8 Discrete Mathematics (mpf23)

(a) Let \( N_+ = \{ \ell \in \mathbb{N} \mid \ell > 0 \} \).

(i) Prove that, for all \( a, b \in N_+ \), if \( a > b \) then \( \gcd(a, b) = \gcd(a - b, b) \). 

\[4 \text{ marks}\]

(ii) Prove the following statement for all \( q \in N_+ \),

\[ \forall n \in N_+. \forall r \in N_+. \gcd(2^{qn+r} - 1, 2^n - 1) = \gcd(2^r - 1, 2^n - 1) \]

[Hint: Proceed by induction on \( q \)].

\[6 \text{ marks}\]

(iii) Prove that, for all \( q, n \in N_+ \), \( \gcd(2^{qn} - 1, 2^n - 1) = 2^n - 1 \).

\[2 \text{ marks}\]

(iv) For \( m, n \in N_+ \), give a formula for \( \gcd(2^m - 1, 2^n - 1) \). Briefly justify your answer.

\[2 \text{ marks}\]

(b) Prove that there is no surjection from \( \mathbb{N} \) to \( (\mathbb{N} \Rightarrow \{0, 1\}) \).

\[6 \text{ marks}\]