$$\left[a_1,\ a_2,\ a_3, \cdots, a_n\right] = \left[\left[a_1,\ a_2,\ a_3, \cdots, a_{n-1}\right],\ a_n\right]$$

We have

$$\begin{aligned}\gcd\left(a,\ b,\ c\right)\times\left[ab,\ ac,\ bc\right] &= \gcd\left(\gcd\left(a,\ b\right),\ c\right)\times\left[ab,\ \left[ac,\ bc\right]\right] \\ &= \gcd\left(\gcd\left(a,\ b\right),\ c\right)\times\left[ab,\ \underbrace{c\left[a,\ b\right]}_{\substack{\text{By result of question 7;}\\ \left[xy,\ xz\right]=x\times\left[y,\ z\right]}}\right]\end{aligned}$$

Applying Proposition (2.22):

$$\gcd\left(x,\ y\right)\times\left[x,\ y\right] = xy$$

To ab gives $\gcd\left(a,\ b\right)\times\left[a,\ b\right] = ab$. Putting this into the above derivation:

$$\begin{aligned}\gcd\left(a,\ b,\ c\right)\times\left[ab,\ ac,\ bc\right] &= \gcd\left(\gcd\left(a,\ b\right),\ c\right)\times\left[ab,\ c\left[a,\ b\right]\right] \\ &= \gcd\left(\gcd\left(a,\ b\right),\ c\right)\times\left[\gcd\left(a,\ b\right)\times\left[a,\ b\right],\ c\left[a,\ b\right]\right] \\ &\underbrace{=}_{\text{by result of question 7}} \left[a,\ b\right]\times\left(\gcd\left(\gcd\left(a,\ b\right),\ c\right)\times\left[\gcd\left(a,\ b\right),\ c\right]\right) \\ &= \left[a,\ b\right]\times \underbrace{\left(\gcd\left(a,\ b\right)\times c\right)}_{\substack{\text{By (2.22) } \gcd\left(x,\ y\right)\times\left[x,\ y\right]=x\times y\\ \text{with } x=\gcd\left(a,\ b\right) \text{ and } y=c}} \\ &= \underbrace{\frac{ab}{\cancel{\gcd\left(a,\ b\right)}}}_{\text{By Proposition (2.22)}} \times \cancel{\gcd\left(a,\ b\right)} \times c \\ &= abc\end{aligned}$$

This is our required result so it completes our proof.

■

Complete Solutions to Supplementary Problems 2

1. (a) We know $100 = 10^2$ and the factors of 10 are 2 and 5 so:

$$100 = 10^2 = \left(2 \times 5\right)^2 = 2^2 \times 5^2$$

(b) Since $1000 = 10^3$ so we have

$$1000 = 10^3 = \left(2 \times 5\right)^3 = 2^3 \times 5^3$$

(c) We are given the integer 161 for which we must find the prime factors. Using a calculator and dividing 161 by 7 (clearly 2, 3 and 5 are not factors of 161):

$$\frac{161}{7} = 23$$

Hence $161 = 7 \times 23$.

(d) Clearly 201 is divisible by 3 (because the sum of the digits add up to 3 and $3 \mid 3$):

$$\frac{201}{3} = 67$$

Is 67 a prime?

Yes because none of the prime factors 2, 3, 5, 7 go into 67. We have

$$201 = 3 \times 67$$

(e) We need to factorize 301 into its prime factors. Dividing 301 by 7 gives

$$\frac{301}{7} = 43$$

Therefore $301 = 7 \times 43$.

2. This question is testing whether you understand the notation $\lfloor\ \rfloor$ which is the floor function and $\lceil\ \rceil$ which is the ceiling function.

(a) $\left\lfloor \frac{1}{2} \right\rfloor$ means the closest integer less than $\frac{1}{2}$ so $\left\lfloor \frac{1}{2} \right\rfloor = 0$.

(b) Similarly we have $\left\lfloor -\frac{1}{2} \right\rfloor = -1$.

(c) Converting $-\frac{\pi}{4}$ into decimal form gives -0.785 (3dp). We have

$$\left\lceil -\frac{\pi}{4} \right\rceil = \left\lceil -0.785 \right\rceil$$

The ceiling function of -0.785 is the closest integer which is greater than -0.785 so

$$\left\lceil -\frac{\pi}{4} \right\rceil = \lceil -0.785 \rceil = 0$$

(d) Similarly $\left\lfloor -\frac{\pi}{4} \right\rfloor = \lfloor -0.785 \rfloor = -1$.

