USEFUL CONCLUSIONS FOR PROBLEM SETS

ZIMO LUO

The conclusions listed below are quite useful for grinding problem sets, but sadly they are not permitted to use unless first proven – that's why we have them right here.

Theorem 1 (Induction)**.** For every statement $P(n)$ where $n \in \mathbb{Z}^+$, if $P(1)$ is true and $P(s) \Rightarrow P(s+1)$ for some $s \in \mathbb{Z}^+$, then the statement $P(n)$ is true for every $n \in \mathbb{Z}^+$.

Proof. Suppose $P(n)$ is a statement such that $P(1)$ is true and $P(s) \Rightarrow P(s+1)$ for some $s \in \mathbb{Z}^+$.

Let $S = \{a \in \mathbb{Z}^+ | P(a) \text{ is false}\} \subseteq \mathbb{Z}^+$. By *WOP*, there exists $l \in S$ such that l is the least element in S. Since $P(1)$ is true, $1 \notin S$, so $l \neq 1$. By *OLE*, 1 is the least element in $\mathbb{Z}^+$ overall. It thus follows $l > 1$. This implies $l - 1 \in \mathbb{Z}^+$. But since l is the least element of S, $l - 1 \notin S$. Therefore, $P(l-1)$ is true. Hence, by definition of $P(n)$, $P(l-1+1) = P(l)$ is also true. This contradicts the fact that $l \in S$, implying that $S = \emptyset$. Therefore, $P(n)$ is true for all $n \in \mathbb{Z}^+$ □

Theorem 2 (Division Algorithm)**.** For $a, b \in \mathbb{Z}^+$, we can write

$$a = bq + r \quad \text{for } r, q \in \mathbb{Z}^+, 0 \leq r < b.$$

Proof. Consider $S = \{bq + r \mid \forall r \in \mathbb{Z}^+, 0 \leq r < b\}$. We will show $a \in S$.

Now, say $B = \{a : a \notin S\}$ is a non-empty subset of $\mathbb{Z}^+$. Since $B \subseteq \mathbb{Z}^+$, by *WOP*, B has a minimal element $1 \notin B$, because $1 = 0 \times 1 + 1$. Thus l, the least element of B, is greater than 1. Note that if $x \in S$, so is $x + 1$.

Thus consider $l - 1$. Since l is the least value of B, $l - 1 \notin B$ because $l - 1 < l$. But if $l - 1 \in S$, then $l \in S$ as well. This contradicts the fact that l is the least element of S, implying that $S = \emptyset$. □

Theorem 3 (Bezout's Identity)**.** For $a, b \in \mathbb{Z}$, we can express $\gcd(a, b)$ as an integer linear combination of a and b. That is, there exists integer solutions for

$$ax + by = \gcd(a, b).$$

Proof. Consider the equation $s = ax + by$, where $s \in \mathbb{Z}^+$. Let $S \subseteq \mathbb{Z}^+$ be the non-empty set of positive integers of solutions for $ax + by$.

Date: June 25, 2023.

Consider l, the least element of S. We thus have

$$ax + by = l$$

Now, apply the division algorithm to a and l.

$$a = ql + r, \quad 0 \leq r < l$$

$$a = qax + qby + r$$

$$r = a(1 - qx) - b(qy)$$

Rearranging the equation, we find that r also satisfy the linear combination of a and b. But since $r < l$, in order not to contradict the fact that l is the least element of S, we must have $r = 0$.

Thus $l \mid a$. By a similar argument we can also show that $l \mid b$. Thus l is a common factor of a and b. Consider $d = \gcd(a, b)$. In Set #3 Problem 11 we've shown that $l \mid d$. Since $d \mid a$ and $d \mid b$, we have that d divides any linear combination of a and b, which includes l. Because $d \mid l$ and $l \mid d$, it follows that $d = l$. Thus there exists integer solutions for the equation

$$ax + by = \gcd(a, b).$$

$\square$