Week 1: Number Theory - Euler Phi Function, Order and Primitive Roots

1 Greatest Common Divisor and the Euler Phi Function

Consider the following problem.

Exercise 1.1 *Let n be a positive integer and d a positive integer such that d divides n. Amongst the fractions*

$$\frac{1}{n}, \frac{2}{n}, \cdots, \frac{1}{n}$$

written in lowest terms, how many of these fractions have denominator d?

Your first thought should definitely be that this problem is related to the notion of *greatest common divisor*. A fraction $\frac{a}{n}$ has denominator d for some $a \in \{1, \cdots, n\}$ if and only if the numerator and denominator are divided by $\frac{n}{d}$ to reduce the fraction to lowest terms. Hence, $\gcd(a/(n/d), d) = 1$, or equivalently, $\gcd(a, n) = \frac{n}{d}$.

Therefore, **the number of such fractions with denominator d is equal to the number of positive integers $a \in \{1, \cdots, n\}$ such that $\gcd(a, n) = \frac{n}{d}$, or equivalently, $\gcd(a/(n/d), d) = 1$.**

For each positive integer n, let $\varphi(n)$ denote the number of positive integers that is at most n and relatively prime to n.

Example 1.2 *$\varphi(12) = 4$, since $\{1, 5, 7, 11\}$ are the only positive integers from 1 to 12 that are relatively prime to 12 and there are four such numbers.*

Let's return to Exercise **??**. Let S_d be the set of the fractions in Exercise **??** with denominator d. Try the following exercise.

Exercise 1.3 *Prove that $|S_d| = \varphi\left(\frac{n}{d}\right)$.*

Based on this exercise, try to prove the following useful result:

Theorem 1.4 *For any positive integer n, prove that*

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

This is an **awesome** result that can come in extremely handy. It is well known enough that you can state it without proof on a competition. But just in case, do know the proof of this result. Now, try the following exercises.

1. Let $n \geq 3$ be a positive integer. n lilypads are placed in a circle, with one lilypad marked *start*. There are n frogs, labeled $1, \cdots, n$, such that frog k in one leap jumps k lilypads in the clockwise direction. For each $k \in \{1, \cdots, n\}$, if frog k is at *start*, how many (positive number of) leaps does the frog make to return to *start* for the first time?

2. (University of Waterloo Big E Competition 1998) Let x be a positive real number such that $|x| < 1$. Prove that

$$\sum_{a,b \geq 0, a+b \geq 1, \gcd(a,b)=1} \frac{x^{a+b}}{1-x^{a+b}} = \frac{x}{(1-x)^2}.$$

2 What Is Your Order Your Majesty?

We recall two important theorems in number theory.

Theorem 2.1 ***Euler's Theorem:*** *Let n be a positive integer and a be a positive integer such that $\gcd(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Of course, Euler's Theorem has a famous child.

Theorem 2.2 ***Fermat's Little Theorem:*** *Let p be a prime number and a a positive integer not divisible by p. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Euler's theorem tells you that the sequence $a^0, a, a^2, a^3, \cdots \pmod{n}$ does eventually reach 1, is periodic, and reaches 1 at $a^{\varphi(n)}$. Of course, this may not be the *first* time that the sequence $a, a^2, a^3 \cdots \pmod{n}$ reaches 1. It is possible that the sequence reaches 1 well before $a^{\varphi(n)}$. But when? Good question. One thing for certain is that there is some *smallest* positive integer m such that $a^m \equiv 1 \pmod{n}$. hmmm.. Maybe we should give m a name.

Definition 2.3 *Let n, a be positive integers such that $\gcd(a, n) = 1$. The smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ is called the order of a modulo n. This is denoted by $ord_n(a)$.*

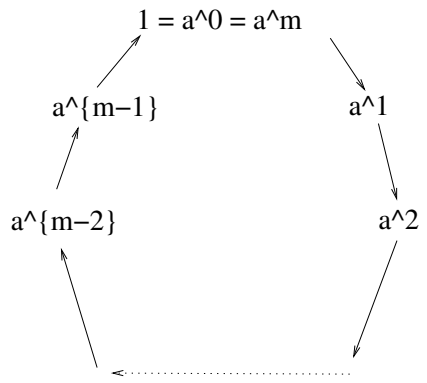

Figure 1: Demonstrating Order

Example 2.4

1. *$ord_{15}(2) = 4$, since $2^4 \equiv 1 \pmod{15}$ and $2, 2^2, 2^3 \not\equiv 1 \pmod{15}$, i.e. we need to reach the fourth term in the sequence $2, 2^2, 2^3, \cdots$ before we reach one that is congruent to 1 modulo 15.*

