Number Theory: Introduction to Euler's Totient Function

Cathal Stephens and Roonak Thapa

May 21 2023

1 Introduction

Number theory is the study of relationships and properties of numbers. We learned about and worked with prime numbers and congruence relations in our study of number theory. This paper focuses on topics from Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery's *An Introduction to The Theory of Numbers*. In particular, the totient function.

Swiss mathematician Leonhard Euler contributed much to the study of prime numbers. Euler's contributions to number theory are still studied and used today, making him one of the most influential mathematicians in history. One of these contributions was Euler's φ-function, also known as the totient function.

In reading *An Introduction to The Theory of Numbers*, one is exposed to the number theory in stages. As we worked through the text, we found the section on congruences and moduli particularly fascinating. The totient function beautifully integrates previous topics, such as primes and divisibility, while forming an entirely new and powerful theorem developing our understanding of reduced residue systems and moduli.

In Section 2 we give contextual definitions and examples of mathematical concepts such as modulo and reduced residue classes, which are crucial to the understanding of the totient function. We then define the totient function. We derive formulas for evaluating $\varphi(n)$ in Section 3. Finally, we consider the surjectivity of the totient function in Section 4. We ask: Over what codomain is φ surjective? Can we give n distinct numbers $x_1, x_2, ...x_n$ such that $\varphi(x_1) = \varphi(x_2)... = \varphi(x_n)$?

2 Background

Before going into the uses and applications of Euler's totient function, we should discuss the preliminary concepts required to understand our ideas and proofs, and to solidify our understanding further, we will go over some examples. We will start with integers as our other ideas show the relationship of integers, developing our understanding of totient function, reduced residue systems, and moduli.

Definition 2.1. An integer b is *divisible* by an integer a when $\frac{b}{a}$ leaves no remainder, this is denoted by $a|b$. We say that a is a *divisor* of b.

Example 2.1. *Consider $20 \div 5 = 4$ which is an integer. This tells us that $5|20$. As opposed to $21 \div 5 = 4.2$ which is not an integer. This tells us that $5 \nmid 21$.*

With this understanding of integers, we should discuss the primary form of comparison used in number theory, divisors, greatest common divisor, and coprimes.

Definition 2.2. A *common divisor* is a divisor that is shared by two or more integers. The *greatest common divisor* (GCD) is the largest divisor that is shared. The greatest common divisor of integers a and b is denoted by $(a, b) = g$.

A set of numbers are *coprime* when their greatest common divisor is 1, while a set of numbers are not coprime when their greatest common divisor is greater than 1.

Example 2.2. *Consider the greatest common divisor of 35 and 21. If we expand both values we get $7 \cdot 5$ and $7 \cdot 3$. Because both integers are multiples of 7, and 7 is the greatest divisor they share, the greatest common divisor of 35 and 21 is 7, denoted by $(35, 21) = 7$.*

Definition 2.3. A function $f : X \to Y$ is *surjective* if for every element y in Y, there exists an element x in X such that $f(x) = y$.

Example 2.3. *Consider the functions $f(x) = x^2$ and $g(x) = x^3$ both over the domain $[-1, 1]$ and the codomain $[-1, 1]$. We see that $f(x)$ is a not a surjective function as $f(x) = x^2$ is never negative. We see that $g(x)$ is a surjective function because for every y in the codomain $[-1, 1]$, there exists x in the domain $[-1, 1]$ such that $g(x) = y$.*

Definition 2.4. *Prime numbers* are positive integers that have no divisor other than itself and 1. *Composite numbers* are positive integers that are not prime.

Example 2.4. *Some example of prime numbers: 2, 3, 5, 7, 11, and 13.Some examples of composite numbers are 4, 6, 8, 10, 12, and 14.*

Definition 2.5. We say that an integer a is *congruent* to an integer b *modulo* m if $a - b$ is divisible by m. This is denoted by $a \equiv b \pmod{m}$, where we call m the *modulus.*

Example 2.5. *Consider the fact that $3|23 - 8$, this gives us the congruence relation $23 \equiv 8 \pmod 3$.*

Definition 2.6. A *reduced residue class* mod m is a set of numbers that are all co prime to the modulus m such that all values in the set are not congrue nt to each other mod m.

Example 2.6. *Let's consider a reduced residue class mod 7. One example of a reduced residue class mod 7 is* $\{1, 2, 3, 4, 5, 6\}$*. Another example is* $\{22, 9, 10, 39, 33, 13\}$ *as all integers will have a unique remainder when dividing by 7.*

Definition 2.7. A function $f : X \to Y$ is *surjective* if for every element y in Y, there exists an element x in X such that $f(x) = y$.

Example 2.7. *Consider the functions* $f(x) = x^2$ *and* $g(x) = x^3$ *both over the domain* $[-1, 1]$ *and the codomain* $[-1, 1]$*. We see that* $f(x)$ *is a not a surjective function as* $f(x) = x^2$ *is never negative. We see that* $g(x)$ *is a surjective function because for every* y *in the codomain* $[-1, 1]$*, there exists* x *in the domain* $[-1, 1]$ *such that* $g(x) = y$*.*

Theorem 2.8. *Unique Prime Factorization* Unique prime factorization *is the idea that any integer greater than 0 can be expressed by unique product of prime numbers.*

The uniqueness mentioned comes from the orientation of the prime numbers as multiplication is commutative, allowing someone to alter the orders of numbers in an expression.

