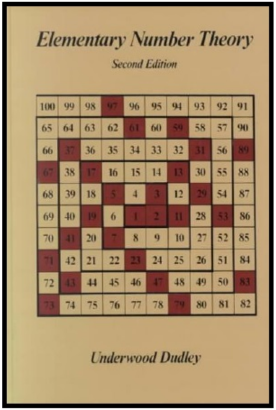
Elementary Number Theory

Section 10. Primitive Roots—Proofs of Theorems



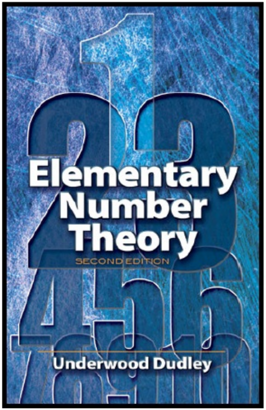


Table of contents

Theorem 10.1

Theorem 10.1. Suppose that $(a, m) = 1$ and a has order t modulo m. Then $a^n \equiv 1 \pmod{m}$ if and only if n is a multiple of t.

Proof. Suppose $n = tq$ for some integer q. Then $a^n \equiv a^{tq} \equiv (a^t)^q \equiv 1^q \equiv 1 \pmod{m}$, since $a^t \equiv 1 \pmod{m}$ by hypothesis.

Theorem 10.1

Theorem 10.1. Suppose that $(a, m) = 1$ and a has order t modulo m. Then $a^n \equiv 1 \pmod{m}$ if and only if n is a multiple of t.

Proof. Suppose $n = tq$ for some integer q. Then $a^n \equiv a^{tq} \equiv (a^t)^q \equiv 1^q \equiv 1 \pmod{m}$, since $a^t \equiv 1 \pmod{m}$ by hypothesis.

Conversely, suppose that $a^n \equiv 1 \pmod{m}$. Since t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, then we must have $n \geq t$. By the Division Algorithm (Theorem 1.2), $n = tq + r$ where $q \geq 1$ and $0 \leq r < t$. Thus

$$1 \equiv a^n \equiv a^{tq+r} \equiv (a^t)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}.$$

But t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, and $q^r \equiv 1 \pmod{m}$ where $0 \leq r < t$, so we must have $r = 0$. Thus, $n = tq$ and n is a multiple of t, as claimed. □

Theorem 10.1

Theorem 10.1. Suppose that $(a, m) = 1$ and a has order t modulo m. Then $a^n \equiv 1 \pmod{m}$ if and only if n is a multiple of t.

Proof. Suppose $n = tq$ for some integer q. Then $a^n \equiv a^{tq} \equiv (a^t)^q \equiv 1^q \equiv 1 \pmod{m}$, since $a^t \equiv 1 \pmod{m}$ by hypothesis.

Conversely, suppose that $a^n \equiv 1 \pmod{m}$. Since t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, then we must have $n \geq t$. By the Division Algorithm (Theorem 1.2), $n = tq + r$ where $q \geq 1$ and $0 \leq r < t$. Thus

$$1 \equiv a^n \equiv a^{tq+r} \equiv (a^t)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}.$$

But t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, and $q^r \equiv 1 \pmod{m}$ where $0 \leq r < t$, so we must have $r = 0$. Thus, $n = tq$ and n is a multiple of t, as claimed. □

Theorem 10.2

Theorem 10.2. If $(a, m) = 1$ and a has order $t \pmod{m}$, then $t \mid \varphi(m)$.

Proof. Since $(a, m) = 1$ by hypothesis, then Euler's Theorem (Theorem 9.1) implies that $a^{\varphi(m)} \equiv 1 \pmod{m}$. By Theorem 10.1, we then have that $\varphi(m)$ is a multiple of t. That is, $t \mid \varphi(m)$ as claimed. □

Theorem 10.2

Theorem 10.2. If $(a, m) = 1$ and a has order $t \pmod{m}$, then $t \mid \varphi(m)$.

