Problem set Week 12

1. Find **all** the quadratic residues for each $n \in \{3, 5, 7, 11, 19\}$. (This is, all integers that are quadratic residues of the corresponding number.)
2. Evaluate $(\frac{7}{11})$.
   (a) Using Euler's criterium
   (b) Using Gauss lemma.
3. Show that if $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ where $p_1, p_2 \dots p_k$ are distinct primes and a_i are non negative integers then $(\frac{n}{q}) = (\frac{p_1}{q})(\frac{p_2}{q}) \dots (\frac{p_k}{q})$ for each prime q not dividing n.
4. Consider the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ where p is prime a, b, c are integers, and p does not divide a.
   (a) Determine which quadratic congruences have solutions when $p = 2$.
   (b) Let $p > 2$ and let $d = b^2 - 4ac$. Show that the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is equivalent to the congruence $y^2 \equiv d \pmod{p}$ where $y = 2ax + b$. Conclude that if $d \equiv 0 \pmod{p}$ there is exactly one solution mod p; if d is a quadratic residue mod p then there are two non congruent solutions and if d is a quadratic non-residue then there are no solutions.
5. (a) Prove that if p is a prime larger than 5 then there are always two consecutive quadratic residues mod p. (Hint: show first that at least one of $2, 5$ and 10 is quadratic residue mod p.
   (b) Prove that if p is a prime larger than 5 then there are always two consecutive quadratic residues of p that differ by 2.
6. Find all solutions of $x^2 \equiv 58 \pmod{77}$
7. Show that there are infinitely many primes of the form $8k + 3$.
8. Let n be a positive integer, such that $p = 2n + 1$ is prime.
   (a) Prove that if $n \equiv 0 \pmod{4}$ or $n \equiv 3 \pmod{4}$ then p divides $2^n - 1$.
   (b) Prove that if $n \equiv 1 \pmod{4}$ or $n \equiv 2 \pmod{4}$ then p divides $2^n + 1$.