Math 567, Assignment #10: Solutions

1. An induction argument shows that $4^n \equiv 4 \pmod{12}$ for all n. Thus if p is a prime of the form $2^{2n}+1$, it follows that $p = 4^n + 1 \equiv 4 + 1 \equiv 5 \pmod{12}$. Theorem 9.10 gives $(\frac{3}{p}) = -1$.

If q is a prime of the form $2^p - 1$, with p an odd prime, then $q = 2^{2k+1} - 1 = 2 \cdot 4^k - 1 \equiv 2 \cdot 4 - 1 \equiv 7 \pmod{12}$. Hence $(\frac{3}{p}) = -1$ by Theorem 9.10

2. (a) It's enough to have $(\frac{-1}{p})$, $(\frac{2}{p})$, and $(\frac{3}{p})$ all equal to 1, since the other conditions then follow. By the Corollary to Theorem 9.2, Theorem 9.6, and Theorem 9.10, respectively, we can rewrite these conditions as $p \equiv 1 \pmod 4$, $p \equiv \pm 1 \pmod 8$, and $p \equiv \pm 1 \pmod{12}$. These three conditions, taken together, are easily seen to imply, and be implied by, the single condition $p \equiv 1 \pmod{24}$. The first such prime is 73.

(b) 1, 2, 3, and 4 are all quadratic residues mod 73, but 5 is not, since quadratic reciprocity gives $(\frac{5}{73}) = (\frac{73}{5}) = (\frac{3}{5}) = -1$.

3. (a) The quadratic congruence $x^2 \equiv 219 \pmod{419}$ is solvable since 219 is a quadratic residue modulo the prime 419: $(\frac{219}{419}) = (\frac{3}{419})(\frac{73}{419}) = (-1)(\frac{419}{3})(+1)(\frac{419}{73}) = -(\frac{419}{3})(\frac{419}{73}) = -(\frac{2}{3})(\frac{54}{73}) = -(-1)(\frac{2}{73})(\frac{3}{73})(\frac{9}{73}) = -(-1)(1)(1)(1) = 1$.

(b) The congruence $3x^2 + 6x + 5 \equiv 0 \pmod{89}$ is equivalent to $3x^2 + 6x + 3 \equiv 87 \pmod{89}$, which is in turn equivalent to $(x+1)^2 \equiv x^2 + 2x + 1 \equiv 29 \pmod{89}$ (since 3 is relatively prime to 89). This congruence is not solvable, since 29 is a quadratic nonresidue modulo 89: $(\frac{29}{89}) = (\frac{89}{29}) = (\frac{2}{29}) = -1$.

(c) The congruence $2x^2 + 5x - 9 \equiv 0 \pmod{101}$ is equivalent to $(4x+5)^2 \equiv 97 \equiv -4 \pmod{101}$. Since $(\frac{-4}{101}) = (\frac{-1}{101})(\frac{4}{101}) = (\frac{-1}{101}) = +1$, -4 has a square root mod 101; subtracting 5 from such a square root of -4, and then multiplying the result by a multiplicative inverse of 4 (mod 101), one can get an x satisfying the original congruence.

4. Let p and q be odd primes satisfying $p = q + 4a$ for some a. Then $p \equiv 4a \pmod q$ and $q \equiv -4a \pmod p$. Since $p \equiv q \pmod 4$, there are two cases to consider. If $p \equiv q \equiv 1 \pmod 4$, then $(\frac{a}{p}) = (\frac{-1}{p})(\frac{4}{p})(\frac{a}{p}) = (\frac{-4a}{p}) = (\frac{q}{p}) = (\frac{p}{q}) = (\frac{4a}{q}) = (\frac{4}{q})(\frac{a}{q}) = (\frac{a}{q})$. If $p \equiv q \equiv -1 \pmod 4$, then $(\frac{a}{p}) = -(\frac{-1}{p})(\frac{4}{p})(\frac{a}{p}) = -(\frac{-4a}{p}) = -(\frac{q}{p}) = (\frac{p}{q}) = (\frac{4a}{q}) = (\frac{4}{q})(\frac{a}{q}) = (\frac{a}{q})$. In either case, $(\frac{a}{p}) = (\frac{a}{q})$.

5. Let p be an odd prime. If $p|n^2+1$, then $n^2 \equiv -1 \pmod{p}$; hence $(\frac{-1}{p}) = 1$ and so $p \equiv 1 \pmod{4}$ by the Corollary to Theorem 9.2. Thus, the prime divisors of n^2+1 are either 2 or primes of the form $4k+1$.

If $p|n^2+2$, then $n^2 \equiv -2 \pmod{p}$, so that $(\frac{-2}{p}) = 1$. Since $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$, it's easy to check that $(\frac{-2}{p}) = 1$ implies $p \equiv 1$ or $3 \pmod{8}$. The prime divisors of n^2+2 are either 2 or primes of the form $8k+1$ or $8k+3$.

If $p|n^2+3$, then $n^2 \equiv -3 \pmod{p}$, so that $(\frac{-3}{p}) = 1$. Since $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p})$, it's easy to check that $(\frac{-3}{p}) = 1$ implies $p \equiv 1 \pmod{6}$. The prime divisors of n^2+3 are either 2 or primes of the form $6k+1$.

6. Since p and q must differ by 4, neither of them can equal 2 or 5. So $\gcd(5,p) = \gcd(10,p) = \gcd(5,q) = \gcd(10,q) = 1$, and all the Legendre symbols in the next paragraph make sense.

If the congruence $x^2 \equiv 5 \pmod{pq}$ has a solution, so must $x^2 \equiv 5 \pmod{p}$ and $x^2 \equiv 5 \pmod{q}$; that is, $(\frac{5}{p}) = (\frac{5}{q}) = +1$. Likewise, if $x^2 \equiv 10 \pmod{pq}$ has a solution, we must have $(\frac{10}{p}) = (\frac{10}{q}) = +1$. By multiplicativity, we must have $(\frac{2}{p}) = (\frac{10}{p})/(\frac{5}{p}) = +1 = (\frac{10}{p})/(\frac{5}{p}) = (\frac{2}{p})$. Hence $p, q \equiv 1 \pmod{8}$, which is impossible if p, q differ by 4.