Constructing normal numbers using residues of selective prime factors of integers

JEAN-MARIE DE KONINCK\textsuperscript{1} and IMRE KÁTAI\textsuperscript{2}

Dedicated to Professor András Benczur
on the occasion of his seventieth anniversary

Édition du 25 janvier 2014

Abstract

Given an integer $N \geq 1$, for each integer $n \in J_N := [e^N, e^{N+1})$, let $q_N(n)$ be the smallest prime factor of $n$ which is larger than $N$; if no such prime factor exists, set $q_N(n) = 1$. Fix an integer $Q \geq 3$ and consider the function $f(n) = f_Q(n)$ defined by $f(n) = \ell$ if $n \equiv \ell \pmod{Q}$ with $(\ell, Q) = 1$ and by $f(n) = \Lambda$ otherwise, where $\Lambda$ stands for the empty word. Then consider the sequence $(\kappa(n))_{n \geq 1} = (\kappa_Q(n))_{n \geq 1}$ defined by $\kappa(n) = f(q_N(n))$ if $n \in J_N$ with $q_N(n) > 1$ and by $\kappa(n) = \Lambda$ if $n \in J_N$ with $q_N(n) = 1$. Then, for each integer $N \geq 1$, consider the concatenation of the numbers $\kappa(1), \kappa(2), \ldots$, that is define $\theta_N := \text{Concat}(\kappa(n) : n \in J_N)$. Then, set $\alpha_Q := \text{Concat}(\theta_N : N = 1, 2, 3, \ldots)$. Finally, let $B_Q = \{\ell_1, \ell_2, \ldots, \ell_{\varphi(Q)}\}$ be the set of reduced residues modulo $Q$, where $\varphi$ stands for the Euler function. We show that $\alpha_Q$ is a normal sequence over $B_Q$.

AMS Subject Classification numbers: 11K16, 11N37, 11N41
Key words: normal numbers, smallest prime factor

1 Introduction

In previous papers ([1], [2], [3]), we showed how one could construct normal numbers by concatenating the digits of the numbers $P(2)$, $P(3)$, $P(4)$, \ldots, where $P(n)$ stands for the largest prime factor of $n$, then similarly by using the $k$-th largest prime factor instead of the largest prime factor and finally by doing the same replacing $P(n)$ by $p(n)$, the smallest prime factor of $n$.

Here, we consider a different approach which uses the residue modulo an integer $Q \geq 3$ of the smallest element of a particular set of prime factors of an integer $n$. But first, we need to set the table.

For a given integer $Q \geq 3$, let $A_Q := \{0, 1, \ldots, Q - 1\}$. Given an integer $t \geq 1$, an expression of the form $i_1i_2\ldots i_t$, where each $i_j \in A_Q$, is called a finite word of length

\textsuperscript{1}Research supported in part by a grant from NSERC.
\textsuperscript{2}Research supported by the Hungarian and Vietnamese TET 10-1-2011-0645.
$t$. The symbol $Λ$ will denote the empty word. We let $A_Q^t$ stand for the set of all words of length $t$. An infinite sequence of digits $a_1a_2\ldots$, where each $a_i \in A_Q$, is called an infinite word.

An infinite sequence $a_1a_2\ldots$ of base $Q$ digits is called a normal sequence over $A_Q$ if any preassigned sequence of $k$ digits occurs at the expected frequency of $1/Q^k$.

Given a fixed integer $Q \geq 3$, let

\begin{equation}
(1.1)\quad f_Q(n) := \begin{cases}
Λ & \text{if } (n, Q) \neq 1, \\
\ell & \text{if } n \equiv \ell \pmod{Q}, \quad (\ell, Q) = 1.
\end{cases}
\end{equation}

Write $p_1 < p_2 < \cdots$ for the sequence of consecutive primes, and consider the infinite word

$$ξ_Q = f_Q(p_1)f_Q(p_2)f_Q(p_3)\ldots$$

Let

$$B_Q = \{\ell_1, \ell_2, \ldots, \ell_{\varphi(Q)}\}$$

be the set of reduced residues modulo $Q$, where $\varphi$ stands for the Euler totient function.

