LECTURE 5

September 15, 2023

1. Prime Numbers

Recall in the previous lecture, we have defined and shown the following:

REMARK 1.1. If $a, b \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, b) = 1$, then a and b are called *relatively prime* or *coprime*. In this case, by Bezout's Theorem (Theorem 2.3), there exists integers $x, y \in \mathbb{Z}$ such that $xa + yb = 1$.

REMARK 1.2. If $n \in \mathbb{N}$ with $n \geq 2$, always $1, n \in \{k \in \mathbb{N} : k \mid n\}$. A number $p \geq 2$ if this set is the smallest possible.

DEFINITION 1.3. A $p \in \mathbb{N}$ is called a prime number if

(1) $p \geq 2$
(2) the number $k \in \mathbb{N}$ such that $k \mid p$ are $k = 1$ and $k = p$.

EXAMPLE 1.4. $p = 7$ is a prime because its divisors are 1 and 7. But $n = 6$ is not prime because its divisors are 1, 2, 3, 6.

PROPOSITION 1.5. *Let $n \in \mathbb{N}$ with $n \geq 2$. If n is not prime, then there exists $a, b \in \mathbb{Z}$ such that $n = ab$ and $2 \leq a, b \leq n - 1$.*

PROOF. Since n is not prime, there exists an $a \in \mathbb{N}$ such that $a \mid n$ and furthermore, $a \neq 1$ and $a \neq n$. In particular, $2 \leq a \leq n - 1$. $a \mid n$ implies that there exists an integer $b \in \mathbb{Z}$ such that $n = ab$. We need to show that $2 \leq b \leq n - 1$. Indeed, $b > 0$ since $n = ab > 0$. Furthermore, $b \neq 1$ since if otherwise, then $n = a$, which is not true. Moreover, $b \neq n$ since that would imply that $a = 1$. Finally, if $b \leq n$, then $b \mid n$. Therefore, $2 \leq b \leq n - 1$ is the only possibility. $\square$

EXERCISE 1.6. Let p, q be prime. If $p \mid q$, then $p = q$.

PROOF. Let p, q be arbitrary prime numbers. Since $p \mid q$, then there exists an integer $k \in \mathbb{Z}$ such that $q = kp$. Since q is prime, it cannot be a product of two other integers, except if $k = 1$. So $q = 1 \cdot p$, and therefore, $p = q$, as desired. $\square$

PROPOSITION 1.7. *Let p be a prime number and $a, b \in \mathbb{Z}$, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

PROOF. Assume that $p \mid a$, then there is nothing to prove. If $p \not| a$, then we will show that $p \mid b$. Since p is prime and $p \not| a$, the $\gcd(a, p) = 1$ (the greatest common divisor of a and p is 1 since p does not divide a, and so the only value left that is a common divisor is 1.) By Bezout's Theorem (Theorem 2.3), there exists $x, y \in \mathbb{Z}$ such that

$$xa + yp = 1 \tag{1}$$

Since $p \mid ab$, there exists an integer $k \in \mathbb{Z}$ such that

$$ab = kp \tag{2}$$

Take (1), and multiply both sides by b so that

$$xab + ypb = b \tag{1}$$

Now, using (2), we can substitute (1) to (2) so that

$$xkp + ypb = b$$

and therefore,

$$(xk + yb)p = b$$

and so $p \mid b$, as desired. $\square$

COROLLARY 1.8. *Let p be a prime number and $a_1, a_2, ..., a_n \in \mathbb{Z}$ such that $p \mid a_1 a_2 \cdots a_n$. For some $1 \leq i \leq n$, $p \mid a_i$.*

PROOF. We will prove the corollary using induction. For the base case when $n = 2$, we have $p \mid a_1 a_2$, and by Proposition 1.7, $p \mid a_1$ or $p \mid a_2$. Now assume that for $n = k \in \mathbb{N}$, $p \mid a_1 a_2 \cdots a_k$ such that for some $1 \leq i \leq k$, $p \mid a_i$. We want to show that for $n = k + 1$, $p \mid a_1 a_2 \cdots a_{k+1}$ such that $p \mid a_i$. We consider the following cases:

(1) $\gcd(p, a_{k+1}) = p$, if so, let $i = n + 1$ and so $p \mid a_i$.
(2) $\gcd(p, a_{k+1}) = 1$, if so, $p \not| a_{n+1}$ so p and a_{n+1} are relatively prime and p divides $(a_1 \cdots a_n) a_{n+1}$, and thus, $p \mid a_1 \cdots a_n$.

