Complete Solutions to Exercises 4.4

1. Each of the given integers is composite because the index is composite. To find the prime factor of each of the given numbers we use Proposition (4.19):

> Let $p = 2n+1$ be prime. Then we have the following:
> (a) If $p \equiv \pm 1 \pmod 8$ then $p \mid \left(2^n - 1\right)$.
> (b) If $p \equiv \pm 3 \pmod 8$ then $p \mid \left(2^n + 1\right)$.

(a) We need to find a prime factor of $2^6 + 1$. Let $n = 6$ then

$$p = 2n + 1 = \left(2 \times 6\right) + 1 = 13 \text{ which is prime.}$$

Since $p = 13 \equiv 5 \equiv -3 \pmod 8$ so by Proposition (4.19) part (b) with $n = 6$ and $p = 13$ we have $13 \mid \left(2^6 + 1\right)$. Hence 13 is a prime factor of the composite number

$$2^6 + 1 = 65.$$

(b) We are asked to find a prime factor of $2^{14} + 1$. Let $n = 14$ and

$$p = 2n + 1 = \left(2 \times 14\right) + 1 = 29 \quad [p = 29 \text{ is prime}]$$

Also $p = 29 \equiv 5 \equiv -3 \pmod 8$. Again applying Proposition (4.19) (b) with $n = 14$ and $p = 29$ we have

$$29 \mid \left(2^{14} + 1\right)$$

So 29 is a prime factor of $2^{14} + 1$.

(c) We are required to find a prime factor of $2^{15} - 1$. Let $n = 15$ and

$$p = 2n + 1 = \left(2 \times 15\right) + 1 = 31$$

31 is prime so we can use Proposition (4.19). We need to check whether 31 is congruent to ± 1 or ± 3 modulo 8:

$$31 \equiv 7 \equiv -1 \pmod 8$$

So by part (a) of Proposition (4.19) with $n = 15$ and $p = 31$ we have

$$31 \mid \left(2^{15} - 1\right)$$

Hence 31 is a prime factor of $2^{15} - 1$.

(d) We need to find a prime factor of $2^{20} - 1$. Let $n = 20$ and

$$p = 2n + 1 = \left(2 \times 20\right) + 1 = 41$$

41 is prime and $41 \equiv 1 \pmod 8$. By part (a) of Proposition (4.19) with $n = 20$ and $p = 41$ we have $41 \mid \left(2^{20} - 1\right)$. Hence 41 is a prime factor of $2^{20} - 1$.

(e) We have to find a prime factor of $2^{114}+1$. Let $n=114$ then

$$p=\left(2\times 114\right)+1=229$$

We need to check that 229 is prime. Using Corollary (2.10):

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

We have

$$\left\lfloor\sqrt{229}\right\rfloor=15$$

Therefore we have to check all the primes below 15 which are 2, 3, 5, 7, 11 and 13. *None* of these primes go into 229 so 229 is prime.

As $229\equiv 5\equiv -3\left(\text{mod } 8\right)$ therefore the prime 229 divides $2^{114}+1$. Hence 229 is a prime factor of $2^{114}+1$.

(f) We need to find a prime factor of $2^{504}-1$. Let $n=504$ then

$$p=\left(2\times 504\right)+1=1009$$

Need to test that 1009 is prime. Again using Corollary (2.10) given in part (e) we find that 1009 is actually a prime number. Also

$$1009\equiv 1\left(\text{mod } 8\right)$$

Applying the above Proposition (4.19) part (a) with $n=504$ and $p=1009$ we have

$$1009\ \Big|\ \left(2^{504}-1\right)$$

A prime factor of $2^{504}-1$ is 1009.

2. Remember the Mersenne number is given by $M_q=2^q-1$.

For these parts (a) and (b) we use Proposition (4.23):

> Any prime factor p of 2^q-1 is of the form $p=\left(2\times k\times q\right)+1$ where q is an odd prime.

(a) We are asked to find a prime factor of $M_{43}=2^{43}-1$. *How do we know there is a non-trivial factor of this* M_{43}*?*

Because we are given in the question that the number M_{43} is *composite*.

Let $q=43$ which is prime and

$$p=\left(2\times k\times q\right)+1=\left(2\times 43\times k\right)+1=86k+1$$

Any prime factor p of $M_{43}=2^{43}-1$ must be of the form $86k+1$.

