Introduction to Modern Algebra

Part IV. Rings and Fields

IV.20. Fermat's and Euler's Theorem

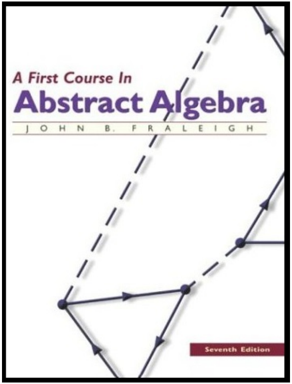

Table of contents

Theorem 20.1. Little Theorem of Fermat

Theorem 20.1. If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$. That is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Proof. By Corollary, $1, 2, 3, \ldots, p-1$ forms a group of order $p-1$ under multiplication modulo p. Since the order of any element in a group divides the order of the group (Theorem 10.12), for $b \neq 0$ and $b \in \mathbb{Z}_p$, we have $b^{p-1} = 1$ in $\mathbb{Z}_p$, or $b^{p-1} \equiv 1 \pmod{p}$.

Theorem 20.1. Little Theorem of Fermat

Theorem 20.1. If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$. That is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Proof. By Corollary, $1, 2, 3, \ldots, p-1$ forms a group of order $p-1$ under multiplication modulo p. Since the order of any element in a group divides the order of the group (Theorem 10.12), for $b \neq 0$ and $b \in \mathbb{Z}_p$, we have $b^{p-1} = 1$ in $\mathbb{Z}_p$, or $b^{p-1} \equiv 1 \pmod{p}$. Now $\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ that both as additive and multiplicative groups (recall that the elements of $\mathbb{Z}/p\mathbb{Z}$ are the cosets of the form $a + p\mathbb{Z}$). So for $a \in \mathbb{Z}$, $a \in 0 + p\mathbb{Z}$, we have $a^{p-1} \in 1 + p\mathbb{Z}$. That is, $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem 20.1. Little Theorem of Fermat

Theorem 20.1. If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$. That is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Proof. By Corollary, $1, 2, 3, \ldots, p-1$ forms a group of order $p-1$ under multiplication modulo p. Since the order of any element in a group divides the order of the group (Theorem 10.12), for $b \neq 0$ and $b \in \mathbb{Z}_p$, we have $b^{p-1} = 1$ in $\mathbb{Z}_p$, or $b^{p-1} \equiv 1 \pmod{p}$. Now $\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ that both as additive and multiplicative groups (recall that the elements of $\mathbb{Z}/p\mathbb{Z}$ are the cosets of the form $a + p\mathbb{Z}$). So for $a \in \mathbb{Z}$, $a \in 0 + p\mathbb{Z}$, we have $a^{p-1} \in 1 + p\mathbb{Z}$. That is, $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem 20.6.

Theorem. 20.6. The set G_n of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisions forms a group under multiplication modulo n.

Proof. First, we show G_n is closed under multiplication. Let $a, b \in G_n$. Suppose $ab \notin G_n$. Then there is some $c \neq 0$ in $\mathbb{Z}_n$ such that $(ab)\,c = 0$ since we have assumed ab is not a division of 0. Now $(ab)\,c = 0$ implies that $a\,(bc) = 0$. Since $b \in G_n$ and $c \neq 0$, then $bc \neq 0$. But with $bc \neq 0$ and $a\,(bc) = 0$, we must have a a 0 divisor (i.e., $a \in G_n$) and G_n is closed under multiplication.

Theorem 20.6.

Theorem. 20.6. The set G_n of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisions forms a group under multiplication modulo n.

Proof. First, we show G_n is closed under multiplication. Let $a, b \in G_n$. Suppose $ab \notin G_n$. Then there is some $c \neq 0$ in $\mathbb{Z}_n$ such that $(ab)\,c = 0$ since we have assumed ab is not a division of 0. Now $(ab)\,c = 0$ implies that $a\,(bc) = 0$. Since $b \in G_n$ and $c \neq 0$, then $bc \neq 0$. But with $bc \neq 0$ and $a\,(bc) = 0$, we must have a a 0 divisor (i.e., $a \in G_n$) and G_n is closed under multiplication.

