

Dirichlet's Theorem

Eitan Chatav

Dirichlet's theorem says that for coprime $a, m \in \mathbb{Z}$ with $m \geq 1$ there are infinitely many primes $\equiv a \pmod{m}$.

A character mod m is a homomorphism $\chi : \mathbb{Z}/m^* \rightarrow \mathbb{C}^*$. It can be extended to a map $\mathbb{N} \rightarrow \mathbb{C}$ by letting $\chi(n) = 0$, if n is not coprime to m .

Note that for a ring R , R^* denotes the multiplicative group of units in R .

The corresponding Dirichlet L -function is $L(s, \chi) = \sum_{n \in \mathbb{N}} \chi(n)n^{-s}$.

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

Proof: $\prod_{p \in P} 1/(1 - \chi(p)p^{-s}) = \prod_{p \in P} \sum_{n \in \mathbb{N}} \chi(p^n)(p^n)^{-s}$. And by the fundamental theorem of arithmetic, the set of products of sums of prime powers is exactly the set of natural numbers, so this $= \sum_{n \in \mathbb{N}} \chi(n)n^{-s}$.

Note: I'm neglecting convergence. L converges absolutely for $\text{Re}(s) > 1$.

Back to characters. Note that units in \mathbb{Z}/m are coprime to m , so that $|\mathbb{Z}/m^*| = \phi(m)$. Here the Euler ϕ -function counts the number of integers in $1, \dots, m$ which are coprime to m . Let C_m denote $\text{Hom}(\mathbb{Z}/m^*, \mathbb{C}^*)$, the set of characters mod m . C_m is finite, say $|C_m| = h$ and forms an abelian group with $(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n)$. And for all n , $\chi(n)$ is a root of unity since $\chi(n)^h = \chi(n^h) = \chi(1) = 1$.

Theorem: The following formulas hold.

(i)

$$\sum_{n \in \mathbb{Z}/m^*} \chi(n) = \begin{cases} \phi(m) & \text{if } \chi = 1 \\ 0 & \text{if } \chi \neq 1 \end{cases}$$

(ii)

$$\sum_{\chi \in C_m} \chi(n) = \begin{cases} h & \text{if } n \equiv 1 \pmod{m} \\ 0 & \text{if } n \not\equiv 1 \pmod{m} \end{cases}$$

(iii)

$$h = \phi(m)$$

(iv)

$$\frac{1}{\phi(m)} \sum_{\chi \in C_m} \frac{\chi(n_1)}{\chi(n_2)} = \begin{cases} 1 & \text{if } n_1 \equiv n_2 \pmod{m} \\ 0 & \text{if } n_1 \not\equiv n_2 \pmod{m} \end{cases}$$

Proof: (i) Clear when $\chi = 1$. If $\chi \neq 1$, then there is some l with $\chi(l) \neq 1$ so $\chi(l) \sum_{n \in \mathbb{Z}/m^*} \chi(n) = \sum_{n \in \mathbb{Z}/m^*} \chi(l)\chi(n) = \sum_{n \in \mathbb{Z}/m^*} \chi(ln) = \sum_{n \in \mathbb{Z}/m^*} \chi(n)$ since ln runs over \mathbb{Z}/m^* as n does. So, $(1 - \chi(l)) \sum_{n \in \mathbb{Z}/m^*} \chi(n) = 0$, but $\chi(l) \neq 1$, so $\sum_{n \in \mathbb{Z}/m^*} \chi(n) = 0$.

(ii) Clear when $n \equiv 1 \pmod{m}$. If $n \not\equiv 1 \pmod{m}$, then there is some χ_0 with $\chi_0(n) \neq 1$ so $\chi_0(n) \sum_{\chi \in C_m} \chi(n) = \sum_{\chi \in C_m} \chi_0(n) \chi(n) = \sum_{\chi \in C_m} (\chi_0 \chi)(n) = \sum_{\chi \in C_m} \chi(n)$ since $\chi_0 \chi$ runs over C_m as χ does. So, $(1 - \chi_0(n)) \sum_{\chi \in C_m} \chi(n) = 0$, but $\chi_0(n) \neq 1$, so $\sum_{\chi \in C_m} \chi(n) = 0$.

