Introduction to number theory-7

May 8, 2017

2.3 The Euler Phi Function

An *arithmetic function* is a function defined on the positive integers. The Euler phi function $\varphi(m)$ is the arithmetic function that counts the number of integers in the set $0, 1, 2, \ldots, m-1$ that are relatively prime to m. We have

$$\begin{array}{lcllcl} \varphi(1) & = & 1, & \varphi(6) & = & 2, \\ \varphi(2) & = & 2, & \varphi(7) & = & 6, \\ \varphi(3) & = & 3, & \varphi(8) & = & 4, \\ \varphi(4) & = & 2, & \varphi(9) & = & 6, \\ \varphi(5) & = & 4, & \varphi(10) & = & 4. \end{array}$$

If p is a prime number, then $(a, p) = 1$ for $a = 1, \ldots, p-1$, and $\varphi(p) = p-1$. If p^r is a prime power and $0 \leq a \leq p^r - 1$, then $(a, p^r) > 1$ if and only if a is a multiple of p. The integral multiples of p in the interval $[0, p^r - 1]$ are the p^{r-1} numbers $0, p, 2p, 3p, \ldots, (p^{r-1} - 1)p$, and so

$$\varphi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).$$

In this section we shall obtain some important properties of the Euler phi function.

Theorem 2.6 *Let m and n be relatively prime positive integers. For every integer c there exist unique integers a and b such that*

$$0 \leq a \leq n-1,$$

$$0 \leq b \leq m-1,$$

and

$$c \equiv ma + nb \pmod{mn}. \tag{2.4}$$

Moreover, $(c, mn) = 1$ if and only if $(a, n) = (b, m) = 1$ in the representation (2.4).

Proof. If a_1, a_2, b_1, b_2 are integers such that

$$ma_1 + nb_1 \equiv ma_2 + nb_2 \pmod{mn},$$

then

$$ma_1 \equiv ma_1 + nb_1 \equiv ma_2 + nb_2 \equiv ma_2 \pmod{n}.$$

Since $(m, n) = 1$, it follows that

$$a_1 \equiv a_2 \pmod{n},$$

and so $a_1 = a_2$. Similarly, $b_1 = b_2$. It follows that the mn integers $ma + nb$ are pairwise incongruent modulo mn. Since there are exactly mn distinct congruence classes modulo mn, the congruence (2.4) has a unique solution for every integer c.

Let $c \equiv ma + nb \pmod{mn}$. Since $(m, n) = 1$, we have

$$(c, m) = (ma + nb, m) = (nb, m) = (b, m)$$

and

$$(c, n) = (ma + nb, n) = (ma, n) = (a, n).$$

It follows that $(c, mn) = 1$ if and only if $(c, m) = (c, n) = 1$ if and only if $(b, m) = (a, n) = 1$. This completes the proof. □

For example, we can represent the congruence classes modulo 6 as linear combinations of 2 and 3 as follows:

$$\begin{aligned}
0 &\equiv 0 \cdot 2 + 0 \cdot 3 \pmod 6, \\
1 &\equiv 2 \cdot 2 + 1 \cdot 3 \pmod 6, \\
2 &\equiv 1 \cdot 2 + 0 \cdot 3 \pmod 6, \\
3 &\equiv 0 \cdot 2 + 1 \cdot 3 \pmod 6, \\
4 &\equiv 2 \cdot 2 + 0 \cdot 3 \pmod 6, \\
5 &\equiv 1 \cdot 2 + 1 \cdot 3 \pmod 6.
\end{aligned}$$

A *multiplicative* function is an arithmetic function $f(m)$ such that $f(mn) = f(m)f(n)$ for all pairs of relatively prime positive integers m and n. If $f(m)$ is multiplicative, then it is easy to prove by induction on k that if $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, then $f(m_1 \cdots m_k) = f(m_1) \cdots f(m_k)$.

