Analytic Number Theory
Lecture 7

Mariusz Mirek
Rutgers University

Padova, April 1, 2025.

Supported by the NSF grant DMS-2154712,
and the CAREER grant DMS-2236493.

Dirichlet characters

Definition

Let $q \in \mathbb{Z}_+$. A Dirichlet character modulo q is a map $\chi : \mathbb{Z}\backslash\{0\} \to \mathbb{C}$ satisfying the following rules for all $a, b \in \mathbb{Z}\backslash\{0\}$:

(i) $\chi(a) = \chi(a \pmod q)$;

(ii) $\chi(ab) = \chi(a)\chi(b)$;

(iii) $\chi(a) = 0$ if $(a, q) > 1$.

Remarks

- In fact, (i) and (ii) mean that Dirichlet character modulo q are homomorphisms of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ and property (iii) extends these maps to $\mathbb{Z}\backslash\{0\}$.
- On the other hand, we can readily see that corresponding to every multiplicative character $\psi \in \widehat{(\mathbb{Z}/q\mathbb{Z})^\times}$ there is $\chi : \mathbb{Z}\backslash\{0\} \to \mathbb{C}$, a Dirichlet character modulo q, defined by

$$\chi(a) = \begin{cases} \psi(a + q\mathbb{Z}) & \text{if } (a, q) = 1, \\ 0 & \text{if } (a, q) > 1. \end{cases}$$

From this definition we immediately see that χ satisfies (i)-(iii).

Remarks

- By the previous remark we see that the set of Dirichlet characters modulo q is a group isomorphic to the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ of the units of the ring $\mathbb{Z}/q\mathbb{Z}$.
- In particular, there are $\varphi(q)$ Dirichlet characters modulo q.
- The identity element of this group is called the principal, or trivial, character modulo q and is usually denoted by χ_0. Thus, χ_0 is defined for all $a \in \mathbb{Z}$ by

$$\chi_0(a) = \begin{cases} 1, & \text{if } (a,q) = 1, \\ 0, & \text{otherwise .} \end{cases}$$

- Let χ be a Dirichlet character modulo q. We define $\overline{\chi}$ by $\overline{\chi}(a) = \overline{\chi(a)}$. Clearly, $\overline{\chi}$ is also a Dirichlet character modulo q called the conjugate character of χ.
- It is also not difficult to see that, if $(a,q) = 1$, then $\chi(a)$ is a $\varphi(q)$ th root of unity. Indeed, if $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, we have

$$(\chi(a))^{\varphi(q)} = \chi\left(a^{\varphi(q)}\right) = \chi(1) = 1.$$

Orthogonality relations

Notation

Let $m \in \mathbb{Z}_+$. We will use the following convenient notation:

- $\sum_{a \pmod m}$ will always denote the sum over a complete set of residue classes modulo m.
- $\sum_{\chi \pmod m}$ will always denote the sum over the $\varphi(m)$ Dirichlet characters modulo m.

Applying the first orthogonality relation from Lecture 6 for $\mathbb{G} = (\mathbb{Z}/m\mathbb{Z})^\times$ we obtain the following orthogonality relation for Dirichlet characters:

Theorem (Orthogonality relation I)

- *If χ is a Dirichlet character modulo m, then*

$$\sum_{a \pmod m} \chi(a) = \begin{cases} \varphi(m) & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

- *If $a \in \mathbb{Z}$, then*

$$\sum_{\chi \pmod m} \chi(a) = \begin{cases} \varphi(m) & \text{if } a \equiv 1 \pmod m, \\ 0 & \text{if } a \not\equiv 1 \pmod m. \end{cases}$$

Orthogonality relations

Applying the second orthogonality relation from Lecture 6 for $\mathbb{G} = (\mathbb{Z}/m\mathbb{Z})^\times$ we obtain the following orthogonality relation for Dirichlet characters:

Theorem (Orthogonality relation II)

- *If χ_1 and χ_2 are Dirichlet characters modulo m, then*

$$\sum_{a \pmod m} \chi_1(a)\overline{\chi_2}(a) = \begin{cases} \varphi(m) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

- *If $a, b \in \mathbb{Z}$, then*

$$\sum_{\chi \pmod m} \chi(a)\overline{\chi}(b) = \begin{cases} \varphi(m) & \text{if } (a,m) = (b,m) = 1 \text{ and } a \equiv b \pmod m, \\ 0 & \text{otherwise .} \end{cases}$$

Examples of Dirichlet characters

- For $k = 2$, the principal character is the only one.
- For $k = 3$, there are two characters, namely

$$\chi_0(n) = \begin{cases} 1 & \text{if } n \equiv 1, 2 \bmod 3, \\ 0 & \text{if } n \equiv 0 \mod 3, \end{cases} \qquad \chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 3, \\ -1 & \text{if } n \equiv -1 \bmod 3, \\ 0 & \text{if } n \equiv 0 \bmod 3. \end{cases}$$

- For $k = 4$, there are again two characters, namely

$$\chi_0(n) = \begin{cases} 1 & \text{if } n \text{ is odd }, \\ 0 & \text{if } n \text{ is even}, \end{cases} \qquad \chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv -1 \bmod 4, \\ 0 & \text{if } n \text{ is even }. \end{cases}$$

- For $k = 5$, there are four characters given in the following table:

$n \pmod 5$	1	2	3	4	0
$\chi_0(n)$	1	1	1	1	0
$\chi_1(n)$	1	i	$-i$	-1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	$-i$	i	-1	0

Conductors, induced, primitive and imprimitive characters

Let χ, χ_1 be Dirichlet characters modulo q and q_1 respectively. Let q_1 be a divisor of q. We say that χ is induced by χ_1 or χ_1 induces χ if

$$\chi(n) = \chi_0(n)\chi_1(n) \quad \text{for all} \quad n \in \mathbb{Z}, \tag{*}$$

where χ_0 is the principal character modulo q.

- A Dirichlet character χ modulo q is said to be imprimitive if there exists a Dirichlet character χ_1 modulo q_1 that induces χ for some proper divisor q_1 of q.
- The conductor of a Dirichlet character χ modulo q is the smallest divisor q_1 of q for which (*) holds.
- A Dirichlet character χ modulo q is said to be primitive if the conductor of χ is simply equal to its modulus q. In other words, χ is primitive, if it is trivially induced by itself and $\chi = \chi_0\chi$.