Substituting $k=1$ into $p=86k+1$ gives

$$p = \left(86 \times 1\right) + 1 = 87 \text{ which is } \textit{composite}.$$

Since 87 is composite so it *cannot* be a prime factor of $M_{43} = 2^{43} - 1$.

Trial the next $k = 2$ into $p = 86k + 1$ gives

$$p = \left(86 \times 2\right) + 1 = 173$$

We can check whether 173 is prime by using Corollary (2.10):

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

$\left\lfloor \sqrt{173} \right\rfloor = 13$ and the only primes less than or equal to 13 are 2, 3, 5, 7, 11 and 13.

None of these primes go into 173 so 173 is prime.

Instead of dividing $M_{43} = 2^{43} - 1$ by 173 we use the second condition on the prime factors of $M_q = 2^q - 1$ which is Proposition (4.24):

> Any prime factor p of the composite $2^q - 1$ satisfies $p \equiv \pm 1 \left(\text{mod } 8\right)$.

With $p = 173$ we have $173 \equiv 5 \equiv -3 \left(\text{mod } 8\right)$ so 173 *cannot* be a factor of $M_{43} = 2^{43} - 1$ because $173 \equiv -3 \not\equiv \pm 1 \left(\text{mod } 8\right)$.

Creating a table for $86k + 1$ with $k = 3, 4, \cdots$:

k	$p = \left(86 \times k\right) + 1$	Prime or composite
3	$\left(86 \times 3\right) + 1 = 259$	Composite (see below)
4	$\left(86 \times 4\right) + 1 = 345$	Composite (obvious)
5	$\left(86 \times 5\right) + 1 = 431$	Prime (see below)

Clearly 345 is composite because 5 is a factor of 345.

It is harder to judge whether 259 is prime but if we trial the first few primes we find that 7 is a factor of 259.

How do we know that 431 is prime?

Again we use the above Corollary (2.10). We need to find

$$\left\lfloor \sqrt{431} \right\rfloor = 20$$

The only primes below 20 are 2, 3, 5, 7, 11, 13, 17 and 19. You can check that none of these primes are factors of 431 so 431 is prime.

Evaluating 431 modulo 8 gives

$$431 \equiv 7 \equiv -1 \left(\text{mod } 8\right)$$

Hence with $p = 431$ we have a prime number which satisfies $p \equiv \pm 1 \left(\text{mod } 8\right)$ so it is a prime factor of $M_{43} = 2^{43} - 1$.

(b) Similarly by Proposition (4.23):

> Any prime factor p of $2^q - 1$ is of the form $p = \big(2 \times k \times q\big) + 1$.

We need to find a prime factor of $M_{73} = 2^{73} - 1$. Let $q = 73$ which is prime and

$$p = \big(2 \times k \times q\big) + 1 = \big(2 \times 73 \times k\big) + 1 = 146k + 1$$

We only need to confine ourselves to primes p of the form $146k + 1$.

Creating a table for $146k + 1$ with various values of k we have:

k	$p = \big(146 \times k\big) + 1$	Prime or composite
1	$\big(146 \times 1\big) + 1 = 147$	Composite (see below)
2	$\big(146 \times 2\big) + 1 = 293$	Prime (see below)
3	$\big(146 \times 3\big) + 1 = 439$	Prime (see below)

147 is composite because adding the digits of 147 we have

$$1 + 4 + 7 = 12 \text{ and } 3 \Big| 12$$

So 3 is a divisor of 147.

Showing that the last two p values, 293 and 439, are both prime we use Corollary (2.10):

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

You can check that both of these are prime.

We now use Proposition (4.24):

> Any prime factor p of the composite $2^q - 1$ is of the form $p \equiv \pm 1 \big(\text{mod } 8\big)$.

Determining the least residues modulo 8 of these prime numbers, 293 and 439:

$$293 \equiv 5 \not\equiv \pm 1 \big(\text{mod } 8\big)$$

$$439 \equiv 7 \equiv -1 \big(\text{mod } 8\big)$$

The larger prime $p = 439$ satisfies $p \equiv \pm 1 \big(\text{mod } 8\big)$ which implies that 439 is a prime factor of composite $M_{73} = 2^{73} - 1$.

None of the indices 43 and 73 are Germain primes.

3. For this question we use Corollary (4.21):

> Let q and $p = 2q + 1$ both be primes. Note that q is a Germain prime.
> (a) If $q \equiv -1 \big(\text{mod } 4\big)$ then $p \Big| \big(2^q - 1\big)$.