Therefore, we have shown that $p \mid a_i$, $\square$

PROPOSITION 1.9. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ and assume that $\gcd(a, b) = 1$ and $a \mid bc$. Then $a \mid c$.*

PROOF. Assume that $\gcd(a, b) = 1$. Then by using Bezout's Theorem (Theorem 2.3), there exists integers $x, y \in \mathbb{Z}$ such that

$$xa + yb = 1 \tag{1}$$

Since $a \mid bc$, there exists an integer $k \in \mathbb{Z}$ such that

$$bc = ka \tag{2}$$

Now multiplying both sides of (1) by c, we have

$$xac + ybc = c \tag{1}$$

and now substituting (2) to (1) we obtain

$$xac + yka = c \Rightarrow a(xc + yk) = c$$

and therefore, $xc + yk \in \mathbb{Z}$ and so $a \mid c$, as desired. $\square$

THEOREM 1.10 (Fundamental Theorem of Arithmetic). *For every integer $n \in \mathbb{N}$ with $n \geq 2$, there exists perhaps repeating prime numbers $p_1 \leq p_2 \leq \cdots \leq p_\ell$, such that*

$$n = p_1 \cdot p_2 \cdots p_\ell$$

Furthermore, these are unique, if $q_1 \leq q_2 \leq \cdots \leq q_m$ are prime numbers such that

$$n = q_1 \cdot q_2 \cdots q_m$$

Then $\ell = m$ and for each $1 \leq i \leq \ell = m$, $p_i = q_i$.

EXAMPLE 1.11. $6 = 2 \cdot 3$, $21 = 3 \cdot 7$, $28 = 2 \cdot 2 \cdot 7$.

REMARK 1.12. By grouping repeating numbers, for $n \geq 2$, $n \in \mathbb{N}$, there exists prime numbers $p_1 < p_2 < \cdots < p_\ell$ and $k_1, k_2, ..., k_\ell \in \mathbb{N}$ such that

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_\ell^{k_\ell}$$

EXAMPLE 1.13. Take $28 = 2 \cdot 2 \cdot 7$ from above. Then $28 = 2^2 \cdot 7$. Take $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. Then $360 = 2^3 \cdot 3^2 \cdot 5$.

PROOF. We will prove the theorem for $n \in \mathbb{N}$ with $n \geq 2$ by strong induction, starting with $n = 2$. Take $p_1 = 2$, i.e. $n = p_1$. Next, assume

$$2 = q_1 \cdot q_2 \cdots q_m$$

where $q_1, q_2, ..., q_m$ are prime. Take $1 \leq i \leq m$, then $q_i \mid 2$ implies that $q_i = 2$, and therefore, $2 = 2^m$ and so $m = 1$.

Let $k \in \mathbb{N}$ with $k \geq 2$ such that for all $2 \leq n \leq k$, the conclusion holds. Take $n = k + 1$, and we want to show that the conclusion also holds. We will take two cases.

1. Assume that $k + 1$ is prime, then we are done...same argument as the base case.
2. Assume that $k + 1$ is not prime, i.e. $k + 1$ is composite. By the Proposition 1.7, there exists $a, b \in \mathbb{Z}$ such that $k + 1 = ab$ and $2 \leq a, b \leq k$, by the inductive hypothesis, there exists $p_1^{(a)}, p_2^{(a)}, ..., p_s^{(a)}$ and $q_1^{(b)}, q_2^{(b)}, ..., q_t^{(b)}$ such that $a = p_1^{(a)} \cdots p_s^{(a)}$ and $b = q_1^{(b)} \cdots q_t^{(b)}$ (and they are all prime), therefore $k + 1 = ab = p_1^{(a)} \cdots p_s^{(a)} \cdot q_1^{(b)} \cdots q_t^{(b)}$. By relabelling, there are prime numbers $p_1 \leq \cdots \leq p_\ell$ such that $k + 1 = p_1 \cdots p_\ell$.

To prove the uniqueness, take prime numbers $q_1 \leq q_2 \leq \cdots \leq q_m$ such that $k + 1 = q_1 \cdots q_m$. We prove that $\ell = m$ and for each $1 \leq i \leq \ell = m$, $p_i = q_i$. Since $q_1 \mid k + 1 = p_1 \cdots p_\ell$, there exists $1 \leq i \leq \ell$ such that $q_1 \mid p_i$ and therefore $q_1 = p_i$. So now, we have $p_1 = q_j \geq q_1 = p_i \geq p_1$, i.e. they are equal or $p_1 = q_1$. Now, $k + 1 = p_1 \cdots p_\ell = q_1 \cdots q_m$, and therefore, by left cancellation,

$$p_2 \cdots p_\ell = q_2 \cdots q_m$$

Now take $c = p_2 \cdots p_\ell$, then $2 \leq c < k+1$, and so $c = p_2 \cdots p_\ell = q_2 \cdots q_m$. By the inductive hypothesis, both ways are equivalent, i.e. length is the same $\ell = m$, and $p_2 = q_2$,..., $p_\ell = q_\ell$, as desired.

$\square$