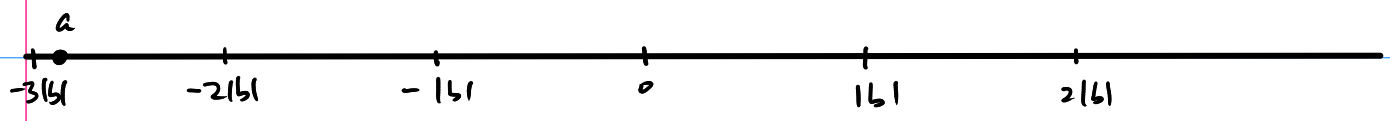
Lecture 1: Let $\mathbb{Z}$ denote the set of integers, that is,

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}.$$

Given two integers a, b, we say that "a divides b" if there is an integer c such that $b = ac$. We also write this as $a \mid b$.

Given two integers a, b with $b \neq 0$, there is a unique way to write $a = bq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < |b|$.



Let $q+1$ be the smallest integer such that $a < (q+1)|b|$. Then $a \geq q|b|$ and so we may write $a = q|b| + r$ $\quad 0 \leq r < |b|$.
If $b > 0$ then $a = qb + r$. If $b < 0$ then $a = -qb + r$.

Clearly, $b \mid a \iff r = 0$.

Greatest Common Denominator (GCD): Let a, b be two integers. The GCD of a and b is the largest $d > 0$, $d \in \mathbb{Z}$ such that $d \mid a$ and $d \mid b$. (Clearly we assume here that at least one of a or b is nonzero). The gcd is denoted (a, b).

Lemma: Let $d = (a, b)$. Then there are integers x and y such that $ax + by = d$.
Proof: Consider the ideal in $\mathbb{Z}$ generated by a and b, that is, the set $S = \{am + bn \mid m, n \in \mathbb{Z}\}$.
Let c be the smallest positive element of S. We claim

that $c|a$. If not, we may write $a = qc + c'$ with $0 < c' < c$. As $c' = a - qc$, it follows that $c' \in S$, which contradicts the minimality of c. Thus, $c|a$. Similarly, $c|b$. As $c = am + bn$ and $d|a, b \Rightarrow d|c$. But d was the largest among all divisors of a and b. This shows that $d = c$.
Thus, we have found m, n such that $d = am + bn$.
This completes the proof of the lemma.

Corollary: Let $d'|a, b$. Then $d'|d$.
Proof: $d = ax + by$. $d'|a, b \Rightarrow d'|d$.

In the same way as above, we can define the gcd of a set of integers $x_1, \dots x_m$. As above we can prove

Lemma: If d is the gcd of $x_1, \dots x_m$, then there are integers $a_1, \dots, a_m$ such that $d = a_1 x_1 + \dots + a_m x_m$.

Lemma: If $d'|x_i \ \forall i$ then $d'|d$.

Definition: If the $\gcd(a, b) = 1$ then we say a and b are coprime.

Euclid's algorithm: Suppose we are given two integers r_0 and r_1. The following algorithm finds the gcd.

We may assume that $r_0 > r_1 > 0$.
Define integers q_i and r_{i+1} as follows:

$r_0 = q_1 r_1 + r_2 \qquad 0 \leq r_2 < r_1$

$r_1 = q_2 r_2 + r_3 \qquad 0 \leq r_3 < r_2$

$\vdots \qquad\qquad \vdots$

$$r_i = q_{i+1} r_{i+1} + r_{i+2} \qquad 0 \leq r_{i+2} < r_{i+1}$$

As the r_i is a strictly decreasing sequence of positive integers, there is some ℓ such that $r_{\ell+2} = 0$. Then we have

$$r_\ell = q_{\ell+1} r_{\ell+1} \Rightarrow r_{\ell+1} \mid r_\ell$$

$$r_{\ell-1} = q_\ell r_\ell + r_{\ell+1} \Rightarrow r_{\ell+1} \mid r_{\ell-1}$$

$$r_{\ell-2} = q_{\ell-1} r_{\ell-1} + r_\ell \Rightarrow r_{\ell+1} \mid r_{\ell-2}$$

$$\vdots$$

$$\Rightarrow r_{\ell+1} \mid r_1$$

$$\Rightarrow r_{\ell+1} \mid r_0$$

$\Rightarrow r_{\ell+1} \mid d$, where $d = \gcd(r_1, r_0)$.

Conversely, note that as $d \mid r_1, r_0$ and $r_0 = q_1 r_1 + r_2$ $\Rightarrow d \mid r_2$. As $r_1 = q_2 r_2 + r_3 \Rightarrow d \mid r_3 \ldots \Rightarrow d \mid r_{\ell+1}$.

Thus, $r_{\ell+1} = d$. This proves that the algorithm finds the gcd.

Definition: Let $n \in \mathbb{Z}$ and assume $n > 1$. We say n is prime if the only integers which divide n are ± 1 and n.

Lemma: Let p be a prime. If $p \mid mn$, then it divides m or n.

Proof: Assume $p \nmid m$. Then there is no $d > 1$ which divides both p and m. Thus, $(p, m) = 1$. Thus, $\exists\, x, y \in \mathbb{Z}$ such that $px + my = 1$. Thus, $pxn + mny = n$. As $p \mid mn$ $\Rightarrow p \mid n$.

Theorem: Let $n > 1$ be an integer. Then there are distinct primes $p_1, \dots, p_\ell$ such that $n = p_1^{a_1} \cdots p_\ell^{a_\ell}$. If n can be written in another way as a product $n = q_1^{b_1} \cdots q_m^{b_m}$, where q_i's are distinct primes, then $\ell = m$, and there is a permutation σ of $\{1, \dots, m\}$ such that $p_i = q_{\sigma(i)}$ and $a_i = b_{\sigma(i)}$.

Proof: The existence of such a factorization follows by induction on n as follows. If n is prime then there is nothing to prove. If n is not prime, then we can write $n = n_1 n_2$, where $n_i > 1$. By induction hypothesis both n_1, n_2 have a prime factorization. Combining these we get a factorization for n.

For uniqueness, we use the previous lemma. We have

$$\prod_{i=1}^{\ell} p_i^{a_i} = \prod_{j=1}^{m} q_j^{b_j}$$

$\Rightarrow p_i$ divides the LHS and so also the RHS. Using the previous lemma we easily conclude that $\{p_1, \dots p_\ell\} \subset \{q_1, \dots q_m\}$. Similarly we conclude that $\{q_1, \dots q_m\} \subset \{p_1, \dots, p_\ell\}$. This shows that $\ell = m$ and both these sets are equal. The rest of the proof of uniqueness is left as an exercise.

Infinitude of primes: It is natural to ask if there are infinitely many primes. That this is true is a theorem of Euclid's who proved it by contradiction. Assume there are only finitely many primes, which we may denote by $p_1, p_2, \dots p_n$. Consider the number $N = p_1 p_2 \cdots p_n + 1$. Then either N is

prime, or it has a prime factor q. This forces that $q = p_i$ for some i. This shows that $p_i \mid p_1 \cdots p_n + 1$

$\Rightarrow p_i \mid 1$, which is a contradiction.