Thm 6: (5.3.2) If a is a nonnegative integer, b is a positive and $r = a \bmod b$, then

$$\gcd(a,b) = \gcd(b,r)$$

pf. Assume a is a nonnegative integer, b is a positive integer and $\underline{r = a \bmod b}$. To show that $\gcd(a,b) = \gcd(b,r)$, we will show that the set of common divisors of a and b is the same as the set of common divisors of b and r. (To show that two sets A and B are equal, we need to show $A \subseteq B$ and $B \subseteq A$.)

($\subseteq$) To show that that the set of common divisors of a and b is a subset of the set of common divisors of b and r, let c be an element of the set of common divisors of a and b.

Thus $c \mid a$ and $\underline{c \mid b}$. Recall that $\underline{a = bq + r}$, or $r = a - bq$

From previous Theorems $c \mid b$ implies that $c \mid bq$. (5.1 #

Hence $c \mid \underbrace{a - bq}_{=r}$ by §5.1 # 27)

So $c \mid b$ and $c \mid r$. Therefore c is a common divisor of b and r.

($\supseteq$) To show the other inclusion, let d be a common divisor of b and r. Then $d \mid b$ and $d \mid \underline{r}$. Since $d \mid b$, it divides $d \mid b\underline{q}$. Therefore $d \mid bq + r = a$. Hence $d \mid b$ and $d \mid a$. Therefore, d is a common divisor of a and b.

Thm 6: (5.3.2) If a is a nonnegative integer, b is a positive integer and $r = a \bmod b$, then

$$\gcd(a,b) = \gcd(b,r)$$

pf.

Assume a is a nonnegative integer, b is a positive integer and $r = a \bmod b$. To show that $\gcd(a,b) = \gcd(b,r)$, we will show that the set of common divisors of a and b is the same as the set of common divisors of b and r. (To show that two sets A and B are equal, we need to show $A \subseteq B$ and $B \subseteq A$.)

($\subseteq$) To show that that the set of common divisors of a and b is a subset of the set of common divisors of b and r, let c be an element of the set of common divisors of a and b.

Thus $c \mid a$ and $c \mid b$. Recall that $a = bq + r$, or $r = a - bq$.

From previous Theorems $c \mid b$ implies that $c \mid bq$. (5.1 #

Hence $c \mid \underbrace{a - bq}_{=r}$ by §5.1 # 27).

So $c \mid b$ and $c \mid r$. Therefore c is a common divisor of b and r.

($\supseteq$) To show the other inclusion, let d be a common divisor of b and r. Then $d \mid b$ and $d \mid r$. Since $d \mid b$, it divides $d \mid bq$. Therefore $d \mid bq + r = a$. Hence $d \mid b$ and $d \mid a$. Therefore, d is a common divisor of a and b.

Therefore the set of common divisor of a, b is the same as the set of common divisors of b and r. Therefore gcd(a,b) = gcd(b,r). ∎

Chapter 7: Recurrence Relation

$F(n) = F(n-1) + F(n-2)$ $\quad F(1) = F(2) = 1$

1, 1, 2, 3, 5, 8, 13, 21, ...

In a recurrence relation, the values of the sequence depend on the previous terms

§ 7.1

#1) Find a recurrence relation & initial conditions that generate a sequence with the terms

$\underbrace{3, 7}_{4}, \underbrace{7, 11}_{4}, \underbrace{11, 15}_{4}, \ldots$

$a_n = a_{n-1} + 4$ $\quad$ (linear of degree 1) $\quad a_1 = 3$

#2) 3, 6, 9, 15, 24, 39, ...

$a_n = a_{n-1} + a_{n-2}$ $\quad a_1 = 3,\ a_2 = 6$

(linear of degree 2)

#3) 1, 1, 2, 4, 16, 128, 4096, ...

$a_n = 2\, a_{n-1}\, a_{n-2}$ $\quad a_1 = a_2 = 1$

nonlinear of degree 2.