COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
34. TOPICS IN CLASSICAL NUMBER THEORY
BUDAPEST (HUNGARY), 1981.

A GAUSSIAN LAW ON $\mathbf{F}_q[X]$

J.L. NICOLAS

1. INTRODUCTION

Let $\mathbf{F}_q$ be the field with q elements and $\mathbf{F}_q[X]$ the polynomial ring in one variable over $\mathbf{F}_q$. Let E_n be the subset of $\mathbf{F}_q[X]$ of monic polynomials of degree n. Thus we have Card $E_n = q^n$. Let I_n be the number of irreducible polynomials in E_n. The following equality (cf. [1],[2])

$$(1) \qquad \prod_{n \geq 1} \left(\frac{1}{1-z^n}\right)^{I_n} = \frac{1}{1-qz}$$

gives the value:

$$I_n = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}$$

where μ is Möbius's function. From this value, we deduce:

$$(2) \qquad \frac{q^n}{n} - \frac{2}{n} q^{n/2} \le I_n \le \frac{q^n}{n} .$$

Every $A \in E_n$ has the standard factorization into irreducible polynomials

$$A = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k}$$

and we set: degree of $P_i = n_i$. The function $r : \mathbf{F}_q[X] \to \mathbf{N}$ is defined by:

$$r(A) = \text{l.c.m.}(n_1, n_2, \dots, n_k)$$

$r(A)$ is the degree of the splitting field of A over $\mathbf{F}_q$. This function r occurs in the study of algorithms of factorization over $\mathbf{F}_q[X]$.

In [8], we have proved with M. MIGNOTTE that the normal value of $\log r(A)$ in E_n is $1/2 \log^2 n$. The aim of this paper is to prove the following theorem:

THEOREM. *With the equiprobability measure on* E_n, *the formula*

$$\text{Prob}\left\{\frac{\log r(A) - 1/2 \log^2 n}{(\log^{3/2} n)/\sqrt{3}} < x\right\} =$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-v^2/2}\, dv + O\left(\frac{(\log \log n)^4}{\sqrt{\log n}}\right)$$

holds uniformly in $x \in \mathbf{R}$.

The proof of this theorem needs first the following result of [8]:

PROPOSITION 1. *There exists a subset* E'_n *of* E_n *with* card $E'_n = O(q^n/\log n)$ *and such that for* $A \in E_n \setminus E'_n$ *the inequality*

$$\exp(-2 \log n (\log \log n)^4) n_1 n_2 \dots n_k \le$$

$$\le r(A) \le n_1 n_2 \dots n_k$$

holds.

And secondly, the proof involves the study of the function

$$f(A) = \sum_{P|A} (\log d^{\circ}P) = \sum_{i=1}^{k} \log n_i$$

where P denotes any irreducible polynomial of $\mathbf{F}_q[X]$. This function f is additive, and the similarity with additive functions over natural integers is well known. The distribution of the values of additive arithmetic functions (the famous Erdős-Kac theorem) has been studied extensively, and recently surveyed in ELLIOTT's book ([5]). It is certainly possible to adapt these methods, in particular Delange's method ([4]). We shall prove

PROPOSITION 2. *The following equality*

$$\mathrm{Prob}\left\{\frac{f(A)-1/2\,\log^2 n}{(\log^{3/2} n)/\sqrt{3}} < x\right\} =$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-v^2/2}\, dv + o\left(\frac{1}{\sqrt{\log n}}\right)$$

holds uniformly in $x \in \mathbf{R}$.

Our proof of Proposition 2 follows P. Erdős and P. Turán's proof (cf.[6]). It allows us to get an explicit remainder term and underlines the similarity

between $r(A)$ and the order of a permutation which is the l.c.m. of the lengths of its cycles. The calculation will be carried out in more detail than in [6], in order to get an error term which seems best possible (cf. for instance, [5], ch.20). The same error term can certainly be obtained in the work of P. Erdős and P. Turán ([6], p.309, footnote ***).

In Proposition 1, and in the theorem, P. Erdős and I entertain hopes to prove that the correct order of the error term is $o(\log\log n/\sqrt{\log n})$.

2. A FEW LEMMAS

The following notation for power series:

$$\sum_{n=0}^{\infty} a_n z^n \ll \sum_{n=0}^{\infty} b_n z^n$$

will mean: for every $n \geq 0$, $|a_n| \leq b_n$.

