Complete Solutions to Exercise 4.2

1. In each case we use Wilson's Theorem because 11 is prime.

   (a) Wilson's Theorem is:

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

   Since 11 is prime so we have

   $$10!\equiv -1\equiv 10 \pmod{11}$$

   Therefore $x\equiv 10 \pmod{11}$.

   (b) Again using Wilson's Theorem on the given $10!+10!\equiv x \pmod{11}$:

   $$10!+10!\equiv -1+\big(-1\big)\equiv -2\equiv 9 \pmod{11}$$

   Hence $10!+10!\equiv 9 \pmod{11}$.

   (c) We are given $10\big(10!\big)+8\big(10!\big)\equiv x \pmod{11}$. Substituting $10!\equiv -1 \pmod{11}$ into this gives

   $$\begin{aligned}10\big(10!\big)+8\big(10!\big)&\equiv 10\big(-1\big)+8\big(-1\big)\\ &\equiv -18\equiv -7\equiv 4\pmod{11}\end{aligned}$$

   We have $10\big(10!\big)+8\big(10!\big)\equiv 4 \pmod{11}$.

   (d) We need to find x in the following $5\big(10!\big)^{101}+3\big(10!\big)^{100}\equiv x \pmod{11}$.

   Using $10!\equiv -1 \pmod{11}$ in this gives

   $$\begin{aligned}5\big(10!\big)^{101}+3\big(10!\big)^{100}&\equiv 5\big(-1\big)^{101}+3\big(-1\big)^{100}\\ &\equiv 5\big(-1\big)+3\big(1\big)\equiv -2\equiv 9\pmod{11}\end{aligned}$$

   Therefore $5\big(10!\big)^{101}+3\big(10!\big)^{100}\equiv 9 \pmod{11}$.

2. We are required to find the remainder when 15! is divided by 17. We use Wilson's Theorem:

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

   Since 17 is prime so substituting $p=17$ into this formula gives

   $$16!\equiv -1 \pmod{17}$$

   We can rewrite 16! as $16\times 15!$:

   $$16\times 15!\equiv -1 \pmod{17} \qquad (\dagger)$$

The inverse of $16 \equiv -1 \pmod{17}$ is $-1 \equiv 16 \pmod{17}$ because $(-1)^2 \equiv 1 \pmod{17}$. Multiplying both sides of (†) by -1 gives

$$\underbrace{-1 \times 16}_{\equiv 1} \times 15! \equiv -1 \times (-1) \equiv 1 \pmod{17}$$

Therefore $15! \equiv 1 \pmod{17}$. The remainder is 1 after 15! has been divided by 17.

3. For this we don't need to apply Wilson's Theorem because

$$25! = 1 \times 2 \times 3 \times \cdots \times 17 \times \cdots \times 25$$

Since 25! contains a multiple of 17 so $25! \equiv 0 \pmod{17}$. Therefore the remainder is 0 after 25! has been divided by 17.

4. *How can we evaluate* $x \equiv 8 \times 9 \times 10 \times 11 \times 16 \times 17 \times 18 \times 19 \pmod{13}$ *?*

Firstly we need to tame the numbers above 13 as we are working with modulo 13:

$$16 \equiv 3, \ 17 \equiv 4, \ 18 \equiv 5 \ \text{ and } \ 19 \equiv 6 \pmod{13}$$

Replacing these in the above $x \equiv 8 \times 9 \times 10 \times 11 \times 16 \times 17 \times 18 \times 19 \pmod{13}$ gives

$$\begin{aligned} x &\equiv 8 \times 9 \times 10 \times 11 \times 16 \times 17 \times 18 \times 19 \\ &\equiv 8 \times 9 \times 10 \times 11 \times 3 \times 4 \times 5 \times 6 \\ &\equiv 3 \times 4 \times 5 \times 6 \times 8 \times 9 \times 10 \times 11 \pmod{13} \ \text{[Putting numbers into ascending order]} \end{aligned}$$

