To solve the simultaneous eqns we can try

$x = 4, 15, 26, 37, 48, 59, 70, 81, 92$ mod 11

$\quad\;\; 3 \quad 14 \quad 2 \quad 13 \quad 1 \quad 12 \quad 0$ mod 23

See the pattern: 6 more 'double' steps gives $92 + 132 = 224$

But this is even so add 253 : 477

OR remember the Chinese remainder theorem and write $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2$ for $N = n_1 \cdots \cancel{n_k} \cdots n_r$, $N_k x_k \equiv 1 \pmod{n_k}$

$= 4 \cdot 23 \cdot 1 + 17 \cdot 11 \cdot 21$

$= 92 + 3553 + 374$

---

(4) (i) Determine remainder when 11^{33} is divided by 155

(Hint: $155 = 5 \times 31$; find remainders for 5, 31 first)

$11^{33} = 11^{31} \cdot 11^2 \equiv 11 \cdot 11^2 \pmod{31}$ Cor. to F.L.T

$= 11 \cdot -3 = -33 \equiv 29 \pmod{31} \equiv -2 \pmod{31}$

$11^{33} = (11^5)^6 \cdot 11^3 \equiv 11^6 \cdot 11^3 \equiv 11^5 \cdot 11^4 \equiv 11 \pmod 5$ Cor F.L.T

$\equiv 1 \pmod 5$

Then $\left.\begin{array}{l} 11^{33} + 13.5 \equiv 1 \pmod{31} \\ 11^{33} + 13.5 \equiv 1 \pmod 5 \end{array}\right\}$ $11^{33} + 13.5 \equiv 1 \pmod{155}$

$11^{33} \equiv -64 \pmod{155}$

$\equiv 91 \pmod{155}$

My argument here was: $\begin{array}{l} a \equiv b \pmod n \\ a \equiv b \pmod m \end{array} \Rightarrow a \equiv b \pmod{nm}$

So I wanted $11^{33} + \square \equiv 29 + \square \equiv 1 \bmod 31$

$11^{33} + \square \equiv 1 + \square \equiv 1 \bmod 5$

thus $\square$ is $5K$ to solve $29 + 5K \equiv 1 \bmod 31$

$5K \equiv 3 \bmod 31$

$K = 13$

Alternatively: say: $x \equiv -2 \pmod{31} \equiv 29, 60, 91$ and $\equiv 1 \pmod 5$ So $91 \pmod{155}$

(ii) Prove the converse of Wilson's Theorem.

Assume $(n-1)! \equiv -1 \pmod n$, n not prime.

then $d \mid n$ $(1 < d < n)$ $\Rightarrow d \mid (n-1)!$ and $d \mid (n-1)! + 1$

$\Rightarrow d \mid 1$ ✗

---

(5) (i) Prove $\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ (you may assume ϕ mul

$\phi(n) =$ no. of pos. integers $\le n$ rel. prime to n

$\phi(p) = p - 1$

$\therefore \phi(n) = \prod_{p \mid n} \phi(p) = \prod (p-1) = \prod p \cdot \frac{(p-1)}{p}$

$= n \prod \left(1 - \frac{1}{p}\right)$

(ii) Determine $\tau(180), \sigma(180)$

$\tau(n) =$ no. of pos divisors of $n = p_1^{k_1} \cdots p_m^{k_m} = \sum_{d \mid n} 1$

$= (k_1 + 1) \cdots (k_m + 1)$

$180 = 2 \times 2 \times 3 \times 3 \times 5$ $\therefore \tau(180) = 3 \cdot 3 \cdot 2 = 18$

$\sigma(n) =$ sum of pos. divisors of $n = \sum_{d \mid n} d$

$= \frac{p_1^{k_1+1}}{p_1 - 1} \cdots$ $\therefore \sigma(180) = \frac{2^3 - 1}{1} \cdot \frac{3^3 - 1}{2} \cdot \frac{5^2 - 1}{4} = 54$

If $\sigma(n) < 2n$ then n is said to be deficient. Is 180 deficient? Show $n = p_1 \cdot p_2$ is deficient except $n = 6$

180 NOT deficient – from the defn.

$\sigma(n) = (p_1 + 1)(p_2 + 1) = p_1 p_2 + p_1 + p_2 + 1$

$\therefore \sigma(n) < 2n \Leftrightarrow p_1 + p_2 + 1 < p_1 p_2$

$\Leftrightarrow p_1 p_2 - p_1 - p_2 - 1 > 0$

$\Leftrightarrow (p_1 - 1)(p_2 - 1) - 2 > 0$

$\Leftrightarrow (p_1 - 1)(p_2 - 1) > 2$

Clearly since $p_1, p_2 \geq 2$, $p_1 \neq p_2$ this holds unless $p_1 = 2, p_2 = 3$

then $n = 6$