UWO CS2214

Tutorial #4

Problem 1 1. Find all integers x such that $0 \leq x < 15$ and $4x + 9 \equiv 13 \mod 15$. Justify your answer.

2. Find all integers x such that $0 \leq x < 15$, $x \equiv 1 \mod 3$ and $x \equiv 2 \mod 5$. Justify your answer.
3. Find all integers x and y such that $0 \leq x < 15$, $0 \leq y < 15$, $x + 2y \equiv 4 \mod 15$ and $3x - y \equiv 10 \mod 15$. Justify your answer.

Solution 1

1. We have $4 \times 4 \equiv 1 \mod 15$. That is, 4 is the inverse of 4 modulo 15. We multiply by 4 each side of:
$$4x + 9 \equiv 13 \mod 15,$$
leading to:
$$x + 4 \times 9 \equiv 4 \times 13 \mod 15,$$
that is:
$$x \equiv 4(13 - 9) \mod 15,$$
which finally yields: $x \equiv 1 \mod 15$.
2. We apply the Chinese Remainder Theorem (as stated in Assignment 2). Using the notations of Assignment 2, we have $m = 3$, $n = 5$, $a = 1$, $b = 2$. We need s and t such that $s\,m + t\,n = 1$, hence we can choose $s = 2$ and $t = -1$. Then, we have
$$c \equiv a + (b - a)\,s\,m \equiv 1 + (2 - 1) \times 2 \times 3 \equiv 7 \mod 15.$$
3. We eliminate y in order to solve for x first. Multiplying $3x - y \equiv 10 \mod 15$ by 2 yields $6x - 2y \equiv 5 \mod 15$. Adding this equation side-by-side with $x + 2y \equiv 4 \mod 15$ yields $7x \equiv 9 \mod 15$. Since $7 \times 13 \equiv 1 \mod 15$, we have $x \equiv 9 \times 13 \mod 15$, that is, $x \equiv 12 \mod 15$. Substituting x with 12 into $3x - y \equiv 10 \mod 15$ yields $y \equiv 11 \mod 15$.

Problem 2 Consider the affine cipher model $c = 5p + 3$ (**mod** 26).

1. Produce ciphertext for “GOOD”

2. Find the unique inverse $\bar{a}$ for $a = 5$ modulo 26 such that $\bar{a}a \equiv 1 \pmod{26}$
3. Specify the inverse function $p(c)$ for $c = 5p + 3$ (**mod** 26).

Solution 2

1. Denote by f the function from $\mathbb{Z}_{26}$ to $\mathbb{Z}_{26}$ which maps p to $5p + 3$ (**mod** 26). The letters G, O, D are mapped to 7, 14, 3 in $\mathbb{Z}_{26}$. Their images by f are 7, 21, 18, which coorrespond to the letters H, V, S. Hence, the ciphertext for GOOD is HVVS.
2. We note that $\gcd(5, 26) = 1$, thus 5 is invertible modulo 26 and we have $5 \times 21 \equiv 1 \mod 26$. From there, it is easy to check that f is injective and srujective. (You should try it). The inverse function of f is:

$$f^{-1} : \begin{array}{ccc} \mathbb{Z}_{26} & \rightarrow & \mathbb{Z}_{26} \\ c & \longmapsto & 21c + 15 \ (\mathbf{mod}\ 26) \end{array}$$

Problem 3 Periodicals are identified using an **International Standard Serial Number (ISSN)**. An ISSN consists of two blocks of four digits. The last digit in the second block is a check digit. This check digit is determined by the congruence

$$d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}$$

The letter X is used to represent the “digit” 10.

1. Given the seven digits $1570 - 868$ of an ISSN, determine the check digit (which may be the letter X).
2. Is the eight-digit $1007 - 120X$ code a possible ISSN? That is, does it end with a correct check digit?

Solution 3

1.
2.