Math 571 Chapter 2 Multiplicative Structures

Robert C. Vaughan

January 6, 2023

- In elementary number theory courses it is usual taught that the reduced residue classes modulo q form a cyclic group under multiplication if and only if $q = p^k$ with $p = 2$ and $k = 1$ or 2, or with $p > 2$ and all $k \geq 1$. A generator g is called a primitive root. It is often also shown that if $p = 2$ and $k \geq 3$, then every reduced residue modulo 2^k is generated by

$$(-1)^u 5^v$$

where $u = 0$ or 1 and $0 \leq v < 2^{k-2}$.

- In elementary number theory courses it is usual taught that the reduced residue classes modulo q form a cyclic group under multiplication if and only if $q = p^k$ with $p = 2$ and $k = 1$ or 2, or with $p > 2$ and all $k \ge 1$. A generator g is called a primitive root. It is often also shown that if $p = 2$ and $k \ge 3$, then every reduced residue modulo 2^k is generated by

$$(-1)^u 5^v$$

where $u = 0$ or 1 and $0 \le v < 2^{k-2}$.
- One can then use the Chinese Remainder Theorem to express each residue modulo q in a suitable form. This was all first proved by Gauss.

- In elementary number theory courses it is usual taught that the reduced residue classes modulo q form a cyclic group under multiplication if and only if $q = p^k$ with $p = 2$ and $k = 1$ or 2, or with $p > 2$ and all $k \geq 1$. A generator g is called a primitive root. It is often also shown that if $p = 2$ and $k \geq 3$, then every reduced residue modulo 2^k is generated by

$$(-1)^u 5^v$$

where $u = 0$ or 1 and $0 \leq v < 2^{k-2}$.
- One can then use the Chinese Remainder Theorem to express each residue modulo q in a suitable form. This was all first proved by Gauss.
- It is also an example of the theorem, usually proved in abstract algebra courses, that each abelian group is a direct product of cyclic groups. The methods of abstract algebra do not necessarily give explicit representations, which are sometimes the easiest way of seeing things.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.
- A Dirichlet character is an arithmetical function $\chi : \mathbb{N} \to \mathbb{C}$ with the following properties.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.
- A Dirichlet character is an arithmetical function $\chi : \mathbb{N} \to \mathbb{C}$ with the following properties.
- 1. χ is totally multiplicative.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.
- A Dirichlet character is an arithmetical function $\chi : \mathbb{N} \to \mathbb{C}$ with the following properties.
- 1. χ is totally multiplicative.
- 2. χ has period q for some $q \in \mathbb{N}$.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.
- A Dirichlet character is an arithmetical function $\chi : \mathbb{N} \to \mathbb{C}$ with the following properties.
- 1. χ is totally multiplicative.
- 2. χ has period q for some $q \in \mathbb{N}$.
- 3. If $(x, q) > 1$, then $\chi(x) = 0$.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.
- A Dirichlet character is an arithmetical function $\chi : \mathbb{N} \to \mathbb{C}$ with the following properties.
- 1. χ is totally multiplicative.
- 2. χ has period q for some $q \in \mathbb{N}$.
- 3. If $(x, q) > 1$, then $\chi(x) = 0$.
- In view of the periodicity we can immediately extend the definition to $\mathbb{Z}$.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.
- A Dirichlet character is an arithmetical function $\chi : \mathbb{N} \to \mathbb{C}$ with the following properties.
- 1. χ is totally multiplicative.
- 2. χ has period q for some $q \in \mathbb{N}$.
- 3. If $(x, q) > 1$, then $\chi(x) = 0$.
- In view of the periodicity we can immediately extend the definition to $\mathbb{Z}$.
- From the theory of multiplicative functions we have $\chi(1) = 1$.

- There is a more abstract and general treat of characters which I have put in the files section if you are interested.
- A Dirichlet character is an arithmetical function $\chi : \mathbb{N} \to \mathbb{C}$ with the following properties.
- 1. χ is totally multiplicative.
- 2. χ has period q for some $q \in \mathbb{N}$.
- 3. If $(x, q) > 1$, then $\chi(x) = 0$.
- In view of the periodicity we can immediately extend the definition to $\mathbb{Z}$.
- From the theory of multiplicative functions we have $\chi(1) = 1$.
- The special character which is 1 whenever $(x, q) = 1$ is called the principal character and is often denoted by χ_0.

