*PROCEEDINGS OF THE*
*ROMAN NUMBER THEORY ASSOCIATION*
*Volume* 1, *Number* 1, *March* 2016, *pages* 59–66

**Joël Rivat**

# Digital properties of prime numbers

written by Claudio Stirpe

## 1 Introduction

This exposition deals with the digits of prime numbers and oulines some recent results in a joint work of Joël Rivat and Christian Mauduit.

Some of the typical questions that mathematicians are likely to think about include:

- "Are prime number random?"
- "What type of results to expect?"

This is an introduction to some ideas focusing on what kind of result one may expect.

## 2 Prime Number Theorem and Möbius Random Principle

Let $p$ be a prime and consider the von Mangoldt function defined as

$$\Lambda(n) = \log p$$

for $n = p^k$ and zero otherwise.

The famous *Prime Number Theorem* due to Hadamard [1] and, independently, to de la Vallée Poussin [2] states that

$$\sum_{n \le x} \Lambda(n) = x + o(x). \tag{1}$$

Let $f$ be a function defined over the natural numbers. We say that $f$ satisfies Prime Number Theorem (PNT) if $\sum_{n \le x} \Lambda(n) f(n)$ admits an asymptotic formula.

The special case when $f(n) = \exp(2\pi i \alpha n)$ is relevant for Vinogradov 3-primes Theorem [13]: *Let*

$$r(N) = \sum_{k_1+k_2+k_3=N} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3).$$

Then

$$r(N) = \frac{1}{2} \prod_{p \mid N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \nmid N} \left(1 + \frac{1}{(p-1)^3}\right) N^2 + O\left(\frac{N^2}{\log^A N}\right) \tag{2}$$

*where $A$ is a fixed positive real number.* The proof of (2) is based on the identity:

$$r(N) = \int_0^1 \left(\sum_{n=1}^{N} \Lambda(n) \exp(2\pi i \alpha n)\right)^3 \exp(-2\pi i \alpha N)\, d\alpha.$$

Vinogradov's result implies that every sufficiently large odd integer $n$ can be written as the sum of three primes. The result was extended by Helfgott [8] to all $n \ge 5$.

An other natural question is "Has $n$ an odd number of primes in its factorization or not?". This is the reason why Möbius function arises as

$$\mu(n) = (-1)^k,$$

where $k$ is the number of distinct primes dividing $n$ for any squarefree $n$ and $\mu(n) = 0$ otherwise.

As above we say that $f$ satisfies Möbius Random Principle (MRP) if $\sum_{n\leq x}\mu(n)f(n)$ is close to zero.

These concepts are strongly related with Sarnak's conjecture [12] which relies on determining types of prime densities and functions produced by zero topological entropy dynamical system.

MRP is easy to prove for $f = 1$ as $\sum_{n\leq x}\mu(n) = o(x)$. The reader may compare this result with (1) which states that $f = 1$ satisfies PNT, but MRP is sometimes easier to show than PNT for general $f$.

## 3 Are prime number digits random?

Now we turn to prime numbers. Are the digits of prime numbers random? This is a difficult question so we formulate it into another way using Gelfond's results [7]. Let $q \geq 2$ be an integer and let $\epsilon_j(n)$ be the $j$-th digit in the $q$-ary expansion of $n$ and consider

$$S(n) = \sum_j \epsilon_j(n).$$

We recall a property of $S(n)$ about arithmetic progressions $\{s+km|\ k \in \mathbb{Z}\}$.

**Theorem 1 (Gelfond [7], 1968)** *Given an integer $m \geq 2$, prime to $q-1$, there exists $\sigma_m > 0$ such that for any integer $m' > 0$ and for any arithmetic progression $A = \{s+km|\ k \in \mathbb{Z}\}$ and $A' = \{s'+km'|\ k \in \mathbb{Z}\}$*

$$\sum_{n\leq x,\ (S(n),n)\in(A,A')} 1 = \frac{x}{m'm} + O(x^{1-\sigma_m}).$$

Again compare this formula with (1). The sum of digits is well distributed in arithmetic progressions !

