MATH 2710 Your name
Homework 2 September 23, 2016

1. If $ac \mid bc$ and $c \neq 0$, prove that $a \mid b$.

Proof. Since $ac \mid bc$ there exists a $q \in \mathbb{Z}$ such that $acq = bc$. Since $c \neq 0$ we can divide both sides by c and get $aq = b$. Therefore $a \mid b$. □

2. Prove that $\gcd(ad, bd) = |d| \gcd(a, b)$

Proof. Since $|d| \mid d$ we have that $|d| \gcd(a, b) \mid ad$ and $|d| \gcd(a, b) \mid bd$. Hence $|d| \gcd(a, b)$ is a common divisor of ad and bd. We will now show that $|d| \gcd(a, b)$ is the largest common divisor. Since $\gcd(a, b) \geq 1$ we have that

$$|d \gcd(a, b)| = |d| \gcd(a, b).$$

By the characterization of the greatest common divisor there exist integers x and y such that $ax + by = \gcd(a, b)$. Hence,

$$adx + bdy = d \gcd(a, b).$$

If c is a common divisor of ad and bd then $c \mid adx + bdy$. Hence, $c \leq |c| \leq |d| \gcd(a, b)$ by Proposition 2.11(iv). □

3. Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$.

Proof. Suppose that $\gcd(a, c) = \gcd(b, c) = 1$. There exist some $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ such that

$$ax_0 + cy_0 = 1$$

and

$$bx_1 + cy_1 = 1.$$

Therefore,

$$1 = bx_1 + cy_1 = b(ax_0 + cy_0)x_1 + cy_1 = ab(x_0x_1) + c(by_0x_1 + y_1)$$

Hence, we have that $\gcd(ab, c) = 1$ by Proposition 2.27 (i).

Conversely, suppose that $\gcd(ab, c) = 1$. There exist some $x, y \in \mathbb{Z}$ such that

$$abx + cy = 1.$$

However, this implies that $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$ by Proposition 2.27 (i) since $ax, bx \in \mathbb{Z}$.

□

4. Prove that any two consecutive integers are relatively prime.

Proof. Let $n \in \mathbb{Z}$ be an arbitrary integer. Suppose for the sake of contradiction that there exists a $q \in \mathbb{Z}$ such that $q \neq 1$ and $q = \gcd(n, n+1)$. Then $q \mid n$ and $q \mid (n+1)$ so $q \mid (n+1) - n$ i.e. $q \mid 1$. Since $1 \mid q$ we have $q = \pm 1$ by 2.11 (iii). This is a contradiction and thus $\gcd(n, n+1) = 1$ for all integers n. □

Alternatively, we can do the following.

Proof. Since for every integer n we have $(n+1)(1) + (n)(-1) = 1$ we have the $\gcd(n, n+1) = 1$ by Proposition 2.27(i). □

5. Prove that $\{ax + by \mid x, y \in \mathbb{Z}\} = \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}$

Proof. We will show the following set inclusions

$$\{ax + by \mid x, y \in \mathbb{Z}\} \subseteq \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\} \tag{1}$$

and

$$\{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\} \subseteq \{ax + by \mid x, y \in \mathbb{Z}\}. \tag{2}$$

To show (1) let $z \in \{ax + by \mid x, y \in \mathbb{Z}\}$ be an arbitrary element. Then

$$z = ax_0 + by_0 \quad \text{for some } x_0, y_0 \in \mathbb{Z}.$$

By Theorem 2.31 the equation

$$z = ax + by$$

has integer solutions if and only if $\gcd(a, b) \mid z$ i.e. $z = n \cdot \gcd(a, b)$ for some $n \in \mathbb{Z}$. Hence we have that $z \in \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}$. Since z was arbitrary we have

$$\{ax + by \mid x, y \in \mathbb{Z}\} \subseteq \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}.$$

To show (2), let n be an arbitrary integer. By the characterization of the greatest common divisor there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax_0 + by_0.$$

Then,

$$n \gcd(a, b) = anx_0 + bny_0 \in \{ax + by \mid x, y \in \mathbb{Z}\}.$$

Since n was arbitrary we have that

$$\{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\} \subseteq \{ax + by \mid x, y \in \mathbb{Z}\}.$$

□