(a) We need to find a prime factor of M_{83}. We follow the same procedures outlined in question 2 to determine a prime factor of $M_{83} = 2^{83} - 1$.

Let $q = 83$ and 83 is prime. Also let

$$p = \left(2 \times q\right) + 1 = \left(2 \times 83\right) + 1 = 167 .$$

You can check that 167 is prime. Since 167 is prime so 83 is a Germain prime.

Finding 167 modulo 4 gives

$$167 \equiv 3 \equiv -1 \left(\text{mod } 4\right).$$

Since 167 is prime and it also satisfies $167 \equiv -1 \left(\text{mod } 4\right)$ so 167 is a prime factor of $M_{83} = 2^{83} - 1$.

(b) We are asked to find a prime factor of $M_{131} = 2^{131} - 1$.

Let $q = 131$ which is prime (check this) and

$$p = \left(131 \times 2\right) + 1 = 263 .$$

Again you can check that $p = 263$ is prime. Therefore $q = 131$ is a Germain prime.

Finding the least residue of 263 modulo 4:

$$263 \equiv 3 \equiv -1 \left(\text{mod } 4\right).$$

Hence 263 is prime and also it satisfies $-1 \left(\text{mod } 4\right)$ so 263 is prime factor of $M_{131} = 2^{131} - 1$.

(c) We have to find a prime factor of $M_{179} = 2^{179} - 1$.

Let $q = 179$ and

$$p = \left(2 \times q\right) + 1 = \left(2 \times 179\right) + 1 = 359 .$$

$p = 359$ is prime; you can check this by using Corollary (2.10). Hence $q = 179$ is a Germain prime so $M_{179} = 2^{179} - 1$ is composite.

Evaluating $p = 359$ modulo 4 yields

$$p = 359 \equiv -1 \left(\text{mod } 4\right).$$

Hence 359 is a prime factor of $M_{179} = 2^{179} - 1$.

(d) We need to find a prime factor of $M_{191} = 2^{191} - 1$.

Let $q = 191$ which is prime (check this) and let

$$p = \left(2 \times 191\right) + 1 = 383 .$$

$p = 383$ is prime. Since $q = 191$ is a Germain prime so M_{191} is composite.

Evaluating $p = 383$ modulo 4 yields

$$p = 383 \equiv 3 \equiv -1 \left(\text{mod } 4\right)$$

Hence 383 is a prime factor of $M_{191} = 2^{191} - 1$.

We are also asked which of these indices are Germain primes.
From our workings above, *all* have a Germain prime index, that is 83, 131, 179 and 191 are Germain primes.

4. This is not a difficult question because we only use the theory of question 2 but we will have to try a number of k's in $p = 2kq + 1$ in order to find a prime factor of

$$M_{79} = 2^{79} - 1$$

Let $q = 79$ and 79 is prime. Let

$$p = \left(2 \times k \times q\right) + 1 = \left(2 \times 79 \times k\right) + 1 = 158k + 1$$

Any prime factors p of $M_{79} = 2^{79} - 1$ will be of the form $p = 158k + 1$.
Substituting $k = 1,\ 2,\ 3,\ \cdots$ into $p = 158k + 1$ gives the following:

k	$p = 158k + 1$	Prime or composite
1	$\left(158 \times 1\right) + 1 = 159$	composite
2	$\left(158 \times 2\right) + 1 = 317$	prime
3	$\left(158 \times 3\right) + 1 = 475$	composite
4	$\left(158 \times 4\right) + 1 = 633$	composite
5	$\left(158 \times 5\right) + 1 = 791$	composite
⋮	⋮	⋮
17	$\left(158 \times 17\right) + 1 = 2687$	prime

Testing the first prime in the table:

$$317 \equiv 5 \not\equiv \pm 1 \left(\text{mod } 8\right)$$

In the above table we have found $p = 158k + 1$ for $k = 1,\ 2,\ 3,\ \cdots,\ 17$ and it is *not* until we hit $k = 17$ that we get a *prime* $p = \left(158 \times 17\right) + 1 = 2687$ which also satisfies $p \equiv -1 \left(\text{mod } 8\right)$ because:

$$p = 2687 \equiv 7 \equiv -1 \left(\text{mod } 8\right)$$

Hence the prime 2687 is a prime factor of $M_{79} = 2^{79} - 1$.
(We *cannot* use the Germain prime proposition because 79 is *not* a Germain prime as $\left(2 \times 79\right) + 1 = 159$ is composite).

