

General Comments

- **Staple your homework.**
- **Write neatly.**

Selected Solutions

Sect 2.2, Ex #14: How many zeros are there at the end of 100!?

Proof: To get a zero at the end of a number, it needs to be a multiple of $10 = 2 \cdot 5$. Each time we have a pair of 2 and 5, we get another zero at the end. Here are two methods of counting the prime factors.

Method 1: We will first count the factors of 2. Every even number contributes at least one factor of 2. Every multiple of 4 contributes at least two factors of 2. Continuing in this manner, every multiple of 2^n contributes at least n factors of 2. We are interested in the exact number, not just “at least” a certain number. Using this counting scheme, every number is counted exactly as many times as the number of factors of 2. If we write $m = 2^n \cdot a$, where a is odd, then m is counted n times, as a multiple of 2, 4, 8, \dots , 2^n . (For example, $24 = 2^3 \cdot 3$ is counted three times: As a factor of 2, of 4, and of 8.)

The number of multiples of n less than or equal to m is given by $\lfloor m/n \rfloor$. So we can count the number of factors of two:

$$\begin{aligned} \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor + \left\lfloor \frac{100}{128} \right\rfloor + \dots \\ = 50 + 25 + 12 + 6 + 3 + 1 + 0 + \dots = 97 \end{aligned}$$

Similarly, we can count the number of factors of five:

$$\left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor + \left\lfloor \frac{100}{125} \right\rfloor + \dots = 20 + 4 + 0 + \dots = 24$$

So there will be 24 zeros at the end of 100!.

Method 2: This method is more “brute force” than the previous one. We’re going to count the factors by rearranging the terms. Counting the factors of 2:

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots 100 &= (2 \cdot 4 \cdot 6 \cdots 100) \cdot (\text{odd numbers}) \\ &= ((2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdots (2 \cdot 50)) \cdot (\text{odd numbers}) \\ &= 2^{50} \cdot (1 \cdot 2 \cdot 3 \cdots 50) \cdot (\text{odd numbers}) \\ &= 2^{50} \cdot (2 \cdot 4 \cdot 6 \cdots 50) \cdot (\text{more odd numbers}) \\ &= 2^{50} \cdot 2^{25} \cdot (1 \cdot 2 \cdot 3 \cdots 25) \cdot (\text{more odd numbers}) \\ &= \dots \\ &= 2^{50} \cdot 2^{25} \cdot 2^{12} \cdot 2^6 \cdot 2^3 \cdot 2^1 \cdot (\text{lots of odd numbers}) \\ &= 2^{97} \cdot (\text{large odd number}) \end{aligned}$$

Counting the factors of 5:

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots 100 &= (5 \cdot 10 \cdot 15 \cdots 100) \cdot (\text{other terms}) \\ &= 5^{20} \cdot (1 \cdot 2 \cdot 3 \cdots 20) \cdot (\text{other terms}) \\ &= 5^{20} \cdot 5^4 \cdot (\text{other terms}) \\ &= 5^{24} \cdot (\text{other terms}) \end{aligned}$$

So there are 24 zeros at the end of $100!$.

Comments:

- It is not enough to just copy down what I write in section. You need to explain the process on your homework, as if you were explaining it to someone who missed section.
- I know that I said “intuitively” in section. I also explained that intuition is not enough to justify anything, but that it does help you figure out what’s going on. Read pages 5-8 in the introduction about things that might seem to be true. You should never use “intuition” in a proof.
- Examples are nice for building understanding, but they are not needed in your proofs.

Web Problem #3a: If a and b are two non-zero integers, consider the set

$$S = \{c \text{ positive: } a|c, b|c\}.$$

Why does this set have a smallest element? (We denote this element by $LCM(a, b)$.)

Proof: S is a set of positive integers, so if we can show that it is non-empty, the well ordering principle will guarantee us a smallest element. The number $|ab|$ is in the set because it is positive, and clearly both a and b divide it.

Web Problem #3b: Show that if c is such that $a|c$ and $b|c$, then $LCM(a, b)$ divides c .

Proof: For convenience, we will let $d = LCM(a, b)$. Applying the division algorithm to c and d , we get

$$c = q \cdot d + r, 0 \leq r < d.$$

From this, we see that if $r = 0$, then $c = q \cdot d$ and $d = LCM(a, b)$ divides c as required.

Suppose that $r > 0$. Then $r = c - q \cdot d$. We are given that $a|c$ and by definition we have $a|d$, so a divides $c - q \cdot d = r$ (Theorem 1.2). By identical reasoning, b divides r . So we have

$$r \in S = \{n \text{ positive: } a|n, b|n\}.$$

By definition, d is the smallest element in S , so $r \geq d$. But from the division algorithm, $r < d$. This is a contradiction, so we cannot have $r > 0$. The only option left is $r = 0$, and we have shown that this gives the desired result.

Comments:

- Most of you did not cite Theorem 1.2 in your proofs.
- Make sure you tell me that you've got a contradiction when you get there. This is how I know you know what you're doing.

Web Problem #4a: We showed in class that if p is prime, then $p|ab \implies p|a$ or $p|b$. Using mathematical induction, show that if p is prime, then

$$p|a_1a_2 \cdots a_k \implies p|a_i \text{ for some } 1 \leq i \leq k.$$

Proof: Using the second principle of mathematical induction, suppose that for $2 < n < k$, if p is prime then

$$p|a_1a_2 \cdots a_n \implies p|a_i \text{ for some } 1 \leq i \leq n.$$

We want to show that

$$p|a_1a_2 \cdots a_k \implies p|a_i \text{ for some } 1 \leq i \leq k.$$

Notice that $a_1a_2 \cdots a_k = (a_1a_2 \cdots a_{k-1})a_k$. We have written this term as a product of two numbers, so by applying the result from class, we have that $p|(a_1a_2 \cdots a_{k-1})$ or $p|k$. By the inductive hypothesis (or possibly by the result proven in class), the first condition implies that $p|a_i$ for some $1 \leq i \leq k-1$. Putting these statements together, we get

$$p|a_1a_2 \cdots a_k \implies p|a_i \text{ for some } 1 \leq i \leq k.$$

By induction, for any k ,

$$p|a_1a_2 \cdots a_k \implies p|a_i \text{ for some } 1 \leq i \leq k.$$

Comments: There are some very subtle technical things going on here. Here is the statement P_k :

$$P_k : p|a_1a_2 \cdots a_k \implies p|a_i \text{ for some } 1 \leq i \leq k.$$

If you used the first principle of mathematical induction and your base case was $k = 2$, then you run into a little problem. In the inductive step, you assume P_k is true and try to prove P_{k+1} is true. However, in the step when you break up the product into two pieces, you need to use P_2 to make it work. However, you are not assuming P_2 is true anymore, so you should not be using it. (Notice that P_2 isn't even part of the induction step using the second principle.)

There are few ways around this. The first one is to just make the base case $k = 3$ so that you don't include $k = 2$ as part of the induction. This gives you the freedom to use this proven fact in your proof without messing up the induction. Another option is to go through the steps of the proof of the $k = 2$ case in the inductive step, so that you're not assuming the P_2 case. The third option is a little silly: Write

$$a_1a_2 \cdots a_k = (a_1a_2 \cdots a_{k-1}) \cdot a_k \cdot \underbrace{1 \cdots 1}_{k-3}$$

to get yourself a product of $k-1$ terms. This allows you to use the inductive hypothesis because the length of the product is correct.

If you understand this, then you probably understand induction very well. If you don't understand this, then you may not understand it as well as you think you do.