Number Theory solutions

Exercise 1.1. In these solutions steps are justified by referring to the axioms 1 - 11, or to the results of earlier questions.

1. The zero element is unique, i.e. if $0'$ is any other integer satisfying $z+0' = z = 0' + z$ for every z then $0' = 0$.

   Solution. Let 0 and $0'$ be two elements satisfying axiom 2. Then considering the element $0 + 0'$ and applying axiom 2 to both elements in turn we find first that
   $$0 + 0' = 0,$$
   and second that
   $$0 + 0' = 0'.$$
   Hence $0 = 0'$ as they are both equal to $0 + 0'$. So we can conclude that the zero element is unique. □

2. Additive inverses are unique, i.e. let $z \in \mathbb{Z}$, if x and x' satisfy $z + x = 0 = z + x'$ then $x = x'$.

   Solution. Assume as in question that we have $z, x, x' \in \mathbb{Z}$ and $z + x = z + x' = 0$. Observe that
   $$\begin{aligned} x &= x + 0, \text{ axiom 2,} \\ &= x + (z + x'), \text{ by assumption above,} \\ &= (z + x) + x', \text{ axioms 1 \& 4,} \\ &= 0 + x', \text{ by assumption above,} \\ &= x', \text{ axiom 2,} \end{aligned}$$
   as required. □

3. The multiplicative element 1 is unique.

   Solution. Exactly similar proof to question 1 above, except using multiplication. Suppose that 1 and $1'$ are two elements satisfying axiom 6. Then consider the element $1 \cdot 1'$ and apply axiom 6 to each in turn to yield the conclusion that $1 = 1'$, i.e. the multiplicative identity element is unique. □

4. For any $z \in \mathbb{Z}$ we have $-(-z) = z$.

   Solution. This is really just a case of examining axiom 3 again but viewing it from the point of view of the element $(-z)$, i.e.
   $$z + (-z) = (-z) + z = 0.$$
   This says that z is the additive inverse of the element $(-z)$. □

5. For all $z \in \mathbb{Z}$ we have $0z = 0$.

Solution. This is quite tricky one to extract from the axioms and takes a bit of puzzling to find. Here is one way to get it.

$$\begin{aligned} 0 \cdot z &= 0 \cdot z + 0, \text{ ax. } 2 \\ &= 0 \cdot z + \big(0 \cdot z + (-(0 \cdot z))\big), \text{ ax. } 3, \\ &= \big(0 \cdot z + 0 \cdot z\big) + (-(0 \cdot z)), \text{ ax. } 1 \\ &= (0+0) \cdot z + (-(0 \cdot z)), \text{ ax. } 8, \\ &= 0 \cdot z + (-(0 \cdot z)), \text{ ax. } 2, \\ &= 0, \text{ ax. } 3. \end{aligned}$$

□

6. For all $z \in \mathbb{Z}$ we have $-z = (-1)z$.

Solution. Let $z \in \mathbb{Z}$ and considering $z + (-1)z$ we see

$$\begin{aligned} z + (-1)z &= 1z + (-1)z, \text{ ax. } 6, \\ &= (1 + (-1))z, \text{ ax. } 8, \\ &= 0z, \text{ ax. } 3, \\ &= 0, \text{ by question 5.} \end{aligned}$$

This shows that $(-1)z$ is indeed the additive inverse of z. □

7. $(-1)^2 = 1$.

Solution. Well considering the result from the previous question (q. 6) with $z = -1$ we see that $(-1)^2 = (-1)(-1) = -(-1)$, i.e. $(-1)^2$ is the additive inverse of the element -1. But from question 4 we know that the additive inverse of the element (-1) is the element 1, (since (-1) is the additive inverse of 1).
Therefore we can conclude that $(-1)^2 = 1$. □

8. For all $x, y \in \mathbb{Z}$ we have

$$x(-y) = (-x)y = -(xy).$$

Solution. This involves splitting the -1 off from the element $(-y)$ (result from question 6) and then moving it around using associativity and commutativity of multiplication (axioms 5 & 7).

$$\begin{aligned} x(-y) &= x((-1)y), \text{ question 6}, \\ &= ((-1)x)y, \text{ axs. 5 \& 7}, \\ &= (-x)y, \text{ question 6}, \\ &= ((-1)x)y, \text{ reversing last step}, \\ &= (-1)(xy), \text{ ax. } 5, \\ &= -(xy), \text{ question 6}. \end{aligned}$$

□

9. For all $x, y \in \mathbb{Z}$ we have $(-x)(-y) = xy$.

Solution. A quick way to do this is to make two application of the results of question 8 and then apply the result of question 4. Using the original axioms instead will take more steps.

$$\begin{aligned}(-x)(-y) &= -\big((-x)y\big), \text{ q. 8,}\\ &= -(-\big(xy\big)), \text{ q. 8,}\\ &= xy, \text{ q. 4.}\end{aligned}$$

□

10. (*Cancellation in* $+$). For all $x, y, z \in \mathbb{Z}$

$$x + z = y + z \quad\Rightarrow\quad x = y.$$

Solution. Take the equation $x + z = y + z$ and add the element $(-z)$ on the right to both sides. Then gather z and $-z$ together using associativity and replace with 0 etc.

$$\begin{aligned}x + z = y + z &\Rightarrow (x+z) + (-z) = (y+z) + (-z),\\ &\Rightarrow x + (z + (-z)) = y + (z + (-z)), \text{ ax. 1,}\\ &\Rightarrow x + 0 = y + 0, \text{ ax. 3,}\\ &\Rightarrow x = y, \text{ ax. 2}\end{aligned}$$

□

11. (*Trichotomy*). For any $z \in \mathbb{Z}$ exactly one of the following is true: $z = 0$, $z > 0$ or $0 > z$. Or more generally, for all $x, y \in \mathbb{Z}$ exactly one of the following is true: $x = y$, $x > y$ or $y > x$.

Solution. This is just a reinterpretation of axiom 9 using the definitions $z > 0$ iff $z \in P$ and $x > y$ iff $x - y \in P$. □

12. (*Transitivity of* $>$). If $x > y$ and $y > z$ then $x > z$.

Solution.

$$\begin{aligned}x > y \;\&\; y > z &\Rightarrow x - y, y - z \in P, \text{ by definition,}\\ &\Rightarrow (x - y) + (y - z) \in P, \text{ ax. 10.}\end{aligned}$$

But using associativity of addition etc. we see that $(x-y)+(y-z) = x - z$ and so we have $x - z \in P$, i.e. $x > z$ as required. □

13. For integers x, y, if $x > 0$ and $y > 0$ then $x + y > 0$ and $xy > 0$.

Solution. Again, this is simply a restatement of axiom 10 in terms of $>$ instead of P. □

14. For integers x, y, if $x > y$ then for all $z \in \mathbb{Z}$ we have $x + z > y + z$.

Solution. This follows from the observation that $(x+z)-(y+z) = x - y$, which can be proved using a combination of associativity of addition, other axioms and previous results. Therefore $x - y \in P$ iff $(x + z) - (y + z) \in P$, which implies the required result. □

15. $1 > 0$.

