8. Del

Primes in arithmetic progressions

Version $-\infty$ — last update: 11/28/14 2:49:53 PM
Preliminar verison prone to errors and subjected to changes.
The version number says all!

Euler gave a proof of there being infinitely many primes build on the ζ-function and the Euler product. Compared to Euclid's short and elegant argument this seems to be a long and complicated detour to this fact, but it has the virtue of being the starting point for other important theorems, like Dirichlet's theorem on primes in arithmetic progressions. Sometimes one stumbles upon gold when making a detour!

To begin with, we state the simplest form of Dirichlet's theorem, and we shall soon come back with a more refined version. The term "arithmetic progression" is slightly old-fashioned, and in modern language it just means a congruence class:

Theorem 8.1 *Given two relatively prime natural numbers a and m. Then there are infinitely many primes p that are congruent to a mod m.*

EXAMPLE 8.1. — EUCLIDEAN PROOFS. In a few cases there are elementary proofs of Dirichlet's theorem. They all mimicking Euclid's proof of there being infinitely many primes (which is Dirichlet's theorem for $a = 1$ and $m = 2$ by the way) and they are therefore called Euclidean proofs (this notion can be made precise).

As an illustration let us do the case $a = 3$ and $m = 4$; that is, we are looking for primes congruent to -1 modulo 4. Assume there is only finitely many such primes, say $p_1, \ldots, p_r$, and let N denote their product, *i.e.*, $N = p_1 \cdot \cdots \cdot p_r$. Assume first that r is even, and in the spirit of Euclid, consider $N + 2$. One has $N + 2 \equiv 1 \mod -1$. Now, any prime q diving $N + 2$ can not be one of the p_i's, and it is certainly not equal to two, hence $q \equiv 1 \mod 4$. It follows that $N + 2 \equiv 1 \mod 4$; which is a contradiction. If r is odd, a similar same reasoning but with $N + 4$ gives a contradiction.

The pairs for which there is an Euclidean proof have classified by I. Schur and R.

M. Murty, see [7] or [8] for good accounts of the story. The result is that there is a Euclidean proof if and only if $a^2 \equiv 1 \mod m$ ❄

PROBLEM 8.1. Prove Dirichlet's theorem à la Euclid for the pairs $a = 2$ and $m = 3$, and $a = 5$ and $m = 6$. ✸

It is an appropriate question to ask if the primes are equally distributed among the residue classes mod m, or if some classes are more populated by primes than others. The answer is not completely clear. First of all, we are speaking about infinite sets, so to compare numbers is difficult. One has to talk about some sort of densities or average distribution in the large. Just like with the primes, it is natural to study the function

$$\pi(x, a, m) = \sum_{p \equiv a(m), p \leq x} 1 = \#\{\, p \mid p \leq x \text{ and } p \equiv a \mod m \,\},$$

and for this function ones has

Proposition 8.1 $\pi(x, a, m) \sim \pi(x)/\phi(x) \sim x/\phi(x) \log x$.

This may be interpreted as the primes being equally distributed in the $\phi(m)$ residue classes, at least asymptotically. However there is a phenomenon called the "Chebychev bias". It seems that in several cases some classes are preferred over others, but of course, in the limit the differences disappear. For example, the inequality $\pi(x, 3, 4) \geq \pi(x, 1, 4)$ occurs more frequently than $\pi(x, 1, 4) \geq \pi(x, 3, 4)$; indeed, the former holds true for primes up to 26833. And for a certain density measure, the set of x such that $\pi(x, 3, 4) > \pi(x, 1, 4)$ has a density close to one: $0.996\ldots$.

Eulers complicated proof

We recall Euler's detour. The point of departure is his product formula

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1},$$

where for the moment s is a real number greater than one. Upon taking logarithms of both sides and developing the ensuing logarithms in power series, one arrives at

$$-\log \zeta(s) = \sum_p \log(1 - p^{-s}) = \sum_p \sum_{k \geq 1} k^{-1} p^{-ks}$$

which holds true for $s > 1$. The trick is now to consider the limit when s tends to one. We now that $\zeta(s)$ has a pole at $s = 1$, so the left side goes to infinity when s approaches one.

