1. Suppose a, b are some fixed integers and let $A(c)$ be the predicate: "If $c \mid a$ and $c \mid b$ then $c^2 \mid ab$."

(a) Write down the negation of $A(c)$.

soln: $c \mid a$, and $c \mid b$, and $c^2 \not| ab$.

(b) Write down the converse of $A(c)$.

soln: If $c^2 \mid ab$ then $c \mid a$ and $c \mid b$.

(c) Is $\forall\, c \in \mathbb{N}\ A(c)$ true or false. Prove your answer. **soln:** True. Proof: Let $c \in \mathbb{N}$ be given. Suppose $c \mid a$, and $c \mid b$. $c \mid a$ means that $a = kc$ for some $k \in \mathbb{Z}$. Similarly $c \mid b$ means that $b = \ell c$ for some $\ell \in \mathbb{Z}$. Thus $ab = (kc)(\ell c) = (k\ell)c^2$. Since $k\ell \in \mathbb{Z}$ this shows that $c^2 \mid ab$. Thus $A(c)$ is true.

2. (6 marks) Let $S = \{1, 2, 3\}$. **State** (no working required) whether or not the following relation on S is reflexive, transitive, symmetric and antisymmetric. Thus state whether or not it is an equivalence relation, a partial ordering, both of these or neither. (No working required) $R_1 = \{(1,1), (2,2), (3,3), (1,2), (2,3), (1,3)\}$
soln: It is: reflexive, not symmetric, transitive, antisymmetric, not an equivalence, and a partial ordering.

3. Let $\sim$ be a relation on $\mathbb{N}$ given by $a \sim b$ if and only if there is a prime which is a factor of both a and b. Show whether or not this is an equivalence relation.
soln:
It is not an equivalence relation. Proof:
Not transitive: For example take 4, 6 and 9 then $4 \sim 6$ since 2 is a factor of both. $6 \sim 9$ since 3 is a factor of both but 4 and 9 are relatively prime and in particular have no common prime factors.
More simply, it is not reflexive, for there is no prime which divides 1.

4. (7 marks) Suppose A, B and C are sets and $f : A \to B$ and $g : B \to C$ are functions. Suppose $g \circ f : A \to C$ is one-one. Prove f is one-one, but g need not be.
soln: Suppose that f is not one-one. Then there are $a_1, a_2 \in A$ with $a_1 \neq a_2$ but $f(a_1) = f(a_2)$. Then $g \circ f(a_1) = g(f(a_1)) = g(f(a_2)) = g \circ f(a_2)$ so this contradicts that $g \circ f : A \to C$ is one-one.

Consider $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$. and $f(1) = 1$, $g(2) = 4$, and $g(3) = 4$. Then $g \circ f : A \to C$ is one-one, but g is not.

5. Use the Euclidean algorithm to find a $\gcd(x^4+x^2+x-1, x^3+1)$ in $\mathbb{R}[x]$. Show the steps in the calculation.
soln:
$x^4+x^2+x-1 = x(x^3+1)+x^2-1$
$x^3+1 = x(x^2-1)+(x+1)$
$x^2-1 = (x-1)(x+1)$
So $(x+1)$ is a $\gcd(x^4+x^2+x-1, x^3+1)$.

6. On $\mathbb{N}$ with the partial order given by 'divides', define $\gcd(a,b,c)$ to be the greatest element of the set of natural numbers which are common divisors of the 3 natural numbers a, b and c. Write $e = \gcd(a,b,c)$ and $f = \gcd(d,c)$ where $d = \gcd(a,b)$. Prove that $e = f$.
soln: Since e is a common divisor of a and b we have $e \mid d$. (As d is the $\gcd(a,b)$.) Also $e \mid c$ so

$$e \mid f \quad (1)$$

as $f = \gcd(d,c)$.

On the other hand $f \mid d$ and d is a common divisor of a and b so $f \mid a$ and $f \mid b$. Also by its definition $f \mid c$ so in fact f is a common divisor of a, b and c. Thus

$$f \mid e \quad (2)$$

as $e = \gcd(a,b,c)$. From (1) and (2) it follows that $e = f$ (since they are both positive integers).