IS309: Network Security Technology
Tutorial 4, Week 4 (March 16)
Due Date: March 23

Chunyu Xue 518021910698

1 Problem 1

(10 points) Determine whether 227 and 79 are relatively prime.

Solution We use **Euclidean Algorithm** to compute $gcd(227, 79)$.

$$\begin{aligned} 227 &= 79 \times 2 + 69 \\ 79 &= 69 \times 1 + 10 \\ 69 &= 10 \times 6 + 9 \\ 10 &= 9 \times 1 + 1 \\ 9 &= 1 \times 9 + 0 \end{aligned} \tag{1}$$

Therefore, we have $gcd(227, 79) = 1$, that is, 227 and 79 are relatively prime.

2 Problem 2

(10 points) Find the multiplicative inverse of $79 \bmod 229$.

Solution We use **Extended Euclidean Algorithm** to solve this problem.
First, we use **Euclidean Algorithm** to compute $gcd(229, 79)$

$$\begin{aligned} 229 &= 79 \times 2 + 71 \\ 79 &= 71 \times 1 + 8 \\ 71 &= 8 \times 8 + 7 \\ 8 &= 7 \times 1 + 1 \\ 7 &= 1 \times 7 + 0 \end{aligned} \tag{2}$$

Therefore, we have $gcd(229, 79) = 1$, that is:

$$\begin{aligned} 1 &= 8 - 7 \times 1 \\ &= 8 - (71 - 8 \times 8) \times 1 = 9 \times 8 - 71 \\ &= 9 \times (79 - 71 \times 1) - 71 = 9 \times 79 - 10 \times 71 \\ &= 9 \times 79 - 10 \times (229 - 79 \times 2) = 29 \times 79 - 10 \times 229 \end{aligned} \tag{3}$$

Therefore, we have $(29 \times 79 - 10 \times 229) \bmod 229 = 29 \times 79 \bmod 229 = 1$. That is, the multiplicative inverse of 79 mod 229 is 29.

3 Problem 3

(10 points) Without calculating anything, by simply looking at the numbers, can you tell whether 7932 has a multiplicative inverse mod 11958? Explain your solution.

Solution It's obvious that 7932 doesn't have a multiplicative inverse mod 11958, and the reason is that:

No matter which number does 7932 multiply, the result must be an even number, and since 11958 is also even, $n \equiv 1 (\text{mod } 11958)$ must requires that n is an odd number. Therefore, 7932 doesn't have a multiplicative inverse mod 11958.

4 Problem 4

(20 points) Show the steps of how to calculate $\phi(315)$.

Solution We first operate **Prime Factorization** on 315, we have:

$$315 = 7 \times 5 \times 3^2$$

Then according to the **Factorization Property**, we have that:

$$\phi(315) = 315 \times (1 - 1/7) \times (1 - 1/5) \times (1 - 1/3) = 144$$

Therefore, we have $\phi(315) = 144$.

5 Problem 5

(20 points) Calculate $227^{54996213} \bmod 21$ as efficient as possible.

Solution We first use Euclidean Algorithm to prove that 227 and 21 are relatively prime.

$$\begin{aligned} 227 &= 21 \times 10 + 17 \\ 21 &= 17 \times 1 + 4 \\ 17 &= 4 \times 4 + 1 \\ 4 &= 1 \times 4 + 0 \end{aligned} \tag{4}$$

That is, $gcd(227, 21) = 1$. Then, according to Generalization of **Fermat's little Theorem**, we know that:

$$
\begin{aligned}
227^{54996213} \bmod 21 &= 227^{54996213 \bmod \phi(21)} \bmod 21 \\
&= 227^{54996213 \bmod 12} \bmod 21 \\
&= 227^{9} \bmod 21 \\
&= (227^4 \times 227^2 \times 227^2 \times 227) \bmod 21 \\
&= ((17^4 \bmod 21) \times (17^2 \bmod 21) \times (17^2 \bmod 21) \times 17) \bmod 21 \\
&= (4 \times 16 \times 16 \times 17) \bmod 21 \\
&= 20
\end{aligned} \tag{5}
$$

6 Problem 6

(30 points) Determine whether the following groups are cyclic. If they are, give a generator of the group.

1. $(Z_5, +)$ (i.e., the set of numbers modulo 5 with addition as the group operation)
2. $(Z_8^*, \times)$

Solution We have:

1. $Z_5 = \{0, 1, 2, 3, 4\}$ is cyclic group, and a generator of it is 1.

   Prove.

$$
\begin{gathered}
i = 1: \ 1 \bmod 5 = 1 \\
i = 2: \ (1+1) \bmod 5 = 2 \\
i = 3: \ (1+1+1) \bmod 5 = 3 \\
i = 4: \ (1+1+1+1) \bmod 5 = 4 \\
i = 5: \ (1+1+1+1+1) \bmod 5 = 0
\end{gathered}
$$

   Prove completed.

2. $Z_8^* = \{1, 3, 5, 7\}$ is not a cyclic group.

   Prove Obviously 1 can't be the generator.
   For 3, we can know that $3^n \bmod 8 = 3^{n \bmod \phi(8)} \bmod 8 = 3^{n \bmod 4} \bmod 8 \in \{1, 3\}$
   For 5, we can know that $5^n \bmod 8 = 5^{n \bmod \phi(8)} \bmod 8 = 5^{n \bmod 4} \bmod 8 \in \{1, 5\}$
   For 7, we can know that $7^n \bmod 8 = 7^{n \bmod \phi(8)} \bmod 8 = 7^{n \bmod 4} \bmod 8 \in \{1, 7\}$
   Prove completed.