Complete Solutions to Supplementary Problems 4

1. (a) We are asked to find the inverse of $10 \pmod{101}$. This means we need to solve $10x \equiv 1 \pmod{101}$. Multiplying both sides of this congruence by 10 gives

$$10 \times 10x \equiv 100x \equiv -x \equiv 10 \pmod{101}$$

Multiplying the last result by -1 yields

$$x \equiv -10 \equiv 91 \pmod{101}$$

Hence $91 \pmod{101}$ is the inverse of $10 \pmod{101}$ or $10^{-1} \equiv 9 \pmod{101}$.

(b) We use Fermat's Little Theorem to find the inverse of $125 \pmod{127}$:

$$a^{p-1} \equiv 1 \pmod{p} \text{ provided } p \nmid a$$

We have

$$125^{126} \equiv 125\left(125^{125}\right) \equiv 1 \pmod{127}$$

Evaluating $125^{125} \equiv ? \pmod{127}$ will be time consuming. *How can we make this problem easier?*

Well $125 \equiv -2 \pmod{127}$ so $125^{125} \equiv (-2)^{125} \pmod{127}$. Working out this power of -2 gives

$$(-2)^{125} \equiv (-1)^{125} \times 2^{125} \equiv (-1) \times 2^{125} \pmod{127} \qquad (\dagger)$$

Determining some simple powers of 2:

$$2^4 \equiv 16,\ \ 2^5 \equiv 32,\ \ 2^6 \equiv 64,\ \ 2^7 \equiv 128 \equiv 1 \pmod{127}$$

The last result $2^7 \equiv 1 \pmod{127}$ is particularly useful because any index with base 1 will be 1. Writing 125 as a multiple of 7 and remainder gives

$$125 = (17 \times 7) + 6$$

Using the rules of indices to evaluate $2^{125} \pmod{127}$ yields

$$2^{125} \equiv \left(2^7\right)^{17} \times 2^6 \equiv 1 \times 2^6 \equiv 64 \pmod{127}$$

Substituting this $2^{125} \equiv 64 \pmod{127}$ into $(\dagger)$ gives

$$(-2)^{125} \equiv (-1) \times 64 \equiv -64 \equiv 63 \pmod{127}$$

Hence the inverse of $125 \pmod{127}$ is $63 \pmod{127}$.

(c) This time we are given $540! \pmod{541}$. We use Wilson's Theorem (4.4):

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

Hence $540! \equiv -1 \pmod{541}$. We have

$$540!\, x \equiv (-1)x \equiv 1 \pmod{541} \quad \Rightarrow \quad x \equiv -1 \equiv 540 \pmod{541}$$

2. (i) We are asked to find $10^{27} \pmod{29}$. Since 29 is prime so by Fermat's Little Theorem we have

$$10^{28} \equiv 1 \pmod{29}$$

Rearranging the indices we have

$$10^{28} \equiv 10\left(10^{27}\right) \equiv 1 \pmod{29}$$

Hence the inverse of $10 \pmod{29}$ is $10^{27} \pmod{29}$. Solving $10x \equiv 1 \pmod{29}$ gives $x \equiv 3 \pmod{29}$ because $10 \times 3 \equiv 30 \equiv 1 \pmod{29}$. Hence

$$10^{27} \equiv 3 \pmod{29}$$

(ii) *How do we solve the linear congruence* $10x \equiv 9 \pmod{29}$ *?*

Multiple both sides of this congruence by the inverse of $10 \pmod{29}$ which is $3 \pmod{29}$ which we found in part (i). Therefore

$$x \equiv 9 \times 3 \equiv 27 \pmod{29}$$

Our solution is $x \equiv 27 \pmod{29}$.

3. We need to evaluate $7^{1\,000\,003} \equiv x \pmod{11}$. By Fermat's Little Theorem (FLT):

$$a^{p-1} \equiv 1 \pmod{p} \text{ provided } p \nmid a$$

We have $7^{10} \equiv 1 \pmod{11}$. Using the rules of indices on the index 1 000 003:

$$7^{1\,000\,003} \equiv 7^{1\,000\,000} \times 7^3 \equiv \left(7^{10}\right)^6 \times 7^3 \equiv (1)^6 \times 7^3 \equiv 7^3 \pmod{11}$$

Working out the last congruence gives

$$7^{1000003} \equiv 7^3 \equiv 343 \equiv 2 \pmod{11}$$

4. (i) We need to find the inverse of $30 \pmod{31}$. Let y be the inverse then

$$30y \equiv 1 \pmod{31}$$

Note that $30 \equiv -1 \pmod{31}$. Using this to rewrite the above congruence gives

$$30y \equiv -y \equiv 1 \quad \Rightarrow \quad y \equiv -1 \equiv 30 \pmod{31}$$

Hence the inverse of $30 \pmod{31}$ is $30 \pmod{31}$.

(ii) We are asked to find x such that $5(29!) \equiv x \pmod{31}$. By Wilson's Theorem (4.4):

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

We have $30! \equiv -1 \pmod{31}$ because 31 is prime. We can rewrite this as

$$29! \times 30 \equiv -1 \pmod{31} \qquad (*)$$

Multiplying both sides of (*) by the inverse of $30 \pmod{31}$ which is $30 \pmod{31}$ by part (i):

$$29! \times \underbrace{30 \times 30}_{\equiv 1 \pmod{31}} \equiv -1 \times 30 \pmod{31}$$

$$29! \equiv -30 \equiv 1 \pmod{31}$$

Substituting $29! \equiv 1 \pmod{31}$ into the given linear congruence $5(29!) \equiv x \pmod{31}$ yields $5(1) \equiv 5 \equiv x \pmod{31}$. Hence $x \equiv 5 \pmod{31}$.

5. We are asked to find the inverse of $11! \pmod{13}$.

As 13 is prime so by Wilson's Theorem we have

$$12! \equiv -1 \pmod{13}$$

We can rewrite $12! = 12 \times 11!$. Substituting this into the above gives

$$12! = 12 \times 11! \equiv -1 \pmod{13}$$

$$(-1) \times 11! \equiv -1 \pmod{13} \qquad \left[\text{Because } 12 \equiv -1 \pmod{13}\right]$$

Multiplying both sides of the last congruence by -1 yields

$$11! \equiv 1 \pmod{13}$$

Hence the inverse of $11! \pmod{13}$ is $1 \pmod{13}$.

