MATH 4440
MISSION 4

AARON ALLEN, DANIEL KUMINKA,
MELANIE NUN, BHARADWAJ THIRUMAL

1. Euler's Phi Function

Definition 1.1 (Euler's Phi Function)**.** For $n \in \mathbb{Z}_{\geq 1}$, **Euler's totient function**, or $\phi(n)$ is the count of all invertible $x \in \mathbb{Z}/n\mathbb{Z}$.

Example 1.2. Here are some examples of Euler's totient function:

i. A simple example is $\mathbb{Z}/4\mathbb{Z}$.

$$1(1) \equiv 1 \bmod(4) \Rightarrow 1^{-1} = 1.$$

$$3(3) \equiv 1 \bmod(4) \Rightarrow 3^{-1} = 3.$$

There does not exist $2^{-1} \in \mathbb{Z}/4\mathbb{Z}$.

$$2(1) \equiv 2 \bmod(4), 2(2) \equiv 0 \bmod(4), 2(3) \equiv 2 \bmod(4), \text{ and } 2(0) \equiv 0 \bmod(4).$$

Likewise, 0 does not have an inverse. Therefore $\phi(4) = 2$.

ii. The integers with inverses modulo 26 are given in the table.

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

Because there are 12 elements in the table, $\phi(26) = 12$.

iii. Every element in $\mathbb{Z}/5\mathbb{Z}$ except 0 has an inverse.

$$1^{-1} = 1 \bmod(5)$$

$$2^{-1} = 3 \bmod(5)$$

$$3^{-1} = 2 \bmod(5)$$

$$4^{-1} = 4 \bmod(5)$$

We conclude $\phi(5) = 4$.

Proposition 1.3. *If p is a prime, then $\phi(p) = p - 1$.*

This proposition requires lemmata.

Lemma 1.4. *Let n and x be coprime integers. Then n is invertible modulo x.*

Proof. Bézout's Identity states that for $a, b \in \mathbb{Z}$ there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b).$$

So let n, x be coprime. We want to show that there is some $z \in \mathbb{Z}$ such that $xz = 1 \mod n$. Recall that there exist some $y, z \in \mathbb{Z}$ such that $xz + ny = 1$. So, $xz = 1 - ny$. So, $xz = 1 \mod n$. □

Lemma 1.5. *Suppose n and x are integers such that n is invertible modulo x. Then n and x are coprime.*

Proof. Let $n, x \in \mathbb{Z}$ such that there exists some $xx^{-1} = 1 \mod n$. Therefore $xx^{-1} = 1 + ny$ for some $y \in \mathbb{Z}$, and $xx^{-1} - ny = 1$. Bézout's identity tells us that $\gcd(n, x) = 1$, so n, x must be coprime. □

These two lemmata combine to give the following statement:

Lemma 1.6. *Let x and n be integers. Then x is invertible modulo n if and only if n and x are coprime.*

Proof of Proposition 1.3. Let there be a set $X = \{x \in \mathbb{Z} : 1 \leq x < p\}$ where p is some prime. Every $x \in X$ is coprime to p. So for each x there exists some x^{-1} such that $xx^{-1} = 1 \mod p$. Therefore

$$\phi(p) = |X| = p - 1$$

. ☐

Proposition 1.7. *Let $n = p^k$, where p is a prime, $k \geq 1$. Then $\phi(n) = p^k - p^{k-1}$.*

Proof. Note: The numbers that are not coprime to and less or equal to (i.e. found in $\mathbb{Z}/p\mathbb{Z}$) p^k can be written as $p\ell$ for some $\ell \in \mathbb{Z}$ where $1 \leq \ell \leq p^{k-1}$. There are exactly $p^k - 1$ such numbers. So

$$\phi(p^k) = p^k - p^{k-1}$$

☐

Proposition 1.8. *Let n and m be coprime. Then $\phi(nm) = \phi(n)\phi(m)$.*

This one needs a lemma again.

Lemma 1.9. *Let n and m be coprime. Then x is invertible modulo nm if and only if it is invertible modulo n and modulo m.*

Proof. First, recall that a is a unit modulo n if and only if $\gcd(a, n) = 1$. So if a is a unit modulo mn, it does not share any divisors with m and n and hence is a unit modulo m and n. Conversely, suppose a is not invertible modulo mn. This means there is a common divisor, which we may take to be prime. Thus p divides a and p divides mn. But this means p divides m or p divides n as p is prime, hence a shares a common divisor with m or n. This means a is not invertible modulo m or n.