In an earlier paper [4], we conjectured that the word $ξ_Q$ is a normal sequence over $B_Q$ in the sense that given any integer $k \geq 1$ and any word $β = r_1\ldots r_k \in B_Q^k$, and further setting

$$ξ_Q^{(N)} = f_Q(p_1)f_Q(p_2)\ldots f_Q(p_N) \quad \text{for each } N \in \mathbb{N}$$

and

$$M_N(ξ_Q|β) := \#\{((γ_1, γ_2)|ξ_Q^{(N)} = γ_1βγ_2\},$$

we have

$$\lim_{N \to \infty} \frac{M_N(ξ_Q|β)}{N} = \frac{1}{\varphi(Q)^k}.$$

In this paper, we consider a somewhat similar but more simple problem, namely by using the residue of the smallest prime factor of $n$ (modulo $Q$) which is larger than a certain quantity, and this time we obtain an effective result.

### 2 Main result

Given an integer $N \geq 1$, for each integer $n \in J_N := [x_N, x_{N+1}) := [e^N, e^{N+1})$, let $q_N(n)$ be the smallest prime factor of $n$ which is larger than $N$; if no such prime factor exists, set $q_N(n) = 1$. Fix an integer $Q \geq 3$ and consider the function $f(n) = f_Q(n)$ defined by (1.1). Then consider the sequence $(κ(n))_{n \geq 1} = (κ_Q(n))_{n \geq 1}$ defined by $κ(n) = f(q_N(n))$ if $n \in J_N$ with $q_N(n) > 1$ and by $κ(n) = Λ$ if $n \in J_N$ with $q_N(n) = 1$.

Then, for each integer $N \geq 1$, consider the concatenation of $κ(1), κ(2), κ(3), \ldots$, that is define

$$θ_N := \text{Concat}(κ(n) : n \in J_N).$$
Then, setting
\[ \alpha_Q := \text{Concat}(\theta_N : N = 1, 2, 3, \ldots), \]
we will prove the following result.

**Theorem 1.** The sequence \( \alpha_Q \) is a normal sequence over \( B_Q \).

### 3 Proof of the main result

We first introduce the notation \( \lambda_N = \log \log N \). Moreover, from here one, the letters \( p \) and \( \pi \), with or without subscript, always stand for primes. Finally, let \( \varphi \) stand for the set of all primes.

Fix an arbitrary large integer \( N \) and consider the interval \( J := [x, x + y] \subseteq J_N \). Let \( p_1, p_2, \ldots, p_k \) be \( k \) distinct primes belonging to the interval \( (N, N^{\lambda_N}) \). Then, set
\[
S_J(p_1, p_2, \ldots, p_k) := \#\{n \in J : q_N(n + j) = p_j \text{ for } j = 1, 2, \ldots, k\}.
\]

We know by the Chinese Remainder Theorem that the system of congruences (*)
\[ n + j \equiv 0 \pmod{p_j}, \quad j = 1, 2, \ldots, k, \]
has a unique solution \( n_0 < p_1p_2\cdots p_k \) and that any solution \( n \in J \) of (*) is of the form
\[ n = n_0 + mp_1p_2\cdots p_k \]
for some non negative integer \( m \).