Definition 2.8. The *Totient functions* or the φ-function is the number of positive integers less than n which are coprime to n.

Example 2.9. *Let us evaluate* $\varphi(6)$*. First we list all positive integers less than 6:* $\{1, 2, 3, 4, 5\}$*, remove* $\{2, 3, 4\}$ *because they share a divisor with 6 and count up the remaining integers being 1 and 5, allowing us to find that* $\varphi(6) = 2$*.*

3 Patterns of the Totient Function

The φ-function is the number of positive integers less than n which are coprime to n. This value can be computed methodically using a formula which is on certain properties of the value n.

Proposition 3.1. *For a prime number* p*,* $\varphi(p) = p - 1$*.*

Proof. Since p is prime, all positive integers less than p are coprime to p. So any reduced residue class $\pmod{p}$ has size $p - 1$. Therefore, $\varphi(p) = p - 1$. □

Proposition 3.2. *For* p *and* q *that are two distinct primes,* $\varphi(pq) = \varphi(p)\varphi(q)$*.*

Proof. Since all numbers between each multiple of p are coprime to p, and there are q multiples of p in (qp) we subtract q from qp. The same is done for all multipled of q by subtracting p, finally we add 1 to account for both primes:

$$\begin{aligned} &= pq - q - p + 1 \\ &= q(p - 1) - 1(p - 1) \\ \varphi(pq) &= (p - 1)(q - 1) \\ \varphi(pq) &= \varphi(p)\varphi(q) \end{aligned}$$

□

Corollary 3.1. *For $(m,n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$. This means the φ-function is a multiplicative function.*

Corollary 3.1 follows from Proposition 3.2 by generalizing the proof.

Proposition 3.3. *For p a prime, $\varphi(p^r) = p^r - p^{r-1}$.*

Proof. Since p is prime,

$$\varphi(p^r) = \#\{1, 2, 3, \dots, p^r\} - \#\{p, 2p, \dots, p^r\}$$

In other words $\varphi(p)$ is the number of positive integers less than or equal to p^r minus the number of multiples of p less than or equal to p^r, which is equal to p^{r-1}. This can be rewritten as:

$$\varphi(p^r) = p^r - p^{r-1}$$

□

Proposition 3.4. *For $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where p_i are prime factors of n, $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$.*

Proof. Note, by Theorem **??** all positive integers can be written uniquely by the prime factorization of that integer.

By Corollary 3.1, $\varphi(n)$ can be written as

$$\varphi(p_1^{e_1} p_2 e_2 \cdots p_r^{e_r}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_r^{e_r}).$$

Since all p_i are prime by Proposition 3.3, we can rewrite all factors as:

$$\begin{aligned}
\varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_r^{e_r}) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1})\cdots(p_r^{e_r} - p_r^{e_r-1}) \\
&= (p_1^{e_1-1}(p_1 - 1))(p_2^{e_2-1}(p_2 - 1))\cdots(p_r^{e_r-1}(p_r - 1)) \\
&= p_1^{e_1}\left(1 - \frac{1}{p_1}\right)p_2^{e_2}\left(1 - \frac{1}{p_2}\right)\cdots p_r^{e_r}\left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)
\end{aligned}$$

□

4 The Surjectivity of the Totient Function

As we continued our study of Euler's Totient function, we wondered "over what co-domain is φ surjective?" as well as if we can "give n distinct numbers $x_1, x_2, ...x_n$ such that ...?"

Proposition 4.1. *For integers $x \geq 3$, $\varphi(x)$ is never odd. $\varphi(x)$ is only odd when $x = 2$.*

Proof. Let us consider the case where n is an odd prime. Since n is prime, all positive integers less than n are relatively prime to n, except for the multiples of n. The number of multiples of n less than or equal to n is precisely 1, namely n itself. Therefore $\varphi(n)$ is equal to $n-1$, and $\varphi(n)$ is even when $n>2$ but is odd when $n=2$.

