Primes and analysis: A powerful combination

Fernando Chamizo

Escuela JAE de Matemáticas 2023

July 7, 2023

Abstract

This paper contains a proof of the existence of infinitely primes having 1 as the last digit. The main goal is to provide an illustration for undergraduates of the effectiveness of analytical tools in prime number theory.

1 A harder than necessary proof

We all know how to prove that there are infinitely many primes. Euclid included a proof in his *Elements* about 23 centuries ago and most probably the one you have in mind is a variation of it.

Many centuries later, Euler got a less elementary proof based on analysis. The starting point is to consider the infinite product of geometric series of ratio p^{-s} where p is prime and $s>1$:

$$\Big(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\dots\Big)\Big(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\dots\Big)\Big(1+\frac{1}{5^s}+\frac{1}{5^{2s}}+\dots\Big)\dots$$

By the fundamental theorem of arithmetic when one expands formally this product each term $1/n^s$ with $n\in\mathbb{Z}^+$ appears exactly once. On the other hand, each parenthesis can be summed with the standard formula and the outcome is the breathtaking *Euler product formula*

$$\prod_p (1-p^{-s})^{-1}=\zeta(s)\qquad \text{where}\quad \zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}. \tag{1.1}$$

Although Euler did not consider it necessary, using basic analysis it is possible to show under 21st century mathematical rigor standards that this formal identity becomes a *bona fide* numerical identity when $s>1$.

If $\epsilon>0$ is very small, $\zeta(1+\epsilon)$ is close to the harmonic series, which diverges. It allows to deduce

$$\lim_{s\to 1^+}\prod_p (1-p^{-s})^{-1}=\infty. \tag{1.2}$$

Of course, this gives a blatant contradiction if the set of primes is finite.

What is the point of giving a harder proof of a simple ancient result? First, the new proof is fancy and arguably a big component of Mathematics is fanciness. On the other hand, it opens new lines for research. For instance, (1.2) implies that the prime sequence cannot grow very quickly and Euler himself already got that $\sum p^{-1}$ diverges. In fact (1.1) suggests that a careful analysis of the singularity of $\zeta(s)$ at $s = 1$ can lead to some result about the growth of the prime numbers. This idea was developed by Riemann. On the other hand, Dirichlet found variations on (1.1) proving the infinitude of the primes in arithmetic progressions (excluding trivial cases) and many people think that it kicked off analytic number theory.

Our goal is to modify Euler's argument to prove an instance of Dirichlet's result, namely that there are infinitely many primes having 1 as the last digit (the one to the right). For instance, 31, 41, 821 and 2011 are some of them. With the notation of congruences $p \equiv 1\ (10)$. In words, 1 is the remainder when the prime p is divided by 10.

2 Expanding the idea

A first natural naive attempt to reach our goal is to conjecture a formula closely resembling (1.1)

$$\prod_{p\equiv 1\ (10)} (1-p^{-s})^{-1} \overset{(?)}{=} \sum_{\substack{n=1\\ n\equiv 1\ (10)}}^{\infty} \frac{1}{n^s}.$$

Too easy to be true. This is **false** because for instance $n = 221 = 13 \cdot 17$ is in the sum and the primes 13 and 17 are not in the product. Summarizing, primes appearing in the factorization of numbers having 1 as last digit do not share in general this property.

Trying to fix the failed attempt, we wonder about the possible generalized Euler product formulas. It is clear that if f is a product preserving function (*completely multiplicative* according to the jargon) $f(mn) = f(m)f(n)$ then we have

$$\prod_{p} \big(1 - f(p)p^{-s}\big)^{-1} = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}. \tag{2.1}$$

We would like to take f such that $f(p) = 1$ if $p \equiv 1\ (10)$ and $f(p) = 0$ otherwise but in this case the divergence of the series is unclear.

