MATH 465 NUMBER THEORY, SPRING 2025, PROBLEMS 6

Return by Monday 24th February

1. (i) Find the order of 2, 3 and 5 modulo 23.
   (ii) Find a primitive root modulo 23 and construct a table of indices.
   (iii) Solve the congruence $x^{39} \equiv 13 \pmod{23}$.

2. First find a primitive root modulo 19 and then find all primitive roots modulo 19.

3. Show that 3 is a primitive root modulo 17 and draw up a table of discrete logarithms to this base modulo 17. Hence, or otherwise, find all solutions to the following congruences.
   (i) $x^{12} \equiv 16 \pmod{17}$,
   (ii) $x^{48} \equiv 9 \pmod{17}$,
   (iii) $x^{20} \equiv 13 \pmod{17}$,
   (iv) $x^{11} \equiv 9 \pmod{17}$.

4. Suppose that p is an odd prime and g is a primitive root modulo p. Prove that g is a quadratic non-residue modulo p.

5. Find a complete set of quadratic residues r modulo 29 in the range $1 \le r \le 28$.