5. We are given the Mersenne number $2^{2617} - 1$ is composite so it has a non – trivial factor. *How can we show that 78 511 is a prime factor of* $2^{2617} - 1$ *?*

We use Proposition (4.23):

> Any prime factor p of $2^q - 1$ is of the form $p = \left(2 \times k \times q\right) + 1$.

In order to apply this Proposition, we first need to check that the index 2617 is prime. Again using Corollary (2.10):

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

We have $\left\lfloor \sqrt{2617} \right\rfloor = 51$ and the primes below 51 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 and 47. None of these primes go into 2617 so 2617 is prime.

Let $q = 2617$ then

$$p = \left(2 \times k \times q\right) + 1 = \left(2 \times 2617 \times k\right) + 1 = 5234k + 1$$

First we need to show that the given factor 78 511 is of this form $p = 5234k + 1$ with a particular value for k. Substituting $p = 78\,511$ into this yields

$$5234k + 1 = 78\,511 \text{ implies } k = 15.$$

Hence for $k = 15$ we have that $5234k + 1 = 78511$. Therefore the given factor 78511 is of the correct form $p = 2kq + 1$. *How do we know this is a factor?*

We also need to check that $q = 78511$ satisfies Proposition (4.24):

> Any prime factor p of $2^q - 1$ satisfies $p \equiv \pm 1 \left(\text{mod } 8\right)$.

We have

$$p = 78\,511 \equiv 7 \equiv -1 \left(\text{mod } 8\right).$$

Therefore 78 511 is a prime factor of $2^{2617} - 1$.

6. (a) We are required to show that $M_{13} = 2^{13} - 1$ is prime. We apply Corollary (2.10):

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

Let p be a prime divisor of $M_{13} = 2^{13} - 1$.

The floor function of $\sqrt{2^{13} - 1}$ is given by

$$p \le \left\lfloor \sqrt{2^{13} - 1} \right\rfloor = 90 \qquad (*)$$

If M_{13} is composite then this prime factor p of M_{13} must satisfy Proposition (4.23):

> Any prime factor p of $2^q - 1$ is of the form $p = 2kq + 1$.

What is q equal to in this case?

$q = 13$ so $p = \left(2 \times k \times q\right) + 1 = \left(2 \times 13 \times k\right) + 1 = 26k + 1$. Any prime factor of $M_{13} = 2^{13} - 1$ must be of the form $26k + 1$.

Substituting $k = 1,\ 2,\ \cdots$ into this $p = 26k + 1$ gives

$$p = \left(26 \times k\right) + 1 = \left(26 \times 1\right) + 1 = 27 \text{ but 27 is composite.}$$

$$p = \left(26 \times k\right) + 1 = \left(26 \times 2\right) + 1 = 53 \text{ and 53 is prime.}$$

For $p = 53$ to be a prime factor of $2^{13} - 1$ it must also satisfy Proposition (4.24):

> Any prime factor p of $2^q - 1$ satisfies $p \equiv \pm 1 \left(\text{mod } 8\right)$.

However $p = 53 \equiv 5 \equiv -3 \left(\text{mod } 8\right)$ so $p = 53$ *cannot* be a factor of $M_{13} = 2^{13} - 1$.

Continuing to substituting the next k which is 3 we have

$$p = 26k + 1 = \left(26 \times 3\right) + 1 = 79 \text{ which is prime.}$$

Again testing this with modulo 8 gives

$$p = 79 \equiv -1 \left(\text{mod } 8\right)$$

Hence 79 may be a prime factor of $M_{13} = 2^{13} - 1$. For $M_{13} = 2^{13} - 1$ to be composite we need to check that 79 is a factor:

Testing this with a calculator shows

$$\frac{2^{13} - 1}{79} = 103.68$$

Thus 79 is not a factor of $M_{13} = 2^{13} - 1$.

If we trial next $k = 4$ in $p = \left(26 \times k\right) + 1 = \left(26 \times 4\right) + 1 = 105$. There is *no* point testing this value of p because from (*) we must have a prime factor $p \leq 90$ for $M_{13} = 2^{13} - 1$ to be composite. Hence we conclude that $M_{13} = 2^{13} - 1$ is prime.

(b) We need to show that $M_{17} = 2^{17} - 1$ is prime. *How?*

By using Corollary (2.10):

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

Let p be a prime divisor of $M_{17} = 2^{17} - 1$. Then

$$p \leq \left\lfloor \sqrt{2^{17} - 1} \right\rfloor = 362 \qquad (\dagger)$$

Remember M_{17} is a Mersenne number so by Proposition (4.23):

> Any prime factor p of $2^q - 1$ is of the form $p = 2kq + 1$.