Let us play with the signs to get examples in which the convergence is easily decided. Consider in (2.1) the choices $f = \chi_0$ and $f = \chi_1$ given by

this table:

	$n \equiv 1$	$n \equiv 3$	$n \equiv 7$	$n \equiv 9$	otherwise
χ_0	1	1	1	1	0
χ_1	1	-1	-1	1	0

It goes without saying that the congruences are modulo 10.

The corresponding functions are:

$$L_0(s) = \prod_p \big(1 - \chi_0(p)p^{-s}\big)^{-1} = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = \sum_{\ell=1,3,7,9} \sum_{k=0}^{\infty} \frac{1}{(10k+\ell)^s}.$$

and

$$L_1(s) = \prod_p \big(1 - \chi_1(p)p^{-s}\big)^{-1} = \sum_{\ell=1,7} \sum_{k=0}^{\infty} \Big(\frac{(-1)^{(l-1)/2}}{(10k+\ell)^s} - \frac{(-1)^{(l-1)/2}}{(10k+\ell+2)^s} \Big).$$

For anyone with a course on calculus it should be clear that $L_0(s) \to \infty$ as $s \to 1^+$ and for anyone with a course on calculus and a computer it should be clear that $L_1(s)$ converge to around 0.6456 as $s \to 1^+$. As a step forward, let us use this information to settle the existence of infinitely many primes having a last digit in $\{3, 7\}$ and the same for a last digit in $\{1, 9\}$.

Imagine that there are only finitely many primes $p \equiv 3, 7$ (10) then $\chi_0(p) = \chi_1(p)$ almost all the time and we would have

$$L_0(s) \approx L_1(s) \qquad \text{for} \quad s > 1$$

where the symbol $\approx$ means that the quotient of both sides is between two positive constants. This contradicts our study of the convergence when $s \to 1^+$. So, there are infinitely many primes with last digit 3 or 7 (this can also be proved with an Euclid like elementary argument).

On the other hand, if there are only finitely many primes $p \equiv 1, 9$ (10) then $\chi_1(p) = -\chi_0(p)$ almost all the time and we would have

$$L_0(s)L_1(s) \approx \prod_p \big(1 - \chi_0^2(p)p^{-2s}\big)^{-1} \approx 1 \qquad \text{for} \quad s > 1.$$

Again it contradict our results for $s \to 1^+$, then there are also infinitely many primes with last digit 1 or 9.

If you are struggling against the last ≈ 1, the only thing you should worry about is that $\prod_{k=2}^{\infty} \big(1 + C/k^2\big)$ converges to a nonzero constant for any $|C| < 4$. In general, if $|f(p)|, |g(p)| \leq 1$ we have for $s > 1$

$$\prod_p \big(1 - f(p)p^{-2s}\big)^{-1} \big(1 - g(p)p^{-2s}\big)^{-1} \approx \prod_p \Big(1 - \frac{1}{2}\big(f(p) + g(p)\big)p^{-2s}\Big)^{-2} \tag{2.2}$$

because the quotient of both sides can be bounded between products of the form $\prod_{k=k_0}^{\infty}\big(1+C/k^2\big)$. In few words, *quadratic or higher order terms do no affect the convergence*. If this is still not clear to you, a good exercise is to work out the details.

Let us rephrase this latter argument. Define $f_{1,9}(p)=\frac{1}{2}\big(\chi_0(p)+\chi_1(p)\big)$ which takes the value 1 if $p\equiv 1,9$ and is zero otherwise. Applying (2.2) with $f=\chi_0$, $g=\chi_1$,

$$\prod_p \big(1-f_{1,9}(p)p^{-s}\big)^{-2}\approx L_0(s)L_1(s) \tag{2.3}$$

and letting $s\to 1^+$ we obtain again the infinitude of primes finishing in 1 or 9.

