3.4 Reduced Residue Systems and Euler's ϕ Function

Recall the following definition from Section 3.2.

Definition. Let n be a positive integer. A set of integers $S = \{a_1, a_2, \ldots, a_n\}$ is called a **complete residue system** (mod n) if for every integer r there is exactly one integer a_j in the set S such that $r \equiv a_j \pmod{n}$.

Thus, each element a of a complete residue system S is congruent to *exactly* one element in S; namely, a is congruent to itself but not congruent to another element in S. Hence, distinct elements of a complete residue system can not be congruent to each other.

Example 1. Let $n = 12$, then the following sets are complete residue systems (mod 12):

1. $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
2. $T = \{13, 14, 16, 19, 23, 34, 41, 54, 57, 63, 68, 72\}$.

Theorem 3.4.1. Let a, b, n be integers where $n \geq 1$. Suppose that $a \equiv b \pmod{n}$. Then $(a, n) = 1$ if and only if $(b, n) = 1$.

Proof. Assume that $a \equiv b \pmod{n}$. We shall prove that $(a, n) = 1$ if and only if $(b, n) = 1$. Assume $(a, n) = 1$. We prove that $(b, n) = 1$. To do this, let $d = (b, n)$. Thus, $d \mid b$ and $d \mid n$. Since $a \equiv b \pmod{n}$, there is an integer i such that $a - b = in$. Thus, $a = b + in$. Because $d \mid b$ and $d \mid n$, we conclude that $d \mid a$. So, $d \mid a$ and $d \mid n$. Since $(a, n) = 1$, it follows that $d = 1$. A similar argument, shows that if $(b, n) = 1$, then $(a, n) = 1$. □

Definition 3.4.2. Let S be a complete residue system (mod n). The set S' consists of those elements in S that are relatively prime to n. The set S' is called the **reduced residue system** (mod n).

Example 2. Let $n = 12$ and consider the complete residue systems (mod 12):

1. $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
2. $T = \{13, 14, 16, 19, 23, 34, 41, 54, 57, 63, 68, 72\}$.

Then the corresponding reduced residue systems S' and T' are given by

1. $S' = \{1, 5, 7, 11\}$
2. $T' = \{13, 19, 23, 41\}$.

Note that S' and T' both have 4 elements and that every element $a \in S'$ is congruent (mod 12) to exactly one element in $b \in T'$. Similarly, for every element $b \in T'$ there is a unique element in $a \in S'$ such that $a \equiv b \pmod{12}$. In fact, there is a one-to-one correspondence between the sets S' and T' as follows:

$$
\begin{aligned}
1 &\equiv 13 \pmod{12} \\
5 &\equiv 19 \pmod{12} \\
7 &\equiv 41 \pmod{12} \\
11 &\equiv 23 \pmod{12}
\end{aligned}
$$

Example 3. Let $n = 20$ and consider the complete residue system (mod 20)

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}.$$

Then the reduced residue system is $S' = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and contains 8 elements. For any other such complete residue system (mod 20), say T, the reduced residue system T' will also have 8 elements. For example let T be the complete residue system (mod 20)

$$T = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60\}.$$

The reduced residue system is $T' = \{3, 9, 21, 27, 33, 39, 51, 57\}$ which has 8 elements. For each $a \in S'$ there is a unique element $b \in T'$ such that $a \equiv b \pmod{20}$. For example, $1 \equiv 21 \pmod{20}$, $9 \equiv 9 \pmod{20}$, $13 \equiv 33 \pmod{20}$. Similarly, for every element $b \in T'$ there is a unique element in $a \in S'$ such that $a \equiv b \pmod{20}$. For instance, note that $51 \in T'$ and there is exactly one element $a \in S'$ such that $a \equiv 51 \pmod{20}$; namely, $a = 11$. Thus, we can list this one-to-one correspondence as follows:

$$\begin{aligned}
1 &\equiv 21 \pmod{20}\\
3 &\equiv 3 \pmod{20}\\
7 &\equiv 7 \pmod{20}\\
9 &\equiv 9 \pmod{20}\\
11 &\equiv 51 \pmod{20}\\
13 &\equiv 33 \pmod{20}\\
17 &\equiv 27 \pmod{20}\\
19 &\equiv 39 \pmod{20}.
\end{aligned}$$

