1.5 Lecture 5

Preamble: In this lecture, we will discuss prime numbers. We will then state and prove the fundamental theorem of arithmetic. We will also mention certain results concerning the distribution of primes in the set of natural numbers.

Keywords: primes, fundamental theorem of arithmetic

1.5.1 Prime Numbers

Prime numbers are crucial for our understanding of natural numbers. They are the building blocks from which all other integers can be composed as products.

Definition 1.20. *A natural number p is called prime if it has exactly two factors, namely 1 and p itself.*

For example, $2,\ 3,\ 5,$ etc are prime numbers. The integer 1 is not considered a prime as 1 has only one factor. Note that we can extend our definition to include negative integers having no non-trivial factors, where trivial factors of an integer n mean ± 1 and $\pm n$. This notion can be readily generalized to define *irreducible elements* in a commutative ring.

Proposition 1.21. *Let p is a prime number and $a,\ b$ are integers such that $p \mid ab$. Then $p \mid a$ or $p \mid b$.*

Proof: Suppose $p \nmid a$. Then p and a are coprime. By corollary 1.15 of lecture 4, we must have $p \mid b$. □

The above property can be considered in any commutative ring leading to the notion of *prime elements* in such a ring. Note that the following corollary follows readily from proposition 1.21.

Corollary 1.22. *If p is a prime number such that $p \mid a_1 \cdot a_2 \cdot \cdots \cdot a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$.*

1.5.2 Fundamental Theorem of Arithmetic

Theorem 1.23. *Any natural number $n > 1$ can be written as a finite product*

$$n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r},$$

where p_i's are distinct primes dividing n and e_i are positive integers. This decomposition is unique up to reordering of the prime powers.

For example, $18 = 2^1 \cdot 3^2, \quad 1000 = 2^3 \cdot 5^3$.

Proof: *Existence*: We can use induction on n. Clearly, the statement is trivially true for $n = 2$, as 2 is a prime anyway. Suppose the statement is true for $n = 2,\ 3,\ \ldots,\ k$. Now consider $k+1$. It is either a prime, in which case the theorem is valid. If $k+1$ is not prime, we have $k+1 = ab$ where $1 < a \leq k$ and $1 < b \leq k$. By the induction hypothesis, we both a and b can be written as a finite product of primes, giving us ab as a finite product of primes too.

Uniqueness: If possible, let

$$n = p_1^{e_1} p_2^{e_2} \cdot \cdots \cdot p_r^{e_r} = q_1^{f_1} q_2^{f_2} \cdot \cdots \cdot p_k^{f_k}.$$

As $p_1 \mid n$, it divides $q_1^{f_1} q_2^{f_2} \cdot \cdots \cdot p_k^{f_k}$, and by corollary 1.22, p divides some prime q_j. We can assume, if necessary by reordering the primes q_j, that p_1 divides q_1. But q_1 is a prime itself, hence $p_1 = q_1$. If $e_1 > f_1$, then after canceling p^{f_1} from both sides, we will see that $p_1 = q_1$ divides $q_2^{f_2} \cdot \cdots \cdot p_k^{f_k}$, which will imply that the prime q_1 divides some other prime $q_j \neq q_1$, which is not possible. Similarly, $e_1 < f_1$ leads to a contradiction. Hence we must have $e_1 = f_1$, so that we can cancel $p_1^{e_1}$ from both the factorizations. Now we can argue similarly for p_2, and then for its index e_2. We cannot have some primes left in one of the factorizations, as it will lead to 1 being expressed as a product of primes. □

As an application, let us prove the following:

Proposition 1.24. *Suppose a and b are relatively prime natural numbers such that their product is a perfect square. Then both a and b must be perfect squares.*

Proof: As ab is a square, we have

$$ab = \left(p_1^{e_1} \cdot \cdots \cdot p_r^{e_r}\right)^2,$$

where p_i's are distinct primes. If some $p_j \mid a$, then $p_j \nmid b$ as $gcd(a,b) = 1$ and we must have $p_j^{2e_j} \mid a$. By uniqueness of factorization, a can not have any prime powers other than those occurring in the factorization of ab. Thus the factorization of a involve only even powers of primes, and it must be a perfect square. Similarly, b must be a perfect square. □

1.5.3 Infinitude of Primes

The following observation was made by the Greek mathematician Euclid in his book *Elements* written in the third century BC.