Proof. Since $(a, m) = 1$ by hypothesis, then Euler's Theorem (Theorem 9.1) implies that $a^{\varphi(m)} \equiv 1 \pmod{m}$. By Theorem 10.1, we then have that $\varphi(m)$ is a multiple of t. That is, $t \mid \varphi(m)$ as claimed. □

Theorem 10.3

Theorem 10.3. If p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Proof. Since $q \mid a^p - 1$ by hypothesis, then $a^p \equiv 1 \pmod{q}$. So by Theorem 10.1, the order of a modulo q is a divisor of p. Since p is prime, the a has order either 1 or p. If the order of a is 1, then $a^1 \equiv 1 \pmod{q}$, so that $q \mid a - 1$.

Theorem 10.3

Theorem 10.3. If p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Proof. Since $q \mid a^p - 1$ by hypothesis, then $a^p \equiv 1 \pmod{q}$. So by Theorem 10.1, the order of a modulo q is a divisor of p. Since p is prime, the a has order either 1 or p. If the order of a is 1, then $a^1 \equiv 1 \pmod{q}$, so that $q \mid a - 1$. If in stead the order of a is p, then by Theorem 10.2, $p \mid \varphi(q)$. Since $\varphi(q) = q - 1$ by Note 9.A, then $p \mid q - 1$. So $q - 1 = rp$ for some integer r. Since p and q are both odd by hypothesis, then r must be even. Hence, $q = rp + 1 = 2kp + 1$ for some integer k, as claimed. □

Theorem 10.3

Theorem 10.3. If p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Proof. Since $q \mid a^p - 1$ by hypothesis, then $a^p \equiv 1 \pmod{q}$. So by Theorem 10.1, the order of a modulo q is a divisor of p. Since p is prime, the a has order either 1 or p. If the order of a is 1, then $a^1 \equiv 1 \pmod{q}$, so that $q \mid a - 1$. If in stead the order of a is p, then by Theorem 10.2, $p \mid \varphi(q)$. Since $\varphi(q) = q - 1$ by Note 9.A, then $p \mid q - 1$. So $q - 1 = rp$ for some integer r. Since p and q are both odd by hypothesis, then r must be even. Hence, $q = rp + 1 = 2kp + 1$ for some integer k, as claimed. □

Theorem 10.4

Theorem 10.4. If the order of a modulo m is t, then $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{t}$.

Proof. First, suppose $a^r \equiv q^s \pmod{m}$; without loss of generality, suppose $r \geq s$. Then $a^{r-s} \equiv 1 \pmod{m}$, so that by Theorem 10.1 we have $r - s$ is a multiple of t. That is, $r \equiv s \pmod{t}$, as claimed.

Theorem 10.4

Theorem 10.4. If the order of a modulo m is t, then $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{t}$.

Proof. First, suppose $a^r \equiv q^s \pmod{m}$; without loss of generality, suppose $r \geq s$. Then $a^{r-s} \equiv 1 \pmod{m}$, so that by Theorem 10.1 we have $r - s$ is a multiple of t. That is, $r \equiv s \pmod{t}$, as claimed.

Conversely, suppose $r \equiv s \pmod{t}$. Then $r = s + kt$ for some integer k. Since the order of a mod m is t by hypothesis, then $a^t \equiv 1 \pmod{m}$, and

$$a^r \equiv a^{s+kt} \equiv a^s(a^t)^k \equiv a^s(1)^k \equiv a^s \pmod{m},$$

as claimed. □

Theorem 10.4

Theorem 10.4. If the order of a modulo m is t, then $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{t}$.

Proof. First, suppose $a^r \equiv q^s \pmod{m}$; without loss of generality, suppose $r \geq s$. Then $a^{r-s} \equiv 1 \pmod{m}$, so that by Theorem 10.1 we have $r - s$ is a multiple of t. That is, $r \equiv s \pmod{t}$, as claimed.

