Throughout, \( \mathbb{N} \) (resp., \( \mathbb{Z} \)) denotes the set of positive integers (resp., all integers). The notation \( a \mid b \) is to be read “\( a \) divides \( b \).” By “prime number,” we always mean “positive prime number.” For all \( m \in \mathbb{Z} \), we write \( U_m \) to denote the group \( (\mathbb{Z}/m\mathbb{Z})^\times \) of units modulo \( m \).

EXERCISE 4.2

Find the smallest nonnegative integer congruent to \( 391 \) modulo 23.

By Fermat’s Little Theorem, \( 3^{22} \equiv 1 \pmod{23} \). Therefore, \( 3^{91} \equiv 3^{44} \cdot 3^{4} \equiv 3^{3} \equiv 4 \pmod{23} \) and 4 is the answer.

EXERCISE 4.14

In Example 4.9 of [13], show that \( k_i \equiv 2 \pmod{5} \) for all \( i \). (In that example, we are inductively given \( x_i \) such that \( 2x_i \equiv 3 \pmod{5^i} \), where \( x_1 = 4 \), and define \( k_i \) according to \( x_{i+1} \equiv x_i + 5^i k_i \pmod{5^{i+1}} \), for all \( i \).)

Write \( 2x_i - 3 = 5^i q_i \). Any odd value of \( q_i \) gives an integer solution to this equation for \( x_i \), but it turns out that if \( x_1 = 4 \), then for all \( i \geq 2 \), only the value \( q_i = 1 \) gives an integer solution \( x_i \) such that \( x_i \equiv x_{i-1} \pmod{5^{i-1}} \), as can be proved by induction. Plugging in \( q_{i+1} = q_i = 1 \), we have

1. \( 2x_i - 3 = 5^i \),
2. \( 2x_{i+1} - 3 = 5^{i+1} \),
3. \( x_{i+1} - x_i \equiv 5^i k_i \pmod{5^{i+1}} \).

Substituting, we find that

\( 5^{i+1} - 5^i \equiv 2(x_{i+1} - x_i) \equiv 2 \cdot 5^i k_i \pmod{5^{i+1}} \).

That is, \( 0 \equiv 5^i(2k_i + 1) \pmod{5^{i+1}} \), from which \( 2k_i + 1 \equiv 0 \pmod{5} \). Therefore, \( k_i \equiv 2 \pmod{5} \), as needed.

Remark 1. Exercises 4.15 and 4.16 were not counted toward the grade for this problem set, as they were assigned on the previous set.

EXERCISE 5.6

Compute \( \varphi(42) \) and verify by finding a full set of representatives for \( U_{42} \).

Since \( 42 = 2 \cdot 3 \cdot 7 \) and \( \varphi \) is a multiplicative arithmetic function, \( \varphi(42) = \varphi(2)\varphi(3)\varphi(7) = 1 \cdot 2 \cdot 6 = 12 \). A full set of representatives for \( U_{42} \) is

\( \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\} \),

which is of size 12, as expected.
Exercise 5.7

For which \( n \) is \( \varphi(n) \) odd? Show that there exist integers \( n \) such that \( \varphi(n) = 2, 4, 6, 8, 10, 12 \), but that there does not exist \( n \) such that \( \varphi(n) = 14 \).

If \( n = 1 \), then \( \varphi(n) = 0 \), which is not odd. If \( n = 2 \), then \( \varphi(n) = 1 \), which is odd. We claim that if \( n \geq 3 \), then \( \varphi(n) \) is even. To prove this claim, we will pair up the invertible residues modulo \( n \). Observe that \( +a \) is coprime to \( n \) if and only if \( -a \) is coprime to \( n \), so it remains to show that when this is the case, \( +a \) and \( -a \) always take distinct residues modulo \( n \). Assume for the sake of contradiction that \( a \equiv -a \pmod{n} \). Then \( 2a \equiv 0 \pmod{n} \), whence \( \varphi(n) \) divides the right-hand side, so either \( i \) or \( \ell \) is odd. But this is impossible because \( n \geq 3 \), as desired. We conclude that \( n = 2 \) is the only value for which \( \varphi(n) \) is odd.

The values \( n = 3, 5, 7, 11, 13 \) yield \( \varphi(n) = 2, 4, 6, 8, 10, 12 \), respectively. Finally, recall that if \( n = p_1^{e_1} \cdots p_r^{e_r} \) is a prime factorization (with the \( p_i \) pairwise distinct), then

\[
\varphi(n) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i-1).
\]

Exercise 5.8

Show that for all \( m \), there exist only finitely many \( n \) such that \( \varphi(n) = m \).

Fix \( m \) and suppose \( \varphi(n) = m \). If \( p \) is a prime factor of \( n \), then \( (p-1) | m \), which forces \( p \leq m + 1 \), so the set of primes that can appear in the prime factorization of an integer \( n \) such that \( \varphi(n) = m \) is finite. Moreover, for any fixed prime \( p \), there are finitely many exponents \( e \) such that \( p^{e-1} | m \). Therefore, for fixed \( m \), the set of possible prime factorizations for an integer \( n \) such that \( \varphi(n) = m \) is finite, i.e., \( \varphi^{-1}(m) \) is finite.

Exercise 3

Find the binary expansions of \( 1/5 \), \( 1/7 \), and \( 2/11 \).

