p1q7
PR

Discrete mathematics – long question

State and prove the Chinese Remainder Theorem concerning the simultaneous solution of a pair of congruences to co-prime moduli, and the uniqueness of that solution. [10 marks]

Define the set of units modulo n, U_n, and Euler's totient function, $\varphi(n)$. [2 marks]

Given natural numbers m and n with no common factors, define $f: U_{mn} \to U_m \times U_n$ by $f(u) = (u \bmod m, u \bmod n)$. Prove carefully that f is a bijective function. [6 marks]

Deduce that φ is multiplicative, and calculate $\varphi(175)$. [2 marks]

Solution

Given $(m,n)=1$ [1]
we can solve $x \equiv a \pmod m$ and $x \equiv b \pmod n$ [2]
and the solution is unique modulo mn [1]
$(m,n) = 1$, so use Euclid to find s and t such that $ms + nt = 1$ [2]
Let $c = bms + ant$ and show it works [2]
Uniqueness [2]

$U_n = \{ x \in N \mid 0 < x < n \ \& \ (x,n) = 1 \}$ [1]
$\varphi(n) = |U_n|$ [1]

observe $c \in U_{mn}$

$(u,mn) = 1 \Rightarrow (u,m) = 1$ so $(u \bmod m, m) = 1$ and f is well-defined [2]
Given $a \in U_m$ and $b \in U_n$, find $c \in Z_{mn}$ using the CRT so f is surjective [2]
$u_1 \equiv u_2 \pmod m \ \& \ u_1 \equiv u_2 \pmod n \Rightarrow u_1 \equiv u_2 \pmod{mn}$, so f is injective [2]

$(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$ [1]
$\varphi(175) = 120$ [1]

Computer Science Tripos Part IA 2005

Paper 1 Question 7

PR — Discrete Mathematics