CRYPTOGRAPHY HANDOUT 12

PRIMITIVE ROOTS

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

1. Review

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

2. Primitive Roots

Definition. Let p be a prime. An integer g such that $\mathrm{ord}_p(g) = p - 1$ is called a *primitive root modulo p*.

Theorem 1. *Let p be a prime and suppose g is a primitive root modulo p. Then the set $\{0, g, g^2, g^3, \cdots, g^{p-1}\}$ forms a complete residue system modulo p.*

Question 1. *For each of the primes p less than 20, find a primitive root and make a chart showing what powers of the primitive root gives each of the natural numbers less than p. Note any observations.*

You might observe the following:

Theorem 2. *Every prime p has a primitive root.*

This is another example of an existence theorem.

Question 2. *Consider the prime $p = 13$. For each divisor $d = 1, 2, 3, 4, 6, 12$ of $12 = p - 1$, mark which of the natural numbers in the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ have order d.*

You might have observed that there are $\varphi(d)$ numbers of order d for each d. So in the case of 12, we have

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)=12=\sum_{d|12}\varphi(d)=12.$$

In general, the more compact way of writing this is

$$\sum_{d|n}\varphi(d)$$

which means the sum of the Euler-φ function of the natural number divisors of the natural number n. There is a more general relationship between the Euler-φ function and divisors, which we'll explore next.

3. Euler-φ and the sums of divisors

Question 3. *Compute the following sums, and make any conjectures based on the patterns you notice. (In particular, notice which numbers n are primes, powers of primes, or products of primes).*

1. $\sum_{d|6}\varphi(d)$

2. $\sum_{d|7}\varphi(d)$

3. $\sum_{d|24} \varphi(d)$

4. $\sum_{d|36} \varphi(d)$

5. $\sum_{d|27} \varphi(d)$

It turns out that we have a series of theorems based on these:

Lemma 3. *If p is a prime, then* $\sum_{d|p} \varphi(d) = p$.

Lemma 4. *If p is a prime, then* $\sum_{d|p^k} \varphi(d) = p^k$.

Lemma 5. *If p and q are two different primes, then* $\sum_{d|pq} \varphi(d) = pq$.

Theorem 6. *If n is a natural number, then* $\sum_{d|n} \varphi(d) = n$.

Using the previous theorem, we can prove the following statement:

Theorem 7. *Every prime p has $\varphi(p-1)$ primitive roots.*

Example.