Theorem 2.7 *The Euler phi function is multiplicative. Moreover,*

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

Proof. Let $(m, n) = 1$. There are $\varphi(mn)$ congruence classes in the ring $\mathbf{Z}/mn\mathbf{Z}$ that are relatively prime to mn. By Theorem 2.6, every congruence class modulo mn can be written uniquely in the form $ma + nb + mn\mathbf{Z}$, where a and b are integers such that $0 \leq a \leq n-1$ and $0 \leq b \leq m-1$. Moreover, the congruence class $ma + nb + mn\mathbf{Z}$ is prime to mn if and only if $(b, m) = (a, n) = 1$. Since there are $\varphi(n)$ integers $a \in [0, n-1]$ that are relatively prime to n, and $\varphi(m)$ integers $b \in [0, m-1]$ relatively prime to m, it follows that $\varphi(mn) = \varphi(m)\varphi(n)$, and so the Euler phi function is multiplicative. If $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, then $\varphi(m_1 \cdots m_k) = \varphi(m_1) \cdots \varphi(m_k)$. In particular, if $m = p_1^{r_1} \cdots p_k^{r_k}$ is the standard factorization of m, where $p_1, \ldots, p_k$ are distinct primes and $r_1, \ldots, r_k$ are positive integers, then

$$\varphi(m) = \prod_{i=1}^{k} \varphi\left(p_i^{r_i}\right) = \prod_{i=1}^{k} p_i^{r_i}\left(1 - \frac{1}{p_i}\right) = m \prod_{p|m}\left(1 - \frac{1}{p}\right).$$

This completes the proof. □

For example, $7875 = 3^2 5^3 7$ and

$$\varphi(7875) = \varphi(3^2)\varphi(5^3)\varphi(7) = (9-3)(125-25)(7-1) = 3600.$$

Theorem 2.8 *For every positive integer m,*

$$\sum_{d|m} \varphi(d) = m.$$

Proof. We first consider the case where $m = p^t$ is a power of a prime p. The divisors of p^t are $1, p, p^2, \ldots, p^t$, and

$$\sum_{d|p^t} \varphi(d) = \sum_{r=0}^{t} \varphi(p^r) = 1 + \sum_{r=1}^{t} \left(p^r - p^{r-1}\right) = p^t.$$

Next we consider the general case where m has the standard factorization

$$m = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k},$$

where $p_1, \ldots, p_k$ are distinct prime numbers and $t_1, \ldots, t_k$ are positive integers. Every divisor d of m is of the form

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

where $0 \leq r_i \leq t_i$ for $i = 1, \ldots, k$. By Theorem 2.7, $\varphi(d)$ is multiplicative, and so

$$\varphi(d) = \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}).$$

Therefore,

$$\begin{aligned}
\sum_{d|m} \varphi(d) &= \sum_{r_1=0}^{t_1} \cdots \sum_{r_k=0}^{t_k} \varphi\left(p_1^{r_1} \cdots p_k^{r_k}\right) \\
&= \sum_{r_1=0}^{t_1} \cdots \sum_{r_k=0}^{t_k} \varphi(p_1^{r_1}) \varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}) \\
&= \prod_{i=1}^{k} \sum_{r_i=0}^{t_i} \varphi\left(p_i^{r_i}\right) \\
&= \prod_{i=1}^{k} p_i^{t_i} \\
&= m.
\end{aligned}$$

This completes the proof. □

For example,

$$\begin{aligned}\sum_{d|12}\varphi(d) &= \varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)\\ &= 1+1+2+2+2+4\\ &= 12\end{aligned}$$

and

$$\begin{aligned}\sum_{d|45}\varphi(d) &= \varphi(1)+\varphi(3)+\varphi(5)+\varphi(9)+\varphi(15)+\varphi(45)\\ &= 1+2+4+6+8+24\\ &= 45.\end{aligned}$$

2.4 Chinese Remainder Theorem

Theorem 2.9 *Let m and n be positive integers. For any integers a and b there exists an integer x such that*

$$x \equiv a \pmod{m} \tag{2.5}$$

and

$$x \equiv b \pmod{n} \tag{2.6}$$

if and only if

$$a \equiv b \pmod{(m,n)}.$$

If x is a solution of congruences (2.5) and (2.6), then the integer y is also a solution if and only if

$$x \equiv y \pmod{[m,n]}.$$

Proof. If x is a solution of congruence (2.5), then $x = a + mu$ for some integer u. If x is also a solution of congruence (2.6), then

$$x = a + mu \equiv b \pmod{n},$$

that is,

$$a + mu = b + nv$$

for some integer v. It follows that

$$a - b = nv - mu \equiv 0 \pmod{(m, n)}.$$

Conversely, if $a - b \equiv 0 \pmod{(m, n)}$, then by Theorem 1.15 there exist integers u and v such that

$$a - b = nv - mu.$$

Then

$$x = a + mu = b + nv$$

is a solution of the two congruences.