Remarks

- The principal character χ_0 is imprimitive for every integer $q > 1$.
- Let $q^\star$ be the conductor of a Dirichlet character χ modulo q. Then $\chi = \chi_0\chi^\star$, where $\chi^\star$ is a Dirichlet character modulo $q^\star$, which is primitive and uniquely determined by χ. This follows from the fact that $q^\star$ is the smallest divisor of q for which (*) holds.

Useful result

Lemma

Let $m, d \in \mathbb{Z}_+$ be such that $d \mid m$. If $\gcd(a, d) = 1$ for some $a \in \mathbb{Z}$, then there exists $b \in \mathbb{Z}$ such that $b \equiv a \pmod{d}$ and $\gcd(b, m) = 1$.

Proof.

- Let $m = \prod_{i \in [k]} p_i^{r_i}$ and $d = \prod_{i \in [k]} p_i^{s_i}$, where $r_i \geq 1$ and $0 \leq s_i \leq r_i$ for $i \in [k]$. Let n be the product of the prime powers that divide m but not d. Then $n = \prod_{\substack{i \in [k] \\ s_i = 0}} p_i^{r_i}$ and $\gcd(n, d) = 1$.
- By the existence of solutions for linear congruences there is $x \in \mathbb{Z}$ such that $dx \equiv 1 - a \pmod{n}$. Then $b = a + dx \equiv 1 \pmod{n}$ and $\gcd(b, n) = 1$.
- Also,
$$b \equiv a \pmod{d}.$$
- If $\gcd(b, m) \neq 1$, there exists a prime $p \in \mathbb{P}$ that divides both b and m. However, p does not divide n since $\gcd(b, n) = 1$. It follows that $p \mid d$, and so p divides $b - dx = a$, which is impossible since $(a, d) = 1$.

Therefore, $\gcd(b, m) = 1$ and we are done. □

Quasiperiod of characters

Definition

Let χ be a Dirichlet character modulo q. We say d is a quasiperiod of χ if $\chi(m) = \chi(n)$ whenever $m \equiv n \pmod{d}$ and $(mn, q) = 1$. Obviously, every period is a quasiperiod.

Proposition

Let χ be a Dirichlet character modulo q. Then, χ is imprimitive if and only if there is a proper divisor d of q which is a quasiperiod of χ. In particular, the conductor of χ is its quasiperiod.

Proof.

- Suppose that χ is imprimitive, then it is induced by a Dirichlet character χ_1 modulo d, that is $\chi = \chi_0\chi_1$. Take $m \equiv n \pmod{d}$ with $(mn, q) = 1$, then $(m, q) = (n, q) = 1$ and

$$\chi(m) = \chi_0(m)\chi_1(m) = \chi_1(m) = \chi_1(n) = \chi_0(n)\chi_1(n) = \chi(n),$$

  since χ_1 has period d.

- For the converse implication, we shall construct a Dirichlet character $\chi^\star$ modulo d such that $\chi = \chi_0\chi^\star$.
- For this purpose we will use the following observation if $d \mid q$ and $(n, d) = 1$, then there is $k \in \mathbb{Z}$ such that $(n + dk, q) = 1$.

Proof

- Then it suffices to set

$$\chi^\star(n) := \begin{cases} \chi(n+dk) & \text{if } (n,d)=1, \\ 0 & \text{if } (n,d)>1, \end{cases}$$

  where $k \in \mathbb{Z}$ is such that $(n+dk, q) = 1$.
- We note that although there are many possible choices of $k \in \mathbb{Z}$, the value of $\chi^\star(n)$ depends only on $n \pmod d$. Indeed, if $n \equiv m \pmod d$ and $(n,d) = (m,d) = 1$ then there are integers $k_n, k_m \in \mathbb{Z}$ such that $(n+dk_n, q) = (m+dk_m, q) = 1$, which immediately implies

$$\chi^\star(n) = \chi(n+dk_n, q) = \chi(m+dk_m, q) = \chi^\star(m),$$

  since d is the quasiperiod of χ and $n+dk_n \equiv m+dk_m \pmod d$.
- It remains to prove that $\chi^\star$ is a homomorphism. Let $m, n \in \mathbb{Z}$ be such that $(mn, d) = 1$, then $(m,d) = (n,d) = 1$ and there are $k_m, k_n, k_{mn} \in \mathbb{Z}$ such that $(m+dk_m, q) = (n+dk_n, q) = (mn+dk_{mn}, q) = 1$. Thus we have $(m+dk_m)(n+dk_n) \equiv mn+dk_{mn} \pmod d$ and since χ is homomorpfism and d is the quasiperiod of χ, we consequently have

$$\begin{aligned} \chi^\star(mn) &= \chi(mn+dk_{mn}) = \chi((m+dk_m)(n+dk_n)) \\ &= \chi(m+dk_m)\chi(n+dk_n) = \chi^\star(m)\chi^\star(n). \end{aligned}$$

□

Quasiperiodic characters

Proposition

Let χ be a Dirichlet character modulo q and let $d \mid q$ and $d < q$. Then, χ has quasiperiod d if and only if $\chi(n) = 1$ for all $n \equiv 1 \pmod{d}$ with $(n, q) = 1$.

Proof.

- Observe that if χ has quasiperiod d, then $\chi(m) = \chi(n)$ whenever $m \equiv n \pmod{d}$ and $(mn, q) = 1$, which implies the condition above by taking $m = 1$, since $\chi(1) = 1$. For the converse, assume that the above condition holds. Take $m \equiv n \pmod{d}$ with $(m, q) = (n, q) = 1$.
- Since $(m, q) = 1$ then we can find $m' \in \mathbb{Z}$ such that $mm' \equiv 1 \pmod{q}$.
- Thus $\chi(mm') = \chi(1) = 1$, since χ has period q.
- We also obtain that $mm' \equiv 1 \pmod{d}$, since $d \mid q$, and consequently

$$nm' \equiv mm' \equiv 1 \pmod{d}.$$

- Since $(mm', q) = (nm', q) = 1$, we obtain by the above condition that

$$\chi(m)\chi(m') = \chi(mm') = 1 = \chi(nm') = \chi(n)\chi(m'),$$

which yields $\chi(n) = \chi(m)$ as desired. □

Characterizations of primitivity

Theorem

Let χ be a Dirichlet character modulo q. Then, χ is primitive if and only if for every proper divisor d of q there exists $m \in \mathbb{Z}$ satisfying $m \equiv 1 \pmod{d}$ and $(m, q) = 1$ such that $\chi(m) \neq 1$.

