Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Joël RIVAT

On Gelfond's conjecture about the sum of digits of prime numbers

Tome 21, n^{o} 2 (2009), p. 415-422.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_2_415_0>

Journal de Théorie des Nombres
de Bordeaux **21** (2009), 415-422

On Gelfond's conjecture about the sum of digits of prime numbers

par Joël RIVAT

Résumé. Dans cet article nous exposons les étapes importantes de la preuve de la conjecture de Gelfond [6] (1968) dans un travail récent en collaboration avec Christian Mauduit [11] concernant la somme des chiffres des nombres premiers, dans l'esprit de l'exposé donné à Edimbourg dans le cadre des Journées Arithmétiques 2007.

Abstract. The goal of this paper is to outline the proof of a conjecture of Gelfond [6] (1968) in a recent work in collaboration with Christian Mauduit [11] concerning the sum of digits of prime numbers, reflecting the lecture given in Edinburgh at the Journées Arithmétiques 2007.

1. The sum of digits function

Let $q \in \mathbb{N}$ with $q \geqslant 2$. All $n \in \mathbb{N}$ can be written uniquely in basis q:

$$n = \sum_{k \geqslant 0} n_k q^k \qquad \text{where } n_k \in \{0, \dots, q-1\}$$

and the sum of digits function is defined by:

$$\mathrm{s}(n) = \sum_{k \geqslant 0} n_k.$$

The sum of digits function has many aspects that have been studied, for instance ergodicity, finite automata, dynamical systems, number theory.

Mahler introduced this function in the context of harmonic analysis:

Theorem A (Mahler [10], 1927)**.** *For $q = 2$, the sequence*

$$\left(\frac{1}{N} \sum_{n<N} (-1)^{s(n)} \, (-1)^{s(n+k)} \right)_{N \geqslant 1}$$

converges for all $k \in \mathbb{N}$ and its limit is different from zero for infinitely many k's.

The origin of our work is the following result of Gelfond:

Theorem B (Gelfond [6], 1968)**.** *Let* $m \geqslant 2$*,* $(m, q-1) = 1$*. Then there exists* $\lambda < 1$ *such that for all* $d \in \mathbb{N}^*$*,* a*,* $r \in \mathbb{Z}$*,*

$$\sum_{\substack{n<N \\ n \equiv r \bmod d \\ \mathrm{s}(n) \equiv a \bmod m}} 1 = \frac{N}{md} + O(N^\lambda).$$

In the same paper Gelfond pose the following problem:
Problem A (Gelfond [6], 1968)**.**

> *Il serait aussi intéressant de trouver le nombre des nombres premiers* $p \leqslant x$ *tels que* $\mathrm{s}(p) \equiv a \bmod m$*.*

(the letter p always denotes a prime number).

2. Prime numbers

The prime numbers constitute a fascinating sequence which poses many difficult questions. Let us mention some open problems:

- are there infinitely many primes of the form $p+2$ (prime twins)?
- are there infinitely many primes of the form n^2+1?
- are there infinitely many primes of the form $2^n - 1$ (Mersenne primes)?
- are there infinitely many primes of the form $2^{2^n}+1$ (Fermat primes)?

and some answers:

- primes of the form $an + b$ (Dirichlet theorem),
- primes such that αp belongs to some prescribed interval $I \subset [0, 1]$, for $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ (Vinogradov theorem [15]),
- primes of the form $\lfloor n^c \rfloor$ where $1 < c < c_0 \approx 1.1$ (Piatetski-Shapiro theorem [12]),
- primes of the form $a^2 + b^4$ (Friedlander-Iwaniec theorem [4, 5]),
- primes of the form $a^3 + 2b^3$ (Heath-Brown theorem [9]),
- primes such that $a_p(E)/(2\sqrt{p})$ belongs to some prescribed interval $I \subset [0, 1]$ (Sato-Tate conjecture for a very large class of elliptic curves E over $\mathbb{Q}$, recently proved by several authors).

3. Historical background

Until recently, very little was known concerning the digits of prime numbers. We can mention a result of Sierpiński [13] (1959), recently generalized by Wolke [16] (2005) and then by Harman [7] (2006), on prime numbers with some prescribed digits.

