SOLUTIONS: PROBLEM SET 24 FROM SECTION 11.1

2.

(a) 1,2,4
(b) 1
(c) 1,4
(d) 1,7,13

6. Since $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, either none or exactly two of these terms must be negative. It follows that either exactly one or all three of a, b and ab are quadratic residues $\pmod p$.

20. Since $77 = 7 \times 11$, this is equivalent to solving the simultaneous congruences, $x^2 \equiv 3 \pmod{11}$ and $x^2 \equiv 2 \pmod 7$. This yields $x \equiv \pm 5 \pmod{11}$ and $x \equiv \pm 3 \pmod 7$, which yields the solutions $x \equiv 17, 38, 39, 60 \pmod{77}$.

48. This congruence reduces to the pair $x^2 \equiv 12 \pmod{47}$ and $x^2 \equiv 10 \equiv -49 \pmod{59}$. But 49 is a quadratic residue $\pmod{59}$, and -1 is not. It follows that -49 is not a quadratic residue $\pmod{59}$, and hence there is no solution to the original congruence.