Solution. Actually this doesn't strictly follow from the axioms as stated in the notes as I neglected to include a crucial extra detail in the notes as originally printed. All 11 axioms (as printed) are true of the trivial ring $R = \{0\}$, which consists solely of the element 0. Note that for this trivial ring R we have $1 = 0$ and the set P of positives is empty, $P = \{\}$. However once we exclude this trivial case (which really requires an extra axiom such as "The system contains more than one element" or altering axiom 6 so that it insists that $1 \neq 0$) then we can proceed.
As $1 \neq 0$, by axiom 9 we have $1 < 0$ or $1 > 0$. If $1 < 0$ then we would have $-1 > 0$. This implies that $(-1)^2 > 0$, by axiom 10. But from question 7 we know that $(-1)^2 = 1$. So it would seem that we have $1 < 0$ AND $1 > 0$. But this contradicts axiom 9, so we conclude that it must be that $1 > 0$. □

16. For all integers z, if $z \neq 0$ then $z^2 > 0$.

Solution. Since $z \neq 0$ we know $z < 0$ or $z > 0$. If $z > 0$ then $z^2 > 0$ by axiom 10.
On the other hand if $z < 0$ then $-z > 0$. But then we get

$$\begin{aligned} z^2 &= 1 \cdot z^2, \text{ ax. } 6, \\ &= (-1)^2 \cdot z^2, \text{ q. } 7, \\ &= (-z)^2, \text{ (see following paragraph)}, \\ &> 0, \text{ since } -z > 0 \text{ and ax. } 10 \end{aligned}$$

The penultimate step was justified by a combination of associativity and commutativity of multiplication and application of the result of question 6.
So in all cases we have $z^2 > 0$ as required. □

17. For integers x, y, z where $x > y$, if $z > 0$ then $xz > yz$. If $z < 0$ then $xz < yz$.

Solution. Suppose that $x > y$ and $z > 0$.

$$\begin{aligned} x > y &\Rightarrow x - y > 0, \text{ by definition}, \\ &\Rightarrow (x - y)z > 0, \text{ ax. } 10, \\ &\Rightarrow xz - yz > 0, \text{ ax. } 8, \\ &\Rightarrow xz > yz, \text{ by definition}, \end{aligned}$$

as required.
If $z < 0$ then we have $(-z) > 0$ and approach to the above will yield $xz < yz$. □

18. (*Zero-divisors law*). For integers x, y, if $xy = 0$ then $x = 0$ or $y = 0$.

Solution. Suppose that $xy = 0$ and that $x \neq 0$ and $y \neq 0$. By multiplying both sides of the first equation by -1 once or twice if necessary, we can arrange that $x, y > 0$. But then $xy > 0$ by axiom 10. But this contradicts our initial assumption. So we conclude that (at least) one of x or y must be zero. □

19. (*Cancellation in* $\cdot$). For integers x, y, if $z \neq 0$ and $xz = yz$, then $x = y$.

Solution. Suppose that $xz = yz$. Then we get $xz - yz = (x-y)z = 0$ using axiom 8. But now applying the zero-divisors law from the previous question we see that one of $x - y$ and z must be zero. We have assumed that $z \neq 0$ and so we must have $x - y = 0$, i.e. $x = y$. □

20. (*More general well-orderedness*). Consider a non-empty subset $A \subset \mathbb{Z}$. If A is bounded above then A contains a greatest element. Similarly, if A is bounded below then A contains a least element.

Solution. □

Exercise 1.2. Induction will play a key role in the some of the results we prove in number theory so students need to be confident in using it.

1. $\forall n \geq 1 \ \sum_{j=1}^{n} j = \frac{1}{2}n(n+1)$.

Solution. When $n = 1$ both sides evaluate to 1. Assume true for an integer $k \geq 1$. Then

$$\begin{aligned}
\sum_{j=1}^{k+1} j &= k + 1 + \sum_{j=1}^{k} j, \\
&= k + 1 + \frac{1}{2}k(k+1), \text{ by assumption}, \\
&= (k+1)\left(1 + \frac{1}{2}k\right), \\
&= (k+1)\frac{1}{2}(k+2), \\
&= \frac{1}{2}(k+1)(k+2),
\end{aligned}$$

i.e. the result for $k+1$ follows. So by the principle of induction the result is true for all $n \geq 1$. □

2. $\forall n \geq 1 \ \sum_{j=1}^{n} j^2 = \frac{1}{6}n(n+1)(2n+1)$.

Solution. When $n = 1$ both sides evaluate to 1. Assume true for an integer $k \geq 1$. Then

$$\begin{aligned}
\sum_{j=1}^{k+1} j^2 &= (k+1)^2 + \sum_{j=1}^{k} j^2, \\
&= (k+1)^2 + \frac{1}{6}k(k+1)(2k+1), \text{ by assumption,} \\
&= (k+1)\left((k+1) + \frac{1}{6}k(2k+1)\right), \\
&= (k+1)\left(\frac{1}{6}\left(6k+6+2k^2+k\right)\right), \\
&= (k+1)\frac{1}{6}\left(2k^2+7k+6\right), \\
&= \frac{1}{6}(k+1)(k+2)(2k+3), \\
&= \frac{1}{6}(k+1)(k+2)\big(2(k+1)+1\big),
\end{aligned}$$

i.e. the result for $k+1$ follows. So by the principle of induction the result is true for all $n \geq 1$. □

3. $\forall n \geq 1 \ \sum_{j=1}^{n}(2j-1) = n^2$.

Solution. When $n = 1$ both sides evaluate to 1. Assume true for an integer $k \geq 1$. Then

$$\begin{aligned}
\sum_{j=1}^{k+1}(2j-1) &= \big(2(k+1)-1\big) + \sum_{j=1}^{k}(2j-1), \\
&= (2k+1) + k^2, \text{ by assumption,} \\
&= (k+1)^2,
\end{aligned}$$

i.e. the result for $k+1$ follows. So by the principle of induction the result is true for all $n \geq 1$. □

4. $\forall n \geq 1 \ \sum_{j=1}^{n} j^3 = \left(\sum_{j=1}^{n} j\right)^2 = \frac{1}{4}n^2(n+1)^2$.

Solution. Can be done in very much the same spirit as the previous problems. □

5. $\forall n \geq 1 \ \sum_{j=1}^{n}(3j-1) = \frac{1}{2}n(3n+1)$.

Solution. Can be done in very much the same spirit as the previous problems. □

6. $\forall n \geq 1 \ \left(1+\frac{1}{2}\right)^n \geq 1 + \frac{n}{2}$,

Solution. When $n = 1$ both sides evaluate to $\frac{3}{2}$ and so the (in)equality holds. Assume result is true for an integer $k \geq 1$. Then

$$\begin{aligned}\left(1+\frac{1}{2}\right)^{k+1} &= \frac{3}{2}\left(1+\frac{1}{2}\right)^{k}, \\ &\geq \frac{3}{2}\left(1+\frac{k}{2}\right), \text{ by assumption,} \\ &= \frac{3}{2}+\frac{3k}{4}, \\ &> \frac{3}{2}+\frac{k}{2}, \\ &= 1+\frac{1}{2}+\frac{k}{2}, \\ &= 1+\frac{k+1}{2}.\end{aligned}$$

Summarising this chain of (in)equalties we have

$$\left(1+\frac{1}{2}\right)^{k+1} > 1+\frac{k+1}{2},$$

i.e. the result for $k+1$ follows. So by the principle of induction the result is true for all $n \geq 1$. $\square$

7. $\forall\, n \geq 1 \; 2^n \leq \frac{(2n)!}{n!n!}$.

Solution. When $n = 1$ both sides evaluate to 2, and so the (in)equality holds. Assume result is true for an integer $k \geq 1$. Then

$$\begin{aligned}
2^{k+1} &= 2 \times 2^k, \\
&\leq 2\frac{(2k)!}{k!k!}, \text{ by assumption}, \\
&= 2\frac{(k+1)(k+1)}{(k+1)(k+1)}\frac{(2k)!}{k!k!}, \\
&= \frac{2(k+1)(k+1)\big[(2k)!\big]}{(k+1)!(k+1)!}, \\
&= \frac{(2k+2)(k+1)\big[(2k)!\big]}{(k+1)!(k+1)!}, \\
&< (k+1)\frac{(2k+2)\big[(2k)!\big]}{(k+1)!(k+1)!} + k\frac{(2k+2)\big[(2k)!\big]}{(k+1)!(k+1)!}.
\end{aligned}$$

In this last step we have simply rewritten what we had by taking the $(k + 1)$ factor from the numerator out to the front, and then added on the second term (which is positive) to produce the strict inequality. Continuing the chain, starting with what we had

$$\begin{aligned}
2^{k+1} &< (k+1)\frac{(2k+2)\big[(2k)!\big]}{(k+1)!(k+1)!} + k\frac{(2k+2)\big[(2k)!\big]}{(k+1)!(k+1)!}, \\
&= (2k+1)\frac{(2k+2)\big[(2k)!\big]}{(k+1)!(k+1)!}, \\
&= \frac{(2k+2)!}{(k+1)!(k+1)!}.
\end{aligned}$$

Summarising, we have shown that the inequality

$$2^{k+1} < \frac{(2k+2)!}{(k+1)!(k+1)!}$$

follows from the assumption that the result holds for the integer k. So by the principle of induction the result is true for all $n \geq 1$. □

Exercise 2.1. The following are consequences of the recently introduced definitions and results along with previous results on divisibility.

