITER, Finite Fields, Encyclopedia of Math. and Its Appl., vol. 20, Addison-Wesley, Reading, Mass., 1983.

[6] H. H. MITCHELL, On the generalized Jacobi-Kummer cyclotomic function, Trans. Amer. Math. Soc. 17, 165-177(1916).

[7] H. NIEDERREITER, Some new exponential sums with applications to pseudo-random numbers, Topics in Number Theory (Debrecen, 1974), Colloquia Math. Soc. János Bolyai, vol. 13, pp. 209-232, North-Holland, Amsterdam, 1976.

[8] H. NIEDERREITER, On the cycle structure of linear recurring sequences, Math. Scand. 38, 53-77(1976).

[9] H. NIEDERREITER, Quasi-Monte Carlo methods and pseudo-random numbers, Bull. Amer. Math. Soc. 84, 957-1041(1978).

[10] H. L. SCHMID, Relationen zwischen verallgemeinerten Gaußschen Summen, J. reine angew. Math. 176, 189-191(1937).

[11] S. A. STEPANOV, Proof of the Davenport-Hasse relations (Russian), Mat. Zametki 27, 3-6(1980).

[12] S. A. STEPANOV, Exponential sums in several variables and L-functions of Artin, Tagungsbericht Analytische Zahlentheorie, Math. Forschungsinst. Oberwolfach, 1982.

[13] S. A. STEPANOV, Rational trigonometric sums and Artin L-functions (Russian), Dokl. Akad. Nauk SSSR 265, 39-42(1982).

[14] L. STICKELBERGER, Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann. 37, 321-367(1890).

Mathematical Institute
Austrian Academy of Sciences
Dr. Ignaz-Seipel-Platz 2
A-1010 Vienna
Austria

A CORRECTION TO "REMARKS ON ELLIOTTs THEOREM ON MEAN-VALUES OF MULTIPLICATIVE FUNCTIONS" (DURHAM 1979/1981) AND SOME REMARKS ON ALMOST-EVEN NUMBER-THEORETICAL FUNCTIONS.

Wolfgang Schwarz
Frankfurt am Main

1. Introduction.

a) Denote by

(1.1) $$\mathfrak{G} = \mathrm{Lin}_{\mathbb{C}} \left[e_\alpha, \alpha \in \mathbb{R}/\mathbb{Z} \right]$$

and

(1.2) $$\mathfrak{B} = \mathrm{Lin}_{\mathbb{C}} \left[c_r,\ r=1,2,\dots \right]$$

the complex vector-spaces of linear combinations of exponentials

(1.3) $$e_\alpha : n \mapsto e^{2\pi i \alpha} ,$$

respectively Ramanujan sums

(1.4) $$c_r : n \mapsto \sum_{d \mid (n,r)} d \cdot \mu\left(\frac{r}{d}\right) = \sum_{\substack{a \bmod r \\ (a,r)=1}} \exp\left(2\pi i \cdot \frac{a}{r} \cdot n\right) .$$

Using the uniform norm

(1.5) $$\|f\|_u = \sup_{n \in \mathbb{N}} |f(n)|$$

respectively for $q \geq 1$ the (semi-)norms

(1.6) $$\|f\|_q = \left\{ \limsup_{x \to \infty} \frac{1}{x} \cdot \sum_{n \leq x} |f(n)|^q \right\}^{\frac{1}{q}} ,$$

we obtain the vector-spaces[1)]

(1.7) $\mathfrak{G}^u$ = $\|\cdot\|_u$-closure of $\mathfrak{G}$, $\mathfrak{B}^u$ = $\|\cdot\|_u$-closure of $\mathfrak{B}$,

(1.8) $\mathfrak{G}^q$ = $\|\cdot\|_q$-closure of $\mathfrak{G}$, $\mathfrak{B}^q$ = $\|\cdot\|_q$-closure of $\mathfrak{B}$,

of <u>almost-periodic</u>, respectively <u>almost-even</u> number-theoretical functions.

Denoting the null-spaces by

(1.9) $\mathfrak{n}^q = \{ f \in \mathfrak{G}^q,\ \|f\|_q = 0 \}$, resp. $\mathfrak{n}_1^q = \{ f \in \mathfrak{B}^q,\ \|f\|_q = 0 \}$,

the quotient spaces

$$A^q = \mathfrak{G}^q / \mathfrak{n}^q \qquad \text{and} \qquad B^q = \mathfrak{B}^q / \mathfrak{n}_1^q$$

are normed vector-spaces and <u>complete</u>[2)]. A^2, B^2 are Hilbert-spaces with the inner product $< f,g > = M(f \cdot \bar{g})$, where

$$M(f) = \lim_{x \to \infty} \frac{1}{x} \cdot \sum_{n \leq x} f(n) \tag{1.10}$$

denotes the <u>mean-value</u> of f (if this mean-value exists).

b) Denote by $\mathfrak{E}_q$ the set of arithmetical functions with the property that the four series

$$\begin{cases} S_1(f) = \sum_p p^{-1} \cdot (f(p)-1) , \\ S_2'(f) = \sum_{|f(p)| \leq \frac{3}{2}} p^{-1} \cdot |f(p)-1|^2 , \\ S_2''(f) = \sum_{|f(p)| > \frac{3}{2}} p^{-1} \cdot |f(p)|^q , \\ S_3(f) = \sum_p \sum_{k \geq 2} p^{-k} \cdot |f(p^k)|^q \end{cases} \tag{1.11}$$

---

1) In fact, $\mathfrak{G}$ and $\mathfrak{B}$ are algebras; $\mathfrak{G}^u$ and $\mathfrak{B}^u$ are complex algebras.

2) See KNOPFMACHER [19] .

are convergent. Extending a famous result of H.Delange [6], P.D.T.A.ELLIOTT[1] and independently H. DABOUSSI[2] proved the following

Theorem A . If $q>1$, and if $f : \mathbb{N} \to \mathbb{C}$ is multiplicative, then the following two conditions are equivalent.

(i) $\|f\|_q < \infty$, and the mean-value $M(f)$ exists and $M(f)$ is non-zero.

(ii) $f \in \mathcal{E}_q$, and for any prime p the relation

$$1 + p^{-1} \cdot f(p) + p^{-2} \cdot f(p^2) + \ldots \neq 0 \tag{1.12}$$

holds.

There are several simplifications or variants of the proof or extensions of this important result (see for example DABOUSSI-DELANGE [5] , H.DABOUSSI [3], HEPPNER [10], SCHWARZ-SPILKER [28] , the survey article [25] , and K.H. INDLEKOFER [12] , [13] , [16], [17]).

c) During the conference at Marseille-Luminy the author presented a simplified proof (due to the author and J.SPILKER jointly, see [29]) for the following result (which is contained in DABOUSSI [3]).

Theorem B_1 . If $f \in \mathcal{G}^q$, $q \geq 1$, is multiplicative and if $M(f) \neq 0$, then $f \in \mathcal{E}_q$ (and (1.12) holds).

For the special case $q=2$ the following stronger result (due to ELLIOTT [7], with a simplified proof by DABOUSSI-DELANGE [5] ; see also [24]) holds; this result was the basis for the above-mentioned proof of Theorem B_1 .

---

1) in [7] for $q=2$, in [9] for $q>1$; see also [8].

2) see [2]; the characterisation of almost-periodic multiplicative number-theoretic functions is given in [3].

Theorem B_2 . If f is multiplicative and $\|f\|_2 < \infty$, and if the mean-value M(f) exists and is non-zero, then $f \in \mathcal{E}_2$.

d) Since our proof of Theorem B_1 is to appear in "Analysis", it will not be reproduced here. Instead, the author would like to take the opportunity of correcting a grieve error in the proof of the main result of SCHWARZ-SPILKER [28] . This result is

Theorem B_3 . Let $q \geq 1$. If $f \in \mathcal{E}_q$ is multiplicative, then $f \in \mathcal{B}^q$.

The proof used the following partial results.

Proposition A. If $f \in \mathcal{E}_1$ is multiplicative, then $f \in \mathcal{B}^1$.

Proposition B. If $f \in \mathcal{E}_q$ is multiplicative, then $\|f\|_q < \infty$.

Proposition C. If $f \in \mathcal{E}_1$ is multiplicative and if $\|f\|_q < \infty$, then $f \in \mathcal{B}^q$.

Proposition A was deduced using RÉNYIs method (see [22]) and a relationship theorem of HEPPNER-SCHWARZ ([11] , stated in this paper as Lemma 3.1). Using the relationship theorem again it is rather easy to show Proposition B . However, in our paper [28] , we made the erroneous statement (Prop.4, p.333)

(1.13) If $f \in \mathcal{B}^1$, $q>1$, and $\|f\|_q < \infty$, then $f \in \mathcal{B}^q$;

due to the missing assumption of multiplicativity, the assertion (1.13) and its proof are wrong, as counter-examples, given in section 2, show.[1)]

It is the aim of this contribution to repair the error in [28] by proving Proposition C, and furthermore, to give some simple results on arithmetical functions belonging to $\mathcal{B}^q$.

---

1) G.HALÁSZ wondered if Proposition 4 is correct (Warszawa Banach Center, Sept.82). J.MAUCLAIRE found that Prop.4 is erroneous (oral communication of H.DABOUSSI, letter of MAUCLAIRE Sept.6, 1983; see also [21] . J.MAUCLAIRE and A.HILDEBRAND (letter of Sept.12,1983) provided me with counter-examples.

