Complete Solutions to Exercises 4.3

1. For parts (a) and (b) we use Proposition (4.6):

$$2^{n-1} \not\equiv 1 \pmod{n} \text{ implies } n \text{ is composite.}$$

(a) We need to show 4097 is a composite number. This means we are required to show that $2^{4096} \not\equiv 1 \pmod{4097}$. Evaluating powers of 2:

$$2^6 \equiv 64,\ 2^7 \equiv 128,\ 2^8 \equiv 256,\ 2^9 \equiv 512,\ 2^{10} \equiv 1024,\ 2^{11} \equiv 2048,\ 2^{12} \equiv 4096 \equiv -1 \pmod{4097}$$

We use the last result $2^{12} \equiv -1 \pmod{4097}$ to find $2^{4096} \equiv ? \pmod{4097}$.

By the division algorithm we have

$$4096 = (12 \times 341) + 4$$

Using the rules of indices gives

$$\begin{aligned} 2^{4096} \equiv 2^{(12\times 341)+4} &\equiv \left(2^{12}\right)^{341} \times 2^4 \\ &\equiv (-1)^{341} \times 16 \equiv -1 \times 16 \equiv -16 \pmod{4097} \end{aligned}$$

Since $2^{4096} \equiv -16 \not\equiv 1 \pmod{4097}$ so by Proposition (4.6) we conclude that 4097 is a composite integer.

(b) We need to show that 32 767 is a composite integer. Using Proposition (4.6) means we need to deduce the following:

$$2^{32\,766} \not\equiv 1 \pmod{32\,767}$$

From part (a) we have $2^{12} \equiv 4096 \pmod{32\,767}$. Evaluating further powers gives

$$2^{13} \equiv 8192,\ 2^{14} \equiv 16\,384,\ 2^{15} \equiv 32\,768 \equiv 1 \pmod{32\,767}$$

We want to use the last result $2^{15} \equiv 1 \pmod{32767}$ in order to compute

$$2^{32766} \equiv ? \pmod{32767}.$$

Applying the division algorithm to 32 766 and 15 we have

$$32\,766 = (2184 \times 15) + 6\,.$$

Now we apply the rules of indices to find $2^{32766} \equiv ? \pmod{32\,767}$:

$$2^{32\,766} \equiv 2^{(2184\times 15)+6} \equiv \left(2^{15}\right)^{2184} \times 2^6 \equiv 1 \times 64 \equiv 64 \not\equiv 1 \pmod{32\,767}$$

Since $2^{32766} \not\equiv 1 \pmod{32767}$ so by Proposition (4.6) we conclude that 32767 is composite.

(c) We want to show that 2197 is composite by using base 13:

$$13^2 \equiv 169 \left(\text{mod } 2197\right) \text{ and } 13^3 \equiv 2197 \equiv 0 \left(\text{mod } 2197\right)$$

Using this $13^3 \equiv 0 \left(\text{mod } 2197\right)$ means that 13^3 is a factor of 2197 or $13^3 \mid 2197$ so 2197 is a composite integer. (Actually $13^3 = 2197$).

2. We need to show 2047 is a composite number and $2^{2046} \equiv 1 \left(\text{mod } 2047\right)$.

Using Corollary (2.10) of chapter 2:

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

The integer 2047 is composite if we can find a prime divisor p such that

$$p \le \left\lfloor \sqrt{2047} \right\rfloor = 45 .$$

We need to test the primes below 45 which are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 and 43. Clearly 2, 3 and 5 are not divisors of 2047. Working through the rest we find that 23 is a proper divisor of 2047 because

$$\frac{2047}{23} = 89 \quad \Rightarrow \quad 2047 = 23 \times 89 .$$

Hence 2047 is composite. In order for 2047 to be a pseudoprime we also need to show

$$2^{2046} \equiv 1 \left(\text{mod } 2047\right).$$

Evaluating powers of 2:

$$2^6 \equiv 64, \; 2^7 \equiv 128, \; 2^8 \equiv 256, \; 2^9 \equiv 512, \; 2^{10} \equiv 1024, \; 2^{11} \equiv 2048 \equiv 1 \left(\text{mod } 2047\right)$$

We use the last result $2^{11} \equiv 1 \left(\text{mod } 2047\right)$ to find $2^{2046} \equiv ? \left(\text{mod } 2047\right)$. By the division algorithm we have

$$2046 = 11 \times 186 .$$

Using the rules of indices gives

$$2^{2046} \equiv 2^{11 \times 186} \equiv \left(2^{11}\right)^{86} \equiv 1^{86} \equiv 1 \left(\text{mod } 2047\right)$$

Hence 2047 is a base 2 - pseudoprime.