Since 13 is prime so each of these numbers a =3, 4, 5, 6, 8, 9, 10 and 11 have an inverse because $\gcd(a, \ 13) = 1$. We have

$$3 \times 9 \equiv 27 \equiv 1 \pmod{13}$$

$$4 \times 10 \equiv 40 \equiv 1 \pmod{13}$$

$$5 \times 8 \equiv 40 \equiv 1 \pmod{13}$$

$$6 \times 11 \equiv 66 \equiv 1 \pmod{13}$$

Pairing these numbers up so that the product is congruent to 1 modulo 13 we have

$$\begin{aligned} x &\equiv 3\times 4\times 5\times 6\times 8\times 9\times 10\times 11 \\ &\equiv \underbrace{3\times 9}_{\equiv 1}\times \underbrace{4\times 10}_{\equiv 1}\times \underbrace{5\times 8}_{\equiv 1}\times \underbrace{6\times 11}_{\equiv 1} \\ &\equiv 1\times 1\times 1\times 1\equiv 1\Big(\text{mod } 13\Big) \end{aligned}$$

Hence $x\equiv 1\Big(\text{mod } 13\Big)$.

5. We need to find $x\equiv 2\times\Big(20!\Big)\Big(\text{mod } 23\Big)$. Since 23 is prime we have

$$22!\equiv -1\Big(\text{mod } 23\Big)$$

We can rewrite 22! as $22\times 21\times 20!$ Using this in the calculation of 20! gives

$$22!\equiv 22\times 21\times 20!\equiv -1\Big(\text{mod } 23\Big) \qquad (*)$$

Note that $22\equiv -1\Big(\text{mod } 23\Big)$. Substituting this $22\equiv -1\Big(\text{mod } 23\Big)$ into (*) yields

$$\Big(-1\Big)\times 21\times 20!\equiv -1\Big(\text{mod } 23\Big)$$

Multiplying this by -1 gives

$$21\times 20!\equiv 1\Big(\text{mod } 23\Big)$$

We have $21\equiv -2\Big(\text{mod } 23\Big)$ and $-2\times 11\equiv -22\equiv 1\Big(\text{mod } 23\Big)$. This implies that $11\Big(\text{mod } 23\Big)$ is the inverse of $21\Big(\text{mod } 23\Big)$ because

$$21\times 11\equiv -2\times 11\equiv 1\Big(\text{mod } 23\Big)$$

Multiplying both sides of $21\times 20!\equiv 1\Big(\text{mod } 23\Big)$ by 11 gives

$$20!\equiv 11\Big(\text{mod } 23\Big)$$

Substituting $20!\equiv 11\Big(\text{mod } 23\Big)$ into the given congruence:

$$x\equiv 2\times\Big(20!\Big)\equiv 2\times 11\equiv 22\equiv -1\Big(\text{mod } 23\Big)$$

Hence $x\equiv -1\Big(\text{mod } 23\Big)$.

6. We need to find x such that $96\times 97\times 98\times 99\times 100\equiv x\Big(\text{mod } 101\Big)$. Writing these numbers as negative residues modulo 101 gives

$$\begin{aligned} x &\equiv 96\times 97\times 98\times 99\times 100 \\ &\equiv \Big(-5\Big)\times\Big(-4\Big)\times\Big(-3\Big)\times\Big(-2\Big)\times\Big(-1\Big) \\ &\equiv -120\equiv -19\equiv 82\Big(\text{mod } 101\Big) \end{aligned}$$

Therefore $x\equiv 82\Big(\text{mod } 101\Big)$.

