Math 118 Winter 2015 Lecture 43 (Mar. 30, 2015)

Note. This lecture is based on Chapters 1 & 2 of *Proofs from the Book* by M. Aigner and G. M. Ziegler, 4th ed., Springer, 2010.

- Infinity of Primes.

Claim. There are infinitely many primes.

  - Calculus Proof 1.

For $n \in \mathbb{N}$ denote by $\pi(n)$ the number of primes $\leqslant n$. Now consider

$$A = \prod_{p \leqslant n} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_{p \leqslant n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right). \tag{1}$$

Exercise 1. Is A a finite number? Why?

On one hand, we have

$$A = \sum_{p_1, \ldots, p_l \leqslant n, k_1, \ldots, k_l \in \mathbb{N}} \frac{1}{p_1^{k_1} \cdots p_l^{k_l}} > \sum_{i=1}^{n} \frac{1}{i} > \ln n. \tag{2}$$

Exercise 2. Justify (2).

On the other hand, we have

$$A = \prod_{p \leqslant n} \frac{p}{p-1} < \prod_{j \leqslant \pi(n)} \frac{j}{j-1} = \pi(n). \tag{3}$$

Exercise 3. Justify (3).

Putting (2) and (3) together, we see that $\pi(n) > \ln n$.

Exercise 4. Explain why this means there are infinitely many primes.

  - Calculus Proof 2.

Let $p_1 < p_2 < p_3 < \cdots$ be the listing of primes. We prove that

$$\sum_{k=1}^{\infty} \frac{1}{p_k} = +\infty. \tag{4}$$

Exercise 5. Show that (4) implies the infinity of primes but the converse does not necessarily hold.

Assume the contrary. Then there is $k_0 \in \mathbb{N}$ such that

$$\sum_{k > k_0} \frac{1}{p_k} < \frac{1}{2}. \tag{5}$$

Exercise 6. Justify (5).

Now let $n \in \mathbb{N}$ be arbitrary. Define two sets

$$N_1 := \{m \in \mathbb{N}, m \leqslant n, m \text{ can be divided by some } p_k \text{ with } k > k_0\}. \tag{6}$$

$$N_2 := \{m \in \mathbb{N}, m \leqslant n, \text{ there is no } p_k \text{ with } k > k_0 \text{ that divides } m\}. \tag{7}$$

Clearly $N_1 \cup N_2 = \{1, 2, \ldots, n\}$. Now we count how many elements are in N_1, N_2.

- N_1. For any prime p, there are no more than $\frac{n}{p}$ numbers in $\{1, 2, \ldots, n\}$ that are multiples of p. Therefore the size of N_1 is no more than

$$\sum_{k > k_0} \frac{n}{p_k} < \frac{n}{2}. \tag{8}$$

- N_2. Let $m \in N_2$ be arbitrary. Then it has a unique prime factorization

$$m = p_1^{l_1} \cdots p_{k_0}^{l_{k_0}}. \tag{9}$$

We know that smallest prime is 2, therefore for any $m \in N_2$ there holds

$$m \geqslant 2^{l_1 + \cdots + l_{k_0}} \Longrightarrow l_1 + \cdots + l_{k_0} \leqslant \log_2 m \leqslant \log_2 n. \tag{10}$$

Thus the size of N_2 can be no more than the number k_0-tuples $(l_1, \ldots, l_{k_0})$ satisfying $l_i \in \mathbb{N} \cup \{0\}$, $l_1 + \cdots + l_{k_0} \leqslant \log_2 n$, which can be bounded as follows

$$\text{size of } N_2 \leqslant \binom{[\log_2 n] + k_0}{k_0} < (\log_2 n + k_0)^{k_0}. \tag{11}$$

Here $[x]$ means the largest integer no more than x.

Exercise 7. Justify (11).

Summarizing, we have, for arbitrary $n \in \mathbb{N}$,

$$n = \text{size of } N_1 + \text{size of } N_2 < \frac{n}{2} + (\log_2 n + k_0)^{k_0} \tag{12}$$

where k_0 is a fixed natural number not dependent on n.

Exercise 8. Show that (12) leads to contradiction and finish the proof.

- Bertrand's Postulate.

Claim. For every $n \in \mathbb{N}$, there is a prime between n and $2n$.

