

CS 1050B: Constructing Proofs

Problem Set 8

Due Wednesday, Nov 29th, after the class

1. Rosen 3.7: 4 (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

Answer:

- a) The calculation of the greatest common divisor takes several steps:

$$\begin{aligned}78 &= 2 \cdot 35 + 8 \\35 &= 4 \cdot 8 + 3 \\8 &= 2 \cdot 3 + 2 \\3 &= 1 \cdot 2 + 1\end{aligned}$$

Then we need to work our way back up, successively plugging in for the remainders determined in this calculation:

$$\begin{aligned}1 &= 3 - 2 \\&= 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 \\&= 3 \cdot (35 - 4 \cdot 8) - 8 = 3 \cdot 35 - 13 \cdot 8 \\&= 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35) \\&= 29 \cdot 35 - 13 \cdot 78\end{aligned}$$

- b) Here are the two calculations - down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}55 &= 2 \cdot 21 + 13 \\21 &= 13 + 8 \\13 &= 8 + 5 \\8 &= 5 + 3 \\5 &= 3 + 2 \\3 &= 2 + 1\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\ &= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot (55 - 2 \cdot 21) \\ &= 21 \cdot 21 - 8 \cdot 55\end{aligned}$$

c) We compute the greatest common divisor using the Euclidean algorithm:

$$\begin{aligned}323 &= 2 \cdot 124 + 75 \\ 124 &= 75 + 49 \\ 75 &= 49 + 26 \\ 49 &= 26 + 23 \\ 26 &= 23 + 3 \\ 23 &= 7 \cdot 3 + 2 \\ 3 &= 2 + 1\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}1 &= 3 - 2 \\ &= 3 - (23 - 7 \cdot 3) = 8 \cdot 3 - 23 \\ &= 8 \cdot (26 - 23) - 23 = 8 \cdot 26 - 9 \cdot 23 \\ &= 8 \cdot 26 - 9 \cdot (49 - 26) = 17 \cdot 26 - 9 \cdot 49 \\ &= 17 \cdot (75 - 49) - 9 \cdot 49 = 17 \cdot 75 - 26 \cdot 49 \\ &= 17 \cdot 75 - 26 \cdot (124 - 75) = 43 \cdot 75 - 26 \cdot 124 \\ &= 43 \cdot (323 - 2 \cdot 124) - 26 \cdot 124 \\ &= 43 \cdot 323 - 112 \cdot 124\end{aligned}$$

2. Rosen 3.7: 8

Find an inverse of 144 modulo 233.

Answer: We need to find s and t such that $144s + 233t = 1$. then clearly s will be the desired inverse, since $144s \equiv 1 \pmod{233}$ (i.e., $144s - 1 = -233t$ is divisible by 233). To do so, we proceed as in Exercise 2. First we go through the Euclidean algorithm computation that $\gcd(144, 233) = 1$. Then we reverse our steps and write 1 as the desired linear combination $1 = 89 \cdot 144 - 55 \cdot 233$. Thus $s = 89$, so an inverse of 144 modulo 233 is 89, since $144 \cdot 89 = 12816 \equiv 1 \pmod{233}$.

3. **Rosen 3.7: 18**

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

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

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

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

Answer: Since 3, 4, and 5 are pairwise relatively prime, we can use the Chinese Remainder Theorem. The answer will be unique modulo $3 \cdot 4 \cdot 5 = 60$. Using the notation in the text, we have $a_1 = 2$, $m_1 = 3$, $a_2 = 1$, $m_2 = 4$, $a_3 = 3$, $m_3 = 5$, $m = 60$, $M_1 = 60/3 = 20$, $M_2 = 60/4 = 15$, $M_3 = 60/5 = 12$. Then we need to find inverse y_i of M_i modulo m_i for $i = 1, 2, 3$. This can be done by inspection (trial and error), since the moduli here are so small or systematically using the Euclidean algorithm (as in Example 3); we find that $y_1 = 2$, $y_2 = 3$, and $y_3 = 3$. Thus our solution is $x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \pmod{60}$. So the solutions are all integers of the form $53 + 60k$, where k is an integer.

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)

Answer: Translating the letters into numbers we have 0019 1900 0210. Thus we need to compute $C = P^{13} \pmod{2537}$ for $P = 19$, $P = 1900$, and $P = 210$. The results of these calculations, done by fast modular multiplication or a computer algebra system are 2299, 1317, and 2117, respectively. Thus the encrypted message is 2299 1317 2117.