6. We are asked to prove the inverse of $(p-3)! \pmod{p}$ is $(p-2) \pmod{p}$.

Proof.

By Question 13 of Exercise 4(b) we have $(p-2)! \equiv 1 \pmod{p}$. Rewriting $(p-2)!$ as

$$(p-2)! \equiv (p-2)(p-3)! \equiv 1 \pmod{p}$$

Since $(p-2)(p-3)! \equiv 1 \pmod{p}$ so $(p-2) \pmod{p}$ is the inverse of $(p-3)! \pmod{p}$.

■

7. *How do we factorize integers of the type* $2^n - 1$ *?*

By Proposition (4.9):

> If $m \mid n$ then $(2^m - 1) \mid (2^n - 1)$.

(a) We are given $2^{14} - 1$. The non-trivial factors of 14 are 2 and 7. Therefore applying this Proposition (4.9) we have the following factors:

$$2^2 - 1 = 3 \text{ and } 2^7 - 1 = 127.$$

Both of these numbers are prime (check this for yourself) so dividing $2^{14} - 1$ by 3×127 gives

$$\frac{2^{14} - 1}{3 \times 127} = 43 \text{ which is prime.}$$

Therefore $2^{14} - 1 = 3 \times 43 \times 127$.

(b) Similarly we have the non-trivial factors of 15 are 3 and 5 so

$$2^3 - 1 = 7 \text{ and } 2^5 - 1 = 31.$$

are prime factors of $2^{15} - 1$. Dividing this $2^{15} - 1$ by 7×31 gives

$$\frac{2^{15} - 1}{7 \times 31} = 151 \qquad (\dagger)$$

Is 151 prime?

By using Corollary (2.10)

> If $n > 1$ is composite then it has a prime divisor p such that $p \le \lfloor \sqrt{n} \rfloor$.

Let $n = 151$ and p be a prime factor of 151 then

$$p \le \lfloor \sqrt{151} \rfloor = 12.$$

The primes below 12 are 2, 3, 5, 7 and 11. None of these go into 151 so 151 is prime.

Hence the prime decomposition of $2^{15} - 1$ by (†) is $7 \times 31 \times 151$.

(c) Since $2 \times 8 = 16$ so $2^2 - 1 = 3$ and $2^8 - 1 = 255$ are factors of $2^{16} - 1$.

Dividing $2^{16} - 1$ by the largest factor 255 gives

$$\frac{2^{16} - 1}{255} = 257.$$

Using Corollary (2.10) to see if 257 is prime. Let p be a prime factor of 257 then

$$p \le \left\lfloor \sqrt{257} \right\rfloor = 16 .$$

The primes below 16 are 2, 3, 5, 7, 11 and 13. None of these primes go into 257 therefore 257 is prime.

Now we only need to find the factors of 255. Clearly 3 and 5 are factors of 255 so $\dfrac{255}{3\times 5} = 17$ which is prime. Therefore $255 = 3\times 5\times 17$. Thus collecting all the factors we have

$$2^{16} - 1 = 255 \times 257 = 3\times 5\times 17\times 257 .$$

8. (a) We are asked to prove 31 is a factor of $2^{5n} - 1$.

Proof.

Since for the index $5 \mid 5n$ so by Proposition (4.9):

> If $m \mid n$ then $\left(2^m - 1\right) \mid \left(2^n - 1\right)$.

We have $2^5 - 1 = 31$ is a factor of $2^{5n} - 1$.

■

(b) This time we need to prove that 2047 is a factor of $2^{1\,100\,001\,111} - 1$. The index 1 100 001 111 is divisible by 11 so by Proposition (4.9) we have

$$2^{11} - 1 = 2047 \text{ is a factor of } 2^{1\,100\,001\,111} - 1 .$$

Since the sum of the digits of the index is given by

$$1+1+0+0+0+0+1+1+1+1 = 6 .$$

And $3 \mid 6$ so $2^3 - 1 = 7$ is also a factor of $2^{1\,100\,001\,111} - 1$.

9. We are asked to prove that if $m \mid n$ then $\left(a^m - 1\right) \mid \left(a^n - 1\right)$.

Proof.

We are given that $m \mid n$ so there is an integer s such that $ms = n$. Using the given hint with $r = m$ and $s = s$ we have

$$a^n - 1 = a^{ms} - 1 = \left(a^m - 1\right)\left(a^{m(s-1)} + a^{m(s-2)} + a^{m(s-3)} + \cdots + a^m + 1\right).$$

Hence $\left(a^m - 1\right) \mid \left(a^n - 1\right)$ which is our required result.

■

10. (a) We are asked to show $5^{11} - 1$ is a factor of $5^{55} - 1$.

Proof.

Using the result of the previous question if $m \mid n$ then $\left(a^m - 1\right) \mid \left(a^n - 1\right)$ with $a = 5$, $m = 11$ and $n = 55$ gives

$$\left(5^{11} - 1\right) \mid \left(5^{55} - 1\right).$$

This is our required result. ■

(b) Using the result of the previous question if $m \mid n$ then $\left(a^m - 1\right) \mid \left(a^n - 1\right)$ with $a = 5$ and $n = 10 = 2 \times 5$ we have

$$5^2 - 1 = 24 \text{ and } 5^5 - 1 = 3124 \text{ are factors of } 5^{10} - 1.$$

Dividing $5^{10} - 1$ by the largest factor 3124 gives

$$\frac{5^{10} - 1}{3124} = 3126 \qquad (\ddagger)$$

Since 3126 is even so we have

$$\frac{3126}{2} = 1563 \qquad (*)$$

Note that the sum of the digits of 1563 are $1 + 5 + 6 + 3 = 15$ and $3 \mid 15$ so 1563 is divisible by 3:

$$\frac{1563}{3} = 521 \qquad (**)$$

Need to check whether 521 is prime as there are no obvious factors of this number. Let p be a prime factor of 521 then

$$p \le \left\lfloor \sqrt{521} \right\rfloor = 22$$

The primes below 22 are 2, 3, 5, 7, 11, 13, 17 and 19. The first 5 primes 2, 3, 5, 7 and 11 are easy to check and these do not go into 521. Just need to see if 13, 17 or 19 go into 521. They don't so 521 is prime.

By (*) and (**) the prime factorization of $3126 = 2 \times 1563 = 2 \times 3 \times 521$.

