CRYPTOGRAPHY HANDOUT 11

FERMAT'S LITTLE THEOREM AND EULER'S THEOREM

Based on Number Theory Through Inquiry (Marshall, Odell, and Starbird).

1. Fermat's Little Theorem and Euler's Theorem

Question 1. *Choose some relatively prime natural numbers a and n and compute the order of a modulo n. Frame a conjecture concerning how large the order of a modulo n can be, depending on n.*

You might have noticed that until the power was congruent to 1 modulo n, the values modulo n never repeated. This is summarized in the theorem:

Theorem 1. *Let a and n be natural numbers with $\gcd(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. Then the numbers $a^1, a^2, a^3, \cdots, a^k$ are pairwise incongruent modulo n.*

Another way to look at this theorem is the following:

Theorem 2. *Let a and n be natural numbers with $\gcd(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. For any natural number m, a^m is congruent modulo n to one of the numbers $a^1, a^2, a^3, \cdots, a^k$.*

Question 2. *Come up with an explicit example of Theorem 2:*

An observation you might have made when doing Question 1 is that, in the definition $a^k \equiv 1 \mod n$, the order k of a natural number in is less than n:

Theorem 3. *Let a and n be natural numbers with $\gcd(a, n) = 1$. Then $\mathrm{ord}_n(a) < n$.*

Question 3. *Compute $a^{p-1} \mod p$ for various numbers a and primes p. Write down any patterns or observations.*

Theorem 4. *Let p be a prime number and let a be an integer such that* $\gcd(a, p) = 1$*. Then $R = \{a, 2a, 3a, \cdots, pa\}$ is a complete residue system modulo p. In other words, no two elements of R are congruent modulo p.*

Question 4. *Double check Theorem 4 by explicitly writing out the elements of R for the following two cases:*

1. $p = 3, a = 8$

2. $p = 5, a = 12$

Theorem 5. *Let p be a prime number and let a be an integer such that* $\gcd(a, p) = 1$*. Then $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$.*

Question 5. *Verify Theorem 5 with the examples:*

1. $p = 3, a = 8$

2. $p = 5, a = 12$

Theorem 5 can be used to prove Fermat's Little Theorem:

Fermat's Little Theorem. Let p be a prime number and let a be an integer such that $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \mod p$.

Euler's Theorem can be seen as a generalization of Fermat's Little Theorem but for composite numbers.

Definition. For a natural number n, the Euler phi-function $\varphi(n)$ is equal to the number of natural numbers less than or equal to n that are relatively prime to n.

Euler's Theorem. Let a and n be integers with $n > 0$ such that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \mod p$.

2. Three-Pass Protocol

Alice wants to send a secret message K to Bob.

Idea.

1. Alice puts K in a box and locks it. She sends the locked box to Bob.
2. Bob puts his lock on the box and sends it back to Alice.
3. Alice takes her lock off and sends it to Bob.
4. Bob takes his lock off, opens the box, and finds K.

Math.

0. Everyone agrees upon a large prime p. Alice chooses a random number a with $\gcd(a, p) = 1$, and Bob chooses a random number b with $\gcd(b, p) = 1$.
1. Alice sends $K_1 \equiv K^a \mod p$ to Bob.
2. Bob sends $K_2 \equiv K_1^b \mod p$ to Alice.
3. Alice sends $K_3 \equiv K_2^{a^{-1}} \mod p$ to Bob.
4. Bob computes $K \equiv K_3^{b^{-1}} \mod p$ and gets the message K.