Number Theory Exercises 2

Jason Sass

July 17, 2023

Divisibility and greatest common divisor

Exercise 1. Let $a, b \in \mathbb{Z}$.
Then $a > b$ implies $a \nmid b$ is false.

Proof. Observe that $1 > 0$ and $1|0$. □

Exercise 2. Let $a, b, c \in \mathbb{Z}$.
If $a + b = c$ and $d|a$ and $d|c$, then $d|b$.

Proof. Suppose $a + b = c$ and $d|a$ and $d|c$.
Since $a+b = c$, then $b = c-a = -a+c = (-1)a+(1)c$ is a linear combination of a and c.
Since $d|a$ and $d|c$, then d divides any linear combination of a and c.
In particular, d divides b, so $d|b$. □

Exercise 3. Let x, y, z, w be integers.
If $3x + 81y + 6z + 363 = w$, then $3|w$.

Proof. Since $w = 3x+81y+6z+363 = 3(x+27y+2z+121)$ and $x+27y+2z+121$ is an integer, then 3 divides w. □

Proof. Since $3|3$ and $3|81$ and $3|6$ and $3|363$, then 3 divides any linear combination of $3, 81, 6, 363$.
Since w is a linear combination of $3, 81, 6, 363$, then this implies 3 divides w, so $3|w$. □

Exercise 4. Let x, y be integers.
If $3x^2 + 15xy + 5y^2 = 0$, then $3|5y^2$ and $5|3x^2$.

Proof. Suppose $3x^2 + 15xy + 5y^2 = 0$.
Then $3x^2 = -15xy - 5y^2$ and $5y^2 = -3x^2 - 15xy$.
Since $3|-3$ and $3|-15$, then 3 divides any linear combination of -3 and -15.
Since $5y^2$ is a linear combination of -3 and -15, then this implies $3|5y^2$.
Since $5|-15$ and $5|-5$, then 5 divides any linear combination of -15 and -5.
Since $3x^2$ is a linear combination of -15 and -5, then this implies $5|3x^2$. □

Exercise 5. Let $n_1, n_2, ..., n_k \in \mathbb{Z}$.

If $N = n_1 * n_2 * * * n_k + 1$, then $\gcd(n_i, N) = 1$ for $i = 1, 2, ..., k$.

Proof. Suppose $N = n_1 * n_2 * * * n_k + 1$.

Then $1 = N - n_1 * n_2 * * * n_k = (1) * N - n_1 * n_2 * * * n_k$.

Since 1 is a linear combination of n_1 and N and any linear combination of n_1 and N is a multiple of $\gcd(n_1, N)$, then 1 is a multiple of $\gcd(n_1, N)$, so $\gcd(n_1, N)$ divides 1.

The only positive integer that divides 1 is 1, so this implies $\gcd(n_1, N) = 1$.

Similar reasoning shows that $\gcd(n_2, N) = 1$ and ... $\gcd(n_k, N) = 1$. □

Exercise 6. Let $d \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$.

Then $\gcd(d, nd) = d$.

Proof. Since every integer divides itself, then $d|d$.

Since d divides any multiple of d, then $d|nd$.

Therefore, d is a common divisor of d and nd.

Let c be any common divisor of d and nd.

Then $c|d$ and $c|nd$, so $c|d$.

Hence, any common divisor of d and nd divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of d and nd and any common divisor of d and nd divides d, then $d = \gcd(d, nd)$. □

Exercise 7. Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$.

If $a|b$ and $b|a$, then $a = b$ or $a = -b$.

Proof. Suppose $a|b$ and $b|a$.

Then $b = ak_1$ and $a = bk_2$ for some integers k_1 and k_2.

Thus, $b = (bk_2)k_1 = b(k_1k_2)$, so $b(k_1k_2) - b = 0$.

Hence, $b(k_1k_2 - 1) = 0$.

Either $b = 0$ or $b \neq 0$.

We consider these cases separately.

Case 1: Suppose $b = 0$.

Since $b|a$, then $0|a$, so $a = 0k_3 = 0$ for some integer k_3.

Hence, $a = 0 = b$, so $a = b$.

Case 2: Suppose $b \neq 0$.

Then $k_1k_2 - 1 = 0$, so $k_1k_2 = 1$.

Since k_1 and k_2 are integers such that $k_1k_2 = 1$, then either $k_1 = k_2 = 1$ or $k_1 = k_2 = -1$.

Hence, either $b = a(k_1) = a(1) = a$ or $b = a(k_1) = a(-1) = -a$, so either $b = a$ or $b = -a$.

Therefore, either $a = b$ or $a = -b$. □

Exercise 8. Let $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}$.

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

Proof. Suppose $a|b$.

Since every integer divides itself, then $a|a$.

Since $a|a$ and $a|b$, then a is a common divisor of a and b.

Let c be any common divisor of a and b.

Then $c|a$ and $c|b$, so $c|a$.

Hence, any common divisor of a and b divides a.

Since $a \in \mathbb{Z}^+$ and a is a common divisor of a and b, and any common divisor of a and b divides a, then $a = \gcd(a, b)$. □

Exercise 9. Let $x \in \mathbb{R}$ and $a, b \in \mathbb{Z}$.

I. If $x^2 + ax + b = 0$ has an integer root, then the root divides b.

II. If $x^2 + ax + b = 0$ has a rational root, then the root is an integer.

Proof. We prove I.

Suppose the equation $x^2 + ax + b = 0$ has an integer root.

