Euler's Totient Function

Q. Zhang KS

1 Introduction

Euler's totient function, denoted by $\phi(n)$, is a fundamental arithmetic function in number theory initially conceived by Euler in his investigations concerning modular arithmetic and power residues modulo composite integers. The function was introduced in 1763 as part of a generalisation of Fermat's Little Theorem, now known as the Euler–Fermat Theorem.

Previously, Pierre de Fermat had established that $a^{p-1} \equiv 1 \pmod{p}$ for any prime $p \nmid a$ such that $\gcd(a, p) = 1$. Euler sought to extend this property to composite moduli. This inquiry motivated the development of the totient function $\phi(n)$, which maps a positive integer n to the number of integers from $1, 2, ..., n$ that are coprime to n.

Definition 1.1. The totient function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined as the cardinality of the set of integers up to n that are coprime to n:

$$\phi(n) = \left|\{k \in \mathbb{Z}^+ : 1 \leq k \leq n,\ \gcd(k, n) = 1\}\right|$$

2 Properties of ϕ

Definition 2.1. An arithmetic function $f : \mathbb{Z}^+ \to \mathbb{C}$ is termed multiplicative if $f(mn) = f(m)f(n)$ given that $\gcd(m, n) = 1$. It is termed completely multiplicative if this condition holds for all $m, n \in \mathbb{Z}^+$ without the restriction of coprimality. Euler's totient function ϕ is multiplicative, however it is not completely multiplicative.

2.1 Multiplicativity of ϕ

Theorem 2.1. *If m and n are coprime positive integers, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. Let $a_1, \ldots, a_{\phi(m)}$ and $b_1, \ldots, b_{\phi(n)}$ be the elements of S_m and S_n respectively. We claim that each element of S_{mn} is made from one unique pair (a_j, b_k) and hence their number $\phi(mn) = \phi(m)\phi(n)$.

Initially we are given a pair (a_j, b_k) so we can create a solution e_{jk} of the simultaneous congruences $x \equiv a_j \pmod{m}$ and $x \equiv b_k \pmod{n}$, by the Chinese Remainder Theorem. We may express this as $e_{jk} = a_j c_j n + b_k d_k m$, containing two terms where the first term has a_j, c_j and n, which are all coprime to m and the second term has b_k, d_k and m, which are all also coprime to n. Thus it follows that e_{jk} is coprime to mn. We may now reduce

$e_{jk} \pmod{mn}$ so that it lies within the range 1 to $mn-1$ and thus belongs to S_{mn}. It is also clear that if j or k is altered we must also get an altered e_{jk}.

Moreover, given an element e_l belonging to S_{mn}, we are able to reduce it $\pmod{n}$ to give an element a_j, and since e_l is coprime to mn it must be that a_j is coprime to m and therefore must belong to S_m. Similarly we can reduce $e_l \pmod{n}$ to give an element b_k which belongs to S_n.

If two elements e_s, e_t result in the same pair (a_j, b_k), then $e_s \equiv e_t \pmod{m}$ and $e_s \equiv e_t \pmod{n}$, and since $gcd(m,n) = 1$ we obtain $e_s \equiv e_t \pmod{mn}$. Thus we have established a bijection between $S_m \times S_n$ and S_{mn}, completing our proof. □

2.2 Totient Function of Prime Powers

Theorem 2.2. *Let p be a prime and k a positive integer. Then*

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

Proof. The totient $\phi(p^k)$ counts the number of integers x given that $1 \leq x \leq p^k$ and $gcd(x, p^k) = 1$. The only prime factor of p^k is p, therefore we must have $p \mid x$ for any x which does not satisfy the given conditions. The only integers between 1 and p^k inclusive that are divisible by p are the multiples of p:

$$1 \cdot p,\ 2 \cdot p,\ 3 \cdot p,\ \ldots,\ p^{k-1} \cdot p = p^k.$$

Upon factoring out the p term, these correspond to the choices of coefficients from the set $\{1, 2, \ldots, p^{k-1}\}$, so there are exactly p^{k-1} such elements that do not satisfy the conditions of the totient function. To calculate the number of integers coprime to p^k, we simply subtract the count of multiples of p from the total number of integers in the interval:

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

and we are done. □

2.3 The Product Formula for $\phi(n)$

Theorem 2.3. *For any integer $n > 1$ with prime factorization $n = \prod_{i=1}^{r} p_i^{k_i}$,*

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Proof. We are able to prove this product formula by mathematical induction on the number of distinct prime factors r of n.

