Sabbir Ahmed

DATE: February 20, 2018

MATH 407 HW 03

1.1 **4** Use the Euclidean algorithm to find the following greatest common divisors.

a $(6643, 2873)$

Ans $GCD(6643, 2873)$

$$\begin{aligned}
6643 &= 2873 \cdot 2 + 197 \\
2873 &= 897 \cdot 3 + 182 \\
897 &= 182 \cdot 4 + 169 \\
182 &= 169 \cdot 1 + 13 \\
169 &= 13 \cdot 13 + 0
\end{aligned}$$

$\therefore GCD(6643, 2873) = 13$ $\square$

c $(26460, 12600)$

Ans $GCD(26460, 12600)$

$$\begin{aligned}
26460 &= 12600 \cdot 2 + 1260 \\
12600 &= 1260 \cdot 10 + 0
\end{aligned}$$

$\therefore GCD(26460, 12600) = 1260$ $\square$

e $(12091, 8439)$

Ans $GCD(12091, 8439)$

$$\begin{aligned}
12091 &= 8439 \cdot 1 + 3652 \\
8439 &= 3652 \cdot 2 + 1135 \\
3652 &= 1135 \cdot 3 + 247 \\
1135 &= 247 \cdot 4 + 147 \\
247 &= 147 \cdot 1 + 100 \\
147 &= 100 \cdot 1 + 47 \\
100 &= 47 \cdot 2 + 6 \\
47 &= 6 \cdot 6 + 5 \\
6 &= 5 \cdot 1 + 1 \\
5 &= 1 \cdot 5 + 0
\end{aligned}$$

$\therefore GCD(12091, 8439) = 1$ $\square$

6 For each part of Exercise 4, find integers m and n such that (a, b) is expressed in the form $ma + nb$.

a $(6643, 2873)$

Ans $\square$

c $(26460, 12600)$

Ans $\square$

e $(12091, 8439)$

Ans $\square$

7 Let a, b, c be integers. Give a proof for these facts about divisors:

a If $b \mid a$, then $b \mid ac$.

Ans Let $a = mb$, $m \in \mathbb{Z}$.

Multiplying both sides by c:

$a \cdot c = mb \cdot c$

$a \cdot c = mc \cdot b$ (commutative law of multiplication)

Let $n = mb$, $n \in \mathbb{Z}$.

$a \cdot c = n \cdot c$

$\therefore b \mid ac$ if $b \mid a$ $\square$

b If $b \mid a$ and $c \mid b$, then $c \mid a$.

Ans Let $a = m \cdot b$ and $b = n \cdot c$ for $m, n \in \mathbb{Z}$

$\because a = m \cdot b$, $b = \frac{a}{m}$.

$$\therefore \frac{a}{m} = n \cdot c$$
$$\Rightarrow a = mn \cdot c$$

$\therefore c \mid a$ $\square$

c If $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$ for any integers m, n.

Ans Since $c \mid a$ and $c \mid b$, they can be expressed as

$a = m \cdot c$ and $b = n \cdot c$ for $m, n \in \mathbb{Z}$.

Then:

$$\begin{aligned} ma + nb &= m(mc) + n(nc) \\ &= m^2c + n^2c \\ &= (m^2 + n^2)c \end{aligned}$$

Thus $c \mid (m^2 + n^2)$ for some $(m^2 + n^2) \in \mathbb{Z}$.

$\therefore c \mid (ma + nb)$ $\square$

11 Show that if $a > 0$, then $(ab, ac) = a(b, c)$

Ans Let $d = (b, c)$, so $d \mid b$ and $d \mid c$.

$\therefore b = m \cdot d$, $c = n \cdot d$, $m, n \in \mathbb{Z}$. Then $ab = m \cdot ad$ and $ac = n \cdot ad$.

Thus $ad \mid ab$ and $ad \mid ac$

$\therefore a(b, c) \Rightarrow (ab, ac)$

Conversely,

Let $x \mid ab$ and $x \mid ac$.

$\therefore ab = k \cdot x$ and $ac = l \cdot x$, for some $k, l \in \mathbb{Z}$.

Since $d = (b, c)$, $d = mb + nc$ for some $m, n \in \mathbb{Z}$.

Then:

$$\begin{aligned} ad &= a \cdot mb + a \cdot nc \\ &= x \cdot km + x \cdot ln \\ &= x(km, ln) \end{aligned}$$

Thus, $x \mid ad$

$\therefore (ab, ac) = a(b, c)$ if $a > 0$. $\square$

14 For what positive integers n is it true that $(n, n+2) = 2$? Prove your claim.

Ans Assume n is even, such that $(n, 2) = 2$.

Let d be a divisor of n and $n+2$.

So $d \mid n$ and $d \mid (n+2)$.

Since $(n, 2) = 2$, then $(n+2, 2) = 2$. Therefore, 2 is a divisor of both n and $n+2$.

Since $d \mid n$ and $d \mid (n+2)$, then $d \mid (|n-(n+2)|) \Rightarrow d \mid 2$.

Therefore, d must be 1 or 2.

$\therefore n$ can be any positive even integer. $\square$

17 Let a, b, n be integers with $n > 1$. Suppose that $a = nq_1 + r_1$ with $0 \leq r_1 < n$ and $b = nq_2 + r_2$ with $0 \leq r_2 < n$. Prove that $n \mid (a-b)$ if and only if $r_1 = r_2$.

Ans Suppose $r_1 \leq r_2$

If $n \mid (a-b)$, then $a - b = nq_3$ for $q_3 \in \mathbb{Z}$.

Therefore:

$$\begin{aligned} a - b &= nq_3 \\ \Rightarrow a - b + b &= nq_3 + b \\ \Rightarrow a &= nq_3 + b \end{aligned}$$

Since $b = nq_2 + r_2$:

$$\begin{aligned} a &= nq_3 + nq_2 + r_2 \\ &= n(q_3 + q_2) + r_2 \end{aligned}$$

Since $a = nq_1 + r_1$:

$$\begin{aligned} nq_1 + r_1 &= n(q_3 + q_2) + r_2 \\ nq_1 - n(q_3 + q_2) &= r_2 - r_1 \\ n(q_1 - q_2 - q_3) &= r_2 - r_1 \end{aligned}$$

Thus, $n \mid (r_2 - r_1)$, $0 \leq r_2 - r_1 < r_2 < n$.

Therefore, $r_2 - r_1 = 0$, $\Rightarrow r_2 = r_1$.

Conversely, suppose $n \mid (a-b)$ if $r_1 = r_2$.

Therefore, $a-b=n(q_1-q_2)+(r_1-r_2)$.

$\therefore n \mid (a-b)$ $\square$

19 Let a,b,q,n be integers such that $b \neq 0$ and $a = bq + r$. Prove that $(a,b) = (b,r)$ by showing that (b,r) satisfies the definition of the greatest common divisor of a and b.

Ans $\square$