7. We need to find $61!\,\big(\mathrm{mod}\ 71\big)$. Since 71 is prime so by Wilson's Theorem we have

$$70! \equiv -1\,\big(\mathrm{mod}\ 71\big)$$

We can rewrite this as

$$70! \equiv 61!\times 62\times\cdots\times 69\times 70 \equiv -1\,\big(\mathrm{mod}\ 71\big)$$

Writing each of these numbers 62, 63, $\cdots$, 69 and 70 as negative least residues modulo 71 in a list:

$$62\equiv -9,\ \ 63\equiv -8,\ \ 64\equiv -7,\ \ 65\equiv -6,\ \ 66\equiv -5,\ \ 67\equiv -4,$$
$$68\equiv -3,\ \ 69\equiv -2\ \ \text{and}\ \ \ 70\equiv -1\,\big(\mathrm{mod}\ 71\big)$$

Multiplying the first two numbers in this list gives

$$62\times 63 \equiv -9\times -8 \equiv 72 \equiv 1\,\big(\mathrm{mod}\ 71\big) \qquad (*)$$

Combining other numbers in the list:

$$65\times 67\times 68 \equiv -6\times\big(-4\big)\times\big(-3\big) \equiv -72 \equiv -1\,\big(\mathrm{mod}\ 71\big) \qquad (**)$$

We are only left with 64, 66, 69 and 70 from the list:

$$\begin{aligned} 64\times 66\times 69\times 70 &\equiv \big(-7\big)\times\big(-5\big)\times\big(-2\big)\times\big(-1\big) \\ &\equiv 70 \equiv -1\,\big(\mathrm{mod}\ 71\big) \qquad \big(***\big)\end{aligned}$$

Substituting each of these results (*), (**) and (***):

$$62\times 63\equiv 1\,,\ 65\times 67\times 68\equiv -1\ \text{ and }\ 64\times 66\times 69\times 70\equiv -1\,\big(\mathrm{mod}\ 71\big)$$

into $70!\equiv 61!\times 62\times\cdots\times 69\times 70\equiv -1\,\big(\mathrm{mod}\ 71\big)$ gives:

$$70!\equiv \big(61\big)!\times 1\times\big(-1\big)\times\big(-1\big)\equiv 61!\equiv -1\,\big(\mathrm{mod}\ 71\big)$$

Hence $61!\equiv -1\equiv 70\,\big(\mathrm{mod}\ 71\big)$.

8. (a) We need to evaluate $\big(n-1\big)!\,\big(\mathrm{mod}\ n\big)$ for $n=15$:

$$\begin{aligned}\big(15-1\big)!&\equiv 14! \\ &\equiv 1\times 2\times 3\times\cdots\times 14 \\ &\equiv \underbrace{3\times 5}_{\equiv 0\ (\mathrm{mod}\ 15)}\times 1\times 2\times 4\times 6\times\cdots\times 14 \equiv 0\,\big(\mathrm{mod}\ 15\big)\end{aligned}$$

We have $\big(15-1\big)!\equiv 0\,\big(\mathrm{mod}\ 15\big)$.

(b) Similarly we have to evaluate $\big(n-1\big)!\,\big(\mathrm{mod}\ n\big)$ for $n=21$:

$$\begin{aligned}\big(21-1\big)! &\equiv 20! \\ &\equiv 1\times 2\times 3\times\cdots\times 20 \\ &\equiv \underbrace{3\times 7}_{\equiv 0\ \pmod{21}}\times 1\times 2\times 4\times\cdots\times 6\times 8\times\cdots\times 20 \equiv 0\ \big(\text{mod } 21\big)\end{aligned}$$

Therefore $\big(21-1\big)! \equiv 0\ \big(\text{mod } 21\big)$.

(c) Repeating the above calculations for $n = 30$ we have

$$\begin{aligned}\big(30-1\big)! &\equiv 29! \\ &\equiv 1\times 2\times 3\times\cdots\times 29 \\ &\equiv \underbrace{2\times 3\times 5}_{\equiv 0\ \pmod{30}}\times 1\times 4\times 6\times 7\times\cdots\times 29 \equiv 0\ \big(\text{mod } 30\big)\end{aligned}$$

We have $\big(30-1\big)! \equiv 0\ \big(\text{mod } 30\big)$.

In each case n is *composite* and we can always find the factors of this number between 1 and $n-1$ therefore $\big(n-1\big)! \equiv 0\ \big(\text{mod } n\big)$. (See question 10.)

