

## Math 259: Introduction to Analytic Number Theory

### Elementary approaches II: the Euler product

Euler [Euler 1737] achieved the first major advance beyond Euclid's proof by combining his method of generating functions with another highlight of ancient Greek number theory, unique factorization into primes.

**Theorem** [Euler product]. *The identity*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}. \quad (1)$$

holds for all  $s$  such that the left-hand side converges absolutely.

*Proof:* Here and henceforth we adopt the convention:

The notation  $\prod_p$  or  $\sum_p$  means a product or sum over prime  $p$ .

Every positive integer  $n$  may be written uniquely as  $\prod_p p^{c_p}$ , with each  $c_p$  a nonnegative integer that vanishes for all but finitely many  $p$ . Thus the formal expansion of the infinite product

$$\prod_{p \text{ prime}} \left( \sum_{c_p=0}^{\infty} p^{-c_p s} \right) \quad (2)$$

contains each term

$$n^{-s} = \left( \prod_p p^{c_p} \right)^{-s} = \prod_p p^{-c_p s}$$

exactly once. If the sum of the  $n^{-s}$  converges absolutely, we may rearrange the sum arbitrarily and conclude that it equals the product (2). On the other hand, each factor in this product is a geometric series whose sum equals  $1/(1 - p^{-s})$ . This establishes the identity (2).  $\square$

The sum on the left-hand side of (1) is nowadays called the *zeta function*

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{n=1}^{\infty} n^{-s};$$

the formula (2) is called the *Euler product* for  $\zeta(s)$ . Euler did not actually impose the convergence condition: the rigorous treatment of limits and convergence was not yet available, and Euler either handled such issues intuitively or ignored them. If  $s$  is a real number — the only case that concerned Euler — then it is well known that  $\sum_{n=1}^{\infty} n^{-s}$  converges if and only if  $s > 1$ , by comparison with  $\int_1^{\infty} x^{-s} dx$  (that is, by the “Integral Test” of elementary calculus). We shall use

complex  $s$  as well, but the criterion for absolute convergence is still easy: if  $s$  has real part  $\sigma$  then

$$|n^{-s}| = |\exp(-s \log n)| = \exp(\operatorname{Re}(-s \log n)) = \exp(-\sigma \log n) = n^{-\sigma},$$

so the Euler product holds in the half-plane  $\sigma > 1$ .

Euler's next step was to set  $s = 1$  in (2). This equates  $\prod_p 1/(1 - p^{-1})$  with the sum  $\sum_{n=1}^{\infty} 1/n$  of the harmonic series. Since the sum diverges to  $+\infty$ , whereas each factor  $\prod_p 1/(1 - p^{-1})$  is finite, there are infinitely many factors. Therefore, there are infinitely many primes. This proof does not meet modern standards of rigor, but it is easy enough to fix: instead of setting  $s$  equal 1, let  $s$  approach 1 from above. The next result is an easy estimate on the behavior of  $\zeta(s)$  for  $s$  near 1.

**Lemma.** *The inequalities*

$$\frac{1}{s-1} < \zeta(s) < \frac{1}{s-1} + 1 \tag{3}$$

hold for all  $s > 1$ .

(More accurate estimates are available using the Euler-Maclaurin formula, but we do not yet need them.)

*Proof:* For all  $n > 0$  we have

$$\int_n^{n+1} x^{-s} dx = \frac{1}{s-1} (n^{1-s} - (n+1)^{1-s}),$$

whence

$$(n+1)^{-s} < \frac{n^{1-s} - (n+1)^{1-s}}{s-1} < n^{-s}.$$

Now sum over  $n = 1, 2, 3, \dots$ . The sum of  $(n^{1-s} - (n+1)^{1-s})/(s-1)$  telescopes to  $1/(s-1)$ . This sum is bounded above by  $\sum_{n=1}^{\infty} n^{-s} = \zeta(s)$ , and below by  $\sum_{n=1}^{\infty} (n+1)^{-s} = \zeta(s) - 1$ . This proves the inequalities (3).  $\square$

The lower bound in (3) shows that  $\zeta(s) \rightarrow \infty$  as  $s \rightarrow 1$  from above. Since each factor  $(1 - p^{-s})^{-1}$  in the Euler product remains bounded, we have vindicated Euler's argument for the infinitude of primes.

