COMPUTATIONAL MATHEMATICS
TOPIC V - EULER PHI FUNCTION

PAUL L. BAILEY

1. Review of Basic Modular Arithmetic

We begin by reviewing some definitions and results.

Let $a, b, d, n \in \mathbb{Z}$, where $n \geq 2$. We say that d *divides* n, and write $d \mid n$, if $n = kd$ for some $k \in \mathbb{Z}$. We say that *a is congruent to b modulo n*, and write $a \equiv b \pmod{n}$, if $n \mid a - b$.

We have shown that the congruence is a equivalence relation, which implies that the set $\mathbb{Z}$ can be broken up into disjoint blocks such that every member of one block is equivalent to a unique integer r such that $0 \leq r < n$. We denote the block that contains r by $\overline{r}$. We let $\mathbb{Z}_n$ be the set of all congruence classes, modulo n. We have seen that $\mathbb{Z}_n$ is a ring under the operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$.

We say that *a is invertible modulo n* if $ac \equiv 1 \pmod{n}$ for some $c \in \mathbb{Z}$. We have a theorem which states that a is invertible modulo n if and only if $\gcd(a, n) = 1$. This is equivalent to the condition that $\overline{a}$ is an invertible element in the ring $\mathbb{Z}_n$. We have also seen that if $a \neq 0$ and $\gcd(a, n) > 1$, then $\overline{a}$ is a zero divisor in $\mathbb{Z}_n$, which means that if $\overline{a} \cdot \overline{b} = \overline{0}$ for some $\overline{b} \neq \overline{0}$.

Set

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ is invertible}\}.$$

Then $x \in \mathbb{Z}_n^*$ if and only if $x = \overline{a}$ for some $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. The inverse of $x \in \mathbb{Z}_n^*$ may be found using the extended Euclidean algorithm. Since the product of invertible elements is also invertible, $\mathbb{Z}_n*$ is closed under multiplication, so $\mathbb{Z}_n^*$ is a group under multiplication.

2. Euler Phi Function

Let $n \in \mathbb{N}$ with $n \geq 2$. The *Euler Phi Function* is defined by declaring $\phi(n)$ to be the number of positive integers less than n which are relatively prime to n. Clearly,

$$\begin{aligned} \phi(n) &= |\{a \in \mathbb{Z} \mid 1 \leq a < n \text{ and } \gcd(a, n) = 1\}| \\ &= |\mathbb{Z}_n^*|. \end{aligned}$$

Proposition 1 (Euler's Theorem)**.** *Let $a, n \in \mathbb{Z}$ with $n \geq 2$ and $\gcd(a, n) = 1$. Then*

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

Proof. If $w \in \mathbb{Z}$, let $\rho(w)$ denote the remainder of w is divided by n.

Let X denote the set of all positive integers less than n and relatively prime to n. Note that if $\gcd(a, n) = 1$ and $\gcd(x, n) = 1$, then $\gcd(ax, n) = 1$; thus if $x \in X$, then $\rho(ax) \in X$.

Date: Wednesday, October 31, 2018.

Define a function

$$\psi : X \to X \quad \text{by} \quad \psi(x) = \rho(ax).$$

We claim that ψ is surjective. To see this, note that since $\gcd(a, n) = 1$, there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$. Let $y \in X$ and set $x = \rho(by)$. Then

$$\psi(x) \equiv aby \equiv y \pmod{n}.$$

Thus ψ is surjective, and since X is finite, ψ is bijective; that is, ψ is a permutation of X, and it follows that

$$\prod_{x \in X} x \equiv \prod_{x \in X} \psi(x) \equiv \prod_{x \in X} ax \equiv a^{\phi(n)} \prod_{x \in X} x \pmod{n}.$$

Canceling $\prod_{x \in X} x$ from both sides leads to

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

□

Remark 1. Euler's Theorem is a specific case of a more general theorem which states that if G is a finite multiplicative group and $a \in G$, then

$$a^{|G|} = 1.$$

Let $n \in \mathbb{Z}$ with $n \geq 2$. There is a formula to compute $\phi(n)$ effectively; we multiply n by the product of factors of the form $(1 - \frac{1}{p})$, where p is a prime that divides n. In order to demonstrate that this formula works, our proof will be built from three lemmas.

