

# Math 342 Tutorial

June 25, 2025

**Question 1.** Show that if  $\bar{a}$  is an inverse of  $a$  modulo  $n$ , then  $\text{ord}_n \bar{a} = \text{ord}_n a$ .

We can show more generally that  $a^t \equiv 1 \pmod{n}$  if and only if  $\bar{a}^t \equiv 1 \pmod{n}$ . If  $a^t \equiv 1 \pmod{n}$ , then  $\bar{a}^t \equiv (\bar{a}^t a^t) a^t \equiv a^t \equiv 1 \pmod{n}$ .

**Question 2.** Assume that  $(a, n) = 1 = (b, n)$ . Do the following. **(a)** If  $(\text{ord}_n a = \text{ord}_n b) = 1$ , then  $\text{ord}_n ab = \text{ord}_n a \cdot \text{ord}_n b$ . **(b)** If we do not assume  $(\text{ord}_n a = \text{ord}_n b) = 1$ , then what can be said about  $\text{ord}_n ab$ .

**(a)** Let  $\alpha = \text{ord}_n a$ ,  $\beta = \text{ord}_n b$ , and  $\gamma = \text{ord}_n ab$ . Since  $(ab)^{\alpha\beta} = (a^\alpha)^\beta (b^\beta)^\alpha \equiv 1 \pmod{n}$ , we have that  $\gamma \mid \alpha\beta$ . On the other hand,  $1 \equiv (ab)^\gamma \equiv (ab)^{\alpha\gamma} \equiv b^{\alpha\gamma} \pmod{n}$ , hence  $\beta \mid \alpha\gamma$ . Since  $(\alpha, \beta) = 1$ , we see that  $\beta \mid \gamma$ . Similarly,  $\alpha \mid \gamma$ . Since  $(\alpha, \beta) = 1$ , we have that  $\alpha\beta \mid \gamma$ . We have shown that  $\text{ord}_n ab = \alpha\beta$ .

**(b)** Use the notation from part (a). Since  $\alpha, \beta \mid [\alpha, \beta]$ , we see at once that  $(ab)^{[\alpha, \beta]} \equiv 1 \pmod{n}$  whereupon  $\gamma \mid [\alpha, \beta]$ ; in particular,  $\gamma \leq [\alpha, \beta]$ . Also, we still have that  $\beta \mid \alpha\gamma$  so that  $\frac{\beta}{(\alpha, \beta)} \mid \gamma$ . Similarly,  $\frac{\alpha}{(\alpha, \beta)} \mid \gamma$ . It follows that  $\frac{\alpha\beta}{(\alpha, \beta)^2} = \frac{[\alpha, \beta]}{(\alpha, \beta)} \mid \gamma$ , hence  $\frac{[\alpha, \beta]}{(\alpha, \beta)} \leq \gamma$ .

**Question 3.** **(a)** Suppose  $d \mid \phi(n)$ . Is it true that there is an integer  $a$  for which  $\text{ord}_n a = d$ . **(b)** Show that if  $(a, n) = 1$  and  $\text{ord}_n a = st$ , then  $\text{ord}_n a^t = s$ . **(c)** Show that if  $(a, n) = 1$  and  $\text{ord}_n a = n - 1$ , then  $n$  is prime.

**(a)** This is false. For a counter example, take  $n = 8$ . Then  $\phi(8) = 4$ . If  $(a, 8) = 1$  if and only if  $a$  is odd. But  $a^2 \equiv 1 \pmod{8}$  for every odd integer  $a$ .

**(b)** Observe

$$\text{ord}_n a^t = \frac{ts}{(ts, t)} = s.$$

**(c)** Suppose that  $n$  is not prime. Then  $\phi(n) < n - 1$ . Since  $\text{ord}_n a \mid \phi(n)$ , we have that  $\text{ord}_n a < n - 1$ .

**Question 4.** Show that  $r$  is a primitive root modulo the prime  $p$  if and only if  $r$  is an integer with  $(r, p) = 1$  such that

$$r^{(p-1)/q} \not\equiv 1 \pmod{p}$$

for every prime divisor  $q$  of  $p - 1$ .