(e) We can evaluate $\lfloor -7.1 \rfloor + \lceil -7.1 \rceil$ by finding the ceiling and floor of -7.1:

$$\lfloor -7.1 \rfloor = -8 \quad \text{and} \quad \lceil -7.1 \rceil = -7$$

Substituting these we have

$$\lfloor -7.1 \rfloor + \lceil -7.1 \rceil = -8 + (-7) = -15$$

(f) We are given $\lfloor -7.1 \rfloor + \lceil 7.1 \rceil$. Using the definition of the ceiling and floor function we have

$$\lfloor -7.1 \rfloor + \lceil 7.1 \rceil = -8 + 8 = 0$$

3. (a) We first find $\lfloor e \rfloor$ and $\lfloor \pi \rfloor$:

$$\lfloor e \rfloor = 2 \quad \text{and} \quad \lfloor \pi \rfloor = 3$$

Therefore

$$\lfloor e \rfloor^{\lfloor \pi \rfloor} + \lfloor \pi \rfloor^{\lfloor e \rfloor} = 2^3 + 3^2 = 8 + 9 = 17$$

(b) Similarly we have $\lceil e \rceil = 3$ and $\lceil \pi \rceil = 4$ so

$$\lceil e \rceil^{\lceil \pi \rceil} + \lceil \pi \rceil^{\lceil e \rceil} = 3^4 + 4^3 = 81 + 64 = 145$$

(c) By our solutions to part (b) we have

$$\begin{aligned} \left\lceil e^{\lceil \pi \rceil} \right\rceil + \left\lceil \pi^{\lceil e \rceil} \right\rceil &= \lceil e^4 \rceil + \lceil \pi^3 \rceil \\ &= \lceil 54.6 \rceil + \lceil 31.01 \rceil = 55 + 32 = 87 \end{aligned}$$

4. We need to find $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor$ and $\left\lfloor \sqrt{x} \right\rfloor$ for the given x values.

(a) Substituting $x = 100$ into $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor$ gives

$$\left\lfloor \sqrt{\lfloor 100 \rfloor} \right\rfloor = \left\lfloor \sqrt{100} \right\rfloor = \lfloor 10 \rfloor = 10$$

Substituting $x = 100$ into $\left\lfloor \sqrt{x} \right\rfloor$ gives

$$\left\lfloor \sqrt{100} \right\rfloor = \lfloor 10 \rfloor = 10$$

(b) Similarly, we have

$$\left\lfloor \sqrt{\lfloor 1000 \rfloor} \right\rfloor = \left\lfloor \sqrt{1000} \right\rfloor = \lfloor 31.62 \rfloor = 31$$

Also $\left\lfloor \sqrt{1000} \right\rfloor = \lfloor 31.622 \rfloor = 31$.

(c) Putting $x = 2.75$ into the above formula yields

$$\left\lfloor \sqrt{\lfloor 2.75 \rfloor} \right\rfloor = \left\lfloor \sqrt{2} \right\rfloor = \lfloor 1.41 \rfloor = 1$$

$$\left\lfloor \sqrt{2.75} \right\rfloor = \lfloor 1.65 \rfloor = 1$$

For these values we have $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \left\lfloor \sqrt{x} \right\rfloor$.