Theorem 3.4.3. Let $n \geq 1$ and let S be a complete residue system (mod n). Let k be an integer. If $(k, n) = 1$, then k is congruent to exactly one member of S'. Let T be any complete residue system (mod n). Then S' and T' have the same number of elements. Furthermore, if $S' = \{a_1, a_2, \ldots, a_k\}$, then there is a listing of $T' = \{b_1, b_2, \ldots, b_k\}$ where

$$\begin{aligned}
a_1 &\equiv b_1 \pmod{n}\\
a_2 &\equiv b_2 \pmod{n}\\
&\vdots\\
a_k &\equiv b_k \pmod{n}.
\end{aligned} \tag{3.27}$$

Proof. Let k be an integer such that $(k, n) = 1$. Since S is a complete residue system (mod n), there is exactly one $a \in S$ such that $k \equiv a \pmod{n}$. Since $(k, n) = 1$ and $k \equiv a \pmod{n}$, Theorem 3.4.1 implies that $(k, n) = 1$ and thus, $a \in S'$.

Now let T be another complete residue system (mod n). Let $a \in S'$. So, $(a, n) = 1$. Since T is also a complete residue system (mod n), there is exactly one $b \in T$ such that $a \equiv b \pmod{n}$. Again, Theorem 3.4.1 implies that $(b, n) = 1$ and thus, $b \in T'$. Similarly, for $b \in T'$ there is a unique $a \in S'$ such that $a \equiv b \pmod{n}$. It follows that

(i) for all $a \in S'$ there is exactly one $b \in T'$ such that $a \equiv b \pmod{n}$, and

(ii) for all $b \in T'$ there is exactly one $a \in S'$ such that $a \equiv b \pmod{n}$.

As noted at the beginning of this section, two distinct elements of a residue system can not be congruent to each other. Thus, (i) implies a "one-to-one" correspondence between the sets S' and T' and (ii) implies that this correspondence is "onto". Therefore, the sets S' and T' have the same number of elements. Suppose now that $S' = \{a_1, a_2, \ldots, a_k\}$. From (i) and (ii) it follows that there is a listing of $T' = \{b_1, b_2, \ldots, b_k\}$ such that

$$\begin{aligned} a_1 &\equiv b_1 \pmod{n} \\ a_2 &\equiv b_2 \pmod{n} \\ &\vdots \\ a_k &\equiv b_k \pmod{n}. \end{aligned}$$

This completes the proof. □

Definition 3.4.4. For each integer $n \geq 1$ let $\phi(n)$ denote the number of elements in a reduced residue system (mod n). This function ϕ is called **Euler's ϕ function**.

Example 4. Let $n = 12$, then the above Example 2 implies that $\phi(12) = 4$. Let $n = 20$, then Example 3 implies that $\phi(20) = 8$.

Theorem 3.4.5. Let $n \geq 1$ be an integer. Then $\phi(n)$ equals the number of positive integers k such that $k \leq n$ and $(k, n) = 1$.

Proof. Let $P = \{1, 2, 3, \ldots, n\}$. We know that P is a complete residue system (mod n). The reduced residue system P' is the set of positive integers k such that $k \leq n$ and $(k, n) = 1$. We see that the number of elements in P' equals $\phi(n)$. □

In the following table, we use $S = \{1, 2, 3, \ldots, n\}$ as our complete residue system (mod n) and list the corresponding reduced residue systems S' for different values of n.

n	reduced residue system S'	$\phi(n)$
1	$\{1\}$	1
2	$\{1\}$	1
3	$\{1,2\}$	2
4	$\{1,3\}$	2
5	$\{1,2,3,4\}$	4
6	$\{1,5\}$	2
7	$\{1,2,3,4,5,6\}$	6
8	$\{1,3,5,7\}$	4
9	$\{1,2,4,5,7,8\}$	6
10	$\{1,3,7,9\}$	4
11	$\{1,2,3,4,5,6,7,8,9,10\}$	10
12	$\{1,5,7,11\}$	4

We make the observation that $\phi(p) = p - 1$ for any prime p.

Building New Complete Residue Systems from Old

Recall that a list of integers $a_1, a_2, \ldots, a_n$ is called a **complete residue system** (mod n) if for every integer r there is exactly one integer a_j in the list such that $r \equiv a_j \pmod{n}$. Thus, if a_i and a_j are members of a complete residue system (mod n) and $a_j \equiv a_i \pmod{n}$, then we must have that $a_i = a_j$.