3 The punchline

How can we separate 1 and 9? Let $f_{1,9}^-$ be like $f_{1,9}$ except for $f_{1,9}^-(n)=-1$ when $n\equiv 9\ (10)$. If we can prove something similar to (2.3) for this function i.e.,

$$\prod_p \big(1-f_{1,9}^-(p)p^{-s}\big)^{-2}\approx L_2(s)L_3(s)$$

with some simple $L_2(s)$ and $L_3(s)$, then the relation

$$\prod_{p\equiv 1\ (10)} \big(1-p^{-s}\big)^{-4}\approx L_0(s)L_1(s)L_2(s)L_3(s), \tag{3.1}$$

coming from (2.2) with $f=f_{1,9}$ and $g=f_{1,9}^-$, may do the job if the convergence of $L_2(s)L_3(s)$ can be decided as $s\to 1^+$.

Let us try to mimic the previous structure assuming $f_{1,9}^-(p)=\frac{1}{2}\big(\chi_2(p)+\chi_3(p)\big)$ where $\chi_2(n)$ and $\chi_3(n)$ satisfy the multiplicative property and take both the value 1 if $n\equiv 1\ (10)$ and -1 if $n\equiv 9\ (10)$. In other words, we want

$$\frac{1}{4}\big(\chi_0(n)+\chi_1(n)+\chi_2(n)+\chi_3(n)\big)$$

to be a detector of the arithmetic progression $n\equiv 1\ (10)$ assigning 1 to its elements and 0 to the rest of the integers.

We have to complete the table

	$n\equiv 1$	$n\equiv 3$	$n\equiv 7$	$n\equiv 9$	otherwise
χ_2	1	♣	♢	-1	0
χ_3	1	♠	♡	-1	0

The multiplicative property implies $\clubsuit^2=\spadesuit^2=-1$ and $\clubsuit\diamondsuit=\spadesuit\heartsuit=1$, because $3^2\equiv 9$ and $3\cdot 7\equiv 1$ modulo 10. Hence, except for swapping the

names of χ_2 and χ_3 the only solution is

	$n\equiv 1$	$n\equiv 3$	$n\equiv 7$	$n\equiv 9$	otherwise
χ_2	1	i	$-i$	-1	0
χ_3	1	$-i$	i	-1	0

The corresponding functions are conjugate, consequently $L_2(s)L_3(s) = \big|L_2(s)\big|^2$ which is

$$\Big(\sum_{k=0}^{\infty}\Big(\frac{1}{(10k+1)^s}-\frac{1}{(10k+9)^s}\Big)\Big)^2+\Big(\sum_{k=0}^{\infty}\Big(\frac{1}{(10k+3)^s}-\frac{1}{(10k+7)^s}\Big)\Big)^2.$$

Then $L_2(s)L_3(s)$ converges to a positive constant (namely $0.9869\ldots$) as $s\to 1^+$.

Summing up, the right hand side in (3.1) tends to ∞ when $s\to 1^+$, because $L_0(s)$ does, and it is deduced that there are infinitely many primes satisfying $p\equiv 1\ (10)$. In fact the sequence of these primes cannot grow very fast because otherwise the infinite product would converge.

4 Extending the trick to a method

What about the primes having 9 as last digit or, for instance, finishing in 2023? Dirichlet proved that if a and q are coprimes, there are always infinitely many primes p satisfying $p\equiv a\ (q)$. Of course, if a and q are not coprimes there are finitely many of them.

The purpose of this section is to illustrate how to get Dirichlet's result enhancing the arguments employed in the previous sections.

We know that the group of units $(\mathbb{Z}/q\mathbb{Z})^*$ is a multiplicative group of order $\varphi(q)$ where φ is Euler's totient function i.e., $\varphi(q)=\#\{1\le n\le q\,:\,\gcd(n,q)=1\}$. An important concept in group theory is that of the *characters* associated to a group. In our simple abelian situation they are just homomorphisms to the group of $\varphi(q)$-roots of the unity

$$\chi\,:\,(\mathbb{Z}/q\mathbb{Z})^*\longrightarrow\mathcal{U}\qquad\text{with}\quad\mathcal{U}=\big\langle e^{2\pi i/\varphi(q)}\big\rangle.$$

