# MAT 301 Problem Set 4

[Posted: February 19, 2012. Due: March 12, 2012. Worth: 100 points]

**Note:** I value *succinct* and *clearly written* solutions *without unnecessary verbiage*. Such solutions will be rewarded with bonus points.

1. **RSA Weakness (20 points)**

   - (3 points) Prove the identity

   $$xy = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2$$

   - (17 points) The RSA encryption system turns out to be insecure if you choose the RSA primes $P$ and $Q$ to be very close to each other. In particular, show that if the difference between $P$ and $Q$ is at most 100 (namely, $|P - Q| \leq 100$), you can quickly find $P$ and $Q$, given only $N = PQ$ in about 100 operations.

2. **Carmichael Numbers (30 points)** Let $N = PQ$ be a product of two distinct primes $P$ and $Q$.

   (a) (10 points) Prove that if $N$ is a Carmichael number, then $P-1$ divides $N-1$, and $Q-1$ divides $N-1$.
   `[Use the fact that` $\mathbb{Z}_P^*$ `has a generator since` $P$ `is prime. So does` $Z_Q^*$`.]`

   (b) (18 points) Let $P$ be the larger of the two prime factors of $N$. Can it be the case that $P-1$ divides $N-1$? If yes, give an example of such a $P$, $Q$ and $N$. If not, why not?

   (c) (2 points) Use the parts above to show that no Carmichael number can be a product of two distinct prime numbers.

3. **Discrete Logarithms (20 points)** Compute the discrete logarithms below, whenever they exist.

   (a) Solve for an $x$ such that $2^x = 7 \pmod{19}$.

   (b) Solve for an $x$ and $y$ such that $2^x 3^y = 5 \pmod{17}$.

4. **Chinese Remaindering (30 points)** What is $18! \pmod{437}$?
   `[Hint:` $437 = 19 \cdot 23$`. Use Wilson's Theorem and the Chinese Remainder Theorem.]`