Optional Homework (7)

Distributions of $Y = g^U \mod n$

In this analysis, we explore the behavior of the modular exponentiation function $Y = g^U \mod n$ for different values of g and n, where U ranges from 1 up to a maximum value $\max(\mathrm{U})$.
We focus on understanding how the choice of g and n affects the distribution of residues Y, and we compute the entropy of these distributions to quantify their randomness.

Modular Exponentiation and Residues

The expression $Y = g^U \mod n$ computes the remainder when g^U is divided by n. The set of possible residues Y depends on the properties of g and n:

- **For prime n**: The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic of order $n-1$.
- **Primitive roots**: An integer g is a primitive root module n if its powers generate all elements of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Case Studies

Case A: $n = 19$, $g \in \{2, 3, 10, 17\}$

- **Prime modulus**: Since 19 is prime, $(\mathbb{Z}/19\mathbb{Z})^\times$ is cyclic with 18 elements.
- **Residue distribution**:
  - If g is a primitive root module 19, Y will uniformly distribute over all integers from 1 to 18.
  - **Example**: If $g = 2$, which is a primitive root module 19, then:

$$\{2^U \mod 19 \mid U = 1, 2, \ldots, 18\} = \{2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1\}$$

Case B: $n = 15$, $g \in \{3, 6, 9, 12\}$

- **Composite modulus**: 15 is not prime, and $(\mathbb{Z}/15\mathbb{Z})^\times$ has order $\phi(15) = 8$.
- **Residue distribution**:
  - The residues may not cover all numbers from 1 to 14.
  - **Example**: For $g = 3$:

$$\{3^U \mod 15 \mid U = 1, 2, \ldots\} = \{3, 9, 12, 6, 3, 9, \ldots\}$$

  - The sequence repeats every 4 steps due to the order of 3 module 15 being 4.

Entropy of Residue Distributions

Entropy measures the randomness of a distribution:

$$H = -\sum_i p_i \log_2 p_i$$

where p_i is the probability of residue i.

- **Uniform distribution**: Maximizes entropy.
- **Non-uniform distribution**: Results in lower entropy.

Mathematical Analysis

Primitive Roots and Uniformity

- **Definition**: g is a primitive root modulo n if:

$$\{g^U \mod n \mid U = 1, 2, \ldots, \phi(n)\} = (\mathbb{Z}/n\mathbb{Z})^\times$$

- **Implication**: The residues are uniformly distributed over $(\mathbb{Z}/n\mathbb{Z})^\times$.

Orders and Periodicity

- **Order of g**: The smallest positive integer k such that:

$$g^k \equiv 1 \mod n$$

- **Residue cycle**: The sequence $g^U \mod n$ repeats every k steps.
- **Non-primitive roots**: If k divides $\phi(n)$ but $k \neq \phi(n)$, the residues cover only a subset of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Calculating Entropy

1. **Compute frequencies**: Count how many times each residue appears for $U = 1$ to $\max(\mathrm{U})$.
2. **Calculate probabilities**:

$$p_i = \frac{\text{Frequency of residue } i}{\text{Total number of exponents } (\max\mathrm{U})}$$

3. **Compute entropy**:

$$H = -\sum_i p_i \log_2 p_i$$

Observations and Conclusion

- **Case A**:
  - When g is a primitive root (e.g., $g = 2$), the entropy is high, indicating a uniform distribution.
  - For non-primitive roots, entropy decreases.
- **Case B**:
  - The entropy is generally lower due to the composite modulus and the lack of primitive roots that generate the full multiplicative group.

The distribution of $Y = g^U \mod n$ is significantly influenced by the choice of g and n:

- **Prime modulus with primitive root g**: Leads to a uniform residue distribution and maximum entropy.
- **Composite modulus or non-primitive root g**: Results in a non-uniform distribution with lower entropy.

Understanding these properties is crucial in fields like cryptography, where the unpredictability of residues is essential for security.