The double sum on the right side of the equation may split into two sums, one over all primes but with $k = 1$ and one over all primes and all $k \geq 2$:

$$-\log \zeta(s) = \sum_p p^{-s} + \sum_p \sum_{k \geq 2} k^{-1} p^{-ks}$$

By the comparison test the last sum is convergent for all $s > 1/2$ uniformly on compacts; indeed, it is dominated by $2\sum_n n^{-2s}$, and so is continuos, and, in this context most importantly, it is bounded near one. So the situation when we let s tend to one, is that the left side tends to infinity and the second sum on the right is bounded. Of course this causes the sum $\sum_p p^{-s}$ to go to infinity, and from this Euler infered that $\sum_p p^{-s}$ is not a finite sum; hence there are infintely many primes!

Now, if we want to prove that there are infinitely many primes in a certain set $\mathcal{P}$, one might try to mimic this proof—in the context of Dirichlet's theorem, $\mathcal{P}$ would be the set $\{\, p \mid p \equiv a \mod m \,\}$. This would require a function, say $G(s)$, taking the place of the ζ-function. It must have a pole at $s = 1$, and there must be some kind of series development

$$G(s) = \sum_{p \in \mathcal{P}} p^{-s} + R(s)$$

where $R(s)$ has a bounded behavior near one. Just as Euler observed, this would imply that $\mathcal{P}$ is an infinite set.

To carry out this program Dirichlet defined his L-functions. There is one such function $L(s, \chi)$ for each character χ modulo m, and the function $g(s)$ will be a linear combination of their logarithms:

$$G(s) = \sum_{\chi} \overline{\chi}(a) \log L(\chi, s) \tag{8.1}$$

The Dirichlet L-functions and Euler product

Let χ be a Dirichlet character of modulus m. One defines the Dirichlet L-function corresponding to χ by

$$L(s, \chi) = \sum_{n} \chi(n) n^{-s}. \tag{8.2}$$

As the values $\chi(n)$ are either zero or roots of unity (and therefore of absolute value one), the series in 8.2 is dominated by the series $\sum_n n^{-s}$ and therefore convergent for $\sigma = \operatorname{Re} s > 1$; uniformly on compact sets. Hence $L(s, \chi)$ is an analytic function in that half plane.

The L-functions enjoy a lot of properties common with the Riemann ζ-functions, among them, they have a Euler product. This is holds true since the Dirichlet's characters are *completly multiplicative*.

Proposition 8.2 *The Dirichlet L-function $L(s, \chi)$ has an Euler product. That is, one has*

$$L(s, \chi) = \prod_{p} (1 - \chi(p) p^{-s})^{-1}.$$

PROOF: First of all, for each of the factors in the product one has the geometric series development

$$(1-\chi(p)p^{-s})^{-1} = \sum_k \chi(p)^k p^{-ks} = \sum_k \chi(p^k)p^{-ks}, \tag{8.3}$$

and series is absolutely convergent ($|\chi(p)| \leq 1$ and $s > 1$). Leaning on Mertens' theorem about products of absolutely convergent series (they equal their Cauchy products) and using that the character χ is completely multiplicative, we infer from 8.3 that

$$\prod_{p\leq x}(1-\chi(p)p^{-s})^{-1} = \sum_{p|n\Rightarrow p\leq x} \chi(n)n^{-s}.$$

When x tends to infinity, the right side of this equality tends to $L(s,\chi)$ (the right side defines a subsequence of the sequence of partial sums of the absolutely convergent series for $L(s,\chi)$). And we are done; the product converges to $L(s,\chi)$. ❑

Taking logarithm and introducing characters

The next step is to take the logarithm of $L(s,\chi)$ and equate it to the logarithm of the Euler product. This must be done with some care since complex logarithms can be insidious. As seen from the Euler product, the L-function $L(s,\chi)$ does not vanish in the half plane $\sigma > 1$ (the absolute value of every factor is at least one), so the half plane being simply connected, the logarithm $\log L(s,\chi)$ is well defined (any branch is defined, but we stick to the principal branch); however when taking the logarithm of the Euler product, one can not immediately infer that one arrive at the sum of the logarithms ($\log zw$ is not necessarily equal to $\log z + \log w$; they might differ by $2\pi i$). Summing the principal logarithm of the factors i the Euler product, and using for the principal branch it holds that $\log(1-z) = \sum_{k\geq 1} k^{-1}z^k$ for $|z| < 1$, we arrive at the following series