LEMMA 1. *We have:*

$$\sum_{m=2}^{\infty} \frac{\log m}{m} z^m - \frac{1}{2} \log^2 \frac{1}{1-z} \ll \log \frac{1}{1-z} = \sum_{m=1}^{\infty} \frac{z^m}{m}.$$

The proof follows easily from:

$$\text{coeff. of } z^m \text{ in } \log^2 \frac{1}{1-z} =$$

$$= \sum_{j=1}^{m-1} \frac{1}{j(m-j)} = \frac{2}{m} \sum_{j=1}^{m-1} \frac{1}{j}$$

and

$$\log m \le \sum_{j=1}^{m-1} \frac{1}{j} \le 1 + \log m. \tag{3}$$

LEMMA 2. *We have*

$$\sum_{m=2}^{\infty} \frac{\log^2 m}{m} z^m - \frac{1}{3} \log^3 \frac{1}{1-z} \ll 2 \sum_{m=2}^{\infty} \frac{\log m}{m} z^m.$$

With the definition of Stirling's numbers of first kind $s(m,k)$, (cf. [3], ch.5), we have:

$$(\log(1+z))^k = k! \sum_{m\ge k} \frac{s(m,k)}{m!} z^m$$

In particular:

$$\log^3 \frac{1}{1-z} = 6 \sum_{m\ge 3} \frac{|s(m,3)|}{m!} z^m$$

and it is known that

$$|s(m,3)| = \frac{(m-1)!}{2} \{(\sum_{j=1}^{m-1} \frac{1}{j})^2 - (\sum_{j=1}^{m-1} \frac{1}{j^2})\}$$

and the lemma follows, using (3) and $1 \le \sum_{1\le j\le m-1} j^{-2} \le$ $\le \pi^2/6 < 2$.

LEMMA 3. *Let a be real positive and $(a_k)_{k\ge 1}$ be a sequence of coefficients satisfying $|a_k| \le a/k$ for $1\le k\le n$. We set:*

$$\exp(\sum_{k\ge 1} a_k z^k) = 1 + \sum_{k\ge 1} b_k z^k.$$

Then, for $1\le k\le n$, we have:

$$|b_k| \le a e^a k^{a-1}.$$

PROOF. Suppose first that the upper bound $|a_k| \le$ $\le a/k$ holds for all $k\ge 1$. With our notation $\ll$, we get:

$$\sum_{k\ge 1} a_k z^k \ll a \log \frac{1}{1-z}$$

and

$$\exp(\sum_{k\ge 1} a_k z^k) \ll (1-z)^{-a}.$$

If we define γ_k by $(1-z)^{-a} = 1 + \sum_{k\geq 1} \gamma_k z^k$, we have:

$$|b_k| \leq \gamma_k = \frac{a}{k}(1+\frac{a}{1})(1+\frac{a}{2})\dots(1+\frac{a}{k-1})$$

and

$$\log \gamma_k \leq \log \frac{a}{k} + a(1+\frac{1}{2}+\dots+\frac{1}{k-1}) \leq$$

$$\leq \log \frac{a}{k} + a(1+\log k).$$

If the upper bound holds only for $1\leq k\leq n$, we just have to observe that the coefficients b_k, for $k\leq n$, depend only on the coefficients a_k for $k\leq n$.

LEMMA 4. *For $n\geq 3$ and $t\in\mathbf{R}$, such that $|t| \leq \sqrt{\log n}$ we set*

$$h(z) = \frac{1}{1-z} \exp\{\frac{it}{2\log^{3/2} n} \log^2 \frac{1}{1-z} -$$

$$- \frac{t^2}{6\log^3 n} \log^3 \frac{1}{1-z}\} = \sum_{m=0}^{\infty} e_m z^m.$$

Then, we have: $e_0=e_1=1$,

$$e_n = \exp\{\frac{it\sqrt{\log n}}{2} - \frac{t^2}{6}\} + O[e^{-t^2/6} \frac{|t|}{\sqrt{\log n}}] +$$

$$+ O(\frac{1}{n})$$

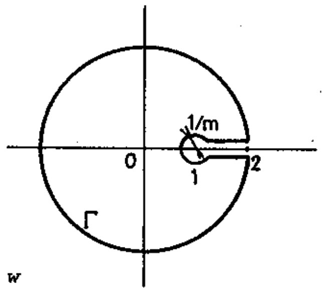
and for $m\leq n$,

$$|e_m| = O[\exp\{-\frac{t^2}{6} \frac{\log^3 m}{\log^3 n}\}] + O(2^{-m})$$

where the "O" mean explicit constants.

PROOF. If $2\leq m\leq n$, we have:

$$e_m = \frac{1}{2i\pi} \int_\Gamma \frac{h(z)dz}{z^{m+1}}.$$



We choose

$$\log w = \log|w| + i \operatorname{Arg} w$$

with $-\pi<\operatorname{Arg} w<\pi$, so that $\log 1/(1-z)$ is holomorphic in $\mathbf{C}\setminus[1,+\infty[$.

On the circle of radius 2, we have:

$$\log|\frac{1}{1-z}| \leq \sqrt{\pi^2 + \log^2 3} \leq 4$$

and, under the hypotheses of our lemma:

$$|h(z)| \le \exp\left(\frac{8}{\log n} + \frac{32}{3\log^2 n}\right).$$

Thus the contribution of the bigger circle is $o(2^{-m})$.