- By Fermat-Euler, when $(x, q) = 1$ we have

$$1 = \chi(1) = \chi(x^{\phi(q)}) = \chi(x)^{\phi(q)},$$

- By Fermat-Euler, when $(x, q) = 1$ we have

$$1 = \chi(1) = \chi(x^{\phi(q)}) = \chi(x)^{\phi(q)},$$

- so $\chi(x)$ is a $\phi(q)$-th root of unity.

- By Fermat-Euler, when $(x, q) = 1$ we have

$$1 = \chi(1) = \chi(x^{\phi(q)}) = \chi(x)^{\phi(q)},$$

- so $\chi(x)$ is a $\phi(q)$-th root of unity.
- Also $|\chi(x)| = 1$.

- By Fermat-Euler, when $(x, q) = 1$ we have

$$1 = \chi(1) = \chi(x^{\phi(q)}) = \chi(x)^{\phi(q)},$$

- so $\chi(x)$ is a $\phi(q)$-th root of unity.
- Also $|\chi(x)| = 1$.
- Hence the number of possible characters modulo q is at most $\phi(q)^{\phi(q)}$, i.e. is finite.

- By Fermat-Euler, when $(x, q) = 1$ we have

$$1 = \chi(1) = \chi(x^{\phi(q)}) = \chi(x)^{\phi(q)},$$

- so $\chi(x)$ is a $\phi(q)$-th root of unity.
- Also $|\chi(x)| = 1$.
- Hence the number of possible characters modulo q is at most $\phi(q)^{\phi(q)}$, i.e. is finite.
- Let their number be h.

- If $(a, q) = 1$, then

$$\sum_{x=1}^{q} \chi(x) = \sum_{x=1}^{q} \chi(ax) = \chi(a) \sum_{x=1}^{q} \chi(x)$$

- If $(a, q) = 1$, then

$$\sum_{x=1}^{q} \chi(x) = \sum_{x=1}^{q} \chi(ax) = \chi(a) \sum_{x=1}^{q} \chi(x)$$

- Hence if there is an a with $(a, q) = 1$ and $\chi(a) \neq 1$, then the sum is 0.

- If $(a, q) = 1$, then

$$\sum_{x=1}^{q} \chi(x) = \sum_{x=1}^{q} \chi(ax) = \chi(a) \sum_{x=1}^{q} \chi(x)$$

- Hence if there is an a with $(a, q) = 1$ and $\chi(a) \neq 1$, then the sum is 0.
- Thus we have

Lemma 1

Suppose that χ is a character modulo q. Then

$$\frac{1}{\phi(q)} \sum_{x=1}^{q} \chi(x) = \begin{cases} 1 & (\chi = \chi_0) \\ 0 & (\chi \neq \chi_0). \end{cases}$$

- If χ_1 and χ_2 are characters modulo q_1 and q_2 respectively, then $\chi_1\chi_2$ is one modulo $q_1 q_2$.

- If χ_1 and χ_2 are characters modulo q_1 and q_2 respectively, then $\chi_1\chi_2$ is one modulo $q_1 q_2$.
- If χ is a character, then so is $\overline{\chi}$, and $\chi\overline{\chi} = \overline{\chi}\chi = \chi_0$.

- If χ_1 and χ_2 are characters modulo q_1 and q_2 respectively, then $\chi_1\chi_2$ is one modulo $q_1 q_2$.
- If χ is a character, then so is $\overline{\chi}$, and $\chi\overline{\chi} = \overline{\chi}\chi = \chi_0$.
- If χ_1, χ_2, χ_3 are characters modulo q and $\chi_1\chi_2(x) = \chi_1\chi_3(x)$ for every x, then $\chi_2 = \chi_3$.

- If χ_1 and χ_2 are characters modulo q_1 and q_2 respectively, then $\chi_1\chi_2$ is one modulo $q_1 q_2$.
- If χ is a character, then so is $\overline{\chi}$, and $\chi\overline{\chi} = \overline{\chi}\chi = \chi_0$.
- If χ_1, χ_2, χ_3 are characters modulo q and $\chi_1\chi_2(x) = \chi_1\chi_3(x)$ for every x, then $\chi_2 = \chi_3$.
- Multiply by $\overline{\chi}_1$.

