Assignment One

Logan Hunt

January 18, 2023

Contents

1 Section 1.1

1.1 Question 5

By reforming the given expression to show ca as a multiple of q and some remainder:

$$a = bq + r$$
$$ca = (cb)q + (c)r$$

and that $0 \leq r < b \Rightarrow 0 \leq cr < cb$, Theorem 1.1 tells us that there is only one unique quotient: which is q, and the remainder is $(c)r$.

1.2 Question 7

By Theorem 1.1, $a = bq + r, 0 \leq rb$ implies that when b = 3, $a = 3q + r$ where $0 \leq rb$, thus $a \in \mathbb{Z} \Rightarrow a = 3q + r$ where $r \in 0, 1, 2$.

By squaring a, we have three options which simplify to the form $3k$ or $3k + 1$:

1. $a^2 = (3q)^2 = 9q^2$ which is $3k \ni k = 3q^2$
2. $a^2 = (3q + 1)^2 = 9q^2 + 3q + 1 = 3(3q^2 + q) + 1$ which is $3k + 1 \ni k = (3q^2 + q)$
3. $a^2 = (3q + 2)^2 = 9q^2 + 6q + 4 = 3(3q^2 + 2q) + 4$ which is $3l + 4 \ni l = (3q^2 + 2q)$ which is also $3l + 1 + 3 = 3(l + 1) + 1$, which again is $3k + 1 \ni k = l + 1$

1.3 Question 8

By Theorem 1.1, $a = bq + r, 0 \leq rb$ implies that when b = 4, $a = 4q + r$ where $0 \leq rb$, and thus $a = 4q + r$ and $r \in 0, 1, 2, 3$.

Therefore we have four cases:

1. $a = 4q$, and a must be even which is invalid
2. $a = 4q + 1$, and $4q + 1 = 2k + 1 \ni k = 2q$ which fits the definition of an odd number
3. $a = 4q + 2$, thus a must be even as $a = 2k \ni k = 2q + 1$

4. $a = 4q + 3$, can be rewritten to $4q + 1 + 2$, which is odd: $2k + 1 \ni k = 2q + 1$

And thus any odd number can be rewritten as $4q + 1$ or $4q + 3$.

1.4 Question 10

The division of a and c by n can each be represented by

$$a = q_a n + r_a$$
$$c = q_c n + r_c$$

where $0 \leq r_a < n$ and $0 \leq r_c < n$ by Theorem 1.1, and we can subtract each side of the second equation from the first:

$$a - c = (q_a n + r_a) - (q_c n + r_c)$$

With this work now in hand, we will prove by showing that the conjecture is true both ways:

For the first, we will suppose that $r_a = r_c$. Then, we find that

$$a - c = n(q_a - q_c)$$
$$a - c = nk$$

for some integer k.

For the second, we will prove that if $a - c = nk$, when a and c are divided by n, they leave the same remainder r.

From the work we did previously, and by substituting $a - c = nk$, we find that

$$\begin{aligned} a - c &= (q_a n + r_a) - (q_c n + r_c) \\ nk &= (q_a n + r_a) - (q_c n + r_c) \\ nk &= n(q_a - q_c) + (r_a - r_c) \\ n(k - q_a + q_c) &= r_a - r_c \end{aligned}$$

and thus $r_a - r_c$ is a multiple of n.

From the inequalities produced previously by Theorem 1.1, if $r_a \geq r_c$ then $0 \leq r_a - r_c < n$ and $-n < r_c - r_a \leq 0$. Else if $r_c \geq r_a$ then $0 \leq r_c - r_a < n$ and $-n < r_a - r_c \leq 0$.

By combining the two cases, it must be that \$ -n $< \mathrm{r_a} - \mathrm{r_c} <$ n \$, and from the above fact that $r_a - r_c$ is a multiple of n, the only multiple of n in $(-n, n)$ is 0. Thus $r_a = r_c$.