Certainly, if  $r$  is a primitive root mod  $p$ , then  $r^{(p-1)/q} \not\equiv 1 \pmod{p}$ . Conversely, Suppose that  $r^{(p-1)/q} \not\equiv 1 \pmod{p}$  for all prime divisors  $q$  of  $p - 1$ , and suppose further that  $r$  is not a primitive root. Then  $p - 1$  has a nontrivial factorization  $p - 1 = ts$  where  $r^t \equiv 1 \pmod{p}$ . Let  $q$  be a prime divisor of  $s$ , then  $r^{(p-1)/q} = (r^t)^{s/q} \equiv 1 \pmod{p}$ , contradicting our original assumption.

**Question 5.** Let  $m = a^n - 1$ . Show the following. **(a)**  $\text{ord}_m a = n$ , and **(b)**  $n \mid \phi(m)$ .

**(a)** Observe that  $a^t < a^n - 1$  whenever  $1 \leq t < n$ , hence  $a^t \not\equiv 1 \pmod{m}$ . But  $a^n \equiv 1 \pmod{m}$  since  $m = a^n - 1$ . It follows that  $\text{ord}_m a = n$ .

**(b)** Since  $\text{ord}_m a = n$ , this is trivial.

**Question 6.** Let  $p$  be a prime, and let  $\phi(p-1) = q_1^{e_1} \cdots q_k^{e_k}$  where each  $q_i$  is prime. **(a)** Show there are integers  $a_1, \dots, a_k$  such that  $\text{ord}_p a_i = q_i^{e_i}$  for each  $i = 1, \dots, k$ . **(b)** Show that  $a = a_1 \cdots a_k$  is a primitive root modulo  $p$ . **(c)** Follow the procedure outlined above to show find a primitive root modulo 29.

- (a)** Since  $q_i^{e_i} \mid \phi(p-1)$ , there are  $\phi(q_i^{e_i})$  incongruent elements of order  $q_i^{e_i} \pmod p$ . Let  $a_i$  be one such element.
- (b)** By question 2(a) and an obvious induction, we have that  $\text{ord}_p(a) = \prod_i \text{ord}_p(a_i) = \prod_i \phi(q_i^{e_i}) = \phi(p-1)$ , i.e.,  $a$  is a primitive element modulo  $p$ .
- (c)** We have (i)  $\phi(29) = 28 = 4 \cdot 7$ , (ii)  $\text{ord}_{29} 12 = 4$ , and (iii)  $\text{ord}_{29} 16 = 7$ . Therefore  $\text{ord}_{29}(12 \cdot 16) = 28$ . Since  $12 \cdot 16 \equiv 18 \pmod{29}$ , we have shown that 18 is a primitive root modulo 29.

**Question 7.** Show that if  $p$  is an odd prime then

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod{8}, \\ -1 & \text{if } p \equiv -1, -3 \pmod{8}. \end{cases}$$

We know that 2 is a quadratic residue mod  $p$  if  $p \equiv 1, 7 \pmod{8}$  and a quadratic nonresidue if  $p \equiv 3, 5 \pmod{8}$ . We also know that  $-1$  is a quadratic residue if  $p \equiv 1 \pmod{4}$  and a quadratic nonresidue if  $p \equiv -1 \pmod{4}$ . Since  $(-2 \mid p) = (-1 \mid p)(2 \mid p)$ , we have that  $-2$  is a quadratic residue if  $p \equiv 1, 3 \pmod{8}$  and a quadratic nonresidue if  $p \equiv 5, 7 \pmod{8}$ . Also

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)(p^2-1)}{16}}.$$

**Question 8.** Determine those primes  $p$  for which  $(-3 \mid p) = -1$  and those primes  $q$  for which  $(-3 \mid q) = 1$ .

By quadratic reciprocity,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{(p-1)/2} (-1)^{(p-1)/2} \left(\frac{p}{3}\right).$$

Therefore,

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3}, \\ -1 & \text{if } p \equiv -1 \pmod{3}, \\ 0 & \text{if } p \equiv 0 \pmod{3}. \end{cases}$$

**Question 9.** Prove that 5 is a quadratic residue of an odd prime  $p$  if  $p \equiv \pm 1 \pmod{10}$ , and that 5 is a non residue if  $p \equiv \pm 3 \pmod{10}$ .

By quadratic reciprocity,  $(5 \mid p) = (p \mid 5)$ . So,

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{5}, \\ -1 & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$