MATH 3375 (Theory of Cryptology) – Fall 2013

Homework Assignment 1

Due: September 19

---

1. From Section 1.1, do Exercises 1, 3, 7.
2. From Section 1.2, do Exercises 7, 9.
3. Prove Theorem 1.1 (g) and (h).
4. Find $\gcd(2013, 642)$, and write the greatest common divisor as a linear combination of 2013 and 642.
5. (i) Use the Euclidean algorithm to find $\gcd(55, 34)$ and $\gcd(144, 89)$.
   (ii) Describe the pattern among the remainders when you apply the division algorithm.
   (iii) Make a conjecture about the pattern you found in part (ii). (you don't need to prove it). Find an example that verifies your conjecture.
6. Let a and b be positive integers. Prove that $\gcd(a, b) = 1$ if and only if there exists integers s and t such that $as + bt = 1$.