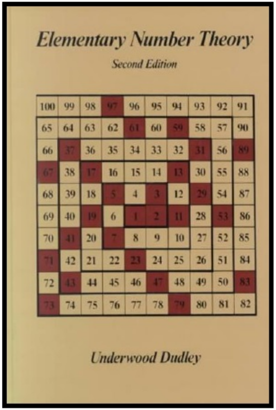
Elementary Number Theory

Section 9. Euler's Theorem and Function—Proofs of Theorems



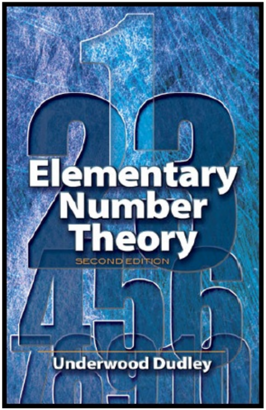


Table of contents

1. Lemma 9.1
2. Theorem 9.1. Euler's Theorem
3. Lemma 9.2
4. Lemma 9.3
5. Corollary 9.A
6. Theorem 9.2
7. Theorem 9.3
8. Theorem 9.4

Lemma 9.1

Lemma 9.1. If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\varphi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues (mod m) of $ar_1, ar_2, ar_3, \ldots, ar_{\varphi(m)}$ are a permutation of $r_1, r_2, r_3, \ldots, r_{\varphi(m)}$.

Proof. There are exactly $\varphi(m)$ numbers in the collection $ar_1, ar_2, \ldots, ar_{\varphi(m)}$. Since there are also $\varphi(m)$ positive integers less than m that are relatively prime to m, namely $r_1, r_2, \ldots, r_{\varphi(m)}$, we just need to show that the least residues (mod m) of $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ are distinct and are relatively prime to m.

Lemma 9.1

Lemma 9.1. If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\varphi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues (mod m) of $ar_1, ar_2, ar_3, \ldots, ar_{\varphi(m)}$ are a permutation of $r_1, r_2, r_3, \ldots, r_{\varphi(m)}$.

Proof. There are exactly $\varphi(m)$ numbers in the collection $ar_1, ar_2, \ldots, ar_{\varphi(m)}$. Since there are also $\varphi(m)$ positive integers less than m that are relatively prime to m, namely $r_1, r_2, \ldots, r_{\varphi(m)}$, we just need to show that the least residues (mod m) of $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ are distinct and are relatively prime to m.

To show that the least residues (mod m) are all different, suppose that some two of them are equal, say $ar_i \equiv ar_j \pmod{m}$ for some $1 \leq i \leq \varphi(m)$ and $1 \leq j \leq \varphi(m)$. Since $(a, m) = 1$ then $ar_i \equiv ar_j \pmod{m}$ implies that $r_i \equiv r_j \pmod{m}$ by Theorem 4.4. Since r_i and r_j are least residues (mod m), we have $r_i = r_j$. We have shown that $ar_i \equiv ar_j \pmod{m}$ implies $r_i \neq r_j$. The contrapositive of this is that $r_i = r_j$ implies $ar_i \not\equiv ar_j$. So the numbers $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ are distinct, as claimed.

Lemma 9.1

Lemma 9.1. If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\varphi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues (mod m) of $ar_1, ar_2, ar_3, \ldots, ar_{\varphi(m)}$ are a permutation of $r_1, r_2, r_3, \ldots, r_{\varphi(m)}$.

Proof. There are exactly $\varphi(m)$ numbers in the collection $ar_1, ar_2, \ldots, ar_{\varphi(m)}$. Since there are also $\varphi(m)$ positive integers less than m that are relatively prime to m, namely $r_1, r_2, \ldots, r_{\varphi(m)}$, we just need to show that the least residues (mod m) of $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ are distinct and are relatively prime to m.