- Given x with $(x,q)=1$ and any character χ_1 modulo q we have

$$\sum_{\chi \pmod q} \chi(x) = \sum_{\chi \pmod q} \chi_1\chi(x) = \chi_1(x) \sum_{\chi \pmod q} \chi(x).$$

- Given x with $(x,q)=1$ and any character χ_1 modulo q we have

$$\sum_{\chi \pmod q} \chi(x) = \sum_{\chi \pmod q} \chi_1\chi(x) = \chi_1(x) \sum_{\chi \pmod q} \chi(x).$$

- Now we have the analogue of the previous lemma.

Lemma 2

If $(x,q)=1$ and there is a χ_1 such that $\chi_1(x) \neq 1$, then

$$\sum_{\chi \pmod q} \chi(x) = 0.$$

If there is no such χ_1, then

$$\sum_{\chi \pmod q} \chi(x) = h.$$

- Given x with $(x,q)=1$ and any character χ_1 modulo q we have

$$\sum_{\chi \pmod q} \chi(x) = \sum_{\chi \pmod q} \chi_1\chi(x) = \chi_1(x) \sum_{\chi \pmod q} \chi(x).$$

- Now we have the analogue of the previous lemma.

Lemma 2

If $(x,q)=1$ and there is a χ_1 such that $\chi_1(x)\neq 1$, then

$$\sum_{\chi \pmod q} \chi(x) = 0.$$

If there is no such χ_1, then

$$\sum_{\chi \pmod q} \chi(x) = h.$$

- Can we always find such a χ_1 when $x \not\equiv 1 \pmod q$?

- The answer is yes.

Lemma 3

Given x with $(x, q) = 1$ and $x \not\equiv 1 \pmod q$ there is a character χ_1 modulo q such that $\chi_1(x) \neq 1$.

- The answer is yes.

Lemma 3

Given x with $(x,q)=1$ and $x\not\equiv 1 \pmod q$ there is a character χ_1 modulo q such that $\chi_1(x)\ne 1$.

- We give a quick and dirty proof. Since $x\not\equiv 1 \pmod q$, there is a prime power p^k such that $p^k|q$ and $p^k\nmid x-1$.

- The answer is yes.

Lemma 3

Given x with $(x, q) = 1$ and $x \not\equiv 1 \pmod{q}$ there is a character χ_1 modulo q such that $\chi_1(x) \neq 1$.

- We give a quick and dirty proof. Since $x \not\equiv 1 \pmod{q}$, there is a prime power p^k such that $p^k | q$ and $p^k \nmid x - 1$.
- If p is odd, or $p = 2$ and $k = 1$ or 2, then we can choose a primitive root g modulo p^k. Then we define a character $\chi_2(z; p^k)$ modulo p^k by taking

$$\chi_2(g^y; p^k) = e(y/\phi(p^k)).$$

- The answer is yes.

Lemma 3

Given x with $(x,q)=1$ and $x \not\equiv 1 \pmod{q}$ there is a character χ_1 modulo q such that $\chi_1(x) \neq 1$.

- We give a quick and dirty proof. Since $x \not\equiv 1 \pmod{q}$, there is a prime power p^k such that $p^k|q$ and $p^k \nmid x-1$.
- If p is odd, or $p=2$ and $k=1$ or 2, then we can choose a primitive root g modulo p^k. Then we define a character $\chi_2(z;p^k)$ modulo p^k by taking

$$\chi_2(g^y;p^k) = e(y/\phi(p^k)).$$

- Note that if $g^y \not\equiv 1 \mod p^k$, then $y \not\equiv 0 \pmod{\phi(p^k)}$.

- The answer is yes.

Lemma 3

Given x with $(x,q)=1$ and $x \not\equiv 1 \pmod{q}$ there is a character χ_1 modulo q such that $\chi_1(x) \neq 1$.

- We give a quick and dirty proof. Since $x \not\equiv 1 \pmod{q}$, there is a prime power p^k such that $p^k|q$ and $p^k \nmid x-1$.
- If p is odd, or $p=2$ and $k=1$ or 2, then we can choose a primitive root g modulo p^k. Then we define a character $\chi_2(z;p^k)$ modulo p^k by taking

$$\chi_2(g^y;p^k) = e(y/\phi(p^k)).$$

- Note that if $g^y \not\equiv 1 \mod p^k$, then $y \not\equiv 0 \pmod{\phi(p^k)}$.
- Now define

$$\chi_1(x) = \chi_2(x;p^k)\chi_0(x;qp^{-k})$$

- The answer is yes.

Lemma 3

Given x with $(x,q)=1$ and $x\not\equiv 1 \pmod q$ there is a character χ_1 modulo q such that $\chi_1(x)\neq 1$.

