CSE232: Discrete Mathematics
Assignment 4: Suggested answers

November 28, 2020

---

1. The following text has been encoded using a shift cipher. Find the plaintext message, and explain how you proceeded.

"AOPZ PZ AOL SHZA HZZPNUTLUA VM AOL ZLTLZALY"

Answer. A shift cipher uses a function $f(p) = (p + k) \bmod 26$ to encrypt the message, where p is the index of the letter we consider in the alphabet. So A is identified with 0, B with 1, ..., Z with 25. To decipher the message, we need to find k, and then apply the function f^{-1} defined by $f^{-1}(p) = (p - k) \bmod 26$.

In the message above, the most frequent letters are: Z (7 occurrences), L (6), A (6). So it is likely that E is one of them.

We first try with $f(E) = Z$, which means that $25 = 4 + k$, and thus $k = 21$. So $f^{-1}(p) = p - 21 \bmod 26 = p + 5 \bmod 26$ for all p. Then the first word AOPZ corresponds to 00 14 15 25, which is mapped by f^{-1} to 05 19 20 04 which is FTUE. Clearly this is not the answer.

So we try with $f(E) = L$, which means that $11 = 4 + k$, and thus $k = 7$.So $f^{-1}(p) = p + 19 \bmod 26$ for all p. Then the first word AOPZ corresponds to THIS. So 7 appears to be the key. We apply f^{-1} to the rest of the message, and obtain:

"THIS IS THE LAST ASSIGNMENT OF THE SEMESTER"

2. Compute $g = \gcd(476, 364)$ using the Euclidean algorithm. Using the intermediate results in this calculation, show how to write $g = 476 \cdot s + 364 \cdot t$ where $s, t \in \mathbb{Z}$.

Answer. We first compute $\gcd(476, 364)$ with the Euclidean algorithm.

$$\begin{aligned} 476 &= 364 \times 1 + 112 \\ 364 &= 112 \times 3 + 28 \\ 112 &= 28 \times 4 \end{aligned}$$

Therefore, $g = 28$. From the calculation above,

$$\begin{aligned} 28 &= 364 - 112 \times 3 \\ &= 364 - 3 \times (476 - 364) \\ &= 4 \times 364 - 3 \times 476, \end{aligned}$$

and thus $s = -3$, $t = 4$.

3. Prove that the product of any three consecutive integers is divisible by 6.

Answer. Let n, $n+1$, $n+2$ be these three integers. At least one of these three integers must be divisible by 2, and one of them is divisible by 3. Let $N = n(n+1)(n+2)$ denote their product, then $2 \mid N$ and $3 \mid N$. So the exponent of 2 in the prime factorization of N is at least 1, and the exponent of 3 is at least 1. It follows that $6 = 2 \times 3 \mid N$.

4. Prove that for all positive integers a, b and c, if $a \mid c$ and $b \mid c$, then $\text{lcm}(a, b) \mid c$.

Answer. Let $\ell = \text{lcm}(a, b)$. By definition of ℓ, we have $\ell \leqslant c$. If $\ell = c$ then we are done, so we may assume that $\ell < c$.

For sake of contradiction, suppose that $\ell \nmid c$. Let $d = c \bmod \ell$, and thus $0 < d < \ell$. Then $\ell \mid c - d$. As a and b divide ℓ, then a and b divide $c - d$. As a and b divide c, it follows that a and b divide d. Hence, d is a multiple of a and b that is smaller than $\ell = \text{lcm}(a, b)$, a contradiction.

5. Let a, b and n be three positive integers such that $\gcd(a, b) = 1$, $a \mid n$ and $b \mid n$. Prove that $ab \mid n$. [Hint: use the result of Question 4.]

Answer. By Question 4, since $a \mid n$ and $b \mid n$, we have $\text{lcm}(a, b) \mid n$. As $\gcd(a, b) = 1$, we know $ab = \gcd(a, b) \cdot \text{lcm}(a, b) = \text{lcm}(a, b)$ from Theorem 5 in Section 4.3. It follows that $ab \mid n$.

6. Prove that for all integers a, b and c, if $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.

Answer. Consider the Euclidean algorithm for computing $\gcd(a, b)$. It constructs a sequence of remainders r_i such that $r_i = r_{i+1}q_{i+1} + r_{i+2}$, starting from $r_0 = a$ and $r_1 = b$, and until $r_n = \gcd(a, b)$ and $r_{n+1} = 0$.

So $r_0 = r_1 q_1 + r_2$, which means that $r_2 = a - bq_1$. As c divides a and b, it implies that $c \mid r_2$. Similarly, as $c \mid r_1$ and $c \mid r_2$, it follows that $c \mid r_3$. So we can say that $c \mid r_n$, which means that $c \mid \gcd(a, b)$.

7. Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2 of Section 4.4. (forward & backward passes through the divisions of the Euclidean algorithm).

