Some Well Ordered Class Notes

**Theorem 1. Well Ordering Principle** Every non-empty subset of $\mathbb{Z}^+$ has a least element.

From this seemingly obvious and innoquous result stem two very important facts about $\mathbb{Z}^+$.

**Corollary 1. Mathematical Induction**

If $P(n)$ is a statement about integers and

1. (Root) $P(1)$ is true.
2. (Inductive Step) $P(k+1)$ is true if $P(k)$ is true.

Then $P(n)$ is true $\forall n \in \mathbb{Z}$.

**Proof.** Let $A = \{ k : P(k) \text{ is false} \}$. If $A \neq \emptyset$, then $A$ has a least element, say $k$. Owing to the “Root” of induction, $k \neq 1$, so $k - 1 \in \mathbb{Z}^+$. And since $k - 1 < k$, $k - 1 \notin A$ so $P(k - 1)$ is not false, it’s true!! But then the “Inductive Step” says that $P((k - 1) + 1) = P(k)$ is true. Hence, our assumption that $A \neq \emptyset$ must have been false. That is, $A = \emptyset$ or, what’s the same thing, $P(n)$ is true $\forall n$. \[\square\]

**Corollary 2. Euclidean Algorithm**

Suppose $m, n \in \mathbb{Z}^+$. Then $\exists q, r \in \mathbb{Z}^+$ such that $m = nq + r$ and $0 \leq r < n$.

**Proof.** Define $A = \{ m - ns : s \in \mathbb{Z} \}$. If $0 \notin A$, then $m = qn$ for some $q$ and we are done. If $0 \notin A$, then $A$ has a least positive element (The least element of $A \cap \mathbb{Z}^+$), say $r$. Then since $r \in A$, there is a $q \in \mathbb{Z}^+$ such that $r = m - nq$ or, $m = nq + r$. If $r > n$, then $m - n(q - 1) = m - nq - n = r - n > 0$ and so $m - n(q - 1)$ would be in $A$ and at the same time, $m - n(q - 1) = r - n < r$. This contradicts the fact that $r$ is the least positive number in $A$. Hence, $0 \leq r < n$. \[\square\]

Here are some definitions for your flashcards.

1. The number $d$ is called a **divisor** of $a$ if $\exists n$ such that $a = dn$.

2. The number $d$ is called a **common divisor** of $a$ and $b$ if $d$ is a divisor of both $a$ and $b$.

3. The number $d$ is called the **greatest common divisor** of $a$ and $b$ if $d$ is a common divisor and if $d_1$ is any other common divisor, $d > d_1$.

**Theorem 2. GCD**

Every pair $(n, m)$ of integers has a greatest common divisor, $d = \gcd(n, m)$. Moreover, $d$ is the least positive element of the set $A = \{ ns + tm : s, t \in \mathbb{Z} \}$.

4. The number $p \in \mathbb{Z}^+$ is **prime** if it has no divisors other than itself and 1.

5. The numbers $a$ and $b$ are called **relatively prime** if $\gcd(a, b) = 1$. 

1
Humke’s ‘Make My Day’ 252
Work Sheet 4

1. Proofs using the definitions.
   (a) If $m|n$ and $n|q$ then $m|q$.
   (b) If $m|n$ and $m|q$ then $m|(na + qb)$ for all $a$ and $b$.

2. Proofs using the GCD theorem.
   (a) If $\gcd(a, b) = 1$ and $a|bc$ then $a|c$.
   (b) If $a|m$, $b|m$ and $\gcd(a, b) = 1$ then $ab|m$.

3. Proof of the GCD theorem
   (a) Let $A = \{nr + ns \mid r, s \in \mathbb{Z}\}$ and let $B = \{a \in A \mid a > 0\}$. $B$ is non-empty and has a smallest element: call it $d = mu + nv$.
   (b) Prove that if $c|m$ and $c|n$ then $c|d$ (use one of the problems above).
   (c) Prove that $d|m$ by:
      i. First use Euclid’s algorithm to divide $m$ by $d$. Solve for $r$ and show that it is an element of $B$.
      ii. If $r > 0$ show that you get a contradiction.
      iii. If $r = 0$ show that $d|m$.
   (d) Since you can repeat the argument above to prove that $d|n$, you have shown that $d$ satisfies the three conditions of being a gcd and the theorem is proved.

Homework 4
Due Wednesday, February 20

1. Problems 1) and 2) from above.
2. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$.
3. If $m|n$ and $n|m$ then $m = \pm n$.
4. If $p$ is prime and $p|rs$ then $p|r$ or $p|s$.
5. The converse of the GCD Theorem holds only when the gcd is 1:
   (a) Show by example that if $d > 1$ and $d = mu + nv$ then $d$ is not necessarily the gcd of $m$ and $n$.
   (b) Prove that if $1 = mu + nv$ then $\gcd(m, n) = 1$. (Thus, we can write: $\gcd(m, n) = 1$ if and only if there exist $u, v \in \mathbb{Z}$ such that $mu + nv = 1$.)