Conversely, suppose $r \equiv s \pmod{t}$. Then $r = s + kt$ for some integer k. Since the order of a mod m is t by hypothesis, then $a^t \equiv 1 \pmod{m}$, and

$$a^r \equiv a^{s+kt} \equiv a^s(a^t)^k \equiv a^s(1)^k \equiv a^s \pmod{m},$$

as claimed. □

Theorem 10.5

Theorem 10.5. If g is a primitive root of m, then the least residues modulo m of $g, g^2, g^3, \ldots, g^{\varphi(m)}$ are a permutation of the $\varphi(m)$ positive integers less than m and relatively prime to it.

Proof. Since g is a primitive root of m, then $(g, m) = 1$ by the definition of "primitive root." o each power of g is relatively prime to m (this follows by The Unique Factorization Theorem/Fundamental Theorem of Arithmetic, Theorem 2.2; if g and m share no prime factors, then neither does g^n and m where $n > 0$).

Theorem 10.5

Theorem 10.5. If g is a primitive root of m, then the least residues modulo m of $g, g^2, g^3, \ldots, g^{\varphi(m)}$ are a permutation of the $\varphi(m)$ positive integers less than m and relatively prime to it.

Proof. Since g is a primitive root of m, then $(g, m) = 1$ by the definition of "primitive root." o each power of g is relatively prime to m (this follows by The Unique Factorization Theorem/Fundamental Theorem of Arithmetic, Theorem 2.2; if g and m share no prime factors, then neither does g^n and m where $n > 0$). Furthermore, no two powers of g, $g, g^2, \ldots, g^{\varphi(m)}$, have the same least residue, because if $g^j \equiv g^k \pmod{m}$ then by Theorem 10.4 we have $j \equiv k \pmod{\varphi(m)}$ (or that $j = k$ since $1 \leq j, k \leq \varphi(m) \leq m - 1$). That is, if $j \not\equiv k \pmod{\varphi(m)}$, where $1 \leq j, k \leq \varphi(m)$, then $g^k \not\equiv g^k \pmod{m}$. Hence, the powers of g are distinct, as claimed. □

Theorem 10.5

Theorem 10.5. If g is a primitive root of m, then the least residues modulo m of $g, g^2, g^3, \ldots, g^{\varphi(m)}$ are a permutation of the $\varphi(m)$ positive integers less than m and relatively prime to it.

Proof. Since g is a primitive root of m, then $(g, m) = 1$ by the definition of "primitive root." o each power of g is relatively prime to m (this follows by The Unique Factorization Theorem/Fundamental Theorem of Arithmetic, Theorem 2.2; if g and m share no prime factors, then neither does g^n and m where $n > 0$). Furthermore, no two powers of g, $g, g^2, \ldots, g^{\varphi(m)}$, have the same least residue, because if $g^j \equiv g^k \pmod{m}$ then by Theorem 10.4 we have $j \equiv k \pmod{\varphi(m)}$ (or that $j = k$ since $1 \le j, k \le \varphi(m) \le m - 1$). That is, if $j \not\equiv k \pmod{\varphi(m)}$, where $1 \le j, k \le \varphi(m)$, then $g^k \not\equiv g^k \pmod{m}$. Hence, the powers of g are distinct, as claimed. □

Lemma 10.1

Lemma 10.1. Suppose that a has order t modulo m. Then a^k has order t modulo m if and only if $(k, t) = 1$.

Proof. Notice that $(a, m) = 1$ from the definition of "order." First, suppose $(k, t) = 1$. Denote the order of a^k modulo m as s. Since a has order t modulo m by hypothesis, then $1 \equiv (1)^k \equiv (a^t)^k \equiv (a^k)^t \pmod{m}$. By Theorem 10.1, we then have that $s \mid t$. Since s is the order of a^k then $(a^k)^s \equiv a^k s \equiv 1 \pmod{m}$, so by Theorem 10.1 (again), $t \mid ks$. Since $(k, t) = 1$, then $t \mid s$ by Corollary 1.1. But since we also have $s \mid t$, then it must be that $s = t$ so that the order of a^k modulo m is t, as claimed.

