March 25–Primitive roots and quadratic residues

We will review a some points about primitive roots, quadratic residues, and the Legendre symbol from before break, then finish those sections.

Review facts about primitive roots

Question 1 *For a prime p, a primitive root there exists modulo p.*

Multiple Choice:

(a) *Always* ✓

(b) *Sometimes*

(c) *Never*

Question 2 *If $n = pq$ where p and q are distinct primes, then there exists a primitive root modulo n.*

Multiple Choice:

(a) *Always*

(b) *Sometimes* ✓

(c) *Never*

Question 3 *If $n = 2^k$ and $k \geq 3$, then there exists a primitive root modulo n.*

Multiple Choice:

(a) *Always*

Learning outcomes:
Author(s):

(b) *Sometimes*

(c) *Never* ✓

Question 4 *If $n = km$ where k and m are relatively prime and greater than 2, then there exists a primitive root modulo n.*

Multiple Choice:

(a) *Always*

(b) *Sometimes*

(c) *Never* ✓

Question 5 *There exists primitive roots modulo n when for $n =$*

Select All Correct Answers:

(a) *1* ✓

(b) *p a prime* ✓

(c) *4* ✓

(d) 2^m *for* $m \geq 3$

(e) p^m *for p an odd prime* ✓

(f) $2p^m$ *for p an odd prime* ✓

(g) *n a composite number with at least two distinct odd prime factors*

Review facts about quadratic residues

Question 6 *Let $p > 2$ be a prime, and let a be an integer between 0 and $p - 1$.*

- *If a is a quadratic residue modulo p, then $a^{\frac{p-1}{2}} = 1$.*
- *If a is a quadratic nonresidue modulo p, then $a^{\frac{p-1}{2}} = -1$.*

- *Otherwise,* $a^{\frac{p-1}{2}} = 0$.

Question 7 *Euler's identity: Let $p > 2$ be a prime, and let a be an integer. Then* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Theorem 1. *Let $p > 2$ be prime.*

- *If $p \equiv 1 \pmod{4}$, then -1 is a quadratic residue modulo p.*
- *If $p \equiv 3 \pmod{4}$, then -1 is a quadratic nonresidue modulo p.*

Proof For an arbitrary prime $p > 2$, Euler's identity tells us that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Note that, we have that $\left(\frac{-1}{p}\right)$ is either $+1$ or -1 by definition, and $(-1)^{\frac{p-1}{2}}$ is also either $+1$ or -1. Since $1 \not\equiv -1 \pmod{p}$, the two sides of the congruence are actually equal. That is, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

The completion of the proof involves applying the answer to the preclass assignment, and the proof is on homework 9. ■

Question 8 *Let $p > 2$ be prime, and let a and b be integers between 1 and $p-1$.*

- *If ab is a quadratic residue, then*

  Select All Correct Answers:

  (a) *a and b are both quadratic residues* ✓
  (b) *a and b are both quadratic nonresidues* ✓
  (c) *One of a and b is a quadratic residue and the other is a quadratic nonresidue*

- *If ab is a quadratic nonresidue, then*

  Select All Correct Answers:

  (a) *a and b are both quadratic residues* ✓
  (b) *a and b are both quadratic nonresidues* ✓
  (c) *One of a and b is a quadratic residue and the other is a quadratic nonresidue*

Quadratic reciprocity

We are going to explore the relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$. Let's look at an example:

Question 9 *We want to know if 3 is a quadratic residue modulo 107. It would be a lot easier to check if 107 is a quadratic residue modulo 3. We know that* $107 \equiv 2 \pmod 3$, *so* $\left(\frac{107}{3}\right) = -1$. *It would be nice if this also gave us* $\left(\frac{3}{107}\right)$.

Question 10 *Another example: Find* $\left(\frac{p}{5}\right)$ *and* $\left(\frac{5}{p}\right)$.

p	3	5	7	11	13
$\left(\frac{p}{5}\right)$	-1	0	-1	1	-1
$\left(\frac{5}{p}\right)$	-1	0	-1	1	-1

Question 11 *Another example: Find* $\left(\frac{p}{7}\right)$ *and* $\left(\frac{7}{p}\right)$.

p	3	5	7	11	13
$\left(\frac{p}{7}\right)$	-1	-1	0	1	-1
$\left(\frac{7}{p}\right)$	1	-1	0	-1	-1

This gives some evidence for our theorem:

Theorem 2. *Let p and q be odd primes with $p \neq q$.*

- *if* $p \equiv 1 \pmod 4$ *or* $q \equiv 1 \pmod 4$, *then* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
- *if* $p \equiv q \equiv 3 \pmod 4$, *then* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Our goal for Friday is to prove this.