Homework 5

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

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

Note that $r^{\frac{p-1}{2}}$ is a root of the polynomial $x^2 - 1$ mod p because

$$\left(r^{\frac{p-1}{2}}\right)^2 - 1 = r^{p-1} - 1 \equiv 0 \mod p$$

by Fermat's little theorem. Since p is prime, Lagrange's theorem indicates that $x^2 - 1$ has at most two roots mod p. In fact, $x^2 - 1$ has two roots mod p: ± 1. Hence

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

However, since r is a primitive root, $r^{\frac{p-1}{2}} \not\equiv 1 \mod p$, so we must have $r^{\frac{p-1}{2}} \equiv -1 \mod p$.

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

Write $S = \{a_1, \ldots, a_{\varphi(p-1)}\}$ and note that since p is an odd prime there is a primitive root r. The $\varphi(p-1)$ primitive roots mod p are given by r^k for $1 \leqslant k \leqslant p-1$ and $(k, p-1) = 1$ and so for each $1 \leqslant i \leqslant \varphi(p-1)$, there exists $1 \leqslant k \leqslant p-1$ with $(k, p-1) = 1$ so that $a_i \equiv r^k \mod p$. Hence,

$$\begin{aligned} a_1 a_2 \cdots a_{\varphi(p-1)} &\equiv \prod_{k \in (\mathbb{Z} / (p-1)\mathbb{Z})^\times} r^k \mod p \\ &\equiv r^S \mod p \end{aligned}$$

where

$$S = \sum_{k \in (\mathbb{Z} / (p-1)\mathbb{Z})^\times} k$$

Problem 1 on Homework 2 shows that $S \equiv 0 \mod p-1$ (since $p > 3$ implying that $p - 1 > 2$) and Problem 1 on Course Portfolio 2 from last term shows that this implies that

$$\begin{aligned} a_1 a_2 \cdots a_{\varphi(p-1)} &\equiv r^S \mod p \\ &\equiv r^0 \mod p \\ &\equiv 1 \mod p \end{aligned}$$

Hence, the product of the primitive roots is congruent to 1 modulo p.

Alternate Solution

We first claim that if r is a primitive root mod p, then so is r^{-1}. Problem 4a on the week 6 group work shows that r and r^{-1} have the same order, so r is a primitive root if and only if r^{-1} is a primitive root. Moreover, note that if r is a primitive root mod p, then $r \not\equiv r^{-1} \mod p$ because that would imply that $r^2 \equiv 1 \mod p$, so $r \equiv \pm 1 \mod p$. But 1 cannot be a primitive root and -1 is only a primitive root if $p = 3$ (since the order of -1 is always two). Since we are assuming that $p > 3$, we find that $r \not\equiv r^{-1}$ mod p.

But now, when considering $a_1 \cdots a_{\varphi(p-1)} \mod p$, we see that we can pair up any a_i with its inverse, resulting in

$$a_1 \cdots a_{\varphi(p-1)} \equiv 1 \mod p$$

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?*

There are

$$\varphi(\varphi(p)) = \varphi(p-1) = \varphi(2q) = \varphi(2)\varphi(q) = q - 1$$

primitive roots mod p.

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

The possible orders of elements mod p are the divisors of $p - 1$. Since $p - 1 = 2q$ and q is an odd prime, we see that the possible orders of elements mod p are $1, 2, q$, and $2q$.

Now pick any n with $1 < n < p - 1$. The order of $-n^2$ cannot be 1 since if it were, we would have $-n^2 \equiv 1 \mod p$, implying that -1 is a quadratic residue mod p. But $p - 1 = 2q$ is not divisible by 4, so $p \equiv 3 \mod 4$ and we see that -1 is not a quadratic residue mod p. Hence, the order of $-n^2$ is not 1.

We can also see that the order of $-n^2$ is not 2. If it were, we would have $n^4 \equiv 1 \mod p$. This implies that n^2 is a root of the polynomial $x^2 - 1$ mod p, so $n^2 \equiv \pm 1 \mod p$. But $n^2 \not\equiv 1 \mod p$ because that would imply that $n \equiv \pm 1 \mod p$ and we have $1 < n < p - 1$. Also, $n^2 \not\equiv -1 \mod p$ because -1 is not a quadratic residue mod p. Hence, the order of $-n^2$ is not 2.

We can also see that the order of $-n^2$ is not q. If it were, we would have $-n^{2q} \equiv 1 \mod p$. But $2q = p - 1$ and by Fermat's little theorem, we would then have

$$1 \equiv -n^{2q} \equiv -n^{p-1} \equiv -1 \mod p$$

contradicting the fact that p is odd. Therefore, the order of $-n^2$ is not q.

We conclude that the order of $-n^2$ must be $2q$ and hence, $-n^2$ is a primitive root mod p.

(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?*

Part (a) indicates that there should be $q - 1$ primitive roots mod p. However, in part (b), it appears that we find $p - 3 = 2(q - 1)$ primitive roots mod p. At first glance, it seems like these two results contradict one another because we found twice as many primitive roots in part (b) as we would expect from part (a). However, if we remember that squaring is a two-to-one map, then we note that it is possible to have $n \not\equiv m \mod p$ with $-n^2 \equiv -m^2 \mod p$. Hence, part (b) does not give $2(q - 1)$ *distinct* primitive roots. In fact, it gives $q - 1$ distinct primitive roots.

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

Suppose that m has a primitive root, say r. Then suppose that $x \in \mathbb{Z}$ satisfies $x^2 \equiv 1 \mod m$. We must have $(x, m) = 1$ since no power of an integer sharing a common factor with m can be congruent to 1 mod m. Since r is a primitive root and $(x, m) = 1$, there exists $1 \leqslant k \leqslant \varphi(m)$ so that $x \equiv r^k \mod m$. Since $x^2 \equiv 1 \mod m$, the order of r^k must be 1 or 2.

Case 1: $\mathrm{ord}_m(r^k) = 1$

In this case, we have $x \equiv r^k \equiv 1 \mod m$ and we are done.

Case 2: $\mathrm{ord}_m(r^k) = 2$

In this case, we have have

$$2 = \mathrm{ord}_m(r^k) = \frac{\varphi(m)}{(k, \varphi(m))}$$

implying that $(k, \varphi(m)) = \frac{\varphi(m)}{2}$. We know that $k < \varphi(m)$ since if $k = \varphi(m)$, we would have $r^k \equiv 1 \mod m$ and so the order of r^k would be 1. Hence, $1 \leqslant k < \varphi(m)$ and k is a multiple of $\frac{\varphi(m)}{2}$, so we must have $k = \frac{\varphi(m)}{2}$. In particular, there is only one element of order 2. Since we know that -1 has order 2, we must have $x \equiv r^{\varphi(m)/2} \equiv -1 \mod m$.

Therefore, if m has a primitive root, then the only solutions to $x^2 \equiv 1 \mod m$ are $x \equiv \pm 1 \mod m$.