p1q2
PR

Discrete mathematics – short question

State the Fermat-Euler theorem, and deduce that $p \mid (2^p-2)$ for any prime, p. [5 marks]

A composite number, m, which satisfies $m \mid (2^m-2)$ is known as a *pseudo-prime*.

Show that $2^{10} \equiv 1 \pmod{11}$ and $2^{10} \equiv 1 \pmod{31}$. Deduce that 341 is a pseudo-prime. [5 marks]

Solution

Given n>1 and a with (a,n)=1, then $a^{\varphi(n)} \equiv 1 \pmod n$ where $\varphi(n)$ is the number of units modulo n. [2]
If p=2 then $2^2-2=2$, whichis divisible by 2 [1]
if p is an odd prime, then (2,p)=1 and $\varphi(p)=p-1$, so $2^{p-1} \equiv 1 \pmod p$, and $2^p \equiv 2 \pmod p$ [2]

$2^{10} = 1024 = 1023+1 = 3\times11\times31+1 \equiv 1$ (mod 11 or 31) [2]
(11,31)=1, so $2^{10} \equiv 1 \pmod{11\times31=341}$ by CRT, so $2^{340} \equiv 1 \pmod{341}$, and $2^{341} \equiv 2 \pmod{341}$ [2]
But $341 = 11\times31$ is composite [1]

Computer Science Tripos Part IA 2005

Paper 1 Question 2

PR — Discrete Mathematics