3. (a) (I) Again we need to show two things:

i) 561 is a composite integer. ii) $560^{560} \equiv 1 \left(\text{mod } 561\right)$.

Showing each of these:

i) Adding the digits of 561 gives $5 + 6 + 1 = 12$ and $3 \mid 12$ so 3 is a divisor of 561.

This implies that 561 is a composite integer.

ii) We need to show that

$$560^{560} \equiv 1 \left(\text{mod } 561\right)$$

First note that $560 \equiv -1 \left(\text{mod } 561\right)$. Then using Proposition (3.8):

> If $a \equiv b \left(\text{mod } n\right)$ then $a^k \equiv b^k \left(\text{mod } n\right)$ where k is a natural number.

We have

$$560^{560} \equiv \left(-1\right)^{560} \equiv 1 \left(\text{mod } 561\right)$$

Hence 561 is a base 560 – pseudoprime.

(II) Similarly we need to show

$$562^{560} \equiv 1 \left(\text{mod } 561\right)$$

(We already know that 561 is composite by part (a).)

Observe that $562 \equiv 1 \left(\text{mod } 561\right)$ so

$$562^{560} \equiv 1^{560} \equiv 1 \left(\text{mod } 561\right)$$

Hence 561 is a base 562 – pseudoprime.

(b) To prove that 91 is *not* a base 2 pseudoprime we have to show that 91 is composite and $2^{90} \not\equiv 1 \left(\text{mod } 91\right)$.

Clearly 91 is composite because $91 = 7 \times 13$. We need to show that

$$2^{90} \not\equiv 1 \left(\text{mod } 91\right)$$

Evaluating powers of 2 gives

$$2^{10} \equiv 1012 \equiv 23, \;\; 2^{11} \equiv 2 \times 23 \equiv 46, \;\; 2^{12} \equiv 2 \times 46 \equiv 92 \equiv 1 \left(\text{mod } 91\right)$$

Using the last result $2^{12} \equiv 1 \left(\text{mod } 91\right)$ and writing the index 90 as a multiple of 12 and any remainder by the division algorithm gives

$$2^{90} \equiv 2^{(7 \times 12)+6} \equiv \left(2^{12}\right)^7 \times 2^6 \equiv 2^6 \equiv 64 \not\equiv 1 \left(\text{mod } 91\right)$$

Since 91 is composite and $2^{90} \equiv 64 \not\equiv 1 \left(\text{mod } 91\right)$ so 91 is *not* a base 2 – pseudoprime.

4. We use Proposition (4.9) for this question:

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

(a) We need to show that $2^{123} - 1$ is composite. The integer 123 is composite because adding the digits gives $1 + 2 + 3 = 6$ and $3 \mid 6$ so 3 is a divisor of 123. By Proposition (4.9) with $3 \mid 123$ we have

$$\left(2^3-1\right) \mid \left(2^{123}-1\right)$$

Since $2^3-1=7$ is a factor of $2^{123}-1$ so $2^{123}-1$ is a composite integer.

(b) We are required to show that $2^{161051}-1$ is a composite integer. We only need to show that 161051 is a composite integer and then by the above proposition we have $2^{161051}-1$ is composite.

Adding the digits of 161051 gives

$$1+6+1+0+5+1=14$$

So 3 *cannot* be a divisor of 161051. Let us check to see if 11 divides into this number. *How?*

By question 32 of Exercises 3.1:

> Let $N=a_n a_{n-1}a_{n-2}\cdots a_2 a_1 a_0$ and $T=a_0-a_1+a_2-a_3+\cdots+\left(-1\right)^n a_n$. Then
>
> $$11 \text{ divides } N \Leftrightarrow 11 \text{ divides } T.$$

Applying this to 161051 gives

$$1-5+0-1+6-1=0 \text{ and } 11 \mid 0$$

Therefore $11 \mid 161051$. By Proposition (4.9) we have

$$\left(2^{11}-1\right) \mid \left(2^{161051}-1\right)$$

Since $2^{11}-1=2047$ is a factor of $2^{161051}-1$ so it is a composite integer.