If we extend the definition to $\mathbb{Z}$ identifying each integer with its congruence class and putting $\chi(n)=0$ if $\gcd(n,q)\neq 1$ we say that the resulting $\mathbb{Z}$-defined functions are the *Dirichlet characters* of modulus q (although, strictly speaking, they are not character in the group theory sense). By construction, they have the multiplicative property $\chi(mn)=\chi(m)\chi(n)$ and (2.1) assures

$$L(s,\chi)=\prod_p\big(1-\chi(p)p^{-s}\big)^{-1}\qquad\text{where}\quad L(s,\chi):=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

Any $n \equiv 1\ (q)$ corresponds to the identity element in $(\mathbb{Z}/q\mathbb{Z})^*$ and hence $\chi(n) = 1$. Conversely, it can be proved [5, p. 254] that if $n \not\equiv 1\ (q)$ there exists a Dirichlet character χ with $\chi(n) \neq 1$. It has as a remarkable consequence the existence of the following detector of the arithmetic progression $n \equiv a\ (q)$ with a and q coprime:

$$\sum_{\chi} \overline{\chi}(a)\chi(n) = \begin{cases} \varphi(q) & \text{if } n \equiv a\ (q), \\ 0 & \text{if } n \not\equiv a\ (q). \end{cases} \tag{4.1}$$

Here the sum is over all Dirichlet characters of modulus q and $\overline{\chi}(a)$ means the complex conjugate of $\chi(a)$. This formula is part of the so called *orthogonality relations* by obvious reasons. Choosing $a = n = 1$ we obtain that there are $\varphi(q)$ Dirichlet characters.

The tables in the previous sections give explicitly the four Dirichlet characters for $q = 10$. Our previous detector of $n \equiv 1\ (10)$ is (4.1) divided by $\varphi(10) = 4$ with $\overline{\chi}(a) = \overline{\chi}(1) = 1$. The advantage here is that the existence of the detector follows from the theory and it does not require any explicit construction.

To prove (4.1), note that as $\chi(n)$ is a root of the unity, $\overline{\chi}(a)\chi(a) = 1$ and it implies, thanks to the multiplicative property, $\overline{\chi}(a)\chi(n) = \chi(a^*)\chi(n) = \chi(a^*n)$ where $a^*a \equiv 1\ (q)$. Hence, renaming n, it is enough to consider the case $a = 1$ in which $\overline{\chi}(a) = 1$. If $n \not\equiv 1\ (q)$ take a Dirichlet character ψ with $\psi(n) \neq 1$. Then

$$\psi(n) \sum_{\chi} \chi(n) = \sum_{\chi} (\psi\chi)(n) = \sum_{\chi} \chi(n).$$

The second equality is deduced because the Dirichlet characters form a group. Since $\psi(n) \neq 1$, the sum is zero. If $n \equiv 1\ (q)$ the sum is clearly the number of characters and this case of the formula follows from a general result in group theory assuring that there is a (not canonical) isomorphism between any abelian group and its group of characters, so both have the same order.

Now, our arithmetic progression detector (4.1) can be employed to obtain

$$\prod_{\chi} L(s,\chi)^{\overline{\chi}(a)} \approx \prod_{\chi} \Big(1 - \frac{p^{-s}}{\varphi(q)} \sum_{\chi} \overline{\chi}(a)\chi(p)\Big)^{-\varphi(q)} \approx \prod_{p \equiv a\ (q)} \big(1 - p^{-s}\big)^{-\varphi(q)}. \tag{4.2}$$

Here $\overline{\chi}(a)$ are in general complex exponents and we can doubt how to decide about the multiple choices of the argument and if this affects the meaning of $\approx$. The really relevant point is to assure the Taylor approximation

$$\big(1 - \chi(p)p^{-s}\big)^{\overline{\chi}(a)} = 1 - \overline{\chi}(a)\chi(p)p^{-s} + \dots$$

where the dots are higher order terms in p^{-s}. If χ is a character, $\overline{\chi}$ is a character too, hence the left hand side in (4.2) is actually real and $\approx$ can

keep its original meaning. The Dirichlet character corresponding to the trivial constant homomorphism $\chi = 1$ is called the *principal character* and it is denoted by χ_0. Clearly,

$$L(s, \chi_0) = \sum_{\substack{n=1 \\ \gcd(n,q)=1}}^{\infty} \frac{1}{n^s} \to \infty \qquad \text{when} \quad s \to 1^+.$$