Here is the general algorithm for finding the binary expansion of a fraction \( m/n \) between 0 and 1:

1. Suppose we have found \( a_1, \ldots, a_k \in \{0, 1\} \) such that

\[
\frac{m}{n} \geq \frac{a_1}{2^1} + \frac{a_2}{2^2} + \cdots + \frac{a_k}{2^k}.
\]

If adding \( 1/2^{k+1} \) to the right-hand side would keep it less than or equal to \( m/n \), then set \( a_{k+1} = 1 \). Otherwise, set \( a_{k+1} = 0 \).

2. Repeat step (1) until we think we have found the period.

3. Suppose we want to confirm that the binary expansion is

\[
\frac{m}{n} = (0.a_1 \cdots a_k a_{k+1} \cdots a_l)_2
\]

\[
= \frac{a_1}{2^1} + \cdots + \frac{a_k}{2^k} + \frac{a_{k+1}}{2^{k+1}} + \cdots + \frac{a_l}{2^l} + \frac{a_{k+1}}{2^{k+1}} + \cdots + \frac{a_l}{2^l} + \cdots
\]
Let \( x = a_1/2^1 + \cdots + a_k/2^k \) and \( y = a_{k+1}/2^1 + \cdots + a_\ell/2^{\ell-k} \). Then the last expression above equals
\[
x + \frac{y}{2^k} + \frac{y}{2^{k+1}(\ell-k)} + \frac{y}{2^{k+2}(\ell-k)} + \cdots = x + \frac{y}{2^k} \left( 1 + \frac{1}{2^{\ell-k}} + \frac{1}{2^{2(\ell-k)}} + \cdots \right) = x + \frac{y/2^k}{1 - 1/2^{\ell-k}},
\]
so to finish, it suffices to check\(^1\) that
\[
\frac{m}{n} = x + \frac{y/2^k}{1 - 1/2^{\ell-k}}.
\]

When we apply the above algorithm to the specific fractions given, we obtain:
\[
\frac{1}{5} = (0.00\text{I})_2,
\]
\[
\frac{1}{7} = (0.\text{I})_2,
\]
\[
\frac{1}{11} = (0.00\text{I}01\text{I}1\text{I}0\text{I})_2,
\]
and the last of these gives
\[
\frac{2}{11} = (0.00\text{I}01\text{I}1\text{I}0\text{I})_2.
\]

(Explicitly, to check (10) for \( m/n = 2/11 \) is to check that
\[
\frac{2}{11} = \frac{1/8 + 1/32 + 1/64 + 1/128 + 1/512}{1 - 1/1024},
\]
which turns out to be true!)

**Exercise 4**

Prove that the binary expansion of any rational number \( m/n \) eventually becomes periodic and that the period length divides \( \varphi(n) \).

Without loss of generality we can assume \( 0 \leq m/n < 1 \). We must show that there exist digits \( a_1, \ldots, a_k, a_{k+1}, \ldots, a_\ell \in \{0, 1\} \) such that
\[
\frac{m}{n} = (0.a_1 \cdots a_k a_{k+1} \cdots a_\ell)_2.
\]

Following the notation of our solution to the previous problem, let
\[
X = 2^k x = 2^k - 1 a_1 + 2^{k-2} a_2 + \cdots + a_k,
\]
\[
Y = 2^{\ell-k} y = 2^{\ell-k} - 1 a_{k+1} + 2^{\ell-k-2} a_{k+2} + \cdots + a_\ell.
\]

That is, \( X = (a_1 \cdots a_k)_2 \) and \( Y = (a_{k+1} \cdots a_\ell)_2 \) in binary notation. Then giving digits \( a_1, \ldots, a_\ell \) such that (16) holds is equivalent to giving \( \ell, k \in \mathbb{N} \) and nonnegative \( X, Y \in \mathbb{Z} \), where \( X < 2^k \) and \( Y < 2^{\ell-k} \), such that (10) holds, i.e., such that
\[
\frac{m}{n} = \frac{X}{2^k} + \frac{Y}{2^{\ell-k}},
\]
or equivalently, such that
\[
(2^{\ell-k} - 2^k) m = ((2^{\ell-k} - 1) X + Y) n.
\]

\(^1\)I did not take off points if you did not show this checking step, but if you got the wrong answer, then showing work for this step would have gained you partial credit.
Recalling the definitions of $X$ and $Y$, we see
\begin{equation}
2^{\ell-k}X + Y = 2^{\ell-1}a_1 + \cdots + 2^{\ell-k}a_k + 2^{\ell-k-1}a_{k+1} + \cdots + a_\ell.
\end{equation}
This is just another binary expansion, so $2^{\ell-k}X + Y$ is a uniquely-defined nonnegative integer $Z$. We have now shown that the problem is equivalent to finding $\ell, k \in \mathbb{N}$ and nonnegative $X, Z \in \mathbb{Z}$, where $X < 2^k$ and $Z < 2^\ell$, such that
\begin{equation}
(2^{\ell-2})m = (Z - X)n.
\end{equation}
By Euler’s Theorem, $2^{\varphi(n)} - 1 \equiv 0 \pmod{n}$, i.e., there exists $d$ such that $nd = 2^{\varphi(n)} - 1$. Letting $\ell = k + \varphi(n)$, we see that $2^\ell - 2^k = 2^k nd$, so it remains to construction $k, X, Z$ such that $X < 2^k$ and $Z < 2^{\varphi(n)+k}$ and
\begin{equation}
2^kd = Z - X.
\end{equation}
Indeed, since $m < n$, we have $2^kd \leq 2^k nd = 2^k(2^{\varphi(n)} - 1) \leq 2^{k+\varphi(n)}$, meaning the construction exists. Moreover, since we were able to take $\ell = k + \varphi(n)$, we have also shown that $\varphi(n)$ is a multiple of the period length.

Reference