Proof.

The proof readily follows by applying the previous two propositions. □

Theorem

Let χ be a Dirichlet character modulo q. Then, the following are equivalent:

(i) *χ is primitive;*

(ii) *if $d \mid q$ and $d < q$, then for any $a \in \mathbb{Z}$, we have*

$$\sum_{\substack{n=1 \\ n \equiv a \bmod d}}^{q} \chi(n) = 0.$$

Proof

- Assume that condition (i) is true. If χ is primitive, then there is $m \in \mathbb{Z}$ satisfying $m \equiv 1 \pmod{d}$ and $(m, q) = 1$ such that $\chi(m) \neq 1$. Then

$$S = \sum_{\substack{n=1 \\ n \equiv a \bmod d}}^{q} \chi(n) = \sum_{\substack{n=1 \\ n \equiv am \bmod d}}^{q} \chi(n) = \sum_{k=1}^{q/d} \chi(am + dkm)$$

$$= \chi(m) \sum_{\substack{n=1 \\ n \equiv a \bmod d}}^{q} \chi(n) = \chi(m)S.$$

- Since $\chi(m) \neq 1$, we deduce that $S = 0$, and we are done.
- Assume that condition (ii) is true. Let $d \mid q$ and $d < q$, and $a = 1$. Then

$$\sum_{\substack{n=1 \\ n \equiv 1 \bmod d}}^{q} \chi(n) = 0,$$

and since $\chi(1) = 1$, there must be $2 \leq m \leq q$ such that $0 \neq \chi(m) \neq 1$.

- But $m \equiv 1 \pmod{d}$ and $(m, q) = 1$, hence by the previous theorem χ must be primitive as desired. □

Primitive characters further characterizations

Lemma

Suppose that $(q_1, q_2) = 1$ *and let* χ_i *be a Dirichlet character* $\pmod{q_i}$ *for* $i \in [2]$. *Then* $\chi = \chi_1\chi_2$ *is primitive* $\pmod{q_1q_2}$ *if and only if* χ_1 *and* χ_2 *are both primitive.*

Proof.

- We first prove the implication ($\Longrightarrow$). Let d_i be the conductor of χ_i. If $(mn, q_1q_2) = 1$ and $m \equiv n \mod d_1d_2$, then $\chi_i(m) = \chi_i(n)$, hence d_1d_2 is a quasiperiod of χ. Thus $d_1d_2 = q_1q_2$ since χ is primitive. Therefore, $d_1 = q_1$ and $d_2 = q_2$ since $d_i \mid q_i$ for $i \in [2]$.
- We now prove the reverse implication ($\Longleftarrow$). Let d be the conductor of χ. Set $d_i = (d, q_i)$ for $i \in [2]$. We show that d_1 is a quasiperiod of χ_1. Suppose $(mn, q_1) = 1$ and $m \equiv n \pmod{d_1}$. Choose $m_0, n_0 \in \mathbb{Z}$ so that

$$m_0 \equiv m \pmod{q_1}, \quad \text{and} \quad n_0 \equiv n \pmod{q_1},$$
$$m_0 \equiv 1 \pmod{q_2}, \quad \text{and} \quad n_0 \equiv 1 \pmod{q_2}.$$

Thus $m_0 \equiv n_0 \pmod{d_1}$ and $m_0 \equiv n_0 \pmod{d_2}$, hence $m_0 \equiv n_0 \pmod{d_1d_2}$, but $d_1d_2 = (d, q_1q_2) = d$ since $d \mid q_1q_2$. Consequently, $m_0 \equiv n_0 \pmod{d}$ and $(m_0n_0, q_1q_2) = 1$, yielding $\chi(m_0) = \chi(n_0)$. Therefore, d_1 is a quasiperiod of χ_1, since $\chi_1(m) = \chi(m_0) = \chi(n_0) = \chi_1(n)$. Since χ_1 is primitive, we must have $d_1 = q_1$. Similarly, $d_2 = q_2$, and finally $d = q_1q_2$. □

Explicit formulas for the Dirichlet characters

- By the Chinise reminder theorem, or more abstractly, by the structure theorem for finite abelian groups if $q = \prod_{p\in\mathbb{P}} p^{\alpha_p(q)}$, then

$$(\mathbb{Z}/q\mathbb{Z})^\times \equiv \bigotimes_{p^{\alpha_p(q)}|q} (\mathbb{Z}/p^{\alpha_p(q)}\mathbb{Z})^\times.$$

  In other words, any multiplicative group modulo q is isomorphic to the direct product of multiplicative groups modulo prime powers.
- Therefore, understanding Dirichlet characters on $(\mathbb{Z}/q\mathbb{Z})^\times$, is reduced to understand Dirichlet characters on $(\mathbb{Z}/p^{\alpha_p(q)}\mathbb{Z})^\times$.
- Let $p \in \mathbb{P}$ be an odd prime number. Then the corresponding group $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is cyclic. This means that there exists a primitive root g in $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. In fact, we can find a primitive root in $(\mathbb{Z}/p\mathbb{Z})^\times$, which is also a primitive root in $(\mathbb{Z}/p^\beta\mathbb{Z})^\times$ for all $\beta \in \mathbb{Z}_+$.
- If $(n,p) = 1$ let $\nu(n) = \operatorname{ind}_g n \pmod{p^\alpha}$, so that $\nu(n)$ is the unique integer satisfying the conditions

$$n \equiv g^{\nu(n)} \pmod{p^\alpha}, \quad \text{where} \quad 0 \le \nu(n) < \varphi(p^\alpha).$$

Explicit formulas for the Dirichlet characters

- For $h \in \mathbb{N}_{<\varphi(p^\alpha)}$, define χ_h by the relations

$$\chi_h(n) = \chi_h(n; p^\alpha) = \begin{cases} e(h\nu(n)/\varphi(p^\alpha)) & \text{if } p \nmid n, \\ 0 & \text{if } p \mid n. \end{cases}$$

- Using the properties of indices $\nu(n) = \operatorname{ind}_g n \pmod{p^\alpha}$ it is easy to verify that χ_h is completely multiplicative and periodic with period p^α, so χ_h is a Dirichlet character $\bmod p^\alpha$, with χ_0 being the principal character. This verification is left as an exercise!
- Since

$$\chi_h(g) = e(h/\varphi(p^\alpha))$$

the characters $\chi_0, \chi_1, \ldots, \chi_{\varphi(p^\alpha)-1}$ are distinct because they take distinct values at g. Therefore, since there are $\varphi(p^\alpha)$ such functions they represent all the Dirichlet characters $\pmod{p^\alpha}$.