Lemma 3.4.6. Let n be a positive integer. Suppose that $a_1, a_2, \ldots, a_n$ is a complete residue system (mod n). Let b be any integer. Then $a_1 + b, a_2 + b, \ldots, a_n + b$ is also a complete residue system (mod n).

Proof. Let n be a positive integer and let b be an integer. Suppose that

$$a_1, a_2, \ldots, a_n \tag{3.28}$$

is a complete residue system (mod n). We now show that

$$a_1 + b, a_2 + b, \ldots, a_n + b \tag{3.29}$$

is a complete residue system. Let r be any integer. We shall show that there is exactly one $a_j + b$ in the list (3.29) such that $r \equiv a_j + b \pmod{n}$. Because $r - b$ is an integer and the list (3.28) is a complete residue system (mod n), it follows that there is an a_j in the list (3.30) such that $r - b \equiv a_j \pmod{n}$. Thus, we have that $r \equiv a_j + b \pmod{n}$. Suppose that some other $a_i + b$ on the list (3.29) also satisfies $r \equiv a_i + b \pmod{n}$. Thus, $a_j + b \equiv a_i + b \pmod{n}$ and we conclude that $a_j \equiv a_i \pmod{n}$. Hence, $a_j = a_i$. Therefore, $a_1 + b, a_2 + b, \ldots, a_n + b$ is a complete residue system (mod n). □

Example 5. Let $n = 12$ and consider the complete residue systems (mod 12):

1. $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
2. $\{13, 14, 16, 19, 23, 34, 41, 54, 57, 63, 68, 72\}$.

By adding 3 to every member of the above residue systems, we create the new complete residue systems (mod 12):

1. $\{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$
2. $\{16, 17, 19, 21, 26, 37, 44, 57, 60, 66, 71, 75\}$.

Lemma 3.4.7. Let n be a positive integer and let a be an integer with $(a, n) = 1$. Suppose that $a_1, a_2, \ldots, a_n$ is a complete residue system (mod n). Then $aa_1, aa_2, \ldots, aa_n$ is also a complete residue system (mod n).

Proof. Let n be a positive integer and let a be an integer with $(a, n) = 1$. Suppose that

$$a_1, a_2, \ldots, a_n \tag{3.30}$$

is a complete residue system (mod n). Because $(a, n) = 1$, Theorem 3.3.5 asserts that the congruence equation $ax \equiv 1 \pmod{n}$ has a solution. Thus, there is an integer c such that $ac \equiv 1 \pmod{n}$. We can now show that

$$aa_1, aa_2, \ldots, aa_n \tag{3.31}$$

is a complete residue system. Let r be any integer. We shall show that there is exactly one aa_j in the list (3.31) such that $r \equiv aa_j \pmod{n}$. Because cr is an integer and the list (3.30) is a complete residue system (mod n), it follows that there is an a_j in the list (3.30) such that $cr \equiv a_j \pmod{n}$. Thus, we have that $acr \equiv aa_j \pmod{n}$. Since $ac \equiv 1 \pmod{n}$, we conclude that $r \equiv aa_j \pmod{n}$. Suppose that some other aa_i on the list (3.31) also satisfies $r \equiv aa_i \pmod{n}$. Thus, $aa_j \equiv aa_i \pmod{n}$ and, since $(a, n) = 1$, we conclude that $a_j \equiv a_i \pmod{n}$. Hence, $a_j = a_i$. Therefore, $aa_1, aa_2, \dots, aa_n$ is a complete residue system (mod n). □

Example 6. Let $n = 12$ and consider the complete residue system (mod 12) given by $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. Since $(5, 12) = 1$, Lemma 3.4.7 states that we can multiply every member of this residue system by 5 and obtain the new complete residue system (mod 12): $\{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\}$.

Corollary 3.4.8. Let n be a positive integer. Let a and b be integers where $(a, n) = 1$. Suppose that $a_1, a_2, \dots, a_n$ is a complete residue system (mod n). Then $aa_1 + b, aa_2 + b, \dots, aa_n + b$ is also a complete residue system (mod n).

Proof. Let a and b be integers where $(a, n) = 1$. Suppose that $a_1, a_2, \dots, a_n$ is a complete residue system (mod n). Lemma 3.4.7 implies that $aa_1, aa_2, \dots, aa_n$ is a a complete residue system (mod n). Now, Lemma 3.4.6 asserts that $aa_1+b, aa_2+b, \dots, aa_n+b$ is also a complete residue system (mod n). □

Building New Reduced Residue Systems from Old

Lemma 3.4.9. Let n be a positive integer and let a be an integer with $(a, n) = 1$. For any integer k we have that $(k, n) = 1$ if and only if $(ak, n) = 1$.

