Elementary Number Theory: Primes and their Distribution

Arjun Vardhan

†
Created: 8th April 2022
Last updated: 21st June 2022

1 The Fundamental Theorem of Arithmetic

- An integer $p > 1$ is said to be prime if its only positive divisors are 1 and p. An integer greater than 1 which is not prime is called composite.
- **If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.** *Proof:* If $p \mid a$, then we are done, so let $p \nmid a$. Then $\gcd(a, p) = 1$ and so by Euclid's lemma, $p \mid b$. ■
- **If $p \mid a_1a_2...a_n$, then $p \mid a_k$ for some k, where $1 \le k \le n$.** *Proof:* If $n = 1$ then this is obviously true. If $n = 2$ then this is equivalent to the theorem right above. Suppose this statement is true for up to $n - 1$ factors, where $n > 2$. Now let $p \mid a_1a_2...a_n$. Then either $p \mid a_n$ (in which case we are done) or $p \mid a_1a_2...a_{n-1}$, in which case by the induction hypothesis, $p \mid a_k$ for some k where $1 \le k \le n - 1$. ■
- **Corollary: If $p, q_1, q_2, ..., q_n$ are all primes and $p \mid q_1q_2...q_n$, then $p = q_k$ for some k, where $1 \le k \le n$.** *Proof:* By the theorem above, $p \mid q_k$ for some k. As q_k is prime, we have $p = q_k$. ■
- **Fundamental Theorem of Arithmetic: Every integer greater than 1 is a prime or a product of primes and its representation as a product of primes is unique.** *Proof:* If n is prime then we are done, so let n be composite. There must exist an integer d such that $d \mid n$ and $1 < d < n$. Let p_1 be the smallest such integer. Then p_1 must be prime, for if it was not, then it would have an even smaller divisor which would be a contradiction. Then $n = p_1n_1$, with $1 < n_1 < n$. If n_1 is prime, then we are done. Otherwise the same process above is repeated to get $n = p_1p_2n_2$ with $1 < n_2 < n_1$. The decreasing sequence $1 > n_1 > n_2 > ...$ cannot continue indefinitely, so this process must terminate. Thus after a finite number of steps n_{k-1} is prime and we call it p_k. Finally we have our prime factorization $n = p_1p_2...p_k$. Now suppose $n = p_1p_2...p_k$ and $n = q_1q_2...q_s$ with $r \le s$, $p_1 \le p_2 \le ... \le p_k$ and $q_1 \le q_2 \le ... \le q_s$. As $p_1 \mid q_1q_2...q_s$, $p_1 = q_k$ for some k, so $p_1 \ge q_1$. Similar reasoning gives $q_1 \ge p_1$, so $q_1 = p_1$. This process can be repeated to get $p_2 = q_2$ and $q_3 = p_3$ and so on. If $r < s$, then we would eventually get $1 = q_{r+1}...q_s$ which can't be true as each $q_i > 1$. So $r = s$ and $p_i = q_i$ for all i, $1 \le i \le r$, making the two factorizations identical. ■
- **Corollary:** Any integer $n > 1$ can be written uniquely in a canonical form $n = p_1^{k_1}p_2^{k_2}...p_r^{k_r}$ where each p_i is prime, each k_i is a positive integer and $p_1 < p_2 < ... < p_r$.

2 Distribution of Primes

- **There is an infinite number of primes.** *Proof:* Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5...$ be the sequence of prime numbers in ascending order. Suppose there is a last prime, called p_n. Consider $P = p_1p_2...p_n + 1$. As $P > 1$, by the fundamental theorem of arithmetic, there exists some prime p that divides P. But $p_1, p_2, ..., p_n$ are all the prime numbers, so p must be equal to one of them. Since $p \mid P$ and $p \mid p_1p_2...p_n$, we have $p \mid P - p_1p_2...p_n = 1$. Then $p = \pm 1$, which is a contradiction. Thus any finite list of prime numbers will have a prime that is not on the list. ■
- **If p_n is the nth prime number, then $p_n \le 2^{2^{n-1}}$.** *Proof:* Clearly true for $n = 1$. Suppose that it holds for all integers up to n. Then
- **Corollary: For $n \ge 1$, there are at least $n + 1$ primes less than 2^{2^n}.**

3 The Goldbach Conjecture