- The same construction works for the modulus 2^α if $\alpha = 1$ or $\alpha = 2$, using $g = 3$ as the primitive root.

Explicit formulas for the Dirichlet characters

- If $\alpha \geq 3$ the modulus 2^α has no primitive root and a slightly different construction is needed to obtain the characters mod 2^α.
- We know that for every $\alpha \geq 3$, and every odd integer $n \in \mathbb{Z}$ there is a uniquely determined integer $\nu(n)$ such that

$$n \equiv (-1)^{(n-1)/2} 5^{\nu(n)} \pmod{2^\alpha}, \quad \text{with} \quad 1 \leq \nu(n) \leq \varphi(2^\alpha)/2.$$

- With this knowledge we can construct all the characters $\pmod{2^\alpha}$ if $\alpha \geq 3$. Let

$$f(n) = \begin{cases} (-1)^{(n-1)/2} & \text{if } n \text{ is odd}, \\ 0 & \text{if } n \text{ is even}, \end{cases}$$

and let

$$g(n) = \begin{cases} e(\nu(n)/2^{\alpha-2}) & \text{if } n \text{ is odd}, \\ 0 & \text{if } n \text{ is even}, \end{cases}$$

where $\nu(n)$ is the integer given in the previous item.

- Then it is easy to verify that each of f and g is a character mod 2^α. So is each product

$$\chi_{a_1,a_2}(n) = \chi_{a_1,a_2}(n; 2^\alpha) = f(n)^{a_1} g(n)^{a_2} = e\left(\frac{a_1(n-1)}{4} + \frac{a_2\nu(n)}{2^{\alpha-2}}\right),$$

where $a_1 \in [2]$ and $a_2 \in [\varphi(2^\alpha)/2]$. Moreover these $\varphi(2^\alpha)$ characters are distinct so they represent all the characters mod 2^α.

Real Dirichlet characters

- If χ is a real-valued Dirichlet character $\pmod m$ and $(n,m)=1$, the number $\chi(n)$ is both a root of unity and real, so $\chi(n)=\pm 1$. From the construction from the previous slides we can determine all real Dirichlet characters $\pmod{p^\alpha}$.

Theorem (Exercise)

For an odd prime $p\in\mathbb{P}$ and $\alpha\in\mathbb{Z}_+$, consider the Dirichlet characters

$$\chi_h(n)=\chi_h(n;p^\alpha)=\begin{cases} e(h\nu(n)/\varphi(p^\alpha)) & \text{if } p\nmid n,\\ 0 & \text{if } p\mid n,\end{cases}\qquad \text{for}\quad h\in[\mathbb{N}_{<\varphi(p^\alpha)}].$$

Then χ_h is real if, and only if, $h=0$ or $h=\varphi(p^\alpha)/2$. Hence there are exactly two real characters $\pmod{p^\alpha}$.

- The next theorem describes the real characters $\bmod 2^\alpha$ when $\alpha\geq 3$.

Theorem (Exercise)

If $\alpha\geq 3$, consider the Dirichlet characters

$$\chi_{a_1,a_2}(n)=\chi_{a_1,a_2}(n;2^\alpha)=e\left(\frac{a_1(n-1)}{4}+\frac{a_2\nu(n)}{2^{\alpha-2}}\right),$$

where $a_1\in[2]$ and $a_2\in[\varphi(2^\alpha)/2]$. Then χ_{a_1,a_2} is real if, and only if, $a_2=\varphi(2^\alpha)/2$ or $a_2=\varphi(2^\alpha)/4$. Hence there are exactly four real characters $\pmod 2^\alpha$ if $\alpha\geq 3$.

Primitive Dirichlet characters

Theorem (Exercise)

For an odd prime $p \in \mathbb{P}$ and $\alpha \geq 2$, consider the Dirichlet characters

$$\chi_h(n) = \chi_h(n; p^\alpha) = \begin{cases} e(h\nu(n)/\varphi(p^\alpha)) & \text{if } p \nmid n, \\ 0 & \text{if } p \mid n, \end{cases} \quad \text{for} \quad h \in [\mathbb{N}_{<\varphi(p^\alpha)}].$$

Then χ_h is primitive $\bmod p^\alpha$ if, and only if, $p \nmid h$.

Theorem (Exercise)

If $\alpha \geq 3$, consider the Dirichlet characters

$$\chi_{a_1,a_2}(n) = \chi_{a_1,a_2}(n; 2^\alpha) = e\left(\frac{a_1(n-1)}{4} + \frac{a_2\nu(n)}{2^{\alpha-2}}\right),$$

where $a_1 \in [2]$ and $a_2 \in [\varphi(2^\alpha)/2]$. Then χ_{a_1,a_2} is primitive $\pmod{2^\alpha}$ if, and only if, a_2 is odd.

Remarks

- The character corresponding to $h = 0$ is the principal character.
- When $\alpha = 1$ the quadratic character $\chi_p(n) = (n \mid p)$ is the only other real character $\pmod p$.
- For the moduli $m = 1, 2$ and 4, all the Dirichlet characters are real.
- There is only one primitive character modulo 4 defined for all odd positive integers n by

$$\chi_4(n) = (-1)^{(n-1)/2}.$$

- There are two primitive characters modulo 8 defined for all odd positive integers n by

$$\chi_8(n) = (-1)^{(n^2-1)/8}, \quad \text{and} \quad \chi_4\chi_8(n) = (-1)^{(n-1)/2+(n^2-1)/8}.$$

- If $q = p^\alpha$ is a prime power, the only real primitive characters of conductor q are $\chi_4, \chi_8, \chi_4\chi_8$ and χ_p. Every real primitive character can be obtained as the product of these characters.
- This implies that the conductor of a real primitive character is of the form $1, m, 4m$ or $8m$ where m is a positive odd squarefree integer.