Proof. Let n be a positive integer and let a be an integer with $(a, n) = 1$. Let k be any integer. Suppose that $(k, n) = 1$. Let $d = (ak, n)$. Assume, for a contradiction, that $d > 1$. Thus, there is a prime p such that $p \mid d$. Since $d = (ak, n)$ and $p \mid d$, we know that $p \mid n$ and $p \mid ak$. Because $p \mid ak$ and p is a prime, we realize that $p \mid a$ or $p \mid k$. Since $(k, n) = 1$, it follows that $p \mid a$ and, because $p \mid n$ and $(a, n) = 1$, we conclude that $p \mid 1$. This is not possible because p is a prime. This contradiction shows that $d = 1$.

Conversely, assume that $(ak, n) = 1$. Let $d = (k, n)$. Thus, $d \mid k$ and $d \mid n$. Since $d \mid k$ it follows that $d \mid ak$. So, $d \mid ak$ and $d \mid n$. But $(ak, n) = 1$, and thus $d = 1$. □

Lemma 3.4.10. Let n be a positive integer and let a be an integer with $(a, n) = 1$. Suppose that $S = \{a_1, a_2, \dots, a_n\}$ is a complete residue system (mod n), and let T be the complete residue system (mod n) defined by $T = \{aa_1, aa_2, \dots, aa_n\}$. Let S' and T' be the corresponding reduced residue system of S and T. Let $S' = \{a'_1, a'_2, \dots, a'_{\phi(n)}\}$. Then $T' = \{aa'_1, aa'_2, \dots, aa'_{\phi(n)}\}$.

Proof. We have that $(a, n) = 1$. Let $a_i \in S$. Lemma 3.4.9 states that $(a_i, n) = 1$ if and only if $(aa_i, n) = 1$. It now follows that $T' = \{aa'_1, aa'_2, \dots, aa'_{\phi(n)}\}$. □

Thus, if $\{r_1, r_2, \dots, r_{\phi(n)}\}$ is a reduced residue system (mod n) and $(a, n) = 1$, then we have a new reduced residue system (mod n) given by $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$.

Example 7. Let $n = 12$ and so, $\phi(12) = 4$. Recall (see Example 2) the reduced residue system (mod 12) given by $S' = \{1, 5, 7, 11\}$. Since $(5, 12) = 1$, Lemma 3.4.10 states that we can multiply every member of S' by 5 to obtain $T' = \{(5 \cdot 1), (5 \cdot 5), (5 \cdot 7), (5 \cdot 11)\}$, a new reduced residue system (mod 12). Recall that every element in S' is congruent (mod 12) to exactly one element in T' and vice versa. Let us identify this correspondence:

$$\begin{aligned} 1 &\equiv (5 \cdot 5) \pmod{12} \\ 5 &\equiv (5 \cdot 1) \pmod{12} \\ 7 &\equiv (5 \cdot 11) \pmod{12} \\ 11 &\equiv (5 \cdot 7) \pmod{12}. \end{aligned}$$

We can now show that $5^{\phi(12)} \equiv 1 \pmod{12}$ [recall that $\phi(12) = 4$] as follows:

$$\begin{aligned} (5 \cdot 1)(5 \cdot 5)(5 \cdot 7)(5 \cdot 11) &\equiv (1 \cdot 5 \cdot 7 \cdot 11) \pmod{12} \\ (1 \cdot 5 \cdot 7 \cdot 11)5^4 &\equiv (1 \cdot 5 \cdot 7 \cdot 11) \pmod{12} \\ 5^4 &\equiv 1 \pmod{12}. \end{aligned}$$

Theorem 3.4.11 (Euler's Theorem)**.** Let n be a positive integer and let a be an integer with $(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Let n be a positive integer and let a be an integer with $(a, n) = 1$. Let $S' = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ be a reduced residue system (mod n). We know by Theorem 3.4.7 that $T' = \{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ is also reduced residue system. Theorem 3.4.3 implies every element in S' is congruent (mod n) to exactly one element in T', and vice versa. Hence, (see Example 7 and Theorem 3.4.3) we have that

$$ar_1 ar_2 \cdots ar_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}.$$

After simplifying we obtain $r_1 r_2 \cdots r_{\phi(n)} a^{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$. Because each r_i satisfies $(r_i, n) = 1$, we can cancel each r_i by Theorem 3.2.6. Thus, $a^{\phi(n)} \equiv 1 \pmod{n}$. This completes the proof. □

Theorem 3.4.12 (Fermat's Theorem)**.** Let p be prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Let p be a prime and assume that $p \nmid a$. Thus $(a, p) = 1$. Since $\phi(p) = p - 1$, we obtain $a^{p-1} \equiv 1 \pmod{p}$ by Theorem 3.4.11. □

Corollary 3.4.13. Let p be a prime. Then for any integer a we have $a^p \equiv a \pmod{p}$.

