MATH 4282 – Cryptography Assignment #5

Winter 2019

Instructions

- Answer each question completely; justify your answers.

1. For each of the following (a, p) pairs, determine whether $a \in QR_p$:
   (a) $(3, 43)$
   (b) $(44, 97)$
   (c) $(789, 5683)$

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

3. 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) $\left(\frac{87}{601}\right)$
   (b) $\left(\frac{5637}{631}\right)$
   (c) $\left(\frac{381}{23}\right)$
   (d) $\left(\frac{82001}{643747}\right)$

4. Without identifying any factors of n, prove that n is composite.
   (a) $n = 4141$
   (b) $n = 18162001$
   (c) $n = 671438107719337150363313$

5. (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?

6. Let p be an odd prime and let $a \geqslant 1$. Prove that the number of solutions in $\mathbb{Z}_p$ to the equation $x^a \equiv 1 \pmod{p}$ is $\gcd(a, p-1)$.

7. Let $n = pq$ where p and q are distinct odd primes. Prove that the number of integers m, $0 \leqslant m < n$, such that $m^e \equiv m \pmod{n}$ is $(d_1 + 1)(d_2 + 1)$ where $d_1 = \gcd(p-1, e-1)$ and $d_2 = \gcd(q-1, e-1)$.

8. Bob has published $(30314385727, 683)$ as his public-key for RSA. Eve intercepts the ciphertext 13490063419 sent from Alice to Bob. What was the plaintext message?