Dirichlet's theorem

Theorem (Dirichlet)

Let $a, q \in \mathbb{Z}_+$ be coprime integers. Then there are infinitely many prime numbers $p \in \mathbb{P}$ such that $p \equiv a \pmod{q}$.

- Around 1837, Dirichlet succeeded in using a generalization of Euler's proof $\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty$ and some group-theoretic tools.
- More precisely, Dirichlet proved the divergence of the series

$$\sum_{p\equiv a(\bmod q)} \frac{1}{p}$$

by discovering a clever expression for the characteristic function

$$\mathbf{1}_{q,a}(n) = \begin{cases} 1, & \text{if } n \equiv a \pmod{q}, \\ 0, & \text{otherwise .} \end{cases}$$

and showing that

$$\lim_{\sigma\to 1^+} \sum_{p\in\mathbb{P}} \frac{\mathbf{1}_{q,a}(p)}{p^\sigma} = \infty.$$

The first key identity

Proposition

Let $a, q \in \mathbb{Z}_+$ be coprime integers and define $\mathbf{1}_{q,a}(n)$ as

$$\mathbf{1}_{q,a}(n) = \begin{cases} 1, & \text{if } n \equiv a \pmod{q}, \\ 0, & \text{otherwise.} \end{cases}$$

For all $n \in \mathbb{Z}_+$ we have

$$\mathbf{1}_{q,a}(n) = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \chi(n)\overline{\chi}(a)$$

where the summation is taken over all Dirichlet characters modulo q.

Proof.

- This readily follows from the identity $a, n \in \mathbb{Z}$, then

$$\sum_{\chi \pmod{q}} \chi(n)\overline{\chi}(a) = \begin{cases} \varphi(q) & \text{if } (n,q) = (a,q) = 1 \text{ and } n \equiv a \pmod{q}, \\ 0 & \text{otherwise,} \end{cases}$$

which is simply the orthogonality relation. □

The second key identity

Proposition

Let $a, q \in \mathbb{Z}_+$ be coprime integers and $N > 1$ be an integer. Then we have

$$\sum_{\substack{p \leq N \\ p \equiv a \,(\mathrm{mod}\, q)}} \frac{1}{p} = \frac{1}{\varphi(q)} \sum_{\substack{p \leqslant N \\ (p,q)=1}} \frac{1}{p} + \frac{1}{\varphi(q)} \sum_{\substack{\chi \,(\mathrm{mod}\, q) \\ \chi \neq \chi_0}} \overline{\chi}(a) \sum_{p \leqslant N} \frac{\chi(p)}{p}$$

Proof.

- By the previous proposition we obtain

$$\sum_{\substack{p \leqslant N \\ p \equiv a \,(\mathrm{mod}\, q)}} \frac{1}{p} = \sum_{p \leqslant N} \frac{\mathbf{1}_{q,a}(p)}{p} = \frac{1}{\varphi(q)} \sum_{\chi \,(\mathrm{mod}\, q)} \overline{\chi}(a) \sum_{p \leqslant N} \frac{\chi(p)}{p}.$$

- We split the sum according to $\chi = \chi_0$ or $\chi \neq \chi_0$, leading to the claim.

This completes the proof. □

Simple bounds for sums of characters

Corollary

Let $a, q \in \mathbb{Z}_+$ be coprime integers and $N > 1$ be an integer. Then for any arithmetic function $f : \mathbb{N} \to \mathbb{C}$ the following holds

$$\sum_{\substack{n \leq N \\ n \equiv a (\bmod q)}} f(n) = \frac{1}{\varphi(q)} \sum_{\substack{n \leq N \\ (n,q)=1}} f(n) + \frac{1}{\varphi(q)} \sum_{\substack{\chi (\bmod q) \\ \chi \neq \chi_0}} \overline{\chi}(a) \sum_{n \leqslant N} \chi(n) f(n).$$

Proposition

For all non-principal Dirichlet characters χ modulo q and all non-negative integers $M < N$, we have

$$\left| \sum_{n=M+1}^{N} \chi(n) \right| \leq \varphi(q).$$

Proof

- Let $K = q\lfloor (N-M-1)/q \rfloor$. By the orthognality relation, for all $\chi \neq \chi_0$, we have
$$\sum_{a(\bmod q)} \chi(a) = 0.$$
- Hence, by periodicity, we obtain
$$\sum_{n=M+1}^{M+K} \chi(n) = \sum_{j=1}^{K/q} \sum_{n=M+1+(j-1)q}^{M+jq} \chi(n) = \sum_{j=1}^{K/q} \sum_{n=M+1}^{M+q} \chi(n) = 0.$$
- The interval $(M+K, N]$ contains at most q integers $n_1, \ldots, n_r$ with $r \in [q]$. Denoting by n_i the residue class of the integer n_i in $(\mathbb{Z}/q\mathbb{Z})^\times$, we obtain
$$\left| \sum_{n=M+1}^{N} \chi(n) \right| \leqslant \sum_{\substack{i=1 \\ (n_i,q)=1}}^{r} |\chi(n_i)| \leqslant \sum_{\substack{n \leqslant q \\ (n,q)=1}} 1 = \varphi(q)$$

as asserted. □

Sums involving Dirichlet characters

Proposition

Let $F \in C^1((1,+\infty))$ be a decreasing function such that $F > 0$ and $\lim_{x\to\infty} F(x) = 0$. For all non-principal Dirichlet characters χ modulo q and all real numbers $x \geqslant 1$, we have

$$\left|\sum_{k>x} \chi(k)F(k)\right| \leqslant 2qF(x).$$

Proof.

- If $(b_k)_{k\in\mathbb{Z}} \subseteq \mathbb{R}_+$ is a monotone, then

$$\left|\sum_{k=m+1}^{n} a_k b_k\right| \leq 2\max\{b_{m+1}, b_n\} \max_{m\leqslant k\leqslant n} |s_k|,$$

  where $s_k = \sum_{x<n\leq k} \chi(n)$.
- Applying this with $a_k = \chi(k)$ and $b_k = F(k)$ the result follows.

