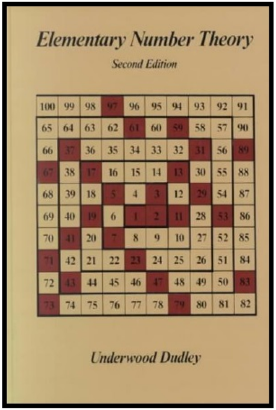
Elementary Number Theory

Section 6. Fermat's and Wilson's Theorems—Proofs of Theorems



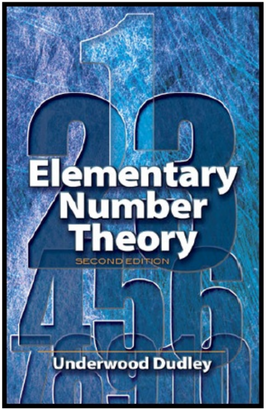


Table of contents

Lemma 6.1

Lemma 6.1. If the greatest common divisor $(a, m) = 1$, then the least residues of

(1) $a, 2a, 3a, \ldots, (m-1)a \pmod{m}$ are (in some order) (2) $1, 2, 3, \ldots, m-1$.

In other words, if $(a, m) = 1$, then each integer is congruent $\pmod{m}$ to exactly one of $a, 2a, 3a, \ldots, (m-1)a$.

Proof. Since m does not divide any of $1, 2, 3, \ldots, (m-1)$ and $(a, m) = 1$ then m does not divide any of $a, 2a, 3a, \ldots, (m-1)a$ by the contrapositive of Corollary 1.1. That is, none of $a, 2a, 3a, \ldots (m-1)a$ is $0 \pmod{m}$. So each of the numbers in (1) is congruent to a number in (2). ASSUME two different numbers of (1) are congruent modulo m, say $ra \equiv rs \pmod{m}$ for $r, s \in \{1, 2, \ldots, m-1\}$ and $r \neq s$.

Lemma 6.1

Lemma 6.1. If the greatest common divisor $(a, m) = 1$, then the least residues of

(1) $a, 2a, 3a, \ldots, (m-1)a$ (mod m) are (in some order) (2) $1, 2, 3, \ldots, m-1$.

In other words, if $(a, m) = 1$, then each integer is congruent (mod m) to exactly one of $a, 2a, 3a, \ldots, (m-1)a$.

Proof. Since m does not divide any of $1, 2, 3, \ldots, (m-1)$ and $(a, m) = 1$ then m does not divide any of $a, 2a, 3a, \ldots, (m-1)a$ by the contrapositive of Corollary 1.1. That is, none of $a, 2a, 3a, \ldots (m-1)a$ is 0 (mod m). So each of the numbers in (1) is congruent to a number in (2). ASSUME two different numbers of (1) are congruent modulo m, say $ra \equiv rs \pmod{m}$ for $r, s \in \{1, 2, \ldots, m-1\}$ and $r \neq s$.

Lemma 6.1 (continued)

Lemma 6.1. If the greatest common divisor $(a, m) = 1$, then the least residues of

(1) $a, 2a, 3a, \ldots, (m-1)a$ (mod m) are (in some order) (2) $1, 2, 3, \ldots, m-1$.

In other words, if $(a, m) = 1$, then each integer is congruent (mod m) to exactly one of $a, 2a, 3, \ldots, (m-1)a$.

Proof (continued). Since $(a, n) = 1$ then by Theorem 4.4 we have $r \equiv s$ (mod m). But r and s are both least residues modulo m and so are equal by Note 5.A. But $r = s$ is a CONTRADICTION and so the assumption that two different numbers of (1) are congruent modulo m is false. Hence no two of the numbers of (1) are congruent modulo m and so each has a different least residue modulo m. Since there are $m-1$ numbers in (1) and $m-1$ least residues in (2), then the least residences of the numbers in (1) must be precisely the numbers in (2), as claimed. □

Lemma 6.1 (continued)

Lemma 6.1. If the greatest common divisor $(a, m) = 1$, then the least residues of

(1) $a, 2a, 3a, \ldots, (m-1)a \pmod{m}$ are (in some order) (2) $1, 2, 3, \ldots, m-1$.

In other words, if $(a, m) = 1$, then each integer is congruent (mod m) to exactly one of $a, 2a, 3, \ldots, (m-1)a$.

