MAT 301 Problem Set 1

Posted: January 7, 2012

Due: January 21, 2012

Worth: 100 points

Problem 1: Breaking Ciphers (10 points)

The following ciphertext is encrypted under either the Caesar Cipher *or* the Scytale cipher. I am not going to tell you which. Decrypt it.

```
TSDAHTSEEWOSLOFAARCR
```

Which scheme was used to encrypt the message?

Problem 2: Euler Totient Function (20 points)

1. **(6 points)** Compute the values of the Euler Totient Function (also called the Euler Phi Function) $\phi(n)$ for the following values of n: (a) $n = 257$, (b) $n = 32768$.
2. **(6 points)** If $n = pqr$ where p, q and r are primes, what is $\phi(n)$? Prove your answer.
3. **(6 points)** Find four numbers n such that $\phi(n) = 4$.
4. **(2 points)** Find the only number n such that $\phi(n)$ is odd.

Problem 3: Greatest Common Divisors (70 points)

1. **(10 points)** Find the following greatest common divisors. Show your work. (a) gcd(252,291), and (b) gcd(16534528044,8332745927).
2. **(10 points)** Find an integer solution to each of the following equations if they exist: (a) 12a+18b = 56, and (b) 16x + 25y = 3.
3. **(15 points)** Prove that if $gcd(x, y) = 1$, then $gcd(x + y, x - y)$ is either 1 or 2.
4. **(10 points)** Are there *positive* integer solutions to

   $$202a + 74b = 7638$$

   If yes, find all of them.
5. **(10 points)** A condo building has units at two rates: most rent at \$87/week, but a few rent at \$123/week. When all are rented the gross income is \$8733/week. How many units of each type are there?

6. **(15 points)** The Fibonacci sequence of numbers $F_0, F_1, F_2, \ldots$ is defined by the following recurrence: $F_0 = 0, F_1 = 1$ and $F_i = F_{i-1} + F_{i-2}$ for all $i > 1$. Thus, the first few Fibonacci numbers are

$$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13, \ldots$$

What does the Euclidean algorithm return on input (F_i, F_{i+1})? Prove your answer. (Hint: try this out with small values of i, observe a pattern and try to generalize. One way to do the proof is using mathematical induction.).