Problem 1.

Proof. (a) By unfolding the definition, \( A + B \) consists of elements only in \( A \) or only in \( B \). Then \((A + B) + C\) consists of (i) elements \( x \) that are either in \( A - B \) or \( B - A \) and not in \( C \); i.e. \( x \in A, x \notin B, x \notin C \) or elements \( x \in B, x \notin A, x \notin C \); and (ii) of elements \( x \) that are in \( C \), but not in \( A + B \). These are precisely the elements of \( C \) that are in neither \( A \) or \( B \) or in both \( A \) and \( B \).

In other words, \((A + B) + C\) consists of elements that are in one of the sets \( A, B, C \) but not in the other two; or elements that are in all three sets. This is a symmetric characterization, hence \((A + B) + C = A + (B + C)\).

(b) If \( x \in A \cdot (B + C) \), then \( x \in A \) and either \( x \in B - C \) or \( x \in C - B \). In the first case \( x \in A \cap B = A \cdot B \) and \( x \notin A \cdot C \). In the second case \( x \in A \cap C = A \cdot C \) and \( x \notin A \cdot B \). This shows \( A \cdot (B + C) \subseteq A \cdot B + A \cdot C \).

To prove that the inclusion going the other way holds, let \( x \in A \cdot B + A \cdot C \). Then either \( x \in A \cdot B - A \cdot C \) or \( x \in A \cdot C - A \cdot B \). In the first case, we have \( x \in A \cap B \) and \( x \notin (A \cap C) \). This implies \( x \in A \) and \( x \in B - C \), i.e. \( x \in A \cdot (B + C) \). The other case, similarly, implies \( x \in A \) and \( x \in C - B \), i.e. \( x \in A \cdot (B + C) \).

(c) \( A \cap A = A \).

(d) \( A + A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset \).

(e) Assume \( x \in B \). If \( x \in A \), then \( x \notin A + B \), since \( A + B \) consists of elements either in \( A \) and not in \( B \) or in \( B \) and not in \( A \). Since \( A + C = A + B \), we then have \( x \notin A + C \). Since \( x \in A \), the latter is possible only if \( x \in C \) (else \( x \in (A - C) \subset A + C \)).

Conversely, any \( x \in C \) is in \( B \). Thus \( B = C \).

\( \square \)

Problem 2.

Proof. (a) Symmetry and transitivity alone do not imply reflexivity. The typical (flawed) argument would go along the lines of: we have \( a \sim b \) and \( b \sim a \) (symmetry). Now take \( c = a \) and use transitivity, therefore \( a \sim c = a \).

In this flawed proof, the argument works only when there exists \( b \) such that \( a \sim b \). Without reflexivity, the empty relation would count as an equivalence relation, for example. Or, one can construct a relation \( R \) such that \( (a, c) \notin R \) for all \( c \), and \( R \) is an equivalence relation on \( A - \{a\} \). Then \( R \) satisfies symmetry and transitivity.

(b) \( a \sim a \) since \( f(a) = f(a) \), thus reflexivity is satisfied. Symmetry is also easy to see: if \( a \sim b \), then \( f(a) = f(b) \), hence \( f(b) = f(a) \), and thus \( b \sim a \).

Finally if \( a \sim b \) and \( b \sim c \), then \( f(a) = f(b) = f(c) \), hence \( a \sim c \). Given \( x \in B \), for any \( a, b \in f^{-1}(x) \subseteq A \) (which is nonempty, since \( f \) is surjective) we have \( a \sim b \) since \( f(a) = f(b) \), thus equivalence classes are the fibers of \( f \).

\( \square \)

Problem 3.
Proof. We say \((S, \leq)\) is a well-ordered set if it is a partial order (reflexive, antisymmetric and transitive), and every non-empty subset of \(S\) has a least element. A partially ordered set \((S; \leq)\) is said to be totally ordered if for all \(a, b \in S\), \(a \in S\) or \(a \leq b\) or \(b \leq a\).

Suppose \(S\) is well-ordered. For all \(x, y \in S\), the subset \(\{x, y\}\) of \(S\) must have a least element. So either \(x \leq y\) or \(y \leq x\). Thus \(S\) is totally ordered. \(\Box\)

Problem 4.

Proof. One can use Problem 5(b) and the formula for \(\varphi\). If \(n = p_1^{e_1} \cdots p_r^{e_r}\) and \(d|n\), then \(d = p_1^{f_1} \cdots p_r^{f_r}\) with \(0 \leq f_i \leq e_i\). Then

\[
\varphi(d) = (p_1 - 1) \cdots (p_r - 1)p_1^{f_1-1} \cdots p_r^{f_r-1}|(p_1 - 1) \cdots (p_r - 1)p_1^{e_1-1} \cdots p_r^{e_r-1} = \varphi(n),
\]

since \(f_i - 1 \leq e_i - 1\) for every \(i\). \(\Box\)

Problem 5.