$$G(s) = \sum_p \log(1-\chi(p)p^{-s}) = \sum_p \sum_{k\geq 1} k^{-1}\chi(p^k)p^{-ks}, \tag{8.4}$$

which converges fore $s > 1$, uniformly on compacts, as it is dominated by $\sum_n n^{-s}$. And since the exponential function behaves better than the logarithm; *i.e.,* it is is continuos and $\exp(z+w) = \exp(z)\exp(w)$ always holds, this series is *a* logarithm of $L(s,\chi)$ (but may be not the principal one); that is, one has

$$\exp G(s) = -L(s,\chi),$$

Proposition 8.3 *For one branch of the logarithm, one has*

$$-\log L(s,\chi) = \sum_p \chi(p)p^{-s} + R(s,\chi) \tag{8.5}$$

where $R(s,\chi)$ is a an analytic function for $\sigma > 1/2$, hence bounded near 1.

PROOF: Splitting the series in 8.4 in two sums, one for $k = 1$ and one for $k \geq 2$, one arrives at

$$G(s) = \sum_p \chi(p)p^{-s} + \sum_{k\geq 2} k^{-1}\chi(p^k)p^{-ks} = \sum_p \chi(p)p^{-s} + R(s,\chi).$$

where $R(s,\chi)$ is analytic for $\sigma > 1/2$ since the series $\sum_{k\geq 2} k^{-1}\chi(p^k)p^{-ks}$ is dominated by $2\sum_n n^{-2s}$. ❑

The insight of Dirichlet was to use the orthogonality relations among the different characters when forming the linear combination in 8.1. The effect on the right side in 8.5 is that the terms $\sum_p \chi(p)p^{-s}$ combine to the sum $\phi(m)\sum_{p\equiv a(m)} p^{-s}$. To see this, we start by recalling the orthogonality relation in 7.6 on page 140 in chapter 7, in a formulation relevant for the present context it reads

$$\sum_\chi \overline{\chi}(a)\chi(p) = \begin{cases} 0 & \text{if } p \not\equiv a \mod m \\ \phi(m) & \text{if } p \equiv a \mod m, \end{cases}$$

where the sum is over all Dirichlet characters modulo m. Introducing this in the linear combination in 8.1 we arrive at

$$-\sum_\chi \overline{\chi}(a)\log L(s,\chi) = \sum_\chi \overline{\chi}(a)\big(\sum_p \chi(p)p_{-s} + R(s,\chi)\big) =$$

$$= \sum_p \sum_\chi \overline{\chi}(a)\chi(p)p^{-s} + \sum_\chi \overline{\chi}(a)R(s,\chi) = \phi(m)\sum_{p\equiv a(m)} p^{-s} + R(s),$$

and this merits the status as a proposition:

Proposition 8.4 *If a and m are relatively prime natural numbers, one has*

$$G(s) = -\sum_\chi \overline{\chi}(a)\log L(s,\chi) = \phi(m)\sum_{p\equiv a(m)} p^{-s} + R(s), \tag{8.6}$$

where $R(s)$ is a function analytic for $\sigma > 1/2$, and where the sum on the left is taken over all Dirichlet characters modulo m.

The equation 8.6 lies at the hart of the proof of Dirichlet's theorem. Once we know the behavior of the different L-functions at $s = 1$ sufficiently well, we can infer Dirichlet's theorem from it. The point— like in Euler's proof of there being infinitely many primes—is that the function $G(s)$ tends to infinity when s tends to 1, then since $R(s)$ is bounded $\sum_{p\equiv a(m)} p^{-s}$ must be infinite. All this follows once we have established the next proposition whose proof occupy the two subsequent paragraphs.

Proposition 8.5 *Let χ be a Dirichlet character modulo m.*

- *The L-function $L(s, \chi_0)$ has a simple pole with residue $\phi(m)$ at $s = 1$*
- *If χ is a not the principal character, the L-function $L(s, \chi)$ can be continued to the half plane $\sigma > 0$, and $L(s, \chi)$ does not vanish at $s = 1$, i.e., one has $L(1, \chi) \neq 0$.*

Indeed, since $L(s, \chi_0)$ has a pole at $s = 1$ and $\chi(a) \neq 0$ (by assumption $\gcd(a, m) = 1$), the term $\chi(a) \log L(s, \chi_0)$ tends to ∞ when s tends to one, and as $L(1, \chi) \neq 0$ for all the non-principal characters, the sum $\sum_{\chi\neq\chi_0} \chi(a) \log L(s, \chi)$ stays bounded when $s \to 1$. Whence the left side in 8.6, *i.e.*, $G(s)$, tends to ∞ when s tends to one.

