Complex roots of unity and normal numbers

Jean-Marie De Koninck[1] and Imre Kátai[2]

Édition du 26 mai 2014

Abstract

Given an arbitrary prime number q, set $\xi = e^{2\pi i/q}$. We use a clever selection of the values of ξ^α, $\alpha = 1, 2, \ldots$, in order to create normal numbers. We also use a famous result of André Weil concerning Dirichlet characters to construct a family of normal numbers.

AMS Subject Classification numbers: 11K16, 11N37, 11N41
Key words: normal numbers, roots of unity, Dirichlet characters

1 Introduction and statement of the results

Let $\lambda(n)$ be the Liouville function (defined by $\lambda(n) := (-1)^{\Omega(n)}$ where $\Omega(n) := \sum_{p^\alpha \| n} \alpha$). It is well known that the statement "$\sum_{n\le x} \lambda(n) = o(x)$ as $x \to \infty$" is equivalent to the Prime Number Theorem. It is conjectured that if $b_1 < b_2 < \cdots < b_k$ are arbitrary positive integers, then $\sum_{n\le x} \lambda(n)\lambda(n+b_1)\cdots\lambda(n+b_k) = o(x)$ as $x \to \infty$. This conjecture seems presently out of reach since we cannot even prove that $\sum_{n\le x} \lambda(n)\lambda(n+1) = o(x)$ as $x \to \infty$.

The Liouville function belongs to a particular class of multiplicative functions, namely the class $\mathcal{M}^*$ of completely multiplicative functions. Recently, Indlekofer, Kátai and Klesov [2] considered a very special function $f \in \mathcal{M}^*$ constructed in the following manner. Let $\wp$ stand for the set of all primes. For each $q \in \wp$, let $C_q = \{\xi \in \mathbb{C} : \xi^q = 1\}$ be the group of complex roots of unity of order q. As p runs through the primes, let ξ_p be independent random variables distributed uniformly on C_q. Then, let $f \in \mathcal{M}^*$ be defined on $\wp$ by $f(p) = \xi_p$, so that $f(n)$ yields a random variable. In their 2011 paper, Indlekofer, Kátai and Klesov proved that, if $(\Omega, \mathcal{A}, \wp)$ stands for a probability space where ξ_p $(p \in \wp)$ are the independent random variables, then for almost all $\omega \in \Omega$, the sequence $\alpha = f(1)f(2)f(3)\ldots$ is a normal sequence over C_q (see Definition 1 below).

Let us now consider a somewhat different set up. Let $q \ge 2$ be a fixed prime number and set $A_q := \{0, 1, \ldots, q-1\}$. Given an integer $t \ge 1$, an expression of the form $i_1 i_2 \ldots i_t$, where each $i_j \in A_q$, is called a *word* of length t. We use the symbol Λ to denote the *empty word*. Then, A_q^t will stand for the set of words of length t over A_q, while A_q^* will stand for the set of all words over A_q regardless of their length,

[1]Research supported in part by a grant from NSERC.
[2]Research supported by the Hungarian and Vietnamese TET 10-1-2011-0645.

including the empty word Λ. Similarly, we define C_q^* to be the set of words over C_q regardless of their length.

Given a positive integer n, we write its q-ary expansion as

$$n = \varepsilon_0(n) + \varepsilon_1(n)q + \cdots + \varepsilon_t(n)q^t,$$

where $\varepsilon_i(n) \in A_q$ for $0 \le i \le t$ and $\varepsilon_t(n) \neq 0$. To this representation, we associate the word

$$\overline{n} = \varepsilon_0(n)\varepsilon_1(n)\ldots\varepsilon_t(n) \in A_q^{t+1}.$$

Definition 1. *Given a sequence of integers $a(1), a(2), a(3), \ldots$, we will say that the concatenation of their q-ary digit expansions $\overline{a(1)}\,\overline{a(2)}\,\overline{a(3)}\ldots$, denoted by Concat$(\overline{a(n)} : n \in \mathbb{N})$, is a normal sequence if the number $0.\overline{a(1)}\,\overline{a(2)}\,\overline{a(3)}\ldots$ is a q-normal number.*

It can be proved using a theorem of Halász (see [1]) that if $f \in \mathcal{M}^*$ is defined on the primes p by $f(p) = \xi_a$ $(a \neq 0)$, then $\sum_{n \le x} f(n) = o(x)$ as $x \to \infty$.