The divergence of  $\prod_p p/(p-1)$  and the behavior of  $\prod_p 1/(1 - p^{-s})$  as  $s \rightarrow 1+$  give us much more specific information on the distribution of primes than we could hope to extract from Euclid's argument. For instance, we cannot have constants  $C, \theta$  with  $\theta < 1$  such that  $\pi(x) < Cx^\theta$  for all  $x$ , because then the Euler product would converge for  $s > \theta$ . To go further along these lines it is convenient to use the logarithm of the Euler product:

$$\log \zeta(s) = \sum_p -\log(1 - p^{-s}). \tag{4}$$

Euler again took  $s = 1$  and concluded that  $\sum_p 1/p$  diverges. Again we justify his conclusion by letting  $s$  approach 1 from above:

**Theorem.** *For any  $s_0 > 1$  there exists  $M$  such that*

$$\left| \sum_p p^{-s} - \log \frac{1}{s-1} \right| < M \quad (5)$$

for all  $s \in (1, s_0]$ . In particular,  $\sum_p 1/p$  diverges.

*Proof:* By our Lemma,  $\log \zeta(s)$  is between  $\log 1/(s-1)$  and  $\log s/(s-1)$ . Since  $0 < \log s < s-1$ , we conclude that  $\log \zeta(s)$  differs from  $\log 1/(s-1)$  by less than  $s-1 < s_0-1$ . In the right-hand side of (4), we approximate each summand  $-\log(1-p^{-s})$  by  $p^{-s}$ . The error is at most  $p^{-2s}$ , so

$$\left| \sum_p p^{-s} - \sum_p (-\log(1-p^{-s})) \right| < \sum_p p^{-2s} < \zeta(2).$$

Hence (5) holds with  $M = s_0 - 1 + \zeta(2)$ . Letting  $s \rightarrow 1$  we obtain the divergence of  $\sum_p 1/p$ .  $\square$

**Interlude on the “Big Oh” notation  $O(\cdot)$ .** The point of (5) is that  $\sum_p p^{-s}$  equals  $\log \frac{1}{s-1}$  within a bounded error, not the specific upper bound  $M$  on this error — which is why we were content with a bound  $s_0 - 1 + \zeta(2)$  weaker than what the method can give. Usually in such approximate formulas we shall be interested only in the existence of constants such as  $M$ , not in their exact values. To avoid distractions such as “ $s_0 - 1 + \zeta(2)$ ”, we henceforth use “big Oh” notation. In this notation, (5) appears as

$$\sum_p p^{-s} = \log \frac{1}{s-1} + O(1). \quad (6)$$

In general,  $f = O(g)$  means that  $f, g$  are functions on some space  $S$  with  $g$  nonnegative, and there exists a constant  $M$  such that  $|f(z)| \leq Mg(z)$  for all  $z \in S$ . In particular,  $O(1)$  is a bounded function, so (6) is indeed the same as (5). An equivalent notation, more convenient in some circumstances, is  $f \ll g$  (or  $g \gg f$ ). For instance, a linear map  $T$  between Banach spaces is continuous iff  $Tv = O(|v|)$  iff  $|v| \gg |Tv|$ . Each instance of  $O(\cdot)$  or  $\ll$  or  $\gg$  is presumed to carry its own implicit constant  $M$ . If the constant depends on some parameter(s), we may use the parameter(s) as a subscript to the “ $O$ ” or “ $\ll$ ”. For instance, we may write  $O_{s_0}(1)$  instead of  $O(1)$  in (6); for any  $\epsilon > 0$ , we have  $\log x \ll_\epsilon x^\epsilon$  on  $x \in [1, \infty)$ . For basic properties of  $O(\cdot)$  and  $\ll$  see the Exercises at the end of this section.

**Back to  $\pi(x)$ .** The estimate (6) for  $\sum_p p^{-s}$  does not explicitly involve  $\pi(x)$ . We thus rearrange this sum as follows. Write  $p^{-s}$  as an integral  $s \int_p^\infty y^{-1-s} dy$ , and sum over  $p$ . Then  $y$  occurs in the interval of integration  $[p, \infty)$  iff  $p < y$ , that is, with multiplicity  $\pi(y)$ . Therefore

$$\sum_p p^{-s} = s \int_1^\infty \pi(y) y^{-1-s} dy, \quad (7)$$

and (6) becomes an estimate for an integral involving  $\pi(\cdot)$ .