Now to show that G_n is a group. Associativity of multiplication modulo n is inherited from $\mathbb{Z}_n\,(\mathcal{G}_1)$. Since 1 is not a 0 division, then $1 \in G_n\,(\mathcal{G}_2)$. If $a \in G_n$, then let $1, a_1, a_2, \ldots, a_r$ be the elements of G_n. As in the proof by Theorem 19.11, the elements of $a1, aa_1, aa_2, \ldots, aa_r$ are all different, for if $aa_i = aa_j$ then $a\,(a_i - a_j) = 0$ and since $a \in G_n$, then $a_i - a_j = 0$ or $a_i = a_j$.

Theorem 20.6.

Theorem. 20.6. The set G_n of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisions forms a group under multiplication modulo n.

Proof. First, we show G_n is closed under multiplication. Let $a, b \in G_n$. Suppose $ab \notin G_n$. Then there is some $c \neq 0$ in $\mathbb{Z}_n$ such that $(ab)\,c = 0$ since we have assumed ab is not a division of 0. Now $(ab)\,c = 0$ implies that $a\,(bc) = 0$. Since $b \in G_n$ and $c \neq 0$, then $bc \neq 0$. But with $bc \neq 0$ and $a\,(bc) = 0$, we must have a a 0 divisor (i.e., $a \in G_n$) and G_n is closed under multiplication.

Now to show that G_n is a group. Associativity of multiplication modulo n is inherited from $\mathbb{Z}_n\,(\mathcal{G}_1)$. Since 1 is not a 0 division, then $1 \in G_n\,(\mathcal{G}_2)$. If $a \in G_n$, then let $1, a_1, a_2, \ldots, a_r$ be the elements of G_n. As in the proof by Theorem 19.11, the elements of $a1, aa_1, aa_2, \ldots, aa_r$ are all different, for if $aa_i = aa_j$ then $a\,(a_i - a_j) = 0$ and since $a \in G_n$, then $a_i - a_j = 0$ or $a_i = a_j$. So $aa_j = 1$ for some $0 \leq j \leq n$ (where $a_0 = 1$), and so a is not a 0 divisor then of coarse the inverse of a is not a 0 divisor. □

Theorem 20.6.

Theorem. 20.6. The set G_n of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisions forms a group under multiplication modulo n.

Proof. First, we show G_n is closed under multiplication. Let $a, b \in G_n$. Suppose $ab \notin G_n$. Then there is some $c \neq 0$ in $\mathbb{Z}_n$ such that $(ab)\,c = 0$ since we have assumed ab is not a division of 0. Now $(ab)\,c = 0$ implies that $a\,(bc) = 0$. Since $b \in G_n$ and $c \neq 0$, then $bc \neq 0$. But with $bc \neq 0$ and $a\,(bc) = 0$, we must have a a 0 divisor (i.e., $a \in G_n$) and G_n is closed under multiplication.

Now to show that G_n is a group. Associativity of multiplication modulo n is inherited from $\mathbb{Z}_n\,(\mathcal{G}_1)$. Since 1 is not a 0 division, then $1 \in G_n\,(\mathcal{G}_2)$. If $a \in G_n$, then let $1, a_1, a_2, \ldots, a_r$ be the elements of G_n. As in the proof by Theorem 19.11, the elements of $a1, aa_1, aa_2, \ldots, aa_r$ are all different, for if $aa_i = aa_j$ then $a\,(a_i - a_j) = 0$ and since $a \in G_n$, then $a_i - a_j = 0$ or $a_i = a_j$. So $aa_j = 1$ for some $0 \leq j \leq n$ (where $a_0 = 1$), and so a is not a 0 divisor then of coarse the inverse of a is not a 0 divisor. □

Theorem 20.8. Euler's Theorem

Theorem. 20.8. If a is an integer relatively prime to n, then $a^{\varphi(n)} - 1$ is divisible by n. That is, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. For integer a relatively prime to n there exists $k \in \mathbb{Z}$ such that $0 < a + kn < n$. Notice that $b = a + kn$ is relatively prime to $n\mathbb{Z}$ (if n and b have a common factor, then the factor would have to divide a but then a and n would not be relatively prime).

