Linear Diophantine Equations

Munir Uz Zaman

Date: February 7, 2022

§1 Bezout's Identity

Theorem 1.1 (Bezout's Identity)
If a, b are non-zero integers and $d = \gcd(a, b)$ then there exists $x, y \in \mathbb{Z}$ such that

$$ax + by = d$$

Proof: We will show that d is the smallest integer in the set

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

By the well ordering principle, the set has a minimum element. Let d be the minimum element of S. We will first show that d is a common divisor of a and b.
Suppose $a = qd + r$ where $0 \leq r < d$. Now

$$a = qd + r \implies a = q(ax + by) + r \implies r = (1 - qx)a + (-qb)y$$

If $r > 0$ then r must be an element of S. But that contradicts our assumption that d is the minimal element of S since $r < d$. Therefore $r = 0 \implies d \mid a$. Likewise we can show that $d \mid b$. Therefore d is a common divisor of a, b. Now we need to show that d is the largest common divisor of d. Suppose g is a common divisor of a, b and $a = gm$ and $b = gn$. Now

$$ax + by = d \implies g(mx + ny) = d \implies g \mid d \implies g \leq d$$

Thus d is the largest common divisor of a and b.

♣

Corollary 1.1.1
If a, b are coprime integers then there exists integers x, y such that

$$ax + by = 1$$

Theorem 1.2 (Euclid's Lemma)
If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

Proof: Suppose $bc = ak$ where $k \in \mathbb{Z}$. Since $\gcd(a, b) = 1$, there exists integers x, y such that

$$\begin{aligned} ax + by = 1 &\implies (ac)x + (bc)y = c \\ &\implies (ac)x + (ak)y = c \\ &\implies a(cx + ky) = c \\ &\implies a \mid c \end{aligned}$$

♣

Theorem 1.3 (General Bezout's Identity)

If $a_1, a_2, \cdots, a_n$ are non-zero integers then there exists integers $x_1, x_2, \cdots, x_n$ such that

$$a_1x_1 + \cdots + a_nx_n = \gcd(a_1, \cdots, a_n)$$