In this case $q = 17$ therefore the prime factor p must take the form

$$p = \left(2 \times k \times q\right) + 1 = \left(2 \times 17 \times k\right) + 1 = 34k + 1$$

We only need to examine prime factors amongst the sequence of numbers of the form $p = 34k + 1$.

Evaluating various p's for $k = 1,\ 2,\ 3,\ \cdots$

k	$p = 34k + 1$	Prime or composite
1	$\left(34 \times 1\right) + 1 = 35$	composite
2	$\left(34 \times 2\right) + 1 = 69$	composite
3	$\left(34 \times 3\right) + 1 = 103$	prime
4	$\left(34 \times 4\right) + 1 = 137$	prime
5	$\left(34 \times 5\right) + 1 = 171$	composite
6	$\left(34 \times 6\right) + 1 = 205$	composite
7	$\left(34 \times 7\right) + 1 = 239$	prime
8	$\left(34 \times 8\right) + 1 = 273$	composite
9	$\left(34 \times 9\right) + 1 = 307$	prime
10	$\left(34 \times 10\right) + 1 = 341$	composite

We don't need to test any numbers of the form $p = 34k + 1$ greater than 341. *Why not?*

Because from (†) we have that the prime factor $p \le 362$.

The primes are highlighted in the middle column:

103, 137, 239 and 307

Testing these prime numbers with modulo 8:

$$103 \equiv 7 \equiv -1 \left(\text{mod } 8\right)$$

$$137 \equiv 1 \left(\text{mod } 8\right)$$

$$239 \equiv -1 \left(\text{mod } 8\right)$$

$$307 \equiv 3 \left(\text{mod } 8\right)$$

There is *no* point testing 307 because $307 \equiv 3 \not\equiv \pm 1 \left(\text{mod } 8\right)$. Dividing $M_{17} = 2^{17} - 1$ by the remaining 3 numbers – 103, 137 and 239 shows that *none* of these numbers go into $M_{17} = 2^{17} - 1$.

Since there is *no* prime factor of $M_{17} = 2^{17} - 1$ which is ≤ 362 so $M_{17} = 2^{17} - 1$ is prime.

7. The error occurs in the last step D because 773 is prime but we also need to check that this number is congruent to $\pm 1 \pmod 8$. However we have

$$773 \equiv 5 \not\equiv \pm 1 \pmod 8$$

Hence 773 is *not* a prime factor of $2^{193} - 1$.

8. The error occurs in the first line (Step A) because our given index 49 is *composite* so we *cannot* use Proposition (4.23):

> Any prime factor p of $2^q - 1$ is of the form $p = 2kq + 1$ where q is a prime.

In our case $q = 49$ which is *not* prime.

9. We are required to prove that if q and $p = 2q + 1$ are primes with $q \equiv 1 \pmod 4$ then $p \mid (2^q + 1)$.

How do we prove this result?

By using Proposition (4.19) part (b):

> If $p \equiv \pm 3 \pmod 8$ then $p \mid (2^n + 1)$

Proof.

We are given $p = 2q + 1$ where q is a prime. Also we have $q \equiv 1 \pmod 4$ so by definition of congruence we have

$$q = 4k + 1 \text{ for some integer } k.$$

Substituting this $q = 4k + 1$ into $p = 2q + 1$ gives

$$p = 2(4k + 1) + 1 = 8k + 2 + 1 = 8k + 3 .$$

Therefore $p = 8k + 3 \equiv 3 \pmod 8$.

Applying proposition (4.19) part (b) with $n = q$ we have $p = 2q + 1$ and

$$p \mid (2^q + 1).$$

Because $p \equiv 3 \pmod 8$. This completes our proof.

■

10. We need to prove:

> If $q \neq 3$ a Germain prime with $q \equiv -1 \pmod 4$ and then the Mersenne number $M_q = 2^q - 1$ is composite and $p \mid (2^q - 1)$.

Proof.

By Corollary (4.21) part (a):

> If $q \equiv -1 \pmod 4$ then $p \mid (2^q - 1)$ where $p = 2q + 1$.

Since we are given $q \equiv -1 \pmod 4$, so applying this proposition we have $p \mid (2^q - 1)$.

Suppose $p = 2^q - 1$.

