On the digits of prime numbers

Joël RIVAT

Institut de Mathématiques de Luminy,
Université d'Aix-Marseille, France.
rivat@iml.univ-mrs.fr

work in collaboration with

Christian MAUDUIT (Marseille)

Prime Number Theorem and Möbius Randomness Principle

p is always a prime number.

Von Mangoldt function: $\Lambda(n) = \log p$ if $n = p^k$, $\Lambda(n) = 0$ otherwise.

Prime Number Theorem (Hadamard, de la Vallée Poussin, 1896, indep.): $\sum_{n \leqslant x} \Lambda(n) = x + o(x)$.

Möbius function: $\mu(n) = (-1)^r$ if $n = p_1 \cdots p_r$ (distinct), $\mu(n) = 0$ if $\exists p$, $p^2 \mid n$.

Given a "reasonable" f, we say that f satisfies a PNT if we can get an assymptotic formula for $\sum_{n \leqslant x} \Lambda(n) f(n)$ while we say that f satisfies the MRP if $\sum_{n \leqslant x} \mu(n) f(n)$ is "small".

These concepts are strongly related with Sarnak's conjecture if f is produced by a zero topological entropy dynamical system.

For $f = 1$ these properties are equivalent: $\sum_{n \leqslant x} \mu(n) = o(x)$.

For more general f the MRP might be (slightly) less difficult to show than the PNT.

Gelfond's paper

In base $q \geqslant 2$ any $n \in \mathbb{N}$ can be written $n = \sum_{j \geqslant 0} \varepsilon_j(n)\, q^j$ where $\varepsilon_j(n) \in \{0, \ldots, q-1\}$.

Theorem A (Gelfond, 1968) *The sum of digits* $\mathsf{s}(n) = \sum_{j \geqslant 0} \varepsilon_j(n)$ *is well distributed in arithmetic progressions: given* $m \geqslant 2$ *with* $(m, q-1) = 1$, *there exists an explicit* $\sigma_m > 0$ *such that*

$$\forall m' \in \mathbb{N}^*,\ \forall (n',\ s) \in \mathbb{Z}^2, \qquad \sum_{\substack{n \leqslant x \\ n \equiv n' \bmod m' \\ \mathsf{s}(n) \equiv s \bmod m}} 1 = \frac{x}{mm'} + O(x^{1-\sigma_m}).$$

Problem A (Gelfond, 1968)

1. *Evaluate the number of prime numbers* $p \leqslant x$ *such that* $\mathsf{s}(p) \equiv a \bmod m$.

2. *Evaluate the number of integers* $n \leqslant x$ *such that* $\mathsf{s}(P(n)) \equiv a \bmod m$, *where* P *is a suitable polynomial* [for example $P(n) = n^2$].

(Not so) Old results

Fouvry–Mauduit (1996):

$$\sum_{\substack{n\leqslant x\\ n=p \text{ or } n=p_1p_2\\ \mathsf{s}(n)\equiv a \bmod m}} 1 \geqslant \frac{C(q,m)}{\log\log x} \sum_{\substack{n\leqslant x\\ n=p \text{ or } n=p_1p_2}} 1.$$

Dartyge–Tenenbaum (2005): For $r \geqslant 2$,

$$\sum_{\substack{n\leqslant x\\ n=p_1\dots p_r\\ \mathsf{s}(n)\equiv a \bmod m}} 1 \geqslant \frac{C(q,m,r)}{\log\log x \log\log\log x} \sum_{\substack{n\leqslant x\\ n=p_1\dots p_r}} 1.$$

Write $\mathrm{e}(t) = \exp(2i\pi t)$.

Dartyge–Tenenbaum (2005) proved the Möbius Randomness Principle for $f(n) = \mathrm{e}(\alpha s(n))$:

$$\sum_{n\leqslant x} \mu(n)\,\mathrm{e}(\alpha s(n)) = O\left(\frac{x}{\log\log x}\right)$$

Sum of digits of primes

Theorem 1 (Mauduit-Rivat, 2010) *If* $(q-1)\alpha \in \mathbb{R}\setminus\mathbb{Z}$, *there exists* $C_q(\alpha) > 0$ *and* $\sigma_q(\alpha) > 0$,

$$\left|\sum_{p\leqslant x} \mathrm{e}(\alpha\,\mathrm{s}(p))\right| \leqslant C_q(\alpha)\, x^{1-\sigma_q(\alpha)}.$$

