Part A

(1) Suppose that $a, b, \in \mathbb{Z}$ with $n \neq 0$. Prove that $\gcd(ab, n) = 1$ if and only if $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$.

Solution. First suppose that $\gcd(ab, n) = 1$, and we show that $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$. Now Bezout's identity tells us that there exist integers s and t so that

$$s \cdot ab + t \cdot n = 1.$$

But then we get $sb \cdot a + t \cdot n = 1$, and since $sb \in \mathbb{Z}$ we rely on Bezout's characterization of relative primality to give us $\gcd(a, n) = 1$. In the same way the previous equation can be viewed as $sa \cdot b + t \cdot n = 1$; this time because $sa \in \mathbb{Z}$, Bezout characterization of relative primality gives $\gcd(b, n) = 1$.

For the opposite direction, assume we are told that $\gcd(a, n) = 1 = \gcd(b, n)$. By Bezout's identity we have integers s, t, u, v so that

$$sa + tn = 1 \qquad \text{and} \qquad ub + vn = 1.$$

Multiplying these two expressions together gives

$$1 = (sa + tn)(ub + vn) = suab + savn + tnub + tvn^2 = (su)ab + (sav + tub + tvn)n.$$

Now since $\mathbb{Z}$ is closed under addition and multiplication, we get $su, sav + tub + tvn \in \mathbb{Z}$, and so Bezout's characterization of relative primality gives $\gcd(ab, n) = 1$. □

(2) Prove that if $c \mid ab$ and $\gcd(c, a) = d$, then $c \mid db$.

Solution. First, note that since $d \mid c$ and $d \mid a$ we have integers γ and α so that $d\gamma = c$ and $d\alpha = a$. Futhermore we saw in class that $\gcd(\gamma, \alpha) = 1$. Since we're told that $c \mid ab$, there is some q with $cq = ab$. Substituting the expressions for c and a above gives

$$d\gamma q = d\alpha b.$$

Because $d \geq 1$ (as we saw in class) we have $d \neq 0$, and so we can cancel the d on both sides to arrive at $\gamma q = \alpha b$. By the definition of divisibility we know that $\gamma \mid \alpha b$, but since $\gcd(\gamma, \alpha) = 1$ a result from class tells us that $\gamma \mid b$. Hence there is some integer k with $\gamma k = b$. If we multiply both sides of the equation by d, then we get $ck = d\gamma k = db$. Again using the definition of divisibility, we get $c \mid db$. □

(3) Prove that if $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.

Solution. By Bezout's identity we have some integers s and t so that $sa + tb = 1$. Cubing this equation (and expanding out the left hand side) gives

$$s^3a^3 + 3s^2a^2tb + 3sat^2b^2 + t^3b^3 = (sa + tb)^3 = 1^1 = 1.$$

Rearranging the left side of this expression produces

$$(s^3a + 3s^2tb)a^2 + (3sat^2 + t^3b)b^2 = 1.$$

Since $\mathbb{Z}$ is closed under addition and multiplication we have $s^3a + 3s^2tb, 3sat^2 + t^3b \in \mathbb{Z}$, and Bezout's characterization of relative primality gives us $\gcd(a^2, b^2) = 1$. □

(4) Prove that if $\gcd(a, b) > 1$, then there exists a common prime divisor of a and b.

Solution. Suppose that $\gcd(a, b) = d > 1$. Since $d > 1$, a result from class tells us that there is some prime p with $p \mid d$. Now since $d \mid a$, transitivity of divisibility tells us that $p \mid a$; in the same way, the fact that $d \mid b$ and divisibility is transitive gives us that $p \mid b$. Hence p is a common prime divisor of a and b. □

Part B

(1) Suppose a and b are integers that are not both zero. Suppose further that c is an integer with $\gcd(a, b) \nmid c$. Prove that there are not integral solutions to the equation

$$ax + by = c.$$

That is, prove that for any values $x, y \in \mathbb{Z}$ we have $ax + by \neq c$.

Solution.

We'll approach this by contradiction. So suppose there are integers s and t with $sa + tb = c$. For the sake of convenience, we'll use the notation $\gcd(a, b) = d$. We know that $d \mid a$ and $d \mid b$, and so divisibility under multiplication tells us that $d \mid sa$ and $d \mid tb$. Divisibility under addition then tells us that $d \mid sa + tb$. Hence d divides c, contrary to the assumption that $d \nmid c$. We've reached our contradiction, and so we conclude that our assumption — that there are integers s and t with $sa+tb = c$ — must be false. Hence the equation $sa + tb = c$ has no solution.

□

(2) Suppose $a, b \in \mathbb{Z}$ are not both zero, and suppose that $\gcd(a, b) \mid c$. Prove that one can find an integral solution the equation

$$ax + by = c.$$

Then prove that if x_0 and y_0 are a given integral solution to the equation, then a pair of integers x and y satisfy the equation if and only if there exists some integer n so that

$$x = x_0 + nu \qquad \text{and} \qquad y = y_0 - nv,$$

where we write u and v as the integers satisfying $a = dv$ and $b = du$.