Now, given $u_0, u_1, \ldots, u_{\ell-1} \in A_q$, let $Q(n) := \prod_{j=0}^{\ell-1}(n+j)^{u_j}$. We believe that if $\max_{j \in \{0,1,\ldots,\ell-1\}} u_j > 0$, then

$$\sum_{n \le x} f(Q(n)) = o(x) \qquad \text{as } x \to \infty. \tag{1.1}$$

If this were true, it would follow that

$$\text{Concat}(f(n) : n \in \mathbb{N}) \quad \text{ is a normal sequence over } C_q.$$

We cannot prove (1.1), but we can prove the following. Let $q \in \wp$ and set $\xi := e^{2\pi i/q}$. Further set $x_k = 2^k$ and $y_k = x_k^{1/\sqrt{k}}$ for $k = 1, 2, \ldots$ Then, consider the sequence of completely multiplicative functions f_k, $k = 1, 2, \ldots$, defined on the primes p by

$$f_k(p) = \begin{cases} \xi & \text{if } k \le p \le y_k, \\ 1 & \text{if } p < k \text{ or } p > y_k. \end{cases} \tag{1.2}$$

Then, set

$$\eta_k := f_k(x_k)f_k(x_k+1)f_k(x_k+2)\ldots f_k(x_{k+1}-1) \qquad (k \in \mathbb{N})$$

and

$$\theta := \text{Concat}(\eta_k : k \in \mathbb{N}).$$

Theorem 1. *The sequence θ is a normal sequence over C_q.*

We now use a famous result of André Weil to construct a large family of normal numbers.

Let q be a fixed prime and set $\xi := e^{2\pi i/q}$ and $\xi_a := e^{2\pi i a/q} = \xi^a$. Recall that C_q stands for the group of complex roots of unity of order q, that is,

$$C_q = \{\varsigma \in \mathbb{C} : \varsigma^q = 1\} = \{\xi^a : a = 0, 1, \ldots, q-1\}.$$

Let $p \in \wp$ be such that $q|p-1$. Moreover, let χ_p be a Dirichlet character modulo p of order q, meaning that the smallest positive integer t for which $\chi_p^t = \chi_0$ is q. (Here χ_0 stands for the principal character.)

Let $u_0, u_1, \ldots, u_{k-1} \in A_q$ and consider the polynomial

$$F(z) = F_{u_0,\ldots,u_{k-1}}(z) = \prod_{j=0}^{k-1} (z+j)^{u_j} \tag{1.3}$$

and assume that its degree is at least 1, that is, that there exists one $j \in \{0, \ldots, k-1\}$ for which $u_j \neq 0$. Further set

$$S_{u_0,\ldots,u_{k-1}}(\chi_p) = \sum_{n \pmod p} \chi_p\left(F_{u_0,\ldots,u_{k-1}}(n)\right).$$

According to a 1948 result of André Weil [4],

$$\left|S_{u_0,\ldots,u_{k-1}}(\chi_p)\right| \leq (k-1)\sqrt{p}. \tag{1.4}$$

For a proof, see Proposition 12.11 (page 331) in the book of Iwaniec and Kowalski [3].

We can prove the following.

Theorem 2. *Let $p_1 < p_2 < \cdots$ be an infinite set of primes such that $q \mid p_j - 1$ for all $j \in \mathbb{N}$. For each $j \in \mathbb{N}$, let χ_{p_j} be a character modulo p_j of order q. Further set*

$$\Gamma_p = \chi_p(1)\chi_p(2)\ldots\chi_p(p-1) \qquad (p = p_1, p_2, \ldots)$$

and

$$\eta := \Gamma_{p_1}\Gamma_{p_2}\ldots \tag{1.5}$$

Then η is a normal sequence over C_q.

As an immediate consequence of this theorem, we have the following corollary.

