Solution to Problem 2
Notation: Let (a,b) be the notation used to denote the ideal generated by a and b, and let gcd (a,b) denote the greatest common divisor of a and b.

($\Longrightarrow$)

Suppose R is a PID. From the lecture notes, any PID is a UFD, so it is sufficient to show that if $a, b \in R$ are non-zero, then gcd (a,b) $\in (a, b)$. But it has already been proven in class that if R is a PID, then (gcd (a,b)) = (a,b), so it follows that gcd (a,b) $\in$ (a,b).

(Quick proof of the fact that gcd (a,b) $\in$ (a,b): Since R is a PID, (a,b) = (q) for some $q \in R$. Then $a \in (q)$ and $b \in (q)$, so a = qc and b = qd for some $c, d \in R$. Then q divides c and q divides b, so q must divide gcd (a,b), so gcd (a,b) = qr for some $r \in R$. Therefore, (gcd (a,b)) $\subset$ (q) = (a,b)).

($\Longleftarrow$)
Outline of the proof:

Step 1: Show that for any $a, b \in R$, (gcd (a,b)) = (a,b). Then by induction, this is true for any finitely generated ideal (that if $r_1, r_2, ..., r_n \in R$, then $(r_1, ..., r_n)$ = (gcd $(r_1, ..., r_n)$)).

Step 2: Show that any UFD satisfies the ascending chain condition for principal ideals.

Step 3: Use Step 2 to show that any ideal in R is finitely generated.

To prove the steps in the outline of the proof:

Step 1: Suppose $a, b, \in R$. Then by assumption, gcd (a,b) $\in (a, b)$, so it is sufficient to show that $a \in (gcd(a, b))$ and $b \in (gcd(a, b))$. Let q = gcd (a,b).

By definition of gcd (a,b), gcd (a,b) divides a and gcd (a,b) divides b, so there exists $s, t \in R$ such that a = sq and b = tq. Then $a \in (q)$ and $b \in (q)$, so $a \in (gcd(a, b))$ and $b \in (gcd(a, b))$.

Then (gcd (a,b)) = (a,b), so by induction, if $r_1, r_2, ..., r_n \in R$, $(r_1, ..., r_n)$ = (gcd $(r_1, ..., r_n)$).

Step 2: We prove the ascending chain condition for principal ideals in this step. The ascending chain condition for principal ideals states that any ascending chain of principal ideals must stabilize. Suppose, by contradiction, that $r_1, r_2, ... \in R$ and $(r_1) \subsetneq (r_2) \subsetneq (r_3)$..., so that we have a infinite chain of principal ideals such that one is strictly contained in the next.

Since R is a UFD, $r_1 = up_1...p_n$ some some unit u and primes $p_1, ..., p_n$. But $(r_1) \subsetneq (r_2)$, so $r_1 = r_2q_2$ for some prime q_2 (this is because $r_1 = r_2r'$ for some $r' \in R$, but if r' was a unit, then $(r_1) = (r_2)$). Similarly, $r_i = r_{i+1}q_{r+1}$, so we have $r_1 = r_2q_2 = r_3q_3q_2 = r_4q_4q_3q_2 = ...$, so r_1 factors into infinitely many primes. This is a contradiction, since $r_1 = up_1...p_n$ and the length of the prime in which r_1 factors into is unique, so r_1 only factors into finitely many primes.

Step 3: Suppose I is an ideal that is not finitely generated, and let $g_1, g_2, ...$ be a countable subset of the minimal generating set for I. Then

$$(g_1) \subsetneq (g_1, g_2) \subsetneq (g_1, g_2, g_3) \subsetneq ...$$

is an ascending chain of ideals, and from Step 1, $(g_1, g_2) = gcd(g_1, g_2)$, $(g_1, g_2, g_3) = gcd(g_1, g_2, g_3)$, ..., so this is an ascending chain of principal ideals. By Step 2, this ascending chain must stabilize, so there exists an $n \in \mathbb{N}$ such that $(g_1, g_2, ..., g_n) = (g_1, ..., g_n, ..., g_m)$ for all $m \geq n$, so $(g_1, ..., g_n, ..., g_m)$ is not a subset of a minimal generating set for I.

Therefore any ideal in R is finitely generated.

Since any ideal is finitely generated, any ideal is of the form I $= (g_1, ..., g_n)$, $g_i's \in R$, so by step 1, $I = (gcd(g_1, .., g_n))$ is principal. Therefore, R is a PID.