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 $P(s) \implies P(s+1)$ 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 $P(s) \implies P(s+1)$ 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

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

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 $S = \emptyset$. □

Date: June 28, 2023

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 $ax + by$.
Consider l, the least element of S. We thus have

$$ax + by = l$$

Now, apply the division algorithm to a and l.

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

$$a = qax + qby + r$$

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

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

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

□

Theorem 4

$\gcd(m, n) = 1$ *implies* $\gcd(mn, m + n) = 1$

Proof. Consider m, n where $\gcd(m, n) = 1$. Assume $\gcd(mn, m+n) > 1$. Then there must be some p that $\gcd(mn, m + n)$. Then $p \mid mn$. Thus $p \mid m$ or $p \mid n$. But since $p \mid m + n$, if p divides one of

m and n, then it also divides the other one. But if $p \mid m$ and $p \mid n$, then $p \leq \gcd(m,n) = 1$, which is not possible. Thus $\gcd(m,n)$ implies $\gcd(mn, m+n) = 1$. $\square$

Theorem 5: Division Algorithm in $\mathbb{Z}_m[x]$

Division algorithm applies in $\mathbb{Z}_m[x]$.

Proof. Let us define S to be the set of polynomials $r(x)$ with degree n with $r(x) = f(x) - q(x) \cdot g(x)$.

We first show that S is non empty. Simply taking $q(x)$ gives $r(x) = f(x)$, which is valid. Therefore $r(x) = f(x)$ must be in the set S.

If 0 is in S, then we are done, since we can take $r(x) = 0$ and $f(x) = q(x) \cdot g(x) + r(x)$. Therefore let $0 \notin S$. Since degrees are nonnegative integers, without 0, it must be positive. We can therefore apply WOP to S and get a polynomial $r_l(x)$ in S with minimal degree and its associated $q_l(x)$. By definition, $\deg(r_l(x)) > \deg(g(x))$. Let the leading coeffecient of $r_l(x)$ be L, and $g(x)$ be G. Since G is a unit in m, let the inverse of G mod m be G^{-1}. We then know $L \equiv L \cdot (G \cdot G^{-1}) \bmod m$.

Assume for contradiction that $r_l(x)$ has degree $n \geq \deg(g(x))$. Now consider the polynomial $p(x) = r_l(x) - (L \cdot G^{-1})(x^{\deg(r_l(x)) - \deg(g(x))})g(x)$. Note that $\deg(p(x)) < \deg(r_l(x))$, since the leading term of $r_l(x)$ is cancelled. But $p(x)$ is also in the set S, since we have $p(x) = f(x) - (r_q(x) + (L \cdot G^{-1})(x^{\deg(r_l(x)) - \deg(g(x))}))g(x)$. This raises a contradiction, since by WOP we assumed $r_l(x)$ has the minimal degree. Therefore, there exist a $r(x)$ with degree n such that $0 \geq n < \deg(g(x))$. $\square$