Corollary 1 *For* $q \geqslant 2$ *the sequence* $(\alpha\,\mathrm{s}(p_n))_{n\geqslant 1}$ *is equidistributed modulo* 1 *if and only if* $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ *(here* $(p_n)_{n\geqslant 1}$ *denotes the sequence of prime numbers).*

Corollary 2 *For* $q \geqslant 2$, $m \geqslant 2$ *such that* $(m, q-1) = 1$ *and* $a \in \mathbb{Z}$,

$$\sum_{\substack{p\leqslant x\\ \mathrm{s}(p)\equiv a \bmod m}} 1 \;\sim\; \frac{1}{m}\sum_{p\leqslant x} 1 \quad (x\to+\infty).$$

Theorem 2 (Drmota-Mauduit-Rivat, 2009) *local result:* $s(p) = k$ *for* k *"central".*

Theorem 3 (Mauduit-Rivat,2009) *If $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$, there exist $C_q(\alpha) > 0$ and $\sigma_q(\alpha) > 0$,*

$$\left| \sum_{n \leqslant x} \mathrm{e}(\alpha\, \mathsf{s}(n^2)) \right| \leqslant C_q(\alpha)\, x^{1-\sigma_q(\alpha)}.$$

Corollary 3 *For $q \geqslant 2$ the sequence $(\alpha\, \mathsf{s}(n^2))_{n \geqslant 1}$ is equidistributed modulo 1 if and only if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*

Corollary 4 *For $q \geqslant 2$, $m \geqslant 2$ such that $(m, q-1) = 1$ and $a \in \mathbb{Z}$,*

$$\sum_{\substack{n \leqslant x \\ \mathsf{s}(n^2) \equiv a \bmod m}} 1 \sim \frac{x}{m} \quad (x \to +\infty).$$

Theorem 4 (Drmota-Mauduit-Rivat,2011) *Idem for $\mathsf{s}(P(n))$ where $P(X) \in \mathbb{Z}[X]$ is of degree $d \geqslant 2$, such that $P(\mathbb{N}) \subset \mathbb{N}$ and with leading coefficient a_d such that $(a_d, q) = 1$ and $q \geqslant q_0(d)$.*

Further questions

Are we able to extend these results to more general digital functions f ?

- For f strongly q-multiplicative, Martin-Mauduit-Rivat:

$$\left|\sum_{n\leqslant x} \Lambda(n) f(n)\, \mathrm{e}(\theta n)\right| \leqslant C_q(f)\ x^{1-\sigma_q(f)}$$

- For block counting related functions (e.g. Rudin-Shapiro sequence)

$$f(n) = \mathrm{e}\left(\alpha \sum_{j\geqslant 1} \varepsilon_{j-1}(n)\varepsilon_j(n)\right) ?$$

  Wait and see...

Sum over prime numbers

By partial summation $\sum_{p\leqslant x} g(p) \longrightarrow \sum_{n\leqslant x} \Lambda(n)\, g(n)$ where $\Lambda(n)$ is von Mangoldt's function.

Advantage: convolutions !

$$\Lambda * 1\!\!1 = \log, \quad \text{i.e.} \quad \sum_{d\,|\,n} \Lambda(d) = \log n.$$

A classical process (Vinogradov, Vaughan, Heath-Brown) remains (using some more technical details), for some $0 < \beta_1 < 1/3$ and $1/2 < \beta_2 < 1$, to estimate uniformly the sums

$$S_I := \sum_{m\sim M} \Big| \sum_{n\sim N} g(mn) \Big| \qquad \text{for } M \leqslant x^{\beta_1} \text{ (type I)}$$

where $MN = x$ (which implies that the "easy" sum over n is long) and for all complex numbers a_m, b_n with $|a_m| \leqslant 1$, $|b_n| \leqslant 1$ the sums

$$S_{II} := \sum_{m\sim M} \sum_{n\sim N} a_m b_n\, g(mn) \qquad \text{for } x^{\beta_1} < M \leqslant x^{\beta_2} \text{ (type II)},$$

(which implies that both sums have a significant length).

Sums of type I

Key idea: the sum over n is free of unknown coefficients.

The knowledge of the function g should permit to estimate the sum $\sum_{n \sim N} g(mn)$.