An integer y is another solution of the congruences if and only if

$$y \equiv a \equiv x \pmod{m}$$

and

$$y \equiv b \equiv x \pmod{n},$$

that is, if and only if $x-y$ is a common multiple of m and n, or, equivalently, $x - y$ is divisible by the least common multiple $[m, n]$. This completes the proof. $\square$

For example, the system of congruences

$$\begin{aligned} x &\equiv 5 \pmod{21}, \\ x &\equiv 19 \pmod{56}, \end{aligned}$$

has a solution, since

$$(56, 21) = 7$$

and

$$19 \equiv 5 \pmod{7}.$$

The integer x is a solution if there exists an integer u such that

$$x = 5 + 21u \equiv 19 \pmod{56},$$

that is,

$$21u \equiv 14 \pmod{56},$$

$$3u \equiv 2 \pmod{8},$$

or

$$u \equiv 6 \pmod{8}.$$

Then

$$x = 5 + 21u = 5 + 21(6 + 8v) = 131 + 168v$$

is a solution of the system of congruences for any integer v, and so the set of all solutions is the congruence class $131 + 168\mathbf{Z}$.

Theorem 2.10 (Chinese remainder theorem) *Let $k \geq 2$. If $a_1, \ldots, a_k$ are integers and $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, then there exists an integer x such that*

$$x \equiv a_i \pmod{m_i} \quad \text{for all } i = 1, \ldots, k.$$

If x is any solution of this set of congruences, then the integer y is also a solution if and only if

$$x \equiv y \pmod{m_1 \cdots m_k}.$$

Proof. We prove the theorem by induction on k. If $k = 2$, then $[m_1, m_2] = m_1 m_2$, and this is a special case of Theorem 2.9.

Let $k \geq 3$, and assume that the statement is true for $k-1$ congruences. Then there exists an integer z such that $z \equiv a_i \pmod{m_i}$ for $i = 1, \ldots, k-1$. Since $m_1, \ldots, m_k$ are pairwise relatively prime integers, we have

$$(m_1 \cdots m_{k-1}, m_k) = 1,$$

and so, by the case $k = 2$, there exists an integer x such that

$$\begin{aligned} x &\equiv z \pmod{m_1 \cdots m_{k-1}}, \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Then

$$x \equiv z \equiv a_i \pmod{m_i}$$

for $i = 1, \ldots, k-1$.

If y is another solution of the system of k congruences, then $x - y$ is divisible by m_i for all $i = 1, \ldots, k$. Since $m_1, \ldots, m_k$ are pairwise relatively prime, it follows that $x - y$ is divisible by $m_1 \cdots m_k$. This completes the proof. □

For example, the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 3 \pmod 5, \\ x &\equiv 5 \pmod 7, \\ x &\equiv 7 \pmod{11} \end{aligned}$$

has a solution, since the moduli are pairwise relatively prime. The solution to the first two congruences is the congruence class

$$x \equiv 8 \pmod{15}.$$

The solution to the first three congruences is the congruence class

$$x \equiv 68 \pmod{105}.$$

The solution to the four congruences is the congruence class

$$x \equiv 1118 \pmod{1155}.$$

There is an important application of the Chinese remainder theorem to the problem of solving diophantine equations of the form

$$f(x_1, \ldots, x_k) \equiv 0 \pmod{m},$$

where $f(x_1, \ldots, x_k)$ is a polynomial with integer coefficients in one or several variables. This equation is *solvable modulo* m if there exist integers $a_1, \ldots, a_k$ such that

$$f(a_1, \ldots, a_k) \equiv 0 \pmod{m}.$$

The Chinese remainder theorem allows us to reduce the question of the solvability of this congruence modulo m to the special case of prime power moduli p^r. For simplicity, we consider polynomials in only one variable.