Concerning Gelfond's question, no progress was made in its original form. Let us mention the two following variants:

Theorem C (Fouvry–Mauduit [2, 3], 1996). *For $m \geqslant 2$ such that $(m, q-1) = 1$, there exists $C(q,m) > 0$ such that for all $a \in \mathbb{Z}$ and $x > 0$,*

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

Theorem D (Dartyge–Tenenbaum [1], 2005). *For $m \geqslant 2$ with $(m, q-1) = 1$ and $r \geqslant 2$, there exists $C(q,m,r) > 0$ such that for all $a \in \mathbb{Z}$ and $x > 0$,*

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

4. Results

Theorem 1 (Mauduit-Rivat). *For $\alpha \in \mathbb{R}$ such that $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$, there exists $C(q,\alpha) > 0$ and $\sigma_q(\alpha) > 0$,*

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

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

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

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

5. Sum over prime numbers

We want to estimate a sum of the form

$$\sum_{p \leqslant x} g(p)$$

where the function g detects the property under consideration. A classical process (Vinogradov [15], Vaughan [14], Heath-Brown [8]) remains (using some more technical details), for some $0 < \beta_1 < 1/3$ and $1/2 < \beta_2 < 1$, to estimate uniformly the sums

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

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

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

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

6. Sums of type I

For the sums of type I we might expect that the knowledge of the function g permits to get a satisfactory estimate of the sum

$$\sum_{n\sim N} g(mn).$$

Indeed in our case where $g(n) = \mathrm{e}(\alpha\, \mathrm{s}(n))$ we were able to adapt successfully arguments from Fouvry and Mauduit [2, 3] (1996).

7. Sums of type II

7.1. Smoothing the sums.

By Cauchy-Schwarz inequality:

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

Here, expanding the square and exchanging the summations, we would get a smooth sum over m, but also two free variables n_1 and n_2. However, we can get a useful control by using van der Corput's inequality:

Lemma 1. *Let $z_1, \ldots, z_L \in \mathbb{C}$. For all $R \in \mathbb{N}^*$ we have*

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

The interest of this inequality is that now we have $n_1 = n+r$ and $n_2 = n$ so that the size of $n_1 - n_2 = r$ is under control.

Now in fact we can take $M = q^\mu$, $N = q^\nu$ and $R = q^\rho$ where μ, ν and ρ are integers such that $\rho/(\mu+\nu)$ is "very small". It remains for $1 \leqslant |r| < q^\rho$ to prove the estimate

$$\left|\sum_{q^{\nu-1}<n\leqslant q^\nu} b_{n+r}\,\overline{b_n} \sum_{q^{\mu-1}<m\leqslant q^\mu} \mathrm{e}(\alpha\, \mathrm{s}(m(n+r)) - \alpha\, \mathrm{s}(mn))\right| = O(q^{\mu+\nu-\rho}).$$

7.2. Truncated sum of digits function.

We want to take advantage of the fact that in the difference $\mathrm{s}(m(n+r)) - \mathrm{s}(mn)$, the product mr is much smaller that mn. In the example:

$$\begin{aligned} mn &= \overbrace{35116790780999806546523475473462336857643565}^{\mu+\nu}, \\ mr &= \underbrace{396576345354568797095646467570}_{\mu+\rho}, \end{aligned}$$

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

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

is bounded by $O(q^{\mu+\nu-\rho})$, we can ignore them and replace $\mathrm{s}(m(n+r)) - \mathrm{s}(mn)$ by $\mathrm{s}_\lambda(m(n+r)) - \mathrm{s}_\lambda(mn)$ where s_λ is the truncated sum of digits function

$$\mathrm{s}_\lambda(n) := \sum_{k<\lambda} n_k,$$

which is periodic of period q^λ.

7.3. Fourier analysis.

The periodicity of s_λ enables us to write

$$\begin{aligned} &\sum_{q^{\mu-1}<m\leqslant q^\mu} \mathrm{e}(\alpha\,\mathrm{s}_\lambda(m(n+r)) - \alpha\,\mathrm{s}_\lambda(mn)) \\ &\qquad = \sum_{0\leqslant u<q^\lambda} \sum_{0\leqslant v<q^\lambda} \mathrm{e}(\alpha\,\mathrm{s}_\lambda(u) - \alpha\,\mathrm{s}_\lambda(v)) \sum_{\substack{q^{\mu-1}<m\leqslant q^\mu \\ m(n+r)\equiv u \bmod q^\lambda \\ mn\equiv v \bmod q^\lambda}} 1. \end{aligned}$$

