Homework 9 Solutions

(You must justify ALL your claims unless otherwise stated)

Problem 1

(a) Prove that $5n+3$ and $3n+2$ are relatively prime for all $n \in \mathbb{N}$.

(b) Prove that if a and b are relatively prime integers then $\gcd(a+b, a-b) = 1$ or 2.

Suggested solutions:

(a) $\gcd(5n+3, 3n+2) = \gcd(2n+1, 3n+2) = \gcd(2n+1, n+1) = \gcd(n, n+1) = \gcd(n, 1) = 1$.

(b) $\gcd(a+b, a-b) = \gcd(2b, a-b)$. If $a-b$ is odd, then $\gcd(2b, a-b) = \gcd(b, a-b) = \gcd(b, a) = 1$. If $a-b$ is even, then $\gcd(2b, a-b) = 2\gcd(b, a-b) = 2\gcd(b, a) = 2$.

Alternative solution:

Let $d = \gcd(a+b, a-b)$. Then $d \mid a+b$ and $d \mid a-b$. Adding and subtracting gives $d \mid 2a$ and $d \mid 2b$. We can conclude that d is a common divisor of $2a$ and $2b$. By the definition of $\gcd(2a, 2b)$, we have $d \mid \gcd(2a, 2b)$. Since $\gcd(a, b) = 1$, we have $\gcd(2a, 2b) = 2$. Thus $d \mid 2$. d can only be 1, 2.

Problem 2

Prove the following:

(a) For all positive integers a, b, c, $\gcd(a, bc) | \gcd(a, b) \cdot \gcd(a, c)$

(b) For all positive integers a, b, c, if $\gcd(a, b)$ and $\gcd(a, c)$ are relatively prime then $\gcd(a, bc) = \gcd(a, b) \cdot \gcd(a, c)$.

Suggested solutions:

(a) Write $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$ and $\gcd(a, c) = ak + cl$ for some $k, l \in \mathbb{Z}$. We need to show that $\gcd(a, bc) | \gcd(a, b) \cdot \gcd(a, c)$. By Bezout's Lemma on a and bc, it suffices to show that $\gcd(a, b) \cdot \gcd(a, c)$ can be written as $as + (bc)t$ for some $s, t \in \mathbb{Z}$. Multiplying the first two equations:

$$\begin{aligned} \gcd(a, b) \cdot \gcd(a, c) &= (ax + by)(ak + cl) \\ &= a(axk + byk + xcl) + (bc)(yl) \end{aligned}$$

So we can take $s = axk + byk + xcl$ and $t = yl$.

(b) By part (a), it suffices to show that $\gcd(a,b)\gcd(a,c) \mid \gcd(a,bc)$. Since $\gcd(a,b) \mid b$ and $\gcd(a,c) \mid c$, we have $\gcd(a,b)\gcd(a,c) \mid bc$. It remains to show that $\gcd(a,b)\gcd(a,c) \mid a$, which implies $\gcd(a,b)\gcd(a,c)$ is a common divisor of a and bc. By the definition of $\gcd(a,bc)$, we have $\gcd(a,b)\gcd(a,c) \mid \gcd(a,bc)$.

Since $\gcd(a,b)$ and $\gcd(a,c)$ are relatively prime, there are $s,t \in \mathbb{Z}$ such that $s\gcd(a,b)+t\gcd(a,c) = 1$. Also, $\gcd(a,b) \mid a$ so there is $u \in \mathbb{Z}$ such that $a = u\gcd(a,b)$; $\gcd(a,c) \mid a$ so there is $v \in \mathbb{Z}$ such that $a = v\gcd(a,c)$. Then

$$\begin{aligned} s\gcd(a,b) + t\gcd(a,c) &= 1 \\ s\gcd(a,b)a + t\gcd(a,c)a &= a \\ s\gcd(a,b)v\gcd(a,c) + t\gcd(a,c)u\gcd(a,b) &= a \\ \gcd(a,b)\gcd(a,c)(sv+tu) &= a \end{aligned}$$

as desired.

Alternative solution:

Notice that both $\gcd(a,b)$ and $\gcd(a,c)$ divide $\gcd(a,bc)$ (from the definition of gcd). Part (a) tells us that $\gcd(a,bc)/\gcd(a,b)$ divides $\gcd(a,c)$. It suffices to show that $\gcd(a,c) \mid \gcd(a,bc)/\gcd(a,b)$. Write $m = \gcd(a,b)$. Since $\gcd(a,c) \mid \gcd(a,bc)$, we have $\gcd(a,c) \mid m(\gcd(a,bc)/m)$. By Theorem 6.1.32 (see the reading from April 7), we have $\gcd(a,c) \mid (\gcd(a,bc)/m)$. In other words, $\gcd(a,c)m \mid \gcd(a,bc)$ as desired.

Problem 3

Let $a,b \in \mathbb{Z}$ with $b \neq 0$ and suppose that a has remainder 1 when divided by b. Prove that a^n has remainder 1 when divided by b for all $n \in \mathbb{N}$.

Suggested solution:

By assumption, there is $k \in \mathbb{Z}$ such that $a = kb+1$.

We prove the statement by induction. When $n = 0$, $a^0 = 1 = 0 \cdot b + 1$ so it has remainder 1 when divided by b.

Assume a^n has remainder 1 when divded by b for some $n \in \mathbb{N}$. Namely, there is $q \in \mathbb{Z}$ such that $a^n = qb+1$.

Inductive step: $a^{n+1} = a \cdot a^n = a(q \cdot b + 1) = aqb + a = aqb + (kb+1) = (aq+k)b+1$. Therefore a^{n+1} also has remainder 1 when divded by b.

Problem 4

Determine which of the following equations have integer solutions $(x,y) \in \mathbb{Z}^2$:

1. $465x + 4920y = 1$
2. $54585x - 4920y = 75$
3. $496185x + 54585y = -10745$

Suggested solutions:

(a) Applying the Euclidean Algorithm: $(4920, 465) \Rightarrow (465, 270) \Rightarrow (270, 195) \Rightarrow (195, 75) \Rightarrow (75, 45) \Rightarrow (45, 30) \Rightarrow (30, 15) \Rightarrow (15, 0)$. Therefore $\gcd(465, 4920) = 15 \nmid 1$. The equation does not have integer solutions.

(b) Applying the Euclidean Algorithm: $(54585, 4920) \Rightarrow (4920, 465)$. By (a) $\gcd(54585, 4920) = 15 \mid 75$. The equation has integer solutions.

(c) Applying the Euclidean Algorithm: $(496185, 54585) \Rightarrow (54585, 4920)$. By (b) $\gcd(496185, 54585) = 15 \nmid -10745$. The equation does not have integer solutions.