Remark 1. Conjectured and verified for $n < 3 \times 10^6$ by Joseph Bertrand. Proved by Pafnuty Chebyshev in 1850. Simple proofs by Ramanujan. The proof here is by Paul Erdos in 1932 when he was 19.

Proof. We prove by contradiction. Assume there is $n \in \mathbb{N}$ such that all the numbers $n+1$, $n+2, \ldots, 2n$ are composite.

Consider the number $N := \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. For any prime p, we count how many times it appears in the denominator and the numerator. In particular, any $p \in (n, 2n]$ appears in the numerator only.

Let $[x]$ denote the largest integer no more than x. Then for any prime p,

$$\text{power of } p \text{ in } N = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right) \leqslant \max \{r : p^r \leqslant 2n\}. \tag{13}$$

Exercise 9. Prove (13). (Hint:[1])

1. For the inequality, show that for arbitrary n, k, p, $\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]$ is either 0 or 1

Exercise 10. Prove that if $p\in\left[\frac{2}{3}n,n\right]$, then it does not appear in the factorization of N.

- An upper bound for N.

  Now we try to estimate N from its prime factorization. If we write

$$N=\prod_{p\leqslant 2n, p|N} p^k=\left(\prod_{p\leqslant\sqrt{2n}, p|N} p^k\right)\left(\prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n, p|N} p\right)=:A\,B, \tag{14}$$

  then we can conclude the following.

  Exercise 11. What happened to $\prod_{2n/3<p\leqslant n} p$ and $\prod_{n<p\leqslant 2n} p$?

  Exercise 12. Why are there no powers on p in the second term?

  – A.

    Thanks to (13), we can simply estimate

$$A\leqslant\prod_{p\leqslant\sqrt{2n}} 2\,n\leqslant(2\,n)^{\sqrt{2n}}. \tag{15}$$

  – B.

    We have trivially

$$B\leqslant\prod_{p\leqslant\frac{2}{3}n} p. \tag{16}$$

  Now we need the following lemma.

  Lemma 2. *Let $n\in\mathbb{N}$. Then $\prod_{p\leqslant n} p\leqslant 4^{n-1}$.*

  Proof. (of Lemma 2)

  Exercise 13. Show that it suffices to prove for $n=q$ a prime.

  Exercise 14. Show that the conclusion holds for $q=2$.

  Now let $q=2\,m+1$ be prime. We prove by induction. We have

$$\prod_{p\leqslant 2m+1} p=\prod_{p\leqslant m+1} p\cdot\prod_{m+1<p\leqslant 2m+1} p\leqslant 4^m\prod_{m+1<p<2m+1} p. \tag{17}$$

  Now observe that any p between $m+1$ and $2\,m+1$ must be a factor of the number $\binom{2\,m+1}{m+1}$. Therefore

$$\prod_{m+1<p\leqslant 2m+1} p\leqslant\binom{2\,m+1}{m+1}. \tag{18}$$

  Exercise 15. Prove that $\binom{2\,m+1}{m+1}\leqslant 2^{2m}$. (Hint:[2])

  Thus we have

$$\prod_{p\leqslant 2m+1} p\leqslant 4^m\cdot 2^{2m}=4^{2m} \tag{19}$$

  and the proof is complete. □

  Therefore we have $B\leqslant 4^{2n/3}$.

2. Binomial expansion of $(1+1)^{2m+1}$ then use the fact that $\binom{2\,m+1}{m+1}=\binom{2\,m+1}{m}$.

Summarizing, we conclude

$$N = A\,B \leqslant (2\,n)^{\sqrt{2n}}\,4^{2n/3}. \tag{20}$$

- A lower bound for N.

  Expanding $(1+1)^{2n}$ we see that

$$\binom{2\,n}{n} \geqslant \frac{4^n}{2\,n}. \tag{21}$$

Exercise 16. Prove (21).

Putting (20) and (21) together, we have

$$4^{n/3} \leqslant (2\,n)^{1+\sqrt{2n}}. \tag{22}$$

Exercise 17. Prove that there is $n_0 \in \mathbb{N}$ such that (22) cannot hold for $n > n_0$.

Exercise 18. Find one such n_0 explicitly. Justify your claim.

As Bertrand has already verified the conclusion for n up to 3×10^6, the proof ends. □

Problem 1. Estimate how many primes are there between n and $2\,n$ by exploring (22).