The other factor of $5^{10} - 1$ is 3124 which you can see from the above (‡).

We have

$$\frac{3124}{2} = 1562 \text{ and } \frac{1562}{2} = 781 \quad \text{implies } 3124 = 4 \times 781$$

Hence $3124 = 4 \times 781$. *Is 781 prime?*

No because if we use the divisibility test of 11 then

$$7-8+1=0 \text{ and } 11 \mid 0$$

Hence 11 is a factor of 781. We have $\frac{781}{11}=71$ and 71 is prime. Hence

$$781=11\times 71.$$

Therefore $3124=4\times 781=2^2\times 11\times 71$.

From (‡) and collecting all the factors together we have

$$5^{10}-1=3124\times 3126=\left(2^2\times 11\times 71\right)\times\left(2\times 3\times 521\right)=2^3\times 3\times 11\times 71\times 521.$$

The prime factorization of $5^{10}-1$ is $2^3\times 3\times 11\times 71\times 521$.

11. We need to factorize $10^5+1=100\,001$. Using the given hint with $n=5$ we have

$$10^5+1=\left(10+1\right)\times\left(10^4-10^3+10^2-10+1\right)=11\times 9091$$

Both these integers, 11 and 9091, are actually prime. We have

$$10^5+1=100\,001=11\times 9091$$

12. We can rewrite $1\,111\,111\,111=\frac{1}{9}\left(10^{10}-1\right)$.

First, we use the test for divisibility by 11 (question 32 of Exercises 3.1):

$$S=a_0-a_1+a_2-a_3+\cdots+\left(-1\right)^n a_n.$$

Putting the digits of 1111111111 into this formula gives

$$S=1-1+1-1+1-1+1-1+1-1=0.$$

Clearly $11 \mid 0$ so 11 is a factor of $\frac{1}{9}\left(10^{10}-1\right)=1\,111\,111\,111$.

Second we use the result of question 9:

$$\text{If } m \mid n \text{ then } \left(a^m-1\right) \mid \left(a^n-1\right).$$

With $a=10,\ n=10$ to factorize $10^{10}-1$. Since $5 \mid 10$ so $10^5-1=99\,999$ is a factor of $10^{10}-1$. Thus $\frac{99\,999}{9}=11\,111$ is a factor of $\frac{1}{9}\left(10^{10}-1\right)$.

Let us try to factorize this integer $11\,111$. This is time consuming but let us try our well-trodden path of trialling primes below $\left\lfloor \sqrt{11\,111} \right\rfloor = 105$. You will find that 41 is a factor of 11 111. Hence

$$\frac{11\,111}{41} = 271$$

Also 271 is prime. Our three factors of $\frac{1}{9}\left(10^{10}-1\right) = 1\,111\,111\,111$ are

$$11,\ 41 \text{ and } 271$$

The actual prime factorization is $11 \times 41 \times 271 \times 9091$.

13. We need to show that $\frac{1}{9}\left(10^{e}-1\right)$ where e is even is divisible by 11.

Proof.

Writing out the bracketed term we have

$$10^{e}-1 = \underbrace{999\cdots999}_{\text{even number of 9's}}$$

Dividing this by 9 yields

$$\frac{1}{9}\left(10^{e}-1\right) = \frac{1}{9}\left(\underbrace{999\cdots999}_{\text{even number of 9's}}\right) = \underbrace{111\cdots111}_{\text{even number of 1's}}$$

Using the test for divisibility by 11 which is given in question 32 of Exercises 3.1

$$S = a_0 - a_1 + a_2 - a_3 + \cdots + \left(-1\right)^{n} a_n \text{ where } a\text{'s are the digits.}$$

Thus applying this to $\frac{1}{9}\left(10^{e}-1\right) = 111\cdots111$ gives

$$S = \underbrace{1-1+1-1+\cdots+1-1}_{\text{even number of 1's in this}} = 0.$$

Clearly $11 \mid 0$ so $11 \mid \frac{1}{9}\left(10^{e}-1\right)$. This is our required result.

■

14. For this question $10^{2n}-1 \equiv 0 \pmod{99}$ we need to show that 99 is a factor of $10^{2n}-1$.

Proof.

We use the result of question 9; if $m \mid n$ then $\left(a^m - 1\right) \mid \left(a^n - 1\right)$.

Let $a = 10$ then clearly $2 \mid 2n$ therefore

$$\left(10^2 - 1\right) \mid \left(10^{2n} - 1\right).$$

$10^2 - 1 = 99$ so 99 is a factor of $10^{2n} - 1$. This implies $10^{2n} - 1 \equiv 0 \pmod{99}$ which is what we needed to show.

■

15. A pseudoprime to the base a is a composite integer n such that for a *particular* a we have

$$a^{n-1} \equiv 1 \pmod{n} \text{ where } \gcd(a, \quad n) = 1.$$

A Carmichael number is a composite integer n such that for *every* a we have

$$a^{n-1} \equiv 1 \pmod{n} \text{ where } \gcd(a, \quad n) = 1.$$

We also need to show that 4349 is a pseudoprime. This means we need to show two things; 4369 is composite and $a^{4368} \equiv 1 \pmod{4369}$ for some base a such that $\gcd(a, \quad 4369) = 1$.

Proof.

Well $4369 = 17 \times 257$ so 4369 is composite.

We will first try base $a = 2$ and try to show that

$$2^{4368} \equiv 1 \pmod{4369}$$

By computing some simple indices of 2 we have

$$2^4 \equiv 16 \pmod{4369}$$

$$2^8 \equiv 16 \times 16 \equiv 256 \pmod{4369}$$

$$2^{16} \equiv 256 \times 256 \equiv 65\,536 \equiv 1 \pmod{4369} \qquad (\dagger)$$

We can write the index 4368 as a multiple of 16 and any remainder:

$$4368 = 273 \times 16.$$

By using (†) we obtain

$$2^{4368} \equiv 2^{16 \times 273} \equiv \left(2^{16}\right)^{273} \equiv 1^{273} \equiv 1 \pmod{4369}$$

Thus $2^{4368} \equiv 1 \pmod{4369}$. Therefore 4369 is a pseudoprime.

16. We are asked to show that 1105 is a Carmichael number.

Proof.

We are required to show two things:

1) 1105 is a composite integer.

