1 Division Algorithm

Problem 5. *Use old-fashioned long division to implement the Division Algorithm and write $a = bq + r$, $0 \leq r < b$, for each a and b listed below:*

(a) $a = 20$, $b = 3$.

(b) $a = 54$, $b = 7$.

Starting with the first subproblem, we can start by finding the maximal q in the set of possible divisors S. By examination we can quickly deduce

$$\boxed{20 = 3(6) + 2, 0 \leq 2 < 3.}$$

We can do the same for the second subproblem:

$$\boxed{54 = 7(7) + 5, 0 \leq 5 < 7.}$$

Problem 8. *Show that when the square of an odd integer is divided by 8, the remainder is 1. (Hint: remember $2|n(n+1)$.)*

We will restate the problem as a proposition and prove it using the Division Algorithm.

Proposition. *Given the square of an odd integer, it's remainder is always 1 when divided by 8.*

Proof. We start with a simple expression of any odd integer, $2n + 1$. We can restate our proposition as $\exists q \in \mathbb{Z}_{\geq 0}$ such that $(2n+1)^2 = 8q + 1$ $\forall n \in \mathbb{Z}_{\geq 0}$. We can rearrange the statement to determine whether q is an integer:

$$\begin{aligned} (2n+1)^2 &= 8q + 1 \\ 4n^2 + 4n + 1 &= 8q + 1 \\ 4n(n+1) &= 8q \\ \frac{1}{2}n(n+1) &= q \end{aligned}$$

Because $n(n+1)$ is even (or 0) we now know that $\forall n \in \mathbb{Z}_{\geq 0} \implies \exists q \in \mathbb{Z}_{\geq 0}$ given a remainder of 1. This is important as it ensures our divisor is an integer. Thus $(2n+1)^2/8$ will yield a remainder of 1 $\forall n \in \mathbb{Z}_{\geq 0}$. □

Remark. Is this too discursive? There is probably a more elegant solution.

Problem 10. *Let $n, m \in \mathbb{N}$ with $m \neq 1$. Show n can be uniquely written in the form $n = \sum_{k=0}^{N} a_k m^k$ for some $N \in \mathbb{Z}_{\geq 0}$ and $a_k \in \{0, 1, \ldots, (m-1)\}$ with $a_N \neq 0$. Hint: Use induction on n and begin by choosing the largest $N \in \mathbb{Z}_{\geq 0}$ so that $m^N \leq n$. Use the Division Algorithm to write $n = a_N m^N + r$ and then apply the inductive hypothesis to r.*

Proposition. *Given two positive integers m, n where $m \neq 1$, there is a unique representation of $n = \sum_{k=0}^{N} a_k m^k$ for some $N \in \mathbb{Z}_{\geq 0}$ while $a_k \in \{0, 1, \ldots, m-1\}$ and $a_N \neq 0$.*

Proof. Suppose $m, n \in \mathbb{N}$ and $m \geq 2$. We'll first show that the representation exists. Starting with the base case of $n = 0$, the representation $0 = n = \sum_{k=0}^{N} = a_k m^k = a_0 m^0 = a_0$ which is true as $a_0 \in \{0, \ldots, m-1\}$ and $N = 0$. Next with the inductive step, we choose an N such that $m^N \leq n \leq m^{N+1}$. Using the Division Algorithm's expression of $n = a_N m^N + r$, we know that r is a recursive iteration of this expression and can thus be expressed as $r = \sum_{k=0}^{N-1} a_N m^N$. Combining our base case and r, we see that

$$n = a_N m^N + \sum_{k=0}^{N-1} a_N m^N \implies n = \sum_{k=0}^{N} a_N m^N.$$

Next, to prove this representation is unique, consider two expressions of n that are supposedly equal in the non-unique case:

$$\begin{aligned} \sum_{k=0}^{N} a_k m^k &= \sum_{k=0}^{M} b_k m^k \\ \sum_{k=0}^{N} a_k m^k - \sum_{k=0}^{M} b_k m^k &= 0 \\ \sum_{k=0}^{\max(M,N)} (a_k - b_k) m^k &= 0. \end{aligned}$$

The third line of the above derivation can only be true if $(a_k - b_k) = 0 \implies a_k = b_k$. Thus the representation is unique. $\square$

2 Divisors

Problem 12. *List all of the divisors of the following:*

(a) 52,

(b) ...

The divisors of 52 are $\pm\{1, 2, 4, 13, 26, 52\}$.

Problem 14. *Evaluate the following:*

(a) (42,56),

(b) ...

The expression $(42, 56)$, otherwise written as $\gcd(42, 56)$, is equivalent to $\max(A \cap B)$ where $A = \{1, 2, 3, 6, 7, 14, 21, 42\}$, the divisors of 42, and $B = \{1, 2, 4, 7, 8, 14, 28, 56\}$, the divisors of 56. Thus the greatest common divisor of these two numbers is 14.

Problem 17. *Let $b, q, r \in \mathbb{Z}$ and let $a = bq + r$ with a and b not both 0.*

(a) *Show a common divisor of a and b is a divisor of r and that a common divisor of b and r is a divisor of a.*

(b) *Conclude that $(a, b) = (r, b)$*

Proposition. *A common divisor of $a, b \in \mathbb{Z}$ divides r $\wedge$ a common divisor of $b, r \in \mathbb{Z}$ divides $a \implies (a, b) = (r, b)$ given $a = br + r$, $a, b \neq 0$.*

Proof. Suppose $b, q, r \in \mathbb{Z}$ such that $a = bq + r$ and that a, b have a common divisor y. The given equation can be rewritten as $iy = jyq + r$ where $iy = a$ and $jy = b$. We can rearrange this equation to isolate r:

$$\begin{aligned} r &= iy - jyq \\ r &= y(i - jq) \\ r &= yk \end{aligned}$$

knowing $k = (i - jq)$. <u>We can then say that $y|r$ using the multiple $k \in \mathbb{Z}$.</u> Similarly let us suppose b, r have a common divisor z; they can be rewritten as $r = mz$ and $b = nz$. Using our given expression, we can say

$$\begin{aligned} a &= nzq + mz \\ a &= z(nq + m) \\ a &= zl \end{aligned}$$

knowing $l = (nq + m)$. <u>Thus $z|a$ using the multiple $l \in \mathbb{Z}$</u>. $\square$

Problem 19. *Let $a, b \in \mathbb{Z}$, not both 0.*

(a) *If $(a, b) = d$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Hint: Write $ax + by = d$ so that $\frac{a}{d}x + \frac{b}{d}y = 1$.*

(b) *...*