(1) Let \(a_1, a_2, ..., a_n\) denote positive integers and let \((a_1, a_2, ..., a_n)\) denote the greatest common divisor of these \(n\) integers. In the textbook \((a_1, a_2, ..., a_n)\) was constructed inductively by

\[
(a_1, a_2, \ldots, a_2) = ((a_1, a_2, ..., a_{n-1}), a_n).
\]

Prove that \((a_1, a_2, ..., a_n)\) is equal to the smallest positive integer in the set

\[
X = \{\sum_{i=1}^{n} a_i m_i \mid m_i \in \mathbb{Z}\}.
\]

(2)
(a) Use the Euclidean algorithm to compute \((198, 210)\).
(b) Find integers \(m, n\) such that \(198m + 210n = (198, 210)\).

(3)
(a) Compute \((198, 210, 231)\).
(b) Compute \(\text{lcm}(198, 210, 231)\).

(4) Let \(p_1, p_2, p_3, ..., p_n, \ldots\) denote a list of all the prime positive integers. Let \(a, b\) denote two positive integers. By Theorem 1.3.3 we may write \(a = \prod_{i=1}^{r} p_i^{m_i}\) and \(b = \prod_{i=1}^{r} p_i^{n_i}\), for some positive integer \(r\) and for natural numbers \(m_i, n_i\).

Show that \(a \mid b\) iff \(m_i \leq n_i\) for all \(1 \leq i \leq r\).

(5) Show that if \([a]_n\) is not a zero divisor \((\text{mod } n)\) then it must be invertible \((\text{mod } n)\).

(6)
(a) Which of the following are invertible? \([18]_{23}, [15]_{25}, [36]_{73}\).
(b) For those congruence classes in part (a) which are invertible find their inverses.

(7) Let \(a, b \in \mathbb{P}\) set \(X = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}\). Show that \(X = \{(a, b)k \mid k \in \mathbb{P}\}\), where \((a, b)\) denotes the greatest common divisor of \(a, b\).

(8) Explain why the simultaneous congruence equations

\[
x \equiv 4 \pmod{11}
\]

\[
3x \equiv 5 \pmod{9}
\]

do not have a solution. Does this contradict the Chinese remainder theorem?
(9) Solve the simultaneous congruence equations
\[
\begin{align*}
    x &\equiv 4 \mod 11 \\
    3x &\equiv 6 \mod 9 \\
    10x &\equiv 15 \mod 20
\end{align*}
\]

(10) Solve the congruence equation \(60x \equiv 40 \mod 110\).

(11) Let \(m, n\) denote positive integers greater than 1, and let \(f: \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{mn}\) be the map defined by \(f([a]_m, [b]_n) = [x]_{mn}\) where \(x\) is a solution to the simultaneous congruence equations
\[
\begin{align*}
    x &\equiv a \mod m \\
    x &\equiv b \mod n
\end{align*}
\]
Then show that \(f\) is a well defined map which is an “isomorphism” of sets (i.e. \(f\) is one-one and onto).

(12) Prove or give a counter example: either some power of \([a]_n\) is equal to \([1]_n\) or some power of \([a]_n\) is equal to \([0]_n\).

(13) Compute the following powers: \(([3]_{11})^{288} = ?; ([3]_{21})^{99} = ?\)

(14)
    (a) List all of the elements in \(G_{20}\).
    (b) How many elements are in the set \(G_{1080}\)?

(15) Show that \(([25]_{1080})^{-1}\) exists; and write \(([25]_{1080})^{-1}\) in the form \(([25]_{1080})^k\) for some positive integer \(k\).