4. Let $a$ and $b$ be integers.

(a) Prove that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$.

If $[a]_n = [b]_n$, then $a \in [a]_n$ implies that $a \in [b]_n$, so by definition we have $a \equiv b \pmod{n}$.

Conversely, suppose that $a \equiv b \pmod{n}$. To show that $[a]_n \subseteq [b]_n$, let $x \in [a]_n$. Then by definition $x \equiv a \pmod{n}$, so our assumption that $a \equiv b \pmod{n}$, together with the transitive property of $\equiv$, implies that $x \equiv b \pmod{n}$, and thus $x \in [b]_n$. To show that $[b]_n \subseteq [a]_n$, let $x \in [b]_n$. Then $x \equiv b \pmod{n}$, and since $a \equiv b \pmod{n}$, the reflexive property for $\equiv$ shows that $b \equiv a \pmod{n}$, so that we can again use the transitive property to get $x \equiv a \pmod{n}$, and thus $x \in [a]_n$. Now since $[a]_n \subseteq [b]_n$ and $[b]_n \subseteq [a]_n$, we have $[a]_n = [b]_n$.

(b) Prove that either $[a]_n \cap [b]_n = \emptyset$ or $[a]_n = [b]_n$.

Suppose that $[a]_n \cap [b]_n \neq \emptyset$. Then there exists $c \in [a]_n$ and $c \in [b]_n$. Hence $a \equiv c \pmod{n}$ and $b \equiv c \pmod{n}$. Thus $a \equiv b \pmod{n}$, and so $[a]_n = [b]_n$.

5. Prove that each congruence class $[a]_n$ in $\mathbb{Z}_n$ has a unique representative in $\{0, 1, \ldots, n-1\}$ that satisfies $0 \leq r < n$.

Given $a \in \mathbb{Z}$ there exist $q, r \in \mathbb{Z}$ such that $a = qn + r$, with $0 \leq r < n$. Thus $a \equiv r \pmod{n}$ and $[a]_n = [r]_n$ with $0 \leq r < n$. To see that $r$ is unique, suppose that $[a]_n = [r]_n$ and $[a]_n = [s]_n$, where $0 \leq r < n$ and $0 \leq s < n$. Then $r \equiv s \pmod{n}$ and so $n|(r-s)$. Since $-n < r-s < n$ we must have $r-s = 0$ and thus $r = s$.

9. Let $(a, n) = 1$. The smallest positive integer $k$ such that $a^k \equiv 1 \pmod{n}$ is called the multiplicative order of $[a]_n$ in $\mathbb{Z}_n^\times$.

†(a) Find the multiplicative orders of $[5]$ and $[7]$ in $\mathbb{Z}_{16}^\times$.


(b) Find the multiplicative orders of $[2]$ and $[5]$ in $\mathbb{Z}_{17}^\times$.


10. Let $(a, n) = 1$. If $[a]$ has multiplicative order $k$ in $\mathbb{Z}_n^\times$, show that $k \mid \phi(n)$.

Suppose that the multiplicative order of $[a]$ is $k$. Write $\phi(n) = k \cdot q + r$, where $0 \leq r < k$. By Euler’s theorem, $[1] = [a]^\phi(n) = [a]^{kq+r} = ([a]^k)^q[a]^r = [1]^q[a]^r = [1][a]^r = [a]^r$. Since $r < k$, we must have $r = 0$, and so $k \mid \phi(n)$.

12. Generalizing Exercise 11, we say that the set of units $\mathbb{Z}_n^\times$ of $\mathbb{Z}_n$ is cyclic if it has an element of multiplicative order $\phi(n)$. Show that $\mathbb{Z}_{10}^\times$ and $\mathbb{Z}_{11}^\times$ are cyclic, but $\mathbb{Z}_{12}^\times$ is not.


We have $\phi(11) = 11(1 - \frac{1}{11}) = 10$. In $\mathbb{Z}_{11}^\times$ we have $[2]^2 = [4]$; $[2]^3 = [8]$; $[2]^4 = [5]$; $[2]^5 = [10]$. We can stop checking here, since by Exercise 10 the multiplicative order of $[2]$ must divide 10, and we have seen that $[2]$ does not have multiplicative order 1, 2 or 5. Thus the multiplicative order of $[2]$ must be 10 and so $\mathbb{Z}_{11}^\times$ is cyclic.