2. Counter-Examples

The statement (1.13) is wrong, as the following counter-examples (for q=2) show.

a) Define

$$f(n) = \begin{cases} n^{1/4} , & \text{if } n \text{ is a square,} \\ 0 , & \text{otherwise.} \end{cases}$$

Then $\|f\|_1 = 0$, $f \in \mathcal{B}^1$, and all Ramanujan coefficients

$$a_r(f) = M(f \cdot c_r) \cdot \frac{1}{\varphi(r)}$$

vanish. However

$$\sum_{n \le x} |f(n)|^2 = \sum_{m \le \sqrt{x}} m \sim \frac{1}{2} \cdot x ,$$

hence $M(|f|^2) = \frac{1}{2}$, therefore Parseval's equation

$$M(|f|^2) = \sum_{r=1}^{\infty} \varphi(r) \cdot |a_r(f)|^2$$

is violated, and so $f \notin \mathcal{B}^2$.

This example is due to J.MAUCLAIRE.

b) Define

$$g(n) = \begin{cases} \sqrt{\log n} , & \text{if } n \text{ is a prime ,} \\ 0 , & \text{otherwise .} \end{cases}$$

Then $\|g\|_1 = 0$, $g \in \mathcal{B}^1$, all the $a_r(f)$ are zero, but $M(|g|^2) = 1$, and so $g \notin \mathcal{B}^2$.

c) The functions $1+f, 1+g$ are in $\mathcal{B}^1$, $M(1+f) = 1 = M(1+g)$, but $1+f \notin \mathcal{B}^2$, $1+g \notin \mathcal{B}^2$.

d) A.HILDEBRANDs example is

$$f_q(n) = \begin{cases} 2^{k/q} , & \text{if } n = 2^k \text{ is a power of 2 ,} \\ 0 , & \text{otherwise .} \end{cases}$$

Then $\|f_q\|_r = 0$ for any $1 \le r < q$, $\|f_q\|_q > 0$, but $f \notin \mathcal{B}^q$.

3. Some Tools from Number Theory and Some Easy Results on Almost-Periodic Functions.

a) Define two multiplicative functions f,g to be *related*, abbreviated $f \sim g$, if

$$(3.1) \qquad \sum_p p^{-1} \cdot |f(p)-g(p)| < \infty .$$

Denote by $\mathcal{G}$ the set of functions

$$(3.2) \qquad \mathcal{G} = \Big\{ f: \mathbb{N} \to \mathbb{C}, f \text{ multiplicative}, \sum_p \sum_{k \geq 2} p^{-k} \cdot |f(p^k)| < \infty, \text{ and } \sum_p \Big| \frac{f(p)}{p} \Big|^2 < \infty \Big\},$$

and by $\mathcal{G}^*$ its subset

$$(3.3) \qquad \mathcal{G}^* = \Big\{ f \in \mathcal{G};\ \omega_f(p,s) := 1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \ldots \neq 0 \text{ in } \operatorname{Re} s \geq 1 \text{ for any prime } p \Big\}.$$

Then the following result is true[1] .

Lemma 3.1. Let f,g be multiplicative, $f \sim g$. Assume that $f,g \in \mathcal{G}$, and $f \in \mathcal{G}^*$. Then the multiplicative function h, defined by $g = f * h$, has the property

$$\sum_{n=1}^{\infty} \Big| \frac{h(n)}{n} \Big| < \infty .$$

Corollary. Let f,g satisfy the assumptions of Lemma 3.1. Then the following assertions are true.

(1) If M(f) exists, then M(g) exists, and

$$M(g) = M(f) \cdot \prod_p \Big(1 + \frac{h(p)}{p} + \ldots\Big) .$$

(2) If $f \in \mathcal{B}^1$ (resp. $f \in \mathcal{G}^1$), then $g \in \mathcal{B}^1$ (resp. $g \in \mathcal{G}^1$) .

(3) If all the Ramanujan-coefficients $a_r(f)$ (resp. all the Fourier-coefficients[2] $\hat{f}(\alpha)$) exist, then all the $a_r(g)$ (resp. all the $\hat{g}(\alpha)$) exist.

---

[1] HEPPNER-SCHWARZ [11] ; for weaker results, see DELANGE [6], LUCHT [20] , SCHWARZ [23].

[2] $\hat{f}(\alpha) = M(f \cdot \overline{e_\alpha})$.

Lemma 3.2. If $f \geq 0$ is multiplicative and if

$$(3.4) \qquad \sum_{p^k \leq y} \sum f(p^k) \cdot \log p^k \leq c_1 \cdot y \quad \text{for any } y \geq 1 ,$$

then

$$(3.5) \qquad \sum_{n \leq x} f(n) \leq c_2 \cdot x \cdot \exp\left\{ \sum_{p \leq x} \frac{f(p)-1}{p} + \sum_{p \leq x} \sum_{k \geq 2} \frac{f(p^k)}{p^k} \right\},$$

where c_2 only depends on c_1 .

This lemma is wellknown, the idea of the proof seems to be due to E.WIRSING ([30], Hilfssatz 2). Much stronger results are contained in WOLKE [31].

(b) The following statements are easily proved by simple approximation arguments, wellknown in the theory of almost-periodic functions.

(1) BESSELs inequality: If f is in $\mathcal{G}^1$ and $\|f\|_2 < \infty$, then

$$(3.6) \qquad \sum_{\alpha \in \mathbb{R}/\mathbb{Z}} |\hat{f}(\alpha)|^2 \leq \|f\|_2^2 .$$

(1') If f is in $\mathcal{B}^1$ and $\|f\|_2 < \infty$, then

$$\sum_{r} |a_r(f)|^2 \cdot \varphi(r) \leq \|f\|_2^2 .$$

(2) If $f \in \mathcal{G}^q$ then $|f| \in \mathcal{G}^q$; if $f \in \mathcal{B}^q$ then $|f| \in \mathcal{B}^q$.

(3) If $f \in \mathcal{G}^q$, $g \in \mathcal{G}^{q'}$, where $\frac{1}{q} + \frac{1}{q'} = 1$, then $f \cdot g \in \mathcal{G}^1$.

(4) If $t_1, t_2 \in \mathcal{B}$ are real-valued, then $\max(t_1,t_2)$ and $\min(t_1,t_2)$ are in $\mathcal{B}$.

(5) If $f \in \mathcal{B}^1$, then for any constant $c \geq 0$ the functions $f^* = \max(c, |f|)$ and $f_* = \min(c, |f|)$ are in $\mathcal{B}^1$.

For statement (5) see the corollary to Lemma 3.4.

Lemma 3.3.[1] If g is a bounded function in $\mathcal{G}^1$, and if f is in $\mathcal{G}^q$, then $g \cdot f$ is in $\mathcal{G}^q$.

[1] DABOUSSI [3], III.8. The same result is true for the spaces $\mathcal{B}^q$.

Lemma 3.4. If $\Psi : \mathbb{C} \to \mathbb{C}$ is Lipschitz-continuous[1], and if $f : \mathbb{N} \to \mathbb{C}$ is in $\mathfrak{B}^1$, then the composed function $\Psi \circ f$ is in $\mathfrak{B}^1$.

Corollary. If g in $\mathfrak{B}^1$ is real-valued and $c \in \mathbb{R}$, then $\max(g,c)$ and $\min(g,c)$ are in $\mathfrak{B}^1$.

Proof of Lemma 3.4. Given $\varepsilon > 0$, choose $t \in \mathfrak{B}$ for which $\|f-t\|_1 < \varepsilon/2K$. Then $\Psi \circ t$ is in $\mathfrak{B}$, and

$$\frac{1}{x} \cdot \sum_{n \le x} |(\Psi f)-(\Psi t)(n)| \le \frac{K}{x} \cdot \sum_{n \le x} |f(n)-t(n)| < \varepsilon ,$$

if x is sufficiently large.

The Corollary is deduced from the fact, that the functions $x \mapsto \max(x,c)$ and $x \mapsto \min(x,c)$ are Lipschitz-continuous.

Lemma 3.5. If f is in $\mathfrak{B}^1$ and if $\|f\|_q$ is finite, where $q > 1$, then $f \in \mathfrak{B}^r$ for any r satisfying $1 \le r < q$.

Proof. Assume without loss of generality that f is real-valued. The truncated function

$$f_K = \max\{-K, \min(f,K)\}$$

is in $\mathfrak{B}^1$ (see Corollary to Lemma 3.4). Since f_K is bounded, f_K is in $\mathfrak{B}^\ell$ for any $\ell \ge 1$ (see Lemma 3.3). Given r, $1 \le r < q$, define s,s' by $s' = \frac{q}{r} > 1$, $\frac{1}{s} + \frac{1}{s'} = 1$. Then, applying HÖLDERs inequality, we obtain

$$\Delta(x) := \frac{1}{x} \cdot \sum_{n \le x} |f(n)-f_K(n)|^r \le \frac{1}{x} \cdot \sum_{\substack{n \le x \\ |f(n)|>K}} |f(n)|^r$$

$$\le \left\{\frac{1}{x} \cdot \sum_{n \le x} |f(n)|^q\right\}^{\frac{1}{s'}} \cdot \left\{\frac{1}{x} \sum_{\substack{n \le x \\ |f(n)|>K}} 1\right\}^{\frac{1}{s}} .$$

---

[1] This means the existence of a constant K with the property $|\Psi(z)-\Psi(z')| \le K \cdot |z-z'|$ for all z, z' in $\mathbb{C}$.

Obviously

$$K^q \cdot \sum_{n\le x,\ |f(n)|>K} 1 \le \sum_{n\le x} |f(n)|^q ,$$

and so

$$\|f-f_K\|_r^r = \overline{\lim_{x\to\infty}}\ \Lambda(x) \le \|f\|_q^{q/s'} \cdot \left\{ \frac{1}{K^q} \cdot \|f\|_q^q \right\}^{\frac{1}{s}} < \epsilon ,$$

if K is sufficiently large. Therefore $f\in\mathfrak{B}^r$.

c) The next result is proved in DABOUSSI [3], using the Weierstraß approximation theorem.