1. Let $a, b \in \mathbb{Z}$ be not both zero. Consider the sets A and B defined by

$$A = \{\, ma + nb \;:\; m, n \in \mathbb{Z} \} \,,$$

$$B = \{\, m \gcd(a, b) \;:\; m \in \mathbb{Z} \} \,.$$

   Show that $A = B$, i.e. linear combinations of a and b correspond exactly with multiples of $\gcd(a, b)$.

Solution. Let $d = \gcd(a, b)$. In order to show equality we need to establish the two set inclusions, $A \subset B$ and $B \subset A$. Let $z \in A$, i.e. $z = ma + nb$, for some pair of integers m, n. Then by property 3 of theorem 2.1, d divides $na + mb$, i.e. $z = rd$, for some integer r. Therefore $z \in B$, and so we can conclude that $A \subset B$.
Now let $z \in B$, i.e. $z = rd$ for some integer r. Now we know from theorem 2.3 that d can be expressed as $d = ma + nb$ for some pair of integers m, n. Multiplying by r we get

$$z = rd = (rm)a + (rn)b.$$

Therefore $z \in A$ and so we can conclude that $B \subset A$. $\square$

2. Prove that a and b are coprime if and only if there exists $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

Solution. This result is an *if and only if* statement, so we need to prove it we will prove the implication in both direction.
First assume that a and b are co-prime, i.e. that $\gcd(a, b) = 1$. Then by theorem 2.3 there exist integers m, n such that $1 = ma + nb$.
Secondly assume that there exist integers m, n such that $1 = ma + nb$. Let $d = \gcd(a, b)$. Since d is a common divisor of a and b we have $d|1$, by property 3 of theorem 2.1. This implies that $d = \pm 1$, and since 1 divides all integers we conclude that $d = 1$.
Both directions of the equivalence have been established. $\square$

3. Suppose that $d = \gcd(a, b)$ and that $a = \alpha d$ and $b = \beta d$. Prove that $\gcd(\alpha, \beta) = 1$.

Solution. Making the assumptions given in the question we can apply theorem 2.3 so that we have a pair of integers m, n such that

$$d = ma + nb = m\alpha d + n\beta d.$$

Cancelling d from this equation gives

$$1 = m\alpha + n\beta,$$

and hence $\gcd(\alpha, \beta) = 1$ by question 2 of Exercises 2.1 . $\square$

4. Prove that if $\gcd(a, b) = d$ then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Solution. Sorry about this repetition. This is simply the previous question expressed slightly differently. $\square$

5. Suppose that $a|c$ and $b|c$ and $\gcd(a, b) = 1$. Prove that $ab|c$.

Solution. Suppose that $a|c$ and $b|c$ and $\gcd(a,b) = 1$. So we have integers α and β such that

$$c = \alpha a = \beta b.$$

Also, by theorem 2.3 we have integers m, n such that

$$1 = ma + nb.$$

Multiplying both sides of this by c gives

$$c = mac + nbc,$$

which when combined with the previous expressions for c leads to

$$c = ma\beta b + nb\alpha a = (m\beta + n\alpha)ab.$$

This last equation shows that $ab|c$. $\square$

6. (Euclid's Lemma). Suppose that $c|ab$ and that $\gcd(c,a) = 1$. Prove that $c|b$.

Solution. Suppose that $c|ab$ and that $\gcd(c,a) = 1$. By theorem 2.3 we have integers m, n such that

$$mc + na = 1,$$

which gives

$$mcb + nab = b.$$

But since $c|ab$, there is an integer z such that $ab = zc$, and so

$$mcb + nzc = (mb + nz)c = b.$$

This last equation shows that $c|b$, as required. $\square$

Exercise 2.2. Here are some questions to help you practice using the Euclidean Algorithm. You should complete these and others until you are confident in using it to find both the gcd and a linear combination for the gcd. It is good practice to make a few notes as you go emphasizing how the pairs we apply the integer division process to all have the same gcd.

1. Use the Euclidean algorithm to find $\gcd(143, 227)$, $\gcd(306, 657)$ and $\gcd(272, 1479)$.

Solution.

$$\begin{aligned}227 &= 143 + 84,\\ 143 &= 84 + 59,\\ 84 &= 59 + 25,\\ 59 &= 2 \times 25 + 9,\\ 25 &= 2 \times 9 + 7,\\ 9 &= 7 + 2,\\ 7 &= 3 \times 2 + 1.\end{aligned}$$

And so $\gcd(143, 227) = 1$.

$$\begin{aligned}657 &= 2 \times 306 + 45,\\ 306 &= 6 \times 45 + 36,\\ 45 &= 36 + 9,\\ 36 &= 4 \times 9.\end{aligned}$$

And so $\gcd(306, 657) = 9$.

$$\begin{aligned}1479 &= 5 \times 272 + 119,\\ 272 &= 2 \times 119 + 34,\\ 119 &= 3 \times 34 + 17,\\ 34 &= 2 \times 17.\end{aligned}$$

And so $\gcd(272, 1479) = 17$. □

2. Find integers m, n that satisfy the following equations,

Solution. These are solved by first applying the Euclidean Algorithm to find the greatest common divisor and then working backwards through the equations to end up with the gcd as a linear combination of the original pair of numbers. □

a) $\gcd(56, 72) = 56m + 72n$,

Solution.

$$\gcd(56, 72) = 8 = 4 \times 56 - 3 \times 72.$$

□

b) $\gcd(24, 138) = 24m + 138n$,

Solution.

$$\gcd(24, 138) = 6 = 6 \times 24 - 1 \times 138.$$

□

c) $\gcd(119, 272) = 119m + 272n$,

Solution.

$$\gcd(119, 272) = 17 = 7 \times 119 - 3 \times 272.$$

□

d) $\gcd(1769, 2378) = 1769m + 2378n$.

Solution.

$$\gcd(1769, 2378) = 29 = 39 \times 1769 - 29 \times 2378.$$

□

Exercise 2.3. These exercises develop some more general results as consequences of the definitions and results we have seen so far.

1. Prove or disprove the following statement: if $a|(b + c)$ then $a|b$ or $a|c$.

Solution. This statement is false in general. A simple counter example is $a = 2$, $b = c = 1$. □

2. Use the process of integer division with remainder to prove that if $a \in \mathbb{Z}$, one of the integers a, $a + 2$ or $a + 4$ is divisible by 3.

Solution. Let $a \in \mathbb{Z}$, then

$$a = 3q + r, \quad r = 0, 1 \text{ or } 3.$$

If $r = 0$ then $3|a$ and we are done. If $r = 1$ then

$$a + 2 = 3q + 1 + 2 = 3(q + 1),$$

and so $3|(a + 2)$ and we are done. If $r = 2$ then

$$a + 4 = 3q + 2 + 4 = 3(q + 2),$$

and so $3|(a + 4)$ and we are done.
So in all cases 3 divides one of a, $a + 2$ or $a + 4$. □

3. Prove that for all $a \in \mathbb{Z}$, $4 \not| (a^2 + 2)$.

Solution. There are just four possibilities for the remainder when an integer a is divided by 4, they are

$$\begin{aligned} a &= 4q, \\ a &= 4q+1, \\ a &= 4q+2, \\ a &= 4q+3. \end{aligned}$$

The corresponding expressions for a^2+2 then are ,

$$\begin{aligned} a^2+2 &= 16q^2+2 = 4(4q^2)+2, \\ a^2+2 &= 16q^2+8q+1+2 = 4(4q^2+2q)+3, \\ a^2+2 &= 16q^2+16q+4+2 = 4(4q^2+4q+1)+2, \\ a^2+2 &= 16q^2+24q+9+2 = 4(4q^2+6q+2)+3. \end{aligned}$$