(c) To show $2^{1769}-1$ we just need to show 1769 is composite. Checking for divisibility by 3 and 11:

$$1+7+6+9=23 \text{ and } 3 \nmid 23$$

$$9-6+7-1=9 \text{ and } 11 \nmid 9$$

Hence 1769 is *not* divisible by 3 or 11. We need to use something else.

We can use the factorization by difference of two squares as discussed in section 3E of chapter 3. For this we need to evaluate the ceiling function of the square root of 1769:

$$\left\lceil \sqrt{1769} \right\rceil = 43$$

Now $43^2-1769=80$ and 80 is *not* a square number. We trial the next integer until we get a square number:

$$44^2-1769=167 \text{ [Not Square]}$$

$$45^2-1769=256=16^2$$

Re-arranging this last result and using the difference of two squares gives

$$1769=45^2-16^2=\left(45-16\right)\times\left(45+16\right)=29\times 61$$

By Proposition (4.9) we have

$$\left(2^{29}-1\right) \mid \left(2^{1769}-1\right) \text{ because } 29 \mid 1769$$

Since $2^{29}-1$ is a factor of $2^{1769}-1$ so it is a composite integer.

5. (a) We need to find the prime factors of $2^{20}-1$. The non-trivial factors of 20 are 2, 4, 5 and 10. We use Proposition (4.9):

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

From this we have $2^2-1=3$, $2^4-1=15$, $2^5-1=31$ and $2^{10}-1=1023$ are factors of $2^{20}-1$. However we want to find the prime factors of this number. We know 31 is prime and $15=3\times5$ are factors of $2^{20}-1$:

$$\frac{2^{20}-1}{3\times5\times31}=2255$$

Clearly 5 is factor of 2255 so

$$\frac{2255}{5}=451 \quad \text{implies} \quad 2255=5\times451$$

By using the test for divisibility by 11 on 451 we have:

$$1-5+4=0 \text{ and } 11 \mid 0$$

Therefore 11 is a factor of 451 and $\frac{451}{11}=41$. Also 41 is prime, so we have $451=41\times11$.

Collecting *all* these factors together we have

$$3\times5\times5\times11\times31\times41=3\times5^2\times11\times31\times41=2^{20}-1$$

(b) We need to find the prime factors of $2^{21}-1$. The non-trivial factors of 21 are 3 and 7. Again we use Proposition (4.9):

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

We have $2^3-1=7$ and $2^7-1=127$ are factors of $2^{21}-1$. Both these numbers 7 and 127 are prime so these are prime factors of $2^{21}-1$:

$$\frac{2^{21}-1}{7\times127}=2359 \quad \text{implies} \quad 2^{21}-1=7\times127\times2359 \qquad (*)$$

We need to check whether 2359 is composite or prime. *How?*

By using Corollary (2.10):

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

2359 is composite if we can find a prime divisor p such that

$$p \le \left\lfloor \sqrt{2359} \right\rfloor = 48$$

We need to test the primes below 48 which are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 and 47. Clearly 2, 3 and 5 are not divisors of 2359. We find the next prime 7 is actually a divisor of 2359 because

$$\frac{2359}{7} = 337 \quad \text{implies} \quad 2359 = 7 \times 337 .$$

We now test to see if 337 is prime. Again using Corollary (2.10) we examine the primes below $\left\lfloor \sqrt{337} \right\rfloor = 18$. None of the primes below 18 go into 337 therefore by Corollary (2.10) we conclude that 337 is prime.

Substituting this $2359 = 7 \times 337$ into (*) gives

$$2^{21} - 1 = 7 \times 127 \times \left(7 \times 337\right) = 7^2 \times 127 \times 337$$

(c) We need to find the prime factors of $2^{24} - 1$. The non – trivial factors of index 24 are

2, 3, 4, 6, 8 and 12.

By Proposition (4.9) we have

$$2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^4 - 1 = 15,\ 2^6 - 1 = 63,$$
$$2^8 - 1 = 255 \text{ and } 2^{12} - 1 = 4095 \qquad (*)$$

These integers are factors of $2^{24} - 1$. Let us examine the largest factor in this list (*), which is 4095. Clearly 5 and 9 are factors of this because

$$\frac{4095}{5 \times 9} = 91 .$$

Also $91 = 7 \times 13$. Collecting the factors of 4095 we have

$$4095 = 5 \times 9 \times 91 = 3^2 \times 5 \times 7 \times 13 .$$

Some of the prime factors of $2^{24} - 1$ are 3, 5, 7 and 13.

