2006 Paper 2 Question 3

Discrete Mathematics I

(a) State the Fermat–Euler theorem, carefully defining any terms that you use. Deduce that $2^p \equiv 2 \pmod{p}$ for any prime p. [5 marks]

(b) Explain how this result can be used to show that a number is composite without actually finding a factor. Give an example. [3 marks]

(c) Let $M_m = 2^m - 1$ be the m^{th} Mersenne number. Suppose that m is composite. Prove that M_m is composite. [3 marks]

(d) A composite number m that satisfies $2^m \equiv 2 \pmod{m}$ is known as a *pseudo-prime*.

- (i) Suppose that m is prime. Prove that M_m is either prime or a pseudo-prime. [3 marks]

- (ii) Suppose that m is a pseudo-prime. Prove that M_m is a pseudo-prime. [3 marks]

- (iii) Deduce that there are infinitely many pseudo-primes. [3 marks]