2) $a^{1104} \equiv 1 \pmod{1105}$ for every a such that $\gcd(a,\ 1105) = 1$.

Proof of 1):

Since $1105 = 5 \times 13 \times 17$ so 1105 is clearly composite.

Proof of 2):

We use the Chinese remainder theorem to show this part.

First using Fermat's Little Theorem (*FlT*) (4.1):

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

With moduli 5, 13 and 17 because $1105 = 5 \times 13 \times 17$ we have

$$a^4 \equiv 1 \pmod{5} \qquad [\text{FLT with } p = 5]$$
$$a^{12} \equiv 1 \pmod{13} \qquad [\text{FLT with } p = 13]$$
$$a^{16} \equiv 1 \pmod{17} \qquad [\text{FLT with } p = 17]$$

We use these indices to show $a^{1104} \equiv 1 \pmod{1105}$, so we are interested in the index 1104. Using the rules of indices and the above results we have

$$a^{1104} \equiv \left(a^4\right)^{276} \equiv 1^{276} \equiv 1 \pmod{5}$$

Similarly by using the rules of indices in the bottom two congruences we have

$$a^{1104} \equiv \left(a^{12}\right)^{92} \equiv 1^{92} \equiv 1 \pmod{13}$$
$$a^{1104} \equiv \left(a^{16}\right)^{69} \equiv 1^{69} \equiv 1 \pmod{17}$$

Let $x = a^{1104}$ and putting this into the above computed congruences we have the simultaneous congruence equations:

$$x \equiv 1 \pmod{5}$$
$$x \equiv 1 \pmod{13}$$
$$x \equiv 1 \pmod{17}$$

Solving these simultaneous equations using the Chinese remainder theorem result, question 8b of Exercises 3.4:

> If $x \equiv M \pmod{p_j}$ then $x \equiv M \pmod{p_1 \times p_2 \times \cdots \times p_k}$.

Applying this to the above simultaneous congruences gives

$$x \equiv 1 \left(\text{mod } 5 \times 13 \times 17\right) \equiv 1 \left(\text{mod } 1105\right).$$

Substituting $x = a^{1104}$ into this yields

$$a^{1104} \equiv 1 \left(\text{mod } 1105\right).$$

Hence we have shown part 2).

This means that for every a we have $a^{1104} \equiv 1 \left(\text{mod } 1105\right)$ provided $\gcd\left(a, \quad 1105\right) = 1$.

Therefore 1105 is a Carmichael number.

■

17. We need to prove $p^{q-1} + q^{p-1} \equiv 1 \left(\text{mod } pq\right)$ where p and q are distinct primes.

Proof.

We are given that p and q are distinct primes so $p \nmid q$ therefore by FLT we have

$$p^{q-1} \equiv 1 \left(\text{mod } q\right) \quad \text{and} \quad q^{p-1} \equiv 1 \left(\text{mod } p\right).$$

Rewriting these as divisors gives

$$q \mid \left(p^{q-1} - 1\right) \text{ and } p \mid \left(q^{p-1} - 1\right).$$

Applying the property of divisibility

$$a \mid b \text{ and } c \mid d \text{ implies } ac \mid bd$$

To $q \mid \left(p^{q-1} - 1\right)$ and $p \mid \left(q^{p-1} - 1\right)$ yields

$$qp \mid \left(p^{q-1} - 1\right)\left(q^{p-1} - 1\right)$$

Writing this result as a congruence:

$$\left(p^{q-1} - 1\right)\left(q^{p-1} - 1\right) \equiv 0 \left(\text{mod } pq\right)$$

$$\underbrace{p^{q-1}q^{p-1}}_{\substack{\equiv 0 \left(\text{mod } pq\right) \\ \text{because it is a multiple of } pq}} - p^{q-1} - q^{p-1} + 1 \equiv 0 \left(\text{mod } pq\right) \qquad \left[\text{Expanding}\right]$$

$$- p^{q-1} - q^{p-1} + 1 \equiv 0 \left(\text{mod } pq\right) \quad \Rightarrow \quad 1 \equiv p^{q-1} + q^{p-1} \left(\text{mod } pq\right)$$

This $1 \equiv p^{q-1} + q^{p-1} \left(\text{mod } pq\right)$ is our required result.

■

18. We need to prove that $p \mid \left(2^{p-1} - 1\right)$ where p is an odd prime.

Proof.

Since we are given that p is an odd prime so $p \not| 2$. We can use *FlT* (4.1):

$$a^{p-1} \equiv 1 \pmod{p} \text{ provided } p \not| a$$

By applying this with $a = 2$ gives

$$2^{p-1} \equiv 1 \pmod{p} \iff p \mid \left(2^{p-1} - 1\right).$$

This completes our proof.

■

19. (i) Substituting $n = p$ and $r = k$ into the given notation we have

$$ {}^{p}C_{k} = \frac{p!}{k!(p-k)!} = \frac{p \times (p-1) \times \cdots \times \left(p - [k-1]\right) \cancel{(p-k)!}}{k! \cancel{(p-k)!}}$$

$$= \frac{p \times (p-1) \times \cdots \times \left(p - [k-1]\right)}{k!} \qquad (*)$$

Note that

$$p - 1 \equiv -1 \pmod{p}, \quad p - 2 \equiv -2 \pmod{p}, \cdots, \quad p - (k-1) \equiv -(k-1) \pmod{p}$$

Therefore

$$p \times (p-1) \times \cdots \left(p - [k-1]\right) \equiv p \times (-1) \times (-2) \times \cdots \times \left[-(k-1)\right]$$

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

Applying Wilson's Theorem (4.4):

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

To the last line gives

$$p \times (p-1) \times \cdots \left(p - [k-1]\right) \equiv (-1)^{k-1} (k-1)!\, p$$

$$\equiv \left[(p-1)!\right]^{k-1} (k-1)!\, p \pmod{p}$$

Putting this into (*) yields

$$ {}^{p}C_{k} = \frac{p \times (p-1) \times \cdots \times \left(p - [k-1]\right)}{k!}$$

$$\equiv \frac{\left[(p-1)!\right]^{k-1} (k-1)!\, p}{k!}$$

$$\equiv \frac{\left[(p-1)!\right]^{k-1} p}{k} \pmod{p} \qquad \left[\text{Because } k! = k \times (k-1)!\right]$$

We are given $1 \le k < p$ so $(p-1)!$ must contain a factor of k. Hence

$$\frac{\left[(p-1)!\right]^{k-1}}{k} = m \text{ where } m \text{ is an integer.}$$

Therefore ${}^{p}C_{k} \equiv \frac{\left[(p-1)!\right]^{k-1} p}{k} \equiv mp \equiv 0 \pmod{p}$. This completes our proof.

