1. (a) No, $\gcd(10, 25) = 5 > 1$.
(b) Yes, $\gcd(11, 25) = 1$. By Euclid $-9 \cdot 11 + 4 \cdot 25 = 1$ so $-9 \cdot 11 \equiv 1 \pmod{25}$ so $11^{-1} \equiv -9$.
(c) Yes, $\gcd(12, 25) = 1$. By Euclid $-2 \cdot 12 + 1 \cdot 25 = 1$ so $-2 \cdot 12 \equiv 1 \pmod{25}$ so $12^{-1} \equiv -2$.
(d) No, $\gcd(30, 42) = 6 > 1$.
(e) Yes, $\gcd(31, 42) = 1$. By Euclid $19 \cdot 31 - 14 \cdot 42 = 1$ so $19 \cdot 31 \equiv 1 \pmod{42}$ so $31^{-1} \equiv 19$.
(f) No, $\gcd(32, 42) = 2 > 1$.

2.

#	Reflexive	Symmetric	Transitive	Antisymmetric	Irreflexive	Equiv Rel	Partial	Total
(a)	Yes	No	Yes	Yes	No	No	Yes	Yes
(b)	No	Yes	No	No	Yes	No	No	No
(c)	Yes	Yes	Yes	No	No	Yes	No	No
(d)	Yes	No	Yes	Yes	No	No	Yes	No
(e)	Yes	No	Yes	Yes	No	No	Yes	Yes
(f)	Yes	Yes	Yes	No	No	Yes	No	No
(g)	No (0)	Yes	Yes	No	No	No	No	No

---

3. (a) f is one-to-one, onto, and a bijection since $f^{-1} = \{(2, 1), (3, 2), (4, 3), (1, 4)\}$ is also a function.
(b) f is not one-to-one since $f(2) = f(4)$ and f is not onto since $\mathrm{im}(f)$ misses 2.
(c) f is one-to-one, onto, and a bijection since it has an inverse $f^{-1}(x) = x/2$.
(d) f is one-to-one but not onto since $\mathrm{im}(f)$ is only the even integers.
(e) f is one-to-one but not onto since its image misses 1.
(f) f is one-to-one, onto, and a bijection since it has an inverse $f^{-1}(x) = x^{1/3}$.

---

4. $R = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (2, 4), (4, 1), (4, 2), (4, 4), (3, 3), (3, 5), (5, 3), (5, 5), (6, 6)\}$.

---

5. R is reflexive since $|x| = |x|$, R is symmetric since $|x| = |y|$ implies $|y| = |x|$, and R is transitive since $|x| = |y|$ and $|y| = |z|$ imply $|x| = |z|$.
Also, $[0] = \{0\}$, $[1] = \{1, -1\}$, $[2] = [-2] = \{2, -2\}$, $[4] = \{4, -4\}$.

---

6. (a) The function $f^{\dagger} : A \to \mathrm{im}(f)$ is one-to-one and onto hence a bijection. Then $\#A = \#\mathrm{im}(f)$ by the definition of cardinality.
(b) If f is one-to-one then by (a), $\#A = \#\mathrm{im}(f)$. Since $\#A = \#B$ and A and B are finite, this means $\mathrm{im}(f) = B$ so f is onto.

---

7. Here are brief outlines of each proof:

(a) If n is the sum of $k, k+1, k+2, k+3, k+4, k+5$ then $n = 6k+15 \equiv 3 \pmod 6$. Conversely if $n \equiv 3 \bmod 6$ so that $n = 3+6a$, then n is the sum of $a-2, a-1, a, a+1, a+2, a+3$.

(b) If R is reflexive and a function, then $R(a) = a$ for all $a \in A$, so the only possibility is to have $R(a) = a$ for all $a \in A$. But clearly the identity function is also an equivalence relation, so it is the only one that works.

(c) Note that $5^n + 6^n \equiv 5^n + (-5)^n \equiv 5^n(1 + (-1)^n) \pmod{11}$. If n is odd then $1 + (-1)^n = 0$ while if n is even then $1 + (-1)^n = 2$, so since $5^n \not\equiv 0 \pmod{11}$, we see $5^n + 6^n \equiv 0$ if and only if n is odd.

(d) Note that B is a subset of $A \cup (B \backslash A)$. If A and $B \backslash A$ are countable then their union is also countable, hence any subset is countable. If B is uncountable then this is a contradiction, so $B \backslash A$ is uncountable.

(e) Note $f(f(a)) = a$ for all $a \in A$ iff $f \circ f = i_A$ iff $f^{-1} = f$ as functions on A iff f^{-1} exists and $f^{-1}(a) = f(a)$ for all $a \in A$.

(f) As proven in class, the Cartesian product of two countable sets is countable, so $\mathbb{Q} \times \mathbb{Z}$ is countable. Also, $\mathbb{R} \times \mathbb{Z}$ contains $\mathbb{R} \times \{1\}$ which is in bijection with $\mathbb{R}$, so it is uncountable.