Theorem 20.8. Euler's Theorem

Theorem. 20.8. If a is an integer relatively prime to n, then $a^{\varphi(n)} - 1$ is divisible by n. That is, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. For integer a relatively prime to n there exists $k \in \mathbb{Z}$ such that $0 < a + kn < n$. Notice that $b = a + kn$ is relatively prime to $n\mathbb{Z}$ (if n and b have a common factor, then the factor would have to divide a but then a and n would not be relatively prime). In other words, the coset $a + n\mathbb{Z}$ of $n\mathbb{Z}$ contains an integer $b < n$ and relatively prime to n. Since a and b from the same coset, then $a \equiv b \pmod{n}$ and so $a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{\ }$.

Theorem 20.8. Euler's Theorem

Theorem. 20.8. If a is an integer relatively prime to n, then $a^{\varphi(n)} - 1$ is divisible by n. That is, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. For integer a relatively prime to n there exists $k \in \mathbb{Z}$ such that $0 < a + kn < n$. Notice that $b = a + kn$ is relatively prime to $n\mathbb{Z}$ (if n and b have a common factor, then the factor would have to divide a but then a and n would not be relatively prime). In other words, the coset $a + n\mathbb{Z}$ of $n\mathbb{Z}$ contains an integer $b < n$ and relatively prime to n. Since a and b from the same coset, then $a \equiv b \pmod{n}$ and so $a^{\varphi(n)} \equiv b^{\varphi(n)}$ (mod). By Theorem 19.3, G_n consists of the elements of $\mathbb{Z}_n$ which are relatively prime to n and so the order of G_n is $\varphi(n)$. Also, $b \in G_n$. Now b generates a subgroup $\langle b \rangle$ of G_n of some order m which divides $\varphi(n)$ (the order of G_n) by Lagrange's Theorem. Now $b^m \equiv 1 \pmod{n}$ (see the proof of Case II of Theorem 6.10) and so $b^{\varphi(n)} \equiv 1 \pmod{n}$. Therefore $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Theorem 20.8. Euler's Theorem

Theorem. 20.8. If a is an integer relatively prime to n, then $a^{\varphi(n)} - 1$ is divisible by n. That is, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. For integer a relatively prime to n there exists $k \in \mathbb{Z}$ such that $0 < a + kn < n$. Notice that $b = a + kn$ is relatively prime to $n\mathbb{Z}$ (if n and b have a common factor, then the factor would have to divide a but then a and n would not be relatively prime). In other words, the coset $a + n\mathbb{Z}$ of $n\mathbb{Z}$ contains an integer $b < n$ and relatively prime to n. Since a and b from the same coset, then $a \equiv b \pmod{n}$ and so $a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{\ }$. By Theorem 19.3, G_n consists of the elements of $\mathbb{Z}_n$ which are relatively prime to n and so the order of G_n is $\varphi(n)$. Also, $b \in G_n$. Now b generates a subgroup $\langle b \rangle$ of G_n of some order m which divides $\varphi(n)$ (the order of G_n) by Lagrange's Theorem. Now $b^m \equiv 1 \pmod{n}$ (see the proof of Case II of Theorem 6.10) and so $b^{\varphi(n)} \equiv 1 \pmod{n}$. Therefore $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Theorem 20.10.

Theorem.20.10. Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_m$.

proof (continued). By Theorem 20.6, a is a unit in $\mathbb{Z}_m$ (since G_n is a multiplicative group and so a has a multiplicative inverse, $a^{-1} \in \mathbb{Z}_m$). So $ax = b$ implies $a^{-1}ax = a^{-1}b$ or $x = a^{-1}b$ and this solutions is unique by the implication (as a result of the first that multiplication is the binary operation in G_n). □

Theorem 20.12.