Corollary 1. *Let $\varphi : C_q \to A_q$ be defined by $\varphi(\xi_a) = a$. Extend the function φ to $\varphi : C_q^* \to A_q^*$ by $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ and let*

$$\varphi(\eta) = \varphi(\Gamma_{p_1})\varphi(\Gamma_{p_2})\ldots$$

and consider the q-ary expansion of the real number

$$\kappa = 0.\varphi(\Gamma_{p_1})\varphi(\Gamma_{p_2})\ldots \tag{1.6}$$

Then κ is a normal number in base q.

Example 1. *Choosing $q = 3$ and $\{p_1, p_2, p_3, \ldots\} = \{7, 13, 19, \ldots\}$ as the set of primes $p_j \equiv 1 \pmod 3$, then, the sequence η defined by (1.5) is normal sequence over $\{0, e^{2\pi i/3}, e^{4\pi i/3}\}$, while κ defined by (1.6) is a ternary normal number.*

2 Proof of Theorem 1

Let ℓ be a fixed positive integer. Let $a_0, a_1, \ldots, a_{\ell-1} \in A_q$. Recall the notation $\xi = e^{2\pi i/q}$. Given a positive integer k, let x, y be such that $x_k \le x < x+y \le x_{k+1} - \ell$. We will now count the number $M([x, x+y] \mid (a_0, \ldots, a_{\ell-1}))$ of those $n \in [x, x+y]$ for which $f_k(n+j) = \xi^{a_j}$ $(j = 0, \ldots, \ell-1)$ holds.

Consider the polynomial

$$P_d(x) = \frac{x^q - 1}{x - \xi^d} = \prod_{\substack{h=0 \\ h \neq d}}^{q-1} (x - \xi^h),$$

so that in particular

$$(x - \xi^d) P_d(x) = x^q - 1.$$

Taking the derivatives on both sides of the above equation yields

$$P_d(x) + (x - \xi^d) P_d'(x) = q x^{q-1}.$$

Thus,

$$P_d(f_k(m)) + (f_k(m) - \xi^d) P_d'(f_k(m)) = q \overline{f_k(m)},$$

where $\overline{z}$ stands for the complex conjugate of z.

We then have

$$P_d(f_k(m)) = \begin{cases} q\overline{f_k(m)} & \text{if } f_k(m) = \xi^d, \\ 0 & \text{if } f_k(m) \neq \xi^d. \end{cases}$$

Write the polynomial P_d as $P_d(m) = \sum_{u=0}^{q-1} e_u(d) m^u$, so that $P_d(0) = \overline{\xi}^d$, that is, $e_0(d) = \overline{\xi}^d$. We then have

$$\begin{aligned} P_{a_0}(f_k(n)) \cdots P_{a_{\ell-1}}(f_k(n+\ell-1)) &= \prod_{h=0}^{\ell-1} \left\{ \sum_{u_h=0}^{q-1} e_{u_h}(a_h) f_k^{u_h}(n+h) \right\} \\ &= \sum_{u_0, \ldots, u_{\ell-1} \in A_q} A(u_0, \ldots, u_{\ell-1}) f_k \left(\prod_{j=0}^{\ell-1} (n+j)^{u_j} \right), \end{aligned} \tag{2.1}$$

where $A(u_0, \ldots, u_{\ell-1}) = e_{u_0}(a_0) \cdots e_{u_{\ell-1}}(a_{\ell-1})$, with $A(0, \ldots, 0) = \overline{\xi}^{a_0 + \cdots + a_{\ell-1}}$.

With integers x, y such that $x_k \le x < x+y \le x_{k+1} - \ell$, we now sum both sides of (2.1) for $n = x, \ldots, x+y$, we then obtain that

$$q^\ell \prod_{j=0}^{\ell-1} \overline{\xi}^{a_j} \cdot M([x, x+y] \mid (a_0, \ldots, a_{\ell-1})) = y \prod_{j=0}^{\ell-1} \overline{\xi}^{a_j}$$

$$+\sum_{\substack{u_0,\ldots,u_{\ell-1}\in A_q\\(u_0,\ldots,u_{\ell-1})\neq(0,\ldots,0)}} A(u_0,\ldots,u_{\ell-1})\sum_{n=x}^{x+y} f_k\left(\prod_{j=0}^{\ell-1}(n+j)^{u_j}\right).$$