On the upper slit, $h(z)$ is

$$\frac{1}{1-r}\exp\left\{\frac{it}{2}\frac{(\log\frac{1}{r-1}+i\pi)^2}{\log^{3/2} n} - \right.$$

$$\left. - \frac{t^2}{6\log^3 n}(\log\frac{1}{r-1}+i\pi)^3\right\}$$

and, on the lower one:

$$\frac{1}{1-r}\exp\left\{\frac{it}{2}\frac{(\log\frac{1}{r-1}-i\pi)^2}{\log^{3/2} n} - \right.$$

$$\left. - \frac{t^2}{6\log^3 n}(\log\frac{1}{r-1}-i\pi)^3\right\}.$$

The difference of these two quantities is $1/(1-r)$ $(\exp(A+B)-\exp(A-B))$ with

$$A = \frac{it}{2}\frac{\log^2\frac{1}{r-1}}{\log^{3/2} n} - \frac{t^2}{6\log^3 n}\log^3\frac{1}{r-1} -$$

$$- \frac{\pi^2 it}{2\log^{3/2} n} + \frac{\pi^2 t^2}{2\log^3 n}\log\frac{1}{r-1}$$

$$B = -\frac{\pi t\log\frac{1}{r-1}}{\log^{3/2} n} - \frac{it^2\pi\log^2\frac{1}{r-1}}{2\log^3 n} + \frac{i\pi^3 t^2}{6\log^3 n}.$$

We have for $1+1/m \le r \le 2$, $0 \le \log 1/(r-1) \le \log m \le \log n$, and for $n \ge 3$, $\log n \ge 1$; so we get:

$$\operatorname{Re} A \le -\frac{t^2}{6\log^3 n}\log^3\frac{1}{r-1} + \frac{\pi^2}{2}$$

and

$$|B| \le \frac{|t|}{\sqrt{\log n}}\left(\pi + \frac{\pi}{2} + \frac{\pi^3}{6}\right) \le \frac{10|t|}{\sqrt{\log n}}.$$

Hence $|B| \le 10$ and $e^B - e^{-B} = O(B)$; and thus the contribution of the segment integrals is

$$\int_{1+1/m}^{2} \frac{1}{1-r}\frac{(\exp A)(\exp B - \exp(-B))dr}{r^{m+1}} =$$

$$= O\left[\frac{|t|}{\sqrt{\log n}} J_2\right]$$

with

$$J_2 = \int_{1+1/m}^{2} \frac{\exp(-\frac{t^2}{6\log^3 n}\log^3\frac{1}{r-1})}{(r-1)r^{m+1}}\,dr.$$

Now:

$$J_2 = \sum_{j=1}^{m-1}\int_{1+j/m}^{1+(j+1)/m} \frac{\exp(-\frac{t^2}{6\log^3 n}\log^3\frac{1}{r-1})}{(r-1)r^{m+1}}\,dr \le$$

$$\le \sum_{j=1}^{m-1} \frac{\exp(-\frac{t^2}{6\log^3 n}\log^3\frac{m}{j+1})}{j(1+j/m)^{m+1}}.$$

To get an upper bound for the numerator, we first observe:

$$\log^3\frac{m}{j+1} \ge \log^3 m - 4\log^2 m\,\log(j+1)$$

and then:

$$-\frac{t^2}{6\log^3 n}\log^3\frac{m}{j+1} \le$$

$$\le -\frac{t^2}{6}\frac{\log^3 m}{\log^3 n} + \frac{4t^2}{6\log^3 n}\log^2 m\,\log(j+1) \le$$

$$\le -\frac{t^2}{6}\frac{\log^3 m}{\log^3 n} + \log(j+1).$$

A lower bound for the denomiantor is obtained using $\log(1+x) \ge x\log 2$ (valid for $0\le x\le 1$), and we get:

$$J_2 \le \exp(-\frac{t^2}{6}\frac{\log^3 m}{\log^3 n})\sum_{j=1}^{m-1}\frac{j+1}{2^j j} \le$$

$$\le 2\exp(-\frac{t^2}{6}\frac{\log^3 m}{\log^3 n})$$

and the contribution of the segment integrals is:

$$O[\frac{|t|}{\sqrt{\log n}}\exp(-\frac{t^2}{6}\frac{\log^3 m}{\log^3 n})].$$

Finally, the integral on the circle $|z-1|=1/m$ is:

$$J_3 = \int_0^{2\pi}\exp\{\frac{it}{2\log^{3/2} n}(\log m+i(\pi-\varphi))^2 -$$

$$-\frac{t^2}{6\log^3 n}(\log m+i(\pi-\varphi))^3\}\times(1+\frac{e^{i\varphi}}{m})^{-(m+1)}d\varphi =$$

$$= \frac{1}{2\pi}\exp\{\frac{it\log^2 m}{2\log^{3/2} n} - \frac{t^3\log^3 m}{6\log^3 n}\}\times$$

$$\times\int_0^{2\pi}\exp(\xi(t,\varphi)-\eta(\varphi))\,d\varphi$$

with:

$$\xi(t,\varphi) = -\frac{t \log m(\pi-\varphi)}{\log^{3/2} n} - \frac{it(\pi-\varphi)^2}{2\log^{3/2} n} -$$

$$-\frac{3\, it^2 \log^2 m(\pi-\varphi)}{6\log^3 n} + \frac{3t^2}{6\log^3 n}\log m(\pi-\varphi)^2 +$$

$$+\frac{it^2}{6\log^3 n}(\pi-\varphi)^3$$

and: $\eta(\varphi) = (m+1)\log(1+e^{i\varphi}/m)$.