Lemma 10.1

Lemma 10.1. Suppose that a has order t modulo m. Then a^k has order t modulo m if and only if $(k, t) = 1$.

Proof. Notice that $(a, m) = 1$ from the definition of "order." First, suppose $(k, t) = 1$. Denote the order of a^k modulo m as s. Since a has order t modulo m by hypothesis, then $1 \equiv (1)^k \equiv (a^t)^k \equiv (a^k)^t \pmod{m}$. By Theorem 10.1, we then have that $s \mid t$. Since s is the order of a^k then $(a^k)^s \equiv a^k s \equiv 1 \pmod{m}$, so by Theorem 10.1 (again), $t \mid ks$. Since $(k, t) = 1$, then $t \mid s$ by Corollary 1.1. But since we also have $s \mid t$, then it must be that $s = t$ so that the order of a^k modulo m is t, as claimed.

Conversely, suppose that a and a^k both have order mod m of t and that $(k, t) = r$. Then $1 \equiv a^t \equiv (a^t)^{k/r} \equiv (a^k)^{t/r} \pmod{m}$. By Theorem 10.1, t/r is a multiple of t, so that we must have $r = (k, t) = 1$, as claimed. □

Lemma 10.1

Lemma 10.1. Suppose that a has order t modulo m. Then a^k has order t modulo m if and only if $(k, t) = 1$.

Proof. Notice that $(a, m) = 1$ from the definition of "order." First, suppose $(k, t) = 1$. Denote the order of a^k modulo m as s. Since a has order t modulo m by hypothesis, then $1 \equiv (1)^k \equiv (a^t)^k \equiv (a^k)^t \pmod{m}$. By Theorem 10.1, we then have that $s \mid t$. Since s is the order of a^k then $(a^k)^s \equiv a^k s \equiv 1 \pmod{m}$, so by Theorem 10.1 (again), $t \mid ks$. Since $(k, t) = 1$, then $t \mid s$ by Corollary 1.1. But since we also have $s \mid t$, then it must be that $s = t$ so that the order of a^k modulo m is t, as claimed.

Conversely, suppose that a and a^k both have order mod m of t and that $(k, t) = r$. Then $1 \equiv a^t \equiv (a^t)^{k/r} \equiv (a^k)^{t/r} \pmod{m}$. By Theorem 10.1, t/r is a multiple of t, so that we must have $r = (k, t) = 1$, as claimed. $\square$

Corollary 10.B

Corollary 10.B. Suppose that g is a primitive root of prime p. Then the least residue of g^k is a primitive root of p if and only if $(k, p-1) = 1$.

Proof. Since g is a primitive root of p, then the order or g is $\varphi(p)$, and $\varphi(p) = p - 1$ by Note 9.A. That is, g is of order $p-1$. Set $t = p-1$. By Lemma 10.1, g^k has order $t = p - 1 = \varphi(p)$ modulo p (and so g^k is also a primitive root of p) if and only if $(k, t) = (k, p-1) = 1$. That is, g^k is a primitive root of p if and only if $(k, p-1) = 1$, as claimed. □

Corollary 10.B

Corollary 10.B. Suppose that g is a primitive root of prime p. Then the least residue of g^k is a primitive root of p if and only if $(k, p-1) = 1$.

Proof. Since g is a primitive root of p, then the order or g is $\varphi(p)$, and $\varphi(p) = p - 1$ by Note 9.A. That is, g is of order $p - 1$. Set $t = p - 1$. By Lemma 10.1, g^k has order $t = p - 1 = \varphi(p)$ modulo p (and so g^k is also a primitive root of p) if and only if $(k, t) = (k, p-1) = 1$. That is, g^k is a primitive root of p if and only if $(k, p-1) = 1$, as claimed. $\square$

Lemma 10.2

Lemma 10.2. If f is a polynomial of degree n, then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x a_0$ have degree n where $a_n \not\equiv 0 \pmod{p}$. We prove the claim by induction. For the base case, consider the equation for $n = 1$: $a_1 x + a_0 \equiv 0 \pmod{p}$. Since $a_n \not\equiv 0 \pmod{p}$, then because p is prime we have $(a_1, p) = 1$, by Theorem 5.1 there is at most one solution.