An alternative way to prove this fact: Assume that $gcd(a, nm) = 1$. This means that there exist integers u, v so that

$$au + mnv = 1.$$

Any common divisor d of a and m divides both terms on the left-hand side of this equation, and so d divides 1. Similarly any common divisor of a and n divides 1, and we conclude that $gcd(a, m) = 1 = gcd(a, n) = 1$. Conversely, if $gcd(a, m) = 1$ and $gcd(a, n) = 1$ then there are integers u, v, x, y so that $au + mv = 1$ and $ax + ny = 1$. Multiplying these equations together, we find

$$1 = (ax + ny)(au + mv) = axau + axmv + nyau + nymv = a(xau + xmv + nyu) + (mn)(yv)$$

and we conclude that $gcd(a, mn) = 1$. ☐

Proof of Proposition 1.8. Given $c \in \{1, 2, ...mn\}$, we can find a unique $a \in \{1, 2, ...n\}$ and $b \in \{1, 2, ...m\}$ such that

$$c \equiv a(\mod n) \text{ and } c \equiv b(\mod m)$$

Conversely, given $a \in \{1, 2, ...n\}$ and $b \in \{1, 2, ...m\}$, there exists a unique $c \in \{1, 2, ...mn\}$ such that the above equations exists by Chinese Reminder Theorem. We have

$$\gcd(c, mn) = \gcd(c, m) \gcd(c, n) = \gcd(a, n) \gcd(b, m)$$

So $\gcd(c, mn) = 1$ iff $\gcd(a, n) = \gcd(b, m) = 1$. There are $\phi(n)$ choices for a such that $\gcd(a, n) = 1$. There are $\phi(m)$ choices for b such that $\gcd(a, m) = 1$. Therefore, there are $\phi(n)\phi(m)$ choices for a and b such that $\gcd(a, n) = \gcd(b, m) = 1$. So there are $\phi(m)\phi(n)$ choices for c such that $\gcd(c, nm) = 1$. This shows that $\phi(mn) = \phi(m)\phi(n)$. ☐

Example 1.10. Demonstrate how to compute $\phi(3 \cdot 7^2 \cdot 11^3)$ using the three propositions of this section. Cite each proposition as you use it.

Suppose we have $(3 \cdot 7^2 \cdot 11^3) = (a \cdot b^2 \cdot c^3)$. We know that a, b, and c are all prime and not equal. This means that if $b^2 = y$ and $c^3 = z$, then $\gcd(a, y, z) = 1$. This means that according to proposition 1.8,

$$\phi(ab^2c^3) = \phi(a)\phi(yz) = \phi(a)\phi(y)\phi(z).$$

Also, since b, and c are prime, proposition 1.7 states that

$$\phi(y) = b^2 - b^1 \text{ and } \phi(z) = c^3 + c^2.$$

Also, since a is prime, proposition 1.3 states that $\phi(a) = a-1$. Combining these equations produces

$$\phi(a \cdot b^2 \cdot c^3) = (a-1) \cdot (b^2 - b) \cdot (c^3 - c^2).$$

Using the real numbers provided produces $(3-1) \cdot (49-7) \cdot (1331-121) = 101640$.

2. Euler's Theorem

Theorem 2.1 (Euler's Theorem)**.** *For **Euler's totient function** $\phi(n)$ as defined above, $a^{\phi n} \equiv 1$ for all a such that* $\gcd(a, n) = 1$.

Before proving this, we will provide an example.

Example 2.2. Let us compute $2^{275} \mod (299)$. Because $299 = 23 \cdot 13$ where 23 and 13 are prime, $\phi(299) = (23-1)(13-1) = 264$. Therefore,

$$2^{365} \equiv 2^{264}(2^{11}) \equiv 1^{264}(2^{11}) \equiv 2048 \equiv 254 \mod (299).$$

We need a lemma, which was proved in class.

Lemma 2.3. *Let a be invertible modulo n. Then the function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $f(x) = ax$ is bijective.*

Proof of Theorem 2.1. Let S be a set, defined as:

$$S = \{x \in \mathbb{Z} | 1 \leq x < p, \gcd(n, x) = 1\}$$

Take $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $f(x) = ax$ as in Lemma 2.3. f is a bijection, which implies that every element $f(x)$ is an element of S.Then $\{a(x_1), a(x_2), ...\} = S$. Therefore,

$$\prod_{x \in S} x \equiv \prod_{x \in S} a(x) \bmod (n),$$

$$\prod_{x \in S} a(x) \equiv a^{|S|} \prod_{x \in S} x \bmod (n)$$

But,

$$|S| = \phi(n) \Rightarrow a^{|S|} \prod_{x \in S} x \equiv a^{\phi(n)} \prod_{x \in S} x.$$

So, dividing $\prod_{x \in S} x \equiv a^{\phi(n)} \prod_{x \in S} x$ gives $1 \equiv a^{\phi(n)}$, as desired. $\square$