ASSIGNMENT 2, MP313, Semester 2, 1999

Please hand in by Monday 5pm, 5th September 1999.

1. Let p be an odd prime.

   (i) Prove that the congruence $-1 \equiv x^4 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{8}$.

   (ii) Use the fact that 6 is a primitive root mod 41 to solve

   $$-1 \equiv x^4 \pmod{41}.$$

2. Let p be a prime, $p > 3$ and suppose that $-3 \equiv x^2 \pmod{p}$. Let $2y + 1 \equiv x \pmod{p}$.

   Prove that $y^3 \equiv 1 \pmod{p}$ and deduce that $p \equiv 1 \pmod{3}$.

3. Let p be an odd prime, $p \equiv 3 \pmod{4}$. Also suppose x is not divisible by p.

   Let $r = \mathrm{ord}_p x,\ s = \mathrm{ord}_p -x$.

   (i) Prove that r and s cannot both be odd;

   (ii) If r is even, prove that $r = 2s$, where s is odd.

4. Let $n = 19 \times 23 = 437$.

   Solve the congruence $x^2 \equiv 82 \pmod{437}$ and find the principal square root of 82 mod 437.