Lemma 10.2

Lemma 10.2. If f is a polynomial of degree n, then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x a_0$ have degree n where $a_n \not\equiv 0 \pmod{p}$. We prove the claim by induction. For the base case, consider the equation for $n = 1$: $a_1 x + a_0 \equiv 0 \pmod{p}$. Since $a_n \not\equiv 0 \pmod{p}$, then because p is prime we have $(a_1, p) = 1$, by Theorem 5.1 there is at most one solution.

For the induction hypothesis, suppose that the lemma is true for polynomials of degree $n - 1$. Now consider f as an n degree polynomial. If $f(x) \equiv 0 \pmod{p}$ has not solution, then the claim holds. So we can suppose that $f(x) \equiv 0 \pmod{p}$ has a solution $x = r$. That is, $f(r) \equiv 0 \pmod{p}$, and r is a least residue modulo p. Next, $x - r$ is a factor of $x^t - r^t$ for $t = 0, 1, \ldots, n$ because $x^t - r^t = (x - r)(x^{t-1} + x^{t-2}r + x^{t-3}r^2 + \cdots x r^{t-2} + r^{t-1})$, as can be shown by simplifying the right-hand side.

Lemma 10.2

Lemma 10.2. If f is a polynomial of degree n, then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x a_0$ have degree n where $a_n \not\equiv 0 \pmod{p}$. We prove the claim by induction. For the base case, consider the equation for $n = 1$: $a_1 x + a_0 \equiv 0 \pmod{p}$. Since $a_n \not\equiv 0 \pmod{p}$, then because p is prime we have $(a_1, p) = 1$, by Theorem 5.1 there is at most one solution.

For the induction hypothesis, suppose that the lemma is true for polynomials of degree $n - 1$. Now consider f as an n degree polynomial. If $f(x) \equiv 0 \pmod{p}$ has not solution, then the claim holds. So we can suppose that $f(x) \equiv 0 \pmod{p}$ has a solution $x = r$. That is, $f(r) \equiv 0 \pmod{p}$, and r is a least residue modulo p. Next, $x - r$ is a factor of $x^t - r^t$ for $t = 0, 1, \ldots, n$ because $x^t - r^t = (x - r)(x^{t-1} + x^{t-2}r + x^{t-3}r^2 + \cdots xr^{t-2} + r^{t-1})$, as can be shown by simplifying the right-hand side.

Lemma 10.2 (continued)

Lemma 10.2. If f is a polynomial of degree n, then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Proof (continued). So we have

$$f(x) \equiv f(x) - 0 \equiv f(x) - f(r)$$

$$\equiv a_n(x^n - r^n) + a_{n-1}(x^{n-1} - r^{n-1}) + \cdots + a_2(x^2 - r^2) + a_1(x - r)$$

$$\equiv (x - r)g(x) \pmod{p}, \qquad (*)$$

where g is a polynomial of degree $n - 1$. Suppose that s is also a solution to $f(x) \equiv 0 \pmod{p}$. The from $(*)$ $f(s) \equiv (s - r)g(s) \equiv 0 \pmod{p}$. Since p is prime, then by Euclid's Lemma (Lemma 2.5) either $s \equiv r \pmod{p}$ or $g(s) \equiv 0 \pmod{p}$. Now g is degree $n - 1$, so by the induction hypothesis, $g(s) \equiv 0 \pmod{p}$ has at most $n - 1$ solutions. Also $s \equiv r \pmod{p}$ has exactly one solution, so we have for degree n polynomial f that the equation $f(x) \equiv 0 \pmod{p}$ has at most n solutions, as needed. So by induction the result holds for all degrees $n \in \mathbb{N}$, as claimed. □

