Homework 1 AJ

1a) Consider the set $S = \{xm + yn : x, y \in \mathbb{Z}\}$.
Now consider the positive elements of S, S^+, where $S^+ = \mathbb{N} \cap S$. Since $S^+ \subseteq \mathbb{N}$, there exists a smallest element $d \in S^+$ such that

$$d = am + bn.$$

According to the Euclidean Algorithm, there exists elements $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$m = q_1 d + r_1 \quad \text{and}$$
$$n = q_2 d + r_2.$$

Consider $r_1 = r_2 = 0$. Then

$$m = q_1 d \quad \text{and}$$
$$n = q_2 d,$$

And therefore $d \mid m$ and $d \mid n$.
Assume d is not the gcd of m and n.
Then there exists $d' \in \mathbb{Z}$ such that

$$d' \mid m, \; d' \mid n, \; \text{and} \; d \mid d',$$

where $d < d'$. However, if $d' \mid m$ and $d' \mid n$ then $d' \mid (am + bn) = d' \mid d$, which is a contradiction as $d' \leq d$.
Therefore d is $\gcd(m,n)$, which means that the $\gcd(m,n)$ can be expressed as a linear combination. $\lozenge$

Homework 1 AJ

Suppose $\gcd(K,m)=1$ and $\gcd(K,n)=1$.

1b) Assume, for the sake of contradiction, that the $\gcd(K,mn)\neq 1$; there exists, therefore, a $d>1$ for which

$$d=\gcd(K,mn).$$

Therefore either $d|m$ or $d|n$, by the property that d is a divisor of mn.

Consider $d|m$: This is a contradiction because if both $d|K$ and $d|m$, then $\gcd(K,m)=d\neq 1$. Therefore $d\nmid m$.

Likewise, consider $d|n$: This is similarly a contradiction because both $d|K$ and $d|n$. Therefore $d\nmid n$ and $d\nmid mn$.

If $d\nmid mn$, then the $\gcd(K,mn)=1$ as our assumption was false. ◊

Homework 1 AJ

1c) Suppose $\gcd(k,n) = 1$ and $k \mid mn$. Assume, for the sake of contradiction, that $k \nmid n$. Since $k \mid mn$, k must divide m by the properties of integer division.

This is a contradiction, however, as both $k \mid k$ and $k \mid m$, but $\gcd(k,m) = 1$. Therefore $k \mid n$.

Homework 1 AJ

2) Let $m, n \in \mathbb{Z}$ be positive integers, $d = \gcd(m,n)$ and $L = \text{lcm}(m,n)$. Consider three cases for d:

Case $d = \gcd = 1$: If the $\gcd(m,n) = 1$ then the smallest number for which $m \mid b$ and $n \mid b$ is $m \cdot n$, as m and n share no common factors. Therefore $d = \gcd(m,n) * b = \text{lcm}(m,n) = 1 \cdot m \cdot n = m \cdot n$.

Case $d = \gcd = \min(m,n)$: If the $\gcd(m,n)$ is one of m or n, then it must be the smaller of the two as $d \mid m$ and $d \mid n$. Assume $d = \gcd(m,n) = m$. Then the smallest integer b for which $m \mid b$ and $n \mid b$ will be some multiple of m, as m is the greatest common divisor. The smallest multiple of both m and n is n, given that $m \mid n$. Therefore $\text{lcm} = n$. Therefore $d = \gcd(m,n) * b = \text{lcm}(m,n) = m \times n = m \cdot n$.

Case $d = \gcd = c$, where $1 < c < \min(m,n)$: If the $\gcd(m,n)$ is not 1, m, or n then d is some integer between 1 and m or n. The smallest integer b for which $m \mid b$ and $n \mid b$ will be some multiple of c, for which $(m/c) \mid b$ and $(n/c) \mid b$. Therefore $b = c \times (m/c) \times (n/c) = mn/c$ as (m/c) and (n/c) are both relatively prime. Therefore $d = \gcd(m,n) \times b = \text{lcm}(m,n) = c \times (mn/c) = m \cdot n$.

Therefore, for every case, $d \cdot b = m \cdot n$. $\diamond$

Homework 1 AJ

3a) Let $\sim$ be an equivalence relation on S. If $a \sim b$ where $a, b \in S$, then $a \in [b]$ and $b \in [a]$ for any two elements of S. ~~Therefore $S = \bigcup S_i$ for any element $i \in S$~~. Therefore the set of equivalence classes, A, is equal to the union of all possible relations of S. Consider $a \neq b$. Observe that $a \in [a]$, as $\sim$ is reflexive. Therefore both $a \in [a]$ and $b \in [a]$, and similarly $a \in [b]$ and $b \in [b]$. Therefore any element $x \in S$ is also $x \in A$, so that $A_i \cap A_j = \emptyset$ if $i \neq j$. Therefore A is a partition of S. $\square$

3b) Let $\{P_i\}_{i \in I}$ be a partition of S. Since $S = \bigcup P_i$, the possible relations of S, then if $x \in \{P\}$ then $x \in S$, and if $x \in S$ then $x \sim x$ which proves reflexivity. Suppose $a \sim b$: Since $a \sim a$ ~~prove~~ then $b \in [a]$ and $a \in [a]$ and since $b \sim b$ $a \in [b]$ and $b \in [b]$. Therefore, as a and b form a relation and therefore a partition of S, $\sim$ must be symmetric. Finally, consider $a \sim b$ and $b \sim c$. Since $a \in [b]$ and $b \in [b]$, and $b \in [c]$ and $c \in [c]$, then $b \in [b] \cap [c]$. Therefore the partition involving a and b must be the partition involving b and c, and so $\sim$ must be symmetric. Therefore $\sim$ is an equivalence relation for which the equivalency classes are related to partitions of S. $\square$