9 Discrete Mathematics (MPF)

(a) Let \( p \) and \( m \) be positive integers such that \( p > m \).

(i) Prove that \( \gcd(p, m) = \gcd(p, p - m) \). [3 marks]

(ii) Without using the Fundamental Theorem of Arithmetic, prove that if \( \gcd(p, m) = 1 \) then \( p | \binom{p}{m} \). You may use any other standard results provided that you state them clearly. [3 marks]

(b) Let \( A^* \) denote the set of strings over a set \( A \).

For a function \( h : X \to Y \), let \( \text{map}_h : X^* \to Y^* \) be the function inductively defined by

\[
\text{map}_h(\varepsilon) = \varepsilon \\
\text{map}_h(x\omega) = (h(x))(\text{map}_h(\omega)) \quad (x \in X, \omega \in X^*)
\]

Prove that, for functions \( f : A \to B \) and \( g : B \to C \),

\[
\text{map}_g \circ \text{map}_f = \text{map}_{g \circ f}
\]

Note: You may use the following Principle of Structural Induction for properties \( P(\omega) \) of strings \( \omega \in A^* \):

\[
(P(\varepsilon) \land \forall \omega \in A^*. P(\omega) \Rightarrow \forall a \in A. P(a\omega)) \implies \forall \omega \in A^*. P(\omega)
\]

[6 marks]

(c) We say that a relation \( T \subseteq A \times B \) is a total cover whenever \( \text{id}_A \subseteq T^{\text{op}} \circ T \) and \( \text{id}_B \subseteq T \circ T^{\text{op}} \). (Recall that \( T^{\text{op}} \subseteq B \times A \) denotes the opposite, or dual, of the relation \( T \subseteq A \times B \).)

For a relation \( R \subseteq \{1, \ldots, m\} \times \{1, \ldots, n\} \) \( (m, n \in \mathbb{N}) \), we define a new relation \( \sim^R \) between strings over a set \( X \) as follows: for all \( u, v \in X^* \),

\[
u \sim^R v \iff R \text{ is a total cover and } u = a_1 \ldots a_m, v = b_1 \ldots b_n, \text{ and } a_i = b_j \text{ for all } (i, j) \in R
\]

(i) Prove that for \( R = \text{id}_{\{1, \ldots, m\}} \), we have that \( u \sim^R u \) for all \( u = a_1 \ldots a_m \).

(ii) Prove that \( u \sim^R v \) implies \( v \sim^{R^{\text{op}}} u \).

(iii) Prove that \( u \sim^R v \) and \( v \sim^S w \) imply \( u \sim^{S \circ R} w \).

(iv) Prove that the further relation \( \sim \) on \( X^* \) defined by

\[
u \sim v \iff \exists R. u \sim^R v
\]

is an equivalence relation. [8 marks]