Base Case ($r = 1$): If $n = p_1^{k_1}$ for some prime p_1, then by Theorem 2.2, we have $\phi(p_1^{k_1}) = p_1^{k_1}(1 - \frac{1}{p_1})$, which satisfies the formula given when the product is tested with the single prime divisor p_1.

Inductive Step: Assume the formula holds for any integer having $r-1$ distinct prime factors. Let n have a prime factorisation of $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. We can express n as $m \cdot p_r^{k_r}$, where $m = \prod_{i=1}^{r-1} p_i^{k_i}$ possesses $r-1$ distinct prime factors and satisfies $\gcd(m, p_r^{k_r}) = 1$.

Since ϕ is a multiplicative function (Theorem 2.1), we can factor the totient as:

$$\phi(n) = \phi(m)\phi(p_r^{k_r}).$$

Applying the inductive hypothesis to $\phi(m)$ and Theorem 2.2 to $\phi(p_r^{k_r})$, we obtain

$$\phi(n) = \left(m \prod_{i=1}^{r-1} \left(1 - \frac{1}{p_i}\right) \right) \left(p_r^{k_r} \left(1 - \frac{1}{p_r}\right) \right).$$

Grouping the scalar terms $mp_r^{k_r} = n$ and combining the other products yields

$$\phi(n) = (mp_r^{k_r}) \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Thus by induction, the formula holds for all integers $n > 1$. □

3 The Euler–Fermat Theorem

The most well-known application of Euler's totient function in number theory and applied cryptography is the Euler–Fermat Theorem, often also referred to as Euler's Theorem, which provides a generalisation of Fermat's Little Theorem, the proof of which we give below.

Theorem 3.1. *(Euler–Fermat) If m is a positive integer and a is an integer such that $\gcd(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof. Let $R = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ be the distinct residues (mod m) which are coprime to m and a is any element of this set. This is known as a reduced residue system modulo n. By our definition, we have that each r_i is coprime to n, so that no two elements are congruent modulo n, and thus the total number of elements in R is exactly $\phi(m)$.

Now consider the set of residue classes formed by multiplying each element of R by a:

$$S = \{ar_1, ar_2, \ldots, ar_{\phi(m)}\} \pmod{m}.$$

We claim that S is also a reduced residue system modulo m by verifying two properties:

1. **Coprimality:** Since $\gcd(a, m) = 1$ and $\gcd(r_i, m) = 1$ for each i, we have that $\gcd(ar_i, m) = 1$. Thus it follows that each element in S must be coprime to m.
2. **Distinctness modulo m:** Suppose for the sake of contradiction that $ar_i \equiv ar_j \pmod{m}$ for some $i \neq j$, then $a(r_i - r_j) \equiv 0 \pmod{m}$. Since $\gcd(a, n) = 1$, we obtain $r_i \equiv r_j \pmod{m}$. Now each r_i lies between 1 and $(m - 1)$ inclusive, hence $r_i = r_j$. As the residues are distinct, this forces $i = j$. Contradiction establishes the result.

