PMAT 4282 – Cryptography Winter 2007 — Assignment #6

Instructions

- Answer each question completely; justify your answers.
- This assignment is due at: 3:00 pm on Tuesday March 13th.

1. For each of the following (a, p) pairs, determine whether $a \in QR_p$:
   (a) $(2, 17)$
   (b) $(44, 97)$
   (c) $(789, 5683)$

2. Let p be an odd prime. Prove that the equation $x^2 \equiv 1 \pmod{p}$ has exactly 2 solutions in $\mathbb{Z}_p^*$.

3. Let $n \geq 3$ be an odd integer. Prove that if $a \in QR_n$ then $\left(\frac{a}{n}\right) = 1$.

4. Calculate the following subject to the restriction that when factoring, you are only allowed to factor out powers of 2 (so, for example, with the number 60, you're allowed to factor this as $2^2 \cdot 15$, but treat the 15 as though you don't know how (or if) it factors).
   (a) $\left(\frac{43}{455}\right)$
   (b) $\left(\frac{87}{601}\right)$
   (c) $\left(\frac{44}{3323}\right)$
   (d) $\left(\frac{5637}{631}\right)$
   (e) $\left(\frac{866}{3531}\right)$
   (f) $\left(\frac{381}{23}\right)$
   (g) $\left(\frac{837}{377}\right)$
   (h) $\left(\frac{82001}{643747}\right)$

5. Without identifying any factors of n, prove that n is composite.
   (a) $n = 4141$
   (b) $n = 75361$
   (c) $n = 18162001$
   (d) $n = 451149769054931$

(continued over...)

6. Let $n \geq 3$ be an odd integer. Given that $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$ whenever p is prime, prove that $\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)}$.

7. (a) Let n be an odd composite integer. Prove that at least half of the elements of $\mathbb{Z}_n^*$ are Euler witnesses.

   (b) What proportion of the elements of $\mathbb{Z}_{25}^*$ are Euler witnesses?