7 Discrete Mathematics (gw104)

(a) Let \( n \) be a positive natural number. Show \( x \equiv y \mod n \) determines an equivalence relation between integers \( x \) and \( y \). \[3\text{ marks}\]

(b) Describe the extended Euclid algorithm which given a pair of positive natural numbers \( (m, n) \) returns not only their gcd, \( \gcd(m, n) \), but also its expression as a linear combination, \( j.m + k.n \), for integers \( j \) and \( k \). \[7\text{ marks}\]

(c) Assume positive natural numbers \( m \) and \( n \) are coprime, so \( \gcd(m, n) = 1 \) with associated linear combination \( j.m + k.n = 1 \), for integers \( j \) and \( k \).

(i) Show that for any natural numbers \( r \) and \( s \) there is a solution to
\[
x \equiv r \mod m \land x \equiv s \mod n.
\]

[Hint: Take \( x = s.j.m + r.k.n \).] \[4\text{ marks}\]

(ii) Show the solution is unique mod \( m.n \), i.e. \( x \equiv y \mod m.n \) for any two solutions \( x \) and \( y \). \[6\text{ marks}\]