

CS 1050B: Constructing Proofs

Problem Set 8

Due Wednesday, Nov 29th, after the class

1. **Rosen 3.7: 2 (c)(d)(f) only**

Express the greatest common divisors of each of these pairs of integers as a linear combination of these integers.

- a) 35, 78
- b) 21, 55
- c) 124, 323

2. **Rosen 3.7: 8**

Find an inverse of 144 modulo 233.

3. **Rosen 3.7: 18**

Find all solutions to the system of congruences (using the Chinese Remainder Theorem).

$$x \equiv 2 \pmod{3}$$

$$x \equiv 1 \pmod{4}$$

$$x \equiv 3 \pmod{5}$$

4. **Rosen 3.7: 46**

Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 11 in the book. (You can use a computer algebra system or write a program to compute the modular exponentiation using Algorithm 5 in Section 3.6)