3. The Division Algorithm

Lemma 3.1. *Let $a, b, c \in \mathbb{Z}$ such that $a < b$. Then*

(1) $a + c < b + c$.
(2) *If* $0 < c$, *then* $ac < bc$.
(3) *If* $c < 0$, *then* $bc < ac$.

Proof: By assumption $a + x = b$, for some $x \in \mathbb{N} \setminus \{0\}$.
(1) Then $(a + c) + x = (b + c)$ and so $a + c < b + c$ ensues.

(2) We have $(a + x)c = bc$ and so $ac + xc = bc$. Since $c > 0$ we have $c \in \mathbb{N} \setminus \{0\}$ and so $xc \in \mathbb{N} \setminus \{0\}$. Thus $ac < bc$.

(3) By (2) we have $a(-c) < b(-c)$. Adding $ac+bc$ onto both sides, it follows from part (1), that $bc < ac$.

□

Definition 3.2. *Let $a, b \in \mathbb{Z}$. We say a* **divides** *b and write $a \mid b$, if there is some $c \in \mathbb{Z}$ such that $ac = b$. Alternatively, we say that a is a* **factor** *of b and b is a* **multiple** *of a.*

Lemma 3.3. *Let $a, b, c \in \mathbb{Z}$. Then*

(1) $a \mid 0$
(2) *If* $0 \mid a$, *then* $a = 0$
(3) $a \mid a$
(4) $1 \mid a$
(5) *If* $a \mid b$ *and* $b \neq 0$, *then* $a \leq |b|$.
(6) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
(7) *If* $a \mid b$ *and* $a \mid c$ *and* $u, v \in \mathbb{Z}$, *then* $a \mid (ub + vc)$.

Proof: (1) $a \cdot 0 = 0$
(2) By assumption $0 \cdot c = a$, for some $c \in \mathbb{Z}$. Hence $a = 0 \cdot c = 0$.
(3) $a \cdot 1 = a$
(4) $1 \cdot a = a$
(5) As surely $a \leq |a|$ it suffices to show that $|a| \leq |b|$. By assumption $ax = b$, for some $x \in \mathbb{Z}$ and so $|a|x = |b|$, for some $x \in \mathbb{N}$. Note that $x \neq 0$, as otherwise $b = 0$. In particular $x \geq 1$. If $x = 1$, then $|a| = |b|$. If $x > 1$, then $|b| = |a|(1 + x - 1) = |a| + |a|(x - 1)$. Note that $|a|(x - 1) \in \mathbb{N} \setminus \{0\}$, and so $|a| < |b|$. Overall $|a| \leq |b|$, as required.
(6) + (7) Homework.

Example 3.4. *We use induction to show that the value* $23^n - 1$ *is divisible by* 11*, for all* $n \geq 0$*. For* $n = 0$ *we get that* $23^n - 1 = 1 - 1 = 0$*, which is divisible by* 11*. Next assume that* $n \geq 0$ *such that* $11 \mid 23^n - 1$*. Then*

$$23^{n+1} - 1 = 23 \cdot 23^n - (23 - 22) = 23 \cdot (23^n - 1) + 22$$

By assumption $11 \mid 23^n - 1$ *and, since* $22 = 11 \cdot 2$ *we have* $11 \mid 22$*. Now by Lemma 3.3(7) we get that* $11 \mid 23 \cdot (23^n - 1) + 22 = 23^{n+1} - 1$*.*

Theorem 3.5 (Division Algorithm)**.** *Let* $a, b \in \mathbb{Z}$ *with* $b \neq 0$*. Then there exist unique* $q, r \in \mathbb{Z}$ *such that*

$$a = qb + r, \quad \text{and } 0 \leq r < |b|.$$

Proof: W.l.o.g $b > 0$. Let $S = \{s \in \mathbb{N} : s = a - qb, \text{ for some } q \in \mathbb{Z}\}$. We claim that S is non-empty. If $a \geq 0$, then choose $q = 0$ and so $s = a - qb = a \in \mathbb{N}$. If $a < 0$, we choose $q = a$. Then $s = a - qb = a - ab = (-a)(-1) + (-a)b = (-a)(b-1)$. But $1 \leq b$, by Corollary 2.6, and so $b - 1 \geq 0$. Since $-a > 0$, we get $s \in \mathbb{N}$.

Now S contains a minimal element r, by Theorem 2.5. Note that $r \geq 0$ and $r = a - qb$, for some $q \in \mathbb{Z}$, or in other words $a = qb + r$. Next we show that $r < b$. Assume otherwise, that is, $b \leq r$. Then $0 \leq r - b$ and so

$$0 \leq r - b = (a - qb) - b = a - b(q + 1).$$

But then $r - b \in S$ and surely $r - b < r$, in contradiction to the minimality of r. In particular we must have $r < b$.

It remains to show uniqueness. So let's have $a = q'b + r'$, for $q', r' \in \mathbb{Z}$ and $0 \leq r' < b$. Without lose of generality we assume that $r \leq r'$. Then

$$0 = a - a = qb + r - (q'b + r') = (q - q')b + (r - r'),$$

and so

$$0 \leq r' - r = (q - q')b.$$

As $b > 0$ we must have that $(q - q') \geq 0$, by Lemma 3.1. On the other hand $r' < b$ and so $r' - r < b - r < b$, by Lemma 3.1. Therefore $(q - q')b < b$ and so $q - q' = 0$. Hence $q = q'$ and consequently $r = r'$.

$\square$

Example 3.6. *(1) We have* $15 = 2 \cdot 6 + 3$*, is the only way to write* 15 *as a multiple of* 6 *plus a natural number less than* 6*.*

(2) Let $n \in \mathbb{Z}$*. Then there are* $q \in \mathbb{Z}$ *and* $r \in \{0, 1\}$ *such that* $n = 2q + r$*. In other words either* $n = 2q$*, in which case we call* n **even***, or* $n = 2q + 1$*, in*

which case we call n **odd**.

(3) We show that every odd square is of the form $8n+1$, for some integer n. Let $k = 2q+1$ be odd. Then $k^2 = (2q+1)^2 = 4q^2+4q+1 = 4q(q+1)+1$. Note that either q or $q+1$ is even and therefore $q(q+1) = 2n$, for some $n \in \mathbb{Z}$. Finally we get that $k^2 = 4q(q+1)+1 = 4 \cdot 2n+1 = 8n+1$.

(4) Let $n \in \mathbb{Z}$. Then $n(n^2+2)/3 \in \mathbb{Q}$. But is it in $\mathbb{Z}$? There are $q \in \mathbb{Z}$ and $r \in \{0,1,2\}$ such that $n = 3q+r$, that is, $n = 3q$ or $n = 3q+1$ or $n = 3q+2$. If $n = 3q$, then surely $3 \mid n$. If $n = 3q+1$, then $n^2+2 = (3q+1)^2+2 = 2 = 9q^2+6q+3 = 3(3q^2+2q+1)$ and so $3 \mid n^2+2$. Finally if $n = 3q+2$, then $n^2+2 = (3q+2)^2+2 = 2 = 9q^2+12q+6 = 3(3q^2+4q+2)$ and so again $3 \mid n^2+2$. Overall we conclude that $3 \mid n(n^2+2)$, that is $n(n^2+2)/3$ is an integer, for all $n \in \mathbb{Z}$.