Let r be an integer root of $x^2 + ax + b = 0$.

Then $r \in \mathbb{Z}$ and $r^2 + ar + b = 0$, so $b = -r^2 - ar = r(-r - a)$.

Since $-r - a \in \mathbb{Z}$, then r divides b. □

Proof. We prove II.

Suppose the equation $x^2 + ax + b = 0$ has a rational root.

Let q be a rational root of $x^2 + ax + b = 0$.

Then $q \in \mathbb{Q}$ and $q^2 + aq + b = 0$.

Since $q \in \mathbb{Q}$, then there exist integers r, s with $s \neq 0$ such that $q = \frac{r}{s}$.

Assume q is in lowest terms. That is, assume $\gcd(r, s) = 1$, so $1 = \gcd(s, r)$.

Since $(\frac{r}{s})^2 + a * \frac{r}{s} + b = 0$, then $r^2 + ars + bs^2 = 0$, so $r^2 = -ars - bs^2 = s(-ar - bs)$.

Since $s|s(-ar - bs)$, then s divides r^2.

Since $s|r^2$ and $\gcd(s, r) = 1$, then $s|r$.

Thus, $r = st$ for some integer t, so $q = \frac{r}{s} = \frac{st}{s} = t$.

Therefore, q is an integer. □

Exercise 10. Let $a, b \in \mathbb{Z}$.

For every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c|\gcd(a, b)$.

Proof. Let $c \in \mathbb{Z}$ such that $c|a$ and $c|b$.

Then c is a common divisor of a and b.

By definition of gcd, any common divisor of a and b must divide $\gcd(a, b)$.

Therefore, c divides $\gcd(a, b)$. □

Exercise 11. Let a and b be nonzero integers.

If there exist integers r and s such that $ar+bs = 1$, then a and b are relatively prime.

Proof. Suppose there exist integers r and s such that $ar + bs = 1$.

Then $1 = ra + sb$ is a linear combination of a and b.

Since any common divisor of a and b divides any linear combination of a and b, then $\gcd(a, b)$ divides 1.

The only positive integer that divides 1 is 1.

Since $\gcd(a, b)$ is a positive integer, then this implies $\gcd(a, b) = 1$.

Therefore, a and b are relatively prime. □

Exercise 12. Let $a, b, c \in \mathbb{Z}$.

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

Proof. Suppose $\gcd(a, b) = 1$ and $c|a$.

Since $\gcd(a, b) = 1$, then $ma + nb = 1$ for some integers m, n.

Since $c|a$, then $a = ck$ for some integer k.

Thus, $1 = ma + nb = m(ck) + nb = m(kc) + nb = (mk)c + nb$ is a linear combination of c and b.

Since any linear combination of c and b is a multiple of $\gcd(c, b)$, then 1 is a multiple of $\gcd(c, b)$, so $\gcd(c, b)$ divides 1.

The only positive integer that divides 1 is 1, so $\gcd(c, b) = 1$. □

Proof. Suppose $\gcd(a, b) = 1$ and $c|a$.

Since 1 divides every integer, then $1|c$ and $1|b$, so 1 is a common divisor of c and b.

Let d be any common divisor of c and b.

Then $d|c$ and $d|b$.

Since $d|c$ and $c|a$, then $d|a$.

Since $\gcd(a, b) = 1$, then $ma + nb = 1$ for some integers m and n.

Since $d|a$ and $d|b$, then d divides any linear combination of a and b, so d divides $ma + nb = 1$,

Hence, $d|1$.

Therefore, any common divisor of c and b divides 1.

Since 1 is a common divisor of c and b and any common divisor of c and b divides 1, then by definition of gcd, $1 = \gcd(c, b)$. □

Exercise 13. Let $a, b, d \in \mathbb{Z}$.

If $d|a$ and $d|b$, then $d^2|ab$.

Proof. Suppose $d|a$ and $d|b$.

Then $a = dk_1$ and $b = dk_2$ for some integers k_1 and k_2.

Hence, $ab = (dk_1)(dk_2) = d^2(k_1k_2)$.

Since $k_1k_2 \in \mathbb{Z}$, then this implies $d^2|ab$. □

Exercise 14. Let $a, b, c, d \in \mathbb{Z}$.

If $c|ab$ and $\gcd(c, a) = d$, then $c|db$.

Proof. Suppose $c|ab$ and $\gcd(c,a) = d$.

Since $\gcd(c,a) = d$, then $d = xc + ya$ for some integers x and y.

Hence, $db = (xc + ya)b = xcb + yab = (xb)c + yab$ is a linear combination of c and ab.

Since $c|c$ and $c|ab$, then c divides any linear combination of c and ab, so $c|db$. □

Exercise 15. Let $a, b \in \mathbb{Z}$.

Disprove: If $a \not| b$, then $\gcd(a,b) = 1$.

Proof. Let $a = 4$ and $b = 10$.

Then $4 \not| 10$, but $\gcd(4,10) = 2 \neq 1$. □

Exercise 16. Let $a, b, d \in \mathbb{Z}$.

If d is odd and $d|(a+b)$ and $d|(a-b)$, then $d|\gcd(a,b)$.

Proof. Suppose d is odd and $d|(a+b)$ and $d|(a-b)$.

Since $d|(a+b)$ and $d|(a-b)$, then d divides the sum $(a+b)+(a-b) = 2a$ and d divides the difference $(a+b)-(a-b) = 2b$, so $d|2a$ and $d|2b$.

