1.2 Lecture 2

Preamble: We will show why any positive integer has a unique decimal expansion. Then we will define the greatest common divisor (gcd). We will prove that the gcd of two integers can be expressed as a linear combination of the two integers.

Keyword: decimal expansion, greatest common divisor, Bezout's lemma

1.2.1 Decimal Expansion of a Positive Integer

We take it for granted that any positive integer has a decimal expansion. Now we will give a rigorous proof based on division algorithm. Our proof will work not just for base 10 but for any base $b > 1$.

PROPOSITION 1.5. *Let $b > 1$ be a positive integer. Any positive integer n can be written uniquely as*

$$n = c_k \cdot b^k + c_{k-1} \cdot b^{k-1} + \cdots + c_1 \cdot b + c_0, \qquad 0 \leq c_i < b, \;\; c_k \neq 0$$

for some non-negative integer.

Proof: We will first show the existence of such an expansion. If $n < b$, then $n = c_0$ is the required expansion. If $n \geq b$, by division algorithm we can write

$$n = bq + c_0, \qquad 0 \leq c_0 < b, \;\; q \geq 1.$$

If $q < b$, then the above is the expansion we are looking for. If $q > b$, we write

$$q = bq_1 + c_1, \qquad 0 \leq c_1 < b, \;\; q_1 \geq 1$$

and obtain

$$n = b(bq_1 + c_1) + c_0 = b^2 q_1 + bc_1 + c_0.$$

As before, we get the required expansion if $q_1 < b$. If $q_1 > b$, we again use the division algorithm. As n is a fixed integer, there will be an integer k such that $b^k \leq n < b^{k+1}$ and we must have $1 < q_k < b$. This proves the existence. Now suppose we have two such expansions for the same integer n, i.e.,

$$c_k.b^k + c_{k-1}.b^{k-1} + \cdots + c_1.b + c_0 = d_r \cdot b^r + d_{r-1} \cdot b^{r-1} + \cdots + d_1 \cdot b + d_0.$$

Let i be the first suffix for which $c_i \neq d_i$. Then, we have

$$\begin{aligned} & b^{i+1} \mid \Big[\big(c_k \cdot b^k + \cdots + c_{i+1} \cdot b^{i+1} + c_i \cdot b^i\big) - \big(d_r \cdot b^r + \cdots + d_{i+1} \cdot b^{i+1} + d_i \cdot b^i\big)\Big] \\ \implies \quad & b^{i+1} \mid \big(c_i \cdot b^i - d_i \cdot b^i\big) \\ \implies \quad & b \mid (c_i - d_i). \end{aligned}$$

As $0 \leq c_i, d_i < b$, the last congruence must imply $c_i - d_i = 0$, which is a contradiction. This proves the uniqueness. □

1.2.2 Greatest Common Divisor

DEFINITION 1.6. *Let a and b be two integers (not both 0). If an integer d divides both a and b, we say that d is a* **common divisor** *of a and b. The* **greatest common divisor** *of two integers a and b is the unique* **positive** *integer d satisfying*
(1) $d \mid a$ and $d \mid b$.
(2) If $c \mid a$ and $c \mid b$ then $c \leq d$.
We denote the greatest common divisor of a and b by $gcd(a, b)$ or simply by (a, b).

When talking about $gcd(a, b)$, we avoid the case of both the integers a and b being 0 as any non-zero integer is a common divisor for both, and it would not be possible to define the greatest amongst those. The definition of *gcd* can easily be extended to any finite set of integers (not all 0). From the second property in the definition above, it is clear that $gcd(a, b)$ is unique.

For example, the set of positive divisors of -32 and 44 are 1, 2 and 4. Hence $gcd(-32, 44) = 4$. Similarly, $gcd(12, 42) = 6$. Observe that

$$\begin{aligned} gcd(-32, 44) &= 8 = -32 \times (-3) + 44 \times (-2) \\ gcd(12, 42) &= 6 = 12 \times 4 + 42 \times (-1). \end{aligned}$$

In the above two examples, the gcd of two integers turns out to be an (integral) linear combination of the integers. The following theorem states that it is always true. This result is known as Bezout's lemma.

LEMMA 1.7. (Bezout's Lemma) *If a and b are two integers, not both zero, then their gcd can be written as $ax + by$ for some integers x and y.*

Proof: Consider the set

$$S = \{ax + by > 0 \mid x, y \in \mathbb{Z}\}.$$

The set S is clearly nonempty, as

$$0 < a \cdot a + b \cdot b \in S.$$

By the well-ordering principle, S has a least element d. As $d \in S$, we can write $d = ax_0 + by_0$ for some integers x_0 and y_0 as $d \in S$. It is now enough to show that d is the gcd of a and b. Observe that if c is a common divisor of a and b, then c also divides $ax + by$ for any choice of integers x and y. Therefore, c divides d, and in particular, $c \leq d$. We next show that d divides a and b. By division algorithm, $a = dq + r$ for some $0 \leq r < d$. Then $r = a - dq = a - (ax_0 + by_0) = a(1 - x_0) + b(-y_0)$. If $r > 0$, r will be an element in S which is smaller than d. This is a contradiction to the minimality of d in S. Hence, $r = 0$ and $d \mid a$. Similarly, $d \mid b$. Thus, $d = ax_0 + by_0$ is the gcd. □

Note that such a linear combination is not unique. In fact, there are infinitely many integers x and y such that $d = ax + by$. If $d = ax_0 + by_0$, then clearly $d = a(x_0 + bn) + b(y_0 - an)$ for any integer n. The above theorem confirms only the existence of a linear combination of two integers a and b expressing the gcd d, but it does not tell us how to find the integers x and y giving $d = ax + by$. In the next lecture we will introduce Euclid's algorithm, which will provide us a method of determining x and y from a and b. Before discussing Euclid's algorithm, we need to characterize the gcd of two integers in the following way as well:

PROPOSITION 1.8. *Let a and b are two integers, not both zero. Then a positive integer d is the gcd of a and b if and only if*

1. $d \mid a, \;\; d \mid b$
2. $c \mid a, \;\; c \mid b \implies c \mid d$

Proof: If d is the gcd of a and b in definition 1.6, the first property clearly holds. Now, by the preceding theorem, we have $d = ax_0 + by_0$ for some integers x_0 and y_0. Hence, any c dividing a and b will divide $ax_0 + by_0 = d$. Conversely, if an integer d satisfies the two properties mentioned above, then any common divisor c of a and b will divide d, and hence will be less that d. □