The second largest factor in the above list (*) is 255. Clearly 5 is a factor:

$$\frac{255}{5} = 51 \text{ and } 51 = 3 \times 17$$

This means that 17 is a new prime factor of $2^{24} - 1$.

Hence $\dfrac{2^{24} - 1}{3^2 \times 5 \times 7 \times 13 \times 17} = 241$. We need to check that 241 is prime.

Using Corollary (2.10):

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

The integer 241 is composite if we can find a prime divisor p such that

$$p \le \left\lfloor \sqrt{241} \right\rfloor = 15$$

We need to test the primes below 15 which are 2, 3, 5, 7, 11 and 13. Testing each of these shows that none of these go into 241 so 241 is prime.

The prime factors of $2^{24}-1$ are

$$3^2 \times 5 \times 7 \times 13 \times 17 \times 241 = 2^{24}-1$$

6. We are asked to show what is wrong with

$$10^{5-1} \equiv 0 \not\equiv 1 \pmod 5 \text{ implies 5 is composite.}$$

Fermat's composite test (4.6):

> $$a^{n-1} \not\equiv 1 \pmod n \text{ for some } a \text{ such that } n \nmid a$$
>
> Then n is a *composite integer*.

In our case we have $5 \mid 10$ this is why we cannot use this composite test.

7. *Proof.*

The index $2 \times n$ has a factor of 2 because $2 \mid (2 \times n)$. By using Proposition (4.9):

> If $x \mid y$ then $(2^x - 1) \mid (2^y - 1)$.

With $x = 2$ and $y = 2 \times n$ we have

$$(2^2 - 1) \mid (2^{2 \times n} - 1)$$

Now $2^2 - 1 = 3$ so 3 is a factor of $2^{2n} - 1$. This completes our proof.

■

8. Very similar to previous solution.

Proof.

The index $3 \times n$ has a factor of 3 because $3 \mid (3 \times n)$. By using Proposition (4.9):

> If $x \mid y$ then $(2^x - 1) \mid (2^y - 1)$.

with $x = 3$ and $y = 3 \times n$ we have

$$(2^3 - 1) \mid (2^{3 \times n} - 1).$$

Now $2^3 - 1 = 7$ so 7 is a factor of $2^{3 \times n} - 1$.

■

9. We are asked to show that 2047 is a factor of $2^{3751} - 1$.

Proof.

The index 3751 is not divisible by 3 because $3+7+5+1=16$ and $3 \not| 16$. Using the test for divisibility by 11 we have

$$1-5+7-3=0 \text{ and } 11 \mid 0$$

Hence 11 is a factor of 3751. Since we have $11 \mid 3751$ so by Proposition (4.9):

> If $x \mid y$ then $\left(2^x-1\right) \mid \left(2^y-1\right)$.

We have $\left(2^{11}-1\right) \mid \left(2^{3751}-1\right)$. Now $2^{11}-1=2047$ so 2047 is a factor of $2^{3751}-1$.

■

10. We are asked to prove that if n is composite then 2^n-1 is also composite.

Proof.

Let n be composite and have a factor r say, where $1<r<n$. By the definition of factor we have $r \mid n$. By Proposition (4.9):

> If $x \mid y$ then $\left(2^x-1\right) \mid \left(2^y-1\right)$.

With $x=r$ and $y=n$ we have

$$\left(2^r-1\right) \mid \left(2^n-1\right)$$

Hence $2^r-1>1$ where $r>1$ is a factor of 2^n-1, so 2^n-1 is a composite integer.

■

11. We need to prove 'If n is a base 2 - pseudoprime then 2^n-1 is also a base 2 - pseudoprime.'

Proof.

We need to prove two things:

1) 2^n-1 is composite

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

Proof of 1).

We are given that n is a pseudoprime so n is composite. By Corollary (4.11):

> If n is composite then 2^n-1 is also composite.

We have 2^n-1 is composite.

Proof of part 2).

