Note Title 8/4/2022

Lecture 4:

Friday, 5/8/2022

3rd proof: To prove that there are infinitely many primes, we first prove the following lemma.

Lemma 1: For any real number $y \geq 2$, $\displaystyle\sum_{p \leq y} \frac{1}{p} > \log\log y - 1$, where the sum is taken over all primes $p \leq y$.

Proof: Let $y \geq 2$ be a real number, Let $p_1, p_2, \ldots, p_m$ be the primes not exceeding y, then we let

$$N_y = \{ p_1^{k_1} \cdots p_m^{k_m} \mid k_1, k_2, \ldots, k_m \geq 0 \}.$$

That is, N_y denotes the set of all those positive integers n that are composed entirely of primes $p \leq y$.

For any prime p, we know that the series $1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots$ converges absolutely to $\left(1-1/p\right)^{-1}$.

Since absolutely convergent series may be arbitrarily rearranged, so we have

this is a finite product

$$\prod_{p\le y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\sum_{n\in N_y}\frac{1}{n} \qquad (1)$$

Now, if n is a positive integer such that $n\le y$, then $n\in N_y$.

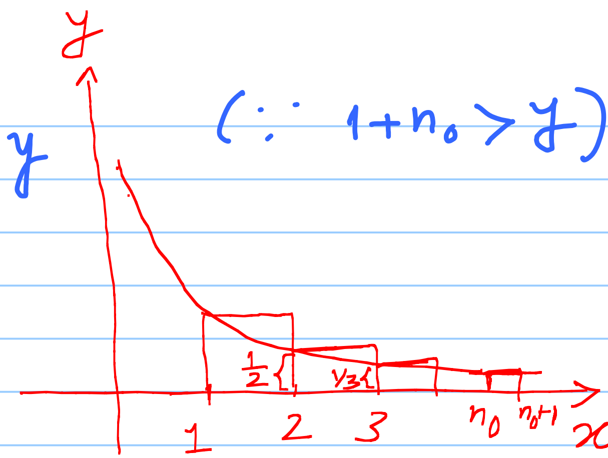
Thus, the sum $\sum_{n\in N_y}\frac{1}{n}$ contains the sum $\sum_{n\le y}\frac{1}{n}$.

Let n_0 denote the largest integer s.t. $n_0\le y$.

We have $\sum_{n=1}^{n_0} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n_0}$

$$\geq \int_1^{n_0+1} \frac{dx}{x} = \log(1+n_0) > \log y$$

$(\because\ 1+n_0 > y)$



From (1), we have

$$\prod_{p\leq y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) = \prod_{p\leq y}\left(1-\frac{1}{p}\right)^{-1} = \sum_{n\in N_y} \frac{1}{n}$$

$$> \sum_{n=1}^{n_0} \frac{1}{n} > \log y. \longrightarrow (2)$$

We next prove that

$$e^{\vartheta+\vartheta^2} \geq (1-\vartheta)^{-1} \quad \forall\ \vartheta \in [0, \tfrac{1}{2}].$$

<u>Proof</u>: Let $f(\vartheta) = (1-\vartheta)\, e^{\vartheta+\vartheta^2}$ for $\vartheta \in [0, \frac{1}{2}]$.

Then, $f'(v) = v(1-2v)\, e^{v+v^2} \geqslant 0 \quad \forall\, v \in [0, 1/2]$

$\therefore$ $f(v)$ is increasing for $0 \leq v \leq 1/2$

$\Rightarrow \quad f(0) \leq f(v) \qquad \forall\, v \in [0, 1/2]$

$\Rightarrow \quad e^{v+v^2} \geqslant (1-v)^{-1} \quad \forall\, v \in [0, \frac{1}{2}]$. #

Now, taking $v = \frac{1}{p}$, we have $\quad e^{\frac{1}{p}+\frac{1}{p^2}} \geqslant \left(1 - 1/p\right)^{-1}$

$$\Rightarrow \prod_{p \leq y} \exp\left(\frac{1}{p} + \frac{1}{p^2}\right) \geqslant \prod_{p \leq y} \left(1 - 1/p\right)^{-1} \underset{[\text{by } (2)]}{>} \log y$$

Taking log on both sides, we have

$$\sum_{y \leq p} \frac{1}{p} + \sum_{y \leq p} 1/p^2 > \log \log y. \longrightarrow (3)$$

The sum $\sum_{n=2}^{\infty} \frac{1}{n^2}$ includes the sum $\sum_{p \le y} \frac{1}{p^2}$.

$$\therefore \sum_{p \le y} \frac{1}{p^2} < \sum_{n=2}^{\infty} \frac{1}{n^2} < 1 \longrightarrow (4)$$

Thus, (3) and (4) $\Rightarrow$ $\displaystyle\sum_{p \le y} \frac{1}{p} > \log\log y - \sum_{p \le y} \frac{1}{p^2}$

$$\Rightarrow \sum_{p \le y} \frac{1}{p} > \log\log y - 1.$$

This completes the proof of the lemma. #

Proof of the fact that there are infinitely many primes:

Suppose that there are only finitely many primes, say $p_1, p_2, \dots, p_m$. Then, for any real $y \geq 2$, the sum $\sum_{p \leq y} 1/p$ is bounded above by $\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_m}$.

