Example 4.10. Because $13 \equiv 3 \pmod 5$ and $7 \equiv 2 \pmod 5$, using Theorem 3.5 we see that $20 = 13 + 7 \equiv 3 + 2 = 5 \pmod 5$, $6 = 13 - 7 \equiv 3 - 2 = 1 \pmod 5$, and $91 = 13 \cdot 7 \equiv 3 \cdot 2 = 6 \pmod 5$. ◀

The following lemma helps us to determine whether a set of m numbers forms a complete set of residues modulo m.

Lemma 4.1. *A set of m incongruent integers modulo m forms a complete set of residues modulo m.*

Proof. Suppose that a set of m incongruent integers modulo m does not form a complete set of residues modulo m. This implies that at least one integer a is not congruent to any of the integers in the set. Hence, there is no integer in the set congruent modulo m to the remainder of a when it is divided by m. Hence, there can be at most $m - 1$ different remainders of the integers when they are divided by m. It follows (by the pigeonhole principle, which says that if more than n objects are distributed into n boxes, at least two objects are in the same box) that at least two integers in the set have the same remainder modulo m. This is impossible, because these integers are incongruent modulo m. Hence, any m incongruent integers modulo m form a complete system of residues modulo m. ■

Theorem 4.6. *If $r_1, r_2, \ldots, r_m$ is a complete system of residues modulo m, and if a is a positive integer with $(a, m) = 1$, then*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

is a complete system of residues modulo m for any integer b.

Proof. First, we show that no two of the integers

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

are congruent modulo m. To see this, note that if

$$ar_j + b \equiv ar_k + b \pmod m,$$

then, by (ii) of Theorem 4.3, we know that

$$ar_j \equiv ar_k \pmod m.$$

Because $(a, m) = 1$, Corollary 4.4.1 shows that

$$r_j \equiv r_k \pmod m.$$

Given that $r_j \not\equiv r_k \pmod m$ if $j \neq k$, we conclude that $j = k$.

By Lemma 4.1, because the set of integers in question consists of m incongruent integers modulo m, these integers form a complete system of residues modulo m. ■

The following theorem shows that a congruence is preserved when both sides are raised to the same positive integral power.