In each case we see that a^2+2 is not divisible by 4 because it has a remainder of 2 or 3 upon division by 4. □

4. Prove the following

Solution. These clearly call for proof by induction. □

a) $\forall n \geq 1\ 7|(2^{3n}-1)$,

Solution. When $n=1$ the statement is $7|7$ which is clearly true. Assume that $7|2^{3k}-1$ for some $k \geq 1$, i.e. $2^{3k}-1 = 7q$ for some $q \in \mathbb{Z}$. Then

$$\begin{aligned} 2^{3(k+1)}-1 &= 2^{3k+3}-1 \\ &= 8\left(2^{3k}-1\right)+7 \\ &= 7 \times (8q+1). \text{ by above assumption} \end{aligned}$$

And so we have that $7|2^{3(k+1)}-1$. So by the principle of induction the result is true for all $n \geq 1$. □

b) $\forall n \geq 1\ 8|(3^{2n}+7)$,

Solution. When $n=1$ the statement is $8|16$ which is clearly true. Assume that $8|3^{2k}+7$ for some $k \geq 1$, i.e. $3^{2k}+7 = 8q$ for some $q \in \mathbb{Z}$. Then

$$\begin{aligned} 3^{2(k+1)}+7 &= 3^{2k+2}+7 \\ &= 9\left(3^{2k}+7\right)-56 \\ &= 8 \times (9q-7). \text{ by above assumption} \end{aligned}$$

And so we have that $8|3^{2(k+1)}?+7$. So by the principle of induction the result is true for all $n \geq 1$. □

c) $\forall n \geq 1\ 3|(2^n+(-1)^{n+1})$.

Solution. When $n = 1$ the statement is $3|3$ which is clearly true. Assume that $3|(2^k + (-1)^{k+1})$ for some $k \geq 1$, i.e. $(2^k + (-1)^{k+1}) = 3q$ for some $q \in \mathbb{Z}$. Then

$$\begin{aligned}
2^{k+1} + (-1)^{(k+1)+1} &= 2^{k+1} + (-1)^{k+2} \\
&= \left(2 \times 2^k + (-1)^{k+2}\right) \\
&= 2 \times \left(2^k + (-1)^{k+1}\right) \pm 3, (\pm \text{ as } k \text{ is resp. even/odd}), \\
&= 3 \times (2q \pm 1). \text{ by above assumption}
\end{aligned}$$

And so we have that $3|2^{k+1} + (-1)^{(k+1)+1}$. So by the principle of induction the result is true for all $n \geq 1$. □

5. Prove that if an integer a is not divisible by 2 nor by 3, then 24 does divide $a^2 - 1$.

Solution. For this we need to show that 24 divides $a^2 - 1$ under the conditions described in the question. In order to do this we shall make use of question 5 from exercises 2.1, which says that if $\gcd(a, b) = 1$ and $a|c$ and $b|c$ then $ab|c$. So we will show that $8|a^2 - 1$ and $3|a^2 - 1$ and then conclude from these that $24|a^2 - 1$.
Suppose that a is not divisible by 2 nor 3. Then applying integer division with remainder to a (dividing by 2 and 3) we can conclude that a can be expressed as

$$a = 2q + 1 = 3r + s,$$

for some integers q and r and where the remainder s is equal to 1 or 2.
Firstly, $a^2 - 1 = 4q^2 + 4q = 4q(q + 1)$. Now one of q and $q + 1$ must be even and the other odd (they are a pair of consecutive integers) so the product $q(q + 1)$ is even, say $q(q + 1) = 2n$. Therefore $a^2 - 1 = 8qn$, and hence $8|a^2 - 1$.
Secondly we shall show that $3|a^2 - 1$. This will come from the expression $a = 3r + s$ and so there are two cases to consider, $s = 1$ and $s = 2$. If $s = 1$ then $a^2 - 1 = 9r^2 + 6r = 3(3r^2 + 2r)$. If $s = 2$ then $a^2 - 1 = 9r^2 + 12r + 3 = 3(3r^2 + 6r + 1)$. In both cases we see that $3|a^2 - 1$.
We've shown that $a^2 - 1$ is divisible by 8 and 3 and so we can conclude that $a^2 - 1$ is divisible by 24 as required.

□

6. Prove that in the linear combination

$$\gcd(a, b) = ma + nb,$$

the coefficients m and n are coprime.

Solution. Suppose that $\gcd(a, b) = d$. So we can write $a = \alpha d$ and $b = \beta d$ for some $\alpha, \beta \in \mathbb{Z}$. Also we can express d as a linear combination of a and b (by theorem 2.3), say,

$$d = ma + nb,$$

which implies that

$$1 = m\alpha + n\beta.$$

But this is a linear combination of m and n, equal to 1. Therefore m and n are coprime by question 2, exercises 2.1 . $\square$

7. Prove that if a is odd then $24|a(a^2 - 1)$.

Solution. We can make use of some of the arguments from the solution to question 5 above. There we showed that if a was odd then $8|a^2-1$ and so $8|a(a^2-1)$. Factorising the number in question we see that

$$a(a^2 - 1) = a(a - 1)(a + 1),$$

and we observe that one of a, $a - 1$ and $a + 1$ must be divisible by 3 (they are a triple of consecutive integers). Therefore $3|a(a^2 - 1)$ and so $24|a(a^2-1)$ as explained in the solution to question 5 above. $\square$

8. Prove that if a and b are both odd then $8|(a^2 - b^2)$.

Solution. Since a and b are both odd we can express them as

$$a = 2q + 1, \quad b = 2r + 1,$$

for some $q, r \in \mathbb{Z}$. Then

$$a^2-b^2 = (a+b)(a-b) = \big[2(q+r+1)\big]\big[2(q-r)\big] = 4(q+r+1)(q-r).$$

Now $q-r$ and $q+r$ have the same parity, i.e. they are either both even or both odd. (To see this consider the four possible cases for the parities of q and r). Therefore the pair $q-r$ and $q+r+1$ have opposite parity, i.e. one is even and the other odd. Therefore the product $(q+r+1)(q-r)$ is even, say $(q+r+1)(q-r) = 2s$, and so

$$a^2 - b^2 = 4 \times 2s = 8s,$$

and hence $a^2 - b^2$ is divisible by 8, as required. $\square$

9. Prove that for all $a \in \mathbb{Z}$, $360|\big(a^2(a^2 - 1)(a^2 - 4)\big)$.

Solution. Note that $360 = 5 \times 8 \times 9$, a product of mutually coprime factors. Using the approach used in previous questions above we shall show that each of 5,8 and 9 divides $a^2(a^2-1)(a^2-4)$, and so we can conclude that it is divisible by 360.
Notice that

$$a^2(a^2-1)(a^2-4) = a^2(a+1)(a-1)(a+2)(a-2) = (a-2)(a-1)a^2(a+1)(a+2),$$

which is a product of 5 consecutive integers, along with the extra factor of a.
In this sequence of 5 consecutive integers, one of them will be divisible by 5, and so so will their product.
One of the integers will be divisible by 4 and there will be at least one other even integer there, and so their product will be divisible by 8.
If a is divisible by 3 then 9 will divide $(a-2)(a-1)a^2(a+1)(a+2)$.
If a is not divisible by 3 then one of $a-1$ and $a-2$ will be divisible by 3, and so so will one of $a+1$ and $a+2$. Therefore the product $(a-2)(a-1)a^2(a+1)(a+2)$ will be divisible by 9.
So in all cases $a^2(a^2-1)(a^2-2)$ is divisible by 5, 8 and 9 and so will be divisible by 360, as required. □

10. Prove the following properties of the gcd,

a) If $\gcd(a,b) = \gcd(a,c) = 1$ then $\gcd(a,bc) = 1$.