5. By substituting certain x values into $\lfloor x \rfloor + \lceil x \rceil$ gives

$$\lfloor 0 \rfloor + \lceil 0 \rceil = 0 + 0 = 0$$

$$\lfloor 0.5 \rfloor + \lceil 0.5 \rceil = 0 + 1 = 1$$

$$\lfloor 1 \rfloor + \lceil 1 \rceil = 1 + 1 = 2$$

$$\lfloor 1.5 \rfloor + \lceil 1.5 \rceil = 1 + 2 = 3$$

$$\lfloor 2 \rfloor + \lceil 2 \rceil = 2 + 2 = 4$$

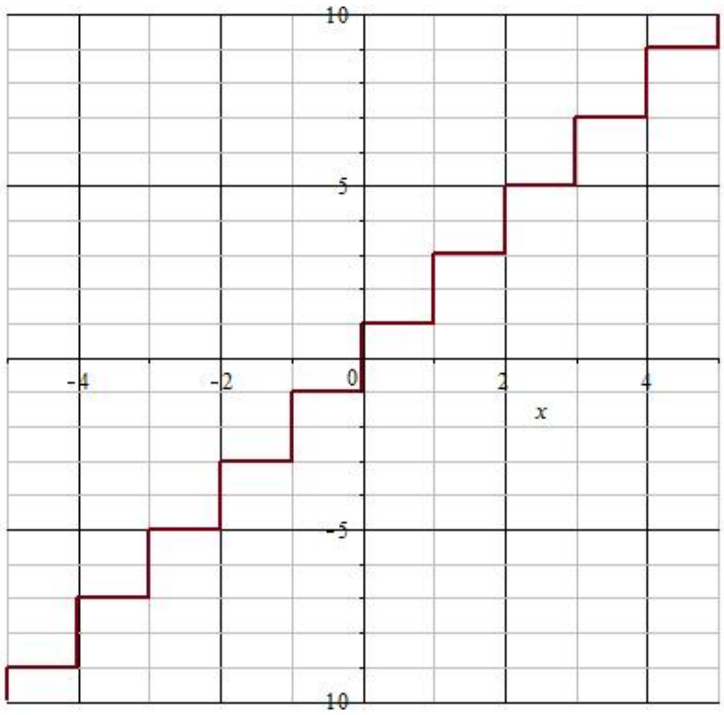
$$\lfloor -0.5 \rfloor + \lceil -0.5 \rceil = -1 + 0 = -1$$

$$\lfloor -1 \rfloor + \lceil -1 \rceil = -1 + (-1) = -2$$

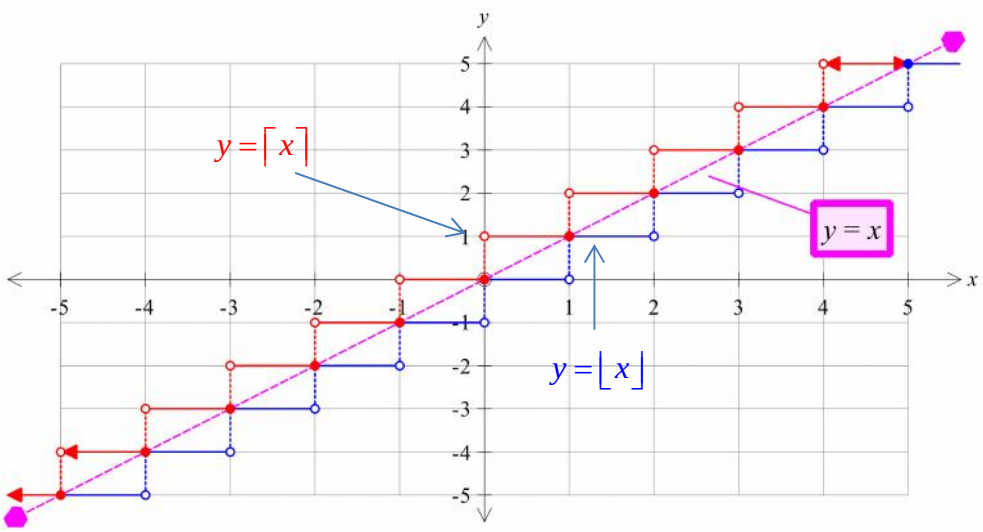
$$\lfloor -1.5 \rfloor + \lceil -1.5 \rceil = -2 + (-1) = -3$$