- We give a quick and dirty proof. Since $x\not\equiv 1 \pmod q$, there is a prime power p^k such that $p^k|q$ and $p^k\nmid x-1$.
- If p is odd, or $p=2$ and $k=1$ or 2, then we can choose a primitive root g modulo p^k. Then we define a character $\chi_2(z;p^k)$ modulo p^k by taking

$$\chi_2(g^y;p^k)=e(y/\phi(p^k)).$$

- Note that if $g^y\not\equiv 1 \mod p^k$, then $y\not\equiv 0 \pmod{\phi(p^k)}$.
- Now define

$$\chi_1(x)=\chi_2(x;p^k)\chi_0(x;qp^{-k})$$

- That leaves the case when $p=2$ and $k\geq 3$, which is a little more complicated.

- Choose y, z so that

$$x \equiv (-1)^y 5^z \pmod{2^k}$$

- Choose y, z so that

$$x \equiv (-1)^y 5^z \pmod{2^k}$$

- Now we construct χ_2 as follows.

- Choose y, z so that

$$x \equiv (-1)^y 5^z \pmod{2^k}$$

- Now we construct χ_2 as follows.
- If $y = 0$, so that $0 \le z < 2^{k-2}$, then take

$$\chi_2((-1)^u 5^v; 2^k) = e(v/2^{k-2}).$$

- Choose y, z so that

$$x \equiv (-1)^y 5^z \pmod{2^k}$$

- Now we construct χ_2 as follows.
- If $y = 0$, so that $0 \le z < 2^{k-2}$, then take

$$\chi_2((-1)^u 5^v; 2^k) = e(v/2^{k-2}).$$

- If $y = 1$, then take

$$\chi_2((-1)^u 5^v; 2^k) = e(u/2).$$

- Choose y, z so that

$$x \equiv (-1)^y 5^z \pmod{2^k}$$

- Now we construct χ_2 as follows.
- If $y = 0$, so that $0 \le z < 2^{k-2}$, then take

$$\chi_2((-1)^u 5^v; 2^k) = e(v/2^{k-2}).$$

- If $y = 1$, then take

$$\chi_2((-1)^u 5^v; 2^k) = e(u/2).$$

- Then proceed as before.

- We now can state the basic theorem for characters.

Theorem 4

There are $\phi(q)$ characters modulo q,

$$\frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a)\chi(x) = \begin{cases} 1 & x \equiv a \pmod q \ \&\ (a,q) = 1, \\ 0 & x \not\equiv a \pmod q \text{ or } (a,q) > 1. \end{cases}$$

and

$$\frac{1}{\phi(q)} \sum_{x \pmod q} \overline{\chi}_1(x)\chi_2(x) = \begin{cases} 1 & \chi_1 = \chi_2 \text{ and } (x,q) = 1, \\ 0 & \chi_1 \neq \chi_2. \end{cases}$$

- Consider the sum

$$\sum_{x \pmod q} \sum_{\chi \pmod q} \chi(x).$$

- Consider the sum

$$\sum_{x \pmod q} \sum_{\chi \pmod q} \chi(x).$$

- The sum over χ contributes 0 if $x \not\equiv 1 \pmod q$, h otherwise, so

$$= h.$$

- Interchanging the order gives

$$\sum_{\chi \pmod q} \sum_{x \pmod q} \chi(x) = \sum_{x \pmod q} \chi_0(x)$$
$$= \phi(q).$$

- Given a character χ modulo q, if there is a character χ^* modulo r, with $r|q$, such that

$$\chi(x;q) = \chi^*(x;r)\chi_0(x;q),$$

then we say that χ^* **induces** χ.

- Given a character χ modulo q, if there is a character χ^* modulo r, with $r|q$, such that

$$\chi(x; q) = \chi^*(x; r)\chi_0(x; q),$$

then we say that χ^* **induces** χ.

- If there is no such character with $r < q$, then we say that χ is **primitive**.

- Given a character χ modulo q, if there is a character χ^* modulo r, with $r|q$, such that

$$\chi(x;q) = \chi^*(x;r)\chi_0(x;q),$$

then we say that χ^* **induces** χ.
- If there is no such character with $r < q$, then we say that χ is **primitive**.
- If χ^* is primitive, then we call r the conductor of χ.

- We now give two useful criteria for primitivity.

