

**Question 3 (Unit 3) - 12 marks**

- (i) Let  $a$  and  $d$  be integers and  $p$  a prime such that  $\gcd(p, d) = 1$ . Prove that one of the numbers

$$a, a + d, a + 2d, \dots, a + (p - 1)d$$

is divisible by  $p$ .

[4]

- (ii) Let  $a$  and  $d$  be positive integers with  $a > 7$ , and suppose that

$$a, a + d, a + 2d, \dots, a + 8d, a + 9d$$

is an arithmetic progression of 10 primes, the largest of which does not exceed 3000.

- (a) Prove that  $d = 210$ . [Hint: Note that  $210 = 2 \times 3 \times 5 \times 7$  and apply part (i) with  $p$  equal to each of the primes 2, 3, 5 and 7 in turn.]

[3]

- (b) Observing that  $210 = 11 \times 19 + 1$ , show that

$$a + md \equiv a + m \pmod{11}$$

for  $m = 0, 1, 2, \dots, 8$  and 9. Deduce that  $a \equiv 1 \pmod{11}$ , by showing that otherwise one of the primes

$$a, a + d, \dots, a + 9d$$

would be divisible by 11.

[4]

- (iii) There is, in fact, just one arithmetic progression of ten primes not exceeding 3000. Use the results of this question and the table of primes to find it.

[1]

**Question 4 (Unit 4) - 16 marks**

All parts of this question involve FLT.

- (i) Find the least positive residue of  $26^{59} \pmod{29}$ .

[4]

- (ii) Solve  $13x \equiv 1 \pmod{29}$ . Explain why the least positive residue of  $13^{27}$  modulo 29 is a solution of this congruence. Write down a linear congruence (modulo 29) whose solution is congruent to  $13^{26}$ , and hence determine the least positive residue of  $13^{26}$  modulo 29.

[8]

- (iii) Prove that  $a^{25} \equiv a \pmod{390}$  for every integer  $a$ .

[4]

**Question 5 (Unit 4) - 9 marks**

Use Wilson's Theorem and its converse in proving that  $p$  and  $p + 2$  are twin primes if, and only if,

$$4[(p - 1)! + 1] + p \equiv 0 \pmod{p(p + 2)}.$$

[Hint: You will need to consider this congruence to moduli  $p$  and  $p + 2$  separately.]

[9]