Proof (continued). Since $(a, n) = 1$ then by Theorem 4.4 we have $r \equiv s \pmod{m}$. But r and s are both least residues modulo m and so are equal by Note 5.A. But $r = s$ is a CONTRADICTION and so the assumption that two different numbers of (1) are congruent modulo m is false. Hence no two of the numbers of (1) are congruent modulo m and so each has a different least residue modulo m. Since there are $m - 1$ numbers in (1) and $m - 1$ least residues in (2), then the least residences of the numbers in (1) must be precisely the numbers in (2), as claimed. □

Theorem 6.1. Fermat's Theorem

Theorem 6.1. Fermat's Theorem. If p is prime and the greatest common divisor $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Given any prime p, Lemma 6.1 says that is $(a, p) = 1$, then the least residues of $a, 2a, 3a, \ldots, (m-1)a$ modulo p are some permutation of $1, 2, 3, \ldots, p-1$. So the products are congruent

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdots 3 \cdots (p-1) \pmod{p},$$

or $a^{-1}(p-1)! \equiv (p-1)! \pmod{p}$. Now p and $(p-1)!$ are relatively prime (this is where the primeness of p is used), so by Theorem 4.4 we have $a^{p-1} \equiv 1 \pmod{p}$, as claimed. □

Theorem 6.1. Fermat's Theorem

Theorem 6.1. Fermat's Theorem. If p is prime and the greatest common divisor $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Given any prime p, Lemma 6.1 says that is $(a, p) = 1$, then the least residues of $a, 2a, 3a, \ldots, (m-1)a$ modulo p are some permutation of $1, 2, 3, \ldots, p-1$. So the products are congruent

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdots 3 \cdots (p-1) \pmod{p},$$

or $a^{-1}(p-1)! \equiv (p-1)! \pmod{p}$. Now p and $(p-1)!$ are relatively prime (this is where the primeness of p is used), so by Theorem 4.4 we have $a^{p-1} \equiv 1 \pmod{p}$, as claimed. □

Lemma 6.2

Lemma 6.2. The congruence $x^2 \equiv 1 \pmod{p}$, where p is an odd prime, has two solutions: 1 and $p-1$.

Proof. Let r be a solution of $x^2 \equiv 1 \pmod{p}$. Then we have $r^2 - 1 = (r+1)(r-1) \equiv 0 \pmod{p}$. That is, $p \mid (r+1)(r-1)$. Since p is prime, by Euclid's Lemma (Lemma 2.5), either $p \mid r+1$ or $p \mid r-1$. That is, either $r+1 \equiv 0 \pmod{p}$ or $r-1 \equiv 0 \pmod{p}$. Hence either $r \equiv p-1 \pmod{p}$ or $r \equiv 1 \pmod{p}$, respectively. Since r is a least residue then either $r = 1$ or $r = p-1$ (both of which are clearly solutions), as claimed. □

Lemma 6.2

Lemma 6.2. The congruence $x^2 \equiv 1 \pmod{p}$, where p is an odd prime, has two solutions: 1 and $p-1$.

Proof. Let r be a solution of $x^2 \equiv 1 \pmod{p}$. Then we have $r^2 - 1 = (r+1)(r-1) \equiv 0 \pmod{p}$. That is, $p \mid (r+1)(r-1)$. Since p is prime, by Euclid's Lemma (Lemma 2.5), either $p \mid r+1$ or $p \mid r-1$. That is, either $r+1 \equiv 0 \pmod{p}$ or $r-1 \equiv 0 \pmod{p}$. Hence either $r \equiv p-1 \pmod{p}$ or $r \equiv 1 \pmod{p}$, respectively. Since r is a least residue then either $r = 1$ or $r = p-1$ (both of which are clearly solutions), as claimed. □

Lemma 6.3

Lemma 6.3. Let p be an odd prime and let a' by the solution of $ax \equiv 1 \pmod{p}$ where $a \in \{1, 2, \ldots, p-1\}$. Then $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$. Furthermore, $a \equiv a' \pmod{p}$ if and only if $a = 1$ or $a = p - 1$.

Proof. Suppose that $a' \equiv b' \pmod{p}$. Then

$$\begin{aligned} b &\equiv aa'b (\bmod p) \text{ since } aa' \equiv 1 \pmod{p} \\ &\equiv ab'b \pmod{p} \text{ since } a' \equiv b' \pmod{p} \\ &\equiv a \pmod{p} \text{ since } b'b \equiv 1 \pmod{p}, \end{aligned}$$

as claimed.

Lemma 6.3

Lemma 6.3. Let p be an odd prime and let a' by the solution of $ax \equiv 1 \pmod{p}$ where $a \in \{1, 2, \ldots, p-1\}$. Then $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$. Furthermore, $a \equiv a' \pmod{p}$ if and only if $a = 1$ or $a = p - 1$.

Proof. Suppose that $a' \equiv b' \pmod{p}$. Then

$$\begin{aligned} b &\equiv aa'b(\bmod p) \text{ since } aa' \equiv 1 \pmod{p} \\ &\equiv ab'b \pmod{p} \text{ since } a' \equiv b' \pmod{p} \\ &\equiv a \pmod{p} \text{ since } b'b \equiv 1 \pmod{p}, \end{aligned}$$

as claimed.