This completes the proof. □

Definition of L-functions

L-functions

Let χ be a Dirichlet character modulo $q \geqslant 2$. The L-function, or L-series, corresponding to χ is the Dirichlet series of χ, given by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad \text{for all} \quad s = \sigma + it \in \mathbb{C} \quad \text{with } \sigma > 1.$$

- By the absolute convergence of $L(s,\chi)$ for $s \in \mathbb{C}$ with $\sigma > 1$ we have

$$L(s,\chi) = \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

- If $\chi = \chi_0$ we also have

$$L(s,\chi_0) = \sum_{\substack{n=1 \\ (n,q)=1}}^{\infty} \frac{1}{n^s} = \zeta(s) \prod_{p \mid q} \left(1 - \frac{1}{p^s}\right).$$

- If $\chi \neq \chi_0$ then $L(s,\chi)$ converges for all $s \in \mathbb{C}$ with $\sigma > 0$, by the previous proposition.

Dirichlet's theorem: the first key step

Theorem

If $\chi \neq \chi_0$ is a non-principal Dirichlet character modulo q satisfying

$$L(1, \chi) \neq 0,$$

then the series

$$\sum_{p \in \mathbb{P}} \frac{\chi(p)}{p}$$

converges.

Proof.

Let $N \geqslant 2$ be an integer. We will estimate in two different ways the sum

$$\sum_{1 \leq n \leqslant N} \frac{\chi(n) \log n}{n}.$$

- Since $\log n = \Lambda \star 1(n)$, we have

$$\sum_{n \leqslant N} \frac{\chi(n) \log n}{n} = \sum_{n \leqslant N} \frac{\chi(n)}{n} \sum_{d \mid n} \Lambda(d).$$

Proof

- Interchanging the order of summation and using multiplicativity of the Dirichlet characters we can write

$$\begin{aligned}\sum_{n\leqslant N}\frac{\chi(n)\log n}{n} &= \sum_{d\leqslant N}\Lambda(d)\sum_{\substack{n\leqslant N\\ d|n}}\frac{\chi(n)}{n}\\ &= \sum_{d\leqslant N}\Lambda(d)\sum_{k\leqslant N/d}\frac{\chi(kd)}{kd}\\ &= \sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d}\sum_{k\leqslant N/d}\frac{\chi(k)}{k}\\ &= L(1,\chi)\sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d} - \sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d}\sum_{k>N/d}\frac{\chi(k)}{k}.\end{aligned}$$

- Since $L(1,\chi)\neq 0$, we infer that

$$\sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d} = \frac{1}{L(1,\chi)}\left(\sum_{n\leqslant N}\frac{\chi(n)\log n}{n} + \sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d}\sum_{k>N/d}\frac{\chi(k)}{k}\right).$$

Proof

- By the previous proposition, since $|\sum_{k>N/d} \frac{\chi(k)}{k}| \leq 2dq/N$, we obtain

$$\left| \sum_{d\in[N]} \frac{\chi(d)\Lambda(d)}{d} \sum_{k>N/d} \frac{\chi(k)}{k} \right| \leq \frac{2q}{N} \sum_{d\in[N]} \Lambda(d) = \frac{2q\Psi(N)}{N}.$$

- By using $\Psi(N) < 2N$ we have

$$\left| \sum_{d\in[N]} \frac{\chi(d)\Lambda(d)}{d} \sum_{k>N/d} \frac{\chi(k)}{k} \right| < 4q.$$

- Inserting this bound to the last identity in the previous slide we have

$$\left| \sum_{d\in[N]} \frac{\chi(d)\Lambda(d)}{d} \right| < \frac{1}{|L(1,\chi)|} \left(\left| \sum_{n\in[N]} \frac{\chi(n)\log n}{n} \right| + 4q \right).$$

- By partial summation we obtain

$$\begin{aligned} \sum_{n\leqslant N} \frac{\chi(n)\log n}{n} &= \frac{\chi(2)\log 2}{2} + \sum_{3\leqslant n\leqslant N} \frac{\chi(n)\log n}{n} \\ &= \frac{\chi(2)\log 2}{2} + \frac{\log N}{N} \sum_{3\leqslant n\leqslant N} \chi(n) + \int_3^N \frac{\log t - 1}{t^2} \left(\sum_{3\leqslant n\leqslant t} \chi(n) \right) dt. \end{aligned}$$

Proof

- Using the fact that $|\sum_{3\leqslant n\leqslant N}\chi(n)|<q$, we obtain

$$\left|\sum_{n\leqslant N}\frac{\chi(n)\log n}{n}\right|\leq\frac{\log 2}{2}+q\left(\frac{\log N}{N}+\int_3^N\frac{\log t-1}{t^2}dt\right)$$
$$=\frac{\log 2}{2}+\frac{q\log 3}{3}<q.$$

- Inserting this bound to the last estimates

$$\left|\sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d}\right|<\frac{5q}{|L(1,\chi)|}.$$

- We also have

$$\sum_{p\leqslant N}\frac{\chi(p)\log p}{p}=\sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d}-\sum_{p\leqslant N}\log p\sum_{\alpha=2}^{\lfloor\log N/\log p\rfloor}\frac{\chi(p^\alpha)}{p^\alpha}.$$

- The second sum is bounded since

$$\left|\sum_{p\leqslant N}\log p\sum_{\alpha=2}^{\lfloor\log N/\log p\rfloor}\frac{\chi(p^\alpha)}{p^\alpha}\right|\leqslant\sum_{p\leqslant N}\log p\sum_{\alpha=2}^{\lfloor\log N/\log p\rfloor}\frac{1}{p^\alpha}\leqslant\sum_{p\in\mathbb{P}}\frac{\log p}{p(p-1)}<C,$$

for some constant $C\in\mathbb{R}_+$, which in fact we can take $C=1$.

