Math 3 (V3020) Exercises, week 1

1. Prove Theorem 1.1.8

For any $m \in \mathbb{N} \setminus \{0\}$,
$(ma, mb) = m(a, b)$.

Proof:

Theorem 1.1.6 states that the greatest common divisor
(a, b) = the least positive value of $ax + by$
$x, y \in \mathbb{Z}$.

Now
(ma, mb) = the least positive value $max + mby$
= ——— // ——— $m(ax + by)$
$= m(a, b)$

□

2. Prove Theorem 1.1.9

If $d \mid a$ and $d \mid b$ and $d > 0$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$

If $(a, b) = g$, then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

Proof:

For the first part, we do the following. $d \mid a$ and $d \mid b \Rightarrow a = dx$ and $b = dy$ for some $x, y \in \mathbb{Z}$.

Therefore $\left(\frac{a}{d}, \frac{b}{d}\right) = (x, y)$ i.e. we are still looking for the greatest common divisor of two integers, so the claim makes sense.

From Theorem 1.1.8 (Ex. 1), we know $(ma, mb) = m(a, b)$, so replacing $m \to \frac{1}{d}$, $ma \to \frac{a}{d}$, $mb \to \frac{b}{d}$, gives us $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$.

The second part is a special case of the first.

$$\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{1}{g}(a, b) = \frac{1}{g} \cdot g = 1$$

3. Find the greatest common divisor of 42823 and 6409.

We use the Euclidean algorithm. Denote $b = 42823$ and $c = 6409$.
We find $b = cq_1 + r_1$, where $q_1 = 6$ and $r_1 = 4369$.
Next we find q_2 and r_2 in $c = r_1 q_2 + r_2$ and so on until the remainder vanishes.
Tabulated, this looks like

$$42823 = 6 \cdot 6409 + 4369 \qquad (42823, 6409)$$
$$6409 = 1 \cdot 4369 + 2040 \qquad = (6409, 4369)$$
$$4369 = 2 \cdot 2040 + 289 \qquad = (4369, 2040)$$
$$2040 = 7 \cdot 289 + 17 \qquad = (2040, 289)$$
$$289 = 17 \cdot 17 \qquad = (289, 17) = 17.$$

The step $r_2 = 2040 = q_4 r_3 + r_4 = 7 \cdot 289 + 17$.
Then $r_4 = 17$ divides $r_3 = 289$ so the algorithm terminates and $(b, c) = (42823, 6409) = r_4 = 17$.

4. Claim: The product of three consecutive integers is divisible by 6.

Proof: We want $k(k+1)(k+2) = 6n$
for all $k \in \mathbb{Z}$, for some $n \in \mathbb{Z}$.

The claim is trivially true if k or $k+1$ or $k+2$ is 0.

Let us show this for $k > 0$ since the negative case is similar with only an extra factor of -1.

Proof by induction:

Check the base case $k = 1$:
$1(1+1)(1+2) = 1 \cdot 2 \cdot 3 = 6$ is divisible by 6.

Assume that the claim works for arbitrary $k = m$, i.e. $m(m+1)(m+2) = 6n$ for some $n \in \mathbb{Z}$

Induction step: Check the case $k = m+1$

$$(m+1)(m+2)(m+3)$$
$$= \underbrace{m(m+1)(m+2)}_{= 6n \text{ from induction assumption}} + 3(m+1)(m+2)$$
$$= 6n + 3(m+1)(m+2)$$

Now one of $m+1$, $m+2$ is even and the other is odd.

The sign depends on which one is even.

$$\Rightarrow 3(m+1)(m+2) = 3(2p)(2p \pm 1)$$
$$= 6[p(2p \pm 1)] = 6q$$

$$\Rightarrow (m+1)(m+2)(m+3) = 6n + 6q \text{ for some } n, q \in \mathbb{Z}, \text{ i.e. it is divisible by 6.}$$ □

5. Claim: If x and y are odd, then x^2+y^2 is even but not divisible by 4.

Proof: Write $x = 2p+1$, $y = 2q+1$, $p, q \in \mathbb{Z}$.

$$\begin{aligned} x^2+y^2 &= (2p+1)^2 + (2q+1)^2 \\ &= 4p^2 + 4p + 1 + 4q^2 + 4q + 1 \\ &= 4(p^2+p+q^2+q) + 2 \\ &= 2[2(p^2+p+q^2+q)+1] \end{aligned}$$

is even since it equals $2m$ for some $m \in \mathbb{Z}$.

To prove the $4 \nmid x^2+y^2$ part, it is enough to notice that $2(p^2+q^2+p+q)+1$ is odd, meaning that it cannot be written as $2k$, for some $k \in \mathbb{Z}$

$\Rightarrow x^2+y^2 = 2[2(p^2+q^2+p+q)+1] \neq 2 \cdot (2k)$, meaning that $2 \cdot 2 = 4 \nmid x^2+y^2$.

□

6. Claim: $(m, m+n) \mid n$ for all integers m, n both not 0.

Proof: By Theorem 1.1.11, $(a, b) = (a, b + ax)$ for any $x \in \mathbb{Z}$.

$\Rightarrow (m, n) = (m, n + m \cdot 1) = (m, n+m)$.

By definition $(m, n) \mid n$ because (m, n) is the greatest common divisor of m and n, so it divides n.

□