Gelfond underlines two important problems:

1. Evaluate the number of prime numbers $p \leq x$ such that $S(p) \equiv a \mod m$;

2. Consider polynomial analogues: evaluate the number of integers $n \leq x$ such that $S(P(n)) \equiv a \mod m$, where $P$ is a polynomial.

In the rest of this note, we will focus on the first question only.

In 2010, for $f(n) = \exp(2\pi i \alpha S(n))$ and $\alpha$ satisfing $(q-1)\alpha \in \mathbb{R} - \mathbb{Z}$, a PNT properties was estabilished in [10]. Namely

$$\left| \sum_{n \leq x} \Lambda(n) \exp(2\pi i \alpha S(n)) \right| \leq C_q(\alpha) x^{1-\sigma_q(\alpha)},$$

for suitable constants $C_q(\alpha)$ and $\sigma_q(\alpha)$ depending on $q$ and $\alpha$.

Let $(p_n)_{n\geq 1}$ denote the sequence of prime numbers. By the previous result, the sequence $(\alpha S(p_n))_{n\geq 1}$ is equidistributed modulo 1 for any $\alpha \in \mathbb{R} - \mathbb{Z}$. Moreover for any integer $a$ and $m \geq 2$, with $m$ prime to $q-1$ we get

$$\sum_{\substack{p \leq x \\ S(p) \equiv a \mod m}} 1 \sim \frac{1}{m} \sum_{p \leq x} 1,$$

for large $x$.

In 2005 Dartyge-Tenenbaum [4] proved a similar result for MRP.

A more difficult result [5] was obtained in 2009 about the number of primes $p$ satisfing $S(p) = k$. This number is close to the expected value $\frac{q-1}{2} \log_q x$ as follows:

$$|\{p \leq x |\ S(p) = k\}| =$$

$$\frac{(q-1)\pi(x)}{\varphi(q-1)\sqrt{2\pi\sigma_q^2 \log_q x}} \exp\left(\frac{-(k - \mu_q \log_q x)^2}{2\sigma_q^2 \log_q x}\right) + O((\log_q x)^{-\frac{1}{2}+\epsilon}),$$

where we denote by $\mu_q$ and $\sigma_q$ the numbers $\frac{q-1}{2}$ and $\frac{q^2-1}{12}$, respectively. and $\epsilon > 0$ is an arbitrary, fixed real number. Such a local result was previously considered "hopelessly difficult" by Erdös!

One may also fix digits and their positions and wonder about asymptotic properties only. Recently, in 2014, Bourgain showed the existence

of an asymptotical formula for the existence of a small constant $c > 0$ such that for given integers $k$ and $\ell$ with $1 \le \ell \le ck$ we get

$$\left|\{p < 2^k, \epsilon_{j_1}(p) = b_1, \dots, \epsilon_{j_\ell}(p) = b_\ell\}\right| \sim \frac{1}{2^\ell}\frac{2^k}{\log 2^k},$$

for large $k$, and for any choise of $1 < j_1 < \dots < j_\ell = k - 1$ and $(b_1, \dots, b_\ell) \in \{0, 1\}^\ell$ with $b_\ell = 1$.

We can also consider more general functions $f$ and try to establish similar properties: similar results are given for strongly $q$-multiplicative functions $f$ (see [9]) and for block counting functions, as Rudin-Shapiro sequence, see the following section.

## 4 Correlations in the Rudin–Shapiro sequence

We need new ideas for handling sequences like $111\dots111$. Such sequences arises in Mersenne primes $2^n - 1$. So in this section we study correlations of digits.