■

(ii) In this part we need to show $(a+b)^{p} \equiv a^{p} + b^{p} \pmod{p}$.

Proof.

By the binomial expansion of $(a+b)^{p}$ we have

$$\begin{aligned}(a+b)^{p} &\equiv a^{p} + {}^{p}C_{1}a^{p-1}b + {}^{p}C_{2}a^{p-2}b^{2} + \cdots + {}^{p}C_{p-1}ab^{p-1} + b^{p} \\ &\equiv a^{p} + 0 + 0 + \cdots + 0 + b^{p} \qquad \left[\text{Because by part (i) } {}^{p}C_{k} \equiv 0 \pmod{p}\right] \\ &\equiv a^{p} + b^{p}\end{aligned}$$

This completes our proof.

■

(iii) We are asked to prove $(a_1 + a_2 + \cdots + a_n)^{p} \equiv a_1{}^{p} + a_2{}^{p} + \cdots + a_n{}^{p} \pmod{p}$.

How do we prove this result?

Use mathematical induction.

Proof.

For $n = 2$ we have our result by part (ii):

$$(a_1 + a_2)^{p} \equiv a_1{}^{p} + a_2{}^{p} \pmod{p}$$

Assume the result is true for $n = k$:

$$(a_1 + a_2 + \cdots + a_k)^{p} \equiv a_1{}^{p} + a_2{}^{p} + \cdots + a_k{}^{p} \pmod{p} \qquad (*)$$

Required to prove the given result for $n = k+1$:

$$(a_1 + a_2 + \cdots + a_k + a_{k+1})^{p} \equiv a_1{}^{p} + a_2{}^{p} + \cdots + a_k{}^{p} + (a_{k+1})^{p} \pmod{p}$$

Rewriting the left - hand side of this we have

$$\begin{aligned}(a_1 + a_2 + \cdots + a_k + a_{k+1})^{p} &\equiv \left(\left[a_1 + a_2 + \cdots + a_k\right] + a_{k+1}\right)^{p} \\ &\equiv \left[a_1 + a_2 + \cdots + a_k\right]^{p} + (a_{k+1})^{p} \\ &\equiv a_1{}^{p} + a_2{}^{p} + \cdots + a_k{}^{p} + (a_{k+1})^{p} \pmod{p} \qquad \left[\text{By } (*)\right]\end{aligned}$$

Hence by mathematical induction we have

$$(a_1 + a_2 + \cdots + a_n)^{p} \equiv a_1{}^{p} + a_2{}^{p} + \cdots + a_n{}^{p} \pmod{p}$$

This completes our proof.

■

20. This time we are asked to prove if $a \equiv b \pmod{p}$ where p is prime then

$$a^p \equiv b^p \pmod{p^2}$$

Proof.

We assume that $a \equiv b \pmod{p}$. We consider two cases; $p \mid a$ and $p \nmid a$.

Case I: $p \mid a$

If $p \mid a$ then $p^2 \mid a^2$ so $a^p \equiv 0 \pmod{p^2}$. Since we have $a \equiv b \equiv 0 \pmod{p}$ so $p \mid b$ and $p^2 \mid b^2$ so $b^p \equiv 0 \pmod{p^2}$. Therefore we have our required result

$$a^p \equiv b^p \equiv 0 \pmod{p^2}$$

Case II: $p \nmid a$

Assume $p \nmid a$. We are given that $a \equiv b \pmod{p}$ implies that $a^p \equiv b^p \pmod{p}$.

We can rewrite this as

$a^p - b^p \equiv 0 \pmod{p}$. Factorizing $a^p - b^p$ gives

$$a^p - b^p = (a-b)\left(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}\right) \qquad (*)$$

Since we are assuming $a \equiv b \pmod{p}$ so $a - b = kp$ where k is an integer.

Examining the second term on the right hand side:

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \qquad (\ddagger)$$

Required to prove that

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \equiv 0 \pmod{p}.$$

In this case $p \nmid a$ so by Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Because we have $a \equiv b \pmod{p}$ therefore

$$a^{p-2}b \equiv a^{p-1} \equiv 1, \ \cdots, \ ab^{p-2} \equiv a^{p-1} \equiv 1, \ b^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}.$$

Putting these results into (‡) gives

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \equiv \underbrace{(1+1+\cdots+1+1)}_{p \text{ copies of } 1} \equiv p \equiv 0 \pmod{p}.$$

By the definition of congruence we have

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} = mp$$

Substituting these results $a - b = kp$ and $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} = mp$ into (*) gives

$$a^p - b^p = \left(a-b\right)\left(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}\right) = kmp^2 .$$

Hence $a^p - b^p \equiv 0 \left(\text{mod } p^2\right)$ which implies $a^p \equiv b^p \left(\text{mod } p^2\right)$.

■

21. To disprove something, we only need a counter example:

Let $x = 3$ and $n = 4$ then

$$3^4 = 81 \equiv 1 \not\equiv 3 \left(\text{mod } 4\right).$$

22. We are required to prove that $x^n - 1 = \left(x^m - 1\right)P_{n-m}\left(x\right)$ where $m > 1$.

Proof.

We are given that n is a composite integer. So let $n = mr$ where $m > 1$ and this implies that $m \mid n$. By the result of question 9:

if $m \mid n$ then $\left(a^m - 1\right) \mid \left(a^n - 1\right)$

We have $\left(x^m - 1\right) \mid \left(x^n - 1\right)$. Hence

$$x^n - 1 = \left(x^m - 1\right)P\left(x\right).$$

Since the polynomial on the left-hand side is of degree n so the product of polynomials on the right-hand side must also be of degree n. By the rules of indices, we have $P\left(x\right)$ must be of degree $n - m$. Therefore $P\left(x\right) = P_{n-m}\left(x\right)$.

This completes our proof.

■

23. (i) *How do we prove* $a^{\frac{n-1}{2}} \not\equiv \pm 1 \left(\text{mod } n\right)$ *then* n *is composite?*

Contrapositive proof.

Proof.