Lemma 1. *Let $p \in \mathbb{Z}$. If p is prime, then $\phi(p) = p - 1$.*

Proof. Every positive integer less than a prime is relatively prime to it. There are exactly $p - 1$ positive integers less than p. Thus

$$\phi(p) = p - 1.$$

□

Lemma 2. *Let $p, r \in bZ$ be positive. If p is prime, then*

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

Proof. Then only positive integers not relatively prime to p^r are multiples of p There are exactly p^r nonnegative integers less than p^r, and exactly one out of every p of them is a multiple of p, so exactly one out of every p of them is not relatively prime to p. Thus there are $\dfrac{p^r}{p} = p^{r-1}$ such integers; the rest of the positive integers less than p^r are relatively prime to p. Thus the number of integers relatively prime to p is

$$\phi(p^r) = p^r - p^{r-1} = p^r\Big(1 - \frac{1}{p}\Big).$$

□

Lemma 3. *Let $m, n \in \mathbb{Z}$ with $m, n \geq 2$. If* $\gcd(m, n) = 1$*, then*

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. Let $\rho : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ be given by $\rho(c) = (c \pmod m, c \pmod n)$. To show that ρ is surjective, let $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. By the Chinese Remainder Theorem, there exists a unique $c \in \mathbb{Z}$ such that $0 \leq c < mn$ and

$$\begin{aligned} c &\equiv a \pmod m \text{ and} \\ c &\equiv b \pmod n. \end{aligned}$$

Thus $\rho(c) = (a, b)$, so ρ is surjective. Now

$$|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn = |\mathbb{Z}_{mn}|,$$

so ρ is bijective. Since m and n are relatively prime,

$$\gcd(c, mn) = 1 \quad \Leftrightarrow \quad \gcd(c, m) = 1 \text{ and } \gcd(c, n) = 1.$$

Thus

$$c \in \mathbb{Z}^*_{mn} \quad \Leftrightarrow \quad c \in \mathbb{Z}^*_m \text{ and } c \in \mathbb{Z}^*_n.$$

It follows that $\mathbb{Z}^*_{mn} = \mathbb{Z}^*_m \times \mathbb{Z}^*_n$. Therefore,

$$\phi(mn) = |\phi^*_{mn}| = |\mathbb{Z}^*_m \times \mathbb{Z}^*_n| = |\mathbb{Z}^*_m| \cdot |\mathbb{Z}^*_n| = \phi(m)\phi(n).$$

□

Proposition 2. *Let $n \in \mathbb{Z}$ with $n \geq 2$. Then*

$$\phi(n) = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big),$$

where p ranges over the set of distinct prime factors of n.

Proof. By the Fundamental Theorem of Arithmetic, n may be expressed as a product to prime power factors:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k},$$

where $p_1 < p_2 < \cdots < p_k$ are the distinct prime factors of n. Since these distinct primes are relatively prime to each other, the previous lemmas imply that

$$\begin{aligned} \phi(n) &= \phi(p_1^{r_1})\phi(p_2^{r_2}) \cdots \phi(p_k^{r_k}) \\ &= p_1^{r_1}(1 - \frac{1}{p_1})p_2^{r_2}(1 - \frac{1}{p_2}) \cdots p_k^{r_k}(1 - \frac{1}{p_k}) \\ &= p_1^{r_1}p_2^{r_2} \cdots p_k^{r_k}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) \\ &= n \prod_{i=1}^{k}(1 - \frac{1}{p_i}). \end{aligned}$$

□

3. Modular Exponentiation

We wish to rapidly compute powers of a where $a \in \mathbb{Z}_n^*$. By convention, let e denote the exponent.

3.1. Exponentiation by Squaring.

Write e in binary as

$$e = \sum_{i=0}^{t-1} b_i 2^i,$$

where $b_i \in \{0, 1\}$ and t is the bitlength of e. Making use of the standard property $a^{m+n} = a^m a^n$, we see that

$$\begin{aligned} a^e &= a^{\sum_{i=0}^{t-1} b_i 2^i} \\ &= \prod_{i=0}^{t-1} a^{b_i 2^i}. \end{aligned}$$

This may be efficiently implemented in a computer using bit rotation.

3.2. Exponentiation with Modular Arithmetic in the Base.

At each phase of forming the product above, we may take the residue modulo n, to reduce the size of the numbers involved. This not only keeps the number within an acceptable number of bits (we need results less than 32 bits if we are computing with 64 bit integers), it also can make the computations faster.

3.3. Exponentiation with Modular Arithmetic in the Exponent.

If the base a is relatively prime to the modulus n, Euler theorem applies, so we can work modulo $\phi(n)$ in the exponent. Divide $\phi(n)$ into e to obtain $e = \phi(n)q + r$. Then

$$a^e \equiv a^{\phi(n)q+r} \equiv (a^{\phi(n)})^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{n};$$

taking the r^{th} power of a is bound to be faster than taking the e^{th} power, unless of course $e < \phi(n)$.

Department of Mathematics and CSci, BASIS Scottsdale
Email address: paul.bailey@basised.com