$$\lfloor -2 \rfloor + \lceil -2 \rceil = -2 + (-2) = -4$$

The graph of $\lfloor x \rfloor + \lceil x \rceil$ is given by



6. We can justify $\lfloor x \rfloor \leq x$ and $\lceil x \rceil \geq x$ by the following graph:



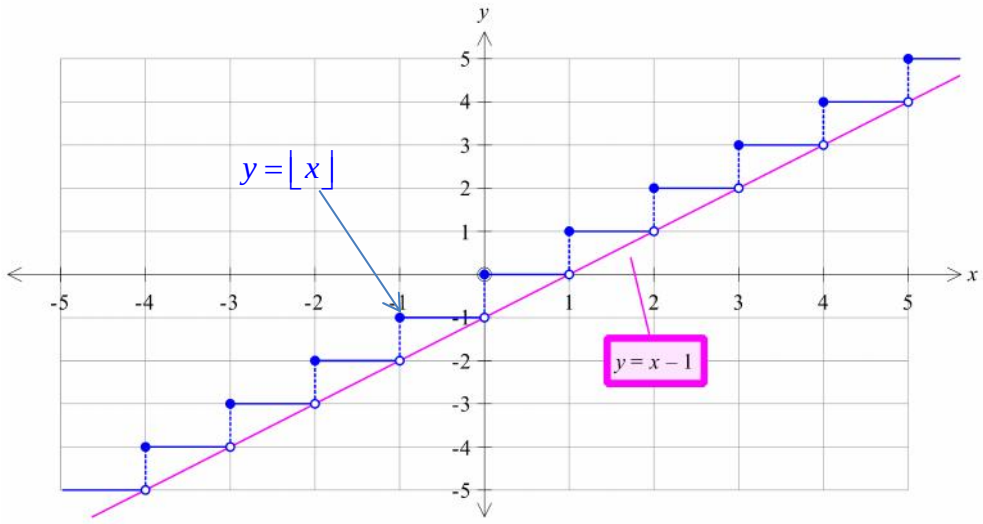
Note that the graph of $y = \lfloor x \rfloor$ is below or on the graph of $y = x$ and the graph of $y = \lceil x \rceil$ is above or on the graph of $y = x$. Therefore, we have

$$\lfloor x \rfloor \leq x \text{ and } \lceil x \rceil \geq x .$$

7. (a) We are asked to show that $x - 1 < \lfloor x \rfloor \leq x$.

By result of question 6 we have $\lfloor x \rfloor \leq x$.

Sketching the graph of $y = x - 1$ and $y = \lfloor x \rfloor$ on the same axes we have

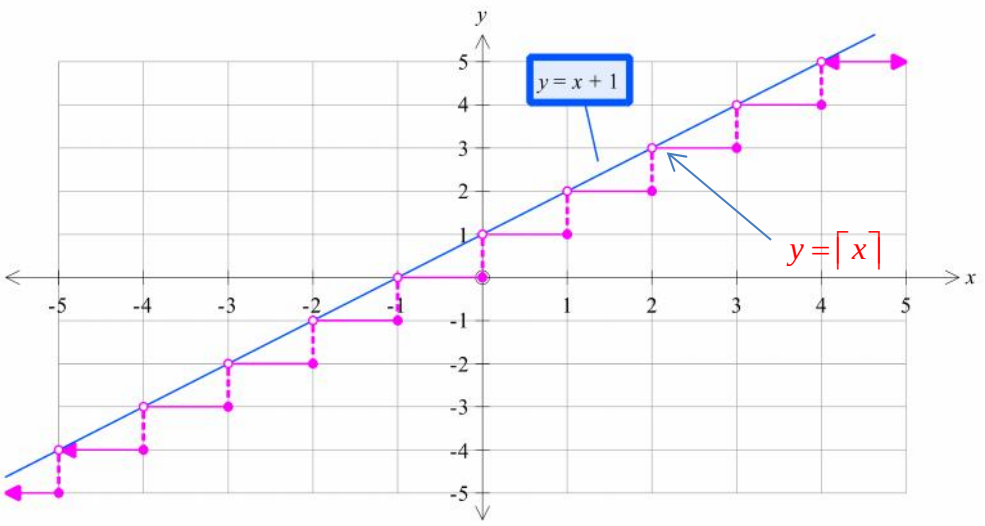


Notice that the graph of $y = x - 1$ is below the graph of $y = \lfloor x \rfloor$ so

$$x - 1 < \lfloor x \rfloor$$

Therefore we have $x - 1 < \lfloor x \rfloor \leq x$.

(b) Similarly sketching the graphs of $y = \lceil x \rceil$ and $y = x + 1$ on the same axes:



Since the graph of $y = x + 1$ lies above the graph of $y = \lceil x \rceil$ so $\lceil x \rceil < x + 1$.

By the result of question 6 and the above graph we have

$$x \le \lceil x \rceil < x + 1$$

8. We need to show that the only prime of the form $n^2 - 1$ is 3.

Proof.

Note that $n^2 - 1$ is the difference of two squares:

$$n^2 - 1 = n^2 - 1^2 = (n-1)(n+1)$$

The only case where $(n-1)(n+1)$ is prime is when $n = 2$ because if $n > 2$ then $n - 1 > 2$ and $n + 1 > 2$ so $(n-1)(n+1)$ is composite. When $n = 2$ then

$$2^2 - 1 = 3$$

Hence the only prime of the form $n^2 - 1$ is 3.