2. *$ord_7(3) = 6$, since $3^6 \equiv 1 \pmod{7}$ and $3, 3^2, 3^3, 3^4, 3^5 \not\equiv 1 \pmod{15}$.*

Let $m = ord_n(a)$. It is important to note that $a^0, a^1, a^2, \cdots, a^{m-1}$ are all distinct modulo n. Suppose $a^i \equiv a^j \pmod{n}$ for $i, j \in \{0, \cdots, m-1\}$. Suppose $i \geq j$. Then $a^{i-j} \equiv 1 \pmod{n}$. Note that the only term in $a^0, a^1, \cdots, a^{m-1}$ that is congruent to 1 modulo n is 2^0. Since $0 \leq i - j \leq m - 1$, $i - j = 0$. Therefore, $i = j$. Therefore,

$$a^0, a^1, \cdots, a^{m-1} \text{ are all distinct modulo } n \ .$$

Since $a^m \equiv 1 \pmod{n}$, the sequence $a^0, a^1, \cdots \pmod{n}$ is periodic with period m. Think of this sequence as a cycle; See Figure **??**.

No element except for $a^0 = a^m$ is equal to 1. Therefore, no other element in the cycle is equal to 1. How does this help us? If $a^k \equiv 1 \pmod{n}$ for some positive integer k, then k is divisible by $m = ord_n(a)$. Wow, this fact is awesome. Better show how awesome it is by putting it as a theorem.

Theorem 2.5 *Let a, n be positive integers such that $\gcd(a, n) = 1$. Suppose $a^k \equiv 1 \pmod{n}$ for some non-negative integer k. Then $ord_n(a)$ divides k*

But wait, we already know that $a^{\varphi(n)} \equiv 1 \pmod{n}$. Nice! What does this mean?

Corollary 2.6 *Using the notation of Theorem* **??**, $ord_n(a)$ *divides* $\varphi(n)$.

Corollary 2.7 *Let* p *be a prime and* a *a positive integer not divisible by* p. *Then* $ord_p(a)$ *divides* $p-1$.

New to the notion of order? Do the following exercises.

Exercises

1. Let a, n, d be positive integers such that $\gcd(a, n) = 1$. Let $m = ord_n(a)$. Express $ord_n(a^d)$ in terms of m and d. (Hint: Think about the frogs problem from the previous section and the cyclic nature of $a^0, a^1, a^2, \cdots \pmod{n}$.

2. Let a, n be positive integers. Prove that $\varphi(a^n - 1)$ is divisible by n. (Hint: There is a short solution to this problem.)

3. Let p be a prime which is not 2 or 5 and $0 < n < p$ be a positive integer. Let $d = ord_n(p)$. Prove that the decimal representation of $\frac{n}{p}$ is periodic with period d.

4. Find all positive integers n such that $n \mid 2^n - 1$. (Hint: If $n > 1$, consider the smallest prime factor p of n.)

5. Let p be a prime number. Prove that $p^p - 1$ contains a prime factor congruent to 1 modulo q.

6. If $3 \leq d \leq 2^{n+1}$, then $d \nmid (a^{2^n} + 1$ for all positive integers a.

3 Primitive Roots

Let's look back at the beautiful figure in Figure **??**. Wow, what a wonderful piece of art. Well, most of the time it is. But what does the figure look like if $a = 1$. Wow, what a boring figure. A single dot. Let's consider another example. Suppose $a = 2$ and $n = 7$. So we have $1, 2, 2^2, 2^3 \equiv 1 \pmod 7$. So the cycle contains the numbers $1, 2, 4 \pmod 7$. The picture is kind of pretty. It contains three numbers. A cycle of three numbers is nice. But you know what would make a super beautiful picture? If the cycle contains everything modulo 7. Well, except 0. Since $\gcd(a, n) = 1$, 0 can never appear.

But what if we want $\{1, 2, 3, 4, 5, 6\}$ to all appear? Can we? Pick another a. Say, $a = 3$. Let's calculate $1, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$. And of course 3^6 is back at the beginning of the cycle. Yes, we can make the cycle contain everything modulo 7. Sweet!

So you may be thinking that seven is just a lucky number. Surely you cannot do this with all prime numbers. Well, I'm telling you that you can. If you believe me, read on. If you don't believe me, well, keep reading on. I will prove it to you. Let's formalize what we are trying to prove.

For a prime number p, we want to find $g \in \{1, \cdots, p-1\}$ such that

$$\{1, 2, \cdots, p-1\} = \{1, g, g^2, \cdots, g^{p-2}\} \pmod p.$$

Equivalently,

$$ord_p(g) = p - 1.$$

Can you see why these two properties of g are equivalent? (Think about the cycle picture again.) Such an element g is called a *primitive root* modulo p.