To show that the least residues (mod m) are all different, suppose that some two of them are equal, say $ar_i \equiv ar_j \pmod{m}$ for some $1 \le i \le \varphi(m)$ and $1 \le j \le \varphi(m)$. Since $(a, m) = 1$ then $ar_i \equiv ar_j \pmod{m}$ implies that $r_i \equiv r_j \pmod{m}$ by Theorem 4.4. Since r_i and r_j are least residues (mod m), we have $r_i = r_j$. We have shown that $ar_i \equiv ar_j \pmod{m}$ implies $r_i \neq r_j$. The contrapositive of this is that $r_i = r_j$ implies $ar_i \not\equiv ar_j$. So the numbers $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ are distinct, as claimed.

Lemma 9.1 (continued)

Lemma 9.1. If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\varphi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues (mod m) of $ar_1, ar_2, ar_3, \ldots, ar_{\varphi(m)}$ are a permutation of $r_1, r_2, r_3, \ldots, r_{\varphi(m)}$.

Proof (continued). Now we show that each of $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ is relatively prime to m. ASSUME that p is a prime common divisor of ar_i and m for some i, where $1 \leq i \leq \varphi(m)$. Since p is prime then either $p \mid a$ or $[\mid r_i$ by Euclid's Lemma (Lemma 2.5). So either p is a common divisor of a and m, or p is a common divisor of r_i and m. But $(a, m) = (r_i, m) = 1$ by hypothesis so this is a CONTRADICTION. So there is no common divisor of ar_i and m and hence $(ar_i, m) = 1$ for all $i = 1, 2, \ldots, \varphi(m)$, as claimed. $\square$

Theorem 9.1. Euler's Theorem

Theorem 9.1. Euler's Theorem. Suppose that $m \geq 1$ and $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof. By Lemma 9.1 we have

$$r_1 r_2 \cdots r_{\varphi(m)} \equiv (ar_1)(ar_2) \cdots (ar_{\varphi(m)}) \equiv a^{\varphi(m)}(r_1 r_2 \cdots r_{\varphi(m)}) \pmod{m}.$$

Since each of $r_1, r_2, \ldots, r_{\varphi(m)}$ is relatively prime to m, then the product $r_1 r_2 \cdots r_{\varphi(m)}$ is also relatively prime to m (by, for example, the contrapositive of Corollary 1.1 and induction). So by Theorem 4.4, we can cancel $r_1 r_2 \cdots r_{\varphi(m)}$ in the congruence above to get $1 \equiv a^{\varphi(m)} \pmod{m}$, as claimed. □

Theorem 9.1. Euler's Theorem

Theorem 9.1. Euler's Theorem. Suppose that $m \geq 1$ and $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof. By Lemma 9.1 we have

$$r_1 r_2 \cdots r_{\varphi(m)} \equiv (ar_1)(ar_2) \cdots (ar_{\varphi(m)}) \equiv a^{\varphi(m)}(r_1 r_2 \cdots r_{\varphi(m)}) \pmod{m}.$$

Since each of $r_1, r_2, \ldots, r_{\varphi(m)}$ is relatively prime to m, then the product $r_1 r_2 \cdots r_{\varphi(m)}$ is also relatively prime to m (by, for example, the contrapositive of Corollary 1.1 and induction). So by Theorem 4.4, we can cancel $r_1 r_2 \cdots r_{\varphi(m)}$ in the congruence above to get $1 \equiv a^{\varphi(m)} \pmod{m}$, as claimed. □

Lemma 9.2

Lemma 9.2. For prime p, $\varphi(p^n) = p^{n-1}(p-1)$ for all positive integers n.

Proof. The positive integers less that or equal to p^n which are *not* relatively prime to p^n are exactly the multiples of p: $p, 2p, 3p, \ldots, (p^n - 1)p$. This includes p^{n-1} such numbers. There are p^n positive integers less than or equal to p^n, we we have $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$, as claimed. $\square$

Lemma 9.2

Lemma 9.2. For prime p, $\varphi(p^n) = p^{n-1}(p-1)$ for all positive integers n.