Proof. Let p be a prime. If $p \mid a$, then $a \equiv 0 \pmod{p}$ and $a^p \equiv 0 \pmod{p}$. Hence, $a^p \equiv a \pmod{p}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ by Theorem 3.4.12. After multiplying by a, we also see that $a^p \equiv a \pmod{p}$. □

Definition 3.4.14. Suppose that $n > 1$ is a composite number such that $n \mid (2^n - 2)$. Then n is called a **pseudoprime**.

Problem 8. Given the prime factorization $341 = 11 \cdot 31$, show that 341 is a pseudoprime.

Solution. We must show that $341 \mid (2^{341} - 2)$. To do this, we will first show that

$$11 \mid (2^{341} - 2) \tag{3.32}$$

by showing that $2^{341} \equiv 2 \pmod{11}$ as follows: Since 11 is a prime and $11 \nmid 2$, Fermat's Theorem implies that $2^{10} \equiv 1 \pmod{11}$. Note that 10 evenly divides 340 and so, $340 = 10 \cdot 34$. Thus,

$$\begin{aligned} 2^{10} &\equiv 1 \pmod{11} && \text{by Fermat's Theorem} \\ (2^{10})^{34} &\equiv 1^{34} \pmod{11} && \text{by congruence algebra} \\ 2^{340} &\equiv 1 \pmod{11} && \text{by prop. of exponents} \\ 2^{341} &\equiv 2 \pmod{11} && \text{by congruence algebra.} \end{aligned}$$

Therefore, (3.32) holds. Now we show that

$$31 \mid (2^{341} - 2) \tag{3.33}$$

by showing that $2^{341} \equiv 2 \pmod{31}$. First we try the argument given above using the prime 31. Since 31 is a prime and $31 \nmid 2$, Fermat's Theorem implies that $2^{30} \equiv 1 \pmod{31}$. However, 30 does not evenly divides 340. So, we cannot use 30. But $2^5 = 32$. Hence $2^5 \equiv 1 \pmod{31}$ and 5 does evenly divide 340. Thus, $340 = 5 \cdot 68$. Hence,

$$\begin{aligned} 2^{5} &\equiv 1 \pmod{31} && \text{since } 2^5 = 32 \\ (2^{5})^{68} &\equiv 1^{68} \pmod{31} && \text{by congruence algebra} \\ 2^{340} &\equiv 1 \pmod{31} && \text{by prop. of exponents} \\ 2^{341} &\equiv 2 \pmod{31} && \text{by congruence algebra.} \end{aligned}$$

Therefore, (3.33) holds. Because (3.32) and (3.33) hold and because $(11, 31) = 1$, Theorem 2.2.2 implies that $(11 \cdot 31) \mid (2^{341} - 2)$. Therefore, $341 \mid (2^{341} - 2)$ and so 341 is a pseudoprime.

Example 9. Consider the prime $p = 13$. We show that $12! \equiv -1 \pmod{13}$. Note that the list $0, 1, 2, \ldots, 12$ is a complete residue system (mod 13). Since 13 is a prime, for any integer a in the list

$$1, 2, 3, \ldots, 12 \tag{3.34}$$

we have that $(a, 13) = 1$. Observe that $1 \cdot 1 \equiv 1 \pmod{13}$ and $12 \cdot 12 \equiv 1 \pmod{13}$. One can show that 1 and 12 are the only integers a in the list (3.34) satisfying $a \cdot a \equiv 1 \pmod{13}$. For every integer a in the list

$$2, 3, \ldots, 11 \tag{3.35}$$

Theorem 3.3.5 implies that there is an integer b in the same list (3.35) such that $ab \equiv 1 \pmod{p}$. Moreover, this integer b is unique and different from a. We now list this paring:

$$\begin{aligned} 11 \cdot 6 &\equiv 1 \pmod{13} \\ 10 \cdot 4 &\equiv 1 \pmod{13} \\ 9 \cdot 3 &\equiv 1 \pmod{13} \\ 8 \cdot 5 &\equiv 1 \pmod{13} \\ 7 \cdot 2 &\equiv 1 \pmod{13}. \end{aligned}$$

