Solutions to Homework 5

Problem 1. Let p be an odd prime number and b a primitive root modulo p.

a) Prove that $b^{(p-1)/2} \equiv -1(\mod p)$. Conclude that $-b \equiv b^{(p+1)/2}(\mod p)$.

b) Show that the congruence $x^2 \equiv b^k(\mod p)$ is solvable if and only if k is even.

Part a) may be useful for problem 13.

Solution. a) Note that

$$[b^{(p-1)/2}]^2 = b^{p-1} \equiv 1(\mod p).$$

Thus $b^{(p-1)/2}$ is a solution of the congruence $x^2 \equiv 1(\mod p)$. This congruence has only two solutions: 1 and -1. Thus $b^{(p-1)/2} \equiv \pm 1(\mod p)$. Since b is a primitive root modulo p, we can not have $b^{(p-1)/2} \equiv 1(\mod p)$. It follows that

$$b^{(p-1)/2} \equiv -1(\mod p).$$

Multiplying both sides of this congruence by b, we get

$$b^{(p+1)/2} \equiv -b(\mod p).$$

b) If $k = 2l$ is even then $x = b^l$ satisfies the congruence $x^2 \equiv b^k(\mod p)$. Conversely, suppose that $a^2 \equiv b^k(\mod p)$. Then

$$(b^k)^{(p-1)/2} \equiv (a^2)^{(p-1)/2} = a^{p-1} \equiv 1(\mod p).$$

Since b is a primitive root modulo p and $b^{k(p-1)/2} \equiv 1(\mod p)$, we have $(p-1)|k(p-1)/2$. Canceling $(p-1)/2$, we get $2|k$, i.e. k is even.

Solution to Problem 4. Suppose that b is the inverse of a modulo m. Thus $ab \equiv 1(\mod m)$. It follows that for any positive integer t we have $a^t b^t \equiv 1(\mod m)$. Thus $a^t \equiv 1(\mod m)$ if and only if $b^t \equiv 1(\mod m)$. In particular, a and b have the same order modulo m.

Solution to Problem 8. Note that $a^n \equiv 1(\mod a^n - 1)$. Also, for $0 < k < n$ we can not have $a^k \equiv 1(\mod a^n - 1)$ since $0 < a^k - 1 < a^n - 1$. It follows that

$\text{ord}_{a^n-1}a = n$. In particular, $n|\phi(a^n-1)$, as the order of any element modulo m divides $\phi(m)$.

Solution to Problem 9. Let $\text{ord}_p(r) = k$. Then $k|\phi(p) = p-1$. If r is not a primitive root modulo p, then $k < p-1$ and therefore the integer $(p-1)/k$ has a prime divisor q. This means that $k|(p-1)/q$ and therefore

$$a^{(p-1)/q} \equiv 1 \pmod{p} .$$

We showed that if p is not a primitive root modulo p then there exists a prime divisor q of $p-1$ such that $a^{(p-1)/q} \equiv 1 \pmod{p}$. By contrapositive, if

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

for all prime divisor q of $p-1$ then r is a primitive root modulo p. Converrsely, if r is a primitive root modulo p then $a^k \not\equiv 1 \pmod{p}$ for every $1 \leq k < p-1$, so in particular $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for every prime divisor q of $p-1$.

Solution to Problem 13. In problem 1a) we proved that $-r \equiv r^{(p+1)/2}(\mod p)$. Thus $-r$ and $r^{(p+1)/2}$ have the same order modulo p. Now

$$\text{ord}_p(r^{(p+1)/2}) = \frac{p-1}{\gcd(p-1,(p+1)/2)}.$$

Note that any common factor of $p-1$ and $(p+1)/2$ is also a common factor of $p-1$ and $p+1$, so it is either 1 or 2.

When $p \equiv 1(\mod 4)$ then $(p+1)/2$ is odd so $p-1$ and $(p+1)/2$ are relatively prime. Thus $-r$ has order $p-1$ in this case, i.e. $-r$ is a primitive root modulo p. This proves part a)

When $p \equiv 3(\mod 4)$ then $(p+1)/2$ is even, so $\gcd(p-1,(p+1)/2) = 2$. Thus $-r$ has order $(p-1)/2$ in this case. This proves part b).

Solution to Problem 19a). The only divisors of $q-1 = 2p$ are $1, 2, p, 2p$. The order of -4 modulo q divides $q-1$, so it is one of $1, 2, p, 2p$. If the order was 1 we would have $-4 \equiv 1(\mod q)$, i.e. $q|5$, so $q = 5$. However, 5 is not of the form $2p+1$ for an odd prime p.

Similarly, if $\mathrm{ord}_q(-4) = 2$ then we would have $(-4)^2 \equiv 1(\mod q)$, i.e. $q|15$. This would imply that q is either 5 or 3, which is not possible.

It follows that the order of -4 modulo q is either p or $2p$. Since p is odd, we have

$$(-4)^p = -2^{2p} = -2^{q-1} \equiv -1(\mod q).$$

Thus p is not the order of -4 modulo q and therefore the order of -4 must be equal to $2p$. Thus -4 is a primitive root modulo q.