Since d is odd, then $2 \not| d$, so $\gcd(d,2) = 1$.

Since $d|2a$ and $\gcd(d,2) = 1$, then we know $d|a$.

Since $d|2b$ and $\gcd(d,2) = 1$, then we know $d|b$.

Hence, d divides any linear combination of a and b.

Since $\gcd(a,b)$ is the least positive linear combination of a and b, then this implies d divides $\gcd(a,b)$.

Therefore, $d|\gcd(a,b)$. □

Exercise 17. Let $a, b, c, d, p \in \mathbb{Z}$.

If $p|(10a - b)$ and $p|(10c - d)$, then $p|(ad - bc)$.

Proof. Suppose $p|(10a - b)$ and $p|(10c - d)$.

Since $p|(10a - b)$, then p divides any multiple of $10a - b$, so $p|c(10a - b)$.

Hence, $p|(10ac - bc)$.

Since $p|(10c - d)$, then p divides any multiple of $10c - d$, so $p|a(10c - d)$.

Hence, $p|(10ac - ad)$.

Thus, p divides the difference $(10ac - bc) - (10ac - ad) = 10ac - bc - 10ac + ad = ad - bc$.

Therefore, $p|(ad - bc)$. □

Exercise 18. Let $a, b, c \in \mathbb{Z}$.

Then $\gcd(a,c) = \gcd(b,c) = 1$ iff $\gcd(ab,c) = 1$.

Proof. Suppose $\gcd(a,c) = \gcd(b,c) = 1$.

Since $\gcd(a,c) = 1$, then $m_1 a + n_1 c = 1$ for some integers m_1 and n_1.

Since $\gcd(b,c) = 1$, then $m_2 b + n_2 c = 1$ for some integers m_2 and n_2.

Thus, $b = 1b = (m_1 a + n_1 c)b = m_1 ab + n_1 bc$, so $m_2(m_1 ab + n_1 bc) + n_2 c = 1$.

Hence, $1 = m_1 m_2 ab + m_2 n_1 bc + n_2 c = (m_1 m_2)(ab) + (m_2 n_1 b + n_2)c$.

Since there exist integers $m_1 m_2$ and $m_2 n_1 b + n_2$ such that $(m_1 m_2)(ab) + (m_2 n_1 b + n_2)c = 1$, then $\gcd(ab,c) = 1$. □

Proof. Conversely, suppose $\gcd(ab, c) = 1$.

Then $xab + yc = 1$ for some integers x and y.

Hence, $1 = xab + yc = (xb)a + yc = (ax)b + yc$.

Since there exist integers xb and y such that $(xb)a+yc = 1$, then $\gcd(a, c) = 1$.

Since there exist integers ax and y such that $(ax)b+yc = 1$, then $\gcd(b, c) = 1$.

Therefore, $\gcd(a, c) = \gcd(b, c) = 1$. □

Exercise 19. If $10|(3^m + 1)$ for some integer m, then $10|(3^{m+4n} + 1)$ for all $n \in \mathbb{Z}^+$.

For which m does $10|(3^m + 1)$?

Proof. □

Theorem 20. *Let S be a nonempty set of integers that is closed under addition and subtraction.*

Then either S consists of zero alone or S contains a smallest positive element, in which case S consists of all multiples of its smallest positive element.

Solution. Since S is not empty, then there exists some element in S.

Let a be some element of S.

Since $a \in S$ and $S \subset \mathbb{Z}$, then $a \in \mathbb{Z}$.

By closure of S under addition, we have $a+a = 2a \in S$ and $2a+a = 3a \in S$ and $3a + a = 4a \in S$, and so on.

Thus, it appears $ka \in S$ for all positive integers k.

By closure of S under subtraction, we have $a-a = 0 \in S$ so $0-a = -a \in S$, so $-a - a = -2a \in S$, so $-2a - a = -3a \in S$, so $-3a - a = -4a \in S$, and so on.

Thus, it appears $ka \in S$ for all negative integers k.

Hence, it appears $ka \in S$ for all integers k, so it appears that $\{ka : k \in \mathbb{Z}\} \subset S$.

We showed that if $a \in S$, then $0 \in S$ and $-a \in S$.

Since S is not empty, then S contains at least one element, so either S contains exactly one element or it contains more than one element. □

Proof. Since S is a nonempty subset of integers, then there is some element in S, say a.

Since $a \in S$ and $S \subset \mathbb{Z}$, then $a \in \mathbb{Z}$.

By closure of S under subtraction, $a - a \in S$, so $0 \in S$.

Since S is not empty, then S contains at least one element, so either S contains exactly one element or S contains more than one element.

We consider these cases separately.

Case 1: Suppose S contains exactly one element.

Since S contains exactly one element and $0 \in S$, then S must contain zero only.

Therefore, $S = \{0\}$.