This transformation from the sum in (6) to the integral (7) is an example of a method we shall use often, known either as partial summation or integration by parts. To explain the latter name, consider that the sum may be regarded as the Stieltjes integral  $\int_1^\infty y^{-s} d\pi(y)$ , which integrated by parts yields (7); that is how we shall write this transformation from now on.

Our eventual aim is the Prime Number Theorem (PNT), which asserts that  $\pi(x)$  is asymptotic to  $x/\log x$  as  $x \rightarrow \infty$ . Our estimate (6) on the integral (7) does not suffice to prove the PNT, but does provide support for it: the estimate holds if we replace  $\pi(x)$  with  $x/\log x$ . That is,<sup>1</sup>

$$\int_2^\infty \frac{y^{-s}}{\log y} dy = \log \frac{1}{s-1} + O(1) \quad (1 < s \leq 2).$$

To prove this, let  $I(s) = \int_2^\infty \frac{y^{-s}}{\log y} dy$ , and differentiate under the integral sign to obtain  $I'(s) = -\int_2^\infty y^{-s} dy = 2^{1-s}/(1-s) = 1/(1-s) + O(1)$ . Thus for  $1 < s \leq 2$  we have

$$I(s) = I(2) - \int_s^2 I'(\sigma) d\sigma = + \int_s^2 \frac{d\sigma}{\sigma-1} + O(1) = \log \frac{1}{s-1} + O(1)$$

as claimed. While this does not prove the Prime Number Theorem, it does show that, for instance, if  $c < 1 < C$  then there are arbitrarily large  $x, x'$  such that  $\pi(x) > cx/\log x$  and  $\pi(x') < Cx'/\log x'$ .

### Remarks

Euler's result  $\sum_p 1/p = \infty$  underlies for our expectation that  $p_{n+1}$  divides  $1 + \prod_{i=1}^n p_i$  infinitely often. The residue of  $\prod_{i=1}^n p_i \bmod p_{n+1}$  should behave like a random element of  $(\mathbf{Z}/p_{n+1}\mathbf{Z})^*$ , and thus should equal  $-1$  with probability  $1/(p-1)$ . The expected value of the number of  $n < N$  such that  $p_{n+1}$  divides  $1 + \prod_{i=1}^n p_i$  is thus  $\sum_{n=2}^N 1/(p-1) > \sum_{n=2}^N 1/p \rightarrow \infty$  as  $N \rightarrow \infty$ . We expect the same behavior for many other problems of the form "how many primes  $p$  are factors of  $f(p)$ ?", notably  $f(p) = ((p-1)! + 1)/p$  (the Wilson quotient),  $f(p) = (a^p - a)/p$  (the Fermat quotient with fixed base  $a > 1$ ), and  $f(p) = p^{-2} \sum_{i=1}^{p-1} 1/i$  (the Wolstenholme quotient). We shall soon see that  $\sum_p 1/p$  diverges very slowly:  $\sum_{p < x} 1/p = \log \log x + O(1)$ . Therefore, while we expect infinitely many solutions of  $p|f(p)$  in each case, we expect that these solutions will be very scarce.

Euler's work on the zeta function includes also its evaluation at positive integers:  $\zeta(2) = \pi^2/6$ ,  $\zeta(4) = \pi^4/90$ , "etc." The silliest proof I know of the infinitude

<sup>1</sup>We shift the lower limit of integration to  $y = 2$  to avoid the spurious singularity of  $1/\log y$  at  $y = 1$ , and suppress the factor  $s$  because only the behavior as  $s \rightarrow 1$  matters, and multiplying by  $s$  does not affect it to within  $O(1)$ . We also made the traditional and convenient choice  $s_0 = 2$ ; the value of  $s_0$  does not matter, as long as  $s_0 > 1$ , because we are concerned with the behavior near  $s = 1$ , and by specifying  $s_0$  we can dispense with a distracting subscript in  $O_{s_0}$ .

of primes is to fix one such integer  $s$ , and observe that if there were finitely many primes then  $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ , and thus also  $\pi^s$ , would be rational, contradicting Lindemann's theorem (1882) that  $\pi$  is transcendental. It is only a bit less silly to take  $s = 2$  and use the irrationality of  $\pi^2$ , which though unknown to Euler was proved a few generations later by Legendre (1794?). This can actually be used to obtain lower bounds on  $\pi(x)$ , but even with modern "irrationality measures" we can obtain no lower bounds on  $\pi(x)$  better than the  $\log \log x$  bound already available from Euclid's proof.

