MATH453 Elementary Number Theory

Lecture 5: Prime Frequency and Factorization

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

5.1 Distribution of Primes

Recall that from calculus, we know that $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$ but $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. Now, one might be interested in knowing how the series

$$\sum_{p \text{ prime}} \frac{1}{p}$$

behaves.

Theorem 5.1. For every $y \geq 2$,

$$\sum_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{p} \geq \log\log y - 1$$

Proof. Let $\mathcal{N}$ be the subset of $\mathbb{Z}^+$ whose prime factorizations contain only primes $\leq y$. Consider $\sum_{n=1}^{\lfloor y \rfloor} 1/n$, which is an upper bound on the sum that we are interested in.

$$\sum_{n=1}^{\lfloor y \rfloor} \frac{1}{n} \geq \int_1^{\lfloor y \rfloor + 1} \frac{dx}{x} = \log(\lfloor y \rfloor + 1) \geq \log(y) \tag{5.1}$$

Now, consider the product of the geometric series over all primes $p \leq y$.

$$\prod_{\substack{p \leq y \\ p \text{ prime}}} \left(\sum_{i=0}^{\infty} \frac{1}{p^i} \right) = \prod_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{1 - 1/p} = \sum_{n \in \mathcal{N}} \frac{1}{n} \geq \sum_{n=1}^{\lfloor y \rfloor} \frac{1}{n} \geq \int_1^{\lfloor y \rfloor + 1} \frac{dx}{x} \geq \log y \tag{5.2}$$

Claim. For $0 \leq v \leq \frac{1}{2}$, $e^{v+v^2} \geq \frac{1}{1-v}$. Let $v = 1/p \leq 1/2$.

Then, from the claim,

$$\prod_{\substack{p \leq y \\ p \text{ prime}}} e^{\frac{1}{p} + \frac{1}{p^2}} \geq \prod_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{1 - 1/p} \geq \log y \tag{5.3}$$

Take the logarithm of both sides,

$$\log \prod_{\substack{p \leq y \\ p \text{ prime}}} e^{\frac{1}{p} + \frac{1}{p^2}} \leq \sum_{\substack{p \leq y \\ p \text{ prime}}} \log e^{\frac{1}{p} + \frac{1}{p^2}} = \sum_{\substack{p \leq y \\ p \text{ prime}}} \left(\frac{1}{p} + \frac{1}{p^2} \right) \geq \log\log y \tag{5.4}$$

Further, we observe that

$$\sum_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{p^2} \leq \sum_{n=2}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} < 1 \tag{5.5}$$

So it follows that

$$\sum_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{p} > \log \log y - \sum_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{p^2} > \log \log y - 1 \tag{5.6}$$

■

We must also prove the claim we have used in the proof of the theorem.

Lemma 5.2. For $0 \leq v \leq 1/2$,

$$e^{v+v^2} \geq \frac{1}{1-v}$$

Proof. Let $f(v) = (1-v)e^{v+v^2}$. $f(0) = 1$. We see that the first derivative is non-negative and thus f is non-decreasing on $[0, \frac{1}{2}]$.

$$f'(v) = -e^{v+v^2} + (1-v)(1+2v)e^{v+v^2} = v(1-2v)e^{v+v^2}.$$

Then, since $f(v) = (1-v)e^{v+v^2}$ is non-decreasing on $[0, 1/2]$, we have

$$f(v) = (1-v)e^{v+v^2} \geq f(0) = 1 \qquad \forall v \in [0, 1/2]$$

This implies that $e^{v+v^2} \geq \frac{1}{1-v}$ for $0 \leq v \leq 1/2$. ■

5.2 Fundamental Theorem of Arithmetic

Now we introduce a few lemmas in preparation for the Fundamental Theorem of Arithmetic.

Lemma 5.3. Let p be prime such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

Proof. Assume that $p \mid ab$. If $p \mid a$, then we are done, so assume that $p \nmid a$. Then, a and p are coprime, so $\gcd(p, a) = 1$. There exists some $m, n \in \mathbb{Z}$ such that $ma + np = 1$ by Prop 4.2.

$b = 1 \cdot b$ so $b = mab + npb$. By assumption, $p \mid ab$. Then, there exists $c \in \mathbb{Z}$ such that $ab = pc$. It follows that

$$b = mpc + npb = p(mc + nb)$$

which, by definition of divisiblity, $p \mid b$. ■

Corollary 5.4. Let p be prime, $a_1, \ldots, a_n \in \mathbb{Z}$ for $n \geq 2$. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_j$ for at least one $j \in \{1, 2, \ldots, n\}$.

Proof. By Lemma 5.3, $p \mid a_1 \ldots a_{n-1}$ or $p \mid a_n$. Prove by induction on $n \geq 2$. ■

Theorem 5.5 (Fundamental Theorem of Arithmetic)**.** Every integer $a > 1$ can be represented **uniquely** as a product of primes

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

where $p_i \neq p_j$ if $i \neq j$ for positive integers a_i.

Now, we are ready to prove the ***Fundamental Theorem of Arithmetic***. It states the factorizability of any positive integers so the theorem is sometimes called the unique factorization theorem.

Proof. By contradiction.

Assume that there exists some integer without a prime factorization. Take c to be the smallest of such counterexamples. Then, c must be composite (otherwise, c itself would be a unique prime factorization of c). Then, $c = ab$ for some $a, b > 1$ and $a, b < c$. Since c is the smallest counterexample, a and b, which are smaller than c, can be represented as products of primes. Therefore, c indeed has a prime factorization that is the product of the prime factorizations of a and b. This is a contradiction, so c **has a prime factorization**.

It remains to be shown that the factorization of c is unique. Suppose for contradiction that c has two prime factorizations. That is

$$c = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}$$

where $p_1 < p_{i+1}$ and $q_j < q_{j+1}$ for all $i \in \{1, \dots, m-1\}$ and $j \in \{1, \dots, n-1\}$.

It suffices to show that $p_j = q_j$, $a_j = b_j$ for all j, $m = n$.

Fix arbitrary p_i. By Corollary 5.4, $p_i \mid q_j$ for some j. Since p_i and q_j are prime, it follows that $p_i = q_j$ because otherwise it would be a contradiction. Similarly, fix q_j, and by the same argument, $q_j \mid p_i$ for some i so $p_i = q_j$. Thus, $p_j = q_j$ for all j. This also implies that $m = n$.

Finally, we show that the exponents are also equal. Suppose for contradiction that there exists some j such that $a_j \neq b_j$. Without loss of generality, assume $a_j < b_j$. Since

$$p_j^{b_j} \mid c = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

so $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} = k p_j^{b_j}$ for some $k \in \mathbb{Z}$. It follows that by dividing both sides by $p_j^{a_j}$,

$$p_1^{a_1} p_2^{a_2} \cdots p_{j-1}^{a_{j-1}} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n} = k p_j^{b_j - a_j}$$

Since $b_j - a_j > 0$, $p_j \mid p_1^{a_1} p_2^{a_2} \cdots p_{j-1}^{a_{j-1}} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n}$. By Corollary 5.4, $p_j \mid p_i$ for some $i \neq j$. But this is not possible because for all $i \in \{1 \dots n\} \setminus \{j\}$, p_i is prime and p_j is **not a factor** of $p_1^{a_1} p_2^{a_2} \cdots p_{j-1}^{a_{j-1}} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n}$. Hence, $p_i \mid p_j$ and $p_i \neq p_j$, which is a contradiction because a prime cannot divide another prime.

Therefore, the prime **factorization is unique**. ■