Proof. (a) There are many approaches, by applying Prop 0.11 repeatedly. Assume \(n = p_1^{e_1} \cdots p_r^{e_r}\) and \(n = q_1^{f_1} \cdots q_s^{f_s}\) with \(p_i, q_j\) primes. Then \(q_s|n\), hence \(q_s|\prod p_i^{e_i}\), hence \(q_s|p_i\) for some \(i\). Without loss of generality \(q_s|p_r\). Since \(p_r\) is prime, we must have \(q_s = p_r\). One can divide \(n\) by \(q_s = p_r\) and repeat the argument for the new number \(n'\). The process stops because \(n\) always decreases, so eventually we have to hit \(n = 1\) (essentially a strong induction argument).

(b) If \(d = p_1^{f_1} \cdots p_r^{f_r}\), with \(0 \leq f_i \leq e_i\), then we have \(d \cdot \prod_{i=1}^{s} p_i^{e_i-f_i} = n\) with \(e_i - f_i \geq 0\). Hence \(d|n\).

Conversely, suppose \(d|n\). Then suppose \(d = \prod_i q_i^{s_i}\) is the unique factorization of \(d\). But we have \(n = d \cdot m\) for some integer \(m\). So using the fact that \(n\) has a unique factorization as given by the hypothesis, \(d\) has to be of the desired form. \(\Box\)

Problem 6.

Proof.

Lemma. \(((a, b), c) = (a, b, c)\).

Proof of lemma: Let \(d = ((a, b), c)\) and \(d' = (a, b, c)\). By definition \(d|(a, b)\) and \(d|c\). Then \(d|a, b, c\), hence \(d|d' = (a, b, c)\). Conversely \(d'\) divides \(a\) and \(b\), hence divides \((a, b)\). Since \(d'\) also divides \(c\), it follows that \(d'\) divides \(((a, b), c) = d\). From \(d|d'\) and \(d'|d\) we conclude that \(d = d'\). \(\Box\)

Now the problem can be shown using an easy induction. For \(r = 2\), the result was proved in class. Suppose \(d = (a_1, \ldots, a_k) = m_1a_1 + \ldots + m_ka_k\). Let \(d' = (a_1, \ldots, a_{k+1})\). Then

\[
d' = (d, a_{k+1}) = m'(m_1a_1 + \ldots + m_ka_k) + m_{k+1}a_{k+1},
\]

which proves the induction step. \(\Box\)

Problem 7.
Proof. Let $c' = c/(m, c)$. Since $ac \equiv bc \pmod{m}$, there is an integer $t$, such that $c(a-b) = mt$, or $c'(m, c)(a-b) = m'(m, c)t$, or $c'(a-b) = m't$. By basic properties of the greatest common divisor, we know that $(c', m') = 1$. We want to show that $m'|a-b$. We use Bezout's identity in the following form:

Lemma. If $m|np$ and $(m, n) = 1$, then $m|p$.

Here is a proof of the lemma: By Bezout, there are integers $x, y$ such that $mx + ny = 1$. Then $mpx + npy = p$. Clearly $m|mpx$ and by assumption $m|np|npy$. Thus $m|mpx + npy = p$, as wanted.

Problem 8.

Proof. By applying the Extended Euclidean Algorithm to compute the gcd, we get

\[
egin{align*}
147 &= 2 \cdot 64 + 19 \\
64 &= 3 \cdot 19 + 7 \\
19 &= 2 \cdot 9 + 1 \\
7 &= 1 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{align*}
\]

Hence $(147, 64) = 1$, and by using back substitution, we get $1 = (147, 64) = 147m + 64n$, where $m = 27$ and $n = -62$. Then the multiplicative inverse of 64 with respect to 147 is $x \equiv 85 \cdot 51 \equiv 72 \pmod{147}$.

Problem 9.

Proof. $\Rightarrow$ was shown in class.

Conversely, assume $\overline{ab} = \overline{0} \Rightarrow \overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$ in $\mathbb{Z}/m\mathbb{Z}$. If $m$ were not prime, we could factor it as $m = a \cdot b$ (in $\mathbb{Z}$), with $1 < a, b < m$. But then $\overline{ab} = \overline{0}$ in $\mathbb{Z}/m\mathbb{Z}$ and $\overline{a} \neq \overline{0}, \overline{b} \neq \overline{0}$, which is a contradiction.