We have:

$$|\xi(t,\varphi)| \leq$$

$$\leq \left(\pi + \frac{\pi^2}{2\log n} + \frac{\pi}{2} + \frac{\pi^2}{2\log n} + \frac{\pi^3}{6\log^2 n}\right)\frac{|t|}{\sqrt{\log n}}$$

and therefore

$$\exp(\xi(t,\varphi)) = 1 + \xi_1(t,\varphi)$$

with $\xi_1(t,\varphi) = O[|t|/\sqrt{\log n}]$.

In the same way,

$$\eta(\varphi) = e^{i\varphi} + \eta_1(\varphi)$$

with $\eta_1(\varphi) = O(1/m)$. Hence:

$$\exp(-\eta(\varphi)) = \exp(-e^{i\varphi}) + \eta_2(\varphi)$$

with $\eta_2(\varphi) = O(1/m)$. Then we have:

$$\int_0^{2\pi} \exp(\xi(t,\varphi)-\eta(\varphi))\,d\varphi =$$

$$= \int_0^{2\pi} (1+\xi_1(t,\varphi))\,(\exp(-e^{i\varphi}) + \eta_2(\varphi))\,d\varphi =$$

$$= 2\pi + O\left[\frac{|t|}{\sqrt{\log n}}\right] + O\left(\frac{1}{m}\right)$$

noticing that:

$$\int_0^{2\pi} \exp(-e^{i\varphi})\,d\varphi = \int_{|z|=1} \frac{e^{-z}}{iz}\,dz = 2\pi.$$

Finally, we have:

$$J_3 = \exp\left\{\frac{it\log^2 m}{2\log^{3/2} n} - \frac{t^2}{6}\frac{\log^3 m}{\log^3 n}\right\} +$$

$$+ \left[\exp\left\{-\frac{t^2}{6}\frac{\log^3 m}{\log^3 n}\right\}\right] O\left[\frac{|t|}{\sqrt{\log n}} + \frac{1}{m}\right]$$

and the proof of Lemma 4 is finished.

LEMMA 5. *The mean value of* $f(A)$ *is:*

$$M_n = \frac{1}{q^n} \sum_{A \in E_n} f(A) = \frac{1}{2} \log^2 n + o(1).$$

PROOF.

$$M_n = \frac{1}{q^n} \sum_{A \in E_n} \sum_{P|A} \log d^{\circ}P$$

$$M_n = \frac{1}{q^n} \sum_{\substack{P \text{ irred} \\ d^{\circ}P \le n}} (\log d^{\circ}P) q^{n-d^{\circ}P} =$$

$$= \sum_{i=1}^{n} \frac{I_i \log i}{q^i} .$$

If we set $I_i = q^i/i + R_i$, (2) gives: $|R_i| \le 2/i \; q^{i/2}$; and:

$$M_n = \sum_{i=1}^{n} \frac{\log i}{i} + \sum_{i=1}^{n} \frac{R_i \log i}{q^i} =$$

$$= \sum_{i=1}^{n} \frac{\log i}{i} + o(1)$$

and we have:

$$\sum_{i=1}^{n} \frac{\log i}{i} = \int_1^n \frac{\log x}{x} dx + o(1) =$$

$$= \frac{1}{2} \log^2 n + o(1).$$

3. PROOF OF PROPOSITION 2 AND OF THE THEOREM

M_n being given by Lemma 5, we set:

$$F_n(x) = \text{Prob}\{\frac{f(A)-M_n}{\log^{3/2} n} < x\}$$

and the characteristic function is defined by the Stieltjes integral:

$$\varphi_n(t) = \int_{-\infty}^{+\infty} e^{itx} \, dF_n(x).$$

We have:

$$\varphi_n(t) = \frac{1}{q^n} \sum_{A \in E_n} \exp\{it[\frac{f(A)-M_n}{\log^{3/2} n}]\}$$

(4) $$\varphi_n(t) = \frac{1}{q^n} \exp[\frac{-itM_n}{\log^{3/2} n}] \sum_{A \in E_n} \exp[\frac{itf(A)}{\log^{3/2} n}].$$

We shall prove that, for any fixed t,

$$\lim_{n\to\infty} \varphi_n(t) = e^{-t^2/6}.$$

Then, a classical theorem of probability, (cf. for instance [5], Vol.1, Lemma 1.11, p.28, or [7], Vol.2, ch. XV, p.508-509) gives, observing that:

$$\frac{1}{2\pi}\int_{-\infty}^{+\infty} e^{-itx}\, e^{-t^2/6}\, dt = \sqrt{\frac{3}{2\pi}}\, e^{-3/2x^2}$$

(5) $$\lim_{n\to\infty} F_n(x) = F(x) = \sqrt{\frac{3}{2\pi}} \int_{-\infty}^{x} e^{-3/2u^2}\, du.$$

For an estimation of the error term, we shall suppose $|t|\le\sqrt{\log n}$. All the upper bounds, and "O" of this paragraph are valid for $|t|\le\sqrt{\log n}$ and $n\ge n_0$, where n_0 is an absolute constant. The idea of the proof is first to write $\varphi_n(t)$ as the coefficient of z^n in some power series, then using Lemmas 1 to 4 to transform this power series in order to get a good estimation of $\varphi_n(t)$. The sixth step uses the above mentioned theorem of probability to estimate $F_n(x)$. The seventh step uses Lemma 5 to prove Proposition 2. The eighth step deduces the Theorem from Propositions 1 and 2.