Lemma 3.6.[1] If $g \ge 0$, $\alpha \ge 1$, and $\beta \ge 1$, then $g^\alpha \in \mathfrak{A}^\beta$ is equivalent with $g\in\mathfrak{A}^{\alpha\beta}$.

Corollary.[1] If $q \ge 1$, $g\in\mathfrak{A}^q$ and $g \ge 0$, then $g^{\frac{1}{2}q}\in\mathfrak{A}^2$.

Lemma 3.7. If $g\in\mathfrak{B}^q$ is nonnegative, $g_K = \min(g,K)$, then

$$\overline{\lim_{K\to\infty}}\ \|g-g_K\|_q = 0 .$$

Moreover, for any $\epsilon > 0$,

$$\limsup_{x\to\infty}\ \frac{1}{x} \cdot \sum_{\substack{n\le x \\ g(n)>K}} |g(n)|^q < \epsilon ,$$

if K is sufficiently large.

Proof. Given $\epsilon > 0$, choose $t\in\mathfrak{B}$, satisfying $\|g-t\|_q < \epsilon$. Assume $K > \sup_n |t(n)|$. Then

$$\frac{1}{x} \cdot \sum_{n\le x} |g(n)-g_K(n)|^q = \frac{1}{x} \cdot \sum_{\substack{n\le x \\ g(n)>K}} |g(n)-K|^q \le \frac{1}{x} \cdot \sum_{\substack{n\le x \\ g(n)>K}} |g(n)-t(n)|^q .$$

For $x\to\infty$ this last sum is less than

$$\|g-t\|_q^q < \epsilon^q .$$

---

[1] The same result is true for the spaces $\mathfrak{B}^q$.

The second assertion follows from

$$\sum_{\substack{n\le x\\ g(n)>K}} |g(n)|^q \le 2^q \cdot \sum_{\substack{n\le x\\ g(n)>\frac{1}{2}K}} |g(n) - \tfrac{1}{2}K|^q \ .$$

e) According to the elementary theory of Hilbert spaces (see for example HEWITT-STROMBERG [11a]) Parseval's equation

(3.7) $\quad f\in\mathfrak{C}^2$ implies $\sum_{\alpha\in\mathbb{R}/\mathbb{Z}} |\hat{f}(\alpha)|^2 = \|f\|_2^2$,

respectively

(3.7') $\quad f\in\mathfrak{B}^2$ implies $\sum_{r=1}^{\infty} |a_r(f)|^2 \cdot \varphi(r) = \|f\|_2^2$

is true, since (by definition of $\mathfrak{B}^2, \mathfrak{C}^2$) the orthonormal systems

$\left\{\frac{c_r}{\sqrt{\varphi(r)}}\ , r=1,2,\ldots\right\}$ resp. $\{e_\alpha, \alpha\in\mathbb{R}/\mathbb{Z}\}$ are "complete" in $\mathfrak{B}^2$ resp. $\mathfrak{C}^2$.

4. Correction of a Proof in [28] .

A first correction of the proof of the main-result of [28] , stated as Theorem B_3 in section 2, was given in [25] . This paper being not yet published, we sketch the procedure:

Having proved Proposition A and Proposition B in [28] , we define a function f_K by

$$f_K(n) = \prod_{p^k\|n,\ |f(p^k)|\le K} f(p^k) \ .$$

Then f_K is near f with respect to $\|\cdot\|_q$, if K is large. Furthermore f_K is in $\mathfrak{B}^1$, according to Proposition A. By Lemma 3.2, $\|f_K\|_r < \infty$ for any $r > q$, and so $f_K\in\mathfrak{B}^q$ by Lemma 3.5 and the proof for $f\in\mathfrak{B}^q$ is complete.

5. A second Proof of Theorem B_3 .

Proposition 5.1. *Suppose, f is multiplicative, the mean-value* $M(f) \neq 0$ *exists*[1], *and* $f \in \mathcal{E}_1$; *then the function* h, *defined by*[2]

$$h(n) = \frac{f(n)}{|f(n)|} ,$$

is in $\mathcal{B}^1$.

Proposition 5.1*. *If* $f \in \mathcal{B}^1$ *is multiplicative with mean-value* $M(f) \neq 0$, *then*[2]

$$h = f/|f|$$

is in $\mathcal{B}^1$.

Corollary 5.1. *If* f *is multiplicative, if* $f \in \mathcal{E}_1$, *if* $M(f) \neq 0$, *and if* $|f| \in \mathcal{B}^q$, *then* $f \in \mathcal{B}^q$.

Corollary 5.1*.[3] *If* $f \in \mathcal{B}^1$ *is multiplicative with mean-value* $M(f) \neq 0$, *and if* $|f| \in \mathcal{B}^q$, *then* $f \in \mathcal{B}^q$.

Proof of Proposition 5.1. Obviously $|h| \leq 1$. According to DELANGEs theorem [6] in the version of SCHWARZ-SPILKER ([27], Theorem 5.1., p.348, or Prop.A) the convergence of

$$S_1(h) = \sum p^{-1} \cdot \{1-h(p)\}$$

is sufficient for $h \in \mathcal{B}^1$. Since $\sum_{|f(p)| \leq \frac{1}{2}} p^{-1}$ and $\sum_{|f(p)| > \frac{1}{2}} p^{-1}$ are convergent (because $f \in \mathcal{E}_1$), we only have to prove that

$$S_1^{\S}(h) = \sum^{(\S)} p^{-1} \cdot \{1-h(p)\}$$

---

[1] The existence of M(f) follows, if Proposition A is used.

[2] If $f(n) = 0$, then define $h(n) = 0$.

[3] For the proof, Theorem B_1 is used.

is convergent, where (§) stands for the condition

$$(\S) \qquad \frac{1}{2} < |f(p)| \leq \frac{3}{2} .$$

Using

$$\frac{1}{|f(p)|} = 1 + \mathcal{O}\left(\big| |f(p)| - 1 \big| \right) ,$$

as long as $\big| |f(p)| - 1 \big| \leq \frac{1}{2}$,

we obtain

$$S_1^{\S}(h) = \Sigma^{(\S)}\, p^{-1} \cdot \left(|f(p)| - 1\right) - \Sigma^{(\S)}\, p^{-1} \cdot \left(f(p) - 1\right)$$
$$+ \mathcal{O}\left(\Sigma^{(\S)}\, p^{-1} \big| |f(p)| - 1 \big|^2 + \Sigma^{(\S)} p^{-1} \cdot |f(p) - 1| \cdot \big| |f(p)| - 1 \big| \right).$$

The convergence[1] of $S_1(|f|)$, $S_1(f)$, $S_2'(|f|)$ and $S_2'(f)$ gives the convergence of $S_1^{\S}(h)$.

Proof of Proposition 5.1*. The assumptions imply $f \in \mathcal{E}_1$ by Theorem $\mathcal{B}_1$, and Proposition 5.1. is applicable.

Proof of Corollary 5.1. By Proposition 5.1. the function h is in $\mathcal{B}^1$, and the assertion follows from Lemma 3.3.

The condition $M(f) \neq 0$ is necessary, as shown by the following

Example. $f(n) = \frac{1}{n} \cdot \mu(n)$ is multiplicative with $M(f) = \|f\|_1 = 0$ and so $f \in \mathcal{B}^1$. However, $h(n) = \mu(n)$ is not in $\mathcal{B}^1$.

Remark. Let $f \in \mathcal{B}^1$; if there exists a constant $\delta > 0$ such that[2]

---

[1] $f \in \mathcal{E}_1$ implies the convergence of $S_1^{\S}(f)$, of $S_1(|f|)$ and of $S_2'(|f|)$, by simple manipulations with infinite series (see [28], for example).

[2] The upper density of a set A of natural numbers is defined as

$$\overline{\operatorname{dens}}(A) = \limsup_{x \to \infty} \frac{1}{x} \cdot \#\{n \leq x, n \in A\} .$$

(5.1) $\overline{\text{dens}}\ \{n\ ;\ |f(n)| < \delta\} = 0$,

then $h = f/|f|$ is in $\mathcal{B}^1$.

Proof. Define $s_\delta : \mathbb{C} \to \mathbb{C}$ by

$$s_\delta(r \cdot e^{i\varphi}) = \begin{cases} e^{i\varphi}\ , & \text{if } r \geq \delta\ , \\ e^{i\varphi} \cdot \frac{r}{\delta}\ , & \text{if } 0 \leq r < \delta\ . \end{cases}$$

Then s_δ is Lipschitz-continuous, $s_\delta \circ f \in \mathcal{B}^1$, and

$$\sum_{n \leq x} |h(n) - s_\delta(f(n))| = \sum_{\substack{n \leq x \\ |f(n)| < \delta}} |h(n) - s_\delta(f(n))| = o(x)$$

by (5.1).

Theorem 5.2. If $f \in \mathcal{C}_1$ is multiplicative with non-zero mean-value $M(f)$, and if $\|f\|_q < \infty$ for some $q > 1$, then $f \in \mathcal{B}^q$.

Remark. The assumption $f \in \mathcal{C}_1$ may be replaced by $f \in \mathcal{B}^1$, according to Proposition A in section 1 and Theorem B_1 (note that $\mathcal{C}^1 \supset \mathcal{B}^1$) .

