Euler's Totient Function and Applications

1 Totient Function Computation

The Euler's totient function $\phi(n)$ counts the number of integers from 1 to n that are coprime to n. The following C++ function computes $\phi(1)$ to $\phi(n)$ efficiently:

```
void phi_1_to_n(int n) {
    vector<int> phi(n + 1);
    phi[0] = 0;
    phi[1] = 1;
    for (int i = 2; i <= n; i++)
        phi[i] = i - 1;

    for (int i = 2; i <= n; i++)
        for (int j = 2 * i; j <= n; j += i)
              phi[j] -= phi[i];
}
```

2 Euler's Theorem

Euler's theorem states that:

$$a^{\phi(m)} \equiv 1 \pmod{m}, \quad \text{if } \gcd(a, m) = 1. \tag{1}$$

A special case of this, when m is prime, reduces to Fermat's Little Theorem:

$$a^{m-1} \equiv 1 \pmod{m}. \tag{2}$$

Euler's theorem is used in computing the modular multiplicative inverse and optimizing modular exponentiation.

3 Modular Reduction Using Totient Function

A useful consequence of Euler's theorem is:

$$a^n \equiv a^{n \bmod \phi(m)} \pmod{m}. \tag{3}$$

This allows efficient computation of large exponents modulo m, especially when n is dynamically computed.

4 Group Theory Interpretation

The function $\phi(n)$ represents the order of the multiplicative group mod n:

$$(\mathbb{Z}/n\mathbb{Z})^{\times}. \tag{4}$$

The multiplicative order of a modulo n, denoted as $\text{ord}_n(a)$, is the smallest k such that:

$$a^k \equiv 1 \pmod{n}. \tag{5}$$

By Lagrange's theorem, $\text{ord}_n(a)$ divides $\phi(n)$. If $\text{ord}_n(a) = \phi(n)$, then a is a primitive root, making the group cyclic.

5 Generalization for Non-Coprime Bases

For any x, m, and large n:

$$x^n \equiv x^{\phi(m)+[n \bmod \phi(m)]} \pmod{m}. \tag{6}$$

Proof: Let $p_1, \ldots, p_t$ be the common prime divisors of x and m with exponents k_i in m. Define $a = p_1^{k_1} \ldots p_t^{k_t}$ so that m/a is coprime to x. Then,

$$x^n \bmod m = x^k \left(x^{n-k \bmod \phi(m/a)} \bmod m/a \right) \bmod m. \tag{7}$$

This shows that the powers of x modulo m eventually form a cycle of length $\phi(m)$.

6 Conclusion

Euler's totient function plays a crucial role in number theory, particularly in modular arithmetic, cryptography, and group theory. It enables efficient modular exponentiation and helps in understanding the structure of multiplicative groups.