We have $\phi(12) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 4$. Since $\mathbb{Z}_{12}^\times = \{[1], [5], [7], [11]\}$ and $[5]^2 = [7]^2 = [11]^2 = [1]$ in $\mathbb{Z}_{12}^\times$, we see that $\mathbb{Z}_{12}^\times$ has no element of multiplicative order 4.
24. Show that if \( p \) is a prime number, then the congruence \( x^2 \equiv 1 \pmod{p} \) has only the solutions \( x \equiv 1 \) and \( x \equiv -1 \).

   If \( x^2 \equiv 1 \pmod{p} \), then \( p|(x^2 - 1) \) and so \( p|(x - 1)(x + 1) \). Hence \( p|(x - 1) \) or \( p|(x + 1) \). Thus \( x \equiv -1 \pmod{p} \) or \( x \equiv 1 \pmod{p} \).

25. Let \( a, b \) be integers, and let \( p \) be a prime number of the form \( p = 2k + 1 \). Show that if \( p \nmid a \) and \( a \equiv b^2 \pmod{p} \), then \( a^k \equiv 1 \pmod{p} \).

   Since \( p = 2k + 1 \), \( \varphi(p) = p - 1 = 2k \). Since \( a \equiv b^2 \pmod{p} \) and \( a \neq 0 \pmod{p} \), we have that \( p \nmid b \). Thus \( b^{\varphi(p)} \equiv 1 \pmod{p} \) and so \( a^k \equiv b^{2k} = b^{\varphi(p)} \equiv 1 \pmod{p} \).

27. Prove Wilson’s theorem, which states that if \( p \) is a prime number, then \( (p-1)! \equiv -1 \pmod{p} \).

   *Hint:* \( (p-1)! \) is the product of all elements of \( \mathbb{Z}_p^* \). Pair each element with its inverse, and use Exercise 24. For three special cases see Exercise 11 in Section 1.3.

   We have \( \mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\} \). If \([a]^2 = [1]\), then \([a] = [1]\) or \([a] = [-1] = [p-1]\) by Exercise 24. Thus none of \([2], [3], \ldots, [p-2]\) is its own inverse. Yet each such \([a]\) also has its inverse in this set. Hence \([2][3] \cdots [p-2] = [1]\). This shows that \((p-2)! \equiv 1 \pmod{p}\). Since \(p-1 \equiv -1 \pmod{p}\) we have \((p-1)! \equiv -1 \pmod{p}\).

3.2

2. Let \( A = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix} \in \text{GL}_2(\mathbb{R}) \). Show that \( A \) has infinite order by proving that

\[
A^n = \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix},
\]

for \( n \geq 1 \), where \( F_0 = 0 \), \( F_1 = 1 \), and \( F_{n+1} = F_n + F_{n-1} \) is the Fibonacci sequence.

Let \( A = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \). Then \( A^2 = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \), \( A^3 = \begin{bmatrix} 3 & -2 \\ -2 & 1 \end{bmatrix} \), \( A^4 = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix} \), etc.

We proceed by induction. Since \( F_2 = F_1 + F_0 = 1 + 0 = 1 \) we have \( A = \begin{bmatrix} F_2 & -F_1 \\ -F_1 & F_0 \end{bmatrix} \). Assume that

\[
A^n = \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix}.
\]

Then

\[
A^{n+1} = A \cdot A^n = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix}
\]

\[
= \begin{bmatrix} F_{n+1} + F_n & -F_n - F_{n-1} \\ -F_{n+1} & F_{n-1} \end{bmatrix}
\]

as required. Since \( F_n > 1 \) for \( n \geq 1 \), we see that \( A \) does not have finite order.

3. Prove that the set of all rational numbers of the form \( m/n \), where \( m, n \in \mathbb{Z} \) and \( n \) is square-free, is a subgroup of \( \mathbb{Q} \) (under addition).

Let \( H = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \text{ is square-free} \right\} \). Since \( 0 \in H \), we have \( H \neq \emptyset \). Let \( a, b \in H \). Then

\[
a = \frac{m_1}{n_1} \quad \text{and} \quad b = \frac{m_2}{n_2}
\]

where \( n_1, n_2 \) are square-free. Let \( n = [n_1, n_2] \) and note that \( n \) is square-free.

Write \( n = n_1k_1 \) and \( n = n_2k_2 \) for \( k_1, k_2 \in \mathbb{Z} \). Since \( a - b = \frac{m_1k_1}{n} - \frac{m_2k_2}{n} = \frac{m_1k_1 - m_2k_2}{n} \) and \( n \) is square-free, \( a - b \in H \) and \( H \) is a subgroup of \( \mathbb{Q} \).