Math 522 Exam 12 Solutions

1. Using EITHER Legendre symbols or Jacobi symbols, determine whether $x^2 \equiv 667 \pmod{919}$ has solutions. Be sure to specify which you use.

   If we use Jacobi symbols, we don't need to factor 667 (nor, subsequently, 63 or 37). We calculate: $\left(\frac{667}{919}\right) = -\left(\frac{919}{667}\right) = -\left(\frac{252}{667}\right) = -\left(\frac{2}{667}\right)^2\left(\frac{63}{667}\right) = -(1)(-1)\left(\frac{667}{63}\right) = \left(\frac{37}{63}\right) = \left(\frac{63}{37}\right) = \left(\frac{26}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{13}{37}\right) = (-1)^{\frac{37^2-1}{8}}\left(\frac{37}{13}\right) = (-1)^{171}\left(\frac{11}{13}\right) = -\left(\frac{13}{11}\right) = -\left(\frac{2}{11}\right) = -(-1)^{\frac{11^2-1}{8}} = -(-1)^{15} = 1.$

   If we use Legendre symbols, we first need to factor $667 = 23 \cdot 29$. *We calculate:* $\left(\frac{667}{919}\right) = \left(\frac{23}{919}\right)\left(\frac{29}{919}\right) = -\left(\frac{919}{23}\right)\left(\frac{919}{29}\right) = -\left(\frac{-1}{23}\right)\left(\frac{20}{29}\right) = -(-1)^{\frac{23-1}{2}}\left(\frac{2}{29}\right)^2\left(\frac{5}{29}\right) = \left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1.$

   In either case, the answer is 'yes'. :-)

   NOTE: Both Legendre and Jacobi symbols can't handle even numbers in the bottom, so there is no "quadratic reciprocity" if the top is even – you need to factor out all the 2's first.

2. For all odd $m \geq 3$, prove that if the Jacobi symbol $\left(\frac{n}{m}\right) = -1$, then $x^2 \equiv n \pmod{m}$ has no solutions.

   Factor $m = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$. *The Jacobi symbol is defined as a product of Legendre symbols:* $\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{a_1}\left(\frac{n}{p_2}\right)^{a_2}\cdots\left(\frac{n}{p_k}\right)^{a_k}$. *Because* $\left(\frac{n}{m}\right) = -1$, *each* $\left(\frac{n}{p_i}\right)$ *must be either 1 or -1 (none of them can be zero); further, at least one of them must be* -1 *(otherwise their product would be 1). Without loss of generality, suppose* $\left(\frac{n}{p_1}\right) = -1$. *Hence,* $x^2 \equiv n \pmod{p_1}$ *has no solutions; in other words,* p_1 *does not divide* $x^2 - n$, *for any integer* x. *Now, suppose that* $x^2 \equiv n \pmod{m}$ *had a solution. Then* $m|x^2 - n$ *for some integer* x. *But* $p_1|m$, *so* $p_1|x^2 - n$, *but we have shown that this is impossible.*

3. Exam grades: 105, 98, 94, 88, 87, 87, 86, 84, 82, 80, 79, 75, 71, 67

4. I've tabulated your overall exam averages; this is after dropping your lowest two exams and counting your best exam double. This is still subject to change a little, since this doesn't account for extra credit on the last exam. Scores:

   101, 100, 97, 93, 93, 90, 90, 89, 86, 84, 83, 82, 80, 71