Now consider n as composite number greater than 2. If n is composite and greater than 2, then n can be written as the product of two or more primes: $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, where $\{p_1,p_2,\ldots,p_k\}$ are distinct primes and $\{a_1,a_2,\ldots,a_k\}$ are positive integers. We can use the formula for Euler's totient function to calculate $\varphi(n)$:

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

We can use the formula for Euler's totient function to calculate $\varphi(n)$: n is composite and greater than 2. If n is composite and greater than 2, then it can be written as the product of two or more primes: $n=p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_k^{a_k}$, where $p_1,p_2,\ldots,p_k$ are distinct primes and $a_1,a_2,\ldots,a_k$ are positive integers. □

Proposition 4.2. *The codomain of the totient function does not contain every even number.*

Proof. To determine this, we computationally check every value $\varphi(x)$ for x in the interval $[15,450]$, we found no value of x such that $\varphi(x)=14$. We chose to search for 14 because when we checked the $\varphi(x)$ in the intervals $[2,100]$, we noticed that 14 wasn't an result.
How we found 15 to be the lower bound of x as $\varphi(x)$ produces a number less than x meaning in order for $\varphi(x)=14$ to possibly be true, $x>14$, the smallest integer greater than 14 is 15.
consider the following lemma:

Lemma 1. *There exists a lower bound for $\varphi(x)$ where no value can $\varphi(x)\geq\sqrt{\frac{x}{2}}$*

With this lemma and the lower bound in mind, we determined the upper bound calculated. We can set $\sqrt{\frac{x}{2}}=15$ and determined that $x=450$.

In terms of how we computationally checked every value of $\varphi(x)$, we created a program to do so.

The program calculates the Euler's totient function (phi function) for numbers ranging from 15 to 450. The program starts in the Main class and the main method.

Inside the main method, a loop determines the value of x in $\varphi(x)$. x is in the interval is between the upper and lower bound set. For each number x, the *calculatePhi* method is called.

calculatePhi first contains a loop to find all values less than x, i. The way i is found is similar to x but i is between the interval $[2,x-1]$. After i is determined, the *areRelativelyPrime* method is called.

The *areRelativelyPrime* function determines whether two given numbers, x and i, are relatively prime. It calculates their greatest common divisor (GCD)

```
class Main
  function main(args: String[]): void
    for $x = 15$ to 450 do
      $phi =$ calculatePhi($x$)
      print(”phi(” +$x$+ ”) = ” +$phi$)
    end for
  end function

  function calculatePhi(number: integer): integer
    count = 0
    for $i = 1$ to $number - 1$ do
      if areRelativelyPrime($i$, $number$) then
        count = count + 1
      end if
    end for
    return count
  end function

  function areRelativelyPrime(a: integer, b: integer): boolean
    gcd = calculateGCD(a, b)
    return gcd == 1
  end function

  function calculateGCD(a: integer, b: integer): integer
    while $b \neq 0$ do
      temp = b
      b = a % b
      a = temp
    end while
    return a
  end function

end class
```

using the Euclidean algorithm implemented in the *calculateGCD function.* The GCD is obtained by repeatedly dividing the more significant number by the smaller number and updating the values until the remainder becomes zero. If the resulting GCD is equal to 1, it signifies that x and i have no common factors other than 1, indicating their relative primality. In such cases, the function returns true. However, if the GCD is greater than 1, it implies the presence of at least one common factor other than 1, indicating that a and b are not relatively prime. In this scenario, the function returns false. Thus, the *areRelativelyPrime* function employs the GCD calculation to assess the relative prim ality of x and i. □

Proposition 4.3. *$\varphi(x_1) = \varphi(x_2)... = \varphi(x_n)$?*

Proof. Consider $\varphi(x_1) = \varphi(x_2)$. By Proposition 3.3 this can be written as:

$$p_1^{e_1-1}(p_1-1)\cdots p_r^{e_r-1}(p_r-1) = q_1^{x_1-1}(q_1-1)\cdots q_k^{x_k-1}(q_k-1)$$

Case 1: Since φ is multiplicative, we can remove some p_i and raise some other p_k to a new power $p_k^{e_k}$. Thus maintaining $\varphi(p_i)$ value, yet forming a new input value x so that $\varphi(x_1) = \varphi(x_2)$.

Example 4.1. *Given $\varphi(30) = 8$, give 4 distinct x_1, x_2, x_3, x_4 such that $\varphi(30) = \varphi(x_1)... = \varphi(x_4)$.*

Using the formula from Proposition 3.4 we can rewrite $\varphi(30) = \varphi(2\cdot3\cdot5)$. Since $\varphi(5) = 4$, and $\varphi(8) = \varphi(2^3) = 4$ we can therefore write new $\varphi(2\cdot3\cdot5) = \varphi(2^3\cdot3)$, a new x value with the same $\varphi(x)$. We can do the same with the prime 3, $\varphi(3) = 2$ we can reach the same φ value from $\varphi(4) = \varphi(2^2) = 2$, then write our new $\varphi(2\cdot3\cdot5) = \varphi(2^3\cdot3) = \varphi(2^2\cdot5)$. We can repeat this process to eventually reach 4 new distinct x_1, x_2, x_3, x_4:

$$\varphi(2\cdot3\cdot5) = \varphi(2^3\cdot3) = \varphi(2^2\cdot5) = \varphi(3\cdot5) = \varphi(2^4).$$

□

5 Conclusion

In conclusion, our interests in Euler's totient function led us to wonder: Can we give n distinct numbers $x_1, x_2, ...x_n$ such that.... We also asked ourselves: Over what co-domain is φ surjective? We determined that a codomain of $\varphi(x)$ consists of but not all even numbers and 1.

References

An Introduction To The Theory of Numbers, 5th edition by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery.