**Some Number Theory Results**
**In-class activity, Week 8**

In this activity, we will consider three different topics: Euler $\phi$-function, properties of the order of elements, and the Wilson's Theorem.

## Euler $\phi$-Function

We know that $\phi(p) = p - 1$ for a prime $p$ by definition of the Euler $\phi$-function, and $\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$ for two different primes $p, q$, and $\phi(p^2) = p^2 - p$ from the pre-class activity. We will use some properties of the Euler $\phi$-function to come up with a formula that gives $\phi(n)$ for any $n$.
First, note that we can write the result $\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$ as $\phi(p \cdot q) = \phi(p)\phi(q)$. This property, more generally, is called the *multiplicative property.* We now prove this more general result.

**Theorem 1:** The Euler $\phi$ function is multiplicative, i.e. for $n_1, n_2$ with $\gcd(n_1, n_2) = 1$, we have $\phi(n_1 n_2) = \phi(n_1)\phi(n_2)$.

**proof:** We know that $\phi(n_1 n_2)$ counts the numbers from 1 to $n_1 n_2$ which are relatively prime to $n_1 n_2$. So we can think of $\phi(n_1)\phi(n_2)$ counting the pairs of numbers where the first number is from 1 to $n_1$ and is relatively prime to $n_1$, and where then second is from 1 to $n_2$ and is relatively prime to $n_2$. To show that $\phi(n_1 n_2)$ is equal to $\phi(n_1)\phi(n_2)$ we will show that these two collections (the first being the collection of numbers from 1 to $n_1 n_2$ relatively prime to $n_1 n_2$ and the second being the pairs of numbers) have the same number of elements. To do so, we will establish a one-to-one pairing between the elements in these two collections.

Consider $m$ with $1 \leq m < n_1 n_2$ and $\gcd(m, n_1 n_2) = 1$. Neither $n_1$ and $n_2$ can divide $m$, so there are remainders $1 \leq r_1 < n_1$ and $1 \leq r_2 < n_2$. This shows that for every $m$ there corresponds a pair of numbers where the first number is from 1 to $n_1$ and is relatively prime to $n_1$, and where then second is from 1 to $n_2$ and is relatively prime to $n_2$. We should also show that for every pair of numbers there is an $m$ which corresponds to this pair. Suppose $(r_1, r_2)$ is a pair where the first number is from 1 to $n_1$ and is relatively prime to $n_1$, and where then second is from 1 to $n_2$ and is relatively prime to $n_2$. Then consider a solution $x$ for the congruence equations

$$\begin{aligned} x &\equiv r_1 \pmod{n_1} \\ x &\equiv r_2 \pmod{n_2} \end{aligned}$$

A solution exists by the Chinese Remainder Theorem. If needed find $m \equiv x \pmod{n_1 n_2}$ such that $0 \leq m < n_1 n_2$. Note that $\gcd(m, n_1 n_2)$ has to be 1 since $\gcd(m, n_1) = \gcd(m, n_2) = 1$.
Now to finish the proof, we will show that the pairing is one-to-one, meaning that there is a unique $m$ corresponding to a pair. This follows from the Chinese Remainder Theorem since $\gcd(n_1, n_2) = 1$. This implies that any two solutions are congruent modulo $n_1 n_2$, both since $1 \leq m < n_1 n_2$, this implies a unique solution. $\square$

From Theorem 1 and the Fundamental Theorem of Arithmetic, in order to calculate $\phi(n)$ for some $n$, it is enough to know how to calculate $\phi(p^k)$ where $p$ is prime and $k$ is a positive integer.

**Proposition 1:** For any prime $p$ and positive integer $k$,

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right) = p^{k-1}(p-1)\,.$$

**proof:** Among integers from 1 to $p^k$, those which are not relatively prime to $p^k$ are powers of p, and there are $p^{k-1}$ such integers. Hence $\phi(p^k) = p^k - p^{k-1}$. $\square$

**Theorem 2:** If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime decomposition of $n$, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

**proof:** Using the multiplicative property, $\phi(n) =$ $\phi(p_1^{k_1})\phi(p_2^{k_2})\cdots\phi(p_r^{k_r})$. Using the above proposition, $\phi(p_i^{k_i}) =$ $p_i^{k_i-1}(p_i-1)$. Therefore,

$$\phi(n) = p_1^{k_1-1}(p_1-1)\,p_2^{k_2-1}(p_2-1)\cdots p_r^{k_r-1}(p_r-1).$$

Factoring out all $p_i^{k_i}$'s and noting that $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, we find that

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

hence proving the theorem. □

**1.** Use Theorem 2 to find $\phi(1552500)$.

$1552500 = 2^2 \cdot 3^3 \cdot 5^4 \cdot 23$

$\phi(1552500) = 1552500\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{23}\right) = 396000$

?? **2.** Determine for which $n$, $\phi(n)$ has exactly three 0's at the end.

$1000 \mid \phi(n)$ but $10000 \nmid \phi(n)$. $\phi(n) = p_1^{k_1-1}(p_1-1)\,p_2^{k_2-1}(p_2-1)\cdots p_r^{k_r-1}(p_r-1)$

$n = 2^2 \cdot 5^4 \cdot m$

$= 2500m$

but also other conditions

$= 2^3 \cdot 5^3 \cdot K$ $\quad 10 \nmid K$

$= 2 \cdot 1 \cdot 5^3 \cdot 4 \cdot K$

$2 \mid p_i - 1$ so $5 \nmid p_i - 1$ for any $i$

$5 \nmid K$

## The Properties of the Order of Elements Modulo $n$

When finding the order of an element $a \pmod{n}$, it seems like we need to check all the powers $a^k$ to see when it is equal to 1. But, by Fermat's Little Theorem, which says that $a^{p-1} \equiv 1 \pmod{p}$ for prime $p$, and Euler-Fermat Theorem, which says that $a^{\phi(n)} \equiv 1 \pmod{n}$ for a general $n$, we know that we do not need to try too many numbers for $k$ when determining the order of an element. We will see shortly that the order is even easier to find than checking all the powers $k$ up to $\phi(n)$.

**Theorem 3:** Suppose $\gcd(a, n) = 1$ and order of $a$ modulo $n$ is $d$. Then

$$a^i \equiv a^j \pmod{n}$$

if and only if $d$ divides $i - j$.

**proof:** Using the division algorithm $i - j = dq + r$ with $0 \le r < d$. Note that $a^i = a^j a^{i-j} = a^j \cdot a^r \cdot (a^d)^q$. Using the fact that $a^d \equiv 1 \pmod{n}$, we find that

$$a^i \equiv a^j a^r \pmod{n}.$$

Since $\gcd(a^i, n) = 1$ and $a^i \equiv a^j \pmod{n}$, we can cancel $a^i$ from both sides of the congruence above to get the equivalent congruence

$$1 \equiv a^r \pmod{n}.$$

But $d$ is the order of $a$ and $r < d$. Therefore $r = 0$ for otherwise we will have a contradiction. Since each step in the proof is reversible, we have proven the 'if and only if'. □

**Corollary 1:** If $p$ is prime and $d$ is the order of $a$ modulo $p$, then $d$ divides $p-1$.

**proof:** This follows from Theorem 3 because $a^{p-1} \equiv a^0 \pmod{p}$ due to Fermat's Little Theorem. $\square$

**Corollary 2:** If $d$ is the order of $a$ modulo $n$, then $d$ divides $\phi(n)$.

**Corollary 3:** If $d$ is the order of $a$ modulo $n$ and $a^m \equiv 1 \pmod{n}$, then $d|m$.

These last three corollaries make calculation of the order of an element easier because we only need to check divisors of $\phi(n)$ to find the order of an element modulo $n$. We can be strategic in checking the divisors to minimize the work in general as well. (How?) Slowly break down the powers of the order's factors

**3.** Find the order of the following elements modulo the given $n$. Explain your work.

**a.** 3 modulo 46 $46=2\cdot 23$, $\phi(46)=46(1-\frac{1}{2})(1-\frac{1}{23})=22=2\cdot 11$

$3^2 \not\equiv 1$, $3^{11} \equiv 1 \pmod{46}$ So order is 11

**b.** 5 modulo 357 $357=3\cdot 7\cdot 17$, $\phi(357)=357(1-\frac{1}{3})(1-\frac{1}{7})(1-\frac{1}{17})=192=2^6\cdot 3$

$5^{96} \equiv 1$, $5^{64} \not\equiv 1$, $5^{48} \equiv 1$, $5^{24} \not\equiv 1$

so we need the 3

order is 48

Note that if $a$ is an element of order $d$ modulo $n$, then $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{n}$ for any integer $k$. Therefore, the order of $a^k$ is a factor of $d$ by Corollary 3. We now make this connection more explicit.

**Proposition 2:** Suppose $\gcd(a,n)=1$ and $d$ the order of $a$ modulo $n$. Then the order of $a^k$ modulo $n$ is $\dfrac{d}{\gcd(d,k)}$.

**proof:** Let $r$ be the order of $a^k$. By definition, $r$ is the smallest power of $a^k$ so that $(a^k)^r \equiv 1 \pmod{n}$. Note that

$$\begin{aligned}(a^k)^{\frac{d}{\gcd(d,k)}} &\equiv (a^d)^{\frac{k}{\gcd(d,k)}} \pmod{n}\\ &\equiv 1 \pmod{n}\end{aligned}$$

because $\dfrac{k}{\gcd(d,k)}$ is an integer and $a^d \equiv 1 \pmod{n}$. Hence, by Corollary 3, the order $r$ of $a^k$ divides $\dfrac{d}{\gcd(d,k)}$.

