Lets look at the important mathematical property of <u>Divisibility</u>.

If division of $a$ by $b$ produce a remainder $r = 0$, we say $a$ is divisible by $b$

Hence, $a$ is divisible by $b$ iff there is an integer $q$ such that $a = bq$

Eg. 45 is divisible by 9, but 44 is <u>not</u> divisible by 9.

Notation we use for divisibility:

$b | a$ denotes $a$ is divisible by $b$

<u>Warning</u>: $b | a$ is not the same as $b/a$

slanted line

relationship between $a$ and $b$

True or false

denotes a rational number.

Now lets define a prime number!

A prime number is an integer $p > 1$ that is divisible only by 1 and $p$
(we exclude 1 from prime numbers!)

eg. 2, 3, 5, 7, 11....

$b \mid a$ iff $\exists_q [a = bq]$

Which of following is true

1) $0 \mid 7$ [False] $b \neq 0$
2) $9 \mid 0$ True
3) $0 \mid 0$ [False]
4) $1 \mid 1$ True
5) $7 \mid 44$ [False] (remainder)
6) $7 \mid (-42)$ True
7 $(-7) \mid 49$ True
8) $(-7) \mid (56)$ True

which of following true:

$b|a$, iff $\exists q[a=bq]$, $b\neq 0$

1) $2708 \mid 569401$ — even / odd $\Rightarrow$ [False]

2) $(\forall n\in\mathbb{N})[2n \mid n^2]$

3) $(\forall n\in\mathbb{N})[2n \nmid n^2]$

4) $(\forall n\in\mathbb{Z})[1 \mid n]$ [True]

5) $(\forall n\in\mathbb{N})[n \mid 0]$ [True]

6) $(\forall n\in\mathbb{Z})[n \mid 0]$ (include $n=0$)

7) $(\forall n\in\mathbb{N})\underbrace{(n \mid n)}_{\text{only natural nums}}$ [True]

8) $(\forall n\in\mathbb{Z})[n \mid n]$ (includes $n=0$)

includes 0

Theorem to prove the basic properties of divisibility

Theorem: Let $a, b, c, d$ be integers, $a \neq 0$, then:

1) $a|0$, $a|a$
2) $a|1$ iff $a = \pm 1$
3) if $a|b$ and $c|d$ then $ac|bd$ (for $c \neq 0$)
4) if $a|b$ and $b|c$, then $a|c$ (for $b \neq 0$)
5) [$a|b$ and $b|a$] iff $a = \pm b$
6) if $a|b$ and $b \neq 0$, then $|a| \leq |b|$
7) if $a|b$ and $a|c$, then $a|(bx+cy)$ for any integers $x, y$

We have proved all of these!

Lets Prove 2 of them!

Proof: (No 4) if $a|b$ and $b|c$, then $a|c$ (for $b \neq 0$)

$\exists d, e$ such that $b = da$, $c = eb$,

So $c = (de)a$, hence $a|c$

(No 6) if $a|b$ and $b \neq 0$, then $|a| \leq |b|$

Since $a|b$, $\exists d$ such that $b = da$.

So $|b| = |d| \cdot |a|$

Since $b \neq 0$, $|d| \geq 1$

So $|a| \leq |b|$

The other statements are proved similarly.

*Lets Prove the Fundamental Theorem of Arithmetic

<u>Theorem:</u> Every natural number greater than 1 is either prime or can be expressed as a product of prime in a way that is unique, except for the order in which they are written.

Eg. $\overset{\downarrow \text{Product of Prim}}{4 = 2 \times 2 = 2^2}$, $\overset{(\text{POP})}{6 = 2 \times 3}$, $\overset{\text{POP}}{8 = 2^3}$, $\overset{\text{POP}}{9 = 3^3}$,

$\overset{\text{POP}}{10 = 2 \times 5}$, $\overset{\text{POP}}{12 = 2^2\cancel{\times}3}$, $\overset{\text{POP}}{3366 = 2 \times 3^2 \times 11 \times 17}$, ....

$\therefore$ above POP = Product of prims

The expression of a number as a product of prims is called its <u>prime decomposition</u>.

– we proved part of this earlier, the existence part.

– the new part is to prove uniqueness.

The uniqueness proof will require "Euclid's" Lemma:

If a prime $p$ divides a product $ab$, then $p$ divides at least one of $a, b$

Lets Look at New Proof of Existence

Theorem: Any natural number greater than 1, is either prime or can be expressed as a product of primes in a way that is unique except for their order.

Proof: Existence [we used method of induction earlier] to illustrate existence

Proof existence here by Contradiction!

Suppose there were a composite number. (ie non prime) that cannot be written as a product of primes — then there must be a smallest such number. Call it $n$

Since $n$ is not prime, there are numbers $a, b$ with $1 < a, b < n$ such that $n = ab$.

If $a, b$ are primes, then $n = ab$ is a prime decomposition of $n$ and we have a contradiction.

If either of $a, b$ is composite, then because it is less than $n$, it must be a product of prime. So by replacing one or both of $a, b$ by its prime decomposition in $n = ab$, we get a prime decomposition of $n$, and again we have a contradiction

That proves existence.

Lets now prove uniqueness

<u>To prove</u>: the prime decomposition of any natural number $n>1$ is unique up to the ordering of the primes.

Proof by Contradiction: Assume there is a number $n>1$, that has two (or more) different prime decompositions. Let $n$ be the smallest such number.

$n$ as product of $r$ primes

Let (*) $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ ← also, $n$ a product of $s$ primes

be two different prime decompositions of $n$

Since $p_1$ divides $(q_1)(q_2 \dots q_s)$, ← done this to apply Euclids lemma

By Euclid lemma, either $p_1 | q_1$

or $p_1 | (q_2 \dots q_s)$

Hence either $p_1 = q_1$ or else $p_1 = q_i$ for some $i$

between 2 ands

But then we can delete $p_1$ and $q_1$ from the two decomposition in (*), which gives us a number smaller than $n$ that has two different prime decompositions, contrary to the choice of $n$ as the smallest of such. That proves uniqueness!