Suppose n is prime. Then we need to prove that $a^{\frac{n-1}{2}} \equiv \pm 1 \left(\text{mod } n\right)$. Since n is prime and $n \nmid a$ so by Fermat's Little Theorem we have

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

Let $a^{\frac{n-1}{2}} = x$ then $x^2 \equiv 1 \left(\text{mod } n\right)$. By Lemma (4.3):

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

Remember our supposition is that n is prime so

$$x = a^{\frac{n-1}{2}} \equiv \pm 1 \left(\text{mod } n\right).$$

This completes our proof.

■

(ii) We need to give a reason why $12^{\frac{1729-1}{2}} \equiv 1 \left(\text{mod } 1729\right)$ but 1729 is composite.

Part (i) does *not* say that if $a^{\frac{n-1}{2}} \equiv \pm 1 \left(\text{mod } n\right)$ then n is composite. We have that if $a^{\frac{n-1}{2}} \equiv \pm 1 \left(\text{mod } n\right)$ then n may be composite or prime.

24. We need to prove that if $2^n - 1$ is composite then n is composite is false.

This suggests that we need to produce a counter example.

Well $2^{11} - 1 = 2047 = 23 \times 89$ is composite but 11 is prime.

25. We need to prove that $n \nmid \left(2^n - 1\right)$ for all $n \geq 2$.

Proof.

We use proof by induction.

Clearly $2 \nmid \left(2^2 - 1\right)$ so the result is true for $n = 2$.

Assume $k \nmid \left(2^k - 1\right)$. Consider $2^{k+1} - 1$, and rewriting this we have

$$2^{k+1} - 1 = 2\left(2^k\right) - 1 = 2\left(2^k - 1\right) + 1 \qquad (*)$$

Since $k > 2$ so $k \nmid 2$ and the induction hypothesis we have $k \nmid \left(2^k - 1\right)$.

Putting both of these together gives $k \nmid 2\left(2^k - 1\right)$. This implies for every integer m we have $2\left(2^k - 1\right) \neq km$ and so

$$2\left(2^k - 1\right) + 1 \neq km + 1 \neq \left(k + 1\right)m$$

From this last line we have $2\left(2^k - 1\right) + 1 \neq \left(k + 1\right)m$ for every integer m so

$$\left(k + 1\right) \nmid \left[2\left(2^k - 1\right) + 1\right].$$

By (*) we have $2\left(2^k - 1\right) + 1 = 2^{k+1} - 1$ therefore $\left(k + 1\right) \nmid \left[2^{k+1} - 1\right]$.

By mathematical induction we conclude that $n \nmid \left(2^n - 1\right)$.

■

26. We need to show that 220 and 284 are amicable.

The prime factorization of each number is given by

$$220 = 2^2 \times 5 \times 11 \quad \text{and} \quad 284 = 4 \times 71 = 2^2 \times 71$$

Using the property that σ is multiplicative we have

$$\begin{aligned}\sigma\left(220\right) &= \sigma\left(2^2 \times 5 \times 11\right) \\ &= \sigma\left(2^2\right) \times \sigma\left(5\right) \times \sigma\left(11\right)\end{aligned}$$

Using Proposition (4.35):

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

And $\sigma\left(p\right) = p + 1$ we have

$$\begin{aligned}\sigma\left(220\right) &= \sigma\left(2^2\right) \times \sigma\left(5\right) \times \sigma\left(11\right) \\ &= \left(\frac{2^3 - 1}{2 - 1}\right) \times 6 \times 12 = 7 \times 6 \times 12 = 504\end{aligned}$$

Recall the proper divisors of 220 does *not* include 220. Therefore, the sum of the proper divisors of 220 is $504 - 220 = 284$.

Similarly, we have

$$\begin{aligned}\sigma\left(284\right) &= \sigma\left(2^2 \times 71\right) \\ &= \sigma\left(2^2\right) \times \sigma\left(71\right) \\ &= 7 \times 72 = 504\end{aligned}$$

Again 284 is *not* a proper divisor of 284 so the sum of the proper divisors is equal to $504 - 284 = 220$.

Hence 220 and 284 are amicable numbers.

27. We are asked to prove $\left[\left(p-1\right)!\right]^{p^n} \equiv -1 \left(\text{mod } p\right)$ for an odd prime p.

Proof.

By Wilson's Theorem we have

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

Since we are given that p is odd so p^n is odd. *Why?*

Let $p = 2m + 1$ then by the binomial expansion:

(I.37) $$\left(a+b\right)^n = C_n a^n + C_{n-1} a^{n-1} b + C_{n-2} a^{n-2} b^2 + C_{n-3} a^{n-3} b^3 + \ldots + C_0 b^n$$

We have

$$p^n = \left(2m+1\right)^n = \underbrace{\left(2m\right)^n + C_{n-1}\left(2m\right)^{n-1} + \cdots + C_1\left(2m\right)}_{=2k} + 1 = 2k + 1$$

Therefore

$$\left[\left(p-1\right)!\right]^{p^n} \equiv \left(-1\right)^{p^n} \equiv \left(-1\right)^{\text{odd index}} \equiv -1 \left(\text{mod } p\right)$$

This completes our proof.

■

28. We have been asked to prove $\left(p-1\right)! \equiv \left(-1\right)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \left(\text{mod } p\right)$.

Proof.

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

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

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

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

This is our required result.

■

29. We need to prove that there are infinitely many pseudoprimes to the base a where $a > 1$.

Proof.

This is the proof given in the book by Hardy and Wright[1].

[1] Hardy and Wright: An Introduction to the Theory of Numbers Fifth edition page 72.