Theorem 1.25. *There are infinitely many primes.*

Proof: If possible, suppose there are only finitely many primes $p_1,\ p_2,\ \cdots,\ p_k$. Consider $N = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$. Now N is not divisible by any of the primes $p_1,\ p_2,\ \cdots,\ p_k$. Hence either N is a prime, or it is divisible by a prime which is not one of $p_1,\ p_2,\ \cdots,\ p_k$. This leads to a contradiction. □

Clearly, any prime number other than 2 is either of the form $4k+1$ or $4k+3$. This follows from division algorithm, when we look at the remainder upon division by 4. One can easily show that there are infinitely many primes of the form $4k+3$.

Theorem 1.26. *There are infinitely many primes of the form $4k+3$.*

Proof: The proof is analogous to Euler's proof of existence for infinitely many primes. If possible, assume that there are only finitely many primes of the form $4k+3$. Suppose we denote them by $3 = p_1, p_2, \cdots, p_n$. Now consider the number

$$N = 4p_2 \cdots p_n + 3.$$

Now, $p_i \mid N$ for $i > 1$ would imply $p_i \mid 3$, which is not possible. Moreover, $3 \mid N$ would mean $3 \mid p_j$ for some prime $p_j > 3$ which is also not possible. Therefore, N is not divisible by any of the listed primes p_i. Therefore, N is either a prime number or is divisible by some prime q other tan p_i's. If all the prime factors of the odd integer N are of the form $4k+1$, then N will also be of the form $4k+1$, which is clearly not the case. Therefore, there must be a prime factor of N of the form $4k+3$, which is not in $\{p_1,\ \cdots,\ p_n\}$. □

Note that 3, 7, 11, 15, $\cdots$ is an arithmetic progression, which contains infinitely many primes by our theorem. One can prove a much stronger result about existence of primes in an arithmetic progression. The stronger result is due to French mathematician Dirichlet.

Theorem 1.27. *Let $a,\ a+d,\ a+2d,\ \dots$ be an infinite arithmetic progression. If a and d are coprime, there are infinitely many primes in the progression.*

For example, one can say that there are infinitely many primes in the sequence 14, 19, 24, 29, ... The proof of the above involves Dirichlet L-function and is beyond the scope of these notes. Roughly speaking, one shows that the sum of the reciprocals of all the primes of the form $a+nd$ (where $\gcd(a,d)=1$ and n is a positive integer) is infinite. It follows that the number of primes in such a progression must be infinite.

The next two results show that while there are arbitrarily large gaps between two successive primes, we can still guarantee that there must be at least n primes not exceeding $2^{2^{n-1}}$.

Theorem 1.28. *For any integer n, there exist n consecutive composite numbers. In other words, the gaps between two successive primes is arbitrarily large.*

Proof: We simply have to observe that each of the consecutive integers

$$(n+1)!+2,\ (n+1)!+3,\ \cdots,\ (n+1)!+n+1$$

is composite. □

Theorem 1.29. *If p_n is the n-th prime number, then*

$$p_n < 2^{2^{n-1}}.$$

Proof: We will prove by induction on n. The assertion is clearly true for $n=1$. Suppose it is true for $n=k$. We know that $M = p_1p_2\cdots p_k+1$ is coprime to each p_i, $i \le k$. Therefore, either M is a prime or has a prime factor other than the $p_1, \cdots, p_k$. Therefore, the $(k+1)$-th rime p_{k+1} can not exceed M. Hence,

$$\begin{aligned} p_{k+1} &\le p_1p_2\cdots p_k+1 \\ &< 2\cdot 2^2\cdot 2^{2^2}\cdots 2^{2^{k-1}} \\ &= 2^{1+2+2^2+\cdots+2^{k-1}} \\ &= 2^{2^k-1} \\ &< 2^{2^k}. \quad \square \end{aligned}$$