Ch. 15 - The Division Theorem

Highlights:
- The Division Theorem
The Division Theorem: Let $a, b \in \mathbb{Z}$ with $b \neq 0$.
Then there are unique integers $q$ and $r$ with
\[ a = bq + r \quad \text{and} \quad 0 \leq r < b \]

Note: The theorem asserts that $q$ and $r$ exist and are unique.

Proof of Existence: Let $a, b \in \mathbb{Z}$ with $b \neq 0$.
Case I: Assume $a \geq 0$. Define
\[ Q = \{ k \in \mathbb{Z} : 0 \leq k \leq a, \ kb \leq a \} \]
Then $Q \neq \emptyset$ since $0 \in Q$ and $Q$ is finite since $Q \leq \mathbb{N}$. So $Q$ has a maximum.
Set $q = \max(Q)$.
Now set $r = a - bq$. Since $q \in Q$ we have $bq \leq a$ and thus $r \geq 0$. Towards a contradiction suppose $r \geq b$. Then
\[ (q+1)b = qb + b = qb + r = a \]
so $q \in Q$. and $q = \max(Q) > q + 1$, a contradiction. Thus $0 \leq r < b$, and $a = bq + r$.

Case 2: $a < 0$. Applying Case 1 to $-a$, we obtain $q_0, r_0 \in \mathbb{Z}$ with $-a = bq_0 + r_0$ and $0 \leq r_0 < b$.

Case A: Assume $r_0 = 0$. Setting $q = -q_0$, $r = 0$ we have
\[ a = -(-bq_0 + r_0) = bq_0 = bq = bq + r \]
and we are done.

Case B: Assume $r_0 > 0$. Setting $q = -q_0 - 1$, $r = b - r_0$, we have
\[ a = -(bq_0 + r_0) = b(-q_0) - r_0 = b(-q_0) - b + b - r_0 = b(q_0) + b - r = bq + r \]
and we are done. \( \square \)
Proof of Uniqueness: Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Suppose $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ satisfy $a = bq_1 + r_1 = bq_2 + r_2$ and $0 \leq r_1, r_2 < b$. Notice that $-b < r_1 - r_2 < b$ and hence $|r_1 - r_2| < |b|$. From $bq_1 + r_1 = bq_2 + r_2$ we obtain $|b| > |r_1 - r_2| = |bq_2 - bq_1| = |b| |q_2 - q_1|$. Since $|b| |q_2 - q_1| < |b|$ we must have $q_2 - q_1 = 0$, meaning $q_1 = q_2$. It follows $r_1 = a - bq_1 = a - bq_2 = r_2$. We conclude that $q_1 = q_2$ and $r_1 = r_2$. □

Cor.: An integer $n$ is odd if and only if there is $p \in \mathbb{Z}$ with $n = 2p + 1$.

Cor.: If $n^2$ is even then $n$ is even.

Prop.: If $n \in \mathbb{Z}$ is a perfect square (i.e. $n = m^2$ for some integer $m$) then $n = 3q$ or $n = 3q + 1$ for some $q \in \mathbb{Z}$.

Proof: Assume $n$ is a perfect square, say $n = m^2$, $m \in \mathbb{Z}$. By the division theorem, there are $q_0 \in \mathbb{Z}$ with $m = 3q_0$ or $m = 3q_0 + 1$ or $m = 3q_0 + 2$. Then $n = m^2 = 3(3q_0^2)$ or $n = m^2 = 3(3q_0^2 + 2q_0) + 1$ or $n = m^2 = 3(3q_0^2 + 4q_0 + 1) + 1$. In all three cases, $n$ is of the form $n = 3q$ or $n = 3q + 1$ for some $q \in \mathbb{Z}$. □

Example: $111111111 = 3 \cdot 3703703703 + 2$ so $111111111$ is not a perfect square.
Ch.'s 16 and 17
Theorem: Let $a, b \in \mathbb{Z}$, not both 0. Then there are $n, m \in \mathbb{Z}$ with $na + mb = \gcd(a, b)$

Proof: Let $c$ be the least element of the set $L = \{ i \in \mathbb{Z} : 0 < i \leq a, \exists n, m \in \mathbb{Z} \text{ such that } na + mb = i \}$. (Notice this set is finite (it's a subset of $Na$) and nonempty since it contains $a$, so the set has a minimum.)

Fix $n, m \in \mathbb{Z}$ with $na + mb = c$. We will show $c = \gcd(a, b)$. First we show $c \leq \gcd(a, b)$. To see this let $i, j \in \mathbb{Z}$ be such that $a = i \cdot \gcd(a, b)$ and $b = j \cdot \gcd(a, b)$. Then

$$c = na + mb = ni \cdot \gcd(a, b) + mj \cdot \gcd(a, b) = (ni + mj) \cdot \gcd(a, b)$$

So $\gcd(a, b)$ divides $c$, and since $c > 0$ it follows that $c \leq \gcd(a, b)$.

Next we check $\gcd(a, b) \leq c$. Towards a contradiction suppose $c > \gcd(a, b)$. Then $c$ cannot divide both $a$ and $b$. Let's assume $c$ does not divide $a$ (the case $c$ does not divide $b$ is nearly identical). By the division theorem, there are $q, r \in \mathbb{Z}$ with $a = cq + r$ and $0 \leq r < c$. Since $c$ does not divide $a$ we must have $r \neq 0$, so $0 < r < c$. Now we have

$$r = a - cq = a - (na + mb)q = (1 - nq)a - mj \cdot b$$

and therefore $r \in L$. But $c$ is the least element of $L$ so $c \leq r$, a contradiction. We conclude $c = \gcd(a, b)$ and thus $na + mb = c = \gcd(a, b)$. □
Cor: Let \( a, b \in \mathbb{Z} \) with \( a \) or \( b \) nonzero, and let \( c \in \mathbb{Z} \). Then there are \( n, m \in \mathbb{Z} \) with \( an + bm = c \) if and only if \( \text{gcd}(a, b) \) divides \( c \).

Proof: Exercise.

Cor: Let \( a, b, c \in \mathbb{Z} \) with \( \text{gcd}(a, b) = 1 \). If \( a \) divides \( bc \), then \( a \) divides \( c \).

Proof: Assume \( a \) divides \( bc \). So there is \( q \in \mathbb{Z} \) with \( aq = bc \). Since \( \text{gcd}(a, b) = 1 \), by the previous theorem there are \( n, m \in \mathbb{Z} \) with \( an + bm = 1 \). Multiplying through by \( c \) we obtain

\[
c = a \cdot 1 \cdot (an + bm) c = acn + bcm = acn + agm = a(cn + gm).
\]

Therefore \( a \) divides \( c \). \( \square \)