9. We are required to find $\left[\left(\frac{\big(29-1\big)}{2}\right)!\right]^2 \big(\text{mod } 29\big)$. Simplifying $\frac{\big(29-1\big)}{2} = 14$ and now finding 14 factorial modulo 29 gives

$$\begin{aligned}14! &\equiv \underbrace{2\times 3\times 5}_{\equiv 30\equiv 1}\times\underbrace{\big(4\times 7\big)}_{\equiv 28\equiv -1}\times\underbrace{\big(6\times 10\big)}_{\equiv 60\equiv 2}\times\underbrace{\big(11\times 13\big)}_{\equiv 143\equiv -2}\times\underbrace{\big(8\times 14\big)}_{\equiv 112\equiv -4}\times\underbrace{\big(9\times 12\big)}_{\equiv 108\equiv -8} \\ &\equiv 1\times\big(-1\big)\times 2\times\big(-2\big)\times\underbrace{\big(-4\big)\times\big(-8\big)}_{\equiv 32\equiv 3} \\ &\equiv 1\times\big(-1\big)\times 2\times\big(-2\big)\times 3 \equiv 12\big(\text{mod } 29\big)\end{aligned}$$

Evaluating $\left[\left(\frac{\big(29-1\big)}{2}\right)!\right]^2 \equiv 12^2 \equiv 144 \equiv -1 \equiv 28\big(\text{mod } 29\big)$.

10. We are asked to prove:

$$\big(n-1\big)! \equiv \begin{cases} -1\ \big(\text{mod } n\big) & \text{if } n \text{ is prime} \\ 2\big(\text{mod } n\big) & \text{if } n = 4 \\ 0\big(\text{mod } n\big) & \text{for all other cases} \end{cases}$$

Proof.

Clearly if n is prime by Wilson's Theorem we have

$$\big(n-1\big)! \equiv -1\big(\text{mod } n\big)$$

If $n = 4$ then

$$(4-1)! \equiv 3! \equiv 6 \equiv 2 \pmod 4$$

We have our result for $n = 4$.

For all other cases n must be composite because either n is prime or composite and we have already covered the case when n is prime. Let $n = d_1 \times d_2$ where d_1 and d_2 are non-trivial factors of n, that is $1 < d_1 < n$ and $1 < d_2 < n$.

Evaluating $(n-1)! \pmod n$ gives

$$\begin{aligned}(n-1)! &\equiv (d_1 \times d_2 - 1)! \\ &\equiv 1 \times 2 \times \cdots \times d_1 \times (d_1+1) \times \cdots \times d_2 \times \cdots \times (d_1 \times d_2 - 1) \\ &\equiv d_1 \times d_2 \times 1 \times 2 \times \cdots \times (d_1 \times d_2 - 1) \\ &\equiv \underbrace{\qquad\qquad}_{\text{Because } d_1 \times d_2 \equiv 0 \pmod{d_1 \times d_2}} \times 1 \times 2 \times \cdots \times (d_1 \times d_2 - 1) \equiv 0 \pmod{d_1 \times d_2}\end{aligned}$$

Hence for all composite numbers n apart from 4 we have

$$(n-1)! \equiv 0 \pmod n$$

This completes our proof.

■

11. We are asked to show that $x^2 \equiv 1 \pmod n \not\Rightarrow x \equiv \pm 1 \pmod n$. This will work for any composite n. Consider $n = 15$ then

$$x^2 \equiv 1 \pmod{15}$$

Let $x = 4$ then we have

$$x^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{15}$$

Hence a solution to $x^2 \equiv 1 \pmod{15}$ is $x \equiv 4 \not\equiv \pm 1 \pmod{15}$.

We only have $x^2 \equiv 1 \pmod n \Rightarrow x \equiv \pm 1 \pmod n$ if n is prime.