Case 2: Suppose S contains more than one element.
Then S contains at least two elements.
One of the elements must be zero and the other element is not zero.
Let a be some element of S that is not equal to zero.
Since $a \in S$ and $S \subset \mathbb{Z}$, then $a \in \mathbb{Z}$.
Since $a \neq 0$, then either $a > 0$ or $a < 0$.
Suppose $a > 0$.
Then $0 - a \in S$, so $-a \in S$.
Suppose $a < 0$.
Then $0 - a \in S$, so $-a \in S$.
Hence, in either case S will always contain both $-a$ and a.
Therefore, without loss of generality, assume $a > 0$.
Then $-a \in S$.
We must prove a is the least positive element of S and that $S = \{na : n \in \mathbb{Z}\}$.
Let $T = \{na : n \in \mathbb{Z}\}$.
To prove $S = T$, we prove $S \subset T$ and $T \subset S$.
To prove $T \subset S$, we must prove every element of T is in S.
Hence, we must prove every multiple of a is in S, so we must prove $(\forall n \in \mathbb{Z})(na \in S)$.
To prove $(\forall n \in \mathbb{Z})(na \in S)$, we prove $(\forall n \in \mathbb{Z}^+)(na \in S)$ and $0 \in S$ and $(\forall n \in \mathbb{Z}^+)(-na \in S)$.
We've already shown that $0 \in S$.
We prove $(\forall n \in \mathbb{Z}^+)(na \in S)$ by induction on n.
Let $p(n) : na \in S$.
For $n = 1$, we have $1 * a = a \in S$, so $p(1)$ holds.
Suppose m is an arbitrary integer such that $p(m)$ holds.
To prove $p(m+1)$ holds, we must prove $(m+1)a \in S$.
Since $p(m)$ holds, then $ma \in S$.
Thus, by closure under addition, $ma + a \in S$.
Hence, $ma + a = (m+1)a \in S$, as desired.
Therefore, by induction, $na \in S$ for all positive integers n.
We now prove $(\forall n \in \mathbb{Z}^+)(-na \in S)$ by induction on n.
Let $q(n) : -na \in S$.
For $n = 1$, we have $-(1 * a) = -a \in S$, so $q(1)$ holds.
Suppose m is an arbitrary integer such that $q(m)$ holds.
To prove $q(m+1)$ holds, we must prove $-(m+1)a \in S$.
Since $q(m)$ holds, then $-ma \in S$.
Thus, by closure under subtraction, $-ma - a \in S$.
Hence, $-ma - a = -(ma + a) = -(m+1)a \in S$, as desired.
Therefore, by induction, $-na \in S$ for all positive integers n.
Hence, $na \in S$ for all integers n, so every multiple of a is in S.
Thus, every element of T is in S, so $T \subset S$.
We prove a is the least positive element of S.
Either $a = 1$ or $a \neq 1$.
We consider these cases separately.
Case 1: Suppose $a = 1$.

The least positive integer is 1.
Since $a = 1$, then 1 is the least positive element of S.
Hence, a is the least positive element of S.
Case 2: Suppose $a \neq 1$.
Since $a > 0$ and $a \neq 1$, then $a > 1$.
Let W be the set of all positive elements of S.
Then $W = \{x \in S : x > 0\}$, so $W \subset S$.
Since $W \subset S$ and $S \subset \mathbb{Z}$, then $W \subset \mathbb{Z}$.
Since each element of W is positive, then $W \subset \mathbb{Z}^+$.
By the well ordering principle of $\mathbb{Z}^+$, W must contain a least element, say $b \in W$.
We prove $b = a$.
Or, we could prove there is no element of W that is less than a by contradiction?
Since $b \in W$ and $W \subset S$, then $b \in S$.
Suppose $b \neq a$.
Since b is the least element of W, then $b < a$.
By closure of S under subtraction, $a - b \in S$.
Since $b < a$, then $a - b > 0$, so $a - b \in W$.
Suppose $a/2 < b$.
Then $a < 2b$, so $a - b < b$.
Thus, $a - b \in W$ and $a - b < b$, so $a - b$ is less than the least positive element of W, a contradiction.
Hence, $a/2$ cannot be less than b.
Thus, either $a/2 = b$ or $a/2 > b$, so either $b = a/2$ or $b < a/2$.
Suppose for the sake of contradiction that a is not the least positive element of S.
Then there exists some element other than a that is the least positive element of S.
Let c be some positive element of S that is the least positive element of S.
Then $c \in S$ and $c > 0$ and $c \neq a$ and $(\forall x \in S)(x > 0 \to c \leq x)$.
Since $a \in S$ and $a > 0$, then $c \leq a$, so either $c < a$ or $c = a$.
Since $c \neq a$, then $c < a$.
Thus, $0 < c < a$.
Since $c \in S$ and $S \subset \mathbb{Z}$, then $c \in \mathbb{Z}$, so $1 \leq c \leq a - 1$.
Since $c > 0$, then we divide a by c.
By the division algorithm, there are unique integers q and r such that $a = cq + r$ and $0 \leq r < c$.
Thus, $r = a - cq$.
Every multiple of an element of S is in S.
Since $c \in S$, then every multiple of c is in S, so in particular, $qc \in S$.
Since $a \in S$ and $qc \in S$ and S is closed under subtraction, then $a - cq \in S$, so $r \in S$.
Either a is a multiple of c or not.
Suppose a is not a multiple of c.
Then $r > 0$.

Thus, r is a positive element of S and c is the least positive element of S and $r < c$.

Hence, there exists some positive element of S that is less than the least positive element of S, a contradiction.

Therefore, a must be a multiple of c.

Thus, there is some integer k such that $a = ck$.

Since a and c are positive, then k must be positive.

Either k is a multiple of c or it is not.

Suppose k is a multiple of c.

Since $c \in S$ and every multiple of an element in S is in S, then $k \in S$.

Now, either $k = c$ or $k \neq c$.

Suppose $k \neq c$.

Then either $k > c$ or $k < c$, so $|k - c| > 0$.

$k = c$ or $k \neq c$.

