M3P14 EXAMPLE SHEET 2

1. Compute $\left(\frac{54}{571}\right)$ and $\left(\frac{164}{641}\right)$ using quadratic reciprocity. (571 and 641 are both prime.)

We have:

$$\left(\frac{54}{571}\right) = \left(\frac{3}{571}\right)^3 \left(\frac{2}{571}\right).$$

Since $571 \equiv 3 \bmod 8$, we have $\left(\frac{2}{571}\right) = -1$ and $\left(\frac{3}{571}\right) = \left(\frac{571}{3}\right) = \left(\frac{1}{3}\right) = 1$. So $\left(\frac{54}{571}\right) = -1$.

We also have:

$$\left(\frac{164}{641}\right) = \left(\frac{2}{641}\right)^2 \left(\frac{41}{641}\right) = \left(\frac{41}{641}\right)$$
$$= \left(\frac{641}{41}\right) = \left(\frac{-15}{41}\right) = \left(\frac{-1}{41}\right)\left(\frac{3}{41}\right)\left(\frac{5}{41}\right)$$
$$= 1 \cdot \left(\frac{41}{3}\right)\left(\frac{41}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = -1.$$

2a. Find all 8 primitive roots modulo 17.

You can do this exhaustively, but there's a shortcut using problem 7. Note that 3 is a primitive root mod 17, as its first sixteen powers are distinct. Now by problem 7, since $\Phi(17) = 16$, the other primitive roots are the odd powers of 3. In particular one has 3, $3^3 = 10$, $3^5 = 5$, $3^7 = 11$, $3^9 = 14$, $3^{11} = 7$, $3^{13} = 12$, and $3^{15} = 6$ are all primitive roots mod 17.

2b. Show that there exist primitive roots modulo 6, 9, and 18.

Note that -1 has order 2 mod 6, and is thus a primitive root, since $\Phi(6) = 2$.

Mod 9, 5 is a primitive root; since $\Phi(9) = 6$, we must show that 5 has order 6. Certainly 5 has order dividing 6 and greater than one, so we must show that the order of 5 is not 2 or 3. But $5^2 \equiv 7 \pmod 9$ and $5^3 \equiv -1 \bmod 9$, so the order of 5 must be 6.

Mod 18, 5 is still a primitive root: $\Phi(18) = 6$, so we must show that the order of 5 is not less than 6 mod 18, but this is true since it is already true mod 9.

2c. Show that if n is odd and there exists a primitive root mod n, then there also exists a primitive root mod $2n$. [HINT: $\Phi(2n) = \Phi(n)$ when n is odd.]

Let a be a primitive root mod n. Then a and $a+n$ both have order $\Phi(n)$ modulo n. Let $g = a$ if a is odd, or $g = a + n$ if a is even. Then g is odd and congruent to a mod n. I claim that g is a primitive root mod $2n$. Note that $\Phi(2n) = \Phi(n)$, so we must show that g has order $\Phi(n)$ mod $2n$. But

if $g^k \equiv 1 \pmod{2n}$ for any $k < \Phi(n)$, the same would be true mod n, and then a would have order less than $\Phi(n)$.

3. Let p be a prime and let a be a primitive root mod p. Show that a is also a primitive root mod p^2 if, and only if, a^{p-1} is not congruent to 1 mod p^2. [HINT: what is the order of a mod p? What does this say about the order of a mod p^2?]

The order of a mod p^2 must divide $\Phi(p^2) = p(p-1)$. On the other hand, suppose the order of a mod p^2 is k. Then $a^k \equiv 1 \pmod{p^2}$, and so $a^k \equiv 1 \pmod{p}$. Since a is a primitive root mod p, this means that $p-1$ divides k. So the order of a mod p^2 is either $p-1$ or $p(p-1)$. Since a^{p-1} is not congruent to 1 mod p^2, the order of a must be $p(p-1)$, which means that a is a primitive root.

4. Let p be a prime, and suppose that a is not divisible by p. Show that the equation $x^d \equiv a \pmod{p}$ has a solution if, and only if, $a^{\frac{p-1}{(d,p-1)}} \equiv 1 \pmod{p}$. Show further that if this is the case then this equation has $(d, p-1)$ solutions mod p. [HINT: what happens when you fix a primitive root g mod p, and take the discrete log of the equation $x^d \equiv a \pmod{p}$?]

Let g be a primitive root mod p. Then $\log_g$ gives an isomorphism of $(\mathbb{Z}/p)^\times$ with $\mathbb{Z}/(p-1)$. Applying $\log_g$ to the equation $x^d \equiv a \pmod{p}$ gives the equation $d \log_g x \equiv \log_g a \pmod{p-1}$. Let $y = \log_g x$, and $z = \log_g a$. We are then trying to solve the equation $dy = z \pmod{p-1}$. We know by our study of linear equations that this has a solution if, and only if, z is divisible by $(d, p-1)$, and that if this is the case that there are $(d, p-1)$ such solutions.

It thus suffices to show that z is divisible by $(d, p-1)$ if, and only if, $a^{\frac{p-1}{(d,p-1)}} \equiv 1 \pmod{p}$. Suppose first that z is divisible by $(d, p-1)$. SInce $z = \log_g a$, we have $a \equiv g^z \pmod{p}$. Thus $a^{\frac{p-1}{(d,p-1)}} \equiv g^{z\frac{p-1}{(d,p-1)}} \pmod{p}$. Since $(d, p-1)$ divides z, the exponent is an integral multiple of $p-1$, and raising g to such a power gives 1 by Fermat's little theorem.