Let us now reorder the primes \( p_1, p_2, \ldots, p_k \) as
\[ p_{i_1} < p_{i_2} < \cdots < p_{i_k}. \]

If \( \pi \in \varphi \) and \( N < \pi < p_{i_1} \), it is clear that we will have \( (n + j, \pi) = 1 \) for each \( j \in \{1, 2, \ldots, k\} \). Similarly, if \( \pi \in \varphi \) and \( p_{i_1} < \pi < p_{i_2} \), then \( (n + j, \pi) = 1 \) for each \( j \in \{1, 2, \ldots, k\} \setminus \{i_1\} \), and so on. Let us now introduce the function \( \rho : \varphi \cap (N, p_k] \to \{0, 1, 2, \ldots, k\} \) defined by
\[
\rho(\pi) = \begin{cases} 
    k & \text{if } N < \pi < p_{i_1}, \\
    k - 1 & \text{if } p_{i_1} < \pi < p_{i_2}, \\
    \vdots & \vdots \\
    1 & \text{if } p_{i_{k-1}} < \pi < p_k, \\
    0 & \text{if } \pi \in \{p_1, p_2, \ldots, p_k\}.
\end{cases}
\]

By using the Eratosthenian sieve (see for instance the book of Halberstam and Richert [5]), we easily obtain that, as \( y \to \infty \),
\[
S_J(p_1, \ldots, p_k) = (1 + o(1)) \frac{y}{p_1 \cdots p_k} \prod_{N < \pi < p_k} \left(1 - \frac{\rho(\pi)}{\pi}\right).
\]
Setting \( U := \prod_{N < \pi < p_k} \left( 1 - \frac{\rho(\pi)}{\pi} \right) \), one can see that, as \( N \to \infty \),

\[
\log U = k \log \log N - k \log \log p_1 - (k - 1) \log \log p_2 + (k - 1) \log \log p_1 \\
- \cdots - \log \log p_k + \log \log p_{k-1} + o(1)
\]

implies that

\[
U = (1 + o(1)) \prod_{j=1}^{k} \frac{\log N}{\log p_j} \quad (N \to \infty).
\]

Hence, in light of (3.2), relation (3.1) can be replaced by

\[
S_J(p_1, \ldots, p_k) = (1 + o(1)) \sum_{p_j \equiv r_j \pmod{Q}} \frac{y}{p_1 \cdots p_k} \prod_{j=1}^{k} \frac{\log N}{\log p_j} \quad (y \to \infty).
\]

Now let \( r_1, \ldots, r_k \) be an arbitrary collection of reduced residues modulo \( Q \) and let us define

\[
B_y(r_1, \ldots, r_k) := \sum_{N < p_j \leq N^{\lambda_N}} S_J(p_1, \ldots, p_k).
\]

From the Prime Number Theorem in arithmetic progressions, we have that

\[
\sum_{1 \leq u \leq u + u/\log u} \frac{1}{p \log p} = (1 + o(1)) \frac{1}{\varphi(Q)} \sum_{u \leq p \leq u + u/\log u} \frac{1}{p \log p} \quad (u \to \infty).
\]

On the other hand, it is clear that, from the Prime Number Theorem,

\[
\sum_{N < p \leq N^{\lambda_N}} \frac{1}{p \log p} = (1 + o(1)) \int_{N}^{N^{\lambda_N}} \frac{du}{u \log^2 u} = \frac{1 + o(1)}{\log N} \quad (N \to \infty).
\]

Combining (3.3), (3.5), and (3.4), it follows that, as \( y \to \infty \),

\[
B_y(p_1, \ldots, p_k) = (1 + o(1)) y \sum_{p_j \equiv r_j \pmod{Q}} \prod_{j=1}^{k} \frac{\log N}{p_j \log p_j}
\]

implies that

\[
B_y(p_1, \ldots, p_k) = (1 + o(1)) y \frac{\varphi(Q)^{\lambda_N}}{\varphi(Q)^k}.
\]

Observe also that

\[
\frac{1}{x_N} \# \{ n \in J_N \cap q_N(n) > N^{\lambda_N} \} \to 0 \quad \text{as } x_N \to \infty.
\]
Indeed, it is clear that if \( q_N(n) > N^{\lambda_N} \), then \( \left( n, \prod_{N < \pi < N^{\lambda_N}} \pi \right) = 1 \). Therefore, for some positive absolute constant \( C \), we have

\[
\# \{ n \in J_N : q_N(n) > N^{\lambda_N} \} \leq C x_N \prod_{N < \pi \leq N^{\lambda_N}} \left( 1 - \frac{1}{\pi} \right) \leq C \frac{x_N}{\lambda_N},
\]

which proves (3.7).

