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

---

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. For the divisibility ordering there are no minimal or smallest elements, but 6 is largest and maximal. For the other ordering, -2 and -1 are minimal but neither is smallest, while 6 is largest and maximal.

---

7. (a) The function $f^\dagger : A \to \text{im}(f)$ is one-to-one and onto hence a bijection. Then $\#A = \#\text{im}(f)$ by the definition of cardinality.
(b) If f is one-to-one then by (a), $\#A = \#\text{im}(f)$. Since $\#A = \#B$ and A and B are finite, this means $\text{im}(f) = B$ so f is onto.
(c) Many examples, such as $f(x) = e^x$ or $f(x) = \arctan(x)$.

---

8. (a) There are finitely many nonzero polynomials of degree at most n whose coefficients are integers and at most n in absolute value (in fact there are n^{n+1} of them). Each of these polynomials has at most n roots, so the total number of roots is finite. Second statement follows by observing that if α is a root of a poly of degree k whose max coeff is M, then $\alpha \in S_{\max(k,M)}$.
(b) By (a), the set of algebraic numbers is a union of countably many finite sets, so it is countable. Since $\mathbb{R}$ is uncountable, this means that the transcendental numbers are uncountable since otherwise $\mathbb{R}$ would be the union of two countable sets hence countable.

---

9. 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 $n \equiv 3$ mod 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 is uncountable.

   (e) If $D \subseteq A$ and $D \subseteq B$ then any $x \in D$ has $x \in A$ and $x \in B$ hence $x \in A \cap B$, so $D \subseteq A \cap B$. But $A \cap B$ is indeed a subset of both A and B, so since it lies above all other such subsets D, it is the largest such set.

   (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) R is reflexive since $f(a) = f(a)$ for all $a \in A$. R is symmetric since $f(a) = f(b)$ implies $f(b) = f(a)$. R is transitive since $f(a) = f(b)$ and $f(b) = f(c)$ imply $f(a) = f(c)$.

   (i) 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 $g = h$.

   (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 $a(b+c) \equiv b(a+d) \pmod n$.