Solution. Suppose that $\gcd(a,b) = \gcd(a,c) = 1$. By theorem 2.3 (or Euclidean Algorithm) we have

$$1 = am + bn, \quad 1 = ar + cs,$$

for some $m, n, r, s \in \mathbb{Z}$. We will construct a linear combination of a and bc which is equal to 1, and so we will conclude that $\gcd(a,bc) = 1$ (using question 5 exercises 2.1). Multiply both sides of $1 = am + bn$ by cs to obtain

$$cs = amcs + bncs,$$

and then use

$$cs = 1 - ar$$

to replace the cs from the left side and the first cs from the right side to obtain

$$1 - ar = am(1 - ar) + bncs,$$

which re-arranges to

$$1 = a(r + m - mar) + bc(ns).$$

This last equation is the required linear combination of a and bc equal to 1. □

b) If $\gcd(a,b) = 1$ and $c|a$ then $\gcd(c,b) = 1$.

Solution. Suppose that $\gcd(a,b) = 1$ and $c|a$. From these we get that
$$1 = am + bn, \quad a = \alpha c,$$
for some integers $m, n, \alpha \in \mathbb{Z}$. Combining these we have
$$1 = c(\alpha m) + bn,$$
a linear combination of c and b equal to 1. Hence $\gcd(c,b) = 1$. □

c) If $\gcd(a,b) = 1$ then $\gcd(ac,b) = \gcd(c,b)$.

Solution. We will show that the pairs (ac,b) and (c,b) have exactly the same common divisors, and so their greatest common divisors will be the same. Suppose that $\gcd(a,b) = 1$. Then we can write
$$1 = ma + bn,$$
for some integers $m, n \in \mathbb{Z}$. Multiplying by c and ac we then obtain
$$c = mac + bnc \ \ (*), \quad ac = ma^2c + bnca \ \ (**).$$
A relevant result we will use is property 3 from theorem 2.1, namely that a common divisor of two integers also divides any linear combination of those two integers. The two equations $(*)$ and $(**)$ provide us with c as a linear combination of ac and b, and ac as a linear combination of c and b.
Firstly, suppose d is a common divisor of ac and b. By $(*)$, d divides c, and so d is a common divisor of c and b also.
Secondly, suppose d is a common divisor of c and b. By $(**)$, d divides ac, and so d is a common divisor of ac and b also. This completes the proof. □

d) If $\gcd(a,b) = 1$ and $c|(a+b)$ then $\gcd(a,c) = \gcd(b,c) = 1$.

Solution. Suppose that $\gcd(a,b) = 1$ and $c|a+b$, i.e. $a+b = qc$, for some $q \in \mathbb{Z}$. Let $\gcd(a,c) = d$. Then we can write $a = \alpha d$ and $c = \gamma d$ for some integers $\alpha, \gamma \in \mathbb{Z}$. Notice that
$$b = (a+b) - a = qc - \alpha d = q\gamma d - \alpha d = (q\gamma - \alpha)d.$$
Therefore $d|b$ and so d is a common divisor a and b. Therefore $d|\gcd(a,b)$, by theorem 2.3, i.e. $d|1$ and so $d = 1$, as required.
A very similar argument will establish that $\gcd(b,c) = 1$ also. □

11. Suppose that a and b are coprime, show that for all $n \geq 1$, a^n and b^n are coprime.

Solution. Assume that a and b are co-prime, i.e. $\gcd(a,b) = 1$. Let $n \geq 1$. By repeatedly applying result (c) of question 10 Exercises 2.3 above we can say

$$1 = \gcd(a,b) = \gcd(a^2,b) = \cdots = \gcd(a^n,b),$$

(apply result (c) with $c = a$).
Making use of this result (c) again, but starting with the equation $1 = \gcd(a^n,b)$ we can say

$$1 = \gcd(a^n,b) = \gcd(a^n,b^2) = \cdots = \gcd(a^n,b^n),$$

(apply result (c) to $1 = \gcd(a^n,b)$ with $c = b$).
This proof could be made more rigorous using induction, but the main idea is present here. □

12. Prove that for all $n \geq 1$, if $a^n|b^n$ then $a|b$.

Solution. This result is true, but I've been unable to arrive at a straightforward proof using the results we've developed to date. We will be able to proof it using the Fundamental Theorem of Arithmetic from Chapter 3. I'd be interested to see a proof of it that doesn't somehow rerun the argument for the FTA □

13. Suppose that c is a common multiple of a and b. Prove that $\text{lcm}(a,b)|c$.

Solution. This is really just a restatement of a result which was established in the proof of theorem 2.6. We proved there that any common multiple of a and b was greater than or equal to the $\text{lcm}(a,b)$ *by showing that it was divisible by* $\text{lcm}(a,b)$. □

Exercise 3.1. Suppose the canonical forms of integers a and b are

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{s} q_i^{\beta_i}.$$

Can you write down the canonical form of $\gcd(a,b)$ and $\text{lcm}(a,b)$ in terms of this information?

Solution. This problem is asking us to characterise the canonical forms of $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in terms of the canonical forms of a and b. We should expect a nice concise characterisation/description of these here as the gcd and lcm are defined in terms of divisibility and multiplicities and the canonical form (or prime factorisation) contains all the information about divisibility and multiplicity of a number.
First we adjust the facorisation representation to

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{r} p_i^{\beta_i},$$

where now the primes $p_1, \dots, p_r$ are all the distinct primes that occur in either the factorisation of a or of b, and the exponents α_i, β_i are non-negative integers. So if $\alpha_i = 0$ this means that $p_i \not| a$, and so on.
Firstly, consider $\gcd(a, b)$. We think of building the canonical form of this prime by prime. In doing so we have to ensure that the number we are building is (1) a common divisor of a and b; (2) the greatest such common divisor. To ensure (1) we should only consider primes p that appear in the factorisations of both a and b. To ensure (2) we need to take the greatest power, p^γ, of p, such that $p^\gamma | a$ and $p^\gamma | b$. These two considerations lead us to the following expression,

$$\gcd(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}.$$

Secondly, consider $\operatorname{lcm}(a, b)$. We think of building the canonical form of this prime by prime. In doing so we have to ensure that the number we are building is (1) a common multiple of a and b; (2) the least such common multiple. To ensure (1) we need to consider primes p that appear in the factorisations of either a or b. To ensure (2) we need to take the least power, p^γ, of this prime p, such that $p^\gamma | a$ or $p^\gamma | b$. These two considerations lead us to the following expression,

$$\operatorname{lcm}(a, b) = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

□

Exercise 3.2. 1. Practice obtaining canonical forms (prime-power factorizations), for example of the following numbers

$$111;\ 1234;\ 2345;\ 111,111;\ 999,999,999.$$

Solution. Factoring integers is a hard problem, in that in general it is a case of trial and error to find the factors from the set of primes in the suitable range. This *hardness* can be exploited to design cryptographic systems, as you shall see later in the unit. Anyhow, for low magnitude integers, computers can provide the factorisation in a reasonable amount of time. You could use the MATLAB (or GNU Octave) `factor` command as follows: □

```
octave:19> factor(111)
ans =

    3   37

octave:20> factor(1234)
ans =

      2   617

octave:21> factor(2345)
ans =

    5    7   67

octave:22> factor(111111)
ans =

    3    7   11   13   37

octave:23> factor(999999999)
ans =

        3         3         3         3        37    333667

octave:24>
```

2. Find some counter-examples to the claim:

$$\forall\, a, b, c \in \mathbb{Z} \quad a|bc \Rightarrow \big(a|b \text{ or } a|c\big).$$

Can you explain how these counter-examples work in terms of the canonical forms of a, b, c?

Solution. A counter-example is provided by $a = 6$, $b = 3$ and $c = 4$. In terms of canonical forms, if $a|bc$ then the prime factorization of a must be contained in the prime factorization of bc. However as long as a is composite (i.e. has more than a single prime factor), its prime factorization can be split so that one part is contained in that of b and the remaining part is contained in that of c. In this way we can have $a|bc$ while also having $a \not| b$ and $a \not| c$. □

3. Consider the canonical form
$$n = \prod_{i=1}^{r} p_i^{\alpha_i}.$$
Prove that n is a square if and only if each α_i is even, $i = 1, \ldots r$.

