Prime Number Estimate

Jiman Hwang

Disclaimer: This document is for self-study only and may contain false information.
Sources: B.4 at [Kor82], CH 5.3.1 and Appendix 4.4 at [NC00]

1 Statement

Let $\pi(n)$ be the number of prime numbers less than $n \in \mathbb{N}$. Then

$$\frac{n}{\lg(2n)} \leq \pi(2n)$$

where lg is base 2 logarithm.

2 Derivation

We assert two inequalities and combine them.

2.1 Relationship between binomial coefficient and LCM

First, we prove

$$\binom{2n}{n} \leq \operatorname{lcm}\{1, 2, \cdots, 2n\} \tag{1}$$

Let $p_1 < p_2 < \cdots < p_{\pi(2n)}$ be prime numbers less than $2n$.
Then, $\exists q_1, q_2, \cdots, q_{\pi(2n)} \in \mathbb{N}$ such that

$$\operatorname{lcm}\{1, 2, \cdots, 2n\} = p_1^{q_1} p_2^{q_2} \cdots p_{\pi(2n)}^{q_{\pi(2n)}} \tag{2}$$

where

$$p_i^{q_i} \leq 2n < p_i^{q_i+1} \quad \text{for } i = 1, 2, \cdots, \pi(2n) \tag{3}$$

Also, $\exists r_1, r_2, \cdots, r_{\pi(2n)} \in \mathbb{N} \cup \{0\}$ such that

$$\binom{2n}{n} = p_1^{r_1} p_2^{r_2} \cdots p_{\pi(2n)}^{r_{\pi(2n)}} \tag{4}$$

Therefore, (1) becomes

$$p_1^{r_1} p_2^{r_2} \cdots p_{\pi(2n)}^{r_{\pi(2n)}} \leq p_1^{q_1} p_2^{q_2} \cdots p_{\pi(2n)}^{q_{\pi(2n)}}$$

If

$$\forall i \; r_i \leq q_i \tag{5}$$

is true, then so is (1).

Assuming p is a prime number, let

$$f(n,p) \overset{\text{def}}{=} \max\{x \in \mathbb{N} \cup \{0\} : p^x | n!\}$$

where $a|b$ means a divides b. So, function f counts how many times prime p is multiplied in $n!$. In fact,

$$f(n,p) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$$

Some factorials are expressed as multiple of prime numbers.

$$\begin{aligned} n! &= p_1^{f(n,p_1)} p_2^{f(n,p_2)} \cdots p_{\pi(2n)}^{f\left(n,p_{\pi(2n)}\right)} = \prod_{i=1}^{\pi(2n)} p_i^{f(n,p_i)} \\ (2n)! &= p_1^{f(2n,p_1)} p_2^{f(2n,p_2)} \cdots p_{\pi(2n)}^{f\left(2n,p_{\pi(2n)}\right)} = \prod_{i=1}^{\pi(2n)} p_i^{f(2n,p_i)} \end{aligned}$$

So, the binomial becomes

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \prod_{i=1}^{\pi(2n)} \frac{p_i^{f(2n,p_i)}}{p_i^{2f(n,p_i)}} = \prod_{i=1}^{\pi(2n)} p_i^{f(2n,p_i)-2f(n,p_i)}$$

From (4),

$$r_i = f(2n,p_i) - 2f(n,p_i) = \sum_{j=1}^{\infty} \left(\left\lfloor \frac{2n}{p_i^j} \right\rfloor - 2 \left\lfloor \frac{n}{p_i^j} \right\rfloor \right)$$

From (3), we can narrow it down to finite terms.

$$r_i = \sum_{j=1}^{q_i} \left(\left\lfloor \frac{2n}{p_i^j} \right\rfloor - 2 \left\lfloor \frac{n}{p_i^j} \right\rfloor \right) \tag{6}$$

Suppose $n = up_i^j + v$ where $u \in \mathbb{Z}, v \in \left\{0, 1, \cdots, p_i^j - 1\right\}$. Then

$$\left\lfloor \frac{n}{p_i^j} \right\rfloor = u \tag{7}$$

Also,

$$\frac{2n}{p_i^j} = 2u + \frac{2v}{p_i^j} \quad \Rightarrow \quad \left\lfloor \frac{2n}{p_i^j} \right\rfloor \leq 2u + 1 \tag{8}$$

(6), (7), and (8) give an upper bound of r_i

$$r_i \leq \sum_{j=1}^{q_i} (2u + 1 - 2u) = q_i$$

This proves (5), hence (1) is true.

2.2 Eliciting $\pi(2n)$

From (1), (4), and (3),

$$\binom{2n}{n} \leq (2n)^{\pi(2n)}$$

Hence

$$\lg \binom{2n}{n} \leq \pi(2n) \lg(2n) \tag{9}$$

Proceeding the left hand side,

$$\begin{aligned} \lg \binom{2n}{n} &= \left(\frac{2n}{n} \times \frac{2n-1}{n-1} \times \cdots \times \frac{n+2}{2} \times \frac{n+1}{1} \right) \\ &= \lg \prod_{j=1}^{n} \frac{n+j}{j} \\ &= \lg \prod_{j=1}^{n} \left(1 + \frac{n}{j}\right) \end{aligned}$$

Since $n/j \geq 1$,

$$\lg \binom{2n}{n} \geq \lg \prod_{j=1}^{n} (1+1) = \lg 2^n = n \tag{10}$$

From (9) and (10),

$$n \leq \pi(2n) \lg(2n)$$

or

$$\frac{n}{\lg(2n)} \leq \pi(2n)$$

References

[Kor82] Jacob Korevaar. On newman's quick way to the prime number theorem. *The Mathematical Intelligencer*, 4(3):108–115, 1982.

[NC00] Michael A Nielson and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.