M3P14 EXAMPLE SHEET 2

1. Compute $\left(\frac{210}{449}\right)$ and $\left(\frac{605}{617}\right)$ using quadratic reciprocity. (449 and 617 are both prime.)

2a. Find all 6 primitive roots modulo 19.

2b. Show that if n is odd and a is a primitive root mod n, then a is a primitive root mod $2n$ if a is odd, and $a+n$ is a primitive root mod $2n$ if a is even. [HINT: $\Phi(2n) = \Phi(n)$ when n is odd.]

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?]

4. Let p be a prime, and let a be an integer 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 $x^d \equiv a \pmod{p}$?]

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 $\left(\frac{p}{7}\right)$.]

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

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

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 equal to a.]

8. Show that if p is a prime congruent to ±1 mod 24 then none of $2, 3, 4, 6$ is a primitive root modulo p. [Hint: show that 2 and 3 are squares mod p.]