Since q is a Germain prime so $p = 2q + 1$ is also prime. Equating these gives

$$p = 2^q - 1 = 2q + 1 \Rightarrow \quad 2^q - 2q = 2$$
$$2(2^{q-1} - q) = 2 \Rightarrow 2^{q-1} - q = 1$$

Therefore $2^{q-1} = q + 1$. This is impossible because $2^{q-1} > q + 1$. (You can prove by mathematical induction that for all positive integers $n > 3$; $2^{n-1} > n + 1$.)

Therefore the prime $p \neq 2^q - 1$ so it is a non – trivial factor which implies $M_q = 2^q - 1$ is composite and $p \mid (2^q - 1)$.

■

11. *How do we show that each of the given integers is composite?*

We use Corollary (4.21).

> Let q and $p = 2q + 1$ both be primes. Note that q is a Germain prime.
> (a) If $q \equiv -1 \pmod 4$ then $p \mid (2^q - 1)$.
> (b) If $q \equiv 1 \pmod 4$ then $p \mid (2^q + 1)$.

(a) We need to show that $2^{41} + 1$ is composite. Let $q = 41 \equiv 1 \pmod 4$ and then

$$p = 2q + 1 = (2 \times 41) + 1 = 83$$

Both 41 and 83 are prime. Therefore 41 is a Germain prime.

Now we can apply part (b) of the above Corollary with $p = 83$ and $q = 41$ which gives

$$83 \mid (2^{41} + 1)$$

Hence 83 is a factor of $2^{41} + 1$ so the given integer $2^{41} + 1$ is composite.

(b) We are asked to find a prime factor of $2^{53} + 1$. Let $q = 53 \equiv 1 \pmod 4$ and

$$p = (2 \times q) + 1 = (2 \times 53) + 1 = 107$$

You can check that both of these numbers $q = 53$ and $p = 107$ are prime. Hence $q = 53$ is a Germain prime.

Since $q = 53 \equiv 1 \pmod 4$ so by Corollary (4.21) part (b) with $q = 53$ and $p = 107$ we have

$$107 \mid \left(2^{53}+1\right)$$

Hence 107 is a prime factor of $2^{53}+1$.

12. (i) First we are asked to show that 239 is a *Germain* prime. *What is a Germain prime?*

The prime q is a Germain prime if $2q+1$ is also prime.

Let $q=239$ then we can check that 239 is prime by using Corollary (2.10):

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

$\left\lfloor \sqrt{239} \right\rfloor = 15$ and the only primes below 15 are 2, 3, 5, 7, 11 and 13. None of these primes go into 239 so 239 is prime.

Let $p = \left(2 \times q\right)+1 = \left(2 \times 239\right)+1 = 479$. For 239 to be a Germain prime we need to show that

$$\left(2 \times 239\right)+1 = 479 \text{ is also prime.}$$

Again using Corollary (2.10) we have

$$\left\lfloor \sqrt{479} \right\rfloor = 21$$

The primes below 21 are 2, 3, 5, 7, 11, 13, 17 and 19. None of these primes go into 479 so 479 is prime. Hence 239 is a Germain prime.

(ii) We first show that $2^{239}-1$ is composite and then find a prime factor. *How do we show $2^{239}-1$ is composite?*

By Proposition (4.22):

> If $q \neq 3$ is a Germain prime with $q \equiv -1 \left(\text{mod } 4\right)$ then the Mersenne number $M_q = 2^q - 1$ is composite.

Since 239 is a Germain prime and $239 \equiv -1 \left(\text{mod } 4\right)$ so $2^{239}-1$ is composite.

By Corollary (4.21) part (a):

> If $q \equiv -1 \left(\text{mod } 4\right)$ then $p \mid \left(2^q - 1\right)$.

We have $239 \equiv 3 \equiv -1 \left(\text{mod } 4\right)$, so applying this Corollary with $q=239$ and $p=479$ gives

$$479 \mid \left(2^{239}-1\right)$$

Hence $2^{239}-1$ is composite because it has a factor 479. Actually

$$2^{239}-1 = 88342353238919216479164875037145925791374194843780947906080310064630988 7$$

We have found a prime factor 479 of $2^{239}-1$.(This $2^{239}-1$ has 72 digits).

(iii) We need to find another prime factor of $2^{239}-1$. *How?*

Use Proposition (4.23):

> Let q be an odd prime. Any prime factor p of the Mersenne number $M_q = 2^q - 1$ is of the form $p = 2kq + 1$ where k is an integer.

