Jan 11th, 2013

Prime numbers: a natural number $p>1$ is called prime if it cannot be written $p=ab$ where $a,b>1$, a b are natural #.

$n=ab$ $a,b>1$ natural # $\Rightarrow$ n is called **composite number**.

Theorem: every natural $n>1$ can be written as a product $n=P_1 \cdots P_k$ where all P_i are prime

Proof: proof by induction ① $n=2$, $2=2$ prime

② induction step: sps we proved that all # $2,3,\cdots,n$ can be written as a product of primes, $n\geq 2$

$\Rightarrow$ want to prove it by $n+1$

if $n+1$ is itself prime $\Rightarrow$ there is nothing to prove

$n+1=n+1$

if $n+1$ is composite $n+1=a\cdot b$, $a,b>1$, natural #

if $a=n+1$ or $b=n+1$, then $a,b>(n+1)\cdot 1=n+1$

$\Rightarrow a\leq n$ and $b\leq n$

$\Rightarrow$ by induction assumption both a and b can be written as products of primes

$$\left.\begin{matrix} a=P_1\cdots P_k \\ b=q_1\cdots q_j \end{matrix}\right\} \Rightarrow n+1=a\cdot b=(P_1\cdots P_k)(q_1\cdots q_j)$$ — product of primes

Theorem:

There are infinitely many prime numbers

in other words, there is no largest prime numbers

Proof: Argument by contradiction.

Assume that there are only finitely many prime numbers.

$P_1, P_2, \cdots, P_k$ all positive prime numbers and any other number is composite.

Let $n=(P_1\cdots P_k)+1$

n is a product of prime numbers + 1

$\Rightarrow n=q_1\cdots q_j$. q_i is prime

$\Rightarrow q_1=P_i$ for some i, after renumbering we can assume

$q_1=P_1$

$$n=P_1\cdots P_k+1=q_1\overbrace{q_2 q_3\cdots q_k}^{= S}+1=q_1 S+1$$

$$\| $$

$$q_1\underbrace{q_2\cdots q_j}_{= m}=q_1 m$$

$$n=q_1 m=q_1 S+1$$

$$1=q_1 m-q_1 S=\underbrace{q_1 (m-S)}_{\text{Integers}}$$ this is impossible

$q_1>1$ this is a contradiction

$\Rightarrow$ an original assumption was wrong.

So far the most tricky proof

How to List prime #?

Find all prime ≤ 50

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

Theorem: if n is a composite number then it has a prime factor $\leq\sqrt{n}$

i.e $n=p_1\cdots p_k$, one of the p_i is $\leq\sqrt{n}$

$\sqrt{49}=7$

$4<\sqrt{50}<8$

$n=a\cdot b$ composite

$a,b>1$

$a\leq b$ or $a\geq b$

say $a\leq b$ then $n=a\cdot b\geq a\cdot a=a^2$

$a=p_1\cdots p_k$ – prime numbers

$a=p_1\cdots p_k$ each $p_i\leq a\leq\sqrt{n}$

each p_i divides $a\Rightarrow$ divides n and it's $\leq\sqrt{n}$

ex: $n=6$

$6=2\cdot 3$ prime

$2<\sqrt{6}<3$

$2^2=4<6<9$