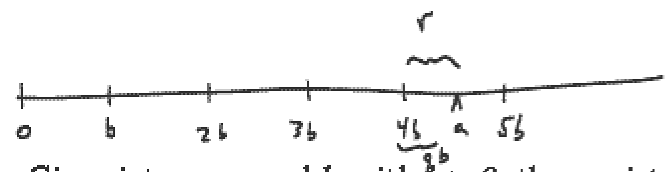
## Number Theory Section Summary: 2.1

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

$$\overline{a = qb + r}$$

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

---

If $a > 0$ as well, then this is an obvious extension of the Archimedean property: if any positive $b$ can be added to itself enough times to exceed any positive $a$, then clearly there will come a point at which $qb \le a$ and $(q+1)b > a$. $r$ just represents the amount by which $qb$ is short (if any!).

(Proof using well-ordering and contradiction.)

Given $a$ + $b$ natural numbers, $\exists!$ $q + r \geq 0$ /

$a = qb + r$ and $\underline{0 \le r < b}$. (uniqueness piece)

Proof:

Existence: By the Archimedean property, $\exists x > 0$ / $xb > a$. By well-ordering, there's a smallest such $x$, call it $y$. Note: $y > 0$, since $a > 0$ and $yb > a$.

Now $(y-1)b \le a$, otherwise $(y-1)$ would be the smallest! Claim: $q = y-1$, $r = a - qb$.

The choice works, if $0 \le r < b$

$\Big\{$ Certainly $a = qb + r$, since $qb + (a - qb) = a$.

Now verify that $0 \le r < b$. $\underbrace{(y-1)b}_{qb} \le a$, so

$0 \le a - qb = r$,

and since $yb > a$ we have that

$\underbrace{(y-1)b}_{qb} + b = yb > a$, or

$b > a - qb = r$.

See p18 for uniqueness.

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

$$\overline{a = qb + r}$$

with $0 \leq r < |b|$.

## 2. Notes

The author shows a couple of interesting properties immediately:

$\underline{a} = q2 + r$

$0 \leq r < 2$

- $b = 2$ leads to the definition of even and odd numbers, as $2q$ or $2q + 1$.
- Furthermore, every square of an integer is of the form $4k$ or $4k+1$.
- $b = 4$ leads to the conclusion that every square of an odd is of the form $8k + 1$.

## 3. 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)

---

#3a p19

Square of any integer is of the form $3k$ or $3k+1$

$3q$ : $(3q)^2 = 9q^2 = 3(3q^2) = 3k$

$3q+1$ : $(3q+1)^2 = (3q)^2 + 2(3q) + 1 = 3[3q^2 + 2q] + 1 = 3k+1$

$3q+2$ : $(3q+2)^2 = (3q)^2 + 2(3q)\cdot 2 + \underbrace{2^2}_{4 = 3+1}$

$= 3[3q^2 + 4q + 1] + 1 = 3k+1$

---

#3c

$5q$

$5q+1$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1

$5q+2$

$5q+3$

$5q+4: \quad (5q+4)^4 = \underbrace{(5q)^4 + 4(5q)^3\cdot 4 + 6(5q)^2\cdot 4^2 + 4(5q)\cdot 4^3}_{5z} + 4^4$

$= 5z + 256$

$= \underbrace{5z + 5\cdot 51}_{5k} + 1$

---

#4 $\quad 3a^2-1$ is never a perfect square.

$3a^2-1 = 3k+\underline{2}$ ✓ $\quad$ Never a perfect square by 3a.

$\underbrace{3a^2-3}_{3k}+2$

#10, p20

For $n \geq 1$ show that

$n(7\underline{n}^2+5)$ is of the form $6k$

One possibility: cases $\underline{6q}, 6q+1, \ldots, 6q+5$

$6\underbrace{q(7(6q)^2+5)}_{k} = 6k$ ✓

$6q+1: \quad (6q+1)\left[7(6q+1)^2+5\right]$

$(6q+1)\left[\underbrace{7(6^2q^2+2\cdot 6\cdot q}_{6z \text{ for some } z}+1) + 5\right]$

$$(6q+1)\left[6z + \underbrace{7+5}_{12}\right]$$

$$6\left[(6q+1)\left[z+2\right]\right] \quad \checkmark$$

$6q+2$ :

$$(6q+2)\left[7(6q+2)^2+5\right]$$

$$(6q+2)\left[7\underbrace{(6^2q^2+4\cdot 6\cdot q}+2^2)+5\right]$$

$$\underbrace{(6q+2)}_{\text{divisible by } 2}\underbrace{(\quad 6z \quad + 33}_{\text{divisible by } 3}\quad]$$

$$6\left[(3q+1)\left[2z+11\right]\right] \quad \checkmark$$

still need to do $6q+3$, $6q+4$, $6q+5$