12. *Proof.*

We are given that p is prime and $\gcd(n, \quad p) = 1$ so by *FlT* (4.1):

$$n^{p-1} \equiv 1 \pmod p$$

We have $n^{p-1} \equiv 1 \pmod p$. Again as p is prime by Wilson's Theorem we have

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

Putting both these $n^{p-1} \equiv 1 \pmod p$ and $(p-1)! \equiv -1 \pmod p$ into $(p-1)! + n^{p-1}$ yields

$$\big(p-1\big)!+n^{p-1}\equiv -1+1\equiv 0\ \big(\text{mod } p\big)$$

We have our required result. This means prime p divides $\big(p-1\big)!+n^{p-1}$.

■

13. We are required to prove that $\big(p-2\big)!\equiv 1\ \big(\text{mod } p\big)$.

Proof.

Let p be prime. By Wilson's Theorem we have

$$\big(p-1\big)!\equiv -1\ \big(\text{mod } p\big)$$

Rewriting $\big(p-1\big)!=\big(p-1\big)\big(p-2\big)!$ and substituting this into the above gives

$$\big(p-1\big)\big(p-2\big)!\equiv -1\ \big(\text{mod } p\big).$$

Note that $p-1\equiv -1\ \big(\text{mod } p\big)$. Substituting this into the above line gives

$$\begin{aligned}\big(-1\big)\big(p-2\big)!&\equiv -1\ \big(\text{mod } p\big)\\ \big(p-2\big)!&\equiv 1\ \big(\text{mod } p\big)\qquad \big[\text{Multiplying by } -1\big]\end{aligned}$$

We have $\big(p-2\big)!\equiv 1\ \big(\text{mod } p\big)$ which is our required result.

■

14. We need to prove $2\big(p-3\big)!\equiv -1\ \big(\text{mod } p\big)$. *How?*

Using the result of previous question.

Proof.

By previous question we have $\big(p-2\big)!\equiv 1\ \big(\text{mod } p\big)$. Rewriting $\big(p-2\big)!$ as follows:

$$\big(p-2\big)!\equiv\big(p-2\big)\big(p-3\big)!\equiv 1$$

Note that $p-2\equiv -2\ \big(\text{mod } p\big)$. Putting this into the above result gives

$$\big(p-2\big)\big(p-3\big)!\equiv\big(-2\big)\big(p-3\big)!\equiv 1\ \big(\text{mod } p\big)$$

Multiplying both sides by -1:

$$2\big(p-3\big)!\equiv -1\ \big(\text{mod } p\big)$$

This $2\big(p-3\big)!\equiv -1\ \big(\text{mod } p\big)$ is the result we needed to prove.

■

15. We need to show that $\big(p-1\big)\big(p-2\big)\cdots\big(p-n\big)\equiv\big(-1\big)^n\,n!$

Proof.

We have

$$\begin{aligned}\big(p-1\big)\times\big(p-2\big)\times\cdots\times\big(p-n\big) &\equiv \big(-1\big)\times\big(-2\big)\times\big(-3\big)\times\cdots\times\big(-n\big)\\ &\equiv \big(-1\big)^n\big[1\times 2\times 3\times\cdots\times n\big]\\ &\equiv \big(-1\big)^n n!\end{aligned}$$

■

16. We are required to prove that $x^2+1\equiv 0\big(\text{mod } p\big)$ has a solution

$$\Leftrightarrow\ \ p=2\ \text{ or } p\equiv 1\ \big(\text{mod } 4\big).$$

Proof.

We divide the proof into two parts; $p=2$ and $p\equiv 1\big(\text{mod } 4\big)$.

If $p=2$ then

$$x^2+1\equiv 0\ \Rightarrow\ x^2\equiv -1\big(\text{mod } 2\big)\ \Rightarrow\ x\equiv \pm 1\big(\text{mod } 2\big).$$

Now we consider the case $p\equiv 1\big(\text{mod } 4\big)$.