(g) Modulo 6 we have $7^n + 5 \equiv 1^n + 5 \equiv 1 + 5 \equiv 0 \pmod 6$, which means $7^n + 5$ is divisible by 6. (Induction also works but the mod-6 argument is much easier.)

(h) Let $x \in A$. Then by hypothesis $(f \circ g)(x) = (f \circ h)(x)$ which means $f(g(x)) = f(h(x))$. But f is one-to-one, so this implies $g(x) = h(x)$. Since g and h agree on all elements in A, that means $g = h$.

(i) For each $a \in A$ we have $(a, a) \in R$ and so $(a, a) \in R^{-1}$ hence $(a, a) \in S$. Next, if $(a, b) \in S$ then $(a, b) \in R$ and $(a, b) \in R^{-1}$ so $(b, a) \in R^{-1}$ and $(b, a) \in R$ so $(b, a) \in S$. Finally if $(a, b), (b, c) \in S$ then $(a, b), (b, c) \in R$ so $(a, c) \in R$ and also $(c, b), (b, a) \in R$ so $(c, a) \in R$ so $(a, c) \in R^{-1}$ so $(a, c) \in S$.

(j) Note $n - 1 \equiv -1 \pmod n$ so $(n-1)^{-1} \equiv (-1)^{-1} \equiv -1 \equiv n - 1 \pmod n$.

(k) Both sets are countably infinite. Hence they are both in bijection with the positive integers, and therefore also with each other.

(l) From homework 8, $S \subseteq f^{-1}(f(S))$. For the reverse, suppose $a \in f^{-1}(f(S))$, so that $f(a) \in f(S)$. Since f is one-to-one, $f(a) = f(b)$ implies $a = b$, so $f(a) \in f(S)$ implies $a \in S$.

(m) From homework 8, $f(f^{-1}(T)) \subseteq T$. For the reverse, suppose $b \in T$. Since f is onto, there exists $a \in A$ with $f(a) = b$, so $a \in f^{-1}(T)$. Hence $b \in f(f^{-1}(T))$.

(n) Note f has an inverse g. Then in fact $\tilde{f}$ has an inverse $\tilde{g} : \mathcal{P}(B) \to \mathcal{P}(A)$ with $\tilde{g}(T) = \{g(t) : t \in T\}$. Explicitly, for $S \subseteq A$, $\tilde{g}(\tilde{f}(S)) = \tilde{g}(\{f(s) : s \in S\} = \{g(f(s)) : s \in S\} = \{s : s \in S\} = S$ and $\tilde{f}(\tilde{g}(T)) = \tilde{f}(\{g(t) : t \in T\}) = \{f(g(t)) : t \in T\} = \{t : t \in T\} = T$.

(o) Note $(a, b) \in R^{-1} \cap S^{-1}$ iff $(a, b) \in R^{-1}$ and $(a, b) \in S^{-1}$ iff $(b, a) \in R$ and $(b, a) \in S$ iff $(b, a) \in R \cap S$ iff $(a, b) \in (R \cap S)^{-1}$.

(p) Since $a \equiv b \pmod n$ and $c \equiv d \pmod n$ we see $b + c \equiv a + d \pmod n$. Then $a(b + c) \equiv b(b + c) \equiv b(a + d) \pmod n$ so $a(b + c) \equiv b(a + d) \pmod n$.

(q) We have $(a, b)\, T\, (a, b)$ since $a\, R\, a$ and $b\, S\, b$, if $(a, b)\, T\, (a', b')$ then $a\, R\, a'$ and $b\, S\, b'$ so $a'\, R\, a$ and $b'\, S\, b$ by symmetry so $(a', b')\, T\, (a, b)$, and if $(a, b)\, T\, (a', b')$ and $(a', b')\, T\, (a'', b'')$ then $a\, R\, a'$ and $a'\, R\, a''$ and $b\, R\, b'$ and $b'\, R\, b''$ so by transitivity we see $a\, R\, a''$ and $b\, S\, b''$ so $(a, b)\, T\, (a'', b'')$.

(r) If we have $(a, b) \in (X \times Y) \cap (X' \times Y')$ then $a \in X \cap X'$ so $X = X'$ and $b \in Y \cap Y'$ so $Y' = Y'$ so the sets are disjoint, and for any $(a, b) \in A \times B$ we have $a \in X$ and $b \in Y$ for some $X \in \mathcal{P}$ and $Y \in \mathcal{Q}$, so then $(a, b) \in X \times Y$ is in $\mathcal{P} \times \mathcal{Q}$. So the sets have union $A \times B$: thus they are a partition. (Note that this item is the previous part phrased in terms of partitions.)

(s) All equivalence relations contain the identity relation. So f is one-to-one iff $[a] = [b]$ is equivalent to $a = b$ iff $a\, R\, b$ is equivalent to $a = b$ iff R equals the identity relation.

(t) If S_n is the set of n-element subsets of $\mathbb{Z}$ then S_n is countable since it is a subset of $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (with n terms) and this set is countable. Then the set of finite subsets of $\mathbb{Z}$ is $\cup_{n=0}^{\infty} S_n$ which is a countable union of countable sets, hence countable.