Proof

- Now by partial summation we can write

$$\sum_{p\leqslant N}\frac{\chi(p)}{p}=\frac{1}{\log N}\sum_{p\leqslant N}\frac{\chi(p)\log p}{p}+\int_2^N\left(\sum_{p\leqslant t}\frac{\chi(p)\log p}{p}\right)\frac{dt}{t(\log t)^2},$$

so that by above we obtain

$$\begin{aligned}\left|\sum_{p\leqslant N}\frac{\chi(p)}{p}\right|<&\frac{1}{\log N}\left(\left|\sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d}\right|+C\right)\\&+\int_2^N\left(\left|\sum_{d\leqslant t}\frac{\chi(d)\Lambda(d)}{d}\right|+C\right)\frac{dt}{t(\log t)^2}.\end{aligned}$$

- The estimate $\left|\sum_{d\leqslant N}\frac{\chi(d)\Lambda(d)}{d}\right|<\frac{5q}{|L(1,\chi)|}$ provides

$$\left|\sum_{p\leqslant N}\frac{\chi(p)}{p}\right|<\frac{1}{\log 2}\left(\frac{5q}{|L(1,\chi)|}+C\right),$$

which completes the proof. □

Dirichlet's theorem: the second key step

Theorem

If $\chi \neq \chi_0$ is a non-principal Dirichlet character modulo q, then

$$L(1,\chi) \neq 0.$$

Proof.

- We form the product of all $L(s,\chi)$:

$$F(s) = \prod_{\chi(\bmod q)} L(s,\chi) = \prod_{p\nmid q} \prod_{\chi(\bmod q)} \frac{1}{1-(\chi(p)/p^s)} \quad \text{for all} \quad s>1.$$

- If m is the smallest positive integer such that $p^m \equiv 1 \pmod{q}$, then $\chi(p)$ is an m-th root of unity, say ε. All such ε occur with the same multiplicity $l = \phi(q)/m$ as χ runs over all the characters modulo q.
- This means that

$$\prod_{\chi(\bmod q)} \left(1-\frac{\chi(p)}{p^s}\right) = \prod_{\varepsilon} \left(1-\frac{\varepsilon}{p^s}\right)^l,$$

where ε runs over all the m-th roots of unity.

Proof

- Now since
$$\prod_{\varepsilon}(x-\varepsilon) = x^m - 1,$$
we have that
$$\prod_{\varepsilon}\left(1-\frac{\varepsilon}{x}\right) = 1 - \frac{1}{x^m}.$$
- Therefore
$$\prod_{\varepsilon}\left(1-\frac{\varepsilon}{p^s}\right) = 1 - \frac{1}{p^{ms}},$$
so that
$$\prod_{\chi(\bmod q)}\left(1-\frac{\chi(p)}{p^s}\right) = \left(1-\frac{1}{p^{ms}}\right)^l \leq 1 - \frac{1}{p^{lms}}.$$
- Here we used the inequality $(1-x)^n \leq 1-x^n$, which is clearly valid for all $n \geq 1$ and $x \in [0,1]$. Setting $h = \phi(q) = lm$, we thus have
$$F(s) = \prod_{\chi(\bmod q)} L(s,\chi) \geq \prod_{p\nmid q}\frac{1}{1-(1/p^{hs})} = \zeta(hs)\prod_{p\mid q}\left(1-\frac{1}{p^{hs}}\right).$$

Proof

- This implies that for $s > 1$, that

$$F(s) = \prod_{\chi(\bmod q)} L(s,\chi) \geq \zeta(hs) \prod_{p|q} \left(1 - \frac{1}{p}\right) > \frac{\phi(q)}{q}. \qquad (*)$$

- We show that (*) precludes that two or more of the $L(1,\chi)$'s vanish.
- Indeed, assume that $L(1,\chi_1) = L(1,\chi_2) = 0$ for two characters χ_1 and χ_2. Clearly, $\chi_1, \chi_2 \neq \chi_0$. Then $F(s)$ would contain, besides other factors that are continuous (thus bounded) at $s = 1$, the factor

$$\begin{aligned} &L(s,\chi_0)\, L(s,\chi_1)\, L(s,\chi_2) \\ &\quad = L(s,\chi_0)\,(s-1)^2\,(L'(1,\chi_1) + \eta_1(s))\,(L'(1,\chi_2) + \eta_2(s)), \end{aligned}$$

  where $\lim_{s\to 1} \eta_1(s) = \lim_{s\to 1} \eta_2(s) = 0$.
- The Riemann zeta function has a simple pole at $s = 1$, and $L(s,\chi_0) = \zeta(s) \prod_{p|k} \left(1 - \frac{1}{p^s}\right)$, thus

$$\lim_{s\to 1} (s-1) L(s,\chi_0) = \phi(q)/q,$$

  and we would get that $\lim_{s\to 1} F(s) = 0$, which would contradict (*).

Proof

- If now $L(1,\chi)=0$ for some complex character χ (that is, which assumes complex non-real values), then $\overline{\chi}$ is also a character of modulus q which is distinct from χ, and clearly $L(1,\overline{\chi})=\overline{L(1,\chi)}=0$. But we have just seen that this is impossible.
- Thus, if $L(s,\chi)=0$ for some χ, then χ is unique and real (it assumes only the values ± 1). In order to complete the proof, we will show that $L(1,\chi)\neq 0$ for all real non-principal characters as well.
- From now on, we assume that χ is real non-principal character.
- Note that $\chi:\mathbb{N}\to\{0,\pm 1\}$ is, in particular, a multiplicative function. So, if we let

$$f(n)=\sum_{d|n}\chi(d)=1*\chi,$$

then f is also multiplicative.

- Note further that since $\chi(p)=\pm 1$, we get that

$$f\left(p^l\right)=\chi(1)+\chi(p)+\cdots+\chi\left(p^l\right)\geq 0$$

for all $l\in\mathbb{Z}_+$, and, in fact, $f\left(p^l\right)\geq 1$ whenever $2\mid l$.