Setting

$$Q(n)=\prod_{j=0}^{\ell-1}(n+j)^{u_j},$$

it remains to prove that

$$\lim_{k\to\infty}\frac{1}{x_k}\max_{x_k\le x<x+y\le x_{k+1}-\ell}\left|\sum_{n=x}^{x+y} f_k\left(Q(n)\right)\right|=0. \tag{2.2}$$

To prove this, we proceed using standard techniques. Let $\rho(\delta)$ stand for the number of solutions of the congruence $Q(n)\equiv 0 \pmod{\delta}$, in which case we have $\rho(p^\alpha)=\rho(p)$ for all primes $p>k$ and integers $\alpha\ge 1$. Now define the completely multiplicative function g_k implicitly by the relation

$$f_k(m)=\sum_{d|m} g_k(d),$$

thus implying, in light of (1.2), that

$$g_k(p)=f_k(p)-1=\begin{cases}0 & \text{if } p<k \text{ or } p>y_k,\\ \xi-1 & \text{if } k\le p\le y_k.\end{cases}$$

It follows that

$$\begin{aligned}\sum_{n\in[x,x+y]} f_k\left(Q(n)\right) &= \sum_{n\in[x,x+y]}\sum_{\delta|Q(n)} g_k(\delta)\\ &= \sum_{\delta} g_k(\delta)\sum_{\substack{n\in[x,x+y])\\ Q(n)\equiv 0 \pmod{\delta}}} 1\\ &= y\sum_{\delta}\frac{g_k(\delta)\rho(\delta)}{\delta}+o(1). \end{aligned}\tag{2.3}$$

Now, observe that since $g_k(p^\alpha)=f_k(p^\alpha)-f_k(p^{\alpha-1})=\xi^{\alpha-1}(\xi-1)$, it follows that

$$\begin{aligned}\sum_{\delta}\frac{g_k(\delta)\rho(\delta)}{\delta} &= \prod_p\left(1+\frac{g_k(p)\rho(p)}{p}+\frac{g_k(p^2)\rho(p^2)}{p^2}+\cdots\right)\\ &= \prod_{k\le p\le y_k}\left(1+\frac{\rho(p)(\xi-1)}{p}\left(1+\frac{\xi}{p}+\frac{\xi^2}{p^2}+\cdots\right)\right)\\ &= \prod_{k\le p\le y_k}\left(1+\frac{\rho(p)(\xi-1)}{p}\cdot\frac{1}{1-\xi/p}\right)\end{aligned}$$

$$= \prod_{k \le p \le y_k} \left(1 + \frac{\rho(p)(\xi - 1)}{p - \xi}\right)$$

$$(2.4) \qquad = \exp\left\{\rho(p)(\xi - 1) \sum_{k \le p \le y_k} \frac{1}{p} + O(1)\right\}.$$

But, since $\Re(\xi - 1) < 0$, we have that

$$(2.5) \qquad \exp\left\{\rho(p)(\xi - 1) \sum_{k \le p \le y_k} \frac{1}{p} + O(1)\right\} \to 0 \quad \text{as } k \to \infty.$$

Hence, combining (2.5) with (2.4) and (2.3), we obtain (2.2).

We have thus established that

$$M([x, x + y] \mid (a_0, \dots, a_{\ell-1})) - \frac{y}{q^\ell} = o(x_k) \qquad (k \to \infty),$$

which completes the proof of Theorem 1.

3 Proof of Theorem 2

As we will see, the proof of Theorem 2 is essentially a consequence of Weil's result (1.4).