Since log is an increasing function, so we can choose y large enough so that

$$\log \log y - 1 > \frac{1}{p_1} + \dots + \frac{1}{p_m} \geq \sum_{p \leq y} 1/p.$$

This is a contradiction to Lemma 1.

This proves that there are infinitely many primes. #

<u>Ex:</u> If n is a composite number, then it must have a prime factor $p \leq \sqrt{n}$. Thus, if we need to check if a number is a prime it suffices to verify whether it is divisible by any of the primes $\leq \sqrt{n}$.

<u>Solution:</u> Let $n = p_1 p_2 \cdots p_k$, $k \geq 2$

If $p_i > \sqrt{n}$ $\forall i$, then $n > (\sqrt{n})^k \geq n$ if $k \geq 2$.

This is a contradiction.

$\therefore \exists$ a prime factor p_j of n such that $p_j \leq \sqrt{n}$.

#

AKS primality test: Manindra Agarwal, Neeraj Kayal, Nitin Saxena of IIT Kanpur

The test is the first unconditional deterministic algorithm to test an n-digit number for primality in a time that has been proven to be polynomial in n.

<u>Article</u>: Primes is in P, Annals of Mathematics, 2004.

<u>Theorem</u>: There are arbitrarily large gaps in the series of primes, that is, given any positive integer k, there exist k consecutive composite integers. #

<u>Proof</u>: Let $k \geq 1$. Then, the k consecutive integers

$(k+1)!+2,\ (k+1)!+3,\ \ldots,\ (k+1)!+k,\ (k+1)!+(k+1)$

are all compositive numbers, since

$$j \mid (k+1)!+j, \qquad 2 \le j \le k+1.$$

#

Let $\pi(x)$ = number of primes $\le x$.

<u>Prime number theorem:</u> (1896)

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

That is, for large x, $\pi(x)$ behaves like $\frac{x}{\log x}$. #

§ <u>Twin prime conjecture:</u> If p and $p+2$ are both primes, then they are called twin primes.

<u>Ex.</u> $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, ...

<u>Conjecture:</u> There are infinitely many twin primes.

In 2013, Yitang Zhang proved that there are infinitely many pairs of primes that differ by 70 million or less.

Again, in 2013, James Maynard employed a different technique and showed that there are infinitely many pairs of primes that differ by 600 or less.

In 2014, under Polymath project, the gap has been reduced to 246.

__Goldbach conjecture:__ Every even integer $n \geq 4$ can be written as a sum of two primes.

__Example:__ $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 5+5$, $12 = 5+7$, ...

§ __Primes in arithmetic progression:__

__Theorem 1:__ There are infinitely many primes of the form $4k+3$.

That is, there are infinitely many primes in the arithmetic progression: $3, 3+4, 3+2\times4, 3+3\times4, 3+4\times4, \ldots$

__Proof:__ Any odd prime p is either of the form $4k+1$ or $4k+3$.

Also, product of two or more integers of the form $4k+1$ is again of the form $4k+1$.

Suppose that there are only finitely many primes of the form $4k+3$, say, $q_1, q_2, \dots, q_s$.

Let $N = 4q_1q_2\cdots q_s - 1 = 4(q_1\cdots q_s - 1) + 3$.

Let $N = p_1p_2\dots p_r$ be its prime factorisation.

N is odd $\Rightarrow$ each p_i is odd $\Rightarrow p_i = 4k+1$ or $p_i = 4k+3$.

If all p_i is of the form $4k+1$, then N will be of the form $4k+1$

But, N is of the form $4k+3$, so $\exists j$ such that p_j is of the form $4k+3$. Since $q_1, \dots, q_s$ are the only primes of the form $4k+3$, so $p_j = q_i$ for some i.

$\therefore\ p_j \mid N - 4q_1q_2\cdots q_s \Rightarrow p_j \mid 1$, which is a contradiction.

This proves that there are infinitely many primes of the form $4k+3$.

#

<u>Theorem (Dirichlet, 1837)</u>: If a and b are relatively prime positive integers, then the arithmetic progression

$$a,\ a+b,\ a+2b,\ a+3b,\ \ldots,\ a+kb,\ \ldots$$

contains infinitely many primes.

(Proof is beyond the scope of this course.)

#