If $k = c$, then $k \in S$, since $c \in S$.

If $k \neq c$, then either $k < c$ or $k > c$.

But, is $k \in S$?

We're stuck here in trying to figure out how to devise a suitable contradiction.

To prove $S \subset T$, we must prove every element of S is a multiple of a.

Hence, we must prove $(\forall b \in S)(a|b)$.

Suppose b is some element of S such that b is not a multiple of a.

We divide b by a.

Since $a > 0$, then by the division algorithm, there are unique integers q, r such that $b = aq + r$ and $0 < r < a$.

Thus, $r = b - qa$.

Every multiple of an element of S is in S.

Since $a \in S$, then every multiple of a is in S, so in particular, $qa \in S$.

Since $b \in S$ and $qa \in S$ and S is closed under subtraction, then $b - qa \in S$, so $r \in S$.

Hence, r is a positive element of S and a is the least positive element of S and $r < a$.

Thus, there exists some positive element of S that is less than the least positive element of S, a contradiction.

Hence, there is no element of S that is not a multiple of a.

Therefore, every element of S is a multiple of a.

Hence, $S \subset T$.

Since $S \subset T$ and $T \subset S$, then we conclude $S = T$. □

Proposition 21. *Let $a, b \in \mathbb{Z}$.*

Then $a - b$ divides $a^n - b^n$ for all $n \in \mathbb{N}$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{N} : a - b | a^n - b^n\}$.

Basis:

Since $a, b \in \mathbb{Z}$, then $a - b \in \mathbb{Z}$.

Since $a - b$ divides $a - b = a^1 - b^1$, then $a - b$ divides $a^1 - b^1$.

Since $1 \in \mathbb{N}$ and $a - b$ divides $a^1 - b^1$, then $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{N}$ and $a - b$ divides $a^k - b^k$.
Since $k \in \mathbb{N}$, then $k + 1 \in \mathbb{N}$.
Since $a - b$ divides $a^k - b^k$, then $a - b$ divides any multiple of $a^k - b^k$.
Since $a \in \mathbb{Z}$, then $a - b$ divides $a(a^k - b^k)$.
Since $a - b$ divides $a - b$, then $a - b$ divides any multiple of $a - b$.
Since $k \in \mathbb{N}$, then $k \geq 1 > 0$, so $k > 0$.
Since $b \in \mathbb{Z}$ and $k > 0$ and $k \in \mathbb{Z}$, then $b^k \in \mathbb{Z}$.
Hence, $a - b$ divides $b^k(a - b)$.
Thus, $a-b$ divides the sum $a(a^k - b^k) + b^k(a-b) = a^{k+1} - ab^k + ab^k - b^{k+1} = a^{k+1} - b^{k+1}$.
Since $k + 1 \in \mathbb{N}$ and $a - b$ divides $a^{k+1} - b^{k+1}$, then $k + 1 \in S$.
Thus, $k \in S$ implies $k + 1 \in S$.
Therefore, by the principle of mathematical induction, $a - b$ divides $a^n - b^n$ for all $n \in \mathbb{N}$, as desired. □

Exercise 22. **1 and -1 are the only divisors of 1**
Let $n \in \mathbb{Z}$.
If $n|1$, then $n = 1$ or $n = -1$.

Proof. Suppose $n|1$.
Then $1 = nm$ for some integer m.
Since $nm = 1$, then by axiom of $\mathbb{Z}$, either $n = m = 1$ or $n = m = -1$.
Therefore, either $n = 1$ or $n = -1$. □

Exercise 23. **zero divides only zero**
Let $n \in \mathbb{Z}$.
If $0|n$, then $n = 0$.

Proof. Suppose $0|n$.
Then $n = 0m$ for some $m \in \mathbb{Z}$.
Therefore, $n = 0m = 0$, so $n = 0$. □

Exercise 24. Let $a, b, c, d \in \mathbb{Z}$.
If $a + b = c$ and $d|a$ and $d|c$, then $d|b$.

Proof. Suppose $a + b = c$ and $d|a$ and $d|c$.
Since $d|c$ and $d|a$, then d divides their difference $c - a$, so $d|b$. □

Exercise 25. Let $x, y \in \mathbb{Z}$.
If $3x^2 + 15xy + 5y^2 = 0$, then $3|5y^2$ and $5|3x^2$.

Proof. Suppose $3x^2 + 15xy + 5y^2 = 0$.
Then $5y^2 = -3x^2 - 15xy$ and $3x^2 = -15xy - 5y^2$.
Since $5y^2 = -3x^2 - 15xy = 3(-x^2 - 5xy)$ and $-x^2 - 5xy \in \mathbb{Z}$, then $3 \mid 5y^2$.
Since $3x^2 = -15xy - 5y^2 = 5(-3xy - y^2)$ and $-3xy - y^2 \in \mathbb{Z}$, then $5 \mid 3x^2$. □

Exercise 26. Let $d, a, b \in \mathbb{Z}$.
Disprove: If $d|ab$, then $d|a$ and $d|b$.

Solution. Let $d = 5$ and $a = 10$ and $b = 6$.
Observe that $5|(10 \cdot 6)$ and $5|10$, but $5 \not| 6$. □

Exercise 27. Let $d, a, b \in \mathbb{Z}$.
Disprove: If $d|ab$, then $d|a$ or $d|b$.

