

## Math 342 Tutorial

July 2, 2025

Recall a group  $G$  is cyclic if there is some  $g \in G$  for which  $G = \{g^n : n \in \mathbf{Z}\}$ . If  $G$  is finite with  $n$  distinct elements, then  $G = \{1, g, g^2, \dots, g^{n-1}\}$ . We often use the notation  $G = \langle g \rangle$  in this case.

**Question 1.** Let  $G = \langle g \rangle$  be a finite cyclic group of order  $n$ . Show that for every divisor  $d$  of  $n$ , there is a unique subgroup  $H$  of  $G$  of order  $d$ . Show, moreover, that  $H$  is cyclic.

**Question 2.** Fill in the details of the following argument to show that  $(\mathbf{Z}/p\mathbf{Z})^*$ , the nonzero residues modulo  $p$ , form a cyclic group.

- (a) Let  $h = q_1^{r_1} \cdots q_s^{r_s}$  be the prime power factorization of  $h = p - 1$ . Show that for every  $1 \leq i \leq s$ , there is a nonzero residue which is not a root of  $x^{h/p_i} - 1$  modulo  $p$ .
- (b) Let  $a_i$  be a nonzero residue which is not a root of  $x^{h/p_i} - 1$ , and define  $b_i = a_i^{h/p_i^{r_i}}$ . Show that  $\text{ord}_p(b_i) = p_i^{r_i}$ .
- (c) Show the element  $b = b_1 \cdots b_s$  has multiplicative order  $h = p - 1$ . In particular, this shows that  $(\mathbf{Z}/p\mathbf{Z})^*$  is cyclic. We call  $b$  a primitive root modulo  $p$ .

Compare the previous question with Question 6 of the previous tutorial set.

**Question 3.** Use Questions 1 and 2 to show the following. (a)  $a^p \equiv a \pmod{p}$  for every integer  $a$ . (b)  $\left(\frac{a}{p}\right) \equiv \pm 1 \pmod{p}$ ; in particular,  $\left(\frac{a}{p}\right) \equiv 1 \pmod{p}$  if and only if  $a$  is a quadratic residue modulo  $p$ .

**Question 4.** We will give a second proof of the fact that  $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ . Fill in the following details.

- (a) Let  $i$  be the principal root of  $-1$ . Show that  $(1+i)^2 = 2i$ . Use this to show that  $(1+i)^p = (1+i)i^{(p-1)/2}2^{(p-1)/2}$ .
- (b) Show that  $\left(\frac{2}{p}\right)(1+i)i^{(p-1)/2} \equiv 1 + i(-1)^{(p-1)/2} \pmod{p}$ . Use this to show that  $\left(\frac{2}{p}\right) \equiv (-1)^{(p\pm 1)/2} \pmod{p}$  predicated upon whether  $\frac{p-1}{2}$  is even or odd.
- (c) Deduce that  $\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8}$ .

**Question 5.** Use quadratic reciprocity to determine  $\left(\frac{3}{p}\right)$ .

**Question 6.** Euler's Theorem is the following. *Let  $p$  be an odd prime, and let  $a$  be an integer not divisible by  $p$ . If  $q$  is a prime with  $p \equiv \pm q \pmod{4a}$ , then  $\left(\frac{a}{p}\right) = \left(\frac{p}{q}\right)$ .* Show that Euler's Theorem is equivalent to the law of quadratic reciprocity shown in class. [Hint: For necessity, it is convenient to consider the cases  $a = 2$ ,  $a$  an odd prime, and  $a$  composite separately.]