The prime factors p of $2^{239}-1$ must be of the form

$$p = 2kq + 1 = \left(2 \times 239 \times k\right) + 1 = 478k + 1$$

Since 239 is a Germain prime so for $k = 1$ we have the prime factor 479 found in part (ii). Substituting $k = 2,\ 3,\ 4, \cdots$ into this $p = 478k + 1$ gives

$$p = \left(478 \times 2\right) + 1 = 957$$

Clearly 3 is a factor of 957 because adding the digits of this $9 + 5 + 7 = 21$ and 3 is a factor of 957. Hence 957 is composite.

Substituting $k = 3$ gives

$$p = \left(478 \times 3\right) + 1 = 1435\,.$$

Clearly 5 is a factor of this number 1435 so it is composite.

Substituting $k = 4$ gives

$$p = \left(478 \times 4\right) + 1 = 1913\,.$$

$p = 1913$ is prime (check this). *Now that we have a prime* $p = 1913$ *but how can we check that this* $p = 1913$ *is a factor of* $2^{239}-1$*?*

Use Proposition (4.24):

> Let q be an odd prime. Any prime factor p of the $M_q = 2^q - 1$ is of the form $p \equiv \pm 1 \left(\mathrm{mod}\ 8\right)$.

We need to check that $p = 1913$ is congruent to plus or minus 1 congruent 8:

$$1913 \equiv 1 \left(\mathrm{mod}\ 8\right)$$

Therefore $p = 1913$ is a prime factor of $2^{239}-1$.

13. Let $q = 1559$. We are given that $q = 1559$ is prime. We have

$$p = 2q + 1 = \left(2 \times 1559\right) + 1 = 3119 \text{ is also prime.}$$

Hence $q = 1559$ is a Germain prime so M_{1559} is composite.

By Corollary (4.21) part (a):

If $q \equiv -1 \pmod 4$ then $p \mid (2^q - 1)$.

We have $q = 1559 \equiv 3 \equiv -1 \pmod 4$ so applying this Corollary with $q = 1559$ and $p = 3119$ gives

$$3119 \mid (2^{1559} - 1)$$

Hence 3119 is a prime factor of $2^{1559} - 1$.

14. The error is in Step E because the given Mersenne number $2^{61} - 1$ is prime. (You may have to use a computer algebra system to establish this.)

Recall by Proposition (4.24) the primes $p = 122k + 1$ must be of the form

$$p \equiv \pm 1 \pmod 8 \text{ to be a factor of } M_n.$$

And $p = 367 \equiv -1 \pmod 8$. However the proposition does *not* claim that every prime of this type $p = 122k + 1$ and satisfies $p \equiv \pm 1 \pmod 8$ is a prime factor of M_n.

If you were given that M_n is composite then you can say that any prime such that $p = 122k + 1$ and satisfies $p \equiv \pm 1 \pmod 8$ is a factor of M_n.

15. *Proof.*

We prove this by considering two cases; n is odd and then n is even but not a power of 2.

Let n be odd:

By using the given hint

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + x^{n-3} - x^{n-4} + \cdots - x + 1).$$

Putting $x = 2$ into this gives

$$\begin{aligned} 2^n + 1 &= (2+1)(2^{n-1} - 2^{n-2} + 2^{n-3} - 2^{n-4} + \cdots - 2 + 1) \\ &= 3(2^{n-1} - 2^{n-2} + 2^{n-3} - 2^{n-4} + \cdots - 2 + 1) \end{aligned}$$

Clearly we can see 3 is a factor of $2^n + 1$ provided n is odd. Also by induction we can show that $2^n + 1 > 3$ which implies the other factor in the above derivation satisfies

$$2^{n-1} - 2^{n-2} + 2^{n-3} - 2^{n-4} + \cdots - 2 + 1 > 1.$$

Let us actually show that $2^n + 1 > 3$.

The base case for $n = 2$ we have $2^2 + 1 = 5 > 3$. Assume the result is true for $n = k$:

$$2^k + 1 > 3 \qquad (*)$$

Required to prove that $2^{k+1} + 1 > 3$. Examining the left – hand side of this

$$2^{k+1}+1=2\left(2^k\right)+1=2^k+\underbrace{2^k+1}_{>3 \text{ by } (*)}>2^k+3>3\,.$$

Let n be even but not a power of 2:

In this case let $n=2^m k$ where $k>1$ is an odd number. Using the given hint with $x=2^{2^m}$ we have

$$\begin{aligned}2^n+1=2^{2^m k}+1&=\left(2^{2^m}\right)^k+1\\&=\left(2^{2^m}+1\right)\left(\left(2^{2^m}\right)^{k-1}-\left(2^{2^m}\right)^{k-2}+\left(2^{2^m}\right)^{k-3}-\left(2^{2^m}\right)^{k-4}+\cdots-\left(2^{2^m}\right)+1\right)\end{aligned}$$

In this case 2^n+1 has a factor of $2^{2^m}+1$ which is greater than 1 but not equal to 2^n+1 because $n=2^m k$ where $k>1$. Hence 2^n+1 has a non – trivial factor so it is composite.