Theorem 2.11 *Let*

$$m = p_1^{r_1} \cdots p_k^{r_k}$$

be the standard factorization of the positive integer m. Let $f(x)$ be a polynomial with integral coefficients. The congruence

$$f(x) \equiv 0 \pmod{m}$$

is solvable if and only if the congruences

$$f(x) \equiv 0 \pmod{p_i^{r_i}}$$

are solvable for all $i = 1, \ldots, k$.

Proof. If $f(x) \equiv 0 \pmod{m}$ has a solution in integers, then there exists an integer a such that m divides $f(a)$. Since $p_i^{r_i}$ divides m, it follows that $p_i^{r_i}$ divides $f(a)$, and so the congruences $f(x) \equiv 0 \pmod{p_i^{r_i}}$ are solvable for $i = 1, \ldots, k$.

Conversely, suppose that the congruences $f(x) \equiv 0 \pmod{p_i^{r_i}}$ are solvable for $i = 1, \ldots, k$. Then for each i there exists an integer a_i such that

$$f(a_i) \equiv 0 \pmod{p_i^{r_i}}.$$

Since the prime powers $p_1^{r_1}, \ldots, p_k^{r_k}$ are pairwise relatively prime, the Chinese remainder theorem tells us that there exists an integer a such that

$$a \equiv a_i \pmod{p_i^{r_i}}$$

for all i. Then

$$f(a) \equiv f(a_i) \equiv 0 \pmod{p_i^{r_i}}$$

for all i. Since $f(a)$ is divisible by each of the prime powers $p_i^{r_i}$, it is also divisible by their product m, and so $f(a) \equiv 0 \pmod{m}$. This completes the proof. $\square$

For example, consider the congruence

$$f(x) = x^2 - 34 \equiv 0 \pmod{495}.$$

Since $495 = 3^2 \cdot 5 \cdot 11$, it suffices to solve the congruences

$$f(x) = x^2 - 34 \equiv x^2 + 2 \equiv 0 \pmod{9},$$

$$f(x) = x^2 - 34 \equiv x^2 + 1 \equiv 0 \pmod{5},$$

and

$$f(x) = x^2 - 34 \equiv x^2 - 1 \equiv 0 \pmod{11}.$$

These congruences have solutions

$$f(5) \equiv 0 \pmod{9},$$

$$f(2) \equiv 0 \pmod{5},$$

and

$$f(1) \equiv 0 \pmod{11}.$$

By the Chinese remainder theorem, there exists an integer a such that

$$\begin{aligned} a &\equiv 5 \pmod 9, \\ a &\equiv 2 \pmod 5, \\ a &\equiv 1 \pmod{11}. \end{aligned}$$

Solving these congruences, we obtain

$$a \equiv 122 \pmod{495}.$$

We can check that

$$f(122) = 122^2 - 34 = 14,850 = 30 \cdot 495,$$

and so

$$f(122) \equiv 0 \pmod{495}.$$

2.5 Euler's Theorem and Fermat's Theorem

Theorem 2.12 (Euler) *Let m be a positive integer, and let a be an integer relatively prime to m. Then*

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

Proof. Let $\{r_1, \ldots, r_{\varphi(m)}\}$ be a reduced set of residues modulo m. Since $(a, m) = 1$, we have $(ar_i, m) = 1$ for $i = 1, \ldots, \varphi(m)$. Consequently, for every $i \in \{1, \ldots, \varphi(m)\}$ there exists $\sigma(i) \in \{1, \ldots, \varphi(m)\}$ such that

$$ar_i \equiv r_{\sigma(i)} \pmod{m}.$$

Moreover, $ar_i \equiv ar_j \pmod{m}$ if and only if $i = j$, and so σ is a permutation of the set $\{1, \ldots, \varphi(m)\}$ and $\{ar_1, \ldots, ar_{\varphi(m)}\}$ is also a reduced set of residues modulo m. It follows that

$$\begin{aligned} a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} &\equiv (ar_1)(ar_2)\cdots(ar_{\varphi(m)}) \pmod{m} \\ &\equiv r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(\varphi(m))} \pmod{m} \\ &\equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}. \end{aligned}$$

Dividing by $r_1 r_2 \cdots r_{\varphi(m)}$, we obtain

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

This completes the proof. □

Theorem 2.13 (Fermat) *Let p be a prime number. If the integer a is not divisible by p, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Moreover,

$$a^p \equiv a \pmod{p}$$

for every integer a.