Let ℓ be a fixed positive integer. Fix a prime p and let $\beta = \xi_{e_0} \dots \xi_{e_{\ell-1}}$ be any word belonging to C_q^ℓ. Consider the expression

$$f_\beta(n) = \prod_{j=0}^{\ell-1} \prod_{\substack{\xi \in C_q \\ \xi \ne \xi_{e_j}}} \left(\chi_p(n + j) - \xi\right).$$

Observe that $f_\beta(n) = 0$ if $\chi(n) \dots \chi(n + \ell - 1) \in C_q^\ell$ is different from β. But if $\chi(n) \dots \chi(n + \ell - 1) = \beta$, then

$$f_\beta(n) = \prod_{j=0}^{\ell-1} \prod_{\substack{\xi \in C_q \\ \xi \ne \xi_{e_j}}} \left(\xi_{e_j} - \xi\right).$$

Since, for each $j = 0, \dots, \ell - 1$,

$$\frac{d}{dx}(x^q - 1)\Big|_{x = \xi_{e_j}} = q\xi_{e_j}^{q-1} = q\overline{\xi_{e_j}},$$

it follows that

$$f_\beta(n) = q^\ell \left(\overline{\xi_{e_0} \dots \xi_{e_{\ell-1}}}\right),$$

where again $\overline{z}$ stands for the complex conjugate of z. Hence, letting $M_p(\beta)$ stand for the number of occurrences of β as a subword in the word Γ_p, we have

$$\overline{\xi_{e_0}\dots\xi_{e_{\ell-1}}}q^\ell M_p(\beta)=\sum_{n=1}^{p-\ell} f_\beta(n). \tag{3.1}$$

Now $f_\beta(n)$ can be written as

$$f_\beta(n)=\sum_{(u_0,\dots,u_{\ell-1})\in A_q^\ell} A(u_0,\dots,u_{\ell-1})\chi(F_{u_0,\dots,u_{\ell-1}}(n)), \tag{3.2}$$

where

$$\begin{aligned} F_{u_0,\dots,u_{\ell-1}}(n) &= \prod_{j=0}^{\ell-1}(n+j)^{u_j}, \\ A(0,\dots,0) &= \overline{\xi_{e_0}}\dots\overline{\xi_{e_{\ell-1}}}. \end{aligned}$$

Thus taking into account (1.3), the Weil inequality (1.4) and the above relations (3.1) and (3.2), we obtain that

$$\begin{aligned} &\left|\overline{\xi_{e_0}\dots\xi_{e_{\ell-1}}}\left(q^\ell M_p(\beta)-(p-\ell)\right)\right| \\ &\le \sum_{\substack{(u_0,\dots,u_{\ell-1})\in A_q^\ell \\ (u_0,\dots,u_{\ell-1})\neq(0,\dots,0)}} |A(u_0,\dots,u_{\ell-1})|\cdot\left|\sum_{n=1}^{p-\ell}\chi(F_{u_0,\dots,u_{\ell-1}}(n))\right| \\ &\le \sum_{\substack{(u_0,\dots,u_{\ell-1})\in A_q^\ell \\ (u_0,\dots,u_{\ell-1})\neq(0,\dots,0)}} |A(u_0,\dots,u_{\ell-1})|\cdot((\ell-1)\sqrt{p}+\ell) \\ &\le c_1(\ell)\sqrt{p}. \end{aligned}$$

We have thus shown that

$$\left|M_p(\beta)-\frac{p-\ell}{q^\ell}\right|\le c(\ell)\sqrt{p},$$

thus completing the proof of Theorem 2.

4 Conflicts of interest

The authors of this manuscript certify that they have no conflicts of interest.

References

[1] G. Halász, *Über die Mittelwerte multiplikativen zahlentheoretischer Funktionen*, Acta Math. Acad. Scient. Hungaricae **19** (1968), 365–404.

[2] K.H. Indlekofer, I. Kátai and O. Klesov, *Renewal theorems for some weighted renewal functions*, Ann. Univ. Sci. Budapest. Sect. Comput. **34** (2011), 179-194.

[3] H. Iwaniec and E. Kowalski, *Analytic number theory*, Volume 53, AMS, 2004.

[4] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci.U. S. A. **34** (1948), 204–207.

Jean-Marie De Koninck
Dép. de mathématiques et de statistique
Université Laval
Québec
Québec G1V 0A6
Canada
jmdk@mat.ulaval.ca

Imre Kátai
Computer Algebra Department
Eötvös Loránd University
1117 Budapest
Pázmány Péter Sétány I/C
Hungary
katai@compalg.inf.elte.hu

JMDK, le 26 mai 2014; fichier: normal-numbers-complex-roots-may-2014.tex