

General Comments

- Staple your homework.
- Write neatly and use paragraphs and spacing to help make your proofs more legible.
- State the problem you are proving. This will help you to identify the correct assumptions for the problem.
- If you are proving something by contradiction, tell me so that I know you know what you're doing.
- Get in the habit of citing theorems (by number) that you use. This will become more important later when there are lots of things that we have proven.
- There are multiple ways to prove many of these problems. For some problems, I might write up multiple proofs to reflect the multiple ways you tried to prove it.
- Take the time to rewrite what is done in section and re-present it as a full proof. In section, I do not proceed linearly through the proof in the most elegant form. I do this because when you actually try to solve these problems, the answer does not always magically fall out of the sky on your first try.
- If in doubt about your presentation, talk to me and I'll help you through it.

Selected Solutions

Sect 1.2, Misc #1: Show that if n is composite then there exists a prime $p \leq \sqrt{n}$ such that $p|n$.

First Proof: Suppose by contradiction that there does not exist a prime $p \leq \sqrt{n}$ such that $p|n$. In other words, suppose that if $p|n$ then $p > \sqrt{n}$. Since n is composite, we can write $n = p \cdot a$ where $p < n$ is a prime and $a > 1$ is an integer. By our assumption, we know that $p > \sqrt{n}$.

We can write $a = q \cdot b$ where $q \leq a$ is a prime and $b \geq 1$ is an integer. Since $n = p \cdot a$, we have that $a|n$. We have $q|a$ and $a|n$, so it follows that $q|n$ (by Theorem 1.3). By our assumption, $q > \sqrt{n}$. But then we have

$$n = p \cdot a = p \cdot q \cdot b > \sqrt{n} \cdot \sqrt{n} \cdot 1 = n,$$

which is a contradiction. Therefore, there must exist a prime $p \leq \sqrt{n}$ such that $p|n$.

Second Proof: Since n is composite, we can write $n = p \cdot a$ where $p < n$ is a prime and $a > 1$ is an integer. If $p \leq \sqrt{n}$, then we are done. If not, then $p > \sqrt{n}$. In this case, $n = p \cdot a > \sqrt{n} \cdot a$ so that $a < \sqrt{n}$. There exists a prime q such that $q|a$ (by Theorem 1.5). Notice that $n = p \cdot a$ so that $a|n$. Since $q|a$ and $a|n$, it follows that $q|n$. But notice that $q \leq a < \sqrt{n}$, therefore we have a prime $q \leq \sqrt{n}$ such that $q|n$.

Comments: When proving by contradiction, make sure you understand the structure of the assumption. The problem is stated in the form “if P then Q”, where P is “ n is composite” and Q

is “there exists a prime $p \leq \sqrt{n}$ such that $p|n$.” In a proof by contradiction, you suppose that Q is false, in other words that “there DOES NOT EXIST a prime $p \leq \sqrt{n}$ such that $p|n$.” The structure of the proof is then “if P and NOT Q then we get a contradiction.” Several students misstated this hypothesis and ended up with very wrong solutions as a result. For example, “Suppose by contradiction that if n is a composite then there does not exist a prime $p \leq \sqrt{n}$ such that $p|n$.” Do you see why this is wrong?

Sect 1.2, Misc #7: Show that if $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, then n is either prime or a product of two primes.

First Proof: Suppose by contradiction that n is neither prime nor the product of two primes. Then n must be the product of three or more primes. Write $n = p_1 \cdot p_2 \cdot p_3 \cdot a$ where the p_i , $i = 1, 2, 3$, are prime and $a \geq 1$ is an integer. There are no primes $p \leq \sqrt[3]{n}$ such that $p|n$ and each p_i divides n , so we must have $p_i > \sqrt[3]{n}$. But then we have

$$n = p_1 \cdot p_2 \cdot p_3 \cdot a > \sqrt[3]{n} \cdot \sqrt[3]{n} \cdot \sqrt[3]{n} \cdot 1 = n,$$

which is a contradiction. Therefore, n must be a prime or the product of two primes.

Second Proof: If n is prime, then we are done.

Suppose that n is not prime. Then we can write $n = p \cdot a$ where $p < n$ is a prime and $a > 1$ is an integer. If a is prime, then n is the product of two primes and we are done.

Suppose that a is not prime. We should get a contradiction since $n = p \cdot a$ would be the product of three or more primes. We can write $a = q \cdot b$ where $q < a$ is a prime and $b > 1$ is an integer. Notice that $n = p \cdot a = p \cdot q \cdot b$ so that both $p|n$ and $q|n$. By hypothesis, this implies that $p > \sqrt[3]{n}$ and $q > \sqrt[3]{n}$. Therefore, $n = p \cdot q \cdot b > \sqrt[3]{n^2} \cdot b$, which is the same as $b < \sqrt[3]{n}$. There is some prime $r|b$ (by theorem 1.5). Since $r|b$ and $b|n$, we must also have that $r|n$. By hypothesis, this implies that $r > \sqrt[3]{n}$. But we also have $r \leq b < \sqrt[3]{n}$, so this is a contradiction. Therefore, a must be prime, and this completes the proof.

