

Header styling inspired by CS 70: <https://www.eecs70.org/>

Problem 1

Problem 2

Let R be a binary predicate such that the following are true:

$$(1) \forall x \forall y (R(x, y) \implies R(y, x))$$

$$(2) \exists x \forall y R(x, y)$$

a) Prove or disprove whether the following are logically implied by the conditions (1) and (2).

$$\text{i) } \forall x \exists y R(x, y)$$

Solution: This is logically implied. From (2), we know that there exists some a such that $R(a, y)$ for all y , and (1) requires that $R(a, y) \implies R(y, a)$, so we know there exists some a such that $R(y, a)$ for all y . This is precisely the statement $\forall x \exists y R(x, y)$, up to variable names. \square

$$\text{ii) } \forall x R(x, x)$$

Solution: This is not logically implied. Part (i) only implies the *existence* of a y such that $\forall x R(x, y)$, but it does not make the claim that $y = x$ always, a necessary condition to guarantee that $\forall x R(x, x)$ is implied. \square

$$\text{iii) } \exists y \forall x R(x, y)$$

Solution: This is logically implied, just swap variable names. \square

$$\text{iv) } \forall x \forall y (R(x, y) \vee R(y, x))$$

Solution: From statement (i), we know that $\forall x$, there *exists* a y such that $R(x, y)$ and condition (1) means that $R(y, x)$ is true as well. However, this does not imply that such an x works such that *all* values of y satisfy $R(y, x)$, hence this is not logically implied. \square

b) Consider the natural numbers with the binary predicate $R(x, y)$ as “ $x \cdot y = 0$ ”.

i) Check that the conditions (1) and (2) are true of R in this setting.

Solution: Condition (1) is true because multiplication is commutative, and select $x = 0$ to satisfy condition (2). \square

ii) Translate conditions (1) and (2), when applied to this setting, into simple English sentences.

Solution: See below

1. For all x, y , if the product $x \cdot y = 0$, then $y \cdot x = 0$
2. There exists a value of x such that for all values of y , $x \cdot y = 0$.

\square

Problem 3

In this problem, we will prove the fundamental theorem of arithmetic: any integer $n \geq 2$ can be factorized as a product of powers of its prime factors. That is, for any integer $n \geq 2$, we can write

$$n = p_1^{q_1} p_2^{q_2} \cdots p_m^{q_m}$$

where p_1, \dots, p_m are prime numbers and q_1, \dots, q_m are positive integers.

- a) We first consider the case where n is prime. Show that the fundamental theorem of arithmetic holds when n itself is a prime number.

Solution: Since n is prime, then $n = p$, which is clearly satisfied. □

- b) Now we consider the case when n is not prime: that is, n is composite. By the definition of a composite number, there exists a positive integer d such that $d \mid n$ and $1 < d < n$. We call d a *nontrivial divisor* of n .

Prove that if d and n/d can be factorized as a product of powers of its prime factors, then n can also be factorized as a product of powers of its prime factors.

Solution: Here we leverage the fact that $d \cdot \frac{n}{d} = n$, so let $d = p_1^{q_1} \cdots p_m^{q_m}$, and $n/d = p_1^{r_1} \cdots p_m^{r_m}$. To make this definition work, we will choose p_m large enough such that the largest prime factor between both numbers is equal to p_m . Consequently, we must allow for the possibility that $q_i = 0$ and $r_i = 0$. Then, the product can be expressed as follows:

$$d \cdot \frac{n}{d} = n = p_1^{q_1+r_1} \cdots p_m^{q_m+r_m}$$

which is of the desired form. □

- c) Using induction and the two parts above, prove the fundamental theorem of arithmetic.

Solution: Base case: $n = 2^1$, which is prime, so we are done.

Inductive hypothesis: For all values less than k , the proposition holds true.

Inductive step: for $k + 1$, we know that it is either prime or composite. If $k + 1$ is prime, then we are immediately done, and if $k + 1$ is composite, then we know it can be written in the desired form based on part (b).

The inductive step holds, and we are done. □

¹We skip $n = 1$ since 1 is neither prime nor composite.