Question 4 (Unit 4) – 14 marks

If we write the sum $1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p}$ as a fraction it will take the form $\frac{m}{np}$ and, curiously, for p prime with $p \geq 5$ it turns out that $m-n$ is always divisible by p^3. For instance:

$$p=5: \quad 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}=\frac{137}{12\times 5} \text{ and } 5^3 \text{ divides } 137-12.$$

$$p=7: \quad 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}=\frac{1089}{60\times 7} \text{ and } 7^3 \text{ divides } 1089-60.$$

In this question you are required to use the results of *Unit 4* to prove that this is generally true. The marks allocated to parts (iv), (v) and (vi) do not necessarily reflect their relative difficulty.

Let p be an odd prime.

(i) Suppose that the polynomial congruence

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has more than n incongruent solutions modulo p. Deduce from Lagrange's Theorem that

$$a_n \equiv a_{n-1} \equiv a_{n-2} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 \pmod{p}. \qquad [1]$$

(ii) Consider the polynomial

$$f(x) = (x-1)(x-2)\ldots(x-(p-1)) + 1 - x^{p-1}.$$

Explain why $x \equiv 0, 1, 2, \ldots, p-1 \pmod{p}$ are incongruent solutions of the congruence $f(x) \equiv 0 \pmod{p}$. Deduce that each coefficient of $f(x)$ is divisible by p. [2]

(iii) Suppose that the polynomial $f(x)$ is multiplied out to give

$$f(x) = c_{p-1}x^{p-1} + c_{p-2}x^{p-2} + \cdots + c_2 x^2 + c_1 x + c_0.$$

Write down the values of the coefficients c_{p-1} and c_0. [2]

(iv) Prove, using mathematical induction, that for any $n \geq 1$, the coefficient of x in $(x-1)(x-2)\ldots(x-n)$ is

$$(-1)^{n-1} n! \left[1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}\right].$$

Hence deduce that c_1, (the coefficient of x in $f(x)$) is

$$c_1 = -(p-1)! \left[1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\right]. \qquad [4]$$

(v) Write down the value of $f(p)$ obtained by putting $x=p$ in the expression for $f(x)$ in part (ii). Write down the value of $f(p)$ obtained by putting $x=p$ in the expression for $f(x)$ in part (iii). By equating these two values (and remembering that each of the coefficients c_i is divisible by p), deduce that, for $p \geq 5$,

$$p^2 \text{ divides } (p-1)! \left[1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\right].$$

[Note from part (iv) that $-(p-1)! \left[1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p}\right]$ is actually an integer!] [3]

(vi) Writing $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p}=\frac{m}{np}$, deduce that p^3 divides $m-n$. [2]