Also note that if $a^{kr} \equiv (a^k)^r \equiv 1 \pmod{n}$, then by Corollary 3, $d$ divides $kr$. Therefore, $\dfrac{d}{\gcd(d,k)}$ divides $r$. This finishes the proof. $\square$

**4.** Suppose the order of 5 modulo 94 is 46. Find the orders of: $5^2, 5^{23}, 5^3, 5^5$.

23, 2, 46, 46

$5^{46} \equiv 1$

**Wilson's Theorem**

As you discovered in the pre-class, $(n-1)! \equiv 0 \pmod{n}$ for a composite $n > 4$ value. To prove this, note that here are $1 < a, b < n$ for which $a \cdot b = n$. If $a \neq b$, then $n|(n-1)!$ since $ab|(n-1)!$. If $a = b$, then $a > 2$ and $n = a^2 > 2a$. This means that both $a, 2a$ appear in $(n-1)!$ and hence $n|(n-1)!$. It turns out that when $n$ is prime, $(n-1)!$ not only does not equal 0 modulo $n$, but it equals a special number.

**Theorem 4:** (Wilson's Theorem) If $p$ is prime, then

$$(p-1)! \equiv -1 \pmod{p}.$$

**proof:** We need to find what the product of all the numbers $1, 2, \ldots, (p-2), (p-1)$ are modulo $p$. We will consider the numbers $2, 3, \ldots, (p-2)$ separately from 1 and $-1$.

If $x$ is one of $2, 3, \ldots, (p-2)$, then there is a unique $y$ among $2, 3, \ldots, (p-2)$ such that $xy \equiv 1 \pmod{p}$ because all nonzero $x \in \mathbb{Z}_p$ are invertible. Furthermore, for each such $x$, $y$ pair, $y \neq x$ because $n^2 \not\equiv 1 \ \% \ p$ for any $n \not\equiv 1, -1 \ \% \ p$.
Therefore, each $x$ among $2, 3, \ldots, (p-2)$ can be paired with a $y$ so that their product is 1.

When we consider $(p-1)!$ modulo $n$, most of the numbers can be paired to give 1. The only numbers which are not paired will be $1, -1$, so the whole product will be congruent to $-1$ modulo $p$, finishing the proof.

□

**5 a.** Now suppose $p = 41$. According to Theorem 1, $(p-1)! \equiv -1 \pmod{41}$. Note that $(p-1)! = 1 \cdot 2 \cdot 3 \cdots 39 \cdot 40$ and that $40 \equiv -1 \pmod{41}$, $39 \equiv -2 \pmod{41}$. Using similar congruences and simplifying, rewrite $(p-1)!$ as a square and hence finding a solution to $x^2 \equiv -1 \pmod{41}$.

$-1 \equiv 40! \equiv (20!)^2 \cdot (-1)^{20} \equiv (20!)^2 \pmod{41}$

$20! \equiv 9 \pmod{41}$

$9^2 \equiv -1 \pmod{41}$

**b.** For which primes would your work for part **a** generalize to give a similar result?

all primes $p$ where $4 | p-1$ or $p = 2$

The others yield $x^2 \equiv 1$

**Theorem 5:** Let $p$ be a prime. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p = 4k + 1$ for some $k$.

**proof:** Suppose $p = 2$ or $p = 4k + 1$, and we will show that there is a solution for $x^2 \equiv -1 \pmod{p}$. If $p = 2$, $x = 1$ is a solution. If $p = 4k + 1$, then $x = 1 \cdot 2 \cdots \frac{p-1}{2}$ is a solution from your previous work.

In order to prove the other direction, we will prove the contrapositive, that if $p = 4k + 3$, then there is no solution for $x^2 \equiv -1 \pmod{p}$. To prove the contrapositive, we will use contradiction. Suppose $p = 4k + 3$ and suppose there is a solution for $x^2 \equiv -1 \pmod{p}$. Consider $x^{p-1} = (x^2)^{2k+1}$. Since $x^2 \equiv -1 \pmod{p}$ and $2k + 1$ is odd, $x^{p-1} \equiv -1 \pmod{p}$. But this contradicts Fermat's Little Theorem. $\square$

We will revisit solving $x^2 \equiv -1 \pmod{n}$ in the activity on Quadratic Residues.

Recall that we have seen that there are infinitely many primes of the form $4k + 3$ earlier. We now prove the counterpart to this result using Theorem 5.

**Corollary 4:** There exists infinitely many primes of the form $4k + 1$.

**proof:** Suppose there are only finitely many such primes and let $N$ be their product. Consider now $M = 4N^2 + 1$. $M$ cannot be prime and any prime factor $p$ of $M$ has to be of the form $4k + 3$. But $(2N)^2 \equiv$ $\underline{-1}$ $\pmod{p}$. This means that $x = 2N$ is a solution for $\underline{x^2 \equiv -1 \pmod{p}}$, which is contradiction because $\underline{p \equiv 3 \pmod{4}, \text{ not } 1}$. $\square$