Proof

- Using the fact that f is multiplicative, we get that $f(m^2) \geq 1$. Thus,

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^{1/2}} \geq \sum_{m \in \mathbb{Z}_+} \frac{f(m^2)}{m} \geq \sum_{m \in \mathbb{Z}_+} \frac{1}{m} = \infty.$$

- Let us take a closer look at this divergence. We have

$$G(x) = \sum_{n \leq x} \frac{f(n)}{n^{1/2}} = \sum_{n \leq x} \frac{1}{n^{1/2}} \sum_{d|n} \chi(d) = \sum_{td \leq x} \frac{\chi(d)}{(td)^{1/2}}.$$

- By using the Dirichlet hyperbola principle and splitting summation according to whether $d \leq \sqrt{x}$ or $d > \sqrt{x}$, we obtain

$$\begin{aligned} G(x) &= \sum_{1 \leq d \leq \sqrt{x}} \frac{\chi(d)}{d^{1/2}} \sum_{1 \leq t \leq x/d} \frac{1}{t^{1/2}} + \sum_{t \leq \sqrt{x}} \frac{1}{t^{1/2}} \sum_{\sqrt{x+1} \leq d \leq x/t} \frac{\chi(d)}{d^{1/2}} \\ &= G_1(x) + G_2(x). \end{aligned}$$

Proof

- By Abel's summation formula, we have that

$$\begin{aligned}
\sum_{1\le t\le y}\frac{1}{t^{1/2}} =& \frac{\lfloor y\rfloor}{y^{1/2}} - \int_1^t \lfloor t\rfloor \left(\frac{1}{t^{1/2}}\right)' dt = \frac{y-\{y\}}{y^{1/2}} + \frac{1}{2}\int_1^y \frac{t-\{t\}}{t^{3/2}}dt \\
=& y^{1/2} + O\left(\frac{1}{y^{1/2}}\right) + \frac{1}{2}\int_1^y \frac{dt}{t^{1/2}} - \frac{1}{2}\int_1^y \frac{\{t\}}{t^{3/2}}dt \\
=& 2y^{1/2} - 1 - \frac{1}{2}\left(\int_1^\infty \frac{\{t\}}{t^{3/2}}dt - \int_y^\infty \frac{\{t\}}{t^{3/2}}dt\right) + O\left(\frac{1}{y^{1/2}}\right) \\
=& 2y^{1/2} + \left(-1 - \frac{1}{2}\int_1^\infty \frac{\{t\}}{t^{3/2}}dt\right) + O\left(\frac{1}{y^{1/2}} + \int_y^\infty \frac{dt}{t^{3/2}}\right) \\
=& 2y^{1/2} + C + O\left(\frac{1}{y^{1/2}}\right),
\end{aligned}$$

where C is the constant given by

$$C = -1 - \frac{1}{2}\int_1^\infty \frac{\{t\}}{t^{3/2}}dt.$$

Proof

- Hence, we obtain

$$G_1(x) = \sum_{1\le d\le\sqrt{x}} \frac{\chi(d)}{d^{1/2}} \left(2\sqrt{\frac{x}{d}} + C + O\left(\sqrt{\frac{d}{x}}\right)\right)$$

$$= 2\sqrt{x} \sum_{1\le d\le\sqrt{x}} \frac{\chi(d)}{d} + C \sum_{1\le d\le\sqrt{x}} \frac{\chi(d)}{d^{1/2}} + O\left(\frac{\sqrt{x}}{\sqrt{x}}\right)$$

$$= 2\sqrt{x} \left(\sum_{d=1}^{\infty} \frac{\chi(d)}{d} - \sum_{d>\sqrt{x}} \frac{\chi(d)}{d}\right) + O(1),$$

where we used the fact that

$$\sum_{1\le d\le\sqrt{x}} \frac{\chi(d)}{d^{1/2}} = L(1/2,\chi) + o(1) = O(1),$$

$$\sum_{d>\sqrt{x}} \frac{\chi(d)}{d} = O\left(\frac{1}{\sqrt{x}}\right).$$

- Hence, we conclude that

$$G_1(x) = 2\sqrt{x}L(1,\chi) + O(1).$$

Proof

- We are left with examining the size of

$$G_2(x) = \sum_{1 \le t \le \sqrt{x}} \frac{1}{t^{1/2}} \sum_{\sqrt{x+1} \le d \le x/t} \frac{\chi(d)}{d^{1/2}}.$$

- The inner sums are bounded by

$$\left| \sum_{\sqrt{x+1} \le d \le x/t} \frac{\chi(d)}{d^{1/2}} \right| = O\left(\frac{1}{x^{1/4}}\right).$$

Therefore, $G_2(x) = O(1)$, since

$$G_2(x) = O\left(\frac{1}{x^{1/4}} \sum_{1 \le t \le x^{1/2}} \frac{1}{t^{1/2}}\right) = O\left(\frac{1}{x^{1/4}}\left(1 + \int_1^{\sqrt{x}} \frac{dt}{t^{1/2}}\right)\right)$$

$$= \frac{1}{x^{1/4}}\left(1 + 2x^{1/4}\right) = O(1),$$

- Combining the above estimates, we obtain

$$G(x) = G_1(x) + G_2(x) = 2\sqrt{x}L(1,\chi) + O(1)$$

Since we know that $G(x)$ tends to infinity with x and, plainly, that this can happen only if $L(1,\chi) \neq 0$. □

Proof of Dirichlet's theorem

Theorem (Dirichlet)

Let $a, q \in \mathbb{Z}_+$ be coprime integers. Then there are infinitely many prime numbers $p \in \mathbb{P}$ such that $p \equiv a \pmod{q}$.

Proof.

- We know that

$$\sum_{\substack{p \leq N \\ p \equiv a \pmod{q}}} \frac{1}{p} = \frac{1}{\varphi(q)} \sum_{\substack{p \leqslant N \\ (p,q)=1}} \frac{1}{p} + \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \overline{\chi}(a) \sum_{p \leqslant N} \frac{\chi(p)}{p}. \qquad (*)$$

- It is easy to see that

$$\lim_{N \to \infty} \sum_{\substack{p \leqslant N \\ (p,q)=1}} \frac{1}{p} = \infty,$$

  since it only differs from $\sum_{p \in \mathbb{P}_{\leq N}} 1/p$ by a finite number of terms.
- On the other hand, we have shown $\sum_{p \leqslant N} \frac{\chi(p)}{p}$ converges, thus we have

$$\left| \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \overline{\chi}(a) \sum_{p \leqslant N} \frac{\chi(p)}{p} \right| = O(1).$$

- Therefore, the series on the left-hand side of (*) must diverge, and consequently the Dirichlet's theorem follows as desired. □