Solution. Let $d = 6$ and $a = 4$ and $b = 9$.
Observe that $6 \mid (4 \cdot 9)$, but $6 \not| 8$ and $6 \not| 9$. □

Exercise 28. Let $a, b, n \in \mathbb{Z}$.
Disprove: If $a|n$ and $b|n$, then $ab|n$.

Solution. Let $n = 12$ and $a = 4$ and $b = 6$.
Observe that $4|12$ and $6|12$, but $(4 * 6) \not| 12$. □

Exercise 29. Let $d, n \in \mathbb{Z}^+$.
Then $\gcd(d, nd) = d$.

Solution. Observe that

$$\begin{aligned} \gcd(d, nd) &= d \cdot \gcd(1, n) \\ &= d \cdot 1 \\ &= d. \end{aligned}$$

□

Exercise 30. Let $a, b, c \in \mathbb{Z}$.
If $\gcd(a, b) = 1$ and $c|a$, then $\gcd(c, b) = 1$.

Proof. Suppose $\gcd(a, b) = 1$ and $c|a$.
Since $\gcd(a, b) = 1$, then there exist integers x and y such that $xa + yb = 1$.
Since $c|a$, then $a = ck$ for some integer k.
Thus, $1 = xa + yb = x(ck) + yb = x(kc) + yb = (xk)c + yb$, so 1 is a linear combination of c and b.
Therefore, $\gcd(c, b) = 1$. □

Exercise 31. There exists an $n \in \mathbb{N}$ for which $11|(2^n - 1)$.

Solution. The statement is $(\exists n \in \mathbb{N})(11|2^n - 1)$.
We can use computer or calculator to determine some value for n. □

Proof. Let $n = 10$.
Then $2^{10} - 1 = 1023 = 11 \cdot 93$, so $11 \mid 2^{10} - 1$. □

Exercise 32. Let $a, b \in \mathbb{Z}$.
If $a \mid b$, then $a^2 \mid b^2$.

Proof. Suppose $a \mid b$.
Then $b = ak$ for some integer k.
Thus, $b^2 = (ak)^2 = a^2k^2$.
Since $k^2 \in \mathbb{Z}$, then $a^2 \mid b^2$. □

Exercise 33. Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Solution. We use proof by contrapositive since we have alot of negative statements and direct proof leads us nowhere. □

Proof. Suppose it is not true that $5 \nmid x$ and $5 \nmid y$.
Then $5|x$ or $5|y$.
There are two cases to consider.
Case 1: Suppose $5 \mid x$.
Then $x = 5a$ for some $a \in \mathbb{Z}$.
Multiply both sides by y to get $xy = 5ay$.
Thus $xy = 5(ay)$, and this means $5 \mid xy$.
Case 2: Suppose $5 \mid y$.
Then $y = 5a$ for some $a \in \mathbb{Z}$.
Multiply both sides by x to get $xy = 5ax$.
Thus $xy = 5(ax)$, and this means $5 \mid xy$.

Both of these cases show that $5 \mid xy$, so it is not true that $5 \nmid xy$. □

Exercise 34. Let $n \in \mathbb{Z}$.
If $5 \mid 2n$, then $5 \mid n$.

Proof. Suppose $5 \mid 2n$.
Then $2n = 5a$ for some integer a.
Observe that

$$\begin{aligned} n &= 5n - 4n \\ &= 5n - 2(2n) \\ &= 5n - 2(5a) \\ &= 5(n - 2a). \end{aligned}$$

Since $n - 2a$ is an integer, then $5 \mid n$. □

Proof. Suppose $5 \mid 2n$.
Then $2n = 5a$ for some integer a.
Thus, $5a$ is a multiple of 2, so $5a$ is even.
Since 5 is odd and $5a$ is even, then a must be even.
Hence, $a = 2b$ for some integer b.
Thus, $2n = 5(2b)$, so $n = 5b$.
Therefore, $5 \mid n$. □

Exercise 35. Let $n \in \mathbb{Z}$.
If $7 \mid 4n$, then $7 \mid n$.

Proof. Suppose $7 \mid 4n$.
Then $4n = 7a$ for some integer a.
Observe that

$$\begin{aligned} n &= 8n - 7n \\ &= 2(4n) - 7n \\ &= 2(7a) - 7n \\ &= 7(2a - n). \end{aligned}$$

Since $2a - n$ is an integer, then $7 \mid n$. □

Proof. Suppose $7 \mid 4n$.
Then $4n = 7a$ for some integer a.
Thus, $2(2n) = 7a$, so $7a$ is even.
Since 7 is odd and $7a$ is even, then a must be even.
Hence, $a = 2b$ for some integer b.
Thus, $4n = 7(2b)$, so $2n = 7b$.
Hence, $7b$ is even.
Since 7 is odd and $7b$ is even, then b must be even.
Hence, $b = 2c$ for some integer c.
Thus, $2n = 7(2c)$, so $n = 7c$.
Therefore, $7|n$. □

Exercise 36. Let $a, b \in \mathbb{Z}$.
If $a|b$, then $(-a)|b$ and $a|(-b)$ and $(-a)|(-b)$.

Proof. Suppose $a|b$.
Then $b = an$ for some integer n.
Thus, $b = an = (-a)(-n)$ and $-b = -an = a(-n)$.
Since $b = (-a)(-n)$ and $-n \in \mathbb{Z}$, then $(-a)|b$.
Since $-b = a(-n)$ and $-n \in \mathbb{Z}$, then $a|(-b)$.
Since $-b = -an$ and $n \in \mathbb{Z}$, then $(-a)|(-b)$. □

Exercise 37. Let $a, b, c \in \mathbb{Z}$.
If $a|b$ and $a|c$, then $a^2|bc$.