1^{st} *step. Calculation of* $\varphi_n(t)$.

Setting $\tau=t/(\log n)^{3/2}$, we have:

$$\sum_{A\in E_n} e^{i\tau f(A)} = \sum_{A\in E_n} \prod_{P|A} (d^oP)^{i\tau}.$$

This quantity is the coefficient of w^n in the power series expansion of:

$$\prod_{P} \{1+(\deg P)^{i\tau}(w^{\deg P} + w^{2\deg P} +\dots)\} =$$

$$= \prod_{k\ge1} \left[1+k^{i\tau}\frac{w^k}{1-w^k}\right]^{I_k} =$$

$$= \prod_{k\ge1} \left[\frac{1}{1-w^k}\right]^{I_k} (1+(k^{i\tau}-1)w^k)^{I_k} =$$

$$= \frac{1}{1-qw} \prod_{k\ge1} (1+(k^{i\tau}-1)w^k)^{I_k}$$

using formula (1). Observing that the coefficient of w^n depends only on the k's $\le n$, and setting $qw=z$, (4) becomes

(6) $$\varphi_n(t) = \exp\left[\frac{-itM_n}{\log^{3/2} n}\right] \text{Coeff. of } z^n \text{ in}$$

$$\frac{1}{1-z} \prod_{k=2}^{n} \left[1+(k^{i\tau}-1)\frac{z^k}{q^k}\right]^{I_k}.$$

2^{nd} *step.*

We set:

$$D_n(z) = \sum_{k=2}^{n} I_k \log(1+u_k)$$

with

$$u_k = (e^{i\tau \log k}-1) \frac{z^k}{q^k} .$$

We write

$$D_n(z) = h_1(z) + h_2(z) + h_3(z) + h_4(z)$$

with

$$h_1(z) = \sum_{k=2}^{n} (i\tau \log k - \frac{\tau^2}{2} \log^2 k) \frac{z^k}{k}$$

$$h_3(z) =$$

$$= \sum_{k=2}^{n} I_k(e^{i\tau \log k}-1-i\tau \log k + \frac{\tau^2}{2} \log^2 k) \frac{z^k}{q^k}$$

$$h_4(z) = \sum_{k=2}^{n} I_k(\log(1+u_k)-u_k).$$

(We remark that $h_1+h_2+h_3=\sum_{k=2}^{n} I_k u_k$).

Using (2) and our notation $\ll$, we get:

$$h_2(z) \ll \sum_{k=2}^{n} \frac{2}{kq^{k/2}} (|\tau|\log k + \frac{\tau^2}{2} \log^2 k)z^k$$

and as $|t|\le\sqrt{\log n}$, and $\log k \le \log n$, we have:

$$h_2(z) \ll \sum_{k=2}^{n} \frac{3|t|}{kq^{k/2}\sqrt{\log n}} z^k.$$

Using the formula, valid for any real x, (cf [7],p.512)

(7) $$|e^{ix}-1-ix-\ldots-\frac{(ix)^{m-1}}{(m-1)!}| \le \frac{|x|^m}{m!} ,$$

we get:

$$h_3(z) \ll \sum_{k=2}^{n} \frac{|t|^3}{6k \log^{9/2} n} \log^3 k \; z^k \ll$$

$$\ll \sum_{k=2}^{n} \frac{|t^3|}{6k \log^{3/2} n} z^k .$$

Finally

$$h_4(z) \ll \sum_{k=2}^{n} I_k \sum_{j=2}^{\infty} \frac{|u_k|^j}{j} \ll$$

$$\ll \sum_{k=2}^{n} \frac{q^k}{k} \sum_{j=2}^{\infty} \frac{(|\tau|\log k)^j z^{kj}}{j q^{kj}}$$

by (2) and (7). Therefore we have:

$$h_4(z) \ll \sum_{l=4}^{\infty} b_l z^l$$

with

$$b_l = \sum_{\substack{j\geq 2,\, kj=l \\ 2\leq k\leq n}} \frac{1}{l q^l} q^k (|\tau|\log k)^j .$$

Observing that:

$$|\tau|\log k \leq \frac{|t|}{\sqrt{\log n}} \leq 1,$$

we have $(|\tau|\log k)^j \leq |t|/\sqrt{\log n}$ for $j\geq 1$, and we have:

$$b_l \leq \frac{1}{l q^l} \frac{|t|}{\sqrt{\log n}} \sum_{2\leq k\leq l/2} q^k \leq \frac{2|t|}{l q^{l/2}\sqrt{\log n}} .$$