■

16. (a) We need to prove that if $8p+7$ be prime then $2^{4p+3}-1$ is composite.

Proof.

If $4p+3$ is composite then by Corollary (4.11):

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

Therefore $2^{4p+3}-1$ is composite.

If $q=4p+3$ is prime then

$$\begin{aligned}2q+1&=2\left(4p+3\right)+1\\&=8p+7\end{aligned}$$

We are given that $8p+7$ is prime therefore $q=4p+3$ is a Germain prime and

$$q=4p+3\equiv 3\equiv -1\left(\text{mod } 4\right)$$

By Proposition (4.22):

> If $q\neq 3$ is a Germain prime and $q\equiv -1\left(\text{mod } 4\right)$ then the Mersenne number $M_q=2^q-1$ is composite and $p\,\big|\,\left(2^q-1\right)$ where $p=2q+1$.

We have $2^{4p+3}-1$ is composite.

■

(b) We need to prove that if $q=4n-1$ and $p=8n-1$ are both prime then $p\,\big|\,\left(2^q-1\right)$.

Proof.

We use Proposition (4.22):

If $q \neq 3$ is a Germain prime and $q \equiv -1 \pmod 4$ then the Mersenne number $M_q = 2^q - 1$ is composite and $p \mid (2^q - 1)$ where $p = 2q + 1$.

Consider $2q + 1 = 2(4n - 1) + 1 = 8n - 1 = p$. Hence q is a Germain prime so by the above Proposition (4.22) we have $p \mid (2^q - 1)$.

■

17. Since 41 and $(2 \times 41) + 1 = 83$ are both primes so 41 is a Germain prime. 83 is not a factor of $2^{41} - 1$ because $41 \equiv 1 \pmod 4$ and *not* $-1 \pmod 4$.

18. We are asked to prove the following result:

Let q be an odd prime. Any prime factor p of the Mersenne number $M_q = 2^q - 1$ is of the form $p = 2kq + 1$ where k is an integer.

Proof.

Let p be a prime factor of $M_q = 2^q - 1$. We have $p \mid (2^q - 1)$.

Required to prove that $p = 2kq + 1$.

By the definition of congruence we have

$$2^q \equiv 1 \pmod p \quad (\dagger)$$

Let k be the smallest positive integer such that

$$2^k \equiv 1 \pmod p \quad (\ddagger)$$

By using the given useful result in the question:

$$a^h \equiv 1 \pmod n \Leftrightarrow k \mid h$$

With $a = 2$ and $h = q$ we have $k \mid q$.

We are given that q is prime so the only divisors of q are 1 and itself which implies that $k = 1$ or $k = q$.

Suppose $k = 1$ then from $(\ddagger)$ we have

$$2^1 \equiv 2 \equiv 1 \pmod p$$

By the definition of congruence we have

$$p \mid (2 - 1) \quad \text{implies} \quad p \mid 1$$

However, a prime p cannot divide 1 therefore $k \neq 1$. Hence $k = q$.

Applying *FlT* (4.1):

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

with $a = 2$ we have

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

Again by using the given result:

$$a^h \equiv 1 \ \left(\text{mod } n\right) \ \Leftrightarrow \ k \mid h$$

With $a = 2$, $k = q$ and $h = p - 1$ we have

$$q \mid \left(p - 1\right)$$

This $q \mid \left(p - 1\right)$ implies there is an integer m such that

$$qm = p - 1 \qquad (*)$$

We now just need to prove that m is even.

We are given that q is an odd prime and also the prime p is odd because it is a factor of $2^q - 1$ which is odd. Since p is odd so $p - 1$ is even, so qm is even which gives m is even. Let $m = 2l$ where l is an integer so substituting this into (*) yields

$$2lq = p - 1 \quad \Rightarrow \quad p = 2lq + 1$$

Hence we have $p = 2lq + 1$ which completes our proof.

■