■

9. We are asked to show that the only prime of the form $n^3 - 1$ is 7.

Proof.

Factorizing $n^3 - 1$ by using the hint gives

$$n^3 - 1 = (n-1)(n^2 + n + 1)$$

The only case where $n^3 - 1$ is prime is when $n = 2$. Substituting $n = 2$ into the above gives

$$2^3 - 1 = (2-1)(2^2 + 2 + 1) = 7$$

If $n > 2$ then $n^3 - 1 = (n-1)(n^2 + n + 1)$ is composite because it has factors of $n - 1 > 2$ and $n^2 + n + 1 > 2$. Hence 7 is the only factor of the form $n^3 - 1$.

■

10. (a) Let $x = 10$ then

$$\lceil 10 \rceil = 10 \text{ but } \lfloor 10 \rfloor + 1 = 11.$$

Therefore, for any real number x we do *not* have $\lceil x \rceil = \lfloor x \rfloor + 1$.

(b) For non – integer x we have $\lceil x \rceil = \lfloor x \rfloor + 1$.

Proof.

Let n be an integer such that $n < x < n+1$. Then

$$\lceil x \rceil = n+1 \text{ and } \lfloor x \rfloor = n.$$

We have

$$\lceil x \rceil = n+1 = \lfloor x \rfloor + 1.$$

This completes our proof.

■

(c) We need to prove $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof.

Let $x = n + y$ where $0 \le y < 1$. Substituting this into $\lfloor x + m \rfloor$ gives

$$\lfloor x + m \rfloor = \lfloor n + y + m \rfloor = n + m \quad [\text{Because } 0 \le y < 1]$$

Substituting $x = n + y$ into $\lfloor x \rfloor + m$ yields

$$\lfloor x \rfloor + m = \lfloor n + y \rfloor + m = n + m$$

Hence $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

■

(d) This time we prove $\lceil x + m \rceil = \lceil x \rceil + m$.

Proof.

Let x be an integer then $\lceil x \rceil = x$ and

$$\lceil x \rceil + m = x + m = \lceil x + m \rceil$$

Let $x = n + y$ where $0 < y < 1$ so x is *not* an integer. Substituting this into $\lceil x + m \rceil$ gives

$$\lceil x + m \rceil = \lceil n + y + m \rceil = n + m + 1$$

Substituting $x = n + y$ into $\lceil x \rceil + m$ yields

$$\lceil x \rceil + m = \lceil n + y \rceil + m = n + 1 + m$$

Hence $\lceil x + m \rceil = \lceil x \rceil + m$.

■

11. For this question we use Corollary (2.10):

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

(a) Using this corollary with $n = 907$ we have primes p such that

$$p \leq \left\lfloor \sqrt{907} \right\rfloor = \left\lfloor 30.12 \right\rfloor = 30$$

Only need to test all the primes below 30 to see if 907 is prime or composite. The prime below 30 are $2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$.

Clearly 2, 3 and 5 do not go into 907. Testing the remaining primes in this list we find that none of these go into 907 therefore by Corollary (2.10) we conclude that 907 is prime.

(b) Arguing along similar lines with $n = 1009$ we have

$$p \leq \left\lfloor \sqrt{1009} \right\rfloor = \left\lfloor 31.76 \right\rfloor = 31$$

The primes p up to 31 are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29 \text{ and } 31$$

Again, none of these numbers go into 1009 so 1009 is prime.

(c) Similarly, with $n = 1331$ we have

$$p \leq \left\lfloor \sqrt{1331} \right\rfloor = \left\lfloor 36.48 \right\rfloor = 36$$

The primes below 36 are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29 \text{ and } 31$$

2, 3, 5 and 7 do not go into 1331. However, 11 is a divisor of 1331 because

$$\frac{1331}{11} = 121 = 11^2$$

Hence $1331 = 11^3$ so 1331 is a composite integer.

12. It is straightforward to check that both 101 and 103 are primes. The primes p which satisfy $p \leq \left\lfloor \sqrt{103} \right\rfloor = 10$ are 2, 3, 5 and 7. None of these numbers go into 101 or 103 so both these numbers are prime.

13. We are asked to prove that $\gcd\left(p+1,\quad p^2+1\right) = 2$ where p is an odd prime.

Proof.

Let $\gcd\left(p+1,\quad p^2+1\right) = g$. Required to prove that $g = 2$.

We are given that p is odd so both $p+1$ and p^2+1 are even which implies that $g \geq 2$.