Proof. If p is prime and does not divide a, then $(a, p) = 1$, $\varphi(p) = p - 1$, and

$$a^{p-1} = a^{\varphi(p)} \equiv 1 \pmod{p}$$

by Euler's theorem. Multiplying this congruence by a, we obtain

$$a^p \equiv a \pmod{p}.$$

If p divides a, then this congruence also holds for a. □

Let m be a positive integer and let a be an integer that is relatively prime to m. By Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. The *order* of a with respect to the modulus m is the smallest positive integer d such that $a^d \equiv 1 \pmod{m}$. Then $1 \leq d \leq \varphi(m)$. We denote the order of a modulo m by $\mathrm{ord}_m(a)$. We shall prove that $\mathrm{ord}_m(a)$ divides $\varphi(m)$ for every integer a relatively prime to p.

Theorem 2.14 *Let m be a positive integer and a an integer relatively prime to m. If d is the order of a modulo m, then $a^k \equiv a^\ell \pmod{m}$ if and only if $k \equiv \ell \pmod{d}$. In particular, $a^n \equiv 1 \pmod{m}$ if and only if d divides n, and so d divides $\varphi(m)$.*

Proof. Since a has order d modulo m, we have $a^d \equiv 1 \pmod{m}$. If $k \equiv \ell \pmod{d}$, then $k = \ell + dq$, and so

$$a^k = a^{\ell+dq} = a^\ell \left(a^d\right)^q \equiv a^\ell \pmod{m}.$$

Conversely, suppose that $a^k \equiv a^\ell \pmod{m}$. By the division algorithm, there exist integers q and r such that

$$k - \ell = dq + r \qquad \text{and} \qquad 0 \leq r \leq d - 1.$$

Then

$$a^k = a^{\ell+dq+r} = a^\ell \left(a^d\right)^q a^r \equiv a^k a^r \pmod{m}.$$

Since $(a^k, m) = 1$, we can divide this congruence by a^k and obtain

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

Since $0 \leq r \leq d-1$, and d is the order of a modulo m, it follows that $r = 0$, and so $k \equiv \ell \pmod{d}$.

If $a^n \equiv 1 \equiv a^0 \pmod{m}$, then d divides n. In particular, d divides $\varphi(m)$, since $a^{\varphi(m)} \equiv 1 \pmod{m}$ by Euler's theorem. $\square$

Theorem 2.15 (Lagrange's theorem) *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.*

Proof. Let G be a group, written multiplicatively, and let X be a nonempty subset of G. For every $a \in G$ we define the set

$$aX = \{ax : x \in X\}.$$

The map $f : X \to aX$ defined by $f(x) = ax$ is a bijection, and so $|X| = |aX|$ for all $a \in G$. If H is a subgroup of G, then aH is called a *coset* of H. Let aH and bH be cosets of the subgroup H. If $aH \cap bH \neq \emptyset$, then there exist $x, y \in H$ such that $ax = by$, or, since H is a subgroup, $b = axy^{-1} = az$, where $z = xy^{-1} \in H$. Then $bh = azh \in aH$ for all $h \in H$, and so $bH \subseteq aH$. By symmetry, $aH \subseteq bH$, and so $aH = bH$. Therefore, cosets of a subgroup H are either disjoint or equal. Since every element of G belongs to some coset of H (for example, $a \in aH$ for all $a \in G$), it follows that the cosets of H partition G. We denote the set of cosets by G/H. If G is a finite group, then H and G/H are finite, and

$$|G| = |H||G/H|.$$

In particular, we see that $|H|$ divides $|G|$. □

Let G be a group, written multiplicatively, and let $a \in G$. Let $H = \{a^k : k \in \mathbf{Z}\}$. Then $1 = a^0 \in H \subseteq G$. Since $a^k a^\ell = a^{k+\ell}$ for all $k, \ell \in \mathbf{Z}$, it follows that H is a subgroup of G. This subgroup is called the *cyclic subgroup generated by* a, and written $\langle a \rangle$. Cyclic subgroups are abelian.

The group G is *cyclic* if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case, the element a is called a *generator* of G. For example, the group $(\mathbf{Z}/7\mathbf{Z})^\times$ is a cyclic group of order 6 generated by $3 + 7\mathbf{Z}$. The congruence class $5 + 7\mathbf{Z}$ is another generator of this group.

