11 OCTOBER 2018

Thm: (Euclid) There are infinitely many primes

Proof ① By contradiction.

Assume there are finitely many primes labelled from $p_1, p_2 \cdots p_k$. Consider $N = p_1 \cdots p_k + 1 \geq 2$. This forms a new number N which like all numbers, has a prime divisor, say p_J (for some $J \in \{1 \cdots k\}$)

→ So $p_J \mid N = p_1 \cdots p_k + 1$ & $p_J \mid p_1 \cdots p_k$ } and $p_J \nmid 1$ → CONTRADICTION

If p_J Divides N (Coeset by 1) → and $p_1 \cdots p_{k+1} = x\, p_J$ (Can't divide both p_{k+1} and p_k)
then p_J also divides $p_1 \cdots p_k$ → then $p_1 \cdots p_k = y\, p_J$

Case

Proof ② Show that for every +INT ($n \geq 2$) there is a prime p so that $p > n$

- consider $n+1$; it has prime divisor say p
- if $p \leq n$ then $p \mid n!$; as $p \mid n! + 1$ then $p \mid 1$

so $p > n$ as desired

Remark For every INT $n \geq 2$, there is a prime $p: n < p \leq n! + 1$

{IN fact: there is a prime p so that $n < p \leq 2n$ "Bertrand's principle"}

50

Prime No Theorem

Let $\pi(n)$ = # of primes in $\{1, \cdots n\}$ then $\pi(n)/n$ is probability of prime. $\frac{\pi(n)}{n}$ goes to 0 $\sim \frac{1}{\ln(n)}$ rate

Fact: For every +INT n, there exist n consecutive numbers which are composite!

Proof: Pick the following n consecutive numbers $[n+1]! + 2, [n+1]! + 3, [n+1]! + 4 \cdots [n+1]! + n+1$

Each $(n+1)! + k$ is divisable by k where $k = 2 \cdots n+1$

Euclids lemma

Let p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Note Not true for composite numbers [eg $8 \mid 4 \cdot 6$ but $8 \nmid 4$ or $8 \nmid 6$]

Cor 1 Let p prime. If $p \mid a_1 \cdots a_n$, then $p \mid a_k$ for some k

Proof By:- Induction Dairy induction on k

51

cor 2 Let p prime. If $p|a^k$ then $p|a$ [after all $p|a \cdot a \cdot a \cdots a$]

Thm
Let p prime Then $\sqrt{p}$ is irrational

Proof: Assume on the contrary that $\sqrt{p} \in \mathbb{Q}$ (rational)
By CONT

So $\sqrt{p} = \frac{a}{b}$ for it to be rational

[assume $a, b \neq 0$
$a, b > 0$
a smallest
simplified
$\gcd(a,b) = 1$]

$\rightarrow a = b\sqrt{p}$
$\hookrightarrow a^2 = b^2 p \rightarrow p|a^2 \xrightarrow{cor^2} p|a$

so $a = p a_0$ $(a_0 \in INT)$

$(p a_0)^2 = b^2 p \rightarrow p^2 a_0^2 = p b^2 \rightarrow b^2 = p a_0^2$

So as above $p|b \Rightarrow b = p b_0$

but then not simplified as $\rightarrow \sqrt{p} = a/b = \sqrt{p} \cdot \frac{p a_0}{p b_0}$

$\hookrightarrow \sqrt{p} = \frac{a_0}{b_0}$

As $(a_0 < a)$ contradiction of choice of a

Fundamental Theorem of Arithmetics

Every possible integer >2 is a product of prime numbers. Furthermore a factorization is unique upto reordering

$\rightarrow 30 = 3 \cdot 10 = 3 \times 5 \times 2$
$\rightarrow 30 = 5 \cdot 6 = 5 \times 2 \times 3$

Proof

By hypothesis, $p|ab$; assume $p \nmid b$, want to show $p|a$

$\hookrightarrow$ consider a certain set of numbers $S = \{k \in \mathbb{N}, k \geq 1 \text{ and } p|kb\}$

$\hookrightarrow$ S are non empty as $p \in S$ & $a \in S$

Let a_0 is the smallest possible element in S

[Claim: a_0 divides every element of S]

$\rightarrow$ once we know this, we find $\rightarrow$ $a_0|p$ and $a_0|a$

[Note a_0 can't be 1 as if so $\rightarrow p|a_0 b \rightarrow p|b$ but $p \nmid b$]

So $\left.\begin{matrix} a_0 = p \\ a_0 | a \end{matrix}\right\} \rightarrow p|a$ as desired