So, if we set:

$$h_2(z) + h_3(z) + h_4(z) = \sum_{k=2}^{\infty} a_k^{(1)} z^k$$

we have proved

$$D_n(z) = h_1(z) + \sum_{k=2}^{\infty} a_k^{(1)} z^k$$

with

(8) $$|a_k^{(1)}| \leq \frac{5|t|}{\sqrt{\log n}\; k q^{k/2}} + \frac{|t^3|}{6k \log^{3/2} n} .$$

3^{rd} *step.*

(6) can now be written:

$$\varphi_n(t) = \exp\left[\frac{-itM_n}{\log^{3/2} n}\right] \text{ Coeff of } z^n \text{ in}$$

$$\left(\frac{1}{1-z}\right)\exp D_n(z)$$

and noticing that exponents of z larger than n do not occur, we get:

$$\varphi_n(t) = \exp[\frac{-itM_n}{\log^{3/2} n}] \text{ Coeff of } z^n \text{ in:}$$

$$\frac{1}{1-z} \exp\{i\tau \sum_{k=2}^{\infty} \frac{\log k}{k} z^k - \frac{\tau^2}{2} \sum_{k=2}^{\infty} \frac{\log^2 k}{k} z^k\} \times$$

$$\times \exp\{\sum_{k=2}^{\infty} a_k^{(1)} z^k\}.$$

By Lemmas 1 and 2, and with the function h as defined in Lemma 4, we get

(9) $$\varphi_n(t) = \exp[\frac{-itM_n}{\log^{3/2} n}] \text{ Coeff of } z^n \text{ in}$$

$$h(z)\exp\{\sum_{k=2}^{\infty} a_k^{(2)} z^k\}$$

with

$$|a_k^{(2)}| \le |a_k^{(1)}| + \frac{|\tau|}{k} + \frac{\tau^2 \log k}{k}, \quad 2 \le k \le n$$

and (8) gives:

$$|a_k^{(2)}| \le \frac{5|t|}{\sqrt{\log n}\; kq^{k/2}} + \frac{12|t|+|t^3|}{6k \log^{3/2} n}, \quad 2 \le k \le n.$$

4^{th} *step.*

We set:

$$\exp[\sum_{k=2}^{\infty} \frac{5|t| z^k}{\sqrt{\log n}\; kq^{k/2}}] = 1 + \sum_{k=2}^{\infty} b_k^{(1)} z^k$$

$$\exp[\sum_{k=2}^{\infty} \frac{12|t|+|t^3|}{6k \log^{3/2} n} z^k] = 1 + \sum_{k=2}^{\infty} b_k^{(2)} z^k$$

$$[1 + \sum_{k=2}^{\infty} b_k^{(1)} z^k][1 + \sum_{k=2}^{\infty} b_k^{(2)} z^k] =$$

$$= 1 + \sum_{k=2}^{\infty} b_k z^k$$

(10) $$\exp(\sum_{k=2}^{\infty} a_k^{(2)} z^k) = 1 + \sum_{k=2}^{\infty} a_k^{(3)} z^k.$$

Then we shall have, for $2 \le k \le n$

$$|a_k^{(3)}| \le b_k.$$

It remains to estimate b_k. We set

$$a = a(t,n) = \frac{12|t|+|t^3|}{6(\log n)^{3/2}}$$

and we remark that for $|t|\le\sqrt{\log n}$ and for n big enough $(n>e^{12})$, we have:

$$0 < a \le \frac{1}{3}.$$

Then Lemma 3 gives, for $n>e^{12}$ and $k\le n$

$$|b_k^{(2)}| \le e^{1/3} \frac{a}{k^{1-a}}.$$

Changing z to $z/\sqrt{q}$, the same lemma gives:

$$|b_k^{(1)}| \le 5 \frac{|t|}{\sqrt{\log n}} \frac{e^5}{k} \frac{k^{5|t|/\sqrt{\log n}}}{q^{k/2}}$$

and for $|t|\le\sqrt{\log n}$,

$$|b_k^{(1)}| \le 5e^5 \frac{|t|}{\sqrt{\log n}} \frac{k^4}{q^{k/2}}, \quad k\le n.$$

Then we have:

$$|b_k| \le |b_k^{(1)}| + |b_k^{(2)}| +$$

$$+ \sum_{j=2}^{k-2} 5e^5 \frac{|t|}{\sqrt{\log n}} e^{1/3} a \frac{j^4}{q^{j/2}} \frac{1}{(k-j)^{1-a}}$$

and

$$\sum_{j=2}^{k-2} \frac{j^4}{q^{j/2}} \frac{1}{(k-j)^{1-a}} \le$$

$$\le \sum_{2\le j\le k/2} \left(\frac{2}{k}\right)^{1-a} \frac{j^4}{q^{j/2}} + k^4 \sum_{j>k/2} \frac{1}{q^{j/2}} =$$

$$= O[\frac{1}{k^{1-a}} + \frac{k^4}{q^{k/4}}].$$

Hence:

$$|a_k^{(3)}| \le |b_k| = O[\frac{|t|}{\sqrt{\log n}} \frac{k^4}{q^{k/4}} + \frac{a}{k^{1-a}}].$$

