MT231 - Finite Maths

Lecture Notes

Angel Cervera Roldan
21319203

25th October 2022

Sieve of Eratosthenes:
Given $n \in \mathbb{N}$, we can define the primes in $S := \{2, ..., n\}$. Then for a $m \in S$, either m is a prime, or $m = pr$, where $p, r \in S$. We can let the minimal in S be p by the well ordering principle. Then $p \leq r$. Now $p^2 \leq pr = m$, and so

$$p \leq \sqrt{m} \leq \sqrt{n}$$

Overall, m is a prime or m is divisible by an integer p with $2 \leq p \leq \sqrt{n}$.

Lemma 5.3

For integers a,b, let p be a prime divisor of ab. Then $p|a$ or $p|b$

If $p|a$, then there is nothing to prove. So assume that $p \nmid a$. Then $gcd(p, a) = 1$. We deduce from Euclid's lemma that $p|b$

Corollary 5.4

Let $p, a_1, a_2, ..., a_k$ be integers where p is prime. If $p|(a_1 \cdot a_2 \cdot ... \cdot a_k)$ then $p|a_i$ for some $i \in \{1, 2, ..., k\}$

Corollary 5.5

Let $q_1, q_2, ..., q_k$ be a prime integer if $p|(q_1 \cdot q_2 \cdot ... \cdot q_k)$, then $p = q_i$ for some i.

Theorem 5.6

Fundamental theorem of arithmetic
Given $n \in \mathbb{Z}$, non-zero, there exists $\varepsilon \in \pm 1$ and primes $p_1, ..., p_k$ such that:

$$n = \varepsilon \cdot p_1 \cdot ... \cdot p_k$$

Without loss of generality, we assume that $n \geq 1$.
The statement holds for $n = 1$. You would choose k to be 0, therefore no prime numbers will be selected, and $\varepsilon = 1$.
Now we assume that it holds for some $n \in \mathbb{Z}$.
In the case that n is a prime,then we choose $\varepsilon = 1$, and we are done.
Otherwise, there is some positive divisor, say m, of n such that $m \notin \{1, n\}$. Then $n = mr$, for some $r \in \mathbb{Z}$. Note that $1 < m, r < n$. By assumption, m and r are products of prime integers, and thus so is n. The uniqueness of this expression can be shown using Corollary 5.5.s So the statement holds for n, and so by induction it holds for all $n \geq 1$

Corollary 5.8

There is an infinite number of prime integers

Suppose $p_1, ..., p_n$ are all prime integers.

$$q = 1 + \prod_{i=1}^{n} p_i$$

q must be an integer which is not divisible by any of the p, hence q is a ‘new’ prime number by theorem 5.6.

Remark 5.9

1

Let $a, b \in \mathbb{Z} - \{0\}$, and let $p_1, ..., p_n$ be a complete list of prime integers dividing into a and/or b. Furthermore let

$$a = \varepsilon_a p_1^{r_1} \cdot ... \cdot p_n^{r_n}$$
$$b = \varepsilon_b p_1^{s_1} \cdot ... \cdot p_n^{s_n}$$

be the the respective prime factorisations of a and b (Note that $r_j, s_j \geq 0$ for all $j \in \{1, ..., n\}$ but some might be 0), then

$$gcd(a, b) = p_1^{min\{r_1, s_1\}} \cdot ... \cdot p_n^{min\{r_n, s_n\}}$$

2

Given $a, b \in \mathbb{Z}$, we let $lcm(a, b)$ denote the smallest =positive integer divisible by both a and b, called the least common multiple of a and b.
With a and b as above, we have

$$lcd(a, b) = p_1^{max\{r_1, s_1\}} \cdot ... \cdot p_n^{max\{r_n, s_n\}}$$

Exercises