M 328K: Lecture 4

Katherine Ho

September 5, 2024

1

1. If $a|c$ and $b|c$, must $ab|c$?
   False: $a = b = c = 2$, $2|2$, $2|2$ but $4 \nmid 2$
2. If $a|bc$ and $a \nmid b$, must $a|c$?
   False: $a = 4, b = c = 2$

But... Proposition: Let $a, b, c \in \mathbb{Z}$

1. If $a|c, b|c$ and $\gcd(a, b) = 1$, then $ab|c$.

   Proof. By Bezout, there exist integers x, y s.t. $ax + by = 1$. Then, $acx + bcy = c$.
   By definition, there exist $r, s \in \mathbb{Z}$ s.t. $c = ar = bs$. Thus,

   $$a(bs)x + b(ar)y = c$$
   $$ab(sx + ry) = c$$

   So, $ab|c$. □

2. If $a|bc$, and $\gcd(a, b) = 1$, then $a|c$. (Euclid's Lemma)

   Proof. Again, there exist $x, y \in \mathbb{Z}$ s.t. $ax + by = 1$. Then $acx + bcy = c$.
   Since $a|bc$, we have $bc = ar$ for some $r \in \mathbb{Z}$. Hence

   $$acx + ary = c$$
   $$a(cx + ry) = c$$

   So, $a|c$ as desired. □

2 Prime Numbers

Definition 2.1. *A prime p is an integer greater than 1 that is only divisible by 1 and p.*

Theorem 2.1 (Euclid's Lemma)**.** *If p is prime and $p|ab$ $(a, b \in \mathbb{Z})$, then $p|a$ or $p|b$ (or both).*

Proof. Suppose $p \nmid a$. Since p is prime, this implies that $\gcd(p, a) = 1$.
Then by Euclid's Lemma, we have $p|b$. □

Corollary 2.1.1. *If p is prime and $p|(a_1 a_2 \ldots a_n)$ then $p|a_k$ for some $k, 1 \leq k \leq n$.*

Proof by Induction. Base case ($n = 1$). Tautology *(If A then A)
Inductive step: Assume that for some $n \geq 1$, if p divides the product of any collection of n integers $a_1 \ldots a_n$, then $p|c_k$ for some k.
Suppose $p|a_1 a_2 \ldots a_n a_{n+1}$. By Euclid's Lemma, $p|a_1 a_2 \ldots a_n$ OR $p|a_n + 1$.
In the latter case, we are done.
Hence assume now that $p|a_1 a_2 \ldots a_n$. By IH, $p|a_k$ for some $k, 1 \leq k \leq n$ as desired. □

Corollary 2.1.2. *If p, q_1, q_2, q_n are primes, and $p|q_1 q_2 \dots q_n$, then $p = q_k$ for some k.*

Proof. By the previous result, $p|q_k$ for some k. Since q_k is prime and $p > 1$, we have $p = q_k$. $\square$

Theorem 2.2 (Fundamental Theorem of Arithmetic, FTA)**.** *Every integer $n > 1$ can be expressed as a product of primes. Moreover, this expression is unique up to reordering the factors.*

Proof by Induction on n. Base case ($n = 2$).
Induction step: Assume that any integer (> 1) less than or equal to n satisfies FTA.
Now consider $n + 1$.
If $n + 1$ is prime, we are done. Otherwise, assume $n + 1 = ab$ for some $1 < a, b < n + 1$. By IH, a and b can be expressed as a product of primes, hence so can $n + 1$. This proves the existence statement.

For uniqueness, take the same IH. Suppose that we can express $n + 1$ as

$$n + 1 = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

where p_r, q_s are prime. Without loss of generality, assume

$$p_1 \leq p_2 \leq \cdots \leq p_r, \text{ and } q_1 \leq q_2 \leq \cdots \leq q_s$$

Note $p_1 | q_1 q_2 \dots q_s$, so $p_1 = q_i$ for some i. By the same argument, $q_1 = p_j$ for some j.
Since $p_1 \leq p_j$ and $q_1 \leq q_2$, this implies $p_1 = q_1$. By cancelling, we have $p_2 \dots p_r = q_2 \dots q_s$.
Since $p_2 \dots p_r = q_1 \dots q_s \leq n$, we can apply IH to conclude that $r = s$ and $p_i = q_i$ for all i. $\square$

Theorem 2.3. *There exist infinitely many primes.*

Proof (Euclid). Assume that $p_1 \dots p_n$ is a list of n primes.
Consider the integer $N = p_1 \dots p_n + 1$. Note that no p_i can divide N, otherwise

$$\begin{aligned} &p_i | (N - p_1 \dots p_n) \\ &p_i | 1 \\ &\quad nooooo \end{aligned}$$

But N is divisible by some prime p with $p \neq p_1, \dots, p_n$. Thus, there are infinitely many primes. $\square$