We need to show $2^{2^n-2} \equiv 1 \left(\text{mod } 2^n-1\right)$ for this part. Since we are given that n is a base 2 - pseudoprime so by the definition of pseudoprime (4.8):

A composite integer is called a base a - pseudoprime or just a pseudoprime if

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

Because n is a base 2 pseudoprime so $2^{n-1} \equiv 1 \pmod{n}$. Multiplying this by 2 gives

$$2 \times 2^{n-1} \equiv 2^n \equiv 2 \pmod{n} \text{ implies } \quad 2^n - 2 \equiv 0 \pmod{n}$$

By the definition of congruence we have for some integer k:

$$2^n - 2 = k \times n \qquad (*)$$

Examining the congruence, we are interested in $2^{2^n-2} \equiv x \pmod{2^n - 1}$. We need to show that $x = 1$. By (*) the index $2^n - 2 = k \times n$ therefore

$$2^{2^n-2} \equiv 2^{k \times n} \pmod{2^n - 1} \qquad (\dagger)$$

Also $2^n - 1 \equiv 0 \pmod{2^n - 1}$ which implies $2^n \equiv 1 \pmod{2^n - 1}$. We have

$$2^{2^n-2} \underbrace{\equiv}_{\text{by } (\dagger)} 2^{kn} \underbrace{\equiv}_{\text{by rules of indices}} \left(2^n\right)^k \equiv 1^k \equiv 1 \pmod{2^n - 1}$$

We have shown that $2^{2^n-2} \equiv 1 \pmod{2^n - 1}$.

Since we have proved both parts so $2^n - 1$ is a base 2 - pseudoprime. This competes our proof.

■

12. *Proof.*

We are required to show two things:

1) 1729 is a composite integer.

2) $a^{1728} \equiv 1 \pmod{1729}$ for every a such that $\gcd(a, \quad 1729) = 1$.

Proof of 1):

Since $1729 = 7 \times 13 \times 19$ so 1729 is clearly composite.

(Note that for any multiple of 7, 13 and 19 and combination of these multiples will *not* give 1 modulo 1729. For example

$$7^{1728} \equiv 742 \not\equiv 1 \pmod{1729}, \ (7 \times 13)^{1728} \equiv 1274 \not\equiv 1 \pmod{1729}, \ \ldots \ )$$

Proof of 2):

First using Fermat's Little Theorem (4.1):

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

With prime moduli 7, 13 and 19 because $1729 = 7 \times 13 \times 19$ we have:

$$a^6 \equiv 1 \left(\text{mod } 7\right)$$
$$a^{12} \equiv 1 \left(\text{mod } 13\right)$$
$$a^{18} \equiv 1 \left(\text{mod } 19\right)$$

However we don't need these indices because we want to show $a^{1728} \equiv 1 \left(\text{mod } 1729\right)$, so we are interested in index 1728. Using the rules of indices in the above we have

$$a^{1728} \equiv \left(a^6\right)^{288} \equiv 1^{288} \equiv 1 \left(\text{mod } 7\right)$$

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

$$a^{1728} \equiv \left(a^{12}\right)^{144} \equiv 1^{144} \equiv 1 \left(\text{mod } 13\right)$$
$$a^{1728} \equiv \left(a^{18}\right)^{96} \equiv 1^{96} \equiv 1 \left(\text{mod } 19\right)$$

Let $x = a^{1728}$ and putting this into the above computed congruences we have the simultaneous congruence equations

$$x \equiv 1 \left(\text{mod } 7\right)$$
$$x \equiv 1 \left(\text{mod } 13\right)$$
$$x \equiv 1 \left(\text{mod } 19\right)$$

Solving these simultaneous equations by applying the result of question 8(b) of Exercises 3(d):

> 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 these simultaneous equation gives

$$x \equiv 1 \left(\text{mod } 7 \times 13 \times 19\right) \equiv 1 \left(\text{mod } 1729\right).$$

Substituting $x = a^{1728}$ into this yields

$$a^{1728} \equiv 1 \left(\text{mod } 1729\right)$$

Hence we have shown part 2).

This means that for every base a we have $a^{1728} \equiv 1 \left(\text{mod } 1729\right)$ provided $\gcd\left(a, \quad 1729\right) = 1$.

Therefore 1729 is a Carmichael number.

■

13. We are required to prove that if $2^n - 1$ is prime then n is prime.

Proof.

We use the contrapositive form of Corollary (4.11):

If n is composite then $2^n - 1$ is also composite.

Since this says

$$n \text{ is composite } \Rightarrow 2^n - 1 \text{ is composite}$$

So the contrapositive form is

$$2^n - 1 \text{ is not composite } \Rightarrow n \text{ is not composite}$$

An integer can only be composite or prime, so not composite means that it is prime. Therefore we have

$$2^n - 1 \text{ is prime } \Rightarrow n \text{ is prime}$$

■

14. We are asked to prove that if $2^p - 1$ is composite where p is prime then it is a base 2 - pseudoprime.

Proof.