$(\Rightarrow)$. Since p is an odd prime it can only be of the form

$$p\equiv 1\ \big(\text{mod } 4\big)\ \text{ or }\ p\equiv 3\ \big(\text{mod } 4\big).$$

Suppose $x^2+1\equiv 0\big(\text{mod } p\big)$ has a solution, $x=a$ say. From this we have

$$a^2\equiv -1\big(\text{mod } p\big)\qquad\qquad (\dagger)$$

By $(\dagger)$ we have $p\not| a$ because if $p\mid a$ then

$$a\equiv 0\big(\text{mod } p\big)\ \Rightarrow\ a^2\equiv 0^2\equiv 0\big(\text{mod } p\big)$$

By *FlT* we have $a^{p-1}\equiv 1\ \big(\text{mod } p\big)$. Using these two results, $a^2\equiv -1\big(\text{mod } p\big)$ and $a^{p-1}\equiv 1\ \big(\text{mod } p\big)$, gives

$$1\equiv a^{p-1}\equiv a^{2\left(\frac{p-1}{2}\right)}\equiv\big(a^2\big)^{\frac{p-1}{2}}\underbrace{\equiv}_{\text{by }(\dagger)}\big(-1\big)^{\frac{p-1}{2}}\ \big(\text{mod } p\big)\qquad (\ddagger)$$

If $p\equiv 3\ \big(\text{mod } 4\big)$ then $\dfrac{p-1}{2}$ is odd. *Why?*

Because we have $p\equiv 3\ \big(\text{mod } 4\big)$ which implies

$$p=3+4k \text{ for some integer } k.$$

Substituting this $p=3+4k$ into $\dfrac{p-1}{2}$ gives

$$\frac{p-1}{2}=\frac{3+4k-1}{2}=\frac{4k+2}{2}=2k+1$$

Hence $\frac{p-1}{2} = 2k+1$ implies that $\frac{p-1}{2}$ is odd.

Therefore $\left(-1\right)^{\frac{p-1}{2}} \equiv \left(-1\right)^{\text{odd index}} \equiv -1\left(\text{mod } p\right)$. We have a contradiction because from (‡) we have $a^{p-1} \equiv \left(-1\right)^{\frac{p-1}{2}} \equiv -1\left(\text{mod } p\right)$ but *FlT* says

$$a^{p-1} \equiv +1\left(\text{mod } p\right)$$

We are given that p is an *odd* prime so $p \not\equiv 3\left(\text{mod } 4\right)$.

Therefore $p \equiv 1\left(\text{mod } 4\right)$.

$\left(\Leftarrow\right)$. Assume $p \equiv 1\left(\text{mod } 4\right)$. We need to show that there is a residue x such that $x^2 + 1 \equiv 0\left(\text{mod } p\right)$ or $x^2 \equiv -1\left(\text{mod } p\right)$. If we can find such an x then we will have proven this part $(\Leftarrow)$ as well. We will find an x such that

$$x^2 \equiv -1\left(\text{mod } p\right)$$

Since we are interested in residue -1 so we use Wilson's Theorem:

$$\left(p-1\right)! \equiv -1\left(\text{mod } p\right) \qquad (\dagger)$$

We can rewrite $\left(p-1\right)!$ as

$$\left(p-1\right)! = 1\times 2\times 3\times\cdots\times\left(\frac{p-1}{2}\right)\times\left(\frac{p+1}{2}\right)\times\cdots\times\left(p-2\right)\times\left(p-1\right) \qquad (*)$$

Note that

$$p-1 \equiv -1\left(\text{mod } p\right)$$
$$p-2 \equiv -2\left(\text{mod } p\right)$$
$$\vdots$$
$$\left(\frac{p+1}{2}\right) \equiv -\left(\frac{p-1}{2}\right)\left(\text{mod } p\right)$$