Proof of Theorem 5.2. By Proposition 5.1 and Lemma 3.3 it is sufficient to prove $|f| \in \mathcal{B}^q$. Put

$$g = |f|^{\frac{1}{2}q}\ .$$

Then g is multiplicative and nonnegative, with norm $\|g\|_2 = \|f\|_q < \infty$; furthermore $g \in \mathcal{B}^1$: If $q \geq 2$, then $1 \leq \frac{1}{2} \cdot q < q$, and so $|f|^{\frac{1}{2}q} \in \mathcal{B}^1$ by Lemma 3.5 ; if $1 < q \leq 2$, then by Lemma 3.6 and its Corollary $|f| \in \mathcal{B}^1$, $|f|^{\frac{1}{2}} \in \mathcal{B}^2$, and

$$|f|^{\frac{1}{2}q} \in \mathcal{B}^{\frac{2}{q}} \subset \mathcal{B}^1\ ,$$

because $1 < q \leq 2$.

Moreover the mean-value M(g) is non-zero: this is simple, if $q \geq 2$; a proof for any $q \geq 1$ is given in [29] .

By the Theorem of ELLIOTT-DABOUSSI-DELANGE (quoted as Theorem B_2) we obtain the convergence of the series

$$S_1(g) = \sum \frac{1}{p} \cdot \big(g(p)-1\big) , \tag{5.21}$$

$$S_2(g) = \sum \frac{1}{p} \cdot (g(p)-1)^2 \tag{5.22}$$

and

$$S_3(g) = \sum_{p,k\geq 2} p^{-k} \cdot g^2(p), \tag{5.23}$$

Using $x^2-1 = (x-1)^2 + 2(x-1)$, (5.21) and (5.22), it follows that the series

$$\sum \frac{1}{p} \cdot (|f(p)|^q-1) \tag{5.31}$$

and

$$\sum_{|f(p)|>\frac{3}{2}} \frac{1}{p} \cdot |f(p)|^q \tag{5.32"}$$

are convergent. The series $S_3(g)$ is equal to

$$\sum_{p,k\geq 2} p^{-k} \cdot |f(p^k)|^q < \infty \ . \tag{5.33}$$

Using $(y^2-1)^2 = \mathcal{O}(|y-1|^2)$ in $0 \leq y \leq c$, and (5.22), we finally get

$$\sum_{|f(p)|\leq \frac{3}{2}} \frac{1}{p} \cdot (|f(p)|^q-1)^2 < \infty \ . \tag{5.32'}$$

Therefore, by Proposition A, the function $|f|^q$ is in $\mathcal{B}^1$, and so

$$|f| \in \mathcal{B}^q \ .$$

Remark. For a proof of Theorem 5.2, by the reduction arguments given in this section, it is sufficient to prove the special case

Theorem 5.2*. If $g \in \mathcal{E}_1$ is multiplicative and nonnegative, with mean-value $M(g) \neq 0$, and if $\|g\|_2 < \infty$, then $g \in \mathfrak{B}^2$.

6. Calculation of Ramanujan Coefficients.

In this section we sketch a proof of

Theorem 6.1. If f in $\mathcal{E}_1$ is completely multiplicative, and $M(f) \neq 0$, then the Ramanujan coefficients are given by

$$(6.1) \qquad a_r(f) = M(f) \cdot \frac{1}{\varphi(r)} \cdot (f*\mu)(r) ,$$

where $*$ denotes the convolution product.

If in addition $\|f\|_2 < \infty$, then

$$(6.2) \qquad \sum_{r=1}^{\infty} |a_r(f)|^2 \cdot \varphi(r) = \prod_p \frac{p-1}{p-|f(p)|^2} .$$

Proof. By a wellknown formula for the Ramanujan sums,

$$a_r(f) = \frac{1}{\varphi(r)} \cdot \lim_{x \to \infty} \frac{1}{x} \cdot \sum_{n \leq x} f(n) \cdot \sum_{d|(n,r)} d \cdot \mu\left(\frac{r}{d}\right)$$

$$= \frac{1}{\varphi(r)} \cdot \sum_{d|r} d\mu\left(\frac{r}{d}\right) \cdot \frac{f(d)}{d} \cdot M(f)$$

$$= M(f) \cdot \frac{1}{\varphi(r)} \cdot (f*\mu)(r)$$

(where $*$ denotes convolution), and so $a_r(f)/M(f)$ is multiplicative. If $\|f\|_2 < \infty$, then BESSELs inequality (Lemma 3.7) implies the absolute convergence of $A = \sum |a_r|^2 \cdot \varphi(r)$. By multiplicativity, with the abbreviation $a_r^* = a_r/M(f)$, we obtain

$$A = |M(f)|^2 \cdot \prod_p \left(1 + |a_p^*|^2 \cdot \varphi(p) + |a_{p^2}^*|^2 \cdot \varphi(p^2) + \ldots\right) .$$

(6.1) gives

$$(6.3) \qquad a^*_{p^k}(f) = \frac{\{f(p)\}^{k-1}}{\varphi(p^k)} \cdot \{ f(p)-1 \} \ ,$$

and so

$$A = |M(f)|^2 \cdot \prod_p \left(1 + \frac{|f(p)-1|^2}{p-1} \cdot \left\{1 - \frac{|f(p)|^2}{p}\right\}^{-1}\right) .$$

Using the product representation

$$M(f) = \prod_p \frac{p-1}{p-f(p)} \ ,$$

we get (after a short calculation)

$$A = \prod_p \frac{(p-1)}{p-|f(p)|^2} \ .$$

Remark. The conditions $f \in \mathcal{E}_1$, $\|f\|_2 < \infty$, and $M(f) \neq 0$ imply, that the geometric series occuring in the proof are convergent and that the denominators do not vanish.

This result enables us, to give another proof of Theorem 5.2* in the special case of completely multiplicative functions.

Theorem 6.2. If $g \in \mathcal{E}_1$ is completely multiplicative and nonnegative with mean-value $M(g) \neq 0$, and if $\|g\|_2 < \infty$, then $g \in \mathcal{B}^2$.

Proof. We are going to show the convergence of the four series

$$(6.4.1) \qquad S_1(g^2) = \sum \frac{g^2(p)-1}{p} \ ,$$

$$(6.4.2') \qquad S'_2(g^2) = \sum_{g^2(p) \leq \frac{3}{2}} \frac{(g^2(p)-1)^2}{p} \ ,$$

$$(6.4.2'') \qquad S''_2(g^2) = \sum_{g^2(p) > \frac{3}{2}} \frac{g^2(p)}{p} \ ,$$

$$(6.4.3) \qquad S_3(g^2) = \sum_{p,k \geq 2} p^{-k} \cdot |g(p^k)|^2 \ .$$

Having done this, $g^2 \in \mathfrak{B}^1$ by proposition A, and so $g \in \mathfrak{B}^2$ (by Lemma 3.6, Corollary).

The assumption $g \in \mathcal{E}_1$ implies the convergence of $S_1(g)$, $S_2'(g)$, $S_2''(g)$, $S_3(g)$. $\|g\|_2 < \infty$, BESSELs inequality and (6.3) imply

$$\sum_{\substack{p,k \geq 1 \\ |g^2(p)| \geq \frac{1}{2}}} p^{-k} \cdot |g(p^k|^2 \leq 9 \cdot \|g\|_2^2 \ .$$

Therefore $S_3(g^2)$ and $S_2''(g^2)$ are convergent. The identities

$$(g^2-1)^2 = (g-1)^2(g+1)^2$$

and

$$g^2-1 = (g-1)^2 + 2(g-1)$$

in connection with the convergence of $S_1(g)$, $S_2'(g)$ and $S_2''(g^2)$ imply the convergence of (6.4.2') and (6.4.1), and Theorem 6.2 is proved.

Bibliography

[1] E.Cohen, A class of arithmetical functions, Proc. Nat.Acad.Sci. USA 41 (1955), 939-944.

[2] H.Daboussi, Sur les fonctions multiplicatives ayant une valeur moyenne non nulle. Preprint Univ.de Paris-Sud 1978, 1-21; Bull.Soc.Math.France 109 (1981), 183-205.

[3] H.Daboussi, Caractérisation des fonctions multiplicatives p.p.B^{λ} à spectre non vide. Preprint Univ.de Paris-Sud 1978; Ann.Inst.Fourier Grenoble 30 (1980), 141-166.

[4] H.Daboussi and H.Delange, Quelques propriétés des fonctions multiplicatives de module au plus égal à 1 . C.R.Acad.Sci Paris 278 (1974), A 657-660.

[5] H.Daboussi and H.Delange, On a theorem of P.D.T.A. Elliott on multiplicative functions. J.London Math.Soc. 14 (1976), 345-356.

[6] H.Delange, Sur les fonctions arithmétiques multiplicatives. Ann.Sci.de l'École Norm.Sup. 78 (1961), 273-304.

[7] P.D.T.A.Elliott, A mean-value theorem for multiplicative functions. Proc.London Math.Soc.(3) 31 (1975), 418-438.

[8] P.D.T.A.Elliott, Probabilistic Number Theory, Vol.I, Vol.II. Springer Grundlehren, New York - Heidelberg - Berlin 1979, 1980.

[9] P.D.T.A.Elliott, Mean Value Theorems for multiplicative functions bounded in mean α-power, $\alpha > 1$. J.Austral.Math.Soc.Ser.A 29 (1980), 177-205.

[10] E.Heppner, Über Mittelwerte multiplikativer zahlentheoretischer Funktionen, Ann.Univ.Sci. Budapest 25 (1982), 85-96.

[11] E.Heppner und W.Schwarz, Benachbarte multiplikative Funktionen, Studies in Pure Mathematics. Dem Andenken Paul Turáns gewidmet, 1983, 323-336.

[11a] E.Hewitt and K.Stromberg, Real and Abstract Analysis, Springer-Grundlehren, Berlin - Heidelberg - New York 1969.

[12] K.H.Indlekofer, A mean value theorem for multiplicative functions, Math.Z. 172 (1989), 255-271.

[13] K.H. Indlekofer, Properties of uniformly summable multiplicative functions, Preprint 1980.