Consequently, S also consists of $\phi(m)$ distinct residue classes, each of which is coprime to m, thus it is a permutation of the residues in R modulo m. Then we may evaluate the product of the elements in S and R congruent modulo m as follows:

$$\prod_{i=1}^{\phi(m)} (ar_i) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.$$

Factoring out $a^{\phi(m)}$ from the left-hand side produces

$$a^{\phi(m)} \left(\prod_{i=1}^{\phi(m)} r_i \right) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.$$

Let $P = \prod_{i=1}^{\phi(m)} r_i$. It is true that each r_i is coprime to m, thus their product P must also be coprime to m. Therefore, there exists some multiplicative inverse for P modulo m, and multiplying both sides by this inverse, we may cancel out the term P and yield

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

□

4 Cryptographic Applications

The totient function forms a key part of the RSA cryptosystem, which uses a public key to encrypt messages and a private key to decrypt them. While anyone is able to use the public key to encrypt a message, a message can only be decrypted when an individual is given access to the private key.

The RSA private key refers to a pair of numbers (d, n) where n is the publicly available modulus and d denotes the private exponent which allows a person to unlock the message m from the ciphertext c:

$$m \equiv c^d \pmod{n}$$

and a key equation connects the public component e and the private key d:

$$ed \equiv 1 \pmod{\phi(n)}$$

Herein lies the vulnerability associated with $\phi(n)$, that is if an adversary were to gain access to it, they could use the *Extended Euclidean Algorithm* to compute the modular inverse of e modulo $\phi(n)$, thereby finding the private exponent d instantly. More significantly, knowing $\phi(n)$ bypasses the intractability of the system upon which RSA's security depends: while multiplying two very large distinct primes p and q to yield n is trivial, reversing the process to recover the prime factors p and q from only n is believed to be infeasible for modern computers given sufficiently large p and q. Knowledge of $\phi(n)$ and its multiplicative properties reduces the issue to elementary algebra as

$$\phi(n) = (p-1)(q-1) = n - (p+q) + 1$$

Thus an attacker may simply rearrange to find the sum of the two primes:

$$p + q = n - \phi(n) + 1$$

and the product $n = pq$ and the sum $p + q$ of the two secret primes satisfy the following quadratic equation:

$$x^2 - (p+q)x + n = 0$$

which can instantly yield p and q.

Therefore $\phi(n)$ is the fundamental architectural tool required to formulate the key during the setup and its preservation is essential to the integrity of a secure system.

5 Conclusion and Discussion

From its origins in modular residue classes and the proof of Euler–Fermat, Euler's totient function $\phi(n)$ acts as a bridge between elements of elementary number theory, abstract algebra and modern applied cryptography. However, the cryptographic significance of $\phi(n)$ remains only a small facet of its overall theoretical importance, with it being a key domain for mathematical inquiry in many other fields.

These include the algebraic generalisation of counting coprime residue classes beyond the ring of integers $\mathbb{Z}$ to general Dedekind domains and algebraic number fields as well as the analytic behaviour of $\phi(n)$ within analytic number theory. The study of its average order reveals elegant asymptotic density properties, as in:

$$\sum_{n \leq x} \phi(n) = \frac{3}{\pi^2} x^2 + O(x \log x)$$

Its broader behaviour directly links to the distribution of primes and longlasting open questions in number theory such as Lehmer's Totient Problem and Carmichael's Totient Conjecture. Ultimately, $\phi(n)$, though simple in its initial combinatorial definition, serves as a magical unifying thread across many fields of pure and applied mathematics.

References

Apostol, Tom M. *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics, Springer-Verlag, 1976. https://doi.org/10.1007/978-1-4757-5579-4.

Hardy, G. H., and E. M. Wright. *An Introduction to the Theory of Numbers.* Revised by D. R. Heath-Brown and J. H. Silverman, 6th ed., Oxford University Press, 2008. https://india.oup.com/product/an-introduction-to-the-theory-of-numbers-sixth-edition-9780199219865.

Ireland, Kenneth, and Michael Rosen. *A Classical Introduction to Modern Number Theory.* 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, 1990. https://doi.org/10.1007/978-1-4757-2103-4.

Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers.* 5th ed., John Wiley & Sons, 1991. https://catalog.hathitrust.org/Record/002430432.

Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120–126. https://doi.org/10.1145/359340.359342.