Does g always exist? The answer is yes!

Theorem 3.1 *Let p be a prime number. Then there exists $g \in \{1, \cdots p-1\}$ such that g is a primitive root modulo p.*

Proof: Since $a^{p-1} \equiv 1 \pmod p$, $ord_p(a)$ is a divisor of $p-1$ for each $a \in \{1, \cdots, p-1\}$.

For each $d|p-1$, let S_d be the subset of $\{1, \cdots, p-1\}$ with order d. We claim that $|S_d| \leq \varphi(d)$. If $|S_d| = 0$, then clearly our claim holds. Otherwise, let $a \in S_d$. Consider $\{1, a, \cdots, a^{d-1}\}$. Every element in this set are roots of the polynomial $x^d - 1 \pmod p$. Such a polynomial

contains at most d roots. Therefore, $\{1, a, \cdots, a^{d-1}\}$ is the complete set of roots of this polynomial. Furthermore, all elements of order d are in this list, namely a^k, where $k \in \{1, \cdots, d-1\}$ and $\gcd(k, d) = 1$. Hence, $|S_d| = \varphi(d)$.
Therefore,

$$p - 1 = \sum_{d|p-1} \varphi(d) \geq \sum_{d|p-1} |S_d| = p - 1.$$

Hence, equality must hold throughout. Specifically, $|S_{p-1}| = \varphi(p-1) > 0$. $\square$

Wow, this is great. Not only did we prove that primitive roots modulo p exist, but also that there are $\varphi(p-1)$ of them.

So how do we find a primitive root modulo p? There is no clean way to do it. In practice, 2 or 3 usually is a primitive root. For now, we will just call it g. We don't know what g is. But g exists. And that's more than enough to make us happy. After all, we have $\varphi(p-1)$ beautiful cycles.

Example 3.2 *Prove that* 2 *is a primitive root modulo* 101.

Solution: So we calculate $2, 2^2, 2^3, \cdots, 2^{99}$ to see that none of them are $1 \pmod{101}$. Or, we can be clever. It suffices to show that 2^{20} and 2^{50} are not $1 \pmod{101}$. (Why? – I'll let you figure this one out.) Now, you do know the trick to calculate $2^m \pmod{n}$ reasonably quickly? Just calculate $2, 2^2, 2^4, 2^8, \cdots \pmod{101}$. (Each term is just the square of the previous term, so this isn't too cumbersome.) I will leave this as an exercise for you.

Okay. Let's use primitive roots to actually solve an olympiad style problem.

Exercise 3.3 *Let $p \geq 5$ be a prime and $1 \leq n < p-1$ a positive integer. Prove that*

$$1^n + 2^n + \cdots + (p-1)^n$$

is divisible by p.

Solution: So we take the general formula for $1^n + 2^n + \cdots + (p-1)^n$ and .... wait, what is that formula again? Oh right. It's ugly and complicated. We need something else. We're trying to prove that $1^n + 2^n + \cdots + (p-1)^n \equiv 0 \pmod{p}$. If only we have an alternate way of representing $\{1, 2, \cdots, p-1\} \pmod{p}$. If only.

Oh wait we do! Let g be a primitive root modulo p. Then $\{1, 2, \cdots, p-1\} = \{1, g, \cdots, g^{p-2}\}$. Then

$$(1^n + 2^n + \cdots + (p-1)^n) \equiv (1 + g^n + g^{2n} + \cdots + g^{(p-2)n} \pmod{p}.$$

Oh nice. A geometric sequence. We know how to sum this. Life is good again.

$$(1 + g^n + g^{2n} + \cdots + g^{(p-2)n} = \frac{1 - g^{(p-1)n}}{1 - g^n}.$$

By Fermat's Little Theorem, the numerator of this expression is divisible by p. Since $n < p-1$ and g is a primitive root, the numerator is not divisible by p. Hence, we are not dividing by zero. This solves the exercise. $\square$

Exercises:

1. Let p be an odd prime and g a primitive root modulo p. Prove that

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

2. Let p be a prime such that $p \equiv 3 \pmod{4}$. Prove that

$$\prod_{j=1}^{p-1}(j^2 + 1) \equiv 4 \pmod{p}.$$

3. (Putnam 1994) For each non-negative integer m, let $n_m = 101m - 100 \cdot 2^m$. Let a, b, c, d be integers such that $0 \leq a, b, c, d \leq 99$ such that $n_a + n_b \equiv n_c + n_d \pmod{10100}$. Prove that $\{a, b\} = \{c, d\}$.

4. (IMO 1984 Variant) Find all pairs of positive integers (a, b) such that $ab(a + b)$ is not divisible by 7, but $(a + b)^7 - a^7 - b^7$ is divisible by 7^7.