Solution. As before, we'll write $\gcd(a, b) = d$ for notational convenience. Since $d \mid c$ there is some integer q with $dq = c$. Furthermore Bezout tells us that there are integers s and t with $sa + tb = d$. Multiplying through by q on both sides gives

$$(sq)a + (tq)b = dq = c.$$

Since $\mathbb{Z}$ is closed under multiplication, we have $sq, tq \in \mathbb{Z}$, and so the equation $ax + by = c$ has an integral solution.

Now suppose that $x_0, y_0 \in \mathbb{Z}$ are a give solution; this means that $ax_0 + by_0 = c$. As in the prompt, we'll write v and u for the integers which satisfy $a = dv$ and $b = du$. Now let $n \in \mathbb{Z}$ be given. We'll first show that $x = x_0 + nu$ and $y = y_0 - nv$ provides a solution. Observe:

$$\begin{aligned} a(x_0 + nu) + b(y_0 - nv) &= ax_0 + anu + by_0 - bnv && \text{(distribution)} \\ &= ax_0 + by_0 + dvnu - dunv && \text{(substitution)} \\ &= ax_0 + by_0 && \text{(cancellation)} \\ &= c \end{aligned}$$

Hence the given values of x and y do provide a solution.

Now we argue the other direction: if x and y are solutions to the given equation, then there is some integer n so that $x = x_0 + nu$ and $y = y_0 - nv$. For the time being, let's assume that neither a nor b is zero, since this is the more general case; we'll handle the case when one of a or b is zero afterwards. Since we know that $ax + by = c$ and $ax_0 + by_0 = c$, we can set them equal to each other to conclude $ax + by = ax_0 + by_0$. Rearranging gives

$$a(x - x_0) = b(y_0 - y).$$

Note that since $x - x_0 \in \mathbb{Z}$, the definition of divisbility gives $a \mid b(y_0 - y)$. By problem 3 of Part A of this assignment, this in turn means that $a \mid d(y_0 - y)$, and so there is some integer n with $an = d(y_0 - y)$. Substituting $a = dv$ into this expression gives $dvn = d(y_0 - y)$, and cancelling the factor of d produces

$vn = y_0 - y$. If we solve for y, we then find that $y = y_0 - nv$. To compute the value of x, note that the equation $vn = y_0 - y$ above can be plugged into our equality $a(x - x_0) = b(y_0 - y)$ to produce

$$a(x - x_0) = bnv.$$

We can use the fact that $b = du$ and $a = dv$ to rewrite the right hand side as $bnv = anu$, so that our equation now becomes $a(x - x_0) = anu$. Since we assume $a \neq 0$ we can cancel it on both sides and solve for x as $x = x_0 + nu$, as desired.

The final thing to wrap up is the case when one of a or b is zero. Without loss of generality we can assume that $a = 0$ and $b \neq 0$. In this case we have $d = \gcd(a, b) = \gcd(0, b) = |b|$, and so we have $u = \pm 1$ and $v = 0$ (in the notation of the problem). Now recall that we're assuming we have both $ax + by = c$ and $ax_0 + by_0 = c$. We define $n = u(x - x_0)$; since $u^2 = 1$ we can multiply on both sides of the expression by u to get $nu = u^2(x - x_0) = x - x_0$, and so $x = x_0 + nu$ as desired. On the other hand, since we assume $a = 0$ we have $ax = ax_0 = 0$. Substituting these expressions into the known equations $ax + by = c = ax_0 + by_0$, we get $by = by_0$. Cancelling the factor of b on both sides (since $b \neq 0$) gives $y = y_0$. But since $v = 0$, this equation is the same as $y = y_0 - nv$. □

(3) Compute $\gcd(29647, 14467)$ by hand. Then, express $\gcd(29647, 14467)$ as an integral linear combination of 29647 and 14467 (again by hand).

Solution. In class we saw a theorem that allows us to compute the greatest common divisor of two numbers by iteratively applying the division algorithm; this result is called the Euclidean algorithm. When we run the Euclidean algorithm for the given numbers, it produces the following equations:

$$\begin{aligned} 29647 &= 2 \cdot 14467 + 713 \\ 14467 &= 20 \cdot 713 + 207 \\ 713 &= 3 \cdot 207 + 92 \\ 207 &= 2 \cdot 92 + 23 \\ 92 &= 4 \cdot 23 + 0. \end{aligned}$$

Now the Euclidean algorithm tells us that $\gcd(29647, 14467) = 23$.

For the second part of this problem, we're asked to find integers s and t so that $29647s + 14467t = 23$. We saw in class that we can work backwards through the equations we produced in the Euclidean algorithm to find these integers. We proceed with the algorithm we outlined in class:

$$\begin{aligned} 23 &= 207 + (-2) \cdot 92 \\ &= 207 + (-2) \cdot (713 - 3 \cdot 207) \\ &= 7 \cdot 207 + (-2) \cdot 713 \\ &= 7 \cdot (14467 - 20 \cdot 713) + (-2) \cdot 713 \\ &= (-142) \cdot 713 + 7 \cdot 14467 \\ &= (-142) \cdot (29647 - 2 \cdot 14467) + 7 \cdot 14467 \\ &= 291 \cdot 14467 - 142 \cdot 29647. \end{aligned}$$

□