Mathematical Reasoning

Chapter 6. Number Theory
6.5. Introduction to Euler's Function—Proofs of Theorems

Undergraduate Texts in Mathematics
UTM

Larry J. Gerstein

Introduction to Mathematical Structures and Proofs

Second Edition

Springer
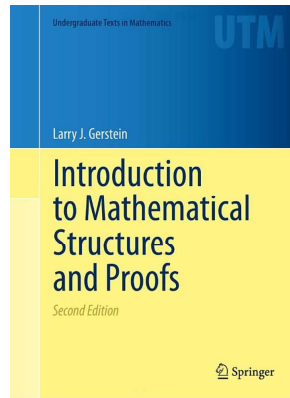
Lemma 6.51

Lemma 6.51.

(i) If $m \mid ab$ and $(m, a) = 1$, then $m \mid b$.

(ii) **(The Cancellation Law.)** If $ax \equiv ay$ (mod m and $(a, m) = 1$, then $x \equiv y$ (mod m).

Proof. (i) Since $m \mid ab$, we can write $ab = mc$. Since $(a, m) = 1$ by hypothesis, then by Corollary 6.21 we know that there are integers x and y such that $ax + my = (a, m) = 1$. Multiplying both sides of this equation by b gives $b = abx + mby = m(cx + by)$, so that $m \mid b$ as claimed.

(ii) Since $ax \equiv ay$ (mod m) by hypothesis, then (by Definition 6.37) $m \mid a(x - y)$. Since $(a, m) = 1$ by hypothesis, the part (i) implies that $m \mid (x - y)$, and so $x \equiv y$ (mod m) as claimed. □

Theorem 6.52

Theorem 6.52. Euler's Theorem.
Suppose m is positive and $(x, m) = 1$. Then $x^{\varphi(m)} \equiv 1$ (mod m).

Proof. Let $S = \{y \mid 1 \leq y \leq m \text{ and } (y, m) = 1\} = \{a_1, a_2, \ldots, a_{\varphi(m)}\}$. By Theorem 6.26 any prime divisor of xa_i must divide either x or a_i, but both x and a_i are relatively prime to m, so $(xa_i, m) = 1$ for each i with $1 \leq i \leq \varphi(m)$. From the Division Algorithm (Theorem 6.17) we have $xa_i = mq + r \equiv r$ (mod m) for some r satisfying $0 \leq r < m$. Now if $(r, m) = k \neq 1$, the $k \mid xa_i$ but this contradicts the fact that $(xa_i, m) = 1$ as shown above. So we must have $(r, m) = 1$ and hence $r \in S$; that is, $r = a_j$ for some j with $1 \leq j \leq \varphi(m)$. Since each a_i satisfies $1 \leq a_i \leq m$, then no two elements $a_1, a_2, \ldots, a_{\varphi(m)}$ are congruent modulo m. So for $i_1 \neq i_2$ with $1 \leq i_1, i_2 \leq \varphi(m)$ we have $a_{i_1} \not\equiv a_{i_2}$ (mod m). Hence, because $(x, m) = 1$ by hypothesis, the contrapositive of the Cancellation Law (Lemma 6.51(ii)) implies that $xa_{i_1} \not\equiv xa_{i_2}$ (mod m). That is, the integers $xa_1, xa_2, \ldots, xa_{\varphi(m)}$ are congruent modulo m to different elements of S.

Theorem 6.52 (continued)

Theorem 6.52. Euler's Theorem.
Suppose m is positive and $(x, m) = 1$. Then $x^{\varphi(m)} \equiv 1$ (mod m).

Proof (continued). So we have a system of $\varphi(m)$ congruences:

$$xa_1 \equiv a_{j_1} \pmod{m}, \ xa_2 \equiv a_{j_2} \pmod{m}, \ \ldots, \ xa_{\varphi(m)} \equiv a_{j_{\varphi(m)}} \pmod{m}$$

where each $a_i \in S$ appears exactly once on each side of this list. By Corollary 6.43, the product of the left-hand sides of these congruences is congruent modulo m to the product of the right hand sides:

$$x^{\varphi(m)} \prod_{i=1}^{\varphi(m)} a_i = \prod_{i=1}^{\varphi(m)} a_m \pmod{m}.$$ But since each a_i is relatively prime to m, then $\prod_{i=1}^{\varphi(m)} a_i$ is also relatively prime to m. The Cancellation Law (Lemma 6.51(ii)) then implies that $x^{\varphi(m)} \equiv 1$ (mod m), as claimed. □

Corollary 6.53. Fermat's Theorem/Fermat's Little Theorem

Corollary 6.53. Fermat's Theorem/Fermat's Little Theorem.
If p is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. This follows from Euler's Theorem (Theorem 6.52) with $m = p$, because $\varphi(p) = p - 1$ by Example 6.50. □