MATH 4282 – Cryptography — Assignment #6
Winter 2012

Instructions

- Answer each question completely; justify your answers.

1. (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?

2. 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 $\mathrm{GCD}(a, p-1)$.

3. 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 $d_1 = \mathrm{GCD}(p-1, e-1)$ and $d_2 = \mathrm{GCD}(q-1, e-1)$.

4. 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?