In our case

$$g(mn) = f(mn)\, \mathsf{e}(\theta mn)$$

where $f(n)$ is some digital function like $f(n) = \mathsf{e}(\alpha\, \mathsf{s}(n))$.

Some arguments from Fouvry and Mauduit (1996) can be generalized.

In particular θ easily disappears in the proof.

Sums of type II - Smoothing the sums

By Cauchy-Schwarz:

$$|S_{II}|^2 \leqslant M \sum_{m\sim M} \left| \sum_{n\sim N} b_n \, f(mn) \, \mathsf{e}(\theta mn) \right|^2 .$$

Expanding the square and exchanging the summations leads to a smooth sum over m, but also two free variables n_1 and n_2 with no control.

Van der Corput's inequality: for $z_1, \ldots, z_L \in \mathbb{C}$ and $R \in \{1, \ldots, L\}$,

$$\left| \sum_{\ell=1}^{L} z_\ell \right|^2 \leqslant \frac{L+R-1}{R} \left(\sum_{\ell=1}^{L} |z_\ell|^2 + 2 \sum_{r=1}^{R-1} \left(1 - \frac{r}{R}\right) \sum_{\ell=1}^{L-r} \Re\left(z_{\ell+r} \overline{z_\ell} \right) \right)$$

where $\Re(z)$ denotes the real part of z.

Now $n_1 = n + r$ and $n_2 = n$ so that the size of $n_1 - n_2 = r$ is small. It remains to estimate

$$\sum_{n\sim N} b_{n+r} \, \overline{b_n} \sum_{m\sim M} f(m(n+r)) \overline{f(mn)} \, \mathsf{e}(\theta mr).$$

Carry propagation

If $f(n) = \mathsf{e}(\alpha\, \mathsf{s}(n))$, then in the difference $\mathsf{s}(m(n+r)) - \mathsf{s}(mn)$, the product mr is much smaller that mn. Take $M \asymp q^{\mu}$, $N \asymp q^{\nu}$ and $R \asymp q^{\rho}$ then

$$\begin{aligned} mn &= \overbrace{\mathsf{35116790780999806546523475473462336857643565}}^{\mu+\nu}, \\ mr &= \underbrace{\mathsf{39657634535456879709564646467570}}_{\mu+\rho}, \end{aligned}$$

we see that in the sum $mn+mr$ the digits after index $\mu+\rho$ may change only by carry propagation.

Proving that the number of pairs (m,n) for which the carry propagation exceeds

$$\mu_2 := \mu + 2\rho$$

is bounded by $O(q^{\mu+\nu-\rho})$, we can ignore them and replace $\mathsf{s}(m(n+r)) - \mathsf{s}(mn)$ by $\mathsf{s}_{\mu_2}(m(n+r)) - \mathsf{s}_{\mu_2}(mn)$ where s_{μ_2} is the truncated s function which considers only the digits of index $< \mu_2$:

$$\mathsf{s}_{\mu_2}(n) := \mathsf{s}(n \bmod q^{\mu_2})$$

which is periodic of period q^{μ_2}.

Sums of type II - Fourier analysis

We are now working modulo q^{μ_2}. For $f_{\mu_2}(n) = \mathsf{e}(\alpha\, \mathsf{s}_{\mu_2}(n))$ and its Discrete Fourier Transform

$$\widehat{f_{\mu_2}}(t) = \frac{1}{q^{\mu_2}} \sum_{0 \leqslant u < q^{\mu_2}} f_{\mu_2}(u)\, \mathsf{e}\left(-\frac{ut}{q^{\mu_2}}\right).$$

By Fourier inversion formula and exchanges of summations we must show that the quantity

$$\sum_{0\leqslant h<q^{\mu_2}} \sum_{0\leqslant k<q^{\mu_2}} \left|\widehat{f_{\mu_2}}(h)\widehat{f_{\mu_2}}(-k)\right| \sum_{n\sim N} \left| \sum_{m\sim M} \mathsf{e}\left(\frac{hm(n+r)+kmn}{q^{\mu_2}} + \theta mr\right)\right|$$

is estimated by $O(q^{\mu+\nu-\rho})$.

The geometric sum over m and the summation over n can be handled by classical arguments from analytic number theory. This can be done uniformly in θ.

