MATH 356 Number Theory
Solutions to Homework Assignment 10

7.2 (a) $\left(\frac{3}{97}\right) = \left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = 1.$

(b) $\left(\frac{5}{389}\right) = \left(\frac{389}{5}\right) = \left(\frac{4}{5}\right) = 1.$

(c) $\left(\frac{2033}{11}\right) = \left(\frac{19}{11}\right) \cdot \left(\frac{107}{11}\right) = \left(\frac{8}{11}\right)\left(\frac{8}{11}\right) = 1.$

(d) $\left(\frac{5!}{7}\right) = \left(\frac{(-1)(-1)(5!)}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{6!}{7}\right) = (-1)(-1) = 1$ (using Wilson's Theorem).

(e) $\left(\frac{6!}{7}\right) = \left(\frac{-1}{7}\right) = -1$ (again using Wilson's Theorem).

7.3 (a) Since $13 \equiv 1 \pmod 4$, $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$. The squares mod 13 are 1, 3, 4, 9, 10, and 12, so $\left(\frac{13}{p}\right) = 0$ if $p = 13$, 1 if $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$, and -1 is $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$.

(b) Since $19 \equiv 3 \pmod 4$, $\left(\frac{19}{p}\right) = \left(\frac{p}{19}\right)$ if $p \equiv 1 \pmod 4$ and $\left(\frac{19}{p}\right) = -\left(\frac{p}{19}\right)$ if $p \equiv 3 \pmod 4$.

The squares mod 19 are 1, 4, 5, 6, 7, 9, 11, 16, 17. If $p \equiv 1 \pmod 4$, then $p \equiv 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69,$ or $73 \pmod{76}$. Of these, only $1, 5, 9, 17, 25, 45, 49, 61,$ and 73 are in the list of squares mod 19.

The non-squares mod 19 are thus $2, 3, 8, 10, 12, 13, 14, 15, 18$. If $p \equiv 1 \pmod 4$, then $p \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63, 67, 71,$ or $75 \pmod{76}$.

The non-squares among these (the values that give $\left(\frac{-1}{p}\right) = -1 = \left(\frac{x}{p}\right)$ are $3, 15, 27, 31, 51, 59, 67, 71,$ and 75.

Primes congruent to the red values mod 19 give $+1$ for the Legendre symbol, 19 gives 0, and all others give -1. (Note that there are no primes congruent to 38 or 57 or any even number mod 76.)

7.6 $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 4 \pmod 5$, so we get -1 if and only if $p \equiv 2, 3 \pmod 5$.

For the second part, $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1$ if and only if either $p \equiv 1, 4 \pmod 5$ and $p \equiv 1 \pmod 4$ or $p \equiv 2, 3 \pmod 5$ and $p \equiv 3 \pmod 4$.

The mod 4 condition in the first case implies $p \equiv 1, 5, 9, 13, 17 \pmod{20}$, and of those, only $p \equiv 1, 9 \pmod{20}$ are also congruent to 1 or 4 mod 5.

In the second case, we have $p \equiv 3, 7, 11, 15, 19 \pmod{20}$, and the mod 5 condition gives only $p \equiv 3, 7 \pmod{20}$.

Therefore, the only solutions are $p \equiv 1, 3, 7, 9 \pmod{20}$.