Then, we observe that, for $k\le n$ and $|t|<\sqrt{\log n}$, we have

(11) $$a_k^{(3)} = o[\frac{1}{k^{2/3}}]$$

and

$$\sum_{k=2}^{n} |a_k^{(3)}| = o[\frac{|t|}{\sqrt{\log n}} + a \sum_{k=2}^{n} \frac{1}{k^{1-a}}].$$

As

$$\sum_{k=2}^{n} \frac{1}{k^{1-a}} \leq \int_{1}^{n} \frac{dx}{x^{1-a}} = \frac{n^a - 1}{a}.$$

we have

(12) $$\sum_{k=2}^{n} |a_k^{(3)}| = o[\frac{|t|}{\sqrt{\log n}}] +$$

$$+ o[\exp[\frac{12|t|+|t|^3}{6\sqrt{\log n}}]-1].$$

5^{th} *step.*

We now calculate the coefficient of z^n in $h(z)[1 + \sum_{k\geq 2} a_k^{(3)} z^k]$. With notations of Lemma 4, this coefficient is:

$$e_n + \sum_{k=2}^{n-1} a_k^{(3)} e_{n-k} + a_n^{(3)}.$$

Then (9) and (10) give:

$$\varphi_n(t) = [\exp[\frac{-itM_n}{\log^{3/2} n}]] \times$$

$$\times [e_n + \sum_{k=2}^{n-1} a_k^{(3)} e_{n-k} + a_n^{(3)}].$$

By Lemma 4 and (11), we have

(13) $$\varphi_n(t) = e_n \exp[\frac{-itM_n}{\log^{3/2} n}] + o(s_1+s_2) + o(n^{-2/3})$$

with

$$s_1 = \sum_{k=2}^{n-1} |a_k^{(3)}| \exp\{- \frac{2}{6} \frac{\log(n-k)}{\log^3 n}\}$$

and:

$$s_2 = \sum_{k=2}^{n-1} |a_k^{(3)}| 2^{-n+k}.$$

We get, by (11)

$$s_2 = o[\sum_{k=2}^{n-1} \frac{1}{k^{2/3}} 2^{-n+k}] =$$

$$= O[2^{-n/2} \sum_{1\le k\le n/2} 1 + (\frac{2}{n})^{2/3} \sum_{n/2\le k\le n-1} 2^{-n+k}]$$

$$s_2 = O(n^{-2/3})$$

Then we have:

$$s_1 \le \sum_{k=2}^{n-\sqrt{n}} |a_k^{(3)}| \exp\{-\frac{t^2}{48}\} + \sum_{n-\sqrt{n}\le k\le n-1} |a_k^{(3)}|$$

and by (11) and (12),

$$s_1 = [\exp(-\frac{t^2}{48})]\ O[\frac{|t|}{\sqrt{\log n}} + \exp[\frac{12|t|+|t|^3}{6\sqrt{\log n}}]-1] +$$

$$+ O(n^{-1/6}).$$

Lemma 5 gives:

$$\exp[\frac{-itM_n}{\log^{3/2} n}] = [\exp(\frac{-it\sqrt{\log n}}{2})][1 + \frac{O(|t|)}{\log^{3/2} n}]$$

and (13) becomes, with the estimation of e_n given by Lemma 4

(14) $$\varphi_n(t) = \exp(-t^2/6) + (\exp(-t^2/48)) \times$$

$$\times\ O[\frac{|t|}{\sqrt{\log n}} + \exp[\frac{12|t|+|t^3|}{6\sqrt{\log n}}]-1] + O(n^{-1/6}).$$

6^{th} *step.*

With the notation of (5) the following formula (cf. [7], p.538):

(15) $$|F_n(x)-F(x)| \le \frac{1}{\pi}\int_{-T}^{+T} |\frac{\varphi_n(t)-e^{-t^2/6}}{t}|\ dt +$$

$$+ \frac{24F'(0)}{\pi T}$$

holds for any real x and $T>0$. We shall choose $T=\alpha\sqrt{\log n}$ with a fixed $\alpha>1$, to be specified.

Formula (7) gives:

$$|\varphi_n(t)-1| \le t\mu_n$$

with

$$\mu_n = \int_{-\infty}^{+\infty} |x|\ dF_n(x) = \frac{1}{q^n} \sum_{A\in E_n} |\frac{f(A)-M_n}{\log^{3/2} n}|$$

and, by Lemma 5, $\mu_n=O(\sqrt{\log n})$. Hence we deduce, with $\varepsilon_n=1/\log n$:

$$\int_{-\varepsilon_n}^{\varepsilon_n} \left|\frac{\varphi_n(t)-e^{-t^2/6}}{t}\right| dt \le$$

$$\le \int_{-\varepsilon_n}^{\varepsilon_n} \left(\mu_n + \frac{1-e^{-t^2/6}}{t}\right) dt = O\left[\frac{1}{\sqrt{\log n}}\right].$$