The principal character

The principal character χ_0 is special among the characters, and its L-function behaves rather differently from the others. The function $L(s, \chi_0)$ is closely related to the $\zeta(s)$-function as the following proposition shows. It has the same principal part as $\zeta(s)$ at $s = 1$, which in our present context is its most important feature; the role it has in this play is to give a pole to the function $G(s)$ at $s = 1$.

Proposition 8.6 *For the principal character χ_0 modulo m one has*

$$L(s, \chi_0) = \prod_{p|m}(1 - p^{-s})\zeta(s).$$

PROOF: This follows immediately from the Euler products of $L(s, \chi_0)$ and $\zeta(s)$; indeed since χ_0 is the characteristic function of the set of numbers relatively prime to m, one has

$$L(s, \chi_0) = \prod_{p}(1 - \chi_0(p)p^{-1})^{-1} = \prod_{p\nmid m}(1 - p^{-s})^{-1} = \prod_{p|m}(1 - p^{-s})\zeta(s).$$

❑

Corollary 8.1 *The L-function $L(s, \chi_0)$ extends to a meromorphic function in the half plan $\sigma > 0$ having a simple pole at $s = 1$ as its sole singularity. The residue at $s = 1$ is $\phi(m)$, the value of the Euler ϕ-function at m.*

The nonprincipal characters

We now turn to the the non-principal characters χ. The first observation is that the cumulative function of such a character is bounded by m; indeed, from the periodicity of χ one deduces that for any $x > 0$ if the integral part $[x]$ satisfy $[x] = qm + b$ where q is a natural number and $0 \leq b < m$, one has

$$\sum_{k \leq x} \chi(k) = q \sum_{0 < k \leq m} \chi(k) + \sum_{0 < k \leq b} \chi(k).$$

The orthogonality relation 7.7 on page 140 in chapter 7 gives us $\sum_{0<k\leq m} \chi(k) = 0$ and hence

$$\Big|\sum_{k \leq x} \chi(k)\Big| = \Big|\sum_{0 < k \leq b} \chi(k)\Big| \leq \sum_{0 < k \leq b} |\chi(k)| \leq m$$

We proved (proposition 6.6 on page 123 in chapter 6) that a Dirichlet series $\sum_n a_n n^{-s}$ whose coefficients have a *bounded* cumulative function, converges to an analytic function for $\sigma > 0$. Hence we have the first part of the following proposition.

Proposition 8.7 *Assume that χ is a non-principal Dirichlet character modulo m. The the L-series $L(s, \chi) = \sum_n \chi(n) n^{-s}$ converges to an analytic function whenever $\sigma > 0$. It holds that $L(1, \chi) \neq 0$.*

The second part, stating that $L(s, \chi)$ does not vanish at 1, is astonishingly deep, and the proof occupies the rest of this chapter. Before diving into that proof, let us do some instructive examples.

EXAMPLE 8.2. Let χ be the non-principal character mod 4. It vanishes on all even numbers and on the odd ones it holds that $\chi(4n + \epsilon) = \epsilon$ where $\epsilon = \pm 1$. Hence the L-series is

$$L(s, \chi) = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \cdots = \sum_{k \geq 0} (-1)^k (2k + 1)^{-s}.$$

When s is real and positive, this series is alternating with terms tending monotonically to zero, hence by what we learned in school, it converges. Putting $s = 1$, we find $L(1, \chi) = \pi/4$; indeed, it is classical that

$$\pi/4 = 1 - 1/3 + 1/5 - 1/7 + \ldots,$$

(This is the Gregory series for $\pi/4$ and follows *e.g.,* from the Taylor series of $\arctan x$ about the origin). ❄

EXAMPLE 8.3. It is instructive also to do the caclculations for the real non-principal character modulo 5 (see example 7.7 on page 138 in chapter 7). The calculations are not very deep just like we did during the first calculus course when finding sums of power series by integration.