[14] K.H. Indlekofer, Some results on the behaviour of additive and multiplicative functions, Preprint, Nov. 1980.

[15] K.H. Indlekofer, Remark on a theorem of G. Halász, Archiv Math. 36 (1981), 145-151.

[16] K.H. Indlekofer, Some remarks on almost-even and almost-periodic functions, Archiv Math. 37 (1981), 353-358.

[17] K.H. Indlekofer, Limiting distributions and mean-values of arithmetical functions, J. Reine Angew. Math. 328 (1981), 116-127.

[18] J. Knopfmacher, Abstract Analytic Number Theory, Amsterdam-Oxford 1975.

[19] J. Knopfmacher, Fourier Analysis of Arithmetical Functions. Annali di Matematica pura ed applicata (IV), Vol. 109 (1976), 177-201.

[20] L. Lucht, Über benachbarte multiplikative Funktionen, Archiv Math. 30 (1978), 40-48.

[21] J. Mauclaire, Fonctions arithmétiques et analyse harmonique, Analytic Number Theory, Proc. Symp. Tokyo 1980, Maison Franco Japonaise, Tokyo, 1981, p. 83-94.

[22] A. Rényi, A new proof of a theorem of Delange, Publ. Math. Debrecen 12 (1965), 323-329.

[23] W. Schwarz, Eine weitere Bemerkung über multiplikative Funktionen, Coll. Math. 28 (1973), 82-89.

[24] W. Schwarz, Fourier-Ramanujan-Entwicklungen zahlentheoretischer Funktionen mit Anwendungen, Festschrift der Wissenschaftlichen Gesellschaft, Franz Steiner Verlag, Wiesbaden 1981, 399-415.

[25] W. Schwarz, Remarks on the Theorem of Elliott and Daboussi, and Applications. Preprint; to appear in the Banach Center Volume, Warszawa (1982).

[26] W. Schwarz und J. Spilker, Eine Anwendung des Approximationssatzes von Weierstraß-Stone auf Ramanujan-Summen, Nieuw Archief voor Wiskunde (3) 19 (1971), 198-209.

[27] W. Schwarz and J. Spilker, Mean-Values and Ramanujan Expansions of Almost Even Functions, Coll. Math. Soc. Jànos Bolyai, Debrecen 1974 (1976), 315-357.

[28] W.Schwarz and J.Spilker, Remarks on Elliott's Theorem on Mean-Values of Multiplicative Functions, Recent Progress in Analytic Number Theory, Durham 1979, Vol.I Academic Press London 1981, 325-339.

[29] W.Schwarz und J.Spilker, Eine Bemerkung zur Charakterisierung der fast-periodischen multiplikativen Funktionen mit von Null verschiedenem Mittelwert, Preprint 1982/83, to appear in Analysis.

[30] E.Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen, Math.Ann. 143 (1961), 75-102.

[31] D.Wolke, Multiplikative Funktionen auf schnell wachsenden Folgen. J.Reine Angew.Math. 251 (1971), 54-67.

Author's address

Dr.Wolfgang Schwarz
Department of Mathematics
University of Frankfurt
Robert-Mayer-Straße 10

D 6000 Frankfurt am Main

Théorèmes taubériens avec restes

Gérald Tenenbaum

En Théorie des Nombres, les théorèmes taubériens servent surtout à relier le comportement analytique d'une série de Dirichlet,

$$\sum_{n=1}^{\infty} a_n n^{-s},$$

au comportement asymptotique de la fonction sommatoire de ses coefficients

$$A(x) = \sum_{n \leqslant x} a_n .$$

Ces théorèmes sont usuellement valables sous des hypothèses très générales et, partant, d'emploi facile. Ils présentent en revanche un défaut de précision endémique, dont la nature intrinsèque est attestée par de nombreux contre-exemples.

Il est pourtant fréquent que l'existence d'un terme reste explicite se révèle indispensable à l'utilisation d'une estimation taubérienne. Considérons par exemple une somme double

$$\sum_{mn \leqslant x} a_{mn} = \sum_{n \leqslant x} \sum_{m \leqslant x/n} a_{mn} .$$

Alors qu'un simple équivalent, pour chaque m fixé, de la somme intérieure est insuffisant dans la plupart des cas, une formule uniforme avec terme reste explicite permet le report dans la somme externe et l'évaluation de l'expression initiale. Dans ce contexte, la qualité de la dépendance en x/n du terme reste s'avère relativement secondaire et c'est l'uniformité en m qui joue un rôle crucial.

Nous nous proposons de présenter ici des formes avec restes des deux théorèmes taubériens les plus utilisés en Arithmétique : le Théorème de Hardy-Littlewood-Karamata, et celui de Wiener-Ikehara.

1. Le Théorème de Hardy-Littlewood-Karamata.

Citons d'abord la forme classique du résultat.

Théorème 1. *Soit $A(u)$ une fonction non décroissante telle que l'intégrale de Laplace-Stieltjes*

$$(1) \qquad f(\sigma) = \int_0^\infty e^{-\sigma u}\, dA(u)$$

converge pour $\sigma > 0$. *S'il existe deux réels* c, ω, $\omega > 0$, *tels que*

$$(2) \qquad f(\sigma) = (c + o(1))\, \sigma^{-\omega} \ , \ (\sigma \to 0+) \ ,$$

alors on a

$$(3) \qquad A(x) = \left(\frac{c}{\Gamma(\omega+1)} + o(1)\right) x^{\omega} \ , \quad (x \to +\infty) \ .$$

Le schéma de la démonstration de Karamata [13] est le suivant. La relation (1) implique

$$\int_0^\infty e^{-n\sigma u}\, e^{-\sigma u}\, dA(u) = \frac{c+o(1)}{[(n+1)\sigma]^{\omega}} = \left(\frac{c}{\Gamma(\omega+1)} + o(1)\right) \sigma^{-\omega} \int_0^\infty e^{-nu}\, e^{-u}\, u^{\omega-1}\, du \ ,$$

$$(n = 0, 1, 2, \ldots) \ ,$$

d'où

$$\int_0^\infty P(e^{-\sigma u})\, e^{-\sigma u}\, dA(u) = \left(\frac{c+o(1)}{\Gamma(\omega)}\right) \sigma^{-\omega} \int_0^\infty P(e^{-u})\, e^{-u}\, u^{\omega-1}\, du \ ,$$

pour chaque polynôme fixé P . On utilise ensuite le Théorème d'Approximation de Weierstrass pour montrer que l'on peut remplacer dans la formule précédente le polynôme P par la fonction χ définie sur $[0,1]$ par

$$e^{-u}\, \chi(e^{-u}) = \begin{cases} 1 \ , & (0 \leqslant u \leqslant 1) \ , \\ 0 \ , & (u > 1) \ . \end{cases}$$

Cela fournit exactement l'estimation souhaitée.

On peut s'attendre à ce qu'une forme effective du Théorème d'Approximation permette de rendre effectif le résultat. Ce projet a été réalisé par G. Freud au début des années 50 [5] .

Théorème 2 (Freud). *Dans les hypothèses du Théorème* 1 , *et si l'on suppose en outre que le terme reste de* (2) *est* $O(\sigma^{\delta})$ *pour un* $\delta > 0$ *fixé, alors le terme reste de* (3) *est* $O(1/\log x)$.

La conclusion est optimale, comme le montre le contre-exemple suivant de Karamata : pour le choix

$$A(u) = \int_0^u (1 + \cos((\log t)^2))\ dt\ ,$$

une étude de l'intégrale (1) par la formule de Cauchy (cf [12], p.p. 168-169) permet d'établir que

$$f(\sigma) = \frac{c}{\sigma} + 0(1)\ ,\quad (\sigma \to 0+)\ ,$$

alors qu'une intégration par parties implique

$$A(x) = Cx + \Omega\left(\frac{x}{\log x}\right)\ ,\quad (x \to +\infty)\ .$$

Il est expliqué dans [5], [7], comment le Théorème 2 découle simplement du résultat d'approximation unilatérale en norme L^1 suivant.

Théorème 3 (Freud [5]; Freud et Ganelius [6]). *Soit h une fonction à variation bornée sur $[0,1]$. Il existe des constantes $A = A(h)$ et $B = B(h)$ telles qu'à chaque entier $n > 1$ correspondent des polynômes de degré n, P^+ et P^-, dont les coefficients ne dépassent pas B^n en valeur absolue, et qui satisfont à*

$$P^-(x) \leqslant h(x) \leqslant P^+(x)\ ,\quad (0 \leqslant x \leqslant 1)\ ,$$

$$\int_0^1 (P^+(x) - P^-(x))\ dx \leqslant A/n\ .$$

Si l'on affaiblit légèrement la conclusion en remplaçant la dernière majoration par $A(h;\varepsilon)\ n^{\varepsilon-1}$ (où $\varepsilon > 0$ est arbitrairement petit), le résultat peut être prouvé très simplement. Nous donnons les détails, à titre de curiosité, dans l'Appendice 1. Le point essentiel est l'utilisation des puissances du noyau de Fejer. Il serait intéressant de savoir si l'emploi d'un autre noyau permet d'obtenir la conclusion optimale du Théorème 3.