We need to show two things:

(i) $2^p - 1$ is composite (ii) $2^{2^p-1-1} \equiv 2^{2^p-2} \equiv 1 \left(\text{mod } 2^p - 1\right)$

Part (i).

We are given that $2^p - 1$ is composite.

Part (ii).

In order for $2^p - 1$ to be a base 2 - pseudoprime we need to show

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

Since p is prime we can use Fermat's Little Theorem (4.1):

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

$2^{p-1} \equiv 1 \left(\text{mod } p\right)$. Multiplying this by 2 gives

$$2^p \equiv 2 \left(\text{mod } p\right).$$

By the definition of congruence, we have for some integer k:

$$2^p - 2 = k \times p \qquad (*)$$

Examining the congruence we are interested in $2^{2^p-2} \equiv x \left(\text{mod } 2^p - 1\right)$. We need to show that $x = 1$. By (*) the index $2^p - 2 = k \times p$ therefore

$$2^{2^p-2} \equiv 2^{k \times p} \left(\text{mod } 2^p - 1\right) \qquad (\dagger)$$

Also $2^p - 1 \equiv 0 \left(\text{mod } 2^p - 1\right)$ which implies $2^p \equiv 1 \left(\text{mod } 2^p - 1\right)$. We have

$$2^{2^p-2} \underbrace{\equiv}_{\text{by } (\dagger)} 2^{k\times p} \underbrace{\equiv}_{\text{by rules of indices}} \left(2^p\right)^k \equiv 1^k \equiv 1 \left(\text{mod } 2^p-1\right).$$

We have shown that $2^{2^p-2} \equiv 1 \left(\text{mod } 2^p-1\right)$.

Since we have proved both parts so 2^p-1 is a base 2 - pseudoprime. This completes our proof.

■

15. We are asked to prove that $\left(2^m-1\right) \mid \left(2^n-1\right) \Rightarrow m \mid n$.

How are we going to prove this?

By contradiction.

Proof.

We are given that $\left(2^m-1\right) \mid \left(2^n-1\right)$ therefore by the definition of congruence we have

$$2^n-1 \equiv 0 \left(\text{mod } 2^m-1\right).$$

Adding 1 to both sides gives

$$2^n \equiv 1 \left(\text{mod } 2^m-1\right) \qquad (\ddagger)$$

Recall we need to prove $m \mid n$. Suppose $m \not| n$. Then by the division algorithm we have

$$n = mq + r \text{ where } 0 < r < m.$$

Substituting this $n = mq + r$ into (‡) yields

$$2^{mq+r} \equiv 1 \left(\text{mod } 2^m-1\right).$$

Using the rules of indices we have

$$2^{mq+r} \equiv \left(2^m\right)^q \times 2^r \equiv 1 \left(\text{mod } 2^m-1\right) \qquad (*)$$

By definition of congruence we have

$$2^m-1 \equiv 0 \left(\text{mod } 2^m-1\right) \text{ implies } 2^m \equiv 1 \left(\text{mod } 2^m-1\right)$$

Putting this $2^m \equiv 1 \left(\text{mod } 2^m-1\right)$ into (*) gives

$$2^{mq+r} \equiv \left(2^m\right)^q \times 2^r \equiv 1^q \times 2^r \equiv 2^r \equiv 1 \left(\text{mod } 2^m-1\right)$$

Using the definition of congruence (3.1):

$$a \equiv b \left(\text{mod } n\right) \quad \Leftrightarrow \quad a-b = kn$$

On $2^r \equiv 1 \pmod{2^m - 1}$ we have $2^r - 1 = k\left(2^m - 1\right)$ for some positive integer k. This is impossible because $0 < r < m$ so $2^r - 1 < 2^m - 1 \le k\left(2^m - 1\right)$. We have a contradiction so $m \mid n$. This completes our proof. ■

16. *How do we show* $\left(2^{2^n} - 1\right) \nmid \left(2^{2^n} + 1\right)$ *?*

By producing a counter example:

$$\frac{2^{2^3} + 1}{2^{2^3} - 1} = \frac{257}{255} \text{ and } \frac{257}{255} \text{ is } \textit{not} \text{ an integer.}$$

Hence $\left(2^{2^n} - 1\right) \nmid \left(2^{2^n} + 1\right)$.