The digital structure of f permits to prove the very strong L^1 estimate

$$\sum_{0\leqslant h<q^{\mu_2}} \left|\widehat{f_{\mu_2}}(h)\right| = O\left(q^{\eta\mu_2}\right) \quad \text{with } \eta < 1/2.$$

This is sufficient to conclude for $f(n) = \mathsf{e}(\alpha\, \mathsf{s}(n))$.

The Rudin-Shapiro sequence

Let $f(n) = \mathrm{e}\left(\frac{1}{2}\sum_{j\geqslant 1}\varepsilon_{j-1}(n)\varepsilon_j(n)\right) = (-1)^{\sum_{j\geqslant 1}\varepsilon_{j-1}(n)\varepsilon_j(n)}$.

$\widehat{f_{\mu_2}}$ is a Shapiro polynomial well known to have small absolute value: $\forall t\in\mathbb{R}$, $\left|\widehat{f_{\mu_2}}(t)\right| \leqslant 2^{\frac{1-\mu_2}{2}}$, (with our normalization).

Pál Erdős always said that every talk should contain a proof. Let us study the L^1 norm of $\widehat{f_{\mu_2}}$. From

$$1 = \sum_{0\leqslant h<2^{\mu_2}} \left|\widehat{f_{\mu_2}}(h)\right|^2 \leqslant 2^{\frac{1-\mu_2}{2}} \sum_{0\leqslant h<2^{\mu_2}} \left|\widehat{f_{\mu_2}}(h)\right|$$

we deduce

$$\sum_{0\leqslant h<2^{\mu_2}} \left|\widehat{f_{\mu_2}}(h)\right| \geqslant 2^{\frac{\mu_2-1}{2}}.$$

Therefore (so to say) $\eta = \frac{1}{2}$.

The proof for the sum of digits function cannot be adapted for the Rudin-Shapiro sequence.

A variant of van der Corput's inequality

(Introduced to solve Gelfond's problem for squares)

For $z_1, \ldots, z_L \in \mathbb{C}$ and integers $k \geqslant 1$, $R \geqslant 1$ we have

$$\left| \sum_{\ell=1}^{L} z_\ell \right|^2 \leqslant \frac{L + kR - k}{R} \left(\sum_{\ell=1}^{L} |z_\ell|^2 + 2 \sum_{r=1}^{R-1} \left(1 - \frac{r}{R}\right) \sum_{\ell=1}^{L-kr} \Re\left(z_{\ell+kr} \overline{z_\ell}\right) \right).$$

For $k = 1$ this is the classical van der Corput's inequality.

Interest: control the indexes modulo k.

Taking $k = q^{\mu_1}$, this may permit to remove the lower digits.

Double truncation

Applying the classical Van der Corput inequality leads to replace f by

$$f_{\mu_2}(n) = \mathrm{e}\left(\alpha \sum_{1 \leqslant j < \mu_2} \varepsilon_{j-1}(n)\varepsilon_j(n)\right).$$

Applying the variant of Van der Corput inequality with $k = q^{\mu_1}$ where $\mu_1 = \mu - 2\rho$ leads to replace f_{μ_2} by

$$f_{\mu_1,\mu_2}(n) = f_{\mu_2}(n)\overline{f_{\mu_1}(n)} = \mathrm{e}\left(\alpha \sum_{\mu_1 \leqslant j < \mu_2} \varepsilon_{j-1}(n)\varepsilon_j(n)\right).$$

More generally we have proved that any digital function satisfying a carry propagation property can be replaced here by a function depending only on the digits of indexes $\mu_0, \ldots, \mu_2 - 1$ for some μ_0 close to μ_1, at the price of an acceptable error term.

For the Rudin-Shapiro sequence, $\mu_0 = \mu_1 - 1$.

Fourier analysis

After some technical steps the "digital part" and the "exponential sum part" are separated.

