Fundamental theorem proof

Theorem: Every positive integer *greater than 1* is a product of (one or more) primes.

Before we prove, let's try some examples:

```
20 = 100 =
```

5 =

Proof by strong induction, with b = 2 and j = 0.

Basis step: WTS property is true about 2.

Since 2 is itself prime, it is already written as a product of (one) prime.

Recursive step: Consider an arbitrary integer $n \geq 2$. Assume (as the strong induction hypothesis, IH) that the property is true about each of $2, \ldots, n$. WTS that the property is true about n + 1: We want to show that n + 1 can be written as a product of primes. Notice that n + 1 is itself prime or it is composite.

Case 1: assume n + 1 is prime and then immediately it is written as a product of (one) prime so we are done.

Case 2: assume that n + 1 is composite so there are integers x and y where n + 1 = xy and each of them is between 2 and n (inclusive). Therefore, the induction hypothesis applies to each of x and y so each of these factors of n + 1 can be written as a product of primes. Multiplying these products together, we get a product of primes that gives n + 1, as required.

Since both cases give the necessary conclusion, the proof by cases for the recursive step is complete.

Least greatest proofs

| For a set of numbers X , how do you formalize "there is a greatest X " or "there is a least X "? |
|--|
| Prove or disprove: There is a least prime number. |
| |
| Prove or disprove: There is a greatest integer. |
| Approach 1, De Morgan's and universal generalization: |
| 11pprodest 1, 20 11organo and anticoreal generalization. |
| |
| |
| |
| Approach 2, proof by contradiction: |
| |
| |
| |
| |
| |
| |
| |
| Extra examples: Prove or disprove that \mathbb{N} , \mathbb{Q} each have a least and a greatest element. |
| |
| |

Gcd definition



Gcd examples

Why do we restrict to the situation where a and b are not both zero?

Calculate gcd((10, 15))

Calculate gcd((10, 20))

Gcd basic claims

| Claim : For any integers a, b (not both zero), $gcd((a, b)) \ge 1$. |
|---|
|---|

Proof: Show that 1 is a common factor of any two integers, so since the gcd is the greatest common factor it is greater than or equal to any common factor.

Claim: For any positive integers a,b, gcd((a,b) $) \leq a$ and gcd((a,b) $) \leq b$.

Proof Using the definition of gcd and the fact that factors of a positive integer are less than or equal to that integer.

Claim: For any positive integers a, b, if a divides b then gcd((a, b)) = a.

Proof Using previous claim and definition of gcd.

Claim: For any positive integers a, b, c, if there is some integer q such that a = bq + c,

$$\gcd(\ (a,b)\)=\gcd(\ (b,c)\)$$

| Proof Pr | ove that | t ann co | nm m on | divisor | of a h | dividee | c and | that and | ı commo | n diviso | r of h | divides a | , |
|----------|----------|----------|---------|-----------------|------------|---------|-------|----------|---------|----------|------------------|-----------|------------|
| 1100117 | ove mai | any co | mmon | <i>aivi</i> sor | $o_j a, o$ | aiviaes | c ana | inai ang | , commo | n aiviso | <i>r 0, 0, c</i> | aiviaes a | , . |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

Gcd lemma relatively prime

Lemma: For any integers p,q (not both zero), $\gcd\left(\left(\frac{p}{\gcd((p,q))},\frac{q}{\gcd((p,q))}\right)\right)=1$. In other words, can reduce to relatively prime integers by dividing by \gcd .

Proof:

Let x be arbitrary positive integer and assume that x is a factor of each of $\frac{p}{\gcd((p,q))}$ and $\frac{q}{\gcd((p,q))}$. This gives integers α , β such that

$$\alpha x = \frac{p}{\gcd((p,q))}$$
 $\beta x = \frac{q}{\gcd((p,q))}$

Multiplying both sides by the denominator in the RHS:

$$\alpha x \cdot gcd((p,q)) = p$$
 $\beta x \cdot gcd((p,q)) = q$

In other words, $x \cdot gcd(p,q)$ is a common divisor of p,q. By definition of gcd, this means

$$x \cdot gcd((p,q)) \le gcd((p,q))$$

and since $\gcd(\ (p,q)\)$ is positive, this means, $x\leq 1.$