Proof. Suppose $a|b$ and $a|c$.
Then $b = am$ and $c = an$ for some integers m and n.
Thus, $bc = (am)(an) = a(ma)n = a(am)n = (aa)(mn) = a^2(mn)$.
Since $m, n \in \mathbb{Z}$, then $mn \in \mathbb{Z}$, so $a^2|bc$. □

Exercise 38. Let $a, b, c \in \mathbb{Z}$.
Disprove: If $a|(b + c)$, then either $a|b$ or $a|c$.

Proof. Let $a = 3$ and $b = 4$ and $c = 5$.
Since $3|9$, then $3|(4 + 5)$, but $3 \nmid 4$ and $3 \nmid 5$. □

Exercise 39. If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Solution. We can make a table of values by plugging in various values to determine if the expression is really a multiple of 4.

n	$1 + (-1)^n(2n-1)$
1	0
2	4
3	-4
4	8
5	-8
6	12
7	-12

We see that for even n, the expression $1+(-1)^n(2n-1) = 1+(1)(2n-1) = 2n$. For odd n, $1 + (-1)^n(2n-1) = 1 - (1)(2n-1) = 1 - 2n + 1 = 2 - 2n$. □

Proof. Suppose $n \in \mathbb{N}$.

Then n is either even or odd. We consider these two cases separately.

Case 1. Suppose n is even.

Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.

Thus $1 + (-1)^n(2n-1) = 1 + (1)(2 \cdot 2k - 1) = 4k$, which is a multiple of 4.

Case 2. Suppose n is odd.

Then $n = 2k + 1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.

Thus $1 + (-1)^n(2n-1) = 1 + (-1)(2(2k+1) - 1) = 1 - (4k+1) = -4k$, which is a multiple of 4.

These two cases show that $1 + (-1)^n(2n-1)$ is always a multiple of 4. □

Exercise 40. Every multiple of 4 has form $1 + (-1)^n(2n-1)$ for some $n \in \mathbb{N}$.

Proof. In conditional form, the proposition is as follows:

If k is a multiple of 4, then there is an $n \in \mathbb{N}$ for which $1+(-1)^n(2n-1) = k$.

What follows is a proof of this conditional statement.

Suppose k is a multiple of 4. Then $k = 4a$ for some integer a.

We must produce an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n-1) = k$.

We consider three cases, depending on whether a is zero, positive, or negative.

Case 1. Suppose $a = 0$.

Let $n = 1$. Then $1+(-1)^n(2n-1) = 1+(-1)(2\cdot 1-1) = 0 = 4\cdot 0 = 4a = k$.

Case 2. Suppose $a > 0$.

Let $n = 2a$, which is an element of $\mathbb{N}$ because a is positive, making n positive.

Also n is even, so $(-1)^n = 1$. Thus $1 + (-1)^n(2n-1) = 1 + (1)(2 \cdot 2a - 1) = 4a = k$.

Case 3. Suppose $a < 0$.

Let $n = 1-2a$, which is an element of $\mathbb{N}$ because a is negative, making $1-2a$ positive.

Also n is odd, so $(-1)^n = -1$. Thus $1 + (-1)^n(2n-1) = 1 + (-1)(2(1-2a) - 1) = 1 - (1 - 4a) = 4a = k$.

These three cases show that no matter whether a multiple $k = 4a$ is zero, positive, or negative, it always equals $1+(-1)^n(2n-1)$ for some natural number n. □

Exercise 41. If $n \in \mathbb{N}$, then $n^2 = 2\binom{n}{2} + \binom{n}{1}$.

Solution. By definition of binomial coefficient we know $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

In particular, for $n > 1$, $\binom{n}{1} = n$ and $\binom{n}{2} = \frac{n(n-1)}{2}$. □

Proof. Suppose n is an integer.

We consider two cases.

Case 1: Suppose $n = 1$.

Then $2\binom{1}{2} + \binom{1}{1} = 2 \cdot 0 + 1 = 1 = 1^2$.

Case 2: Suppose $n > 1$.

Then $2\binom{n}{2} + \binom{n}{1} = 2\frac{n(n-1)}{2} + n = n(n-1) + n = n^2$.

Both cases show $n^2 = 2\binom{n}{2} + \binom{n}{1}$. □

Exercise 42. Let $a \in \mathbb{Z}$.

Then either a or $a + 2$ or $a + 4$ is divisible by 3.

Proof. By the division algorithm, there exist unique integers q and r such that $a = 3q + r$ with $0 \leq r < 3$.

Thus, either $a = 3q$ or $a = 3q + 1$ or $a = 3q + 2$.

We consider these cases separately.

Case 1: Suppose $a = 3q$.

Since $a = 3q$ and $q \in \mathbb{Z}$, then $3|a$, so a is divisible by 3.

Case 2: Suppose $a = 3q + 1$.

Then $a + 2 = (3q + 1) + 2 = 3q + 3 = 3(q + 1)$.

Since $a + 2 = 3(q + 1)$ and $q + 1 \in \mathbb{Z}$, then $3|(a + 2)$, so $a + 2$ is divisible by 3.

Case 3: Suppose $a = 3q + 2$.

Then $a + 4 = (3q + 2) + 4 = 3q + 6 = 3(q + 2)$.

