Discussion Solutions 2

Problem One: Prime Numbers

Theorem: Every natural number greater than one can be written as the product of primes.

Proof: By complete induction. Let $P(n)$ be "n can be written as the product of primes." We will prove $P(n)$ holds for all $n \geq 2$.

As a base case, we need to show $P(2)$, that 2 can be written as the product of primes. Since 2 is prime, it is the product of just itself.

For the inductive step, assume for some $n \geq 2$ that $P(0)$, $P(1)$, …, $P(n)$ hold. This means that for any n' in the range $2 \leq n' \leq n$, that n' can be written as a product of primes. We want to prove $P(n+1)$, that $n+1$ can be written as the product of primes. If $n+1$ is prime, then it is the product of just itself. Otherwise, $n+1$ is composite, so it can be written as $r \cdot s$ for some natural numbers $r > 1$ and $s > 1$. Since $r > 1$ and $s > 1$, we know $r \geq 2$ and $s \geq 2$. Since $2 \leq r < n+1$ and $2 \leq s < n + 1$, by our inductive hypothesis r and s can be written as the product of primes. Thus the product of the two sets of primes is equal to $rs = n + 1$, so n is the product of primes. Thus $P(n+1)$ is true, completing the induction. ■

Why we asked this question: Notice how complete induction is employed to its fullest here. A normal induction couldn't correctly conclude that r and s are the products of primes, since they could be much smaller than n. However, since we're using complete induction, any natural number between 2 inclusive and n exclusive is assumed to be the product of primes.

Looking beyond: This proof is one of the two parts of the *fundamental theorem of arithmetic* (FTA), which says that any natural number greater than one can be written *uniquely* as the product of primes. It is a cornerstone of number theory and is often used as a first example when discussing complete induction. In order to show that the representation is unique, you need another lemma called *Euclid's lemma*, which says that if a prime number divides some product mn, then either that prime divides m or it divides n.

Problem Two: Picking Coins

Theorem: If this game is played with the pile containing $11n$ coins for some natural number n, the second player can always win the game.

Proof: By induction. Let $P(n)$ be "if the game is played with the pile containing n coins, the second player can always win." We show that $P(n)$ holds for all natural numbers n that are multiples of 11.

As a base case, we need to prove $P(0)$, that if the game is played with a pile containing 0 coins, the second player always can win. This is true because there are no coins in the pile when the game starts, and so the second player wins because the first player loses.

For the inductive step, assume that for some $n \in \mathbb{N}$, $P(n)$ holds and if the game is played with n coins, the second player can always win. We need to show $P(n + 11)$ holds: the second player can always win in a game with $n + 11$ coins. To do this, consider the first player's move, which must remove k coins from the pile, where $1 \leq k \leq 10$. This leaves $n + 11 - k$ coins remaining. The second player can then remove $11 - k$ coins from the pile. This leaves $n + 11 - k - (11 - k) = n$ coins, and it's now the first player's turn again. By the inductive hypothesis, this means that the second player can force a win in this situation, so the second player will eventually win the game. Consequently, starting with $n + 11$ coins, the second player can win, so $P(n + 11)$ holds, completing the induction. ■

Why we asked this question: Notice how this proof works by explicitly stating the second player's strategy, which is to make the total number of coins removed by her move and the first player's move come out to 11. This enables the inductive hypothesis to guarantee that the strategy can then force a win from the previous multiple of eleven. When proving that a certain player can win a game given some setup, a common technique is to see if that player can react to the first player's turn in a way that reduces the game to a case that is already known to be solved.

Additionally, notice that the proof uses induction with a step size other than one. In this case, our induction takes steps of size 11. It's not necessary to do this. The induction could also take steps of size one if we redefine $P(n)$ to be

"if the game is played with a pile of $11n$ coins, the
second player can always win if she plays correctly."

Looking beyond: The technique employed here, in which we use inductive reasoning to prove that a player has a certain strategy, can be generalized to a technique called *backwards induction*, which reasons about a situation by considering the very last action and then working backwards to see how each player would try to make that action work in their favor.

Problem Three: Factorials! Multiplied together!

Theorem: For any $m, n \in \mathbb{N}$, that $m!n! \le (m + n)!$

Proof: By induction on n. Let $P(n)$ be "for any $m \in \mathbb{N}$, $m!n! \le (m+n)!$." We will prove $P(n)$ holds for all $n \in \mathbb{N}$.

For our base case, we prove $P(0)$, that for any $m \in \mathbb{N}$, $m!0! \le (m + 0)!$. Note that

$$m!0! = m! \cdot 1 = m! = (m + 0)!$$

Therefore, $m!0! \le (m + 0)!$.

For our inductive step, assume that for some $n \in \mathbb{N}$ that $P(n)$ holds, so for any $m \in \mathbb{N}$, we have $m!n! \le (m+n)!$. We will prove $P(n)$, that for any $m \in \mathbb{N}$, we have $m!(n+1)! \le (m+n+1)!$ To do this, note that for any $m \in \mathbb{N}$, we have

$$m!(n+1)! = m!n!(n+1) \le (m+n)!(n+1) \le (m+n)!(m+n+1) = (m+n+1)!$$

Thus $P(n+1)$ holds, completing the induction. ■

Intuitively, notice that $m!n! = 1 \cdot 2 \cdot \ldots \cdot m \cdot 1 \cdot 2 \cdot \ldots \cdot n$. This quantity should be no greater than the quantity $1 \cdot 2 \cdot \ldots \cdot m \cdot (m+1) \cdot (m+2) \cdot \ldots \cdot (m+n)$. The induction formalizes this reasoning.

Why we asked this question: Notice how our property $P(n)$ internally ranges over all possible choices of m. It is often possible to do induction on claims involving multiple variables by doing normal induction on just one variable and proving the claim is true for the remaining variables as normal.

Looking beyond: This style of induction (where we do induction on one variable and use a proof of the form "pick an arbitrary..." on another) is quite common when working with multiple variables. We hope this example gives some guidance on how to structure those sorts of proofs.