Proof. The positive integers less that or equal to p^n which are *not* relatively prime to p^n are exactly the multiples of p: $p, 2p, 3p, \ldots, (p^n - 1)p$. This includes p^{n-1} such numbers. There are p^n positive integers less than or equal to p^n, we we have $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$, as claimed. $\square$

Lemma 9.3

Lemma 9.3. If $(a, m) = 1$ and $a \equiv b \pmod{m}$, then $(b, m) = 1$.

Proof. Since $a \equiv b \pmod{m}$ then $b = a + km$ for some positive integer k. Then by Lemma 1.3 (with a, b, r of Lemma 1.3 as b, m, a) we have $(b, m) = (a, m) = 1$, as claimed. □

Lemma 9.3

Lemma 9.3. If $(a, m) = 1$ and $a \equiv b \pmod{m}$, then $(b, m) = 1$.

Proof. Since $a \equiv b \pmod{m}$ then $b = a + km$ for some positive integer k. Then by Lemma 1.3 (with a, b, r of Lemma 1.3 as b, m, a) we have $(b, m) = (a, m) = 1$, as claimed. $\square$

Corollary 9.A

Corollary 9.A. If the least residues modulo m of $r_1, r_2, \ldots, r_m$ are a permutation of $0, 1, \ldots, m-1$, then the list $r_1, r_2, \ldots, r_m$ contains exactly $\varphi(m)$ elements relatively prime to m.

Proof. First, the least residue of r_i modulo m is some j where $0 \leq j \leq m-1$; that is $j \equiv r_i \pmod{m}$. If $(j, m) = 1$ then by Lemma 9.3 we have $(r_i, m) = 1$, so that for j relatively prime to m we have r_i relatively prime to m.

Corollary 9.A

Corollary 9.A. If the least residues modulo m of $r_1, r_2, \ldots, r_m$ are a permutation of $0, 1, \ldots, m-1$, then the list $r_1, r_2, \ldots, r_m$ contains exactly $\varphi(m)$ elements relatively prime to m.

Proof. First, the least residue of r_i modulo m is some j where $0 \leq j \leq m-1$; that is $j \equiv r_i \pmod{m}$. If $(j, m) = 1$ then by Lemma 9.3 we have $(r_i, m) = 1$, so that for j relatively prime to m we have r_i relatively prime to m. Conversely, if $(j, m) = d > 1$ then $d \mid j$ and $d \mid m$, so that $d \mid (km + j)$ for every integer k, by Lemma 1.2. Since $j \equiv r_i \pmod{m}$ then $r_i = km + j$ for some integer k and so $d \mid r_i$. That is, if j and m are not relatively prime, then r_i and m are not relatively prime. So r_i is relatively prime to m if and only if j is relatively prime to m. Therefore, since the list $0, 1, \ldots, m-1$ contains exactly $\varphi(m)$ elements relatively prime to m, then the list $r_1, r_2, \ldots, r_m$ contains exactly $\varphi(m)$ elements relatively prime to m, as calimed. □

Corollary 9.A

Corollary 9.A. If the least residues modulo m of $r_1, r_2, \ldots, r_m$ are a permutation of $0, 1, \ldots, m-1$, then the list $r_1, r_2, \ldots, r_m$ contains exactly $\varphi(m)$ elements relatively prime to m.