Let p be an odd prime such that $p \not| \, a\left(a^2-1\right)$. Let m be the integer given by

$$m = \frac{a^{2p}-1}{a^2-1} = \frac{\left(a^p-1\right)\left(a^p+1\right)}{\left(a-1\right)\left(a+1\right)} \qquad \left[\begin{matrix}\text{By difference}\\ \text{of two squares}\end{matrix}\right]$$
$$= \left(\frac{a^p-1}{a-1}\right)\times\left(\frac{a^p+1}{a+1}\right)$$

This integer m is composite. *Why?*

Because by applying the following algebraic identities:

$$x^n-1 = \left(x-1\right)\left(x^{n-1}+x^{n-2}+\cdots+x+1\right)$$
$$x^n+1 = \left(x+1\right)\left(x^{n-1}-x^{n-2}+\cdots-x+1\right) \text{ provided } n \text{ is odd.}$$

to $m = \left(\frac{a^p-1}{a-1}\right)\times\left(\frac{a^p+1}{a+1}\right)$ gives

$$m = \left(\frac{a^p-1}{a-1}\right)\times\left(\frac{a^p+1}{a+1}\right)$$
$$= \left[\frac{\cancel{\left(a-1\right)}\left(a^{n-1}+a^{n-2}+\cdots+a+1\right)}{\cancel{a-1}}\right]\times\left[\frac{\cancel{\left(a+1\right)}\left(a^{n-1}-a^{n-2}+\cdots-a+1\right)}{\cancel{a+1}}\right]$$
$$= \left(a^{n-1}+a^{n-2}+\cdots+a+1\right)\times\left(a^{n-1}-a^{n-2}+\cdots-a+1\right)$$

Both these factors $a^{n-1}+a^{n-2}+\cdots+a+1$ and $a^{n-1}-a^{n-2}+\cdots-a+1$ are greater than 2 (you can show this by induction).

Now if a is odd then a^p is also odd and similarly if a is even then a^p is also even. Therefore adding these implies that $2 \,\Big|\, \left(a^p+a\right)$.

By *FlT* (4.1) we have

$$p \,\Big|\, \left(a^{p-1}-1\right)$$

Since the prime p is odd so $p-1$ is even so we can write this as $p-1=2m$ where m is an integer. We can factorize $a^{p-1}-1=a^{2m}-1$ as

$$a^{p-1}-1 = a^{2m}-1 = \left(a^2-1\right)\left(a^{2(m-1)}+a^{2(m-2)}+\cdots+a^2+1\right)$$

Hence $\left(a^2-1\right) \,\Big|\, \left(a^{p-1}-1\right)$. We have $p \,\Big|\, \left(a^{p-1}-1\right)$ and $\left(a^2-1\right) \,\Big|\, \left(a^{p-1}-1\right)$ but we have chosen our prime such that $p \not| \, a\left(a^2-1\right)$ which implies $p \not| \, \left(a^2-1\right)$.

By question 3(a) of Exercises 2.1:

$$\text{If } p \not| \, x \text{ then } \gcd\left(p, \quad x\right) = 1\,.$$

Applying this to $p \not\mid \left(a^2-1\right)$ gives $\gcd\left(p,\ \ a^2-1\right)=1$. By question 12(i) of Exercises 1.3:

If $a \mid c,\ b \mid c$ and $\gcd\left(a,\ \ b\right)=1$ then $ab \mid c$.

Applying this to $p \mid \left(a^{p-1}-1\right)$ and $\left(a^2-1\right) \mid \left(a^{p-1}-1\right)$ yields

$$p\left(a^2-1\right) \mid \left(a^{p-1}-1\right).$$

Recall the integer m is given by

$$m=\frac{a^{2p}-1}{a^2-1}.$$

Re-arranging this we have

$$\begin{aligned} m-1 &= \frac{a^{2p}-1}{a^2-1}-1 \\ &= \frac{a^{2p}-1-a^2+1}{a^2-1}=\frac{a^{2p}-a^2}{a^2-1} \qquad (\dagger) \end{aligned}$$

From this we deduce that

$$\left(m-1\right)\left(a^2-1\right)=a^{2p}-a^2=a\left(a^{2p-1}-a\right)=a\left(a^{p-1}-1\right)\left(a^p+a\right). \qquad (*)$$

Recall that a^p+a is even and from above we have $p\left(a^2-1\right) \mid \left(a^{p-1}-1\right)$

therefore from (*) we obtain

$2p\left(a^2-1\right) \mid \left(m-1\right)\left(a^2-1\right)$ which implies $2p\left(a^2-1\right)\ell=\left(m-1\right)\left(a^2-1\right)$

for some integer ℓ. Since $a>1$ so $a^2-1\neq 0$ and we can cancel this out to give

$$2p\ell=\left(m-1\right) \text{ which implies } m=2p\ell+1.$$

By the two expanding the left – hand side of (*) we have

$$\left(m-1\right)\left(a^2-1\right)=m\left(a^2-1\right)-a^2+1=a^{2p}-a^2 \quad \left[\text{By } (\dagger)\right]$$

Adding a^2 to both sides of this yields

$$a^{2p}=m\left(a^2-1\right)+1\equiv 1\left(\text{mod } m\right) \qquad (**)$$

Recall that $m=2p\ell+1$ so $m-1=2p\ell$ which gives

$$a^{m-1}\equiv a^{2p\ell}=\left(a^{2p}\right)^{\ell}\equiv 1^{\ell}\equiv 1\left(\text{mod } m\right)$$

Hence we have $a^{m-1}\equiv 1\left(\text{mod } m\right)$ and m is composite so it is a base a pseudoprime.

Since there are infinitely many odd primes p such that

$$m=\frac{a^{2p}-1}{a^2-1} \text{ and } p \not\mid a\left(a^2-1\right)$$

so there are infinitely many base a pseudoprimes.

■

30. We are asked to proof that

$$\tau\left(p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_r^{k_r}\right)=\left(k_1+1\right)\times\left(k_2+1\right)\times\cdots\times\left(k_r+1\right)$$

How do we prove this result?

By mathematical induction.

Proof.

For base case $r=1$ we need to show that $\tau\left(p_1^{k_1}\right)=\left(k_1+1\right)$. The divisors of $p_1^{k_1}$ are $1,\ p_1,\ p_1^2,\ \cdots,\ p_1^{k_1}$ so the number of divisors is k_1+1.

Assume the result is true for $r=s$:

$$\tau\left(p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_s^{k_s}\right)=\left(k_1+1\right)\times\left(k_2+1\right)\times\cdots\times\left(k_s+1\right)\qquad(\dagger)$$

Required to prove the result for $r=s+1$:

$$\tau\left(p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_s^{k_s}\times p_{s+1}^{k_{s+1}}\right)=\left(k_1+1\right)\times\left(k_2+1\right)\times\cdots\times\left(k_s+1\right)\times\left(k_{s+1}+1\right)$$

Assuming the hint that the $\tau\left(n\right)$ is multiplicative we have

$$\begin{aligned}\tau\left(p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_s^{k_s}\times p_{s+1}^{k_{s+1}}\right)&=\tau\left(p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_s^{k_s}\right)\times\tau\left(p_{s+1}^{k_{s+1}}\right)\\&=\underbrace{\left(k_1+1\right)\times\left(k_2+1\right)\times\cdots\times\left(k_s+1\right)}_{\text{by }(\dagger)}\times\left(k_{s+1}+1\right)\end{aligned}$$

Hence by mathematical induction we have our result.