The orthogonality formula

$$\frac{1}{q^\lambda} \sum_{0\leqslant h<q^\lambda} \mathrm{e}\left(\frac{h\ell}{q^\lambda}\right) = \begin{cases} 1 & \text{if } \ell \equiv 0 \bmod q^\lambda, \\ 0 & \text{if } \ell \not\equiv 0 \bmod q^\lambda, \end{cases}$$

leads us to introduce the discrete Fourier transform of $u \mapsto \mathrm{e}(\alpha\,\mathrm{s}_\lambda(u))$:

$$F_\lambda(h) = q^{-\lambda} \sum_{0\leqslant u<q^\lambda} \mathrm{e}\left(\alpha\,\mathrm{s}_\lambda(u) - \frac{hu}{q^\lambda}\right),$$

and summing over n and taking absolute values we must show that

$$\sum_{0\leqslant h<q^\lambda}\sum_{0\leqslant k<q^\lambda}\left|F_\lambda(h)\,\overline{F_\lambda(-k)}\right| \sum_{q^{\nu-1}<n\leqslant q^\nu}\left|\sum_{q^{\mu-1}<m\leqslant q^\mu}\mathrm{e}\left(\frac{hm(n+r)+kmn}{q^\lambda}\right)\right| = O(q^{\mu+\nu-\rho}).$$

Here we observe that the summations over m (geometric sum !) and n can be handled by classical arguments from analytic number theory, while we hope that the digital structure hidden in F_λ will produce a huge saving.

7.4. Heuristic end of the proof.

On average, for fixed (h,k), the geometric sum over m is small so that the sum over n should be $O(q^{\nu+\varepsilon})$. Hence after many technical steps to handle the exceptions, we will need to get the crucial upper bound

$$\sum_{0\leqslant h<q^\lambda}|F_\lambda(h)| = O\left(q^{\eta\lambda}\right) \quad \text{with } \eta<1/2,$$

which means that we need an upper bound sharper than the square root of the trivial estimate.

Indeed suppose this has been done, then we get

$$\sum_h\sum_k\sum_n\sum_m\cdots = O(q^{2\eta\lambda+\nu+\varepsilon}),$$

and since $\lambda=\mu+2\rho$, we have

$$2\eta\lambda+\nu+\varepsilon \leqslant \mu+\nu-\rho$$

for μ, ν large enough.

8. The discrete Fourier transform

Let us take $q=2$ to simplify all formulas.

It follows from the definition of F_λ that

$$F_0(h)=1,$$

and that for $\lambda\geqslant 1$,

$$F_\lambda(h)=\frac{1}{2^\lambda}\sum_{0\leqslant u<2^\lambda}\mathrm{e}\left(\alpha\,\mathrm{s}(u)-\frac{uh}{2^\lambda}\right)$$

so that

$$F_\lambda(h)=\frac{1}{2^\lambda}\sum_{0\leqslant u<2^{\lambda-1}}\left(\mathrm{e}\left(\alpha\,\mathrm{s}(2u)-\frac{2uh}{2^\lambda}\right)+\mathrm{e}\left(\alpha\,\mathrm{s}(2u{+}1)-\frac{(2u{+}1)h}{2^\lambda}\right)\right).$$

We have

$$s(2u)=s(u) \quad\text{and}\quad s(2u+1)=s(u)+1,$$

hence

$$F_\lambda(h) = \frac{1}{2}\left(1 + \mathrm{e}\left(\alpha - \frac{h}{2^\lambda}\right)\right) F_{\lambda-1}(h)$$

thus

$$|F_\lambda(h)| = \prod_{i=1}^{\lambda} \left|\cos\pi\left(\alpha - \frac{h}{2^i}\right)\right|.$$

We recall that we want to prove that

$$\sum_{0 \leqslant h < 2^\lambda} |F_\lambda(h)| = O(2^{\eta\lambda}) \quad \text{with } \eta < \tfrac{1}{2}.$$

9. Norm 1 of the discrete Fourier transform

Let the transfer operator

$$\begin{aligned}
&\Phi_0(x) = 1\\
&\Phi_i(x) = \left|\cos\pi(\alpha - \tfrac{x}{2})\right| \Phi_{i-1}(\tfrac{x}{2}) + \left|\sin\pi(\alpha - \tfrac{x}{2})\right| \Phi_{i-1}(\tfrac{x+1}{2}).
\end{aligned}$$

We write

$$\begin{aligned}
\sum_{0 \leqslant h < 2^\lambda} |F_\lambda(h)| &= \sum_{0 \leqslant h < 2^{\lambda-1}} \left(|F_\lambda(h)| + \left|F_\lambda(h + 2^{\lambda-1})\right|\right)\\
&= \sum_{0 \leqslant h < 2^{\lambda-1}} |F_{\lambda-1}(h)| \left(\left|\cos\pi(\alpha - \tfrac{h}{2^\lambda})\right| + \left|\sin\pi(\alpha - \tfrac{h}{2^\lambda})\right|\right)\\
&= \sum_{0 \leqslant h < 2^{\lambda-1}} |F_{\lambda-1}(h)| \ \Phi_1\left(\frac{h}{2^{\lambda-1}}\right).
\end{aligned}$$