Less frivolously, we note that the integral  $\int_1^\infty \pi(y)y^{-s} dy/y$  appearing in (7) is the *Mellin transform* of  $\pi(y)$ , evaluated at  $-s$ . The Mellin transform may not be as familiar as the integral transforms of Fourier and Laplace, but the change of variable  $y = e^u$  yields

$$\int_1^\infty \pi(y)y^{-s} \frac{dy}{y} = \int_0^\infty \pi(e^u)e^{-su} du,$$

which is the Laplace transform of  $\pi(e^u)$ , evaluated at  $s$ . In general, if  $f(u)$  is a nonnegative function whose Laplace transform  $\mathcal{L}f(s) := \int_0^\infty f(u)e^{-su} du$  converges for  $s > s_0$ , then the behavior of  $\mathcal{L}f(s)$  as  $s \rightarrow s_0+$  detects the behavior of  $f(u)$  as  $u \rightarrow \infty$ . In our case,  $s_0 = 1$ , so we expect that our estimate on  $\int_1^\infty \pi(y)y^{-s} dy/y$  for  $s$  near 1 will give us information on the behavior of  $\pi(x)$  for large  $x$ . Moreover, inverting the Laplace transform requires a contour integral over complex  $s$ ; this suggests that we shall need to consider  $\log \zeta(s)$ , and thus the solutions of  $\zeta(s) = 0$ , in the complex plane. We shall return to these ideas and the Mellin transform before long.

### Exercises

Concerning the Big Oh (equivalently " $\ll$ ") notation:

1. If  $f \ll g$  and  $g \ll h$  then  $f \ll h$ . If  $f_1 = O(g_1)$  and  $f_2 = O(g_2)$  then  $f_1 f_2 = O(g_1 g_2)$  and  $f_1 + f_2 = O(g_1 + g_2) = O(\max(g_1, g_2))$ . Given a positive function  $g$ , the functions  $f$  such that  $f = O(g)$  constitute a vector space.
2. If  $f \ll g$  on the interval  $(a, b)$  or  $(a, b]$  then  $\int_a^x f(y) dy \ll \int_a^x g(y) dy$  for all  $x$  in the same interval such that the integrals exist. (We already used this to obtain  $I(s) = \log(1/(s-1)) + O(1)$  from  $I'(s) = 1/(1-s) + O(1)$ .) In general differentiation does not commute with " $\ll$ " (why?). Nevertheless, prove that  $\zeta'(s) [= -\sum_{n=1}^\infty n^{-s} \log n]$  is  $-1/(s-1)^2 + O(1)$  on  $s \in (1, \infty)$ .
3. So far all the implicit constants in the  $O(\cdot)$  or  $\ll$  we have seen are *effective*: we didn't bother to specify them, but we could if we really had to. Moreover the transformations in exercises 1,2 preserve effectivity: if the input constants are effective then so are the output ones. However, it can happen that we know that  $f = O(g)$  without being able to name a constant  $M$  such that  $|f| \leq Mg$ . Here is a prototypical example. Suppose  $x_1, x_2, x_3, \dots$  is a sequence of positive reals which we suspect are all  $\leq 1$ , but all we can show is that if  $i \neq j$  then  $x_i x_j < x_i + x_j$ . Prove that the  $x_i$  are bounded, i.e.,  $x_i = O(1)$ , but that as long as we do not find some  $x_i$  greater than 1, we cannot use this to exhibit a

specific  $M$  such that  $x_i < M$  for all  $i$  — and indeed if our suspicion that every  $x_i \leq 1$  is correct then we shall never be able to find  $M$ .

We shall encounter this sort of unpleasant ineffectivity (where it takes at least two outliers to get a contradiction) in Siegel’s lower bound on  $L(1, \chi)$ ; it arises elsewhere too, notably in Faltings’ proof of the Mordell conjecture, where the number of rational points on a given curve of genus  $> 1$  can be effectively bounded but their size cannot.

Applications of the Euler product for  $\zeta(s)$ :

4. Complete the proof that for each  $c < 1$  there are arbitrarily large  $x$  such that  $\pi(x) > cx/\log x$  and for each  $C > 1$  there are arbitrarily large  $x'$  such that  $\pi(x') < Cx'/\log x'$ .

5. It is known that there exists a constant  $M$  such that  $|\pi^2 - a/b| \gg 1/b^M$  for all positive integers  $a, b$ . Use this together with the Euler product for  $\zeta(2)$  to prove that  $\pi(x) \gg \log \log x$ .