En termes de séries de Dirichlet, le Théorème de Hardy-Littlewood-Karamata lie le comportement de $\sum_{n=1}^{\infty} a_n n^{-\sigma}$ pour $\sigma > 1$ à celui de $\sum_{n \leqslant x} a_n n^{-1}$. On peut concevoir ce théorème comme un passage à la limite, du cas $\sigma > 1$ au cas $\sigma = 1$. Un tel "théorème taubérien limite" ne suppose rien sur les valeurs en des points non réels de la série de Dirichlet et ne permet pas de prouver le Théorème des Nombres Premiers. Ainsi le Théorème 2, par exemple, appliqué à

$$A(u) = \sum_{n \leqslant e^u} (1 + \mu(n))/n\ ,$$

fournit seulement l'estimation

$$\sum_{n \leqslant x} \mu(n)/n \ll \log x / \log\log x , \quad (x \to +\infty) .$$

2. Le Théorème de Wiener-Ikehara.

Il s'agit maintenant de donner une information asymptotique sur la fonction sommatoire $\sum_{n \leqslant x} a_n$ en n'utilisant que des hypothèses sur les valeurs de la série de Dirichlet en des points $s = \sigma + i\tau$ d'abscisse $\sigma > 1$. Intuitivement, on passe du cas $\sigma > 1$ au cas $s = 0$; il y a discontinuité entre l'hypothèse et la conclusion - ce qui suggère l'appellation de "théorème taubérien transcendant". Un résultat de ce type est de "profondeur" équivalente à celle du Théorème des Nombres Premiers.

Enonçons maintenant une forme classique [4] , essentiellement due à Ingham [11], du Théorème de Wiener-Ikehara, dont elle constitue en fait une généralisation.

Théorème 4 (Wiener-Ikehara-Ingham). *Soit $A(u)$ une fonction non décroissante telle que l'intégrale*

$$(4) \qquad f(s) = \int_0^\infty e^{-su} \, dA(u)$$

converge pour $\sigma > a > 0$. S'il existe des constantes c, ω, $\omega > -1$, telles que la fonction

$$(5) \qquad g(s) = \frac{f(s+a)}{s+a} - \frac{c}{s^{\omega+1}} , \quad (\sigma > 0) ,$$

satisfasse pour chaque $T > 0$ fixé à

$$(6) \quad \eta(\sigma,T) := \sigma^\omega \int_{-T}^{T} |g(2\sigma+i\tau) - g(\sigma+i\tau)| \, d\tau = o(1) , \quad (\sigma \to 0+) ,$$

alors on a

$$(7) \qquad A(x) = \left(\frac{c}{\Gamma(\omega+1)} + o(1) \right) e^{ax} x^\omega , \quad (x \to +\infty) .$$

De nombreuses démonstrations de ce théorème ou de ses variantes ou généralisations sont disponibles dans la littérature - cf. par exemple [2], [3], [4], [11]. A notre connaissance, la seule qui conduise à un terme reste est celle de Ganelius dans son livre [9] . Son argument repose sur une version locale de l'inégalité de Bohr [1]

$$\|f\|_\infty \ll \|f'\|_\infty / T$$

valable pour toute fonction f intégrable, bornée ainsi que sa dérivée sur $\mathbb{R}$, et

dont la transformée de Fourier $\hat{f}(\tau)$ est nulle pour $|\tau| \leqslant T$. Nous citons ici une forme légèrement affaiblie du théorème de Ganelius, qui est cependant suffisante pour les applications que nous envisageons. La démonstration procède d'idées très voisines de celle du Théorème de Berry et Esseen en Probabilités.

Théorème 5 (Ganelius). *Soit g une fonction intégrable et bornée sur $\mathbb{R}$. Il existe une constante absolue C telle que, sous les conditions*

$$\sup_{x < y \leqslant x+1/T} (g(y) - g(x)) \leqslant K \quad , \quad (x \in \mathbb{R}) \ ,$$

$$\hat{g}(\tau) = \int_{-\infty}^{+\infty} e^{-i\tau u}\, g(u)\, du = 0 \quad , \quad (|\tau| \leqslant T) \ ,$$

on ait

$$\|g\|_\infty = \sup_{x \in \mathbb{R}} |g(x)| \leqslant CK \ .$$

Un emploi du Théorème 5 calqué sur celui qu'en fait Ganelius conduirait à un théorème taubérien effectif aux hypothèses assez inhabituelles et ne généralisant pas entièrement le Théorème 4. Nous procédons d'une manière un peu différente, en remarquant que le Théorème 5 implique directement un résultat qui contient à la fois le théorème de Berry et Esseen (cf. Appendice 2) et une forme avec reste du Théorème 4.

Théorème 6. *Soit g une fonction intégrable et bornée sur $\mathbb{R}$. Sous l'hypothèse (8), on a*

$$\|g\|_\infty \ll K + \int_{-T}^{T} |\hat{g}(\tau)|\, d\tau \ .$$

Démonstration. Il suffit d'appliquer le Théorème 5 à $g - f$ où f est la convolée de g avec la fonction intégrable $\alpha(u) = (2/\pi u^2\varepsilon)\, \sin(\varepsilon u/2)\, \sin(u(T+\varepsilon/2))$ dont la transformée de Fourier est la fonction trapezoïdale

$$\hat{\alpha}(\tau) = \begin{cases} 1 & , \ (|\tau| \leqslant T) \ , \\ (T + \varepsilon - |\tau|)/\varepsilon & , \ (T < |\tau| \leqslant T+\varepsilon) \ , \\ 0 & , \ (|\tau| > T+\varepsilon) \ . \end{cases}$$

Comme $\hat{f} = \hat{g}\hat{\alpha}$ est à support compact, on a

$$\|f\|_\infty \leqslant \frac{1}{2\pi}\, \|\hat{f}\|_1 \leqslant \frac{1}{2\pi} \int_{-T-\varepsilon}^{T+\varepsilon} |\hat{g}(\tau)|\, d\tau$$

La conclusion en découle en faisant tendre ε vers 0 .

Théorème 7 (Wiener-Ikehara-Ingham "effectif"). *Avec les hypothèses et les notations du Théorème* 4, *posons*

$$\rho(x) = \inf_{T > 0} \left(\frac{1}{T} + \eta(T, \frac{1}{x}) + (\frac{1}{Tx})^{\omega+1} \right)$$

Alors on a

$$A(x) = \left(\frac{c}{\Gamma(\omega+1)} + O(\rho(x)) \right) e^{ax} x^{\omega} .$$

Démonstration. Supposons sans restreindre la généralité que $A(0) = 0$ et prolongeons $A(u)$ par 0 pour $u < 0$. Dans un premier temps, nous appliquons le Théorème 6 à la fonction

$$g_\sigma(u) := A(u)\ e^{-(a+\sigma)u}\ (1 - e^{-\sigma u}) , \quad (\sigma > 0) ,$$

dont la transformée de Fourier est donnée par

$$\hat{g}_\sigma(\tau) = g(\sigma + i\tau) - g(2\sigma + i\tau) + c((\sigma + i\tau)^{-\omega} - (2\sigma + i\tau)^{-\omega}) .$$

On a d'abord

$$\int_{-T}^{T} |\hat{g}_\sigma(\tau)|\ d\tau \ll \sigma^{-\omega}\ (T + \eta(T,\sigma)) , \quad (0 < \sigma < 1) .$$

De plus, la croissance et la positivité de A impliquent pour $x, y > 0$

$$g_\sigma(x+y) - g_\sigma(x) \geqslant A(x)\ e^{-(a+\sigma)x}\ (1 - e^{-\sigma x})\ (e^{-(a+\sigma)y} - 1)$$

$$\geqslant - (a+\sigma)\ \|g_\sigma\|_\infty\ y .$$

Appliquant le Théorème 6 avec $K = (a+\sigma)\ \|g_\sigma\|_\infty / T$, il vient

$$\|g_\sigma\|_\infty \ll \sigma^{-\omega}(T + \eta(T,\sigma)) + \|g_\sigma\|_\infty\ T^{-1} .$$

En choisissant T grand mais fixé, on en déduit que

$$\|g_\sigma\|_\infty \ll \sigma^{-\omega} .$$

Posons

$$F(u) = \begin{cases} \dfrac{c}{\Gamma(\omega+1)}\ e^{-u}\ (1-e^{-u})\ u^{\omega} & , \quad (u > 0) \\ 0 & , \quad (u \leqslant 0) \ . \end{cases}$$

La seconde étape de la démonstration consiste à appliquer une nouvelle fois le Théorème 6, mais à la fonction

$$G_\sigma(u) := g_\sigma(u) - \sigma^{-\omega}\ F(\sigma u) \ ,$$

dont la transformée de Fourier vaut

$$\hat{G}_\sigma(\tau) = g(\sigma + i\tau) - g(2\sigma + i\tau) \ .$$

Si $\omega \geqslant 0$, on a $F'(u) = O(1)$. Si $-1 < \omega < 0$, on a $F'(u) = O(\min(1,u^{\omega}))$ et $F(u) = O(\min(1,u^{\omega+1}))$. On en déduit dans tous les cas, pour $x \geqslant 0$, $0 \leqslant y \leqslant 1/T \leqslant 1$,

$$F(\sigma x + \sigma y) - F(\sigma x) \leqslant O((\sigma/T) + (\sigma/T)^{\omega+1}) \ .$$

D'où

$$\begin{aligned} G_\sigma(x+y) - G_\sigma(x) &\geqslant -(a+\sigma)\ \|g\|_\infty\ y - \sigma^{-\omega}(F(\sigma x + \sigma y) - F(\sigma x)) \\ &\geqslant -\ O(\sigma^{-\omega}\ T^{-1} + \sigma T^{-\omega-1}) \ . \end{aligned}$$

Par le Théorème 6, il vient finalement

$$|G_\sigma(x)| \ll \sigma^{-\omega}(T^{-1} + \eta(T,\sigma) + (\sigma/T)^{\omega+1})$$

d'où la conclusion, en choisissant $\sigma = 1/x$.

