MATH 108 Fall 2019 - **Problem Set 4 solutions**

due October 25

1. Let $n = a_1 a_2 \cdots a_k$ with $k \geq 1$ and $a_1, a_2, \ldots, a_k$ positive integers and let p be a prime. Use Euclid's Lemma and induction on k to prove that if p divides n, then p divides a_i for some $1 \leq i \leq k$.

   Base case: Let $k = 1$ in which case $n = a_1$. If p divides n, then p divides a_1 since they are equal.

   Assume for some $k \geq 1$ that if p divides $a_1 a_2 \cdots a_k$ then p divides a_i for some $1 \leq i \leq k$. Now let $n = a_1 a_2 \cdots a_k a_{k+1}$. So n can be factored in to $a_1 a_2 \cdots a_k$ times a_{k+1}. Suppose that p divides n. By Euclid's Lemma, either p divides $a_1 a_2 \cdots a_k$ or p divides a_{k+1}. By the induction hypothesis, if p divides $a_1 a_2 \cdots a_k$ then p divides a_i for some $1 \leq i \leq k$. Therefore we can conclude that p divides a_i for some $1 \leq i \leq k+1$.

2. A positive integer n is called *square-free* if it is not divisible by any perfect square except for 1. Prove that n is square-free if and only if n is a product of distinct primes.

   Suppose n is not square-free, so k^2 divides n for some $k \geq 2$. There is a prime p that divides k, so p^2 divides n. Therefore the prime factorization of n includes p at least twice. Since the prime factorization is unique, n cannot be the product of distinct primes.

   Suppose that n is not a product of distinct primes, so there is some p that appears at least twice in the prime factorization of n. Then n is divisible by p^2, which is a perfect square that is not equal to 1, so n is not square-free.

3. For positive integers x and y, the *greatest common divisor* of x and y is the largest postive integer that divides both x and y, denoted $\gcd(x, y)$. Let a, b, c be postive integers.

   (a) Prove that $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are integers that have no common factor.

   Let $\gcd(a, b) = d$. Since d is a divisor of a, a/d is an integer, and similarly for b/d. We proceed by contradiction. Suppose that a/d and b/d have a common factor $c > 1$. Then cd divides a and also divides b. Since $cd > d$, this violates the fact that d is the largest integer that divides both a and b, which is a contradiction.

   (b) For p a prime, prove that p divides a and p divides b if and only if p divides $\gcd(a, b)$.

   Let $\gcd(a, b) = d$. Suppose that p divides d. Since d divides a and b, and divisibility is transitive, p also divides a and b.

   Suppose that p divides a and b. We have $a = dk$ and $b = dl$ for some positive integers k and l, and k and l have no common factor by part (a). By Euclid's Lemma, p divides either d or k. Similarly p divides d or l. Since k and l have no common factor, it cannot be that p divides both k and l. Either p does not divide k or p does not divide l, and in either case we can conclude that p divides d.

4. For positive integers a and b with $\gcd(a, b) = d$, prove that

$$\{as + bt \mid s, t \in \mathbb{Z}\} = d\mathbb{Z}.$$

From Problem 3, we have that a/d and b/d are integers with no common factor. By Bezout's Identity, there exist integers s, t such that $(a/d)s + (b/d)t = 1$. Multiplying both sides by d gives $as + bt = d$.

Let $S = \{as + bt \mid s, t \in \mathbb{Z}\}$. For any $x \in d\mathbb{Z}$, $x = dk$ for some intger k. Then

$$x = kd = aks + bkt$$

so $x \in S$. This proves that $S \supseteq d\mathbb{Z}$.

Let $x \in S$, so $x = as + bt$ for some integers s and t. Since d divides as and d divides bt, d must also divide x. Therefore $x \in d\mathbb{Z}$. This proves that $S \subseteq d\mathbb{Z}$.

5. For each relation, list which of the following properties it has: symmetric, antisymmetric, transitive, reflexive, irreflexive.

   (a) $\leq$ on $\mathbb{Z}$.
   Antisymmetric, transitive, reflexive.

   (b) $\neq$ on $\mathbb{Z}$.
   Symmetric, irreflexive.

   (c) $\subseteq$ on $\mathcal{P}(\mathbb{Z})$.
   Antisymmetric, transitive, reflexive.

   (d) "is the child of" on people.
   Antisymmetric, irreflexive.

   (e) $\{(1, 5), (5, 1), (1, 1)\}$ on $A = \{1, 2, 3, 4, 5\}$.
   Symmetric.

   (f) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x + y = 10\}$ on $\mathbb{Z}$.
   Symmetric.

6. Let $A = \{1, 2, 3, 4, 5\}$ and let $\sim$ be the relation on $\mathcal{P}(A)$ defined by $S \sim T$ if $|S| = |T|$.

   (a) Prove that $\sim$ is an equivalence relation.
   To prove $\sim$ is an equivalence relation we need to show it is reflexive, symmetric and transitive. For reflexivity, for any set S we have $|S| = |S|$ so $S \sim S$. For symmetry, for sets S and T if $S \sim T$ then $|S| = |T|$ and $|T| = |S|$ so $T \sim S$. For transitivity, suppose that $S \sim T$ and $T \sim R$. Then $|S| = |T| = |R|$, so $S \sim R$.

   (b) How many equivalence classes does $\sim$ have and how many elements are in each class?
   The relation has 6 equivialence classes, which consist of the sets of size 0, 1, 2, 3, 4, 5. These classes have 1, 5, 10, 10, 5, 1 elements respectively.

7. Let $\sim$ be a relation on set A with the property that for all $a \in A$, there exists $b \in A$ such that $a \sim b$. Prove that if $\sim$ is transitive and symmetric, then $\sim$ is reflexive.

   Suppose that $\sim$ is transitive and symmetric. For any $a \in A$, there exists $b \in A$ such that $a \sim b$. By symmetry, $b \sim a$. By transitivity, since $a \sim b$ and $b \sim a$, we have $a \sim a$. Therefore $\sim$ is reflexive.