Lemma 6.3 (continued)

Lemma 6.3. Let p be an odd prime and let a' by the solution of $ax \equiv 1 \pmod{p}$ where $a \in \{1, 2, \ldots, p-1\}$. Then $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$. Furthermore, $a \equiv a' \pmod{p}$ if and only if $a = 1$ or $a = p - 1$.

Proof (continued). Next, suppose that $a \equiv b \pmod{p}$. Then

$$\begin{aligned} b' &\equiv b'aa' (\bmod\ p) \text{ since } aa' \equiv 1 \pmod{p} \\ &\equiv b'ba' \pmod{p} \text{ since } a \equiv b \pmod{p} \\ &\equiv a' \pmod{p} \text{ since } b'b \equiv 1 \pmod{p}, \end{aligned}$$

as claimed.

Now for the furthermore part, if either $a = 1$ or $a = p - 1$, then either $1 \cdot 1 \equiv 1 \pmod{p}$ or $(p-1)(p-1) \equiv 1 \pmod{p}$ as needed. Finally, if $a \equiv a' \pmod{p}$, then $1 \equiv aa'a^2 \pmod{p}$, and from Lemma 6.2 this holds if and only if $a = 1$ or $a = p - 1$, as claimed. □

Lemma 6.3 (continued)

Lemma 6.3. Let p be an odd prime and let a' by the solution of $ax \equiv 1 \pmod{p}$ where $a \in \{1, 2, \ldots, p-1\}$. Then $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$. Furthermore, $a \equiv a' \pmod{p}$ if and only if $a = 1$ or $a = p - 1$.

Proof (continued). Next, suppose that $a \equiv b \pmod{p}$. Then

$$\begin{aligned} b' &\equiv b'aa' (\bmod\ p) \text{ since } aa' \equiv 1 \pmod{p} \\ &\equiv b'ba' \pmod{p} \text{ since } a \equiv b \pmod{p} \\ &\equiv a' \pmod{p} \text{ since } b'b \equiv 1 \pmod{p}, \end{aligned}$$

as claimed.

Now for the furthermore part, if either $a = 1$ or $a = p - 1$, then either $1 \cdot 1 \equiv 1 \pmod{p}$ or $(p-1)(p-1) \equiv 1 \pmod{p}$ as needed. Finally, if $a \equiv a' \pmod{p}$, then $1 \equiv aa'a^2 \pmod{p}$, and from Lemma 6.2 this holds if and only if $a = 1$ or $a = p - 1$, as claimed. □

Theorem 6.2 Wilson's Theorem

Theorem 6.2. Wilson's Theorem. Positive integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Proof. By Note 6.A, the numbers $2, 3, \ldots, p-2$ can be separated into $(p-3)/2$ pairs such that each pair consists of an integer a and its associated multiplicative inverse a'. The product of the two integers in each pair is congruent to $1 \pmod{p}$, so the product satisfies $2 \cdot 3 \cdots (p-3) \cdot (p-2) \equiv 1 \pmod{p}$. Hence

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-3) \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p},$$

as claimed.

Theorem 6.2 Wilson's Theorem

Theorem 6.2. Wilson's Theorem. Positive integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Proof. By Note 6.A, the numbers $2, 3, \ldots, p-2$ can be separated into $(p-3)/2$ pairs such that each pair consists of an integer a and its associated multiplicative inverse a'. The product of the two integers in each pair is congruent to $1 \pmod{p}$, so the product satisfies $2 \cdot 3 \cdots (p-3) \cdot (p-2) \equiv 1 \pmod{p}$. Hence

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-3) \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p},$$

as claimed.

Theorem 6.2 Wilson's Theorem (continued)

Theorem 6.2. Wilson's Theorem. Positive integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Proof (continued). For the converse, suppose $(n-1)! \equiv -1 \pmod{n}$. ASSUME n is not prime and that $n = ab$ for integers a and b with $b \neq n$. Since $(n-1)! \equiv -1 \pmod{n}$, then $n \mid (n-1)! + 1$, and since $a \mid n$ then $a \mid (n-1)! + 1$. Since $a \neq n$ then $0 < a \leq n - 1$ and so a must be one of the factors of $(n-1)!$. But then $a \mid (n-1)!$. But the only way we can have $a \mid (n-1)! + 1$ and $a \mid (n-1)!$, is for $a = 1$ (by Lemma 1.2) which implies $b = n$, a CONTRADICTION. This contradiction shows that the assumption that n is not prime is false, and hence n is prime as claimed. □