Substituting these into (*) and working with modulo p gives

$$\begin{aligned}\left(p-1\right)! &\equiv 1\times 2\times 3\times\cdots\times\left(\frac{p-1}{2}\right)\times\left(\frac{p+1}{2}\right)\times\cdots\times\left(p-2\right)\times\left(p-1\right)\\ &\equiv 1\times 2\times 3\times\cdots\times\left(\frac{p-1}{2}\right)\times\left(-\frac{p-1}{2}\right)\times\cdots\times\left(-2\right)\times\left(-1\right)\\ &\equiv \left(-1\right)^{\frac{p-1}{2}}\left[1^2\times 2^2\times 3^2\times\cdots\times\left(\frac{p-1}{2}\right)^2\right]\\ &\equiv \left(-1\right)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2\left(\text{mod } p\right) \qquad (\dagger\dagger)\end{aligned}$$

All this is congruent to $-1\left(\text{mod } p\right)$ because of (†). Equating these gives

$$\left(-1\right)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1\left(\text{mod } p\right) \qquad (**)$$

Let $x=\left(\frac{p-1}{2}\right)!$ then we can rewrite (**) as

$$\left(-1\right)^{\frac{p-1}{2}} x^2 \equiv -1\left(\text{mod } p\right) \qquad (***)$$

We only now need to show that for the appropriate prime p that

$$\left(-1\right)^{\frac{p-1}{2}} = +1$$

For this part we are assuming that $p \equiv 1\left(\text{mod } 4\right)$ so $p=4k+1$. Substituting this $p=4k+1$ into $\frac{p-1}{2}$ gives $\frac{p-1}{2}=\frac{4k+1-1}{2}=2k$ $\left[\text{even}\right]$. Hence $\left(-1\right)^{\frac{p-1}{2}}=+1$ so substituting this into (***) yields

$$\left(-1\right)^{\frac{p-1}{2}} x^2 \equiv +1x^2 \equiv x^2 \equiv -1\left(\text{mod } p\right)$$

Therefore we have found a solution $x=\left(\frac{p-1}{2}\right)!$ such that $x^2 \equiv -1\left(\text{mod } p\right)$ or $x^2+1 \equiv 0\left(\text{mod } p\right)$. This completes our proof.

■

17. We are asked to prove Wilson's Theorem $\left(p-1\right)! \equiv -1\left(\text{mod } p\right)$ by using *FlT*.

Proof.

For the even prime 2 we have $\left(2-1\right)! \equiv 1 \equiv -1\left(\text{mod } 2\right)$. The result holds for $p=2$.

Let p be an odd prime such that it does *not* divide x. Then by *FlT* we have

$$x^{p-1} \equiv 1\left(\text{mod } p\right)$$

Rewriting this as

$$x^{p-1}-1 \equiv 0\left(\text{mod } p\right) \qquad (*)$$

By *FlT* the solutions to this are $x=1, 2, 3, 4, \cdots, p-1$. Therefore factorizing (*) gives

$$x^{p-1}-1 \equiv \left(x-1\right)\left(x-2\right)\cdots\left(x-\left(p-1\right)\right) \equiv 0\left(\text{mod } p\right)$$

Substituting $x=0$ into this yields

$$\begin{aligned}
0-1 &\equiv \big(0-1\big)\big(0-2\big)\cdots\Big(0-\big(p-1\big)\Big)\\
-1 &\equiv \big(-1\big)\big(-2\big)\cdots\Big(-\big(p-1\big)\Big)\\
&\equiv \underbrace{-\,-\cdots-}_{\substack{\text{There are } p-1=\text{even}\\ \text{minuses}}}\ \big(1\big)\big(2\big)\cdots\big(p-1\big)\\
&\equiv \big(p-1\big)!\big(\bmod\ p\big)
\end{aligned}$$

Hence we have our result.

■

18. We need to prove $\Big(1\times 3\times 5\times\cdots\times\big(p-2\big)\Big)^2 \equiv \big(-1\big)^{\frac{p+1}{2}}\ \big(\bmod\ p\big)$.

Proof.

