

1. *Suppose that r is a primitive root mod p for an odd prime p . Show that*

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Your answer here...

2. *Suppose that p is an odd prime greater than 3 and S is a set of $\phi(p-1)$ primitive roots modulo p . What is the least positive residue of the product of all elements of S modulo p ?*

Your answer here...

3. Suppose that p is prime and $p = 2q + 1$ where q is an odd prime.

(a) How many primitive roots are there mod p ?

Your answer here...

(b) Show that for any positive integer n with $1 < n < p - 1$, the integer $-n^2$ is a primitive root modulo p .

Your answer here...

(c) Why do the answers to the previous two parts appear like they might contradict each other? Why do they not actually contradict each other?

Your answer here...

4. *Show that if the integer m has a primitive root then the only solutions to the congruence $x^2 \equiv 1 \pmod{m}$ are $x \equiv \pm 1 \pmod{m}$.*

Your answer here...