Proof. First, the least residue of r_i modulo m is some j where $0 \leq j \leq m-1$; that is $j \equiv r_i \pmod{m}$. If $(j, m) = 1$ then by Lemma 9.3 we have $(r_i, m) = 1$, so that for j relatively prime to m we have r_i relatively prime to m. Conversely, if $(j, m) = d > 1$ then $d \mid j$ and $d \mid m$, so that $d \mid (km + j)$ for every integer k, by Lemma 1.2. Since $j \equiv r_i \pmod{m}$ then $r_i = km + j$ for some integer k and so $d \mid r_i$. That is, if j and m are not relatively prime, then r_i and m are not relatively prime. So r_i is relatively prime to m if and only if j is relatively prime to m. Therefore, since the list $0, 1, \ldots, m-1$ contains exactly $\varphi(m)$ elements relatively prime to m, then the list $r_1, r_2, \ldots, r_m$ contains exactly $\varphi(m)$ elements relatively prime to m, as calimed. $\square$

Theorem 9.2

Theorem 9.2. Euler's φ-function is multiplicative.

Proof. Suppose $(m, n) = 1$. Then consider the numbers from 1 to mn written consecutively in columns as:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & mn. \end{array}$$

Suppose $(m, r) = d$ where $d > 1$. Since $d \mid m$ and $d \mid r$ then by Lemma 1.2 $d \mid (km + r)$ for any nonnegative integer k. Notice that the rows in the array are of the form $r \;\; m+r \;\; 2m+r \;\; \cdots \;\; km+r \;\; \cdots \;\; (n-1)m+r$.

Theorem 9.2

Theorem 9.2. Euler's φ-function is multiplicative.

Proof. Suppose $(m, n) = 1$. Then consider the numbers from 1 to mn written consecutively in columns as:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & mn. \end{array}$$

Suppose $(m, r) = d$ where $d > 1$. Since $d \mid m$ and $d \mid r$ then by Lemma 1.2 $d \mid (km + r)$ for any nonnegative integer k. Notice that the rows in the array are of the form $r \;\; m + r \;\; 2m + r \;\; \cdots \;\; km + r \;\; \cdots \;\; (n-1)m + r$. So if $d > 1$ divides m and r, then d divides every entry in row r. Hence, any positive number relatively prime to mn (and less than mn) must appear in the array above in a row for which the number is relatively prime to the *first entry* in that row.

Theorem 9.2

Theorem 9.2. Euler's φ-function is multiplicative.

Proof. Suppose $(m, n) = 1$. Then consider the numbers from 1 to mn written consecutively in columns as:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & mn. \end{array}$$

Suppose $(m, r) = d$ where $d > 1$. Since $d \mid m$ and $d \mid r$ then by Lemma 1.2 $d \mid (km + r)$ for any nonnegative integer k. Notice that the rows in the array are of the form $r \;\; m+r \;\; 2m+r \;\; \cdots \;\; km+r \;\; \cdots \;\; (n-1)m+r$. So if $d > 1$ divides m and r, then d divides every entry in row r. Hence, any positive number relatively prime to mn (and less than mn) must appear in the array above in a row for which the number is relatively prime to the *first entry* in that row.

Theorem 9.2 (continued 1)

Proof (continued). Now the numbers in the rth row of the array are $r \;\; m+r \;\; 2m+r \;\; \cdots \;\; km+r \;\; \cdots \;\; (n-1)m+r$. We first claim that when r and m are relatively prime, these numbers have least residues modulo n of some permutation of $0, 1, 2, \ldots, (n-1)$. To verify this, it is sufficient to show that no two of the numbers in the rth row are congruent modulo n. Suppose $km + r \equiv jm + r \pmod{n}$ with $0 \leq k < n$ and $0 \leq j < n$. Then $km \equiv jm \pmod{n}$, and since $(m, n) = 1$ (by our initial hypothesis in the proof) then we have $k \equiv j \pmod{n}$ by Theorem 4.4. Since both k and j are between 0 and $n-1$, then we must have $k = j$. That is, with $0 \leq k < n$ and $0 \leq j < n$, if $km + r \equiv jm + r \pmod{n}$ then $k = j$. The contrapositive of this result is that (with $0 \leq k < n$ and $0 \leq j < n$) if $k \neq j$ then $km + r \not\equiv jm + r \pmod{n}$. Therefore no two elements of the rth row are congruent modulo n and hence the least residues modulo n of the numbers in the rth row are some permutation of $0, 1, 2, \ldots, (n-1)$, as claimed.