The character is given by $\chi(5n+2) = \chi(5n-2) = -1$ and $\chi(5n+1) = \chi(5n-1) = 1$, and of course $\chi(5n) = 0$. The Dirichlet series therefore is

$$L(s,\chi) = 1 - 2^{-s} - 3^{-s} + 4^{-s} + 6^{-s} + \dots,$$

and we shall show that

$$L(1,\chi) = 1 - 1/2 - 1/3 + 1/4 + 1/6 + \cdots = \frac{1}{\sqrt{5}} \log(3/2 + \sqrt{5}/2).$$

We introduce the Taylor series

$$f(x) = \sum_{0\le n} \sum_{0\le k\le 4} \chi(k)(5n+k)^{-1} x^{5n+k}$$

whose value at $x = 1$ equals $L(1,\chi)$. Taking the derivative we arrive at

$$\begin{aligned} f'(x) &= \sum_{0\le n} \Big(\sum_{0\le k\le 4} \chi(k) x^{k-1} \Big) x^{5n} = \Big(\sum_{0\le k\le 4} \chi(k) x^{k-1} \Big) \sum_{n\ge 0} x^{5n} = \\ &= (x^3 - x^2 - x + 1)(1 - x^5)^{-1} \end{aligned}$$

Factoring the enumerator and the demoninator one finds $x^3 - x^2 - x + 1 = (x-1)^2(x+1)$ and $(1 - x^5) = (1 - x)(x^2 + \alpha_+ x + 1)(x^2 + \alpha_- x + 1)$ where $\alpha_\pm = 1/2 \pm \sqrt{5}/2$. Then, doing the partial fraction computations and the subsequent standard integration one arrives at the announce value; the function to integrate is:

$$\frac{(1-x)(1+x)}{(x^2 + \alpha_+ x + 1)(x^2 + \alpha_- x + 1)} = \frac{1}{\sqrt{5}} \Big(\frac{2x + \alpha_+}{x^2 + \alpha_+ x + 1} - \frac{2x + \alpha_-}{x^2 + \alpha_- x + 1} \Big)$$

❄

PROBLEM 8.2. Let χ be the character modulo 8 given by $\chi(8n\pm 1) = 1$ and $\chi(8n\pm 3) = -1$ and $\chi(2n) = 0$. Show that $L(1,\chi) = \log(3 + 2\sqrt{2})/\sqrt{8}$. ✸

PROBLEM 8.3. Let χ be the character modulo 12 such that $\chi(12n \pm 1) = 1$ and $\chi(12n \pm 5) = -1$ and $\chi(n) = 0$ in all other cases. Show that $L(1,\chi) = \log(7 + 4\sqrt{3})/\sqrt{12}$. ✸

The previous examples and exercises are worth commenting on; the values are not only non-zero, but they are amazing! They are closely related to the basic invariants of quadratic fields. Recall that the quadratic field $\mathbb{Q}(\sqrt{d}) = \{ x + y\sqrt{d} \mid x, y \in \mathbb{Q} \}$ has a norm map associated to it, it is given as $N(x + y\sqrt{d}) = x^2 - dy^2$, and is multiplicative. The units in the ring of integers of $\mathbb{Q}(\sqrt{d})$ are precisely those elements $a = x + y\sqrt{d}$ such that $N(a) = \pm 1$; that is the solutions of the equations $x^2 - dy^2 = \pm 1$.

If $d < 0$, there are not many solutions, and the equations are not particularly interesting. However, if $d > 0$ there are infinitely many solutions. This not obvious and was proven by Lagrange. The equations have been, and still are, studied by many people. They are called Pell's equations; according to Hendrik Willem Lenstra as a result of a mistake of Euler. The english mathematician John Pell had nothing to do with the equations and Euler mixed him up with another englishman William Brouncker who worked on the equations.

If you take $d = 2$, you see that $\epsilon_2 = 3 + 2\sqrt{2}$ is a solution of Pell's equation $x^2 - 2y^2 = 1$. Therefore ϵ_2 is a unit in $\mathbb{Z}[\sqrt{2}]$, and one may show that it is the so called *fundamental unit*, *i.e.,* any other unit is a power of ϵ_2. And, amazingly, the value of the L-function $L(1, \chi_8)$, where χ_8 is the character from problem 8.2, is expressible in terms of thew fundamental unit ϵ_2! One has $L(1, \chi_8) = \log \epsilon_2/\sqrt{4 \cdot 2}$. There is of course a close relation between the field $\mathbb{Q}(\sqrt{2})$ and the character χ_8. Recall that 2 is a square mod an odd prime p, if and only if $p^2 - 1 \equiv 0 \mod 8$, that is $p \equiv \pm 1 \mod 8$; so the character χ_8 is exactly the quadratic character checking if 2 is a square or not mod p.