If $a^k \neq a^\ell$ for all integers $k \neq \ell$, then the cyclic subgroup generated by a is infinite. If there exist integers k and ℓ such that $k < \ell$ and $a^k = a^\ell$, then $a^{\ell-k} = 1$. Let d be the smallest positive integer such that $a^d = 1$. Then the group elements $1, a, a^2, \ldots, a^{d-1}$ are distinct. Let $n \in \mathbf{Z}$. By the division algorithm, there exist integers q and r such that $n = dq + r$ and $0 \leq r \leq d - 1$. Since

$$a^n = a^{dq+r} = \left(a^d\right)^q a^r = a^r,$$

it follows that

$$\langle a \rangle = \{a^n : n \in \mathbf{Z}\} = \{a^r : 0 \leq r \leq d - 1\},$$

and the cyclic subgroup generated by a has order d. Moreover, $a^k = a^\ell$ if and only if $k \equiv \ell \pmod{d}$.

Let G be a group, and let $a \in G$. We define the *order* of a as the cardinality of the cyclic subgroup generated by a.

Theorem 2.16 *Let G be a finite group, and $a \in G$. Then the order of the element a divides the order of the group G.*

Proof. This follows immediately from Theorem 2.15, since the order of a is the order of the cyclic subgroup that a generates. □

Let us apply these remarks to the special case when $G = (\mathbf{Z}/m\mathbf{Z})^\times$ is the group of units in the ring of congruence classes modulo m. Then G is a finite group of order $\varphi(m)$. Let $(a, m) = 1$ and let d be the order of $a + m\mathbf{Z}$ in G, that is, the order of the cyclic subgroup generated by $a + m\mathbf{Z}$. By Theorem 2.16, d divides $\varphi(m)$, and so

$$a^{\varphi(m)} + m\mathbf{Z} = (a + m\mathbf{Z})^{\varphi(m)} = \left((a + m\mathbf{Z})^d\right)^{\varphi(m)/d} = 1 + m\mathbf{Z}.$$

Equivalently,

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

This is Euler's theorem.

Proof. Let S be the set of all integers u such that $a^u \in H$. If $u, v \in S$, then $a^u, a^v \in H$. Since H is a subgroup, it follows that $a^u a^v = a^{u+v} \in H$ and $a^u (a^v)^{-1} = a^{u-v} \in H$. Therefore, $u \pm v \in S$, and S is a subgroup of $\mathbf{Z}$. By Theorem 1.3, there is a unique nonnegative integer d such that $S = d\mathbf{Z}$, and so H is the cyclic subgroup generated by a^d. Since $a^m = 1 \in H$, we have $m \in S$, and so d is a positive divisor of m. It follows that H has order m/d. $\square$

Theorem 2.18 *Let G be a cyclic group of order m, and let a be a generator of G. For every integer k, the cyclic subgroup generated by a^k has order m/d, where $d = (m, k)$, and $\langle a^k \rangle = \langle a^d \rangle$. In particular, G has exactly $\varphi(m)$ generators.*

Proof. Since $d = (k, m)$, there exist integers x and y such that $d = kx + my$. Then

$$a^d = a^{kx+my} = \left(a^k\right)^x \left(a^m\right)^y = \left(a^k\right)^x,$$

and so $a^d \in \langle a^k \rangle$ and $\langle a^d \rangle \subseteq \langle a^k \rangle$. Since d divides k, there exists an integer z such that $k = dz$. Then

$$a^k = \left(a^d\right)^z,$$

and so $a^k \in \langle a^d \rangle$ and $\langle a^k \rangle \subseteq \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$ and a^k has order m/d. In particular, a^k generates G if and only if $d = 1$ if and only if $(m, k) = 1$, and so G has exactly $\varphi(m)$ generators. This completes the proof. □

We can now give a group theoretic proof of Theorem 2.8. Let G be a cyclic group of order m. For every divisor d of m, the group G has a unique cyclic subgroup of order d, and this subgroup has exactly $\varphi(d)$ generators. Since every element of G generates a cyclic subgroup, it follows that

$$m = \sum_{d|m} \varphi(d).$$

thank you