MATH 4282 – Cryptography   Assignment #5
Winter 2012

Instructions

- Answer each question completely; justify your answers.

1. Prove that each of the following numbers is composite by finding a Fermat witness:

   (a) 123

   (b) 52687

   (c) 1263739430742009409841

2. Show that 75361 is composite and also that it has no Fermat witnesses.

3. For each of the following (a, p) pairs, determine whether $a \in QR_p$:

   (a) $(3, 43)$

   (b) $(44, 97)$

   (c) $(789, 5683)$

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

5. 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) $\left(\dfrac{87}{601}\right)$

   (b) $\left(\dfrac{5637}{631}\right)$

   (c) $\left(\dfrac{381}{23}\right)$

   (d) $\left(\dfrac{82001}{643747}\right)$

6. Without identifying any factors of n, prove that n is composite.

   (a) $n = 4141$

   (b) $n = 18162001$

   (c) $n = 671438107719337150363313$