2 Section 1.2

2.1 Question 1

2.1.1 c

1, 57 and 112 are co-prime

2.2 Question 3

$$\begin{aligned} a|b &\Rightarrow \exists n \in \mathbb{Z} \ni an = b \\ b|c &\Rightarrow \exists m \in \mathbb{Z} \ni bm = c \\ (an)m = c &\Rightarrow a|c \end{aligned}$$

2.3 Question 4

2.3.1 a

$$\begin{aligned} a|b &\Rightarrow \exists n \in \mathbb{Z} \ni an = b \\ a|c &\Rightarrow \exists m \in \mathbb{Z} \ni am = c \\ a|(b+c) &\Rightarrow \exists l \in \mathbb{Z} \ni al = b + c \\ al &= an + am \\ b + c = a(n+m) &\Rightarrow a|b+c \end{aligned}$$

2.3.2 b

By continuing from "a":

$$\begin{aligned} br + ct &= (an)r + (am)t \\ \Rightarrow br + ct &= a(nr + mt) \\ &\Rightarrow a|(br + ct) \end{aligned}$$

2.4 Question 7

$|a|$ since $|a||a$ and $|a||0$, and there cannot be an integer larger than $|a|$ that divides a.

2.5 Question 9

No, not every multiple of two factors of an integer divides that integer.

For example, $3|9$ and $9|9$ but $27 \nmid 9$.

2.6 Question 15

2.6.1 c

$$\begin{aligned} 1003 &= (2)(456) + 91 \\ 456 &= (5)(91) + 1 \\ 91 &= (91)(1) + 0 \\ &\Rightarrow (1003, 456) = 1 \end{aligned}$$

2.6.2 d

$$\begin{aligned} 322 &= (2)(148) + 26 \\ 148 &= (5)(26) + 18 \\ 26 &= (1)(18) + 8 \\ 18 &= (2)(8) + 2 \\ 8 &= (4)(2) + 0 \\ &\Rightarrow (322, 148) = 2 \end{aligned}$$

2.7 Question 17

$$\begin{aligned} a|c \Rightarrow \exists n \in \mathbb{Z} \ni an = c \\ b|c \Rightarrow b|an \end{aligned}$$

And by Theorem 1.4, $(a, b) = 1 \Rightarrow b|n \Rightarrow ab|an \Rightarrow ab|c$:

2.8 Question 19

Given some d such that $d|a$ and $d|b$, then $a = nd$ and $b = md$.

$$\begin{aligned} a|(b + c) \Rightarrow \exists p \in \mathbb{Z} \ni ap = b + c \\ c = ap - md \Rightarrow c = (nd)p - md \Rightarrow c = d(np - md) \Rightarrow d|c \end{aligned}$$

Since we're given that $(b, c) = 1 \Rightarrow (md, c) = 1$ and from the above fact that $d|c$, we can conclude that $md = 1$. Therefore $(a, b) = (a, md) = (a, 1) = 1$.

Given some e such that $e|a$ and $e|c$, then $a = ue$ and $c = we$.

$$a|(b + c) \Rightarrow \exists o \in \mathbb{Z} \ni ao = b + c$$
$$b = ao - we \Rightarrow b = (ue)o - we \Rightarrow b = e(uo - w) \Rightarrow e|b$$

And from similar reasoning we can conclude that $(a, c) = (a, we) = (a, 1) = 1$.

2.9 Question 31

2.9.1 a

$[6, 10] = 60$

$[4, 5, 6, 10] = 60$

$[20, 42] = 840$

$[2, 3, 14, 36, 42] = 252$

2.9.2 b

Let $m = [a_1, a_2, \ldots, a_k]$, then by the Division Algorithm, $t = mq + r$ for integers q and r, with $0 \leq r < m$.

As given that all $a_i|t \Rightarrow a_i|mq + r$, and as mq is a multiple of the LCM including $\mathrm{a_i}$, a_i must divide mq, and thus $a_i|r$.

Because $a_i|r$, $r = na_i$ and is thus a multiple of all a_i, but the above statement that $0 \leq r < m$ shows that m - the LCM by definition - is greater than r. Therefore, $r = 0$ and $t = mq \Rightarrow m|t$.