■

31. We are asked to prove $x^{(5\times29\times73)-1}\equiv1\left(\mathrm{mod}\left(5\times29\times73\right)\right)$.

Proof.

We are given $\gcd\left(x,\ \ 5\right)=\gcd\left(x,\ \ 29\right)=\gcd\left(x,\ \ 73\right)=1$ so by *FLT* because 5, 29 and 73 are all prime:

$$x^4\equiv1\left(\mathrm{mod}\ 5\right)$$

$$x^{28}\equiv1\left(\mathrm{mod}\ 29\right)$$

$$x^{72}\equiv1\left(\mathrm{mod}\ 73\right)$$

Applying the rules of indices gives

$$\left(x^4\right)^{29\times73}\equiv\left(1\right)^{29\times73}\equiv1\left(\mathrm{mod}\ 5\right)$$

$$\left(x^{28}\right)^{5\times73}\equiv\left(1\right)^{5\times73}\equiv1\left(\mathrm{mod}\ 29\right)$$

$$\left(x^{72}\right)^{5\times 29} \equiv \left(1\right)^{5\times 29} \equiv 1\left(\text{mod } 73\right)$$

Multiplying each of these congruences by x yields

$$x^{5\times 29\times 73} \equiv x\left(\text{mod } 5\right)$$
$$x^{5\times 29\times 73} \equiv x\left(\text{mod } 29\right)$$
$$x^{5\times 29\times 73} \equiv x\left(\text{mod } 73\right)$$

Applying the result of question 8(b) of Exercises 3.4

> If $x \equiv M\left(\text{mod } p_j\right)$ then $x \equiv M\left(\text{mod } p_1 \times p_2 \times p_3 \times \cdots \times p_k\right)$.

To the above congruences gives

$$x^{5\times 29\times 73} \equiv x\left(\text{mod } 5\times 29\times 73\right) \qquad (*)$$

Recall we are given $\gcd\left(x,\ \ 5\right) = \gcd\left(x,\ \ 29\right) = \gcd\left(x,\ \ 73\right) = 1$ therefore $x^{-1}\left(\text{mod } 5\times 29\times 73\right)$ exists and multiplying (*) by this inverse we have

$$x^{5\times 29\times 73}x^{-1} \equiv x^{5\times 29\times 73-1} \equiv xx^{-1} \equiv 1\left(\text{mod } 5\times 29\times 73\right)$$

Hence, we have our result $x^{(5\times 29\times 73)-1} \equiv 1\left(\text{mod } \left(5\times 29\times 73\right)\right)$.

■

32. We need to prove $2^2 4^2 6^2 \cdots \left(p-1\right)^2 \equiv \left(-1\right)^{\frac{p+1}{2}} \left(\text{mod } p\right)$.

Proof.

Rewriting the given congruence $2^2 4^2 6^2 \cdots \left(p-1\right)^2 = \left[2\times 4\times 6\times \cdots \times \left(p-1\right)\right]^2$:

$$\begin{aligned}
\left[2\times 4\times 6\times \cdots \times \left(p-1\right)\right]^2 &= \left[2\times 4\times \cdots \times \left(\frac{p-3}{2}\right)\times \left(\frac{p+1}{2}\right)\times \left(\frac{p+5}{2}\right)\times \cdots \times \left(p-3\right)\times \left(p-1\right)\right]^2 \\
&= \left[2\times 4\times \cdots \times \left(\frac{p-3}{2}\right)\times \left(p-\frac{p-1}{2}\right)\times \left(p-\frac{p-5}{2}\right)\times \cdots \times \left(p-3\right)\times \left(p-1\right)\right]^2 \\
&= \left[2\times 4\times \cdots \times \left(\frac{p-3}{2}\right)\times \left(-\frac{p-1}{2}\right)\times \left(-\frac{p-5}{2}\right)\times \cdots \times \left(-3\right)\times \left(-1\right)\right]^2 \\
&= \left[2\times 4\times \cdots \times \left(\frac{p-3}{2}\right)\times \left(-1\right)\left(\frac{p-1}{2}\right)\times \left(-1\right)\left(\frac{p-5}{2}\right)\times \cdots \times \left(-3\right)\times \left(-1\right)\left(1\right)\right]^2 \\
&= \left[2\times 4\times \cdots \times \left(\frac{p-3}{2}\right)\times \left(\frac{p-1}{2}\right)\times \left(\frac{p-5}{2}\right)\times \cdots \times 3\times \left(1\right)\right]^2 \left[\left(-1\right)\times \cdots \times \left(-1\right)\right]^2 \\
&= \left[2\times 4\times \cdots \times \left(\frac{p-3}{2}\right)\times \left(\frac{p-1}{2}\right)\times \left(\frac{p-5}{2}\right)\times \cdots \times \left(1\right)\right]^2 \qquad (*)
\end{aligned}$$

All this is equal to $\left[\left(\frac{p-1}{2}\right)!\right]^2$. *Why?*

Because

$$\left(\frac{p-1}{2}\right)! = \left(\frac{p-1}{2}\right)\times\left(\frac{p-1}{2}-1\right)\times\left(\frac{p-1}{2}-2\right)\times\left(\frac{p-1}{2}-3\right)\times\cdots\times 3\times 2\times 1$$
$$= \left(\frac{p-1}{2}\right)\times\left(\frac{p-3}{2}\right)\times\left(\frac{p-5}{2}\right)\times\left(\frac{p-7}{2}\right)\times\cdots\times 3\times 2\times 1$$

Therefore we have

$$\left[2\times 4\times 6\times\cdots\times(p-1)\right]^2 = \left[\left(\frac{p-1}{2}\right)!\right]^2$$

From the result of question 28 we have

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

By Wilson's Theorem we have

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

Equating these last two equations gives

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

Multiplying both sides of this by $(-1)^{\frac{p-1}{2}}$ yields

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

We have

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

Putting this into (*) yields

$$2^2 4^2 6^2 \cdots (p-1)^2 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

This completes our proof.

■