Theorem 5

Let χ be a character modulo q. Then the following are equivalent:
(1) χ is primitive.
(2) If $d \mid q$ and $d < q$ then there is a c such that $c \equiv 1 \pmod{d}$, $(c, q) = 1$, $\chi(c) \neq 1$.
(3) If $d \mid q$ and $d < q$, then for every integer a,

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

- We now give two useful criteria for primitivity.

Theorem 5

Let χ be a character modulo q. Then the following are equivalent:
(1) χ is primitive.
(2) If $d \mid q$ and $d < q$ then there is a c such that $c \equiv 1 \pmod{d}$, $(c, q) = 1$, $\chi(c) \neq 1$.
(3) If $d \mid q$ and $d < q$, then for every integer a,

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

- The proof is usually given in Math 568, and can be found in the files section.

- Given a character χ modulo q, we define the Gauss sum $\tau(\chi)$ of χ to be

$$\tau(\chi) = \sum_{a=1}^{q} \chi(a) e(a/q).$$

- Given a character χ modulo q, we define the Gauss sum $\tau(\chi)$ of χ to be

$$\tau(\chi) = \sum_{a=1}^{q} \chi(a)e(a/q).$$

- The Gauss sum is a special case of the more general sum

$$c_\chi(n) = \sum_{a=1}^{q} \chi(a)e(an/q).$$

- Given a character χ modulo q, we define the Gauss sum $\tau(\chi)$ of χ to be

$$\tau(\chi) = \sum_{a=1}^{q} \chi(a)e(a/q).$$

- The Gauss sum is a special case of the more general sum

$$c_\chi(n) = \sum_{a=1}^{q} \chi(a)e(an/q).$$

- When χ is the principal character, this is Ramanujan's sum

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(an/q),$$

- We now show that the sum $c_\chi(n)$ is closely related to $\tau(\chi)$.

Theorem 6

Suppose that χ is a character modulo q. If $(n,q)=1$ then

$$\chi(n)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a)e(an/q), \tag{1}$$

and in particular

$$\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi}).$$

Proof.

If $(n,q)=1$ then the map $a\mapsto an$ permutes the residues modulo q, and hence

$$\chi(n)c_\chi(n)=\sum_{a=1}^{q}\chi(an)e(an/q)=\tau(\chi).$$

On replacing χ by $\overline{\chi}$, this gives (6), and (7) follows by taking $n=-1$. □

•

- There is a mulitplicative property of Gauss sums which is useful.

Theorem 7

Suppose that $(q_1, q_2) = 1$, *that* χ_i *is a character modulo* q_i *for* $i = 1, 2$, *and that* $\chi = \chi_1 \chi_2$. *Then*

$$\tau(\chi) = \tau(\chi_1)\tau(\chi_2)\chi_1(q_2)\chi_2(q_1).$$

- There is a mulitplicative property of Gauss sums which is useful.

Theorem 7

Suppose that $(q_1, q_2) = 1$*, that* χ_i *is a character modulo* q_i *for* $i = 1, 2$*, and that* $\chi = \chi_1\chi_2$*. Then*

$$\tau(\chi) = \tau(\chi_1)\tau(\chi_2)\chi_1(q_2)\chi_2(q_1).$$

- This is standard.

Proof.

By the Chinese remainder theorem, each $a \pmod{q_1q_2}$ can be written uniquely as $a_1q_2 + a_2q_1$ with $1 \le a_i \le q_i$. Thus the general term in (3) is $\chi_1(a_1q_2)\chi_2(a_2q_1)e(a_1/q_1)\ e(a_2/q_2)$, so the result follows. □

- For primitive characters the hypothesis that $(n, q) = 1$ in the first theorem can be removed.

Theorem 8

Suppose that χ is a primitive character modulo q. Then

$$\chi(n)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a)e(an/q), \tag{2}$$

holds for all n, and $|\tau(\chi)| = \sqrt{q}$.

- We will make use of this when studying the large sieve.

Proof.

It suffices to prove (2) when $(n, q) > 1$. Choose m and d so that $(m, d) = 1$ and $m/d = n/q$. Then

$$\sum_{a=1}^{q} \chi(a)e(an/q) = \sum_{h=1}^{d} e(hm/d) \sum_{\substack{a=1 \\ a\equiv h \pmod{d}}}^{q} \chi(a).$$

Since $d \mid q$ and $d < q$, the inner sum vanishes by Theorem 5. Thus (2) holds. □