

## 3. WOP.

a) Apply the WOP to prove that there cannot be an infinite strictly decreasing sequence of natural numbers.

Let  $S = \{n \in \mathbb{N} : \text{infinite strictly decreasing sequence starting with } n\}$ , which  $S \subseteq \mathbb{N}$ .

WTS:  $S = \emptyset$ .

I'll use prove by contradiction. Assume  $S \neq \emptyset$ .

Since  $S \neq \emptyset, S \subseteq \mathbb{N}$ , according to WOP, there exist  $n_0 \in S$  s.t.  $\forall s' \in S, n_0 \leq s'$ .  
However, since  $S$  is a strictly decreasing sequence, gives, starting from  $n_0$ , we have,  $n_0 > n_0' > n_0'' > \dots > n_0^{(i)}$  in  $S$ , contradicts to  $\forall s' \in S, n_0 \leq s'$  (e.g. when  $s' = n_0'$  it contradicts).

Therefore,  $S = \emptyset$ , which there can not be an infinite strictly decreasing sequence of natural numbers. ■

b) Apply WOP to prove that, for any integers  $n$  and  $d > 0$ , there are unique integers  $r \in \{0, 1, 2, \dots, d-1\}$  and  $q$  such that

$$n = dq + r.$$

Note: How is this a proof of the fact given in the paragraph preceding Theorem 3.1.4?

Let  $n \in \mathbb{Z}$ . Let  $d \in \mathbb{Z}, d > 0$

WTP: ①  $r \in \{0, 1, 2, \dots, d-1\}$ ,  $q$  exists ②  $r, d$  is unique.

Proof: ① Since  $d \in \mathbb{Z}, d > 0$ , gives  $d \in \mathbb{N}$ .

Let  $S = \{n - dq, \text{ where } q \in \mathbb{Z}, n - dq \geq 0\}$ , I'll show  $S$  is not an empty set, and  $S \subseteq \mathbb{N}_0$ .

Case ①  $n \geq 0$ .

When  $n \geq 0$ , take  $q \in \mathbb{N}_0$ . Since  $n - dq \geq 0$ , gives  $n - dq \in \mathbb{N}_0$ , which  $S \subseteq \mathbb{N}_0$ . Take  $q = 0$ , gives  $n - dq = n \geq 0$ , which is in  $S$ , gives  $S \neq \emptyset$ .

Case ②  $n < 0$ .

When  $n < 0$ , take  $q = n, q \in \mathbb{Z}, q < 0$ . Since  $d > 0, d \in \mathbb{N}$ , gives  $n - dq = n - d \cdot n = (1-d)n \geq 0$ , which is in  $S$ .

gives  $S \neq \emptyset$ . Since  $n - dq \geq 0$ , gives  $n - dq \in \mathbb{N}_0$ , which  $S \subseteq \mathbb{N}_0$ .

Thus, I'll use WOP on  $S$  as  $S$  is non-empty and  $S \subseteq \mathbb{N}_0$ .

By WOP,  $S$  contains smallest element called  $r'$ , gives  $r' \geq 0$ .

Since  $r' \in S$ , gives  $\exists q' \in \mathbb{N}$  s.t.  $r' = n - d \cdot q'$ , which  $n = r' + d \cdot q'$ .

WTP:  $r' < d$ .

I'll use prove by contradiction.

Assume that  $r' \geq d$ , gives  $r' - d \geq 0$

Since  $r' - d = n - d \cdot q' - d = n - d \cdot (q' + 1)$ . Since  $q' + 1 \in \mathbb{N}, d \in \mathbb{N}$ , gives  $r' - d \in S$ , called  $r'' = r' - d$

Since  $d > 0, d \in \mathbb{N}$ , gives  $r'' < r'$ , contradicts to  $r'$  is the smallest element in  $S$ .

Therefore, I've proved the existence of  $r \in [0, d)$  and  $q$ .

②. Since  $d \in \mathbb{Z}, d > 0$ , gives  $d \in \mathbb{N}$

I'll prove by using contradiction  $r_1, r_2 \in \mathbb{Z}$ .

Assume.  $\exists q_1, q_2 \in \mathbb{Z}, \exists r_1, r_2 \in [0, d)$ , which  $q_1 \neq q_2, r_1 \neq r_2$ , that  $n = d \cdot q_1 + r_1$  and  $n = d \cdot q_2 + r_2$ .

From assumption, gives  $d \cdot q_1 + r_1 = d \cdot q_2 + r_2$ , which.

$$d \cdot q_1 - d \cdot q_2 + r_1 - r_2 = 0 \Rightarrow d \cdot (q_1 - q_2) + (r_1 - r_2) = 0.$$

Since from the definition of divisibility,  $d \mid 0$ , as  $d > 0, d \in \mathbb{N}$ .

Gives  $d \cdot (q_1 - q_2) + (r_1 - r_2)$  should also divides  $d$ , which  $d \mid (r_1 - r_2)$ .

Since  $0 \leq r_1, r_2 < d$ , gives  $-d < r_1 - r_2 < d$ , which when  $r_1 - r_2 = 0$ ,  $d \mid (r_1 - r_2)$ , that  $r_1 = r_2$ .

Since  $r_1 - r_2 = 0, d > 0, d \in \mathbb{N}$ , gives  $q_1 - q_2 = 0$ , which  $q_1 = q_2$ .

Thus, contradicts to  $r_1 \neq r_2, q_1 \neq q_2$ .

Therefore, I've prove the uniqueness. ■