In a similar fashion, when $d = 3$, the algebraic integer $\epsilon_3 = 7 + 4\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ is a unit in $\mathbb{Z}[\sqrt{3}]$; *i.e.,* a solution of Pell's equation $x^2 - 3y^2 = 1$, and one can check that it is the fundamental unit. Again, $L(1, \chi_{12}) = \log(\epsilon_3)/\sqrt{4 \cdot 3}$ where χ_{12} is the character from problem 8.3!

So a pattern emerges! And indeed, Dirichlet showed that

$$L(1, \chi_\Delta) = h \log(\epsilon_d)/\sqrt{\Delta},$$

where χ_d is the quadratic character associated to d and ϵ_d is a fundamental unit in $\mathbb{Q}(\sqrt{d})$. The number Δ is the so called discriminant, *i.e.,* $\Delta = d$ if $d \equiv 1 \mod 4$ and $4d$ otherwise, and h is the class number of $\mathbb{Q}(\sqrt{d})$, a number one associates to $\mathbb{Q}(\sqrt{d})$ in algebraic number theory. The relation above is just one of many similar ones. The leading coefficient of a Dirichlet series associated to an algebraic or geometric object at special points often has a very deep significance.

Non vanishing of $L(1, \chi)$ for complex characters

This is the easy case the reason being that complex characters come in pairs χ and $\overline{\chi}$, and these two characters are different (this is just the meaning of not being real).

We form the product $\prod_\chi L(s, \chi)$, and when the variable s takes real values, this product must be real; indeed $\overline{L(s, \chi)} = L(\overline{s}, \overline{\chi}) = L(s, \overline{\chi})$. But a lot more can be said:

Lemma 8.1 *When s is real and $s > 1$, it holds true that $\prod_\chi L(s, \chi) \geq 1$*

PROOF: Taking logarithms (remember that $s > 1$) we obtain

$$\sum_p \log L(s, \chi) = \sum_{p,k} (\sum_\chi \chi(p^k)) k^{-1} p^{-ks} = \phi(m) \sum_{p \equiv 1(m), k} k^{-1} p^{-ks} > 0,$$

where we use the orthogonality relations $\sum_\chi \chi(a) = 0$ if $a \not\equiv 1 \mod m$ and $\sum_\chi \chi(a) = \phi(m)$ in case $a \equiv 1 \mod m$ (proposition 7.7 on page 140 in chapter **??**). ❑

Now, assume that χ_1 is a complex character modulo m whose L-function vanishes at $s = 1$. Then of course $L(s, \overline{\chi}_1)$ vanishes at $s = 1$ as well, and in the product $\prod_\chi L(s, \chi)$ at least two of the factors vanish. However the only factor having a pole at $s = 1$ is the one corresponding to the principal character and that pole is simple. So there is no way the two zeros can be compensated for, and one deduces that the product $\prod_\chi L(s, \chi)$ vanishes for $s = 1$ in flagrant contradiction with lemma 8.1 above. Hence we have proven

Proposition 8.8 *If χ is a complex Dirichlet character modulo m, then $L(1, \chi) \neq 1$.*

The non vanishing for real characters

This about the real characters modulo m and is somehow more elaborate than the complex case. The proof has been simplified over time, is now not too involved. There are two ingredients; a general property of Dirichlet series with non negative coefficients, and as usual a smart trick, which this time due to de la Vallee Poussin.

The general property is that in some sense Dirichlet series with non-negative coefficient must be decreasing; of course to speak about decreasing functions, we must restrict the variable to be real. This is obvious for series itself— each term $a_n n^{-s}$ decreases for $s > 0$—but indeed it holds for any extension to the positive real axis, that is to $s > 0$.

