Number Theory Section Summary: 2.1

The Division Algorithm

"...the foundation stone upon which our whole development rests." (p. 17)

1. Theorems

Division Algorithm: Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

$$a = qb + r$$

with $0 \le r < b$. q is called the **quotient**, and r is called the **remainder**.

(Proof using well-ordering and contradiction.)

Corollary: Given integers a and b, with $b \neq 0$, there exist unique integers q and r satisfying

$$a = qb + r$$

with $0 \le r < |b|$. q is called the **quotient**, and r is called the **remainder**.

2. Summary

Burton comments that the focus will fall on the **applications** of the division algorithm: "...it allows us to prove assertions about all the integers by considering only a finite number of cases." (p. 19)

Proof of the Division Algorithm:

Given $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\exists\, !\, (q,r) \in \mathbb{Z} \times \mathbb{Z}$ /

unique

$$a = qb + r \quad , \quad 0 \le r < b$$

Consider

$$S = \{ a - xb \mid x \in \mathbb{Z},\ a - xb \geq 0 \}$$

S is non-empty: $x = -|a|$ works, because

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$$

By well-ordering, S contains a least member, call it $\underline{r}$:

$$r = a - qb \geq 0$$

So

$$a = qb + r \qquad \text{(there is a pair).}$$

Now to show that $r < b$: (by contradiction)

Assume $r \geq b$. Then

$$r - b = \underline{a - (q+1)b} \geq 0$$

but $a - (q+1)b$ would be in

$S, \ni \quad r-b<r$;

this contradicts the fact that r was the least element of S. Hence,

$$r<b.$$

Let's prove uniqueness directly:

Suppose

$$a = q_1 b + r_1 = q_2 b + r_2$$

Thus

$$(q_1 - q_2) b = r_2 - r_1$$

$$\Rightarrow \quad |q_1 - q_2| b = |r_2 - r_1|$$

But

$$-b < -r_1 \le 0$$

$$0 \le r_2 < b$$

$$-b < r_2 - r_1 < b$$

$a<b<c$

$d<e<f$

$a+d<b+e<c+f$

So

$$|r_2 - r_1| < b, \qquad \text{and}$$

$$|q_1 - q_2| b < b$$

$$\Rightarrow \quad |\underbrace{q_1 - q_2}_{\text{integers!}}| < 1$$

$$\Rightarrow \quad q_1 = q_2$$

So $\quad 0 \cdot b = |r_2 - r_1|$, or

$r_1 = r_2$

(QED)

10, p20 :

For $n \geq 1$ Establish That

$n(7n^2+5)$ is of the form $6k$

Cases :

$6q$

$6q+1$

$6q+2$

$6q+3$

$6q+4$

$6q+5$