We can now show that

$$(11)(10)\cdots(2) \equiv 1 \pmod{13} \tag{3.36}$$

as follows:

$$\begin{aligned}(11)(10)(9)(8)(7)(6)(5)(4)(3)(2) &\equiv (11\cdot 6)(10\cdot 4)(9\cdot 3)(8\cdot 5)(7\cdot 2) \pmod{13}\\ &\equiv (1)(1)(1)(1)(1) \pmod{13}\\ &\equiv 1 \pmod{13}.\end{aligned}$$

Since $12 \equiv -1 \pmod{13}$, by multiplying the corresponding sides of equation (3.36), we see that $(12)(11)(10)\cdots(2) \equiv -1 \pmod{13}$. Consequently, $12! \equiv -1 \pmod{13}$.

Theorem 3.4.15 (Wilson's Theorem)**.** If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Let p be a prime and note that the list $0, 1, 2, \ldots, (p-1)$ is a complete residue system $\pmod{p}$. Since p is a prime, for each integer a in the list

$$1, 2, 3, \ldots, (p-1) \tag{3.37}$$

we have that $(a, p) = 1$ and Theorem 3.3.5 implies that there is an integer b in the same list (3.37) such that $ab \equiv 1 \pmod{p}$. Moreover, this integer b is unique. Suppose that $ab \equiv 1 \pmod{p}$ and $ac \equiv 1 \pmod{p}$ for integers b, c in the list (3.37). Thus, $ab \equiv ac \pmod{p}$. Since $(a, p) = 1$, we conclude that $b \equiv c \pmod{p}$. Therefore, $b = c$. Note that $1\cdot 1 \equiv 1 \pmod{p}$ and $(p-1)(p-1) \equiv 1 \pmod{p}$. We now show that 1 and $p-1$ are the only integers a in the list (3.37) satisfying $a \cdot a \equiv 1 \pmod{p}$. If $a \cdot a \equiv 1 \pmod{p}$, then $p \mid (a^2 - 1)$ and thus, $p \mid (a-1)(a+1)$. Since p is a prime, we must have that $p \mid (a-1)$ or $p \mid (a+1)$. It now follows, because a is in the list (3.37) that either $a = 1$ or $a = p-1$. Therefore, for every integer a in the list

$$2, 3, \ldots, (p-2) \tag{3.38}$$

there is exactly one integer b, not equal to a, in this list (3.38) such that $ab \equiv 1 \pmod{p}$. It now follows that $(p-2)(p-3)\cdots(2) \equiv 1 \pmod{p}$. Since $(p-1) \equiv -1 \pmod{p}$, we obtain $(p-1)(p-2)(p-3)\cdots(2) \equiv -1 \pmod{p}$. Consequently, $(p-1)! \equiv -1 \pmod{p}$. □

Exercises 3.4

Do problems #2, 3, ~~4~~, 5, 8, 10 on page 82 of text.

Exercise Notes. Problem 3: Change to read: "when 2 is multiplied by every member". Problem 4: See the above Problem 8 in these notes.

- Problem 5: If $3 \mid a$, then $a \equiv 0 \pmod{3}$ and $a^{561} \equiv 0 \pmod{3}$. Thus, $a^{561} \equiv a \pmod{3}$. If $3 \nmid a$ we use the same ideas as those used in the above Problem 8 in these notes. Since $3 \nmid a$, we have that $a^2 \equiv 1 \pmod{3}$ by Fermat's Theorem. Since $2 \mid 560$, we also conclude that $a^{560} \equiv 1 \pmod{3}$. Therefore, for any a we have that $a^{561} \equiv a \pmod{3}$. Similarly, one can show for any integer a that $a^{561} \equiv a \pmod{11}$ and $a^{561} \equiv a \pmod{17}$. Now use Theorem 2.2.2 to show that $561 \mid (a^{561} - a)$ and therefore $a^{561} \equiv a \pmod{561}$.
- Problem 8: First show that $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, and $a^{16} \equiv 1 \pmod{17}$; then note $2 \mid 80$, $10 \mid 80$ and $16 \mid 80$.
- Problem 10: If $n > 1$ is odd, then $n = 2k + 1$ for $k > 0$.