MATH220

Discrete Mathematics and Cryptography

Tutorial 3 **Week starting 9 March 2020**

---

1. By trial and error, find a multiplicative inverse of

(a) 3 mod 7 and

(b) 5 mod 11.

2. Use Euclid's algorithm to find a multiplicative inverse of

(a) 21 mod 25 and

(b) 12 mod 29.

3. Draw the multiplication table for $\mathbb{Z}_{12}^*$. Use this to find the inverse of each element in $\mathbb{Z}_{12}^*$.

4. Solve each of the following congruence equations:

(a) $2x \equiv 1 \bmod 17$, and

(b) $40x \equiv 777 \bmod 1777$.

5. Solve the system of simultaneous equations for x and y:

$$x + 2y \equiv 3 \bmod 7$$
$$3x + y \equiv 2 \bmod 7$$

6. In the U.S., identification numbers printed on bank cheques consist of an eight digit number $a_1a_2 \cdots a_8$ and a check digit a_9 so that

$$7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 + 9a_9 \equiv 0 \bmod 10$$

Show that this method detects all single-digit errors, that is, errors where only one digit is changed.

7. Construct the multiplication table for $\mathbb{Z}_{15}^*$ and answer the following:

(a) For each element $g \in \mathbb{Z}_{15}^*$, find g^{-1} from this table.

(b) For each element g, calculate the powers $g, g^2, \cdots, g^k$ stopping when $g^k = 1$. (This value of k is called the *order* of g.)

(c) If $g^k = 1$, explain why $g^{k-1} = g^{-1}$.

8. Let m be a positive integer, and let $a \in \mathbb{Z}_m^*$. Prove that a is invertible if and only if there is a positive integer k such that $a^k = 1$ in $\mathbb{Z}_m$.

9. Let $m \geq 3$. Show that $|\mathbb{Z}_m^*|$ is even, that is, the number of invertible elements in $\mathbb{Z}_m$ is even.

Hint. Consider the element $m - 1$.

10. Compute $3^{75} \bmod 73$.

11. If p is a prime number and a is a positive integer, show that

$$a^{(p-1)!+1} \equiv a \bmod p.$$

12. Use Euclid's Algorithm to find 38^{-1} in $\mathbb{Z}_{51}$.