It can be proved that for $\chi \neq \chi_0$, $L(s, \chi)$ has a finite nonzero limit c_χ when $s \to 1^+$, actually $L(1, \chi) = c_\chi$. Then taking $s \to 1^+$ in (4.2) we conclude that there are infinitely many primes in the arithmetic progression $n \equiv a\ (q)$.

Proving that c_χ is finite and well defined is not very hard. It follows via Dirichlet's test for the convergence of series [1, §22] using another instance of the orthogonality relations giving this dual version of (4.1):

$$\sum_{n=1}^{q} \chi(n) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

It was much harder for Dirichlet to get a proof of $c_\chi \neq 0$. For each q fixed we could construct explicitly the Dirichlet characters and check with the help of a computer $L(1, \chi) \neq 0$. The question is how to do it in general. Dirichlet employed a highly nontrivial connection with Gauss theory of binary quadratic forms. Nowadays we know a more elementary tricky approach. After some reductions one can focus on real characters. The underlying idea to treat them is that $c_\chi = 0$ would force a cancellation of the infinity in $\zeta(s)L(s, \chi)$ when $s \to 1^+$ but this contradicts, with some extra arguments, that this product is $\sum_{n=1}^{\infty} a_n/n^s$ with $a_n \geq 0$ and $a_n = 1$ many times. The complete modern argument reflecting this outline is in [8, §4.3].

Where can I learn more? If you are now very interested in analytic number theory, one of the modern classics is [4]. It is concise and you will probably have to read more than twice some lines. It deserves the effort. The first chapter already obtains Dirichlet result for primes in arithmetic progressions with prime difference appealing to some classic results coming back to Gauss.

If conciseness is your second name and you want to have all the details anyway, you will love the book [10]. His author devoted a big part of his mathematical life to get simple proofs of not so simple mathematical results. He got a lot of credit by a simple proof of the prime number theorem included in this booklet with some other results.

If your method is to learn by doing, [9] contains an interesting selection of problems with solutions preceded by excerpts of the theory.

To be fair, [4] has two related drawbacks, it is a little bit outdated and does not offer a complete overview of the subject. A good modern book in analytic number theory is [6]. The treatment of some topics is highly original and it contains helpful explanations of the underlying ideas. It is not a book for absolute beginners though.

Another noticeable book is [3]. It is the part corresponding to "analytic and modern tools" of a two volume treatise on number theory.

In principle, [8] should be the first volume of a longer work but after many years it seems that the project does not evolve. It is devoted only to a part of analytic number theory. The clear and complete explanations will be praised by the beginners.

The relation between some specific topics of number theory and analysis is explored in [7]. Although strictly speaking it is not a general book on analytic number theory, it is an interesting reading for anyone interested in the subject, no doubt.

If you are reading this note surely written with some English grammar flaws, perhaps you will appreciate some valuable references in Spanish. To my knowledge there are very few. I only mention [2] even knowing that it is very difficult to find beyond local libraries.

References

[1] T. J. I. Bromwich. An introduction to the theory of infinite series. 2nd ed., revised with the assistance of T. M. MacRobert. London-New York: Macmillan, 1926.

[2] J. Cilleruelo and A. Córdoba. *La teoría de los números*. Biblioteca Mondadori. Mondadori España, Madrid, 1992.

[3] H. Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[4] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1980. Revised by H. L. Montgomery.

[5] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[6] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[7] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994.

[8] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[9] M. R. Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

[10] D. J. Newman. *Analytic number theory*, volume 177 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.