Solution. Suppose that n is a square, i.e. $n = m^2$ for some $m \in \mathbb{Z}$. Let the canonical form of m be
$$m = \prod_{i=1}^{s} q_i^{\beta_i}.$$
Therefore the canonical form of $m^2 = n$ would be
$$m^2 = \prod_{i=1}^{s} q_i^{2\beta_i} = n.$$
Now by the uniqueness of canonical forms we must have $r = s$, $p_i = q_i$ and $\alpha_i = 2\beta_i$ for each $i = 1, \ldots, r$. Hence, each α_i is even, as required.
On the other hand if each α_i is even, say $\alpha_i = 2\gamma_i$, then $n = a^2$, where a is the integer with canonical form
$$a = \prod_{i=1}^{r} p_i^{\gamma_i}.$$
□

4. Formulate, and prove, the corresponding result for the mth root of n.

Solution. Let $n \in \mathbb{Z}$, with canonical form $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. The corresponding result is that $\sqrt[m]{n} \in \mathbb{Z}$ iff $\forall\, i,\ m|\alpha_i$. The proof of this proceeds in exactly the same manner as the previous one for square roots. □

5. Show that the only prime number of the form $n^3 - 1$ is 7.

Solution. Consider the general factorisation result
$$a^m - b^m = (a - b) \sum_{i=0}^{m-1} a^{m-1-i} b^i,$$
which holds for any integer $m \geq 1$. Applying this to $n^3 - 1 = n^3 - 1^3$ we get
$$n^3 - 1 = (n - 1)(n^2 + n + 1).$$
When the integer n is strictly greater than 2, both these factors are strictly greater than 1 and so $n^3 - 1$ is composite. When $n = 2$, $n^3 - 1 = 7$, which is prime. □

6. Consider the possible outcomes from performing integer division of a prime p with 6, i.e. $p = 6q+?$. Use the results of this analysis to prove that $p^2 + 2$ is never prime, for any prime $p \geq 5$.

Solution. Let $p \geq 5$ be a prime. Attempting to divide p by 6 will lead to

$$p = 6q + r, \quad r = 1 \text{ or } 5.$$

The remainders $r = 0, 2, 3$, or 4 can not occur as they would imply that p is divisible by, respectively, $6, 2, 3$ or 2, whereas p is prime. So $p^2 + 2$ is one of

$$p^2 + 2 = (6q + 1)^2 + 2 = 36q^2 + 12q + 3 = (12q^2 + 4q + 1) \times 3,$$

or

$$p^2 + 2 = (6q + 5)^2 + 2 = 36q^2 + 60q + 27 = (12q^2 + 20q + 9) \times 3.$$

In both cases $p^2 + 2$ is divisible by 3 as shown, and so cannot be prime. $\square$

7. Prove that for p a prime, if $p|a^n$ then $p^n|a^n$.

Solution. This can be shown relatively straightforwardly by applying corollary to Euclid's Lemma (Lemma 3.4). If $p|a^n$ then $p|a$. Say $a = rp$, for some $r \in \mathbb{Z}$. Then $a^n = r^n p^n$, which shows that $p^n|a^n$, as required. $\square$

8. Suppose that $p, q \geq 5$ are prime. Prove that $p^2 - q^2$ is divisible by 24.

Solution. Let $p, q \geq 5$ be primes. As before, to prove such a divisibility result we can make use of question 5 from Exercises 2.1. This says that if $a|c$ and $b|c$ and $\gcd(a, b) = 1$ then $ab|c$. So we consider 24 as $24 = 3 \times 8$. We shall endeavour to show that $3|p^2 - q^2$ and $8|p^2 - q^2$.
Firstly, dividing by 3 will give $p = 3n + r$ and $q = 3m + s$, where the remainders r and s can only take the values 1 or 2 (since p and q are prime and greater than 3). We then have

$$\begin{aligned} p^2 - q^2 &= 9n^2 + 6nr + r^2 - (9m^2 + 6mr + s^2) \\ &= 3(3n^2 + 2nr - 3m^2 - 3mr) + r^2 - s^2. \end{aligned}$$

Considering all four possibilities for the values of r and s we see that $r^2 - s^2$ will takes the values 0, -3 or 3. Thus in all cases $3|p^2 - q^2$.
Secondly, p, q must both be odd, as they are primes greater than 2. So $p = 2n + 1$ and $q = 2m + 1$ for some $m, n \in \mathbb{Z}$. Then

$$\begin{aligned} p^2 - q^2 &= 4n^2 + 4n - 4m^2 - 4m \\ &= 4n(n + 1) - 4m(m + 1). \end{aligned}$$

But the integers $n(n + 1)$ and $m(m + 1)$ must both be even, as they are each the product of a pair of consecutive integers. Say $n(n+1) = 2n'$ and $m(m+1) = 2m'$, for some $n', m' \in \mathbb{Z}$. But then

$$p^2 - q^2 = 8(n' - m'),$$

and so $8|p^2 - q^2$, as required. □

9. Is $n^4 + 4$ ever a prime, where $n > 1$?

Solution. Clearly, when $n = 1$ it is prime. So assume that $n > 1$. It is not immediately clear how to proceed with this. There is no straightforward general factorisation result that might apply to the expression $n^4 + 4$ that I am aware of. In a situation like this, maybe some numerical investigations will provide some clues. So let us get `GNU Octave` (or `Matlab` or any other suitable software) to show us the integers $n^4 + 4$ for $n = 1, \ldots, 30$ say, □

```
>>> for n=1:30
n,n^4+4
end

>>>n =  1
ans =  5
n =  2
ans =  20
n =  3
ans =  85
n =  4
ans =  260
```

```
n =  5
ans =  629
n =  6
ans =  1300
n =  7
ans =  2405
n =  8
ans =  4100
n =  9
ans =  6565
n =  10
ans =  10004
n =  11
ans =  14645
n =  12
ans =  20740
n =  13
ans =  28565
n =  14
ans =  38420
n =  15
ans =  50629
n =  16
ans =  65540
n =  17
ans =  83525
n =  18
ans =  104980
n =  19
ans =  130325
n =  20
ans =  160004
n =  21
ans =  194485
n =  22
ans =  234260
n =  23
ans =  279845
n =  24
ans =  331780
n =  25
ans =  390629
n =  26
ans =  456980
n =  27
ans =  531445
n =  28
ans =  614660
n =  29
ans =  707285
```

```
n =  30
ans =  810004
>>>
```

Solution. (contd.) Looking at these we first notice that most of the numbers end in 0 or 5. So these will certainly not be prime as they will be divisible by 5. Examining further we notice that for every n that is not a multiple of 5, $n^4 + 4$ seems to be a multiple of 5. Let's now focus our attention on the multiples of 5. $\square$

```
>>> for n=1:20
5*n,(5*n)^4+4
end

>>>ans =  5
ans =  629
ans =  10
ans =  10004
ans =  15
ans =  50629
ans =  20
ans =  160004
ans =  25
ans =  390629
ans =  30
ans =  810004
ans =  35
ans =  1500629
ans =  40
ans =  2560004
ans =  45
ans =  4100629
ans =  50
ans =  6250004
ans =  55
ans =  9150629
ans =  60
ans =  12960004
ans =  65
ans =  17850629
ans =  70
ans =  24010004
ans =  75
ans =  31640629
ans =  80
ans =  40960004
ans =  85
ans =  52200629
ans =  90
ans =  65610004
```

```
ans =  95
ans =  81450629
ans =  100
ans =  100000004
>>>
```

Solution. These are alternating between even and odd. The even ones are naturally composite. The odd ones all end in the digits 629. Interesting. Let's check the prime factorizations of some of these odd ones. □

```
>>> for n=1:10
5*(2*n+1),(5*(2*n+1))^4+4, factor((5*(2*n+1))^4+4)
end

>>>ans =  15
ans =  50629
ans =

   197   257

ans =  25
ans =  390629
ans =

   577   677

ans =  35
ans =  1500629
ans =

     13     89   1297

ans =  45
ans =  4100629
ans =

    13    29    73   149

ans =  55
ans =  9150629
ans =

   2917   3137

ans =  65
ans =  17850629
ans =

     17    241   4357
```

```
ans =  75
ans =  31640629
ans =

     53    109   5477

ans =  85
ans =  52200629
ans =

     13    569   7057

ans =  95
ans =  81450629
ans =

     13    709   8837

ans =  105
ans =  121550629
ans =

    17    29   373   661

>>>
```