17. We are asked to explain why $2^n \mid 2^{2^n}$.

Because by the rules of indices:

$$\frac{2^{2^n}}{2^n} = 2^{2^n - n} \qquad \left[\text{By } \frac{a^y}{a^x} = a^{y-x} \text{ with } y = 2^n \text{ and } x = n\right]$$

How do we know $2^{2^n - n} = \textit{integer?}$

Well $2^n > n$ which can be proven by induction;

If $n = 1$ then $2^1 > 1$.

Assume that $2^k > k$. Consider

$$2^{k+1} = 2^k \times 2 > 2k > k + 1.$$

Hence by induction we conclude that $2^n > n$ so $2^{2^n - n} = \text{integer}$.

18. (a) We need to show that 25 is a base 7 - pseudoprime.

We are required to show two things:

i) 25 is composite ii) $7^{24} \equiv 1 \pmod{25}$

Showing part i):

Clearly $5^2 = 25$ is composite.

Showing part ii):

Computing powers of 7 gives

$$7^2 \equiv 49 \equiv -1 \pmod{25}$$

Writing 24 as a multiple of 2 and any remainder gives

$$24 = 2 \times 12$$

Using the rule of indices

$$7^{24} \equiv \left(7^2\right)^{12} \equiv \left(-1\right)^{12} \equiv 1 \left(\text{mod } 25\right)$$

Hence 25 is a base 7 - pseudoprime.

We are also asked to show that 25 is *not* a Carmichael number. *How do we prove this?*

We must show $a^{24} \not\equiv 1 \left(\text{mod } 25\right)$ for a base a such that $\gcd\left(a, \ \ 25\right) = 1$. We first trial the easiest base of 2:

$$2^8 \equiv 256 \equiv 6, \ \ 2^{24} \equiv \left(2^8\right)^3 \equiv 6^3 \equiv 216 \equiv 16 \not\equiv 1 \left(\text{mod } 25\right)$$

Hence $2^{24} \not\equiv 1 \left(\text{mod } 25\right)$ so it is *not* a base 2 – pseudoprime. Therefore it *cannot* be a Carmichael number.

(b) We need to show that 217 is a base 5 - pseudoprime.

We are required to show two things:

i) 217 is composite ii) $5^{216} \equiv 1 \left(\text{mod } 217\right)$

<u>Showing part i)</u>:

Clearly 7 is a divisor of 217 because $217 = 7 \times 31$.

<u>Showing part ii)</u>:

Computing powers of 5 gives

$$5^2 \equiv 25, \ \ 5^3 \equiv 125, \ \ 5^4 \equiv 625 \equiv 191, \ 5^5 \equiv 87, \ \ 5^6 \equiv 1 \left(\text{mod } 217\right)$$

Using the last result $5^6 \equiv 1 \left(\text{mod } 217\right)$ to find $5^{216} \equiv x \left(\text{mod } 217\right)$ where x is the least non-negative residue modulo 217. Writing 216 in terms of 6 we have

$$216 = \left(6 \times 36\right)$$

Using the rule of indices

$$5^{216} \equiv \left(5^6\right)^{36} \equiv 1^{36} \equiv 1 \left(\text{mod } 217\right)$$

Hence 217 is a base 5 - pseudoprime.

We are also asked to show that 217 is *not* a Carmichael number. *How do we prove this?*

We have to show $a^{216} \not\equiv 1 \left(\text{mod } 217\right)$ for a base a such that $\gcd\left(a, \ \ 217\right) = 1$. We first trial the easiest base of 2:

$$2^9 \equiv 78, \ \ 2^{10} \equiv 156, \ \ 2^{11} \equiv 95, \ \ 2^{12} \equiv 190, \ \ 2^{13} \equiv 163, \ \ 2^{14} \equiv 109, \ \ 2^{15} \equiv 1 \left(\text{mod } 217\right).$$

We use $2^{15} \equiv 1 \left(\text{mod } 217\right)$ to find $2^{216} \equiv ? \left(\text{mod } 217\right)$. Writing 216 as a multiple of 15 and any remainder gives

$$216 = \left(14 \times 15\right) + 6\,.$$

By the rules of indices we have

$$2^{216} \equiv 2^{(14\times 15)+6} \equiv \left(2^{15}\right)^{14} \times 2^6 \equiv 2^6 \equiv 64 \not\equiv 1 \left(\text{mod } 217\right).$$

Hence $2^{216} \not\equiv 1 \left(\text{mod } 217\right)$ so it is *not* a base 2 – pseudoprime. Therefore it *cannot* be a Carmichael number.

