Chapter 3 Homework 1-7, 10

1.

a) Find integers x and y such that $17x + 101y = 1$.
b) $17^{-1} \pmod{101}$.

a) Since $(17, 101) = 1$, we know there will be a unique solution to $17x + 101y = 1$. Using the Euclidean Algorithm, we have

$$\begin{aligned} 101 = 5 \cdot 17 + 16 \Rightarrow 16 &= 101 - 5 \cdot 17 \\ 17 = 1 \cdot 16 + 1 \Rightarrow 1 &= 17 - 1 \cdot 16 \\ 16 &= 16 \cdot 1 + 0 \end{aligned}$$

So, we have

$$\begin{aligned} 1 &= 17 - 1 \cdot 16 \\ &= 17 - 1 \cdot (101 - 5 \cdot 17)) \\ &= 17 - 1 \cdot 101 + 5 \cdot 17 \\ &= 6 \cdot 17 - 1 \cdot 101 \end{aligned}$$

That is, $17(6) + 101(-1) = 1$. So, $x = 6$ and $y = -1$ is a solution.

b) Using (a), we see $17^{-1} \pmod{101} \equiv 6$. Why?

$$\begin{aligned} 6 \cdot 17 - 1 \cdot 101 &= 1 \\ 6 \cdot 17 &= 102 \\ 6 \cdot 17 &\equiv 1 \text{ mod}(101) \\ 6 &\equiv \frac{1}{17} \text{ mod}(101) \\ 6 &\equiv 17^{-1} \text{ mod}(101) \end{aligned}$$

2.

a) Solve $7d \equiv 1 \pmod{30}$.
b) Suppose you write a message as a number $m \pmod{31}$. Encrypt m as $m^7 \pmod{31}$. How do you decrypt?

a) By using the product property of mods, we have

$$\begin{aligned} 13 \cdot 7d &\equiv 13 \cdot 1 \pmod{30} \\ 91d &\equiv 13 \pmod{30} \end{aligned}$$

Since $91 \equiv 1 \pmod{30}$, we have $d \equiv 13 \pmod{30}$.

b) To decode,we need to find the appropriate power to raise m^7 when taken modulo 31 to arrive at m. That is, we need to find p such that

$$(m^7)^p \equiv m (\text{mod } 31)$$

By Fermat's Little Theorem, we know $m^{30} \equiv 1 (\text{mod } 31)$. This leads to

$$\begin{aligned} m^{7p} &\equiv m \cdot (m^{30})^3 (\text{mod } 31) \\ m^{7p} &\equiv m^{91} (\text{mod } 31) \end{aligned}$$

So, $p = 13$. This means that by raising m^7 to the 13^{th} power, we will decode m^7 to result at m.

3.

a) Find all solutions of $12x \equiv 28 (\text{mod } 236)$

b) Find all solutions of $12x \equiv 30 (\text{mod } 236)$

a) $(12, 236) = 4$, we we can reduce the original congruence to $3x \equiv 7 (\text{mod } 59)$. $x = 22$ satisfies this congruence, so the solution to the original congruence is $22 + 59n$, $n = 0, 1, 2, 3$.

b) $(12, 236) = 4$, but $4 \not| 30$. However, all are even numbers, so we can reduce by a factor of 2 to get $6x \equiv 15 (\text{mod } 118)$. Since 6 and 118 are even, any choice of x will produce an even remainder, making 15 impossible. So, this has no solution.

4.

a) Use the Euclidean Algorithm to compute $gcd(30030, 257)$.

b) Using the result of part (a) and the fact that $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, show that 257 is prime.

a) $(30030, 257) = (257, 218) = (218, 39) = (39, 23) = 1$

b) $13 < \sqrt{257} < 17$, so only primes less than equal to 13 need to be considered. But, since $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ and since $(30030, 57) = 1$, we can conclude that 257 is prime.

5.

a) Compute $gcd(4883, 4369)$.

b) Factor 4883 and 4369 into the product of primes.

a) $(4883, 4369) = (4369, 514) = (514, 257) = 257$

b) $4883 = 19 \cdot 257$ and $4369 = 17 \cdot 257$

6.

a) Let $F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$ define the Fibonacci numbers $1, 1, 2, 3, 5, 8, \cdots$ Use the Euclidean Algorithm to compute $gcd(F_n, F_{n-1})$ for all $n \geq 1$.

b) Find $gcd(11111111, 11111)$.

c) Let $a = 111\cdots11$ be formed with F_n repeated 1's and let $b = 111\cdots11$ be formed with F_{n-1} repeated 1's. Find $gcd(a, b)$.

a) $(F_n, F_{n-1}) = 1$

b) $(11111111, 11111) = (11111, 111) = (111, 11) = (11, 1) = 1$

c) $(a, b) = 1$

7.

a) Let p be prime. Suppose a and b are integers such that $ab \equiv 0 (\text{mod } p)$. Show that either $a \equiv 0$ or $b \equiv 0 (\text{mod } p)$.

b) Show that if a, b, n are integers with $n|ab$ and $gcd(a, n) = 1$ then $n|b$.

a) $ab \equiv 0 (\text{mod } p)$ implies that $p|ab$, which means that $p|a$ or $p|b$. If $p|a$ then $a \equiv 0 (\text{mod } p)$ and if $p|b$ then $b \equiv 0 (\text{mod } p)$.

b) $n|ab$ implies that $ab \equiv 0 (\text{mod } n)$. So, $n|a$ or $n|b$. But, since $n \not| a$, it must be so that $n|b$.

10. A group of people are arranging themselves for a parade. If they line up three to a row, one person is left over, if they line up four to a row, there are two people left over, and if they line up five to a row, three people are left over. What is the smallest number of people? What is the next smallest number?

We can express this situation with the congruences

$$x \equiv 1 (\text{mod } 3)$$
$$x \equiv 2 (\text{mod } 4)$$
$$x \equiv 3 (\text{mod } 5)$$

First consider the first two congruences. by the Chinese Remainder Theorem, we are looking for the unique solution to both and we see that

$$10 \equiv 1 (\text{mod } 3)$$
$$10 \equiv 2 (\text{mod } 4)$$

So $x \equiv 10 (\text{mod } 12)$.
Now, can consider this congruence with the third original one.

$$x \equiv 10 (\text{mod } 12)$$
$$x \equiv 3 (\text{mod } 5)$$

By trial and error (because we are working with small integers) we wee that

$$58 \equiv 10 (\text{mod } 12)$$
$$58 \equiv 3 (\text{mod } 5)$$

So, $x \equiv 58 (\text{mod } 60)$ and therefore 58 is the x we seek.

The next integer that satisfies all three of these simultaneously is 118. We can find this as the solutions will be of the form $x \equiv 58 + 60k$ for some integer k.