Consider the left-hand-side residue without the square:

$$\begin{aligned}
1\times 3\times 5\times\cdots\times\big(p-2\big) &\equiv 1\times 3\times\cdots\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-1}{2}\right)\times\left(\frac{p+3}{2}\right)\times\left(\frac{p+7}{2}\right)\times\cdots\times\big(p-4\big)\times\big(p-2\big)\\
&\equiv 1\times 3\times\cdots\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-1}{2}\right)\times\left(p-\frac{p-3}{2}\right)\times\left(p-\frac{p-7}{2}\right)\times\cdots\times\big(p-4\big)\times\big(p-2\big)\\
&\equiv 1\times 3\times\cdots\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-1}{2}\right)\times\left(-\frac{p-3}{2}\right)\times\left(-\frac{p-7}{2}\right)\times\cdots\big(-4\big)\times\big(-2\big)\\
&\equiv 1\times 3\times\cdots\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-1}{2}\right)\times\big(-1\big)\left(\frac{p-3}{2}\right)\times\big(-1\big)\left(-\frac{p-7}{2}\right)\times\cdots\times\big(-1\big)\big(4\big)\times\big(-1\big)\big(2\big)
\end{aligned}$$

Squaring both sides of this because we are given $\Big(1\times 3\times 5\times\cdots\times\big(p-2\big)\Big)^2$:

$$\begin{aligned}
\Big(1\times 3\times 5\times\cdots\times\big(p-2\big)\Big)^2 &\equiv \left(1\times 3\times\cdots\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-1}{2}\right)\times\big(-1\big)\left(\frac{p-3}{2}\right)\times\big(-1\big)\left(\frac{p-7}{2}\right)\times\cdots\times\big(-1\big)\big(4\big)\times\big(-1\big)\big(2\big)\right)^2\\
&\equiv \left(1\times 3\times\cdots\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-1}{2}\right)\times\left(\frac{p-3}{2}\right)\times\left(\frac{p-7}{2}\right)\times\cdots\times\big(4\big)\times\big(2\big)\right)^2\Big(\big(-1\big)\times\cdots\times\big(-1\big)\Big)^2\\
&\equiv \left(1\times 3\times\cdots\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-1}{2}\right)\times\left(\frac{p-3}{2}\right)\times\left(\frac{p-7}{2}\right)\times\cdots\times 4\times\big(2\big)\right)^2\\
&\equiv \left(1\times 2\times 3\times 4\times\cdots\times\left(\frac{p-7}{2}\right)\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-3}{2}\right)\times\left(\frac{p-1}{2}\right)\right)^2\\
&\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2\ \big(\bmod\ p\big)\quad (*)\qquad \left[\text{Because } 1\times 2\times\cdots\times\left(\frac{p-3}{2}\right)\times\left(\frac{p-1}{2}\right)=\left(\frac{p-1}{2}\right)!\right]
\end{aligned}$$

From the calculation of question 16 (††) we have

$$\big(p-1\big)!\equiv\big(-1\big)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2\big(\bmod\ p\big)\qquad(\dagger\dagger)$$

By Wilson's Theorem we have

$$\big(p-1\big)!\equiv -1\ \big(\bmod\ p\big).$$

Equating these last two equations gives

$$\left(-1\right)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1\left(\text{mod } p\right).$$

Multiplying both sides of this $\left(-1\right)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1$ by $\left(-1\right)^{\frac{p-1}{2}}$ yields

$$\left(-1\right)^{\frac{p-1}{2}}\left(-1\right)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv \underbrace{\left(-1\right)^{2\left(\frac{p-1}{2}\right)}}_{=1}\left[\left(\frac{p-1}{2}\right)!\right]^2$$

$$\equiv \left(-1\right)^1\left(-1\right)^{\frac{p-1}{2}} \equiv \left(-1\right)^{1+\frac{p-1}{2}} \equiv \left(-1\right)^{\frac{p+1}{2}}\left(\text{mod } p\right)$$

We have

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv \left(-1\right)^{\frac{p+1}{2}}\left(\text{mod } p\right)$$

Putting this into (*) yields

$$\left(1\times 3\times 5\times\cdots\times\left(p-2\right)\right)^2 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv \left(-1\right)^{\frac{p+1}{2}}\left(\text{mod } p\right)$$

This completes our proof.

■