6. Prove that there are  $N/\zeta(2) + O(N^{1/2})$  squarefree integers in  $[1, N]$ . Obtain similar estimates for the number of natural numbers  $< N$  not divisible by  $n^s$  for any  $n > 1$  ( $s = 3, 4, 5, \dots$ ). NB this and the next few exercises are not quite as easy as they may seem: remember the final exercise for the previous lecture! A hint as to the solution: use the Euler product for  $\zeta(s)$  to obtain a series expansion for  $1/\zeta(s)$ .

It follows that an integer chosen uniformly at random from  $[1, N]$  is squarefree with probability approaching  $1/\zeta(2) = 6/\pi^2$  as  $N \rightarrow \infty$ . Informally, “a random integer is squarefree with probability  $6/\pi^2$ ”. We shall see that the error estimate  $O(N^{1/2})$  can be improved, and that the asymptotic growth of the error hinges on the Riemann Hypothesis.

7. Prove that there are  $N^2/\zeta(2) + O(N \log N)$  ordered pairs of relatively prime integers in  $[1, N]$ . What of relatively prime pairs  $(x_1, x_2)$  with  $x_1 < N_1$  and  $x_2 < N_2$ ? Generalize.

Again we may informally deduce that two random integers are coprime with probability  $6/\pi^2$ . Alternatively, we may regard a coprime pair  $(x_1, x_2)$  with  $x_i \leq N$  as a positive rational number  $x_1/x_2$  of height at most  $N$ . Dropping the positivity requirement, we find that there are asymptotically  $2N^2/\zeta(2)$  rational numbers of height at most  $N$ . This has been generalized to number fields other than  $\mathbf{Q}$  by Schanuel [1979]; a function-field analogue, concerning rational functions of bounded degree on a given algebraic curve over a finite field, was announced by Serre [1989, p.19] and proved by DiPippo [1990] and Wan [1992] (independently but in the same way). The function-field result was the starting point of our estimate on the size of the nonlinear codes obtained from rational functions on modular curves [Elkies 2001]. Schanuel also obtained asymptotics for rational points of height at most  $N$  in projective space of dimension  $s - 1$  over a number field  $K$ ; when  $K = \mathbf{Q}$  this recovers the asymptotic enumeration of coprime  $s$ -tuples of integers.

8. Prove that as  $N \rightarrow \infty$  the number of ordered quadruples  $(a, b, c, d)$  of integers in  $[1, N]$  such that  $\gcd(a, b) = \gcd(c, d)$  is asymptotic to  $2N^4/5$ .

Can this be proved without invoking the values of  $\zeta(2)$  or  $\zeta(4)$ ? This can be regarded as a form of a question attributed to Wagstaff in [Guy 1981, B48]: “Wagstaff asked for an elementary proof (e.g., without using properties of the Riemann zeta-function) that  $\prod_p (p^2 + 1)/(p^2 - 1) = 5/2$ .”

## References

- [DiPippo 1990] DiPippo, S.A.: *Spaces of Rational Functions on Curves Over Finite Fields*. Ph.D. Thesis, Harvard, 1990.
- [Elkies 2001] Elkies, N.D.: Excellent nonlinear codes from modular curves, pages 200–208 in *STOC'01: Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, Hersonissos, Crete, Greece*. Isomorphic with [math.NT/0104115](https://arxiv.org/abs/math/0104115) at [arXiv.org](https://arxiv.org).
- [Euler 1737] Euler, L.: *Variae observationes circa series infinitas*, *Commentarii academiae scientiarum Petropolitanae* **9** (1744), 160–188 (presented to the St. Petersburg Academy in 1737) = *Opera Omnia Ser. 1* **14**, 217–244.
- [Guy 1981] Guy, R.K.: *Unsolved Problems in Number Theory*. Springer, 1981.
- [Legendre 1794] Legendre, A.-M.: *Éléments de Géométrie*. Paris: Didot, 1794.
- [Schanuel 1979] Schanuel, S.H.: Heights in number fields. *Bull. Soc. Math. France* **107**, 433–449 (1979).
- [Serre 1989] Serre, J.-P.: *Lectures on the Mordell-Weil Theorem* (trans. M. Brown). F. Vieweg & Sohn, Braunschweig 1989.
- [Wan 1992] Wan, D.: Heights and Zeta Functions in Function Fields. In *The Arithmetic of Function Fields*, pages 455–463. Berlin: W. de Gruyter, 1992.