Homework 7, solutions

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.

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 7. a) Suppose that $\mathrm{ord}_m(a) = xy$ with x, y positive integers. Then

$$\mathrm{ord}_m(a^x) = \frac{xy}{\gcd(xy, x)} = y.$$

b) Suppose that $\mathrm{ord}_m(a) = m-1$. Then $m-1|\phi(m)$. But $\phi(m) < m$ so we must have $\phi(m) = m-1$. This can happen only when m is a prime number. In fact, if

$m = xy$ is not a prime, then x and m are two distinct positive integers which are not relatively prime to m and are $\leq m$. Thus $\phi(m) \leq m - 2$ in this case.

Solution to Problem 8. Note that $a^n \equiv 1(\mod a^n - 1)$. Also, for $0 < k < n$ we can not have $a^k \equiv 1(\mod a^n - 1)$. It follows that $\mathrm{ord}_{a^n-1} a = n$. In particular, $n|\phi(a^n - 1)$, as order of any element modulo m divides $\phi(m)$.

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

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

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.

Solution to Problem 58. a) Suppose that $a^p \equiv b^p(\mod p)$. Since $a^p \equiv a(\mod p)$ and $b^p \equiv b(\mod p)$ by Fermat's Little Theorem, we conclude that

$$a \equiv a^p \equiv b^p \equiv b(\mod p).$$

b) Note that

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1}) = (a-b)\sum_{k=0}^{p-1} a^k b^{p-1-k}.$$

By part a) we know that $a \equiv b(\mod p)$. Thus $a^k \equiv b^k(\mod p)$ and $a^k b^{p-1-k} \equiv b^k b^{p-1-k} = b^{p-1}(\mod p)$, for $k = 0, 1, \ldots, p-1$. Therefore,

$$\sum_{k=0}^{p-1} a^k b^{p-1-k} \equiv \sum_{k=0}^{p-1} b^{p-1} = pb^{p-1} \equiv 0(\mod p).$$

Thus, in the product $(a-b)(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1})$ both factors are divisible by p, so the product, which is $a^p - b^p$, is divisible by p^2, i.e.

$$a^p \equiv b^p(\mod p^2).$$

Remark. The assumption that a and b are not divisible by p is not needed for this problem. If p divides one of them then p divides both of them and the result is obvious in this case.

Problem 2. We proved that if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$ by showing that the map $U_{mn} \longrightarrow U_m \times U_n$ sending $a \in U_{mn}$ to the pair $(a(\mod m), a(\mod n))$ is a bijection. Verify "by hand" that this is indeed a bijection when $m = 3$, $n = 7$.

Solution. We have $U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, , 16, 17, 19, 20\}$ and $U_3 \times U_7 = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,1), (2,2), (2,3), (2,4), (2,5), (2.6)\}$. Our function works as follows:

$1 \mapsto (1,1)$

$2 \mapsto (2,2)$

$4 \mapsto (1,4)$

$5 \mapsto (2,5)$

$8 \mapsto (2,1)$

$10 \mapsto (1,3)$

$11 \mapsto (2,4)$

$13 \mapsto (1,6)$

$$16 \mapsto (1,2)$$
$$17 \mapsto (2,3)$$
$$19 \mapsto (1,5)$$
$$20 \mapsto (2,6)$$