En utilisant seulement les majorations élémentaires

$$\begin{aligned} \zeta(s) &\ll \log(2+|\tau|) \\ \zeta'(s) &\ll (\log(2+|\tau|))^2 \end{aligned} \qquad (\sigma \geqslant 1)$$

et la minoration classique de de la Vallée Poussin

$$\zeta(\sigma)^3\ |\zeta(\sigma+i\tau)|^4\ |\zeta(\sigma+2i\tau)| \geqslant 1 \ , \quad (\sigma \geqslant 1) \ ,$$

le Théorème 6 fournit l'estimation

$$\sum_{n \leqslant x} \mu(n) \ll x \frac{(\log\log x)^8}{\sqrt{\log x}} .$$

Appendice 1.

Nous établissons ici la forme affaiblie du Théorème 3 dans laquelle la dernière majoration A/n est remplacée par $An^{\varepsilon-1}$, avec $A = A(h;\varepsilon)$.

Le réel positif ε étant fixé, définissons q comme le plus petit entier tel que $(2q-1)\varepsilon \geqslant 1$ et posons $r = [n/2q]$. Nous désignons par K_r le noyau de Fejer d'ordre r :

$$K_r(t) = \left(\frac{\sin((r+1)t/2)}{\sin(t/2)}\right)^2 = r+1+2\sum_{j=1}^{r}(r+1-j)\cos jt .$$

Nous introduisons les quantités :

$$\alpha_n = r^{\varepsilon-1} \ll_\varepsilon n^{\varepsilon-1}, \quad \beta_n = \left(\int_\pi K_r(t)^q \, dt\right)^{-1} \ll_\varepsilon n^{1-2q}, \text{ et}$$

$$\gamma_n = \beta_n \int_{|t|>\alpha_n} K_r(t)^q \, dt \ll_\varepsilon n^{-\varepsilon(2q-1)} \leqslant n^{-1} .$$

Après avoir remarqué que, par différence, nous pouvons nous restreindre au cas où h est non décroissante sur $[0,1]$, nous définissons deux fonctions g^+ et g^-, paires et périodiques de période 2π, par

$$g^{\pm}(u) = \begin{cases} h(0), & (0 \leqslant u < \pi/2 \mp \alpha_n) \\ h(-\sqrt{2}\cos(u \pm \alpha_n)), & (\pi/2 \mp \alpha_n < u \leqslant 3\pi/4 \mp \alpha_n) \\ h(1), & (3\pi/4 \mp \alpha_n < u \leqslant \pi) . \end{cases}$$

Nous supposons n suffisamment grand pour que les inégalités précédentes soient cohérentes. Les fonctions g^+ et g^- sont non décroissantes sur $[0,\pi]$. Nous notons V leur variation commune sur cet intervalle et nous posons, pour $x = -\cos u$,

$$Q^{\pm}(x) = \beta_n \int_{-\pi}^{\pi} g^{\pm}(t) \, K_r(t-u)^q \, dt .$$

Ces fonctions sont des combinaisons linéaires à coefficients $O_q(1)$ des polynômes de Tchebychef $T_j(x) = \cos(ju)$, $0 \leqslant j \leqslant n$. En effet, on a

$$K_r(t)^q = \sum_{0 \leqslant j \leqslant 2qr} a_j \cos(jt) \text{ , avec } a_j = 0_q(r^{q+1}) \text{ d'où}$$

$$Q^{\pm}(x) = \sum_{0 \leqslant j \leqslant 2qr} b_j^{\pm} T_j(x)$$

avec $b_j^{\pm} = a_j \beta_n \int_{-\pi}^{\pi} g^{\pm}(t) \cos(jt)\, dt$. De plus, on a pour $\pi/2 \leqslant u \leqslant 3\pi/4$,

$$Q^-(x) = \beta_n \int_{-\pi}^{\pi} g^-(t+u)\, K_r(t)^q\, dt \leqslant \beta_n\, g^-(u+\alpha_n) \int_{-\alpha_n}^{\alpha_n} K_r(t)^q\, dt + \gamma_n\, g^-(\pi)$$

$$= h(\sqrt{2}x) + \gamma_n(g^-(\pi) - g^-(u+\alpha_n)) \leqslant h(\sqrt{2}x) + \gamma_n V$$

et similairement

$$Q^+(x) \geqslant h(\sqrt{2}x) - \gamma_n V \quad .$$

Comme les coefficients des T_j ne dépassent pas 3^n en valeur absolue, on voit que les polynômes

$$P^{\pm}(x) = Q^{\pm}(x/\sqrt{2}) \pm \gamma_n V$$

satisfont aux deux premières conditions du Théorème 3. Enfin, on a

$$\int_0^1 (P^+(x) - P^-(x))\, dx \leqslant \int_0^1 (P^+(x) - P^-(x)) \frac{dx}{\sqrt{1 - x^2/2}}$$

$$= \frac{\pi}{\sqrt{2}} \gamma_n V + \beta_n \int_{\pi/2}^{3\pi/4} \int_{-\pi}^{\pi} (g^+(t+u) - g^-(t+u))\, K_r(t)^q\, dt\, du$$

$$= 0(\gamma_n + \alpha_n) = 0_q(n^{\varepsilon-1}) \quad .$$

Cela achève la démonstration.

Appendice 2.

Nous montrons ici comment le Théorème 6 implique l'inégalité classique de Berry et Esseen.

Soient F et G deux fonctions de répartitions de fonctions caractéristiques respectives f et g . On suppose que G est dérivable et que G' est bornée sur $\mathbf{R}$. Nous allons montrer que l'on a pour tout $T > 0$

$$\|F - G\|_\infty \ll \|G'\|_\infty/T + \int_{-T}^{T} |(f(\tau) - g(\tau))/\tau| \, d\tau \quad .$$

A cette fin, posons $H = F - G$ et introduisons pour chaque $\varepsilon < 0$ une fonction

$$H_\varepsilon(x) = -\int_0^\infty e^{-\varepsilon u} \, dH(x-u) = e^{-\varepsilon x} \int_{-\infty}^{x} e^{\varepsilon u} \, dH(u) \quad .$$

On vérifie aisément que H_ε est intégrable et que sa transformée de Fourier vaut

$$\hat{H}_\varepsilon(\tau) = \frac{f(-\tau) - g(-\tau)}{\varepsilon + i\tau} \quad .$$

De plus, on a par intégration par parties

$$H_\varepsilon(x) = H(x) - \varepsilon \, e^{-\varepsilon x} \int_{-\infty}^{x} e^{\varepsilon u} \, H(u) \, du \quad .$$

Comme $H(u) \to 0$ quand $u \to -\infty$, cela implique que $H_\varepsilon(x) \to H(x)$ quand $\varepsilon \to 0$. En outre, posant $\alpha := \|G'\|_\infty$, on a pour $y > 0$

$$H(x+y) - H(x) \geqslant -\alpha y$$

et

$$\frac{d}{dx}\left\{\varepsilon \, e^{-\varepsilon x} \int_{-\infty}^{x} e^{\varepsilon u} \, H(u) \, du\right\}$$

$$= -\varepsilon^2 \, e^{-\varepsilon x} \int_{-\infty}^{x} e^{\varepsilon u} \, H(u) \, du + \varepsilon H(x) \leqslant 4\varepsilon \quad .$$

On peut donc appliquer le Théorème 6 à $-H_\varepsilon$, avec $K = (\alpha + 4\varepsilon)/T$. Il vient

$$H(x) \ll (\alpha + 4\varepsilon)/T + \int_{-T}^{T} |(f(\tau) - g(\tau))/\tau| \, d\tau \quad ,$$

d'où le résultat annoncé, en faisant tendre ε vers 0.

Bibliographie

[1] Bohr, H., Ein allgemeiner Satz über die Integration eines trigonometrischen Polynoms, *Prace Matem. Fiz.* 43 (1935), 273-288 (= *Collected Mathematical Works* II, C 36)

[2] Delange, H., Généralisation du Théorème de Ikehara, *Ann. Sci. Ec. Norm. Sup.* (3) 71 (1954), 213-242.

[3] Diamond, H.G., Changes of sign of $\pi(x) - li(x)$, *L'enseignement math.* 21 fasc. 1 (1975), 1-14.

[4] Ellison, W.J., Mendes France, M., *Les nombres premiers*, Hermann (1975).

[5] Freud, G., Restglied eines Tauberschen Satzes I, Acta Math. Acad. Sci. Hung. 2 (1951), 299-308 ; II, *ibid.* 3 (1952), 299-307 ; III, ibid. 5 (1955), 275-288.

[6] Freud, G., Über einseitige Approximation durch Polynome I, *Acta Sci. Math. Szeged* 16 (1955), 12-28.

[7] Freud, G., Ganelius, T., Some remarks on one-sided approximation, *Math. Scand.* 5 (1957), 276-284.

[8] Ganelius, T., On one sided approximation by trigonometrical polynomials, *Math. Scand.* 4 (1956), 247-258.

[9] Ganelius, T., *Tauberian Remainder Theorems*, Lecture Notes 232, Springer (1971).

[10] Ikehara, S., An extension of Landau's theorem in the analytic theory of numbers, *J. of Math. and Phys.*, Mass. Inst. of Techn. 10 (1931), 1-12.

[11] Ingham, A.E., On Wiener's method in tauberian theorems, *Proc. London Math. Soc.* (2) 38 (1935), 458-480.

[12] Ingham, A.E., On tauberian theorems, *Proc. London Math. Soc.* (3) 14A (1965), 157-173.

[13] Karamata, J., Neuer Beweis und Verallgemeinerung der Taubeschen Sätze, welche die Laplacesche und Stieltjesche Transformation betreffen, *J. für die Reine und ang. Math* 164 (1931), 27-39.

