2002 Paper 1 Question 7

Discrete Mathematics

State Fermat's Little Theorem and derive the Diffie–Hellman protocol for key exchange. [6 marks]

The protocol requires repeated multiplication (mod p), for some prime p, to achieve exponentiation. A procedure which avoids the potentially slow division by p after each multiplication to calculate the remainder is known as *Montgomery multiplication* . . .

Given an odd prime p, let B be a power of 2 with $B > p$. Define $m(x) \equiv xB (\text{mod } p)$. Prove that:

- $m : \mathbb{Z}_p \to \mathbb{Z}_p$ is a bijection;
- $m(x \times y) = m^{-1}(m(x) \times m(y))$. [6 marks]

Given $u < pB$, let $v \equiv -up^{-1} (\text{mod } B)$ and $x = (u + vp) \div B$. If $x \geqslant p$, then subtract p from x. Prove that:

- x is an integer;
- $x \equiv uB^{-1} (\text{mod } p)$;
- $x < p$. [6 marks]

Deduce that $x = m^{-1}(u)$, observing that its calculation involves division only by B. [2 marks]