By the definition of gcd we have

$$g \mid (p+1) \quad \text{and} \quad g \mid (p^2+1)$$

Applying the Linear Combination Theorem (1.3):

> If $a \mid b$ and $a \mid c$ then $a \mid (bx+cy)$ for any integers x and y.

to $g \mid (p+1)$ and $g \mid (p^2+1)$ gives

$$g \mid [(p^2+1)-(p+1)] \Rightarrow g \mid (p^2-p) \Rightarrow g \mid p(p-1)$$

We are given that p is prime and from above we have $g \geq 2$ so $g \nmid p$ and the $\gcd(g, p) = 1$. By Euclid's Lemma $g \mid (p-1)$.

We have $g \mid (p+1)$ and $g \mid (p-1)$. Again applying the Linear Combination Theorem (1.3) we obtain

$$g \mid [(p+1)-(p-1)] \Rightarrow g \mid 2 \underbrace{\Rightarrow}_{\text{Because } g \geq 2} g = 2$$

Thus, we have our result, and this completes our proof.

■

14. We need to show that there are infinitely many primes that end in 111.

Proof.

To prove this result, we use Dirichlet's Theorem (2.17):

> Let a and b be relatively prime positive integers, then the arithmetic progression
> $$a, \ a+b, \ a+2b, \ a+3b, \ \cdots$$
> contains infinitely many primes.

Let $a = 111$ and $b = 1000$ then $\gcd(111, 1000) = 1$ which means we can apply Dirichlet's theorem with $a = 111$ and $b = 1000$. The list

$$\begin{aligned} &111, \ 111+1000, \ 111+2(1000), \ 111+3(1000), \ \cdots \\ &= 111, \ 1111, \ 2111, \ 3111, \ 4111, \cdots \end{aligned}$$

contains infinitely many primes. This completes our proof.

■

15. We are asked to prove infinitely many primes of the form $8n+3$. *How?*

Use Dirichlet's Theorem:

Proof.

Let $a = 3$ and $b = 8$ then $\gcd(3, 8) = 1$ and applying Dirichlet's Theorem with $a = 3$ and $b = 8$ we have the list of integers:

$$3,\ 3+8,\ 3+2\big(8\big),\ 3+3\big(8\big),\ \cdots,\ 3+8n,\ \cdots$$

There are an infinite number of primes in this list. Hence there are infinitely many primes of the form $8n+3$.

■

16. We are asked to show that p^2+2p+1 is composite for all primes p.

Proof.

We can factorize p^2+2p+1 into

$$p^2+2p+1=\big(p+1\big)^2$$

This means that $p+1$ is a factor of p^2+2p+1 so this number is composite.

■

17. We are required to prove that p^n is odd for primes $p\geq 3$.

Proof.

Since primes $p\geq 3$ so p is odd which we can write as $p=2m+1$. Using mathematical induction we have

$$p^1=p=2m+1 \text{ which is odd.}$$

Assume p^k is also odd, that is

$$p^k=2m'+1.$$

Required to prove p^{k+1} is also odd. We have

$$\begin{aligned} p^{k+1}=p^kp^1&=\big(2m'+1\big)\big(2m+1\big) \qquad \big[\text{From above}\big]\\ &=4mm'+2m'+2m+1\\ &=2\big(2mm'+m'+m\big)+1 \end{aligned}$$

This number $p^{k+1}=2\big(2mm'+m'+m\big)+1$ is odd because it is of the format

$$2\big(\text{integer}\big)+1$$

By mathematical induction we have p^n is odd for primes $p\geq 3$.

■

18. We need to show that p^4+4p^2+5 is composite for prime p.

Proof.

Completing the square on p^4+4p^2+5:

$$p^4+4p^2+5=\big(p^2+2\big)^2+1$$

By the result of the previous question we know that p^2 is odd. Also odd number plus 2 is also odd. *What about* $\big(odd\big)^2$ *?*

The odd number can be written as $2m+1$ where m is an integer. Then

$$\left(2m+1\right)^2 = 4m^2 + 4m + 1$$

This is odd. Therefore, we have $\left(p^2+2\right)^2$ is an odd number. Hence

$$p^4 + 4p^2 + 5 = \left(p^2+2\right)^2 + 1 = \left(\text{odd integer}\right) + 1 = \text{even}$$

Hence $p^4 + 4p^2 + 5$ is an even integer so it is composite because the only even which is prime is 2 and $p^4 + 4p^2 + 5$ cannot equal 2 for prime p. We have our result.

■

19. *Proof.* Let $n' = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ be the prime decomposition of the square root of n. Then

$$n = \left(n'\right)^2 = \left(p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}\right)^2 = p_1^{2k_1} p_2^{2k_2} \cdots p_m^{2k_m}$$

Every exponent of the prime is even. This is our required result.

■

20. We need to prove that $n^3 + 1$ is composite for $n \geq 2$.

Proof.

Factorizing $n^3 + 1$ gives

$$n^3 + 1 = \left(n+1\right)\left(n^2 - n + 1\right) \qquad (\dagger)$$

We are given that $n \geq 2$ so the factor $n+1 \geq 3$ in (†). Also, for $n \geq 2$ we have

$$n^2 - n + 1 = n\left(n-1\right) + 1 \geq 2 + 1 = 3$$

Since we have a factor of 3 or greater so $n^3 + 1$ is composite.

■

21. We are asked to prove that $n^m - 1$ is composite for $n > 2$ and $m \geq 2$.

Proof.

We use the identity

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

Substituting $x = n$ into this gives

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

We are given that $n > 2$ so the factor $n - 1 > 2$ therefore the integer in (*) is composite. This completes our proof.

■

22. (a) Substituting $n = 1$ to 10 into $f\left(n\right) = 2n^2 + 11$ gives a prime number. However, when $n = 11$ then

$$f\left(11\right) = 2\left(11\right)^2 + 11 = 11\left[2\left(11\right) + 1\right]$$

Of course, this integer is composite because it has a factor of 11.

(b) Similarly we have $f\left(n\right) = 2n^2 + 29$ is prime for all the integers between 1 and 28 (inclusive) but when $n = 29$ we have

$$f\left(29\right) = 2\left(29\right)^2 + 29 = 29\left[2\left(29\right) + 1\right]$$

This is clearly a composite number with a factor of 29.

23. We are asked to show that $\left\lfloor x\right\rfloor + \left\lfloor -x\right\rfloor = \begin{cases} 0 & \text{if } x \text{ is an integer} \\ -1 & \text{if } x \text{ is not an integer} \end{cases}$

Proof.

We consider the two different cases.

Case I: Let x be an integer, then

$$\left\lfloor x\right\rfloor + \left\lfloor -x\right\rfloor = x + \left(-x\right) = 0$$

Case II: Assume x is *not* an integer. Let $x = n + y$ where $0 < y < 1$. Then

$$\begin{aligned} \left\lfloor x\right\rfloor + \left\lfloor -x\right\rfloor &= \left\lfloor n + y\right\rfloor + \left\lfloor -\left(n + y\right)\right\rfloor \\ &= n + \left\lfloor -n - y\right\rfloor \\ &= n - n - 1 = -1 \end{aligned}$$

In both cases we have our given result.

24. We need to prove that $\left[a,\ \ b\right] = a \times b$ provided a and b are relatively prime.

Proof.

We are given that a and b are relatively prime so there exists integers r and s such that $ar + bs = 1$. Let $\left[a,\ \ b\right] = m$ then by the definition of LCM we have

$$a \mid m\,,\ b \mid m \text{ implies } ak = m,\ \ bl = m$$

We have

$$\begin{aligned} m = 1 \times m &= \left(ar + bs\right)m \\ &= arm + bsm \\ &= arbl + bsak = ab\left(rl + sk\right) \end{aligned}$$

Clearly $a \mid (a \times b)$ and $b \mid (a \times b)$ therefore by definition of LCM

$$m = [a, \quad b] \leq a \times b \qquad (*)$$

Applying the result of question 12(i) of Exercises 1.3:

$$x \mid z \text{ and } y \mid z \text{, and } \gcd(x, \quad y) = 1 \text{ then } (x \times y) \mid z$$

To $a \mid m$, $b \mid m$ where $\gcd(a, \quad b) = 1$ implies

$$(a \times b) \mid m \text{ implies } a \times b \leq m$$

In (*) we had $m \leq a \times b$ and now we have $a \times b \leq m$ therefore

$$[a, \quad b] = m = a \times b$$

This completes our proof.

■

25. We are asked to prove that $\gcd(a, \quad b) \times [a, \quad b] = a \times b$.

Proof.

