1.a Because 811 is prime we can apply Wilson's theorem

$(p-1)! \equiv -1 \pmod{p}$

$810! \equiv -1 \pmod{811}$ 810 mod

$809! \cdot 810 \equiv -1 \pmod{811}$

$809!(-1) \equiv -1 \pmod{811}$

$809! \equiv 1 \pmod{811}$

809! has a remainder of 1 when divided by 811

1.b Because 983 is prime we can apply Wilsons theorem

$982! \equiv -1 \pmod{983}$

$980! \cdot 981 \cdot 982 \equiv -1 \pmod{983}$

$980!(-2)(-1) \equiv -1 \pmod{983}$

$2 \cdot 980! \equiv -1 \equiv 982 \pmod{983}$

2.980! has a remainder of 982 when divided by 983.

2. $2 \cdot 12 = 24 \equiv 1 \pmod{23}$

$3 \cdot 8 = 24 \equiv 1 \pmod{23}$

$4 \cdot 6 = 24 \equiv 1 \pmod{23}$

$5 \cdot 14 = 70 \equiv 1 \pmod{23}$

$6 \cdot 4$

$7 \cdot 10 = 70 \equiv 1 \pmod{23}$

$8 \cdot 3$

$9 \cdot 18 \equiv 5 \cdot 14 \equiv 1 \pmod{23}$

$10 \cdot 7$

$11 \cdot 21 \equiv 2 \cdot 12 \equiv 1 \pmod{23}$

$12 \cdot 2$

$13 \cdot 16 \equiv 10 \cdot 7 \equiv 1 \pmod{23}$

$14 \cdot 5$

$15 \cdot 20 \equiv 8 \cdot 3 \equiv 1 \pmod{23}$

$14 \cdot 13$

$17 \cdot 19 \equiv 6 \cdot 4 \equiv 1 \pmod{23}$

$18 \cdot 9$

$19 \cdot 17$

$20 \cdot 15$

$21 \cdot 11$

already paired

congruent

3. $18! \overset{?}{\equiv} -1 \pmod{437}$

Because $437 = 19 \cdot 23$ the congruence $18! \equiv -1 \pmod{437}$ is equivalent to the following simultaneous congruence WLOG:

$18! \equiv -1 \pmod{19}$

Because 19 is prime we can apply wilsons theorem to proove this congruence as

$(p-1)! \equiv -1 \pmod{p}$ ✓

$(18! \equiv -1 \pmod{23})$

Because 23 is prime we may use Wilson's theorem to find

$22! \equiv -1 \pmod{23}$

$18! \cdot 19 \cdot 20 \cdot 21 \cdot 22 \equiv -1 \pmod{23}$

$18!(-4)(-3)(-2)(-1) \equiv -1 \pmod{23}$

$18! \, 24 \equiv -1 \pmod{23}$

$18! \equiv -1 \pmod{23}$ ✓

4. $p \in 4k+3$, p is prime $[p>0]$

4. $k = 0$, and $k = 1$ it can be trivally verified as following

$k=0$: $\left(\left(\frac{3-1}{2}\right)!\right)^2 \equiv (1!)^2 \equiv 1 \pmod{3}$

$k=1$: $\left(\left(\frac{7-1}{2}\right)!\right)^2 \equiv (3 \cdot 2)^2 \equiv 36 \equiv 1 \pmod{7}$

The textbook shows that for a prime p, where p as before

$$(p-1)! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p}$$

which because it has $\frac{p-1}{2}$ minus signs is the same as

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}$$

applying wilsons formula we have $(p-1)! \equiv -1 \pmod{p}$

and $(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} = -1$ as $p \in 4k+3$ giving us

$$-1 \equiv -1 \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}$$

$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$ going back ↑

using this result

$$\left(\left(\left(\frac{p-1}{2}\right)!\right)^2\right)^2 \equiv (1)^2 \equiv 1 \pmod{p}$$

thus proving the proposition

4.6. as shown in (a)

$$\left(\frac{p-1}{2}\right)! = 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)$$

because of the result found in (a).

the $\left(\frac{p-1}{2}\right)!$ could be congruent with $\pm 1 \pmod{p}$ and still give the same result when squared and as you can see with the first few values of p both occur.

3. $18! \equiv -1 \pmod{437}$

7. $233^2 \equiv 3^2 \cdot 5 \pmod{13561}$ $\quad 1281^2 \equiv 2^4 \cdot 5 \pmod{13561}$

$233^2 \cdot 1281^2 \equiv 3^2 \cdot 5^2 \cdot 2^4 \pmod{13561}$

$(233 \cdot 1281)^2 \equiv (3 \cdot 5 \cdot 4)^2 \pmod{13561}$

$\gcd(233 \cdot 1281 - 3 \cdot 5 \cdot 4,\ 13561) = 71$

$\gcd(233 \cdot 1281 + 3 \cdot 5 \cdot 4,\ 13561) = 191$

using sagemath to compute gcd

only two prime factors of 13561

$71 \cdot 191 = 13561$ ✓

[redacted]