Proposition 8.9 *Let $\phi(s) = \sum_n a_n n^{-s}$ be a Dirichlet series with $a_n \geq 0$, and assume that it converges for $s > 1$. Let $a > 1$ and $\alpha < 1$ be two numbers: If $\phi(s)$ can be extended analytically to the interval (α, ∞), then $\phi(s) \geq \phi(a)$ for $s \in (\alpha, a)$.*

PROOF: The point of the proof is to develop $\phi(s)$ in Taylor series about a. Taking successive derivatives, one finds

$$\phi^k(a) = \sum_n (-1)^k a_n (\log n)^k n^{-a} = (-1)^k c_k$$

where $c_k \geq 0$. Hence the Taylor series is

$$\phi(s) = \sum_n (-1)^n c_n / n! (s - a)^n = \sum_n c_n / n! (a - s)^n,$$

and it converges to $\phi(s)$ in an interval containing (α, a) since there is an analytic continuation of $\phi(s)$ to this interval. Since $a - s > 0$ if $s \in (\alpha, a)$, it follows that $\phi(s) > \phi(a) = c_0$. ❑

PROBLEM 8.4. With assumptions as in the proposition, show that $\phi(s)$ decreases on the interval (α, a). ✸

Now, let χ be a real character whose L-function we assume vanishes for $s = 1$. The only real roots of unity being ± 1, the values of χ are either 0 or ± 1, and typically the

L-functions look like the ones we wrote done in the two examples above. We form the meromorphic function

$$\phi(s) = \frac{L(s,\chi)L(s,\chi_0)}{L(2s,\chi_0)}.$$

The enumerator is analytic for $\sigma > 0$ since the zero of $L(s,\chi)$ at $s = 1$ neutralizes the pole $L(s,\chi_0)$ has there, and the denominator is analytic and non-zero for $\sigma > 1/2$, but when s tends to $1/2$ it tends to ∞. Hence $\lim_{s\to 1/2}\phi(s) = 0$. The next point is that $\phi(s)$ has a development as a Dirichlet series for $s > 1$ whose coefficients are non-negative; the proposition 8.9 then ends the story, since we shall see that $\phi(s) \geq 1$ for any $s > 1$.

$$\begin{aligned}\phi(s) &= \prod_p (1-\chi_0(p)p^{-2s})(1-\chi(p)p^{-s})^{-1}(1-\chi_0(p)p^{-s})^{-1} = \\ &= \prod_{p\nmid m}(1-p^{-2s})(1-\chi(p)p^{-s})^{-1}(1-p^{-s})^{-1} = \\ &= \prod_{p\nmid m}(1+p^{-s})(1-\chi(p)p^{-s})^{-1} = \prod_{\chi(p)=1}\frac{1+p^{-s}}{1-p^{-s}}.\end{aligned}$$

One easily finds

$$\frac{1+p^{-s}}{1-p^{-s}} = 1 + 2p^{-s} + 2p^{-2s} + \cdots = 1 + \sum_{1\leq k} 2p^{-ks}, \tag{8.7}$$

which gives

Lemma 8.2 *One has for $s > 1$*

$$\phi(s) = \sum 2^{\omega(n)} n^{-s}, \tag{8.8}$$

where $\omega(n)$ denotes the number of distinct prime numbers dividing n, and where the sum extends to all numbers whose prime divisors all satisfy $\chi(p) = 1$.

Indeed, one has by equation 8.7

PROOF:

$$\prod_{\chi(p)=1, p\leq x}\frac{1+p^{-s}}{1-p^{-s}} = \prod_{\chi(p)=1,p\leq x}\left(1+\sum_{1\leq k}2p^{-ks}\right) = 1 + \sum_{p|n\Rightarrow p\leq x,\chi(p)=1} 2^{\omega(n)}n^{-s} \tag{8.9}$$

and the lemma follows since the product converges *a priori*. (The sums on the right side form a subsequence of the sequence of partial sums of the series in 8.7, but terms are positive so this suffices to have convergence in 8.7). ❑

Bibliografi

[1] Joseph H. Silverman, *The Arithmetic of Elliptic curves*, GTM 106

[2] J. S. Milne, *Elliptic curves*,

[3] Dale Husemöller, *Elliptic curves*, GTM 111

[4] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves*, Undergraduate text in Mathematics, Springer

[5] Anthony W. Knapp: *Elliptic curves*, Mathematical notes, Princeton University Press, 1992. ISBN 0-691-08559-5(BP)

[6] Keith Conrad: *The congruent number problem* at http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/congnumber.pdf

[7] R. M. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University, (1988) 161-169. Also to be found on Murty's home page.

[8] Keith Conrad, *Euclidean Proofs of Dirichlet Theorem*, http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/dirichleteuclid.pdf.