Lemma 10.2 (continued)

Lemma 10.2. If f is a polynomial of degree n, then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Proof (continued). So we have

$$f(x) \equiv f(x) - 0 \equiv f(x) - f(r)$$

$$\equiv a_n(x^n - r^n) + a_{n-1}(x^{n-1} - r^{n-1}) + \cdots + a_2(x^2 - r^2) + a_1(x - r)$$

$$\equiv (x - r)g(x) \pmod{p}, \qquad (*)$$

where g is a polynomial of degree $n-1$. Suppose that s is also a solution to $f(x) \equiv 0 \pmod{p}$. The from $(*)$ $f(s) \equiv (s - r)g(s) \equiv 0 \pmod{p}$. Since p is prime, then by Euclid's Lemma (Lemma 2.5) either $s \equiv r \pmod{p}$ or $g(s) \equiv 0 \pmod{p}$. Now g is degree $n-1$, so by the induction hypothesis, $g(s) \equiv 0 \pmod{p}$ has at most $n-1$ solutions. Also $s \equiv r \pmod{p}$ has exactly one solution, so we have for degree n polynomial f that the equation $f(x) \equiv 0 \pmod{p}$ has at most n solutions, as needed. So by induction the result holds for all degrees $n \in \mathbb{N}$, as claimed. $\square$

Lemma 10.3

Lemma 10.3. If $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Proof. By Fermat's (Little) Theorem (Theorem 6.1), the congruence $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions, namely $1, 2, \ldots, p-1$. Moreover,

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1) = (x^d - 1)h(x).$$

Lemma 10.3

Lemma 10.3. If $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Proof. By Fermat's (Little) Theorem (Theorem 6.1), the congruence $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions, namely $1, 2, \ldots, p-1$. Moreover,

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1) = (x^d - 1)h(x).$$

By Lemma 10.2, $h(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ solutions. Hence $x^d \equiv 1 \pmod{p}$ has at least $(p-1)-(p-1-d) = d$ solutions. By Lemma 10.2 again, but applied to $x^d \equiv 1 \pmod{p}$, we see that this equation has at most d solutions, and hence has exactly d solutions, as claimed. $\square$

Lemma 10.3

Lemma 10.3. If $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Proof. By Fermat's (Little) Theorem (Theorem 6.1), the congruence $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions, namely $1, 2, \ldots, p-1$. Moreover,

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1) = (x^d - 1)h(x).$$

By Lemma 10.2, $h(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ solutions. Hence $x^d \equiv 1 \pmod{p}$ has at least $(p-1) - (p-1-d) = d$ solutions. By Lemma 10.2 again, but applied to $x^d \equiv 1 \pmod{p}$, we see that this equation has at most d solutions, and hence has exactly d solutions, as claimed. $\square$

Theorem 10.6

Theorem 10.6. Every prime p has $\varphi(p-1)$ primitive roots.

Proof. By Theorem 10.2, we know that each of the integers $1, 2, \ldots, p-1$ has an order that is a divisor of $p-1$. For each divisor t of $p-1$, let $\psi(t)$ denote the number of these integers that have order t. Notice that this gives $\psi(p-1)$ as the number of these integers of order $p-1$, and hence the number of primitive roots of p. Then we have $\sum_{t \mid p-1} \psi(t) = p-1$. By Theorem 9.4, we have $\sum_{t \mid p-1} \psi(t) = p-1 = \sum_{t \mid p-1} \varphi(t)$.

Theorem 10.6

Theorem 10.6. Every prime p has $\varphi(p-1)$ primitive roots.