Theorem. 20.12. Let m be a natural number and let $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof. First, suppose $s \in \mathbb{Z}_m$ in a solution of $ax = b$. Then $as - b = qm = 0 \pmod{m}$ for some $q \in \mathbb{Z}$. Since d divides a and m, it must also divide b. So if $ax = b$ has a solution then d divides b.

Now suppose d divides b. Let $a = a_1 d$, $b = b_1 d$, and $m = m_1 d$. Then the equation $as - b = qm$ can be written as $d(a_1 s - b_1) = dqm_1$ or $a_1 s - b_1 = qm_1$. So $as - b$ is a multiple of m if and only if $a_1 s - b_1$ is a multiple of m_1. So the solutions s of $ax \equiv b \pmod{m}$ are precisely the elements that satisfy $a_1 x \equiv b_1 \pmod{m_1}$. Since a_1 and m_1 are relatively prime (by the choice of d), then there is one solution s to $a_1 x \equiv b_1 \pmod{m_1}$ in $\mathbb{Z}_m$, by Theorem 20.10.

Theorem 20.12.

Theorem. 20.12. Let m be a natural number and let $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof. First, suppose $s \in \mathbb{Z}_m$ in a solution of $ax = b$. Then $as - b = qm = 0 \pmod{m}$ for some $q \in \mathbb{Z}$. Since d divides a and m, it must also divide b. So if $ax = b$ has a solution then d divides b.

Now suppose d divides b. Let $a = a_1 d$, $b = b_1 d$, and $m = m_1 d$. Then the equation $as - b = qm$ can be written as $d(a_1 s - b_1) = dqm_1$ or $a_1 s - b_1 = qm_1$. So $as - b$ is a multiple of m if and only if $a_1 s - b_1$ is a multiple of m_1. So the solutions s of $ax \equiv b \pmod{m}$ are precisely the elements that satisfy $a_1 x \equiv b_1 \pmod{m_1}$. Since a_1 and m_1 are relatively prime (by the choice of d), then there is one solution s to $a_1 x \equiv b_1 \pmod{m_1}$ in $\mathbb{Z}_m$, by Theorem 20.10. The elements of Z_m which reduce to s modulo m_1 (and hence are solutions to $ax \equiv b$(mod m) are $s, s + m_1, s + 2m_1, \ldots, s + (d - 1) m_1$. These are the solutions to $ax \equiv b \pmod{m}$ and therefore there are d solutions. □

Theorem 20.12.

Theorem. 20.12. Let m be a natural number and let $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof. First, suppose $s \in \mathbb{Z}_m$ in a solution of $ax = b$. Then $as - b = qm = 0 \pmod{m}$ for some $q \in \mathbb{Z}$. Since d divides a and m, it must also divide b. So if $ax = b$ has a solution then d divides b.
Now suppose d divides b. Let $a = a_1 d$, $b = b_1 d$, and $m = m_1 d$. Then the equation $as - b = qm$ can be written as $d(a_1 s - b_1) = dqm_1$ or $a_1 s - b_1 = qm_1$. So $as - b$ is a multiple of m if and only if $a_1 s - b_1$ is a multiple of m_1. So the solutions s of $ax \equiv b \pmod{m}$ are precisely the elements that satisfy $a_1 x \equiv b_1 \pmod{m_1}$. Since a_1 and m_1 are relatively prime (by the choice of d), then there is one solution s to $a_1 x \equiv b_1 \pmod{m_1}$ in $\mathbb{Z}_m$, by Theorem 20.10. The elements of Z_m which reduce to s modulo m_1 (and hence are solutions to $ax \equiv b(\bmod\ m)$ are $s, s + m_1, s + 2m_1, \ldots, s + (d-1)m_1$. These are the solutions to $ax \equiv b \pmod{m}$ and therefore there are d solutions. $\square$