Solution. They all seem to be coming up as composite. But there don't seem to be any common primes coming up all the time.
Well these numerical investigations seem to suggest that $n^4 + 4$ is composite for $n > 1$, and we've made some interesting observations on the (some of the) factors of $n^4 + 4$ for the various cases with respect to dividing n by 5. Of course none of this amounts to a proof of anything beyond the composite nature of the particular integers $n^4 + 4$ that have been encountered here.
Since we've got the computer running now. Let's see if it can tell us anything about the factors of n^4+4 for the various cases of n with respect to dividing it by 5 mentioned above. Using `Matlab` we define a ymbolic variable `n` and examine the various cases mentioned above. □

```
>> n=sym('n')

n =

n


>> factor((5*n+1)^4+4)
```

```
ans =

5*(5*n^2+4*n+1)*(25*n^2+1)


>> factor((5*n+2)^4+4)

ans =

5*(25*n^2+10*n+2)*(5*n^2+6*n+2)


>> factor((5*n+3)^4+4)

ans =

5*(5*n^2+4*n+1)*(25*n^2+40*n+17)


>> factor((5*n+4)^4+4)

ans =

5*(5*n^2+6*n+2)*(25*n^2+50*n+26)


>> factor((5*2*n)^4+4)

ans =

4*(50*n^2-10*n+1)*(50*n^2+10*n+1)


>> factor((5*(2*n+1))^4+4)

ans =

(100*n^2+120*n+37)*(100*n^2+80*n+17)


>>
```

Solution. These cases cover all possibilities and so demonstrate that the integer $n^4 + 4$ is composite for $n > 1$. $\square$

10. Prove that if $2^n - 1$ is prime then so is n.

Solution. Trying to prove this directly seems hard at first. If $2^n - 1$ is prime then that doesn't give us much many handles to get at n directly. So maybe let's think about it differently. We could use a proof by contradiction. Or equivalently, let us prove the contrapositive instead. Remember that the *contrapositive* of an implication $A \Rightarrow B$ is the statement $\neg B \Rightarrow \neg A$. A statement and its contrapositive are logically equivalent, i.e. they are either both true or both false.
The contrapositive of the result in question is the statement: If n is composite then so is $2^n - 1$ composite. This seems more approachable to try and prove directly, as we immediately can introduce factors of n and see what the consequences are.
So assume that n is composite, i.e. we can write $n = rs$ for some $r, s \in \mathbb{Z}$ and $r, s > 1$. We can produce a factorisation for $2^n - 1$ as follows using a standard factorisation for differences of powers (recalled earlier in question 5 above):

$$\begin{aligned} 2^n - 1 &= 2^{rs} - 1 \\ &= (2^r)^s - 1^s \\ &= (2^r - 1) \sum_{i=0}^{s-1} (2^r)^{s-1-i} . \end{aligned}$$

Is this a genuine factorisation of $2^n - 1$? Yes, both factors are strictly greater than 1 as $r, s > 1$. So this shows that $2^n - 1$ is composite. So we have proved the appropriate contrapositive, so we can concluded that the result in the question is true. □

11. Prove that if $2^n + 1$ is prime then n is a power of 2.

Solution. Similar introductory remarks apply here as in the previous question. So let us prove the contrapositive, namely, that if n is not a power of 2 then $2^n + 1$ is composite.
Suppose the integer n is not a power of 2. This means that we can factorise it as $n = 2^r s$, for some $r, s \in \mathbb{Z}$ where $r \geq 0$, $s > 1$ and s is odd. Now we consider $2^n + 1$ and find a neat way to exploit the general factorisation result used in the previous question and question 5.

$$\begin{aligned}
2^n + 1 &= 2^{2^r s} + 1 \\
&= \left(2^{2^r}\right)^s - (-1)^s, \text{ (remember } s \text{ is odd)} \\
&= \left[2^{2^r} - (-1)\right] \left[\sum_{i=0}^{s-1} \left(2^{2^r}\right)^{s-1-i} (-1)^i\right] \\
&= \left[2^{2^r} + 1\right] \left[\sum_{i=0}^{s-1} \left(2^{2^r}\right)^{s-1-i} (-1)^i\right]
\end{aligned}$$

We just need to be sure that this is a genuine factorisation. Well since $r \geq 0$ the first factor $2^{2^r} + 1 > 1$ and since $s > 1$, $2^{2^r} + 1 < 2^{2^r s} + 1 = 2^n + 1$. So the factorisation is genuine and so the contrapositive, and hence the original result, has been proved. $\square$

12. Recall the Fibonacci sequence $\{f_n\}_{n=1}^{\infty}$ defined by

$$f_1 = f_2 = 1, \quad f_{n+1} = f_n + f_{n-1}.$$

Prove that $\gcd(f_n, f_{n+1}) = 1$ for every $n \geq 1$.

Solution. Since this is an infinite sequence of results, indexed by the positive integers $n \geq 1$, we should immediately think of induction as a proof strategy here.
$\gcd(f_1, f_2) = \gcd(1, 1) = 1$, so the result is true for $n = 1$. Assume that the result holds for and integer $k \geq 1$, i.e. that $\gcd(f_k, f_{k+1}) = 1$. We need to establish that $\gcd(f_{k+1}, f_{k+2}) = 1$.

$$\begin{aligned}\gcd(f_{k+1}, f_{k+2}) &= \gcd(f_{k+1}, f_{k+1} + f_k), \text{ by definition of } f_{k+2} \\ &= \gcd(f_{k+1}, f_k), \text{ property of gcd (*see below)} \\ &= 1, \text{ by induction assumption above.}\end{aligned}$$

So by the principle of induction, $\gcd(f_n, f_{n+1}) = 1$ for all $n \geq 1$.
(*gcd result)
Here we have made use of the following result about gcd

$$\gcd(a, b) = \gcd(a, a + b).$$

This follows from the fact that the pairs (a, b) and $(a, a + b)$ have exactly the same common divisors. For if $d|a$ and $d|b$, then $d|a + b$ since $a + b$ is a linear combination of a and b (theorem 2.1), and so d is a common divisor of a and $a+b$. In addition, if $d|a$ and $d|a+b$ then $d|b$ since $b = (a + b) - a$, a linear combination of a and $a + b$, and so d is a common divisor of a and b. □

Exercise 4.1. In the following let $a, b, a', b', c \in \mathbb{Z}$ with $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Prove that each of the following holds:

1. $a + b \equiv a' + b' \pmod{m}$,

   Solution. Proved in lectures, see 'chalk board' pages below □

2. $ab \equiv a'b' \pmod{m}$,

   Solution. Proved in lectures, see 'chalk board' pages below □

How does $\equiv \pmod{m}$ interact with $+, \times$ on $\mathbb{Z}$?

Let $a \equiv a'$, $b \equiv b' \pmod{m}$

1. $a + b \equiv a' + b' \pmod{m}$

<u>Pf</u> We know $a \equiv a'$, $b \equiv b' \pmod{m}$

$\Rightarrow m \mid a - a'$, $m \mid b - b'$

$\Rightarrow m \mid a - a' + b - b'$, by Th 2.1 part (3)

$\Rightarrow m \mid (a+b) - (a'+b')$

$\Rightarrow a + b \equiv a' + b' \pmod{m}$

2. $ab \equiv a'b' \pmod{m}$

<u>Pf</u>. We know

$m \mid a - a'$, $m \mid b - b'$

$$ab - a'b' = (a-a')(b-b') - 2a'b' + a'b + b'a.$$

$$= (a-a')(b-b') + a'(b-b') + b'(a-a').$$

$\Rightarrow m \mid ab - a'b'$, since RHS is a lin. comb. of things div. by m

$\Rightarrow ab \equiv a'b' \pmod{m}$

Say $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_i \in \mathbb{Z}$.