Let $\delta$ be a positive integer. We define

$$\beta_\delta(n) = \sum_k \epsilon_{k-\delta-1}(n)\epsilon_k(n).$$

This is the number of pairs of 1 in the representation of $n$ with given distance $\delta + 1$. A recent result [11] states that for any real $\alpha$ and $\theta$ there exists explicit constants $C(\delta)$ and $\sigma(\alpha) > 0$ such that

$$\left|\sum_{n\le x} \Lambda(n)\exp(\beta_\delta(n)\alpha + \theta n)\right| \le C(\delta)(\log x)^{\frac{11}{4}} x^{1-\sigma(\alpha)}$$

and

$$\left|\sum_{n\le x} \mu(n)\exp(\beta_\delta(n)\alpha + \theta n)\right| \le C(\delta)(\log x)^{\frac{11}{4}} x^{1-\sigma(\alpha)}.$$

A second generalization about blocks of $d$ consecutive 1's gives very similar results.

**Remark 2** *Our approach can be summarized in a few steps:*

1. *A first step is reducing the problem to an exponential sum.*
2. *Then we remove some digits, namely the upper range and the lower range, using Van der Corput's inequality, and this leads to focus on the digits in the middle range only.*
3. *Separating the problem in two parts is also useful: a discrete part and an analytical part.*
4. *For the first part we may use discrete Fourier transform. For the second we use analytic methods to see which Fourier estimates are needed. We may study the lowest terms of the string by passing n modulo any integer l. We may also consider the first digits by dividing with powers of q.*
5. *Finally, obtain the corresponding Fourier estimates.*

## 5 Open problems

We finish this overview with three open problems.

1. What about the digits of $p^2$?

   This problem is completely open and not so easy to handle.

2. Consider the sequence $(t_{P(p_n)})_{n\in\mathbb{N}}$, where $t_n = (-1)^{S(n)}$ is the Thue-Morse sequence and $P$ is a non constant polynomial with $P(n) \in \mathbb{N}$ for any $n \in \mathbb{N}$. Is it true that this sequence is normal?

3. What can we say from a dynamical system point of view?

## References


[1] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. Soc. Math. France **24**, 199–220 (1896).

[2] Ch.-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Brux. S. sc. **21**, 183–256, 281–362, 363–397 (1896).

[3] J. Bourgain, *Prescribing the binary digits of primes*, Israel J. Math. **194**, no. 2, 935–955 (2013).

[4] C. Dartyge, and G. Tenenbaum, *Sommes des chiffres de multiples d'entiers*, Ann. Inst. Fourier (Grenoble) **55**, 2423–2474 (2005).

[5] M. Drmota, C. Mauduit, and J. Rivat, *Primes with an average sum of digits*, Compos. Math. **145**, no. 2, 271–292 (2009).

[6] M. Drmota, C. Mauduit, and J. Rivat, *The sum-of-digits function of polynomial sequences*. J. Lond. Math. Soc. (2), **84**, 81–102 (2011).

[7] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arithmetica **13**, 259–265 (1968).

[8] H. A. Helfgott, *The ternary Goldbach problem*, `arXiv:1501.05438v2 [math.NT]`.

[9] B. Martin, M. Mauduit, and J. Rivat, *Prime Number Theorem for digital functions*, Acta Arith. **165**, no. 1, 11–45 (2014).

[10] C. Mauduit, and J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) **171**, no. 3, 1591–1646 (2010).

[11] C. Mauduit, and J. Rivat, *Prime numbers along Rudin–Shapiro sequences*, J. Eur. Math. Soc. **27**, 2595–2642 (2015).

[12] P. Sarnak, *Mobius randomness and dynamics*, lecture slides summer 2010 http://www.math.princeton.edu/sarnak/.

[13] I. M. Vinogradov, *The method of Trigonometrical Sums in the Theory of Numbers, translated from the Russian, revised and annotated by K. F. Roth and A. Davenport*, Interscience, London 1954.

Claudio Stirpe
Dipartimento di Matematica
Sapienza Università di Roma
Piazzale Aldo Moro 5
I–00185 Rome, ITALY
email: stirpe@mat.uniroma1.it