Conversely, if $g^{z\frac{p-1}{(d,p-1)}} \equiv 1 \pmod{p}$, then (since g has order $p-1$) we must have $z\frac{p-1}{(d,p-1)}$ divisible by $p-1$, and thus z is divisible by $(d, p-1)$.

5. Let p be an odd prime different from 7. Show that 7 is a square mod p if, and only if, p is congruent to $1, 3, 9, 19, 25$ or 27 modulo 28. [HINT: use quadratic reciprocity to relate $\left(\frac{7}{p}\right)$ to $\left(\frac{p}{7}\right)$.]

If $p \equiv 1 \bmod 4$, then $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$. The quadratic residues mod 7 are $1, 2, 4$. Thus 7 is a square mod p if p is congruent to 1 mod 4 and $1, 2$, or 4 mod 7, and not a square if p is congruent to 1 mod 4 and $3, 5$, or 6 mod 7. Using the Chinese Remainder theorem, we see that 7 is a square mod p if p is congruent to 1, 9, or 25 mod 28, and not if p is congruent to 17, 5, or 13 mod 28.

If $p \equiv 3 \bmod 4$, then $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$. Thus 7 is a square mod p is p is congruent to 3 mod 4 and $3, 5$, or 6 mod 7, and not if p is congruent to 3 mod 4 and $1, 2$, or 4 mod 7. Using the Chinese Remainder theorem, we see that 7 is a square mod p if p is congruent to 3, 19, or 27 mod 28, and not if p is congruent to 15, 23, or 11 mod 28.

6a. Let n and m be relatively prime. Show that every element of $(\mathbb{Z}/nm)^\times$ has order dividing the least common multiple of $\Phi(n)$ and $\Phi(m)$.

Let a be in $(\mathbb{Z}/nm)^\times$. Then $a^{\Phi(n)} \equiv 1 \pmod{n}$, and $a^{\Phi(m)} \equiv 1 \pmod{m}$. Thus, if k is the least common multiple of $\Phi(n)$ and $\Phi(m)$, then $a^k \equiv 1 \pmod{n}$ and $a^k \equiv 1 \pmod{m}$. By the Chinese remainder theorem this means that $a^k \equiv 1 \pmod{mn}$. Thus the order of a divides k.

6b. Show that if n and m are relatively prime, then $\mathbb{Z}/nm$ has a primitive root if, and only if, both $\mathbb{Z}/n$ and $\mathbb{Z}/m$ have primitive roots, and $(\Phi(n), \Phi(m)) = 1$.

Suppose that $\mathbb{Z}/mn$ has a primitive root g. Then the order of $g \bmod mn$ is $\Phi(mn) = \Phi(m)\Phi(n)$. On the other hand, the order of $g \bmod mn$ divides the least common multiple of $\Phi(m)$ and $\Phi(n)$. Thus $\Phi(m)\Phi(n)$ must be the least common multiple of $\Phi(m)$ and $\Phi(n)$, and thus $(\Phi(m), \Phi(n)) = 1$. Finally, note that the powers of g contain every invertible congruence class mod mn, and thus contain every invertible congruence class mod m. Thus g is a primitive root mod m, and similarly is a primitive root mod n.

Conversely, if a is a primitive root mod m and b is a primitive root mod n, choose a g congruent to a mod m and b mod n. Let k be the order of $g \bmod mn$. Then $g^k \equiv 1 \bmod m$, so (since $g \equiv a \pmod{m}$), the order of $a \bmod m$ divides k. Thus $\Phi(m)$ divides k. Similarly $\Phi(n)$ divides k. Since $(\Phi(n), \Phi(m)) = 1$, the product $\Phi(m)\Phi(n)$ divides k, and thus $k = \Phi(n)\Phi(m)$, and g is a primitive root mod mn.

7. Suppose a is a primitive root modulo n. Show that a^d is also a primitive root modulo n for all d such that $(d, \Phi(n)) = 1$. [Hint: show that there exists k such that $(a^d)^k$ is congruent to a modulo n.]

Let k be a multiplicative inverse of $a \bmod \Phi(n)$. Then $dk \equiv 1 \bmod \Phi(n)$, and so $(a^d)^k = a^{1+m\Phi(n)}$ for some integer m. Thus $(a^d)^k \equiv a \bmod n$ by Euler's theorem.

Now let r be the order of $a^d \bmod n$. Then $(a^d)^r \equiv 1 \bmod n$, so, raising both sides to the kth power, we have $((a^d)^k)^r \equiv 1 \bmod n$ and thus $a^r \equiv 1 \bmod n$. Thus r must be divisible by $\Phi(n)$ since a is a primitive root. Since r is the order of a^d, it divides $\Phi(n)$ and thus must equal $\Phi(n)$.

8. Show that if p is a prime congruent to 1 mod 120 then none of $2, 3, 4, 5, 6$ is a primitive root modulo p. [Hint: show that 2, 3, and 5 are squares mod p.]

By Euler's criterion, if a is a quadratic residue mod p then $a^{\frac{p-1}{2}} \equiv 1 \bmod p$; in particular the order of a is NOT $p-1$, so a can't be a primitive root. We will show that if p is congruent to 1 mod 120 then $2, 3, 4, 5, 6$ are all quadratic residues mod p. This is clear for 4, and if 2 and 3 are quadratic residues then so is 6, so it suffices to show this for 2, 3, and 5.

If p is congruent to 1 mod 120, then p is congruent to 1 mod 8, so $\left(\frac{2}{p}\right) = 1$.

Similarly, since p is congruent to 1 mod 4, and 1 mod 3, we have $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.

Finally, since p is congruent to 1 mod 4 and 1 mod 5, we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$.