Theorem 9.2 (continued 1)

Proof (continued). Now the numbers in the rth row of the array are $r \;\; m+r \;\; 2m+r \;\; \cdots \;\; km+r \;\; \cdots \;\; (n-1)m+r$. We first claim that when r and m are relatively prime, these numbers have least residues modulo n of some permutation of $0, 1, 2, \ldots, (n-1)$. To verify this, it is sufficient to show that no two of the numbers in the rth row are congruent modulo n. Suppose $km + r \equiv jm + r \pmod{n}$ with $0 \le k < n$ and $0 \le j < n$. Then $km \equiv jm \pmod{n}$, and since $(m, n) = 1$ (by our initial hypothesis in the proof) then we have $k \equiv j \pmod{n}$ by Theorem 4.4. Since both k and j are between 0 and $n - 1$, then we must have $k = j$. That is, with $0 \le k < n$ and $0 \le j < n$, if $km + r \equiv jm + r \pmod{n}$ then $k = j$. The contrapositive of this result is that (with $0 \le k < n$ and $0 \le j < n$) if $k \ne j$ then $km + r \not\equiv jm + r \pmod{n}$. Therefore no two elements of the rth row are congruent modulo n and hence the least residues modulo n of the numbers in the rth row are some permutation of $0, 1, 2, \ldots, (n-1)$, as claimed.

Theorem 9.2 (continued 2)

Proof (continued). Since the least residues modulo n of the numbers in the rth row are some permutation of $0, 1, 2, \ldots, (n-1)$, then by Corollary 9.A we have that the rth row of the array (when r and m are relatively prime) contains exactly $\varphi(n)$ elements relatively prime to n. By Lemma 9.3 (where r and m are relatively prime), every element in the rth row of the array, $r \;\; m+r \;\; 2m+r \;\; \cdots \;\; km+r \;\; \cdots \;\; (n-1)m+r$, is relatively prime to m. Such an rth row contains exactly $\varphi(n)$ elements that are relatively prime to both m and n, and hence are relatively prime to mn (this follows, say, from Euclid's Lemma [Lemma 2.5] which states that if prime p divides ab then either $p \mid a$ or $p \mid b$). We have seen that a positive number relatively prime to mn (and less than mn) appears in the rth row only when r and m are relatively prime (there are $\varphi(m)$ such rows), and each such row contains $\varphi(n)$ entries relatively prime to mn. So the array contains $\varphi(m)\varphi(n)$ elements relatively prime to mn. That is, $\varphi(mn) = \varphi(m)\varphi(n)$ and φ is multiplicative, as claimed. □

Theorem 9.2 (continued 2)

Proof (continued). Since the least residues modulo n of the numbers in the rth row are some permutation of $0, 1, 2, \ldots, (n-1)$, then by Corollary 9.A we have that the rth row of the array (when r and m are relatively prime) contains exactly $\varphi(n)$ elements relatively prime to n. By Lemma 9.3 (where r and m are relatively prime), every element in the rth row of the array, $r \;\; m+r \;\; 2m+r \;\; \cdots \;\; km+r \;\; \cdots \;\; (n-1)m+r$, is relatively prime to m. Such an rth row contains exactly $\varphi(n)$ elements that are relatively prime to both m and n, and hence are relatively prime to mn (this follows, say, from Euclid's Lemma [Lemma 2.5] which states that if prime p divides ab then either $p \mid a$ or $p \mid b$). We have seen that a positive number relatively prime to mn (and less than mn) appears in the rth row only when r and m are relatively prime (there are $\varphi(m)$ such rows), and each such row contains $\varphi(n)$ entries relatively prime to mn. So the array contains $\varphi(m)\varphi(n)$ elements relatively prime to mn. That is, $\varphi(mn) = \varphi(m)\varphi(n)$ and φ is multiplicative, as claimed. $\square$

Theorem 9.3

Theorem 9.3. If n has a prime-power decomposition given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then
$\varphi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1)$.

