

8 Discrete Mathematics (mpf23)

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

(i) Prove that, for all $a, b \in \mathbb{N}_+$, if $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$. [4 marks]

(ii) Prove the following statement for all $q \in \mathbb{N}_+$,

$$\forall n \in \mathbb{N}_+. \forall r \in \mathbb{N}_+. \gcd(2^{q \cdot n + r} - 1, 2^n - 1) = \gcd(2^r - 1, 2^n - 1)$$

[Hint: Proceed by induction on q]. [6 marks]

(iii) Prove that, for all $q, n \in \mathbb{N}_+$, $\gcd(2^{q \cdot n} - 1, 2^n - 1) = 2^n - 1$. [2 marks]

(iv) For $m, n \in \mathbb{N}_+$, give a formula for $\gcd(2^m - 1, 2^n - 1)$. Briefly justify your answer. [2 marks]

(b) Prove that there is no surjection from \mathbb{N} to $(\mathbb{N} \Rightarrow \{0, 1\})$. [6 marks]