Formula (14) is then used to estimate the following integral:

$$\int_{\varepsilon_n \le |t| \le T} (\varphi_n(t)-\exp(-t^2/6))\ dt/|t|.$$

We have:

$$\int_{\varepsilon_n \le |t| \le T} O\left[\frac{1}{\sqrt{\log n}}\right] \exp\left(-\frac{t^2}{48}\right) dt = O\left[\frac{1}{\sqrt{\log n}}\right]$$

$$\int_{\varepsilon_n \le |t| \le T} \frac{dt}{|t| n^{1/6}} = \frac{2}{n^{1/6}}(\log T - \log \varepsilon_n) =$$

$$= O\left[\frac{1}{\sqrt{\log n}}\right])$$

finally, for $|t|<(\log n)^{1/6}$, we have:

$$\exp\left[\frac{12|t|+|t^3|}{6\sqrt{\log n}}\right] - 1 = O\left[\frac{12|t|+|t^3|}{6\sqrt{\log n}}\right]$$

and for $(\log n)^{1/6} \le t \le \alpha\sqrt{\log n}$,

$$\exp\left[\frac{12|t|+|t|^3}{6\sqrt{\log n}}\right] - 1 \le \exp\left(2\alpha + \frac{\alpha}{6}\, t^2\right)$$

and this implies:

$$\int_{\varepsilon_n \le |t| \le T} \left\{\exp\left[\frac{12|t|+|t|^3}{6\sqrt{\log n}}\right]-1\right\} \exp\left(-\frac{t^2}{48}\right) \frac{dt}{|t|} =$$

$$= O\left[\frac{1}{\sqrt{\log n}}\right] \int_{|t| \le \log^{1/6} n} \frac{12+t^2}{6} \exp\left(-\frac{t^2}{48}\right) dt +$$

$$+ O\left(\int_{\log^{1/6} n \le |t| \le T} \exp\left[\left(\frac{\alpha}{6} - \frac{1}{48}\right)t^2\right]\frac{dt}{|t|}\right) =$$

$$= O\left[\frac{1}{\sqrt{\log n}}\right],$$

if we choose $\alpha<1/8$. Then (15) becomes:

(16) $$F_n(x) - F(x) = O(1/\sqrt{\log n})$$

uniformly in x.

7^{th} *step.*

The proof of Proposition 2 follows easily from (16) and Lemma 5: If we set:

$$G_n(x) = \text{Prob}\{\frac{f(A)-1/2\ \log^2 n}{(\log^{3/2} n)/\sqrt{3}} < x\},$$

we have $G_n(x)=F_n(y)$ with

$$y = \frac{x}{\sqrt{3}} + \frac{1/2\ \log^2 n - M_n}{\log^{3/2} n} = \frac{x}{\sqrt{3}} + O[\frac{1}{\log^{3/2} n}]$$

and

$$G_n(x) - F(\frac{x}{\sqrt{3}}) = F_n(y) - F(y) + F(y) - F(\frac{x}{\sqrt{3}}) =$$

$$= O[\frac{1}{\sqrt{\log n}}] + O(y - \frac{x}{\sqrt{3}}) = O[\frac{1}{\sqrt{\log n}}]$$

and, by (5),

$$F(x/\sqrt{3}) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-v^2/2}\, dv.$$

8^{th} *step. Proof of the Theorem.*

If we set:

$$R_n(x) = \text{Prob}\{\frac{\log r(A)-\frac{1}{2}\log^2 n}{(\log^{3/2} n)/\sqrt{3}} < x\}$$

since $\log r(A) \le f(A)$, we deduce

$$R_n(x) \ge G_n(x)$$

and Proposition 1 gives:

$$R_n(x) \le G_n(y) + O(\frac{1}{\log n})$$

with $y=x+2\sqrt{3}\ (\log\log n)^4/\sqrt{\log n}$. Therefore we have

$$R_n(x) = G_n(x) + O[\frac{(\log\log n)^4}{\sqrt{\log n}}]$$

and the proof of the theorem is finished.

REFERENCES

[1] Berlekamp, E.R., *Algebraic coding theory*, Mc Graw Hill, New-York, 1968.

[2] Carlitz, L., Some topics in the Arithmetic of polynomials, *Bull. Amer. Math. Soc.* 48, 1942, 679-691.

[3] Comtet, L., *Analyse combinatoire*, Presses Universitaires de France, Paris, 1970, collection SUP.

[4] Delange, H., Sur certaines fonctions arithmétiques additives, Séminaire Delange-Pisot (Théorie des nombres), 2^{e} année, 1960-1961, n^{o} 6, 17p.

[5] Elliott, P.D.T.A., *Probabilistic number theory* 2 Vols., Springer Berlin Heidelberg New York, 1979, Grundlehren der mathematischen Wissenschaften n^{o} 239-240.

[6] Erdős P. and Turán P., On some problems of a statistical group-theory III, Acta Math. Acad.Sci. 18(1967), 309-320.

[7] Feller, W., *An introduction to probability theory and its applications*, Vol II, 2nd edition, J.Wiley and sons, 1966-1971.

[8] Mignotte, M. and Nicolas, J.L., Statistiques sur $F_q[X]$, to appear in Annales de l'Institut Henri Poincarré, 1983, n^{o}2.

J.L. Nicolas
Département de Mathématiques
U.E.R. des Sciences de Limoges
123 Avenue Albert Thomas
F-87060 Limoges Cédex
FRANCE