G. Tenenbaum
UER de Mathématiques
Université de Nancy I
Boîte Postale 239
54506 Vandoeuvre les Nancy Cedex

RESUMES DES AUTRES CONFERENCES

ALLOUCHE J.-P. (E.N.S. Fontenay)

PROPRIETES ARITHMETIQUES D'UN AUTOMATE CELLULAIRE:

Etude des propriétés spatio-temporelles de l'automate cellulaire introduit par Greenberg et Hastings comme modèle de réaction-diffusion en milieu excitable; un tel automate engendre des suites ultimement périodiques d'états du plan: nous prouvons qu'il n'y a (sauf dans un cas) qu'une période possible.

DELANGE H. (Paris-Sud)

UNE REMARQUE SUR LA FONCTION DE DICKMAN:

De Brujn a établi une "formule exacte" pour la fonction de Dickman:

$$\rho(u)=\frac{e^{\gamma}}{2\pi i}\int_{-i\infty}^{+i\infty}\{\exp(-uz+\int_0^z(e^s-1)\frac{ds}{s})\}dz \quad (u>0)\ .$$

Il considère a priori cette expression et montre qu'elle est égale à $\rho(u)$. *On pourrait obtenir cette formule par inversion de la transformée de Laplace de* $\rho(u)$. *Nous montrons qu'un raisonnement très simple permet de déterminer cette transformée de Laplace à partir de la définition de* $\rho(u)$ *comme limite pour* x *tendant vers* $+\infty$ *de* $x^{-u}N_x(u)$, *où* $N_x(u)$ *est le nombre des entiers* $\leqslant x^u$ *dont tous les diviseurs premiers sont* $\leqslant x$.

DUMONT J.-M. (Aix-Marseille II)

DISCREPANCE DES PROGRESSIONS ARITHMETIQUES DANS LA SUITE DE MORSE:

Soit $\mu(n) = +1$ (resp. -1) *si la somme des chiffres du développement binaire de* n *est paire (resp. impaire). Soit* n *entier impair,* N *entier quelconque,* $i \in \{0,1,\ldots,r-1\}$ *et*

$$s_i(N) = \sum_{\substack{n\leq N \\ n\equiv i(r)}} \mu(n)\ .$$

Soit $k(r)$ *le plus petit entier tel que* r *divise* 2^k-1 , $P_r(Z)$ *le polynôme* $\prod_{j=0}^{k(r)-1}(1-Z^{2^j})$ *et* $\beta(r)=\sup\{|P_r(Z)| / Z$ *racine* $r^{ième}$ *de* $1\}$. *Soit enfin:*

$$\alpha(r)=(\log\beta(r))/k(r)\log 2.$$

Alors pour tout i , $s_i(N)$ *est en* $O(N^{\alpha(r)})$ *et pour (au moins) un indice pour une infinité de* N,

$$|s_i(N)| \geqslant C_i N^{\alpha(r)} \ , \ C_i \text{ indépendant de } N\ .$$

En particulier si r *est premier et* $k(r)=r-1$, $\beta(r)=r$, *ce qui généralise le cas* $r=3$, *déjà étudié par d'autres Auteurs.*

FAURE H. (Aix-Marseille I)

LEMME DE BOHL POUR LES SUITES DE VAN DER CORPUT:

Le lemme de Bohl relie les restes relatifs à deux intervalles J , J' *de même longueur pour les suites* $(n\alpha)$:

Pour tout $N \geqslant 1$, *il existe* $N' \geqslant 1$ *tel que* $E(J,N,(n\alpha))=E(J',]N',N+N'],(n\alpha))$.

Nous montrons un théorème analogue pour les suites de Van der Corput généralisées. Le résultat présente les mêmes avantages que pour les suites $(n\alpha)$ *: il permet de déter-*

miner le comportement asymptotique du reste pour un intervalle quelconque en fonction de sa seule longueur; il en résulte évidemment la caractérisation des intervalles à restes bornés déjà connue.

FURSTENBERG H. (Hebrew University)

DYNAMICAL SYSTEMS AND NUMBER THEORY:

I.- Review of uses of Dynamical Systems: Minimal and uniquely ergodic dynamical systems. Applications to equidistribution of $P(n)$, $P(X)$ *a polynomial with irrational coefficient. Notion of disjointness of dynamical systems. Applications to distribution of* $(2^n 3^m \alpha \bmod 1)$ *and semigroups of endomorphisms of torus. Properties of subsets of* $\mathbb{Z}$ *of positive density and recurrence of ergotic systems.*

II.- Some open questions and conjectures regarding the sequences $(p^n\alpha \bmod 1)$, $(q^n\alpha \bmod 1)$ *for* $(p,q)=1$.
Related questions on Hausdorff dimension and ergodic theory.

HEVERTSE J. (Leiden)

ON THE NUMBER OF SOLUTIONS OF THE THUE-MAHLER EQUATION:

We shall deal with the so-called Thue-Mahler equation

$$(1) \quad |F(X,Y)| = p_1^{h_1} p_2^{h_2} \ldots p_t^{h_t}$$

in X, Y, $h_1, h_2, \ldots, h_t \in \mathbb{Z}$, *with* $(X,Y) = 1$, *where* F *is an irreducible binary form of degree* $n \geqslant 3$ *with coefficients in* $\mathbb{Z}$. *By using Siegel's hypergeometric polynomials and Mahler's p-adic approximation technique, it is possible to show that* (1) *has at most*

$$7^{2n^3(t+2)}$$

solutions. This bound has the property that it does not depend on the coefficients of F *or on* $p_1, \ldots, p_t$.

LANGEVIN M. (E.N.S. de Saint-Cloud)

DISTANCE D'UN ENTIER ALGEBRIQUE AU DISQUE UNITE ET PROBLEME DE LEHMER:

On se propose de montrer comment des méthodes élémentaires comme: petit théorème de Fermat, majorations de discriminants et de résultants, inégalité de Hadamard et orthogonalisation de Schmidt permettent d'obtenir des résultats très actuels sur le problème de Lehmer (comme les améliorations des travaux de Dobrowolski (1979) apportées récemment par Cantor et Straus (1982) puis Louboutin (1983)). En raffinant ces calculs, on obtiendra des renseignements sur la distance au disque-unité des entiers algébriques de module > 1 *et de mesure* $\leqslant 2$. *Relativement à ce problème, on comparera aussi les techniques d'approche en caractéristique 0 et en caractéristique p et, d'autre part, on donnera des améliorations des résultats connus dans le cas abélien ainsi qu'une démonstration d'une extrême simplicité d'un résultat de Favard sur la borne inférieure de* $\sup(|z-z'|; P(z)=P(z'))$ *quand* P *décrit l'ensemble des polynômes unitaires à coefficients entiers.*

MAUDUIT C. (Aix-Marseille 2)

SUITES RECONNAISSABLES PAR AUTOMATES FINIS ET EQUIREPARTITION MODULO UN:

On détermine à quelles conditions la suite $(u_n\xi)$ *est équirépartie pour tout* ξ *irrationnel et où* (u_n) *est une suite strictement croissante d'entiers, reconnaissable par un automate fini. On conclue dans le cadre le plus général par une condition qui s'exprime entre autres sur le graphe associé à l'automate en disant qu'il suffit qu'au moins un des sommets qui reconnaît la suite* u *soit précédé dans le graphe par un sommet possédant au moins deux chemins fermés distincts.*

NARKIEWICZ W. (Wrocław)

PROPRIETES BIZARRES DE $\sigma_k(n)$:

Rapport sur les propriétés d'équirépartition de valeurs des fonctions $\sigma_k(n)$ dans les progressions arithmétiques, fondé sur les résultats à Dobrowolski, Rayner et du Rapporteur.

QUEFFELEC M. (Paris-Nord)

ETUDE SPECTRALE DES SUBSTITUTIONS:

On étudie le système dynamique associé à une suite définie par substitution et on détermine, quand la substitution est de longueur constante, le type spectral maximal de ce système.

ROBIN G. (Limoges)

IRREGULARITE DANS LA DISTRIBUTION DES NOMBRES PREMIERS DANS LES PROGRESSIONS ARITHMETIQUES:

Si

$$\pi(x;k,\ell) = \sum_{\substack{p \leqslant x \\ p \equiv \ell\ (h)}} 1 \quad ; \quad \theta(x;k,\ell) = \sum_{\substack{p \leqslant x \\ p \equiv \ell\ (h)}} \log p \ ,$$

on étudie:(i) l'expression $A(x;k,\ell) = \mathrm{li}(\varphi(k)\theta(x;k,\ell)) - \varphi(k)\pi(x;k,\ell)$ *généralisant ainsi une étude de* $\mathrm{li}(\theta(x))-\pi(x)$. *(ii) une généralisation des conjectures de D. SHANKS et R.P. BRENT sous la forme de*

$$\sum_{n \leqslant x} (\varphi(k)\pi(x;k,\ell) - \pi(n))n^{-\alpha}\log^{\beta} n \ .$$

VOLKMANN B. (Stuttgart)

A PROPOS DU THEOREME DE CASSELS-SCHMIDT:

Il est bien connu que, étant donnés deux entiers $r,s \geqslant 2$, *il existe des nombres normaux en base* r *et à la fois non-normaux en base* s *si et seulement si* $r^n \neq s^m$ (n, $m = 1,2,\ldots$). *Ce théorème a été démontré indépendamment par J.W.S. Cassels (1959, version partielle) et par W. Schmidt (1960, version générale). Une nouvelle démonstration a été donnée récemment par C.E.M. Pearce et M.S. Keane (1982).*
Le conférencier a généralisé le théorème de Cassel-Schimdt en exigeant qu'en plus d'être non-normaux en base s, *les nombres possèdent des fréquences asymptotiques données pour les chiffres* $0,1,..,s-1$. *Une deuxième généralisation concerne le cas où les fréquences asymptotiques n'existent pas nécessairement.*
La méthode est basée sur l'approche de Pearce et Keane.

*
* *

N° d'impression 817

1er trimestre 1986