19. *Proof.*

We can assume the Fermat number $F_n = 2^{2^n} + 1$ is composite. We need to prove

$$2^{2^{2^n}+1-1} = 2^{2^{2^n}} \equiv 1 \left(\text{mod } 2^{2^n} + 1\right).$$

We have the congruence $2^{2^n} + 1 \equiv 0 \left(\text{mod } 2^{2^n} + 1\right)$ because $2^{2^n} + 1$ is a multiple of itself. Subtracting 1 from both sides of this congruence gives

$$2^{2^n} \equiv -1 \left(\text{mod } 2^{2^n} + 1\right) \qquad (\ddagger)$$

Since we want to establish $2^{2^{2^n}} \equiv 1 \left(\text{mod } 2^{2^n} + 1\right)$ so we need to find the power, say m, of 2^{2^n} which is equal to $2^{2^{2^n}}$. That is we want to find m in the following:

$$\left(2^{2^n}\right)^m = 2^{2^{2^n}} \qquad (*)$$

Taking logs to the base 2 of (*) yields

$$\begin{aligned}
\log_2\left[\left(2^{2^n}\right)^m\right] &= \log_2\left[2^{2^{2^n}}\right] \\
m \times \log_2\left(2^{2^n}\right) &= \log_2\left[2^{2^{2^n}}\right] && \left[\text{Using the rule } \log\left(a^b\right) = b\log\left(a\right)\right] \\
m \times 2^n \times \log_2\left(2\right) &= 2^{2^n} \times \log_2\left(2\right) && \left[\text{Using the rule } \log\left(a^b\right) = b\log\left(a\right)\right] \\
m \times 2^n &= 2^{2^n} && \left[\text{Because } \log_2\left(2\right) = 1\right] \\
m &= \frac{2^{2^n}}{2^n} = 2^{2^n - n}
\end{aligned}$$

Applying Proposition (3.8):

$$a \equiv b \left(\text{mod } k\right) \;\Rightarrow\; a^m \equiv b^m \left(\text{mod } k\right)$$

To the congruence in (‡) with $m = 2^{2^n - n}$ gives

$$\begin{aligned}
\left(2^{2^n}\right)^{2^{2^n-n}} &\equiv \left(-1\right)^{2^{2^n-n}} \left(\text{mod } 2^{2^n} + 1\right) \\
\underbrace{2^{2^{2^n}}}_{\text{By (*)}} &\equiv \underbrace{1}_{\substack{\text{Because } (-1) \\ \text{to even idex is 1}}} \left(\text{mod } 2^{2^n} + 1\right)
\end{aligned}$$

We have $2^{2^{2^n}} \equiv 1 \pmod{2^{2^n}+1}$ which is what we wanted to prove. Therefore, the Fermat number $F_n = 2^{2^n}+1$ is a base 2 – pseudoprime.

■

20. We are asked to prove that there are an infinite number of base 2 - pseudoprimes.

Proof.

We know pseudoprimes exist. Let n_1 be a base 2 - pseudoprime. Then by Proposition (4.13):

If n is a base 2 - pseudoprime then $2^n - 1$ is also a base 2 - pseudoprime.

We have $n_2 = 2^{n_1} - 1$ is also an odd pseudoprime. Using this we can generate a third pseudoprime by $n_3 = 2^{n_2} - 1$. This again is a pseudoprime. By repeating this process we have kth pseudoprime given by

$$n_k = 2^{n_{k-1}} - 1$$

We continue this process for $k = 1,\ 2,\ 3,\ \cdots$. Therefore there are an infinite number of base 2 - pseudoprimes.

■

21. We need to show that the following is false:

A composite number n is a Carmichael number $\Leftrightarrow$ for every prime p which satisfies $p \mid n$ we have $(p-1) \mid (n-1)$.

Using the hint, we consider $n = p^k$. Then $p \mid p^k$ and $(p-1) \mid (p^k - 1)$ because

$$p^k - 1 = (p-1)\left(p^{k-1} + p^{k-2} + p^{k-3} + \cdots + p + 1\right)$$

This means that numbers such as $3^2 = 9$ are Carmichael numbers. However

$$2^{9-1} \equiv 2^8 \equiv 256 \equiv 4 \not\equiv 1 \pmod{9}$$

This shows that $3^2 = 9$ is *not* a base 2 – pseudoprime so it cannot be a Carmichael number.