

Review of proof concepts

(Hypothesis, conclusion, etc.)

Here are some theorems and proofs that we did in class. For each, I ask several questions about the structure of the proof.

Lemma If N is composite then N has a prime factor $\leq \sqrt{N}$

Proof: (1) Since N is composite, there are integers $A, B > 1$ such that $AB = N$

(2) Without loss of generality (WOLG), $A \leq B$

(3) For some prime p , $p|A$

(4) $p \leq A$

(5) $p \leq B$

(6) $p^2 \leq AB$

(7) $p^2 \leq N$

(8) $p \leq \sqrt{N}$

(9) But also $p|A$ and $A|N$ so $p|N$ (which completes the proof)

...

Questions:

(1) Which of the following statements are *hypotheses* of the Lemma, which are *conclusions*, and which are neither?

- a) p is prime
- b) N has a prime factor
- c) N is composite
- d) N has a prime factor $\leq \sqrt{N}$

(2) For each of the numbered lines of the proof, indicate whether (a) it is a hypothesis, (b) it follows from earlier lines by basic rules of arithmetic, (c) it follows from earlier lines by a fact we've proved in class or the text, (d) It follows from the definition of a term, or (e) None of the above.

Lemma $\sqrt{2}$ is irrational (that is, it can *not* be written as a fraction p/q with $p, q \in \mathbb{Z}$)

Proof: (1) Suppose that $\sqrt{2}$ is rational.

- (2) there exist integers m and n such that $\sqrt{2} = \frac{m}{n}$.
- (3) Without loss of generality, m and n have no common factors.
- (4) $n\sqrt{2} = m$
- (5) Squaring, $2n^2 = m^2$
- (6) Therefore $2|m^2$
- (7) So $2|m$
- (8) $\exists k (m = 2k)$
- (9) $2n^2 = (2k)^2$, so $2n^2 = 4(k^2)$, so $n^2 = 2k^2$
- (10) So $2|n$
- (11) Since also $2|m$, this contradicts the assumption (3), completing the proof.

...

Questions:

- (1) As the theorem is stated, it is not obvious what the hypothesis and conclusion are. Which of the following is an equivalent formulation? For the correct formulation, state the hypothesis and the conclusion.
 - a) If $\sqrt{2}$ is rational then it equals m/n for some integers m and n .
 - b) For any number r , if $\sqrt{2} \neq r$ then r is rational.
 - c) If r is a rational number then $\sqrt{2} \neq r$
- (2) The last line of the proof claims to complete the proof. Why is this claim true? (Hint: What kind of proof is this?)
- (3) For each of the numbered lines of the proof, indicate whether (a) it follows from earlier lines by basic rules of arithmetic, (b) it follows from earlier lines by a fact we've proved in class or the text, (c) It follows from the definition of a term, or (d) None of the above.

Lemma (Division Algorithm) Suppose a and d are positive integers; then there are $k, r \in \mathbb{N}$ such that $a = kd + r$ and $0 \leq r < d$

Proof: (1) *Some* multiple of d must larger than a ; let $k + 1$ be the least such multiple.

(2) Then $kd \leq a < (k + 1)d$. (Note: This is shorthand for “ $kd \leq a$ and $a < (k + 1)d$ ”)

(3) Then $0 \leq a - kd$ and $a - kd < (k + 1)d - kd$

(4) $(k + 1)d - kd = kd + d - kd = d$, so $a - kd < d$

(5) Let $r = a - kd$

(6) $0 \leq r < d$

...

Questions:

- (1) Which of the following statements are *hypotheses* of the Lemma, which are *conclusions*, and which are neither?
- a) a is a positive integer
 - b) a has a prime factor
 - c) there are $k, r \in \mathbb{N}$ such that $a = kd + r$
 - d) d is a positive integer
- (2) For each of the numbered lines of the proof, indicate whether (a) it follows from earlier lines by basic rules of arithmetic, (b) it follows from earlier lines by a fact we’ve proved in class or the text, (c) It follows from the definition of a term, or (d) None of the above.