Proof. Since φ is multiplicative, then Theorem 7.5 implies that

$$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}).$$

By Lemma 9.2, $\varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$ for each $1 \leq i \leq k$, and the claim follows. $\square$

Theorem 9.3

Theorem 9.3. If n has a prime-power decomposition given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then
$\varphi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1)$.

Proof. Since φ is multiplicative, then Theorem 7.5 implies that

$$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}).$$

By Lemma 9.2, $\varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$ for each $1 \leq i \leq k$, and the claim follows. $\square$

Theorem 9.4

Theorem 9.4. If $n \geq 1$, then $\sum_{d \mid n} \varphi(d) = n$.

Proof. Let positive integer n be given. For the set of integers $S = \{1, 2, \ldots, n\}$, define the set C_d (where $1 \leq d \leq n$) to consist of those numbers in S that have greatest common divisor with n or d. That is, for given n we have $m \in C_d$ if and only if $(m, n) = d$. But $(m, n) = d$ if and only if $(m/d, n/d) = 1$ by Theorem 1.1. So $m \in C_d$ if and only if m/d is relatively prime to n/d.

Theorem 9.4

Theorem 9.4. If $n \geq 1$, then $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Proof. Let positive integer n be given. For the set of integers $S = \{1, 2, \ldots, n\}$, define the set C_d (where $1 \leq d \leq n$) to consist of those numbers in S that have greatest common divisor with n or d. That is, for given n we have $m \in C_d$ if and only if $(m, n) = d$. But $(m, n) = d$ if and only if $(m/d, n/d) = 1$ by Theorem 1.1. So $m \in C_d$ if and only if m/d is relatively prime to n/d. The number of positive integers less than or equal to n/d and relatively prime to n/d is, by definition, $\varphi(n/d)$. So the number of elements in C_d is $\varphi(n/d)$. Since each element of $S = \{1, 2, \ldots, n\}$ is in exactly one C_d, then $n = \sum_{d \mid n} \varphi(n/d)$. Now if $d \mid n$, then $n = dc$ for some c where $c \mid n$ (and $c = n/d$). So summing $\varphi(n/d)$ over all $d \mid n$, is equivalent to summing $\varphi(c)$ over all $c \mid n$. That is, $\sum_{d \mid n} \varphi(n/d) = \sum_{c \mid n} \varphi(c)$. So $n = \sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d)$, as claimed. □

Theorem 9.4

Theorem 9.4. If $n \geq 1$, then $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Proof. Let positive integer n be given. For the set of integers $S = \{1, 2, \ldots, n\}$, define the set C_d (where $1 \leq d \leq n$) to consist of those numbers in S that have greatest common divisor with n or d. That is, for given n we have $m \in C_d$ if and only if $(m, n) = d$. But $(m, n) = d$ if and only if $(m/d, n/d) = 1$ by Theorem 1.1. So $m \in C_d$ if and only if m/d is relatively prime to n/d. The number of positive integers less than or equal to n/d and relatively prime to n/d is, by definition, $\varphi(n/d)$. So the number of elements in C_d is $\varphi(n/d)$. Since each element of $S = \{1, 2, \ldots, n\}$ is in exactly one C_d, then $n = \sum_{d \mid n} \varphi(n/d)$. Now if $d \mid n$, then $n = dc$ for some c where $c \mid n$ (and $c = n/d$). So summing $\varphi(n/d)$ over all $d \mid n$, is equivalent to summing $\varphi(c)$ over all $c \mid n$. That is, $\sum_{d \mid n} \varphi(n/d) = \sum_{c \mid n} \varphi(c)$. So $n = \sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d)$, as claimed. $\square$