We need to estimate the following sum:

$$\sum_{|h_0| \leqslant q^{\mu_2-\mu_0+2\rho}} \sum_{|h_1| \leqslant q^{\mu_2-\mu_0+2\rho}} \min\left(\frac{q^{\mu_2-\mu_0}}{\pi\,|h_0|}, 1\right) \min\left(\frac{q^{\mu_2-\mu_0}}{\pi\,|h_1|}, 1\right)$$
$$\sum_{h_2 < q^{\mu_2-\mu_0}} \sum_{h_3 < q^{\mu_2-\mu_0}} \left|\widehat{g}(h_0 - h_2)\, \widehat{g}(h_3 - h_1)\, \widehat{g}(-h_2)\, \widehat{g}(h_3)\right|$$
$$\sum_r \sum_s \left| \sum_m \sum_n \mathrm{e}\left(\frac{(h_0+h_1)mn + h_1 mr + (h_2+h_3)q^{\mu_1} sn}{q^{\mu_2}}\right)\right|$$

where g is the $q^{\mu_2-\mu_0}$ periodic function defined by

$$\forall k \in \mathbb{Z},\ g(k) = f_{\mu_1,\mu_2}(q^{\mu_0}k).$$

End of the proof

The "exponential sum part" can be handled by appropriate estimates of exponential sums and similar tools. We need to average over all variables m, n, r, s.

For $\widehat{g}$ we need "only" that the L^∞-norm is small.

This property is known for the sum of digits function and also for the classical Rudin-Shapiro sequence.

For generalized Rudin-Shapiro sequences we can prove it using a well chosen matrix norm.

In general it is very difficult.

Conclusion

We obtain a PNT and MRP for the Rudin-Shapiro sequence and its natural generalizations: counting $1\underbrace{*\cdots*}_{k}1$ for any $k \geqslant 0$, counting (overlapping) blocks $\underbrace{1\cdots1}_{k}$ for $k \geqslant 2$.

More generally we get a PNT and a MRP for any digital function satisfying a carry propagation property for which we can control uniformly the Discrete Fourier Transform.

General result – Definitions

Let $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$.

Definition 1 *A function* $f : \mathbb{N} \to \mathbb{U}$ *has the* carry property *if, uniformly for* $(\lambda, \kappa, \rho) \in \mathbb{N}^3$ *with* $\rho < \lambda$, *the number of integers* $0 \leqslant \ell < q^\lambda$ *such that there exists* $(k_1, k_2) \in \{0, \ldots, q^\kappa - 1\}^2$ *with*

$$f(\ell q^\kappa + k_1 + k_2)\,\overline{f(\ell q^\kappa + k_1)} \neq f_{\kappa+\rho}(\ell q^\kappa + k_1 + k_2)\,\overline{f_{\kappa+\rho}(\ell q^\kappa + k_1)}$$

is at most $O(q^{\lambda-\rho})$ *where the implied constant may depend only on* q *and* f.

Definition 2 *Given a non decreasing function* $\gamma : \mathbb{R} \to \mathbb{R}$ *satisfying* $\lim_{\lambda\to+\infty} \gamma(\lambda) = +\infty$ *and* $c > 0$ *we denote by* $\mathcal{F}_{\gamma,c}$ *the set of functions* $f : \mathbb{N} \to \mathbb{U}$ *such that for* $(\kappa, \lambda) \in \mathbb{N}^2$ *with* $\kappa \leqslant c\lambda$ *and* $t \in \mathbb{R}$*:*

$$\left| q^{-\lambda} \sum_{0 \leqslant u < q^\lambda} f(uq^\kappa)\, \mathrm{e}\,(-ut) \right| \leqslant q^{-\gamma(\lambda)}.$$

General result

Theorem 5 *Let* $\gamma : \mathbb{R} \to \mathbb{R}$ *be a non decreasing function satisfying* $\lim_{\lambda \to +\infty} \gamma(\lambda) = +\infty$, $c \geqslant 10$ *and* $f : \mathbb{N} \to \mathbb{U}$ *be a function satisfying Definition 1 and* $f \in \mathcal{F}_{\gamma,c}$ *in Definition 2. Then for any* $\theta \in \mathbb{R}$ *we have*

$$\left| \sum_{n \leqslant x} \Lambda(n) f(n) \, \mathrm{e}\,(\theta n) \right| \ll c_1(q) (\log x)^{c_2(q)} \, x \, q^{-\gamma(2\lfloor (\log x)/80 \log q \rfloor)/20},$$

with

$$c_1(q) = \max(\tau(q), \log^2 q)^{1/4} \, (\log q)^{-2-\frac{1}{4}\max(\omega(q),2)}$$

and

$$c_2(q) = \frac{9}{4} + \frac{1}{4} \max(\omega(q), 2).$$