(a) $a = 4, m = 9$

(b) $a = 19, m = 141$

Answer a. First, we use the Euclidean algorithm to find $\gcd(4, 9)$.

$$9 = 4 \cdot 2 + 1$$
$$4 = 1 \cdot 4.$$

Now we obtain

$$\gcd(4, 9) = 1 = 9 + 4 \cdot (-2).$$

The last equation tells that $-2 \bmod 9 = \mathbf{7}$ is the multiplicative inverse of 4 modulo 9.

Answer b. First, we use the Euclidean algorithm to find $\gcd(141, 19)$.

$$\begin{aligned}141 &= 19 \cdot 7 + 8\\ 19 &= 8 \cdot 2 + 3\\ 8 &= 3 \cdot 2 + 2\\ 3 &= 2 \cdot 1 + 1\\ 2 &= 1 \cdot 2.\end{aligned}$$

Now we obtain

$$\begin{aligned}\gcd(141, 19) = 1 &= 3 - 2 \cdot 1\\ &= 3 - (8 - 3 \cdot 2) \cdot 1 = 3 \cdot 3 - 8\\ &= (19 - 8 \cdot 2) \cdot 3 - 8 = 19 \cdot 3 - 8 \cdot 7\\ &= 19 \cdot 3 - (141 - 19 \cdot 7) \cdot 7\\ &= 19 \cdot 52 + 141 \cdot (-7)\end{aligned}$$

The last equation tells that **52** is the multiplicative inverse of 19 modulo 141.

8. Show that if m is an integer greater than 1 and $ac \equiv bc \pmod m$, then $a \equiv b \pmod{m/\gcd(c, m)}$.

Answer. Let $m' = m/\gcd(c, m)$. Because all the common factors of m and c are divided out of m to obtain m', it follows that m' and c are relatively prime. Because m divides $ac - bc = (a - b)c$, it follows that m' divides $(a - b)c$. By Lemma 2 in Section 4.3, we see that m' divides $(a - b)$, so $a \equiv b \pmod{m'}$.

9. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences

$$\begin{aligned}x &\equiv 1 \pmod 2\\ x &\equiv 2 \pmod 3\\ x &\equiv 3 \pmod 5\\ x &\equiv 4 \pmod{11}.\end{aligned}$$

For example, the answer can be written as follow: the solutions to the system of congruences are all integers of the form $a + bk$, where k is an integer (so the problem is equivalently to find a and b in this form).

Answer. To solve the system of congruences, first let $m = 2 \cdot 3 \cdot 5 \cdot 11 = 330$, $\widehat{m}_1 = m/2 = 165$, $\widehat{m}_2 = m/3 = 110$, $\widehat{m}_3 = m/5 = 66$, and $\widehat{m}_4 = m/11 = 30$. Let y_k be an inverse of $\widehat{m}_k$ modulo m_k for $k = 1, 2, 3, 4$. Then,

- $y_1 = 1$ is an inverse of 165 modulo 2, because $165 \cdot 1 \equiv 1 \pmod 2$;
- $y_2 = 2$ is an inverse of 110 modulo 3, because $110 \cdot 2 \equiv 1 \pmod 3$;
- $y_3 = 1$ is an inverse of 66 modulo 5, because $66 \cdot 1 \equiv 1 \pmod 5$;
- $y_4 = 7$ is an inverse of 30 modulo 11, because $30 \cdot 7 \equiv 1 \pmod{11}$;

The solutions to this system are those x s.t.

$$\begin{aligned} x &\equiv 1 \cdot \widehat{m}_1 \cdot y_1 + 2 \cdot \widehat{m}_2 \cdot y_2 + 3 \cdot \widehat{m}_3 \cdot y_3 + 4 \cdot \widehat{m}_3 \cdot y_3 \\ &\equiv (1 \cdot 165 \cdot 1) + (2 \cdot 110 \cdot 2) + (3 \cdot 66 \cdot 1) + (4 \cdot 30 \cdot 7) \\ &\equiv 1643 \equiv 323 \pmod{330}. \end{aligned}$$

It follows that 323 is the smallest positive integer that is a simultaneous solution. We conclude that the solutions to the system of congruences are all integers of the form $323 + 330k$, where k is an integer.

10. What is the remainder when $(1! + 2! + 3! + 4! + 5! + 6! + \cdots)$ is divided by 9?

Answer. It is easy to know that $k! \equiv 0 \pmod 9$ for all $k \geqslant 6$. Thus, it suffices to find $(1! + 2! + 3! + 4! + 5!) \pmod 9$. Then, we have

$$\begin{aligned} 1! &\equiv 1 \pmod 9 \\ 2! &\equiv 2 \pmod 9 \\ 3! &\equiv 6 \pmod 9 \\ 4! &\equiv 6 \pmod 9 \\ 5! &\equiv 3 \pmod 9 \end{aligned}$$

Therefore, $(1! + 2! + 3! + 4! + 5!) \equiv 1 + 2 + 6 + 6 + 3 \equiv 18 \equiv 0 \pmod 9$, so the remainder is **0.**