

Announcements

1) Notes available under
"Resources" on CTools

2) Introductions

Notation: " \forall " means "for all"
" \exists " means "there exists"

We were listing
methods of proof.

First method contradiction.

We used this method

to show there are

infinitely many primes.

2) Proof by Induction

Let S be a statement about the natural numbers. If S is true for $n=1$ and if whenever S is true for $n \in \mathbb{N}$, S is true for $n+1$, then S holds for all natural numbers.

Variant. $n=1$ plus (all $k < n+1$
 $\Rightarrow n+1$)

Theorem: Let n be a natural number, suppose $n > 1$.

Then there are unique prime numbers p_1, p_2, \dots, p_k for some k in \mathbb{N} and powers m_1, m_2, \dots, m_k in \mathbb{N} such that

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_k^{m_k}.$$

Proof:

Start with $n=2$.

2 is prime, so there is only one prime in its factorization.

(This is the first step in the induction.)

Assume the statement is true for all natural numbers k with $2 \leq k < n+1$.

Consider $n+1$, which is a natural number.

Then $n+1$ is either prime
or composite (not a prime).

If $n+1$ is prime, we're
done.

If $n+1$ is composite, then

\exists a prime p with
 p dividing $n+1$. We can
write

$n+1 = p \cdot t$ for some natural
number t .

Observe that $t < n+1$.

Apply the inductive

hypothesis to t :

\exists primes q_1, q_2, \dots, q_L

and powers s_1, s_2, \dots, s_L

with $t = q_1^{s_1} \cdot q_2^{s_2} \cdot \dots \cdot q_L^{s_L}$

uniquely. Then

$$n+1 = p \cdot q_1^{s_1} \cdot q_2^{s_2} \cdot \dots \cdot q_L^{s_L}$$

and by relabeling the primes,

we are done - almost! \square

3) Contraposition

Given the statement

" P implies Q ", this

is logically equivalent to

"not Q implies not P ".

If you can show either

one of these statements is true,

that will imply the truth

of the other.

Theorem: If p is a prime number, then \sqrt{p} is irrational.

Proof: The contrapositive of this theorem's statement is "If \sqrt{p} is rational, then p is composite".

Let's prove the contrapositive.

Suppose \sqrt{p} is rational.

Then there are integers
a and b with

$$\sqrt{p} = \frac{a}{b} \quad (b \neq 0)$$

Square both sides.

$$p = \frac{a^2}{b^2}$$

Multiply both sides by b^2

$$p b^2 = a^2$$

By unique factorization,

there exist primes

p_1, \dots, p_n and natural

numbers k_1, \dots, k_n with

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$$

$$a^2 = p_1^{2k_1} \cdot p_2^{2k_2} \cdots p_n^{2k_n}$$

If $a^2 = pb^2$, then

$p_i^{2k_i}$ occurs in the factorization

of pb^2 for all $1 \leq i \leq n$.

Then again by unique

factorization, \exists primes

q_1, \dots, q_m and natural

numbers l_1, \dots, l_m with

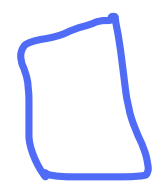
$$b = q_1^{l_1} \cdot q_2^{l_2} \cdot \dots \cdot q_m^{l_m}$$

$$b^2 = q_1^{2l_1} \cdot q_2^{2l_2} \cdot \dots \cdot q_m^{2l_m}$$

We have

$$\begin{aligned} p(q_1^{2l_1} \cdot \dots \cdot q_m^{2l_m}) &= p b^2 \\ &= a^2 \\ &= p_1^{2k_1} \cdot \dots \cdot p_n^{2k_n} \end{aligned}$$

By unique factorization again,
 p must be the product
of even powers of primes
by dividing out all the
primes. Hence, p cannot
be prime. In fact,
we have shown that
 p is equal to t^2 for
some natural number $t > 1$.



4) Proof by exhaustion

Divide the statement into

finitely many cases Prove

for each case,

Theorem: (triangle inequality for real numbers)

If a and b are real numbers, then

$$|a + b| \leq |a| + |b|$$

proof: Divide into cases.

Case 1: $a, b \geq 0$.

We have $a = |a|$, $b = |b|$

$|a + b| = a + b$. We then have equality in the triangle inequality.

Case 2: $a \geq 0, b \leq 0$

Subcases

i) $|a| \geq |b|$ Then

$$|a+b| = a+b$$

$$\leq a = |a| \leq |a| + |b|$$

ii) $|a| \leq |b|$

$$|a+b| = -(a+b)$$

$$\leq -b = |b| \leq |a| + |b|$$

Case 3 $a \leq 0, b \leq 0$

$$|a+b| = -(a+b)$$

$$= -a - b$$

$$= |a| + |b|$$

