PMAT 4282 – Cryptography — Assignment #7
Winter 2009

Instructions

- Answer each question completely; justify your answers.
- This assignment is due at: 3:00 pm on Thursday April 2nd.

1. Let p be an odd prime and let $a \geq 1$. Prove that the number of solutions in $\mathbb{Z}_p$ to the equation $x^a \equiv 1 \pmod{p}$ is $\text{GCD}(a, p-1)$.
2. Let $n = pq$ where p and q are distinct odd primes. Prove that the number of integers m, $0 \leq m < n$, such that $m^e \equiv m \pmod{n}$ is $(d_1 + 1)(d_2 + 1)$ where $d_1 = \text{GCD}(p-1, e-1)$ and $d_2 = \text{GCD}(q-1, e-1)$.
3. Let p be a prime such that $p \equiv 3 \pmod{4}$, and let $c \in \mathbb{Z}_p^*$. Prove that $x \equiv \pm c^{(p+1)/4} \pmod{p}$ is the solution to $x^2 \equiv c \pmod{p}$.
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?
5. Use Pollard's $p - 1$ algorithm to factor $n = 31294769970890356462369 20257$. What is the smallest B value that will yield a factorisation?
6. Use the Pollard ρ algorithm to factor $n = 1002468832301$.
7. Using the Quadratic Sieve Method, factor at least two of the following integers.
   (a) $n = 39961$
   (b) $n = 49981$
   (c) $n = 99067$