We can repeat this process and get

$$\sum_{0 \leqslant h < 2^\lambda} |F_\lambda(h)| = \sum_{0 \leqslant h < 2^{\lambda-2}} |F_{\lambda-2}(h)| \ \Phi_2\left(\frac{h}{2^{\lambda-2}}\right).$$

Now

$$\Phi_1^2(x) = \left(\left|\cos\pi(\alpha - \tfrac{x}{2})\right| + \left|\sin\pi(\alpha - \tfrac{x}{2})\right|\right)^2 = 1 + \left|\sin 2\pi(\alpha - \tfrac{x}{2})\right|,$$

and

$$\begin{aligned}
\Phi_2^2(x) &\leqslant \Phi_1^2(\tfrac{x}{2}) + \Phi_1^2(\tfrac{x+1}{2})\\
&= 2 + \left|\sin 2\pi(\alpha - \tfrac{x}{4})\right| + \left|\sin 2\pi(\alpha - \tfrac{x+1}{4})\right|\\
&= 2 + \left|\sin 2\pi(\alpha - \tfrac{x}{4})\right| + \left|\cos 2\pi(\alpha - \tfrac{x}{4})\right|,\\
&\leqslant 2 + \sqrt{2}.
\end{aligned}$$

Hence

$$\sum_{0 \leqslant h < 2^\lambda} |F_\lambda(h)| \leqslant (2 + \sqrt{2})^{1/2} \sum_{0 \leqslant h < 2^{\lambda-2}} |F_{\lambda-2}(h)|,$$

and finally

$$\sum_{0\leqslant h<2^\lambda} |F_\lambda(h)| = O\left((2+\sqrt{2})^{\lambda/4}\right).$$

Since

$$(2+\sqrt{2})^{1/4} < 4^{1/4} = \sqrt{2},$$

we indeed have

$$\sum_{0\leqslant h<2^\lambda} |F_\lambda(h)| = O\left(2^{\eta\lambda}\right)$$

for some $\eta < 1/2$.

References

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

[2] E. Fouvry and C. Mauduit, *Sommes des chiffres et nombres presques premiers*. Mathematische Annalen **305** (1996), 571–599.

[3] E. Fouvry and C. Mauduit, *Méthodes de crible et fonctions sommes des chiffres*. Acta Arithmetica **77** (1996), 339–351.

[4] J. Friedlander and H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*. Ann. of Math. (2) **148** (1998), 945–1040.

[5] J. Friedlander and H. Iwaniec, *Asymptotic sieve for primes*. Ann. of Math. (2) **148** (1998), 1041–1065.

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

[7] G. Harman, *Primes with preassigned digits*. Acta Arith. **125** (2006), 179–185.

[8] D. R. Heath-Brown, *Prime numbers in short intervals and a generalized Vaughan identity*. Can. J. Math. **34** (1982), 1365–1377.

[9] D. R. Heath-Brown, *Primes represented by $x^3 + 2y^3$*. Acta Math. **186** (2001), 1–84.

[10] K. Mahler, *The Spectrum of an Array and Its Application to the Study of the Translation Properties of a Simple Class of Arithmetical Functions. II: On the Translation Properties of a Simple Class of Arithmetical Functions*. J. of Math. Phys. Mass. Inst. Techn. **6** (1927), 158–163.

[11] C. Mauduit, J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*. Annals of Mathematics, à paraître.

[12] I. I. Piatetski-Shapiro, *On the distribution of prime numbers in sequences of the form $[f(n)]$*. Mat. Sbornik N.S. **33**(75) (1953), 559–566.

[13] W. Sierpiński, *Sur les nombres premiers ayant des chiffres initiaux et finals donnés*. Acta Arith. **5** (1959), 265–266.

[14] R. C. Vaughan, *An elementary method in prime number theory*. Acta Arithmetica **37** (1980), 111–115.

[15] 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.

[16] D. Wolke, *Primes with preassigned digits*. Acta Arith. **119** (2005), 201–209.

Joël Rivat
Institut de Mathématiques de Luminy
CNRS-UMR 6206
163 avenue de Luminy
Case 907
13288 Marseille Cedex 9, France.
E-mail: rivat@iml.univ-mrs.fr