Proof. By Theorem 10.2, we know that each of the integers $1, 2, \ldots, p-1$ has an order that is a divisor of $p-1$. For each divisor t of $p-1$, let $\psi(t)$ denote the number of these integers that have order t. Notice that this gives $\psi(p-1)$ as the number of these integers of order $p-1$, and hence the number of primitive roots of p. Then we have $\sum_{t \mid p-1} \psi(t) = p-1$. By Theorem 9.4, we have $\sum_{t \mid p-1} \psi(t) = p-1 = \sum_{t \mid p-1} \varphi(t)$. If we can show that $\psi(t) \leq \varphi(t)$ for each t, then the equality of the sums will imply equality of $\psi(t)$ and $\varphi(t)$ for each t; in particular, we will have $\psi(p-1) = \varphi(p-1)$ so that the number of primitive roots will be $\varphi(p-1)$ as claimed.

Theorem 10.6

Theorem 10.6. Every prime p has $\varphi(p-1)$ primitive roots.

Proof. By Theorem 10.2, we know that each of the integers $1, 2, \ldots, p-1$ has an order that is a divisor of $p-1$. For each divisor t of $p-1$, let $\psi(t)$ denote the number of these integers that have order t. Notice that this gives $\psi(p-1)$ as the number of these integers of order $p-1$, and hence the number of primitive roots of p. Then we have $\sum_{t \mid p-1} \psi(t) = p-1$. By Theorem 9.4, we have $\sum_{t \mid p-1} \psi(t) = p-1 = \sum_{t \mid p-1} \varphi(t)$. If we can show that $\psi(t) \leq \varphi(t)$ for each t, then the equality of the sums will imply equality of $\psi(t)$ and $\varphi(t)$ for each t; in particular, we will have $\psi(p-1) = \varphi(p-1)$ so that the number of primitive roots will be $\varphi(p-1)$ as claimed.

Theorem 10.6 (continued)

Theorem 10.6. Every prime p has $\varphi(p-1)$ primitive roots.

Proof (continued). Fix some t. If $\psi(t) = 0$ then $\psi(t) \leq \varphi(t)$ and out claim is demonstrated. If $\psi(t) \neq t$, then there is some integer in $\{1, 2, \ldots, p-1\}$ with order t; denote it as a. The congruence $x^t \equiv 1 \pmod{p}$ has exactly t solutions by Lemma 10.3. Also, for $x \in \{a, a^2, a^3, \ldots, a^t\}$ we have $x^t \equiv 1 \pmod{p}$. By Theorem 10.4, no two of $a, a^2, a^3, \ldots, a^t$ have the same least residue (mod p), so (the least residues of) these give all solutions of $x^t \equiv 1 \pmod{p}$ (and hence the list includes all elements of order t, and maybe some other elements). By Lemma 10.1, the numbers in $\{a, a^2, a^3, \ldots, a^t\}$ that are order t mod p (of which there are, by definition, $\psi(t)$ such numbers) are those powers a^k with $(k, t) = 1$. By the definition of Euler's function, the number of such k is $\varphi(t)$. Therefore, $\psi(t) = \varphi(t)$ for all $t \mid p-1$, and the claim now follows as explained above. □

Theorem 10.6 (continued)

Theorem 10.6. Every prime p has $\varphi(p-1)$ primitive roots.

Proof (continued). Fix some t. If $\psi(t) = 0$ then $\psi(t) \le \varphi(t)$ and out claim is demonstrated. If $\psi(t) \ne t$, then there is some integer in $\{1, 2, \ldots, p-1\}$ with order t; denote it as a. The congruence $x^t \equiv 1 \pmod{p}$ has exactly t solutions by Lemma 10.3. Also, for $x \in \{a, a^2, a^3, \ldots, a^t\}$ we have $x^t \equiv 1 \pmod{p}$. By Theorem 10.4, no two of $a, a^2, a^3, \ldots, a^t$ have the same least residue (mod p), so (the least residues of) these give all solutions of $x^t \equiv 1 \pmod{p}$ (and hence the list includes all elements of order t, and maybe some other elements). By Lemma 10.1, the numbers in $\{a, a^2, a^3, \ldots, a^t\}$ that are order t mod p (of which there are, by definition, $\psi(t)$ such numbers) are those powers a^k with $(k, t) = 1$. By the definition of Euler's function, the number of such k is $\varphi(t)$. Therefore, $\psi(t) = \varphi(t)$ for all $t \mid p-1$, and the claim now follows as explained above. $\square$

Theorem 10.B

Theorem 10.B. If p is an odd prime then $(p-1)! \equiv -1 \pmod{p}$.