(iii) Follows since $h = \sum_{\chi \in C_m} \sum_{n \in \mathbb{Z}/m^*} \chi(n) = \sum_{n \in \mathbb{Z}/m^*} \sum_{\chi \in C_m} \chi(n) = \phi(m)$.

(iv) Follows since $(1/h) \sum_{\chi \in C_m} \chi(n_1)/\chi(n_2) = (1/h) \sum_{\chi \in C_m} \chi(n_1 n_2^{-1})$. Plug this into formula (ii) and use (iii).

Theorem:

$$\frac{1}{\phi(m)} \sum_{\chi \in C_m} \frac{\ln(L(s, \chi))}{\chi(a)} = \sum_{\substack{p \in P, n \in \mathbb{N} \\ p^n \equiv a \pmod{m}}} \frac{p^{-sn}}{n}.$$

Proof:

$$\ln(L(s, \chi)) = \sum_{p \in P} -\ln(1 - \chi(p)p^{-s}) = \sum_{p \in P} \sum_{n \in \mathbb{N}} \frac{1}{n} (\chi(p)p^{-s})^n.$$

So,

$$\frac{1}{\phi(m)} \sum_{\chi \in C_m} \frac{\ln(L(s, \chi))}{\chi(a)} = \sum_{p \in P} \sum_{n \in \mathbb{N}} \frac{p^{-sn}}{n} \frac{1}{\phi(m)} \sum_{\chi \in C_m} \frac{\chi(p^n)}{\chi(a)} = \sum_{\substack{p \in P, n \in \mathbb{N} \\ p^n \equiv a \pmod{m}}} \frac{p^{-sn}}{n}.$$

Theorem: $\sum_{\chi \in C_m} \frac{\ln(L(s, \chi))}{\chi(a)}$ diverges as $s \rightarrow \infty$.

Proof: Split the sum as $\sum_{\chi \in C_m} = \sum_{\chi=1} + \sum_{\chi=\bar{\chi}} + \sum_{\chi \neq \bar{\chi}, 1}$. If, $\chi = 1$, then

$$\chi(n) = \begin{cases} 1 & \text{if } \gcd(n, m) = 1 \\ 0 & \text{if } \gcd(n, m) \neq 1 \end{cases}.$$

So, $L(s, 1) = \prod_{\gcd(p, m)=1} (1 - p^{-s})^{-1} = \zeta(s) \prod_{p|m} (1 - p^{-s})$. But $\zeta(s) \rightarrow \infty$ as $s \rightarrow 1$, so $L(s, 1) \rightarrow \infty$ as $s \rightarrow \infty$. One might think one is done at this point except that the other terms in the sum might cancel this contribution. This will only occur if $L(1, \chi) = 0$ for some χ , for then $\ln(L(1, \chi)) = -\infty$. Suppose that χ is not real-valued and that $L(s, \chi) = 0$. We'll derive a contradiction. First note that $L(s, \chi^{-1}) = L(s, \bar{\chi}) = \overline{L(s, \chi)} = \overline{0} = 0$. By the previous theorem with $a = 1$,

$$\sum_{\chi \in C_m} \ln(L(s, \chi)) = \phi(m) \sum_{\substack{p \in P, n \in \mathbb{N} \\ p^n \equiv 1 \pmod{m}}} \frac{p^{-sn}}{n} > 0.$$

Hence, $|\prod_{\chi \in C_m} L(s, \chi)| > 1$. But if $L(1, \chi) = L(1, \chi^{-1}) = 0$, then since there are two zeros and only one simple pole $L(1, 1) = \infty$, $\prod_{\chi \in C_m} L(s, \chi) = 0$, a contradiction. This line of proof only worked for χ not real-valued. The proof for real-valued χ is more difficult, but it's still true. All this is to say that the theorem is considered proved.

Corollary: Dirichlet's Theorem

Proof: Suppose Dirichlet's Theorem were false. Then $\prod_{p \equiv a \pmod{m}} p^{-1}$ converges since it's a finite product. But then, $\sum_{\substack{p \in P, n \in \mathbb{N} \\ p^n \equiv a \pmod{m}}} \frac{p^{-sn}}{n}$ converges since $\sum_{p \in P} \sum_{n > 1} (np^n)^{-1}$ converges. Therefore, $\frac{1}{\phi(m)} \sum_{\chi \in C_m} \frac{\ln(L(s, \chi))}{\chi(a)}$ converges, contradicting the last theorem.