Sect 1.2, Misc #8: Let p and q (with $p < q$) be consecutive odd primes. Show that every factorization of $p + q$ into primes involves at least three primes.

Proof: Since p and q are odd, $p + q$ is even. Therefore, $2|p + q$, which gives us our first prime.

It is sufficient to show that $(p + q)/2$ is not prime, for then $(p + q)/2$ would involve at least two primes, so that $2 \cdot (p + q)/2$ would involve at least three primes. Since p and q are consecutive primes, for any integer n such that $p < n < q$, it must be the case that n is not prime. But $(p + q)/2$ is an integer satisfying $p < (p + q)/2 < q$, so it is not prime.

Web Problem #1a: Using mathematical induction, show that for all integers $n \geq 1$,

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2} \right)^2.$$

Proof: We will prove this using the first principle of mathematical induction.

Base case, $n = 1$:

$$1^3 = 1 \text{ and } \left(\frac{1(1+1)}{2}\right)^2 = 1^2 = 1,$$

so the base case is true.

Inductive step: Suppose that

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

We want to show that

$$1^3 + 2^3 + \cdots + (n+1)^3 = \left(\frac{(n+1)((n+1)+1)}{2}\right)^2.$$

We perform a series of calculations:

$$\begin{aligned} (1^3 + 2^3 + \cdots + n^3) + (n+1)^3 &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3, \text{ by the inductive hypothesis} \\ &= \frac{(n+1)^2}{2^2} (n^2 + 4(n+1)) \\ &= \frac{(n+1)^2(n+2)^2}{2^2}, \end{aligned}$$

which is what we wanted to prove for the inductive step. Therefore, by the first principle of mathematical induction, for all integers $n \geq 1$,

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Comments: When proving statements using mathematical induction, make sure you conclude your proof by stating what it is that you proved. Some of your proofs ended on a statement similar to "... and since $(n+1)^2 = (n+1)^2$, we're done." Done with what?

Also, make sure you know what it is you're actually proving with induction. We are trying to prove infinitely many statements, corresponding to $n \geq 1$. What are those statements?

$$\begin{aligned} 1^3 &= \left(\frac{1(1+1)}{2}\right)^2 & n = 1 \\ 1^3 + 2^3 &= \left(\frac{2(2+1)}{2}\right)^2 & n = 2 \\ 1^3 + 2^3 + 3^3 &= \left(\frac{3(3+1)}{2}\right)^2 & n = 3 \\ &\vdots & \end{aligned}$$

Then for each $n \geq 1$, P_n is the statement

$$1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

You could write this as

$$P_n : 1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Here are a few examples of what you should NOT write:

$$P_n = 1^3 + 2^3 + \dots + n^3$$

(P_n is not a formula, it is a (mathematical) sentence. It makes no sense to ask whether “ $1^3 + 2^3 + \dots + n^3$ ” is true.)

$$P_n = 1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

(This still says P_n is a formula. Do you see why?)

$$P_n : 1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2, \text{ for all } n \geq 1.$$

(Besides being self-referential, this says that P_n itself is a collection of infinitely many statements.)

Web Problem #4: Assuming the result in Web Problem #3, show that if n is of the form $8k + 7$, then one cannot find integers x, y, z such that

$$n = x^2 + y^2 + z^2.$$

Proof: Since n is odd, there are two cases to consider:

- All of x, y, z are odd.
- One of x, y, z is odd and the others are even.

In the first case, from Web Problem #3 we can write $x^2 = 8a + 1$, $y^2 = 8b + 1$, and $z^2 = 8c + 1$. Then we have

$$x^2 + y^2 + z^2 = (8a + 1) + (8b + 1) + (8c + 1) = 8(a + b + c) + 3 = 8d + 3.$$

But n is supposed to be of the form $8k + 7$. These two statements are incompatible, x, y, z cannot all be odd.

In the second case, without loss of generality we can write $x^2 = 8a + 1$, $y^2 = 4b$, and $z^2 = 4c$. Then we have

$$x^2 + y^2 + z^2 = (8a + 1) + 4b + 4c = 4(2a + b + c) + 1.$$

But n is supposed to be of the form $8k + 7$, which is of the form $4k' + 3$. This is a contradiction, so we cannot have one odd and two evens.

Since there are no more possibilities, it must be impossible to find integers x, y, z such that $n = x^2 + y^2 + z^2$ when n is of the form $8k + 7$.

Comments: A lot of you ended up using the same letter in multiple different ways. For example: $x^2 = 8k + 1$, $y^2 = 8k + 1$, and $z^2 = 8k + 1$. This would say that x, y, z are all the same number! You should use new symbols whenever you have a new variable which you cannot control.

So how can I get away with using a, b, c twice? Notice the extent of these symbols. I use them once in each separate case and there is nothing carried over going from the first to the second. In a sense, those variables are wiped clean once I leave the first case (programmers understand this well).