Proof. By Theorem 10.6, there is some primitive root g of prime p. By Theorem 10.5, the least residues mod p of $g, g^2, g^3, \ldots, g^{p-1}$ (notice $\varphi(p) = p - 1$) are a permutation of $1, 2, \ldots, p-1$. Multiplying, we have

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv g \cdot g^2 \cdot g^3 \cdot \cdots \cdot g^{p-1}$$

or, since $\sum_{i=1}^{p-1} = p(p-1)/2$,

$$(p-1)! \equiv g^{p(p-1)/2} \equiv (g^p)^{p-1} \pmod{p}.$$

Theorem 10.B

Theorem 10.B. If p is an odd prime then $(p-1)! \equiv -1 \pmod{p}$.

Proof. By Theorem 10.6, there is some primitive root g of prime p. By Theorem 10.5, the least residues mod p of $g, g^2, g^3, \ldots, g^{p-1}$ (notice $\varphi(p) = p-1$) are a permutation of $1, 2, \ldots, p-1$. Multiplying, we have

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv g \cdot g^2 \cdot g^3 \cdot \cdots \cdot g^{p-1}$$

or, since $\sum_{i=1}^{p-1} = p(p-1)/2$,

$$(p-1)! \equiv g^{p(p-1)/2} \equiv (g^p)^{p-1} \pmod{p}.$$

Theorem 10.B (continued)

Theorem 10.B. If p is an odd prime then $(p-1)! \equiv -1 \pmod{p}$.

Proof (continued). ...

$$(p-1)! \equiv g^{p(p-1)/2} \equiv (g^p)^{p-1} \pmod{p}.$$

But $g^{(p-1)/2}$ satisfies $x^2 \equiv 1 \pmod{p}$ (since $(g^{(p-1)/2})^2 \equiv g^{p-1} \equiv g^{\varphi(p)} \equiv 1 \pmod{p}$ by Euler's Theorem, Theorem 9.1), so $g^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$ (notice that these valid values for x in $x^2 \equiv 1 \pmod{p}$ and by Lemma 10.2 there are at most 2 such values of x). But we cannot have $g^{(p-1)/2} \equiv 1 \pmod{p}$, since this would mean that the order of g is at most $(p-1)/2$, and we hypothesized that g is a primitive root and so is order $\varphi(p) = p-1$. Therefore, $g^{(p-1)/2} \equiv -1 \pmod{p}$, and hence $(p-1)! \equiv -1 \pmod{p}$, as claimed. $\square$

Theorem 10.B (continued)

Theorem 10.B. If p is an odd prime then $(p-1)! \equiv -1 \pmod{p}$.

Proof (continued). ...

$$(p-1)! \equiv g^{p(p-1)/2} \equiv (g^p)^{p-1} \pmod{p}.$$

But $g^{(p-1)/2}$ satisfies $x^2 \equiv 1 \pmod{p}$ (since $(g^{(p-1)/2})^2 \equiv g^{p-1} \equiv g^{\varphi(p)} \equiv 1 \pmod{p}$ by Euler's Theorem, Theorem 9.1), so $g^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$ (notice that these valid values for x in $x^2 \equiv 1 \pmod{p}$ and by Lemma 10.2 there are at most 2 such values of x). But we cannot have $g^{(p-1)/2} \equiv 1 \pmod{p}$, since this would mean that the order of g is at most $(p-1)/2$, and we hypothesized that g is a primitive root and so is order $\varphi(p) = p-1$. Therefore, $g^{(p-1)/2} \equiv -1 \pmod{p}$, and hence $(p-1)! \equiv -1 \pmod{p}$, as claimed. $\square$