Question 3

(i) (a) If $a \equiv b \pmod n$ then there exists an integer r such that $a - b = rn$. Therefore

$$(ka + c) - (kb + c) = k(a - b) = krn$$

which is an integer multiple of n. Hence

$$ka + c \equiv kb + c \pmod n .$$

(b) If $ka \equiv b \pmod n$ and $kc \equiv d \pmod n$ then there exists integers r and s such that

$$ka - b = rn \quad \text{and} \quad kc - d = sn.$$

Therefore

$$ad - bc = a(kc - sn) - c(ka - rn) = (cr - as)n,$$

which is an integer multiple of n. Thus $ad \equiv bc \pmod n$.

(ii)

$$5x \equiv 1 \pmod{13} \iff 5x \equiv 40 \pmod{13} \iff x \equiv 8 \pmod{13};$$
$$7x \equiv 10 \pmod{11} \iff 7x \equiv 21 \pmod{11} \iff x \equiv 3 \pmod{11};$$
$$31x \equiv 6 \pmod 7 \iff 3x \equiv 6 \pmod 7 \iff x \equiv 2 \pmod 7 .$$

For simultaneous solution:

$x \equiv 8 \pmod{13} \Rightarrow x = 8, 21, 34, 47, \ldots$, increasing by 13 to a solution of $x \equiv 3 \pmod{11}$,

and

$x \equiv 3 \pmod{11} \Rightarrow x = 47, 190, 333, 476, 619, 762, 905, \ldots$, increasing by 143 to a solution of $x \equiv 2 \pmod 7$,

and

$x \equiv 2 \pmod 7 \Rightarrow x \equiv 905 \pmod{1001}$.

The least positive solution is 905.

Question 4

(i) Proof of Wilson's Theorem.
If $p = 2$ then $1! \equiv -1 \pmod 2$ is true.
If $p = 3$ then $2! \equiv -1 \pmod 3$ is true.

If $p \geq 5$ consider the set $S = \{1, 2, 3, \ldots, p-1\}$. If $a \in S$ then $\gcd(a, p) = 1$ and so the congruence $ax \equiv 1 \pmod p$ has a unique solution modulo p, say $a' \in S$. Now $a = a'$ when $a = 1$ and when $a = p - 1$, and these are the only cases since $a^2 \equiv 1 \pmod p$ has at most two solutions, being of degree 2.

It follows that the $p - 3$ numbers in $\{2, 3, \ldots, p-2\}$ fall into pairs each with product congruent to 1 modulo p, and consequently

$$(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-1) \equiv 1 \times (p-1) \equiv -1 \pmod p$$

as required.

(ii) From Wilson's Theorem

$$(p-1)(p-2)(p-3)\ldots 2 \times 1 \equiv -1 \pmod p .$$

That is

$$(-1)(-2)(p-3)! + 1 \equiv 0 \pmod p ,$$

and so

$$2(p-3)! + 1 \equiv 0 \pmod p .$$

(iii) As $41 \equiv 7 \pmod{17}$, $41^{41} \equiv 7^{41} \pmod{17}$. Now FLT gives $7^{16} \equiv 1 \pmod{17}$ and so $41^{41} \equiv 7^{41} \equiv 7^{16}7^{16}7^{9} \equiv 7^{9} \equiv 49^{4} \times 7 \equiv (-2)^{4} \times 7 \equiv -7 \equiv 10 \pmod{17}$. So the remainder when 41^{41} is divided by 17 is 10.