Since $a + 4 = 3(q + 2)$ and $q + 2 \in \mathbb{Z}$, then $3|(a + 4)$, so $a + 4$ is divisible by 3. □

Exercise 43. A product of 3 consecutive integers is divisible by 3

Let $a \in \mathbb{Z}$.

Then $3|a(a + 1)(a + 2)$.

Proof. By the division algorithm, either $a = 3k$ or $a = 3k + 1$ or $a = 3k + 2$ for some integer k.

We consider these cases separately.

Case 1: Suppose $a = 3k$.

Then $3|a$, so 3 divides any multiple of a.

Hence, $3|a(a + 1)(a + 2)$.

Case 2: Suppose $a = 3k + 1$.

Then $a + 2 = (3k + 1) + 2 = 3k + 3 = 3(k + 1)$, so $3|(a + 2)$.

Hence, 3 divides any multiple of $a+2$, so $3|a(a+1)(a+2)$.
Case 3: Suppose $a = 3k+2$.
Then $a+1 = (3k+2)+1 = 3k+3 = 3(k+1)$, so $3|(a+1)$.
Hence, 3 divides any multiple of $a+1$, so $3|a(a+1)(a+2)$.

Therefore, in all cases, $3|a(a+1)(a+2)$. □

Exercise 44. Let $a \in \mathbb{Z}$.
Then $4 \not| (a^2+2)$.

Proof. By the division algorithm, there exist unique integers q and r such that $a = 4q + r$ with $0 \leq r < 4$.
Thus, either $a = 4q$ or $a = 4q+1$ or $a = 4q+2$ or $a = 4q+3$.
We consider these cases separately.
Case 1: Suppose $a = 4q$.
Then $a^2+2 = (4q)^2+2 = 4^2q^2+2 = 4(4q^2)+2$.
Let $k = 4q^2$.
Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+2$.
Case 2: Suppose $a = 4q+1$.
Then $a^2+2 = (4q+1)^2+2 = (16q^2+8q+1)+2 = 16q^2+8q+3 = 4(4q^2+2q)+3$.
Let $k = 4q^2+2q$.
Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+3$.
Case 3: Suppose $a = 4q+2$.
Then $a^2+2 = (4q+2)^2+2 = (16q^2+16q+4)+2 = 4(4q^2+4q+1)+2$.
Let $k = 4q^2+4q+1$.
Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+2$.
Case 4: Suppose $a = 4q+3$.
Then $a^2+2 = (4q+3)^2+2 = (16q^2+24q+9)+2 = 16q^2+24q+11 = 16q^2+24q+(4*2+3) = 4(4q^2+6q+2)+3$.
Let $k = 4q^2+6q+2$.
Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+3$.

Therefore, in all cases, either $a^2+2 = 4k+2$ or $a^2+2 = 4k+3$ for some integer k.
Hence, 4 cannot divide a^2+2. □

Exercise 45. Let $n \in \mathbb{Z}$.
If $2 \mid n$ and $3 \mid n$, then $6 \mid n$.

Proof. Suppose $2 \mid n$ and $3 \mid n$.
Since $2 \mid n$, then $n = 2a$ for some integer a.
Since $3 \mid n$, then $n = 3b$ for some integer b.

Observe that

$$\begin{aligned} n &= 3n - 2n \\ &= 3(2a) - 2(3b) \\ &= 6a - 6b \\ &= 6(a - b). \end{aligned}$$

Since $a - b$ is an integer, then $6 \mid n$. ☐

Proof. Suppose $2 \mid n$ and $3 \mid n$.
Since $2 \mid n$, then $3 * 2 \mid 3n$, so $6 \mid 3n$.
Since $3 \mid n$, then $2 * 3 \mid 2n$, so $6 \mid 2n$.
Thus, 6 is a common divisor of $2n$ and $3n$, so $6 \mid \gcd(2n, 3n)$.
Hence, $6 \mid n * \gcd(2, 3)$, so $6 \mid n * 1$.
Therefore, $6 \mid n$. ☐

Exercise 46. Let n be an integer.
If $3 \mid n$ and $5 \mid n$, then $15 \mid n$.

Proof. Suppose $3 \mid n$ and $5 \mid n$.
Since $3 \mid n$, then $n = 3a$ for some integer a.
Since $5 \mid n$, then $n = 5b$ for some integer b.
Observe that

$$\begin{aligned} n &= 6n - 5n \\ &= 6(5b) - 5(3a) \\ &= 30b - 15a \\ &= 15(2b - a). \end{aligned}$$

Since $2b - a$ is an integer, then $15 \mid n$. ☐

Exercise 47. Let $n \in \mathbb{Z}$.
Then $14 \mid n$ if and only if $7 \mid n$ and $2 \mid n$.

Proof. We first prove: if $14 \mid n$ then $7 \mid n$ and $2 \mid n$.
Suppose $14 \mid n$.
Then $n = 14k$ for some $k \in \mathbb{Z}$.
Since $n = 7(2k)$ and $2k \in \mathbb{Z}$, then $7 | n$.
Since $n = 2(7k)$ and $7k \in \mathbb{Z}$, then $2 | n$.
Therefore, $7 \mid n$ and $2 \mid n$.

Conversely, we prove: if $7 \mid n$ and $2 \mid n$, then $14 \mid n$.
Suppose $7 \mid n$ and $2 \mid n$.
Since $7 \mid n$, then $n = 7a$ for some integer a.
Since $2 \mid n$, then $n = 2b$ for some integer b.

Observe that

$$\begin{aligned} n