We now examine the first \( M \) digits of \( \alpha_Q \), say \( \alpha_Q(M) \). Let \( N \) be such that \( x_N \leq M < x_{N+1} \) and set \( x := x_N, y := M - x_N \) and \( J_0 = [x, x + y] \).

It follows from (3.6) that, as \( y \to \infty \),

\[
\# \{ n \in J_0 : q_N(n+j) \equiv r_j \pmod{Q} \text{ for } j = 1, \ldots, k \} = (1 + o(1)) \frac{y}{\varphi(Q)^k} + O \left( \frac{x_N}{\lambda_N} \right),
\]

where the error term comes from (3.7) and accounts for those integers \( n \in J_N \) for which \( q_N(n) > N^{\lambda_N} \). Running the same procedure for each positive integer \( H < N \), each time choosing \( J_H = [x_H, x_{H+1}] \), we then obtain a formula similar to the one in (3.8).

Gathering the resulting relations allows us to obtain that, for \( X = x + y \),

\[
\lim_{X \to \infty} \frac{1}{X} \# \{ n \leq X : q_N(n+j) \equiv r_j \pmod{Q} \text{ for } j = 1, \ldots, k \} = \lim_{X \to \infty} \frac{1}{X} \left( \sum_{H=1}^{N-1} \# \{ n \in J_H : q_N(n+j) \equiv r_j \pmod{Q} \text{ for } j = 1, \ldots, k \} + \# \{ n \in J_0 : q_N(n+j) \equiv r_j \pmod{Q} \text{ for } j = 1, \ldots, k \} \right)
\]

\[
= \frac{1}{\varphi(Q)^k},
\]

thus completing the proof of Theorem 1.

4 Final remarks

Let \( \Omega(n) := \sum_{p^n \parallel n} \alpha \) stand for the number of prime factors of \( n \) counting their multiplicity. Fix an integer \( Q \geq 3 \) and consider the function \( u_Q(m) = \ell \), where \( \ell \) is the unique non negative number \( \leq Q - 1 \) such that \( m \equiv \ell \pmod{Q} \). Now consider the infinite sequence

\[
\xi_Q = \text{Concat } (u_Q(\Omega(n)) : n \in \mathbb{N}).
\]

We conjecture that \( \xi_Q \) is a normal sequence over \( \{0, 1, \ldots, Q - 1\} \).
Moreover, let $\tilde{\wp} \subset \wp$ be a subset of primes such that $\sum_{p \in \tilde{\wp}} 1/p = +\infty$ and consider the function $\Omega_{\tilde{\wp}}(n) := \sum_{\substack{p \nmid n \atop p \in \tilde{\wp}}} \alpha$. We conjecture that

$$\xi_Q(\tilde{\wp}) := \text{Concat} (u_Q(\Omega_{\tilde{\wp}}(n)) : n \in \mathbb{N})$$

is also a normal sequence over $\{0, 1, \ldots, Q - 1\}$.

Finally, observe that we can also construct normal numbers by first choosing a monotonically growing sequence $(w_N)_{N \geq 1}$ such that $w_N > N$ for each positive integer $N$ and such that $(\log w_N) / N \to 0$ as $N \to \infty$, and then defining $q_N(n)$ as the smallest prime factor of $n$ larger than $w_N$ if $n \in J_N$, setting $q_N(n) = 1$ otherwise. The proof follows along the same lines as the one of our main result.

References


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 25 janvier 2014; fichier: normal-smallest-prime-factor-Q-2014.tex