Let $m = [a, \quad b]$ and $g = \gcd(a, \quad b)$ then

$$a \mid \frac{ab}{g} \text{ and } b \mid \frac{ab}{g} \text{ implies } \frac{ab}{g} \geq [a, \quad b] = m \qquad (\dagger)$$

We also have

$$a \mid m, \ b \mid m \text{ which implies } ak = m, \ bl = m$$

From $g = \gcd(a, \quad b)$ we have integers r and s such that

$$g = ar + bs \ \Rightarrow \ 1 = \frac{ar + bs}{g}$$

Now we show that $\frac{ab}{g} \mid m$:

$$\begin{aligned} m = m \times 1 = m\left(\frac{ar + bs}{g}\right) &= \frac{ar}{g}m + \frac{bs}{g}m \\ &= \frac{ar}{g}bl + \frac{bs}{g}ak \quad [\text{Because } m = bl = ak] \\ &= \frac{ab}{g}(rl + sk) \end{aligned}$$

This $m = \frac{ab}{g}(rl + sk)$ implies $\frac{ab}{g} \mid m$. Hence $\frac{ab}{g} \leq m = [a, \quad b]$.

By (†) and this we have

$$\frac{ab}{g} \geq m \text{ and } \frac{ab}{g} \leq m \text{ which implies } \frac{ab}{g} = m$$

Therefore $ab = gm = \gcd\left(a,\quad b\right)\times\left[a,\quad b\right]$. This completes our proof.

■

26. (a) We are asked to prove that if $a^n - 1$ is prime then $a = 2$ and n is prime.

Proof.

Factorizing $a^n - 1$ gives

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

If $a = 1$ then $a^n - 1$ is zero because $a - 1$ is a factor of this number.

If $a \geq 3$ then $a^n - 1$ is composite because $a - 1 \geq 2$ is a factor of $a^n - 1$. This implies that we must have $a = 2$ because we are given $a^n - 1$ is prime.

We also need to show that n is prime. We prove this part by contradiction.

Suppose $n = rs$ is composite so $r > 1$ and $s > 1$. Then by using the following identity:

$$x^{rs} - 1 = \left(x^r - 1\right)\left(x^{r(s-1)} + x^{r(s-2)} + x^{r(s-3)} + \cdots + x^r + 1\right)$$

With $x = a$ we have

$$a^n - 1 = a^{rs} - 1 = \left(a^r - 1\right)\left(a^{r(s-1)} + a^{r(s-2)} + a^{r(s-3)} + \cdots + a^r + 1\right) \qquad (\dagger)$$

We have already established that $a = 2$. The first factor on the right hand side of (†) is equal to $a^r - 1 = 2^r - 1$ and from above we have $r > 1$ so $a^r - 1 = 2^r - 1$ is a factor greater than 2. Hence the integer $a^n - 1$ in (†) is composite. This is a contradiction because we are given that $a^n - 1$ is prime. Therefore, our supposition $n = rs$ is composite must be false so n is prime. This completes our proof.

■

(b) We need to prove that if $a \geq 3$ then $a^n - 1$ is composite.

Proof.

We need to use the following algebraic identity:

$$x^n - 1 = \left(x-1\right)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right)$$

Substituting $x = a$ into this gives

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

The first factor $a - 1 \geq 3 - 1 \geq 2$ and the second factors are all greater than 2 because $a^{n-1} + a^{n-2} + \cdots + a + 1 \geq 3 + 1 = 4$. Hence $a^n - 1$ is composite.

■

27. We are asked to prove that if $p \mid a^n$ then $p \mid a$.

Proof.

Suppose $p \nmid a$ then by the result of question 3(a) Exercises 2.1 we have the $\gcd(p,\ a) = 1$. Writing

$$p \mid a^n \text{ as } p \mid a\left(a^{n-1}\right)$$

Applying Euclid's Lemma (1.13):

> If $x \mid yz$ with $\gcd(x,\ y) = 1$ then $x \mid z$.

To $p \mid a\left(a^{n-1}\right)$ we have $p \mid a^{n-1}$. We can rewrite this as $p \mid a\left(a^{n-2}\right)$. Again, applying Euclid's Lemma to this $p \mid a\left(a^{n-2}\right)$ gives $p \mid a^{n-2}$. We can repeat this process until we get to $p \mid a^2$ and applying Euclid's Lemma to this gives $p \mid a$. We have a contradiction because we started with $p \nmid a$ and now we have $p \mid a$. Therefore, our supposition $p \nmid a$ must be wrong so $p \mid a$.

■