$ac = bc$ $\quad a, b, c \in \mathbb{Z}$

$\Rightarrow a = b$, provided $c \neq 0$.

$a\cancel{c} \equiv b\cancel{c} \pmod{m}$?

modulus

$ac \equiv bc \pmod{m}$

$\Rightarrow a \equiv b \pmod{\frac{m}{d}}$

where $d = \gcd(c, m)$.

---

eg.

$45 \equiv 75 \pmod{5}$

$15 \cdot 3 \equiv 25 \cdot 3 \pmod{5}$

3. $\forall c \in \mathbb{Z}\ a + c \equiv a' + c \pmod{m}$,

Solution. This comes out no trouble at all, for we simply observe that

$$(a + c) - (a' + c) = a - a',$$

and so the result immediately follows from the fact that $a \equiv a' \pmod{m}$. □

4. $\forall c \in \mathbb{Z}\ ac \equiv a'c \pmod{m}$,

Solution. To establish the required congruence we need to examine the difference

$$ac - a'c = (a - a')c.$$

Now since $m|a - a'$ (as $a \equiv a' \pmod{m}$) we can conclude that $m|(a - a')c$ and hence that $ac \equiv a'c \pmod{m}$. □

5. $\forall k \in \mathbb{Z}$ such that $k \geq 0,\ a^k \equiv (a')^k \pmod{m}$,

Solution. This is an application of question 2 above. The base case $k = 0$ is true as both sides of the congruence evaluate to 1. Assuming it is true for $k = j$, for some $j \geq 0$,

$$a^j \equiv (a')^j \pmod{m}.$$

Now since $a \equiv a' \pmod{m}$ we can multiply the left-hand side by a and the right-hand side by a' and invoke question 2 (with $b = a^j$ and $b' = (a')^j$) to conclude that

$$a^{j+1} \equiv (a')^{j+1} \pmod{m}.$$

So by induction the congruence holds for all $k \geq 0$. □

6. $f(a) \equiv f(a') \pmod{m}$, where f is any polynomial with integer coefficients.

Solution. Let f be a polynomial (of degree N) with integer coefficients, which we could write as

$$f(x) = \sum_{j=0}^{N} \alpha_j x^j.$$

We then consider $f(a)$ and $f(a')$,

$$f(a) = \sum_{j=0}^{N} \alpha_j a^j, \quad f(a') = \sum_{j=0}^{N} \alpha_j (a')^j.$$

The previous question 5 established that for all j

$$a^j \equiv (a')^j \pmod{m}.$$

Then applying question 4 to this gives for all j

$$\alpha_j a^j \equiv \alpha_j (a')^j \pmod{m}.$$

Then repeated applications of question 1 allows us to add all the terms of the polynomials together while still preserving the congruence. So we have shown that

$$\sum_{j=0}^{N} \alpha_j a^j \equiv \sum_{j=0}^{N} \alpha_j (a')^j \pmod{m},$$

as required. □

Exercise 4.2. The following exercises describe more properties of the congruence relation as well as other results about dealing with large integers.

1. Prove that if $a \equiv b \pmod{n}$ and $m|n$ then $a \equiv b \pmod{m}$.

Solution. Suppose that $a \equiv b \pmod{n}$ and $m|n$, i.e. $n|(a-b)$ and $n = n'm$ for some $n' \in \mathbb{Z}$. Since $n|a-b$ we have

$$a - b = rn = rn'm,$$

for some $r \in \mathbb{Z}$. This last equation shows that $m|a-b$ and so $a \equiv b \pmod{m}$. □

2. Prove that if $a \equiv b \pmod{n}$ and $d|a$, $d|b$ and $d|n$ then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

Solution. Writing out the consequences of the definitions this proof falls out easily. We have $a \equiv b \pmod{n}$, i.e. $n|a-b$, i.e.

$$a - b = rn$$

for some integer r. Assuming that a, b and n are all divisible by n we can divide both sides of this equation by d to get

$$\frac{a}{d} - \frac{b}{n} = r\frac{n}{d},$$

where we note that the fractions shown are actually all integers. Or in other words $\frac{n}{d}$ divides $\frac{a}{d} - \frac{b}{d}$, and so $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ as required. □

3. Find some counter-examples to the claim

$$\text{“}a^2 \equiv b^2 \pmod{n} \Rightarrow a \equiv b \pmod{n}\text{”}.$$

Solution. The difference $a^2 - b^2$ has the well-known factorization

$$a^2 - b^2 = (a+b)(a-b),$$

so counterexamples can be constructed by choosing a and b so that $a + b$ is divisible by the modulus n but $a - b$ is not. For instance, with the modulus $n = 15$ we could choose $a = 9$ and $b = 6$. Now $9 \not\equiv 6 \pmod{15}$ but

$$9^2 - 6^2 = 81 - 36 = 45 = 3 \times 15$$

and so $9^2 \equiv 6^2 \pmod{15}$. □

4. Prove that if $a \equiv b \pmod{n}$ then $\gcd(a, n) = \gcd(b, n)$.

Solution. Suppose that $a \equiv b \pmod{n}$, i.e. $a - b = rn$ for some integer r. Consider the two pairs (a, n) and (b, n). If d is a common divisor of a and n since $b = a - rn$ we also have $d|b$, as b is a linear combination of a and n. So d must also be a common divisor of b and n. Similarly we can argue that a common divisor of b and n must also be a common divisor of a and n. So both pairs (a, n) and (b, n) have the same common divisors, and so their gcds must be equal. □

5. What is the remainder left when 2012^{2012} is divided by 5?

Solution. We perform calculations on the congruence classes using the properties we have established. $2012 \equiv 2 \pmod{5}$ and notice that $2^4 \equiv 1 \pmod{5}$. Now note that $2012 = 4 \times 503$ so that

$$2012^{2012} \equiv 2^{4\times 503} = \left(2^4\right)^{503} \equiv 1^{503} = 1, (\text{mod } 5).$$

So the remainder left after 2012^{2012} is divided by 5 is 1. □

6. What remainders are left when 2^{50} is divided by 7? When 41^{65} is divided by 7?

Solution. Similar approach to the previous question. Firstly, $2^3 \equiv 1 \pmod 7$ and so

$$2^{50} = \left(2^3\right)^{16} 2^2 \equiv 1^{16} 2^2 = 4, (\bmod\ 7).$$

Secondly, $41 \equiv -1 \pmod 7$ and so

$$41^{65} \equiv (-1)^{65} = -1, (\bmod\ 7).$$

□

7. Prove that is a is odd then

$$\forall\, n \geq 1\ a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

Solution. The form of this statement makes it a likely candidate for proof by induction. The base case is when $n = 1$ where it states that $a^2 \equiv 1 \pmod 8$. There are only 4 congruence classes of odd integers modulo 8. They are the congruence classes of 1, 3, 5 and 7. So the odd integer a is congruent to one of these modulo 8. By checking we confirm that all four of these satisfy $a^2 \equiv 1 \pmod 8$. So the base case is true.
Assume now that the results holds when $n = k$, where $k \geq 1$. We wish to show that $a^{2^{k+1}}$ is congruent to 1 modulo 2^{k+3}. This amounts to showing that 2^{k+3} divides $a^{2^{k+1}} - 1$. We observe that

$$a^{2^{k+1}} - 1 = \left(a^{2^k}\right)^2 - 1^2 = \left(a^{2^k} + 1\right)\left(a^{2^k} - 1\right).$$

So we have expressed $a^{2^{k+1}} - 1$ as a product of two factors. The first of these we know to be an even number, since a is odd. The second of these is covered by the induction hypothesis, so we know it is divisible by 2^{k+2}. So we have, for some integers r, s

$$a^{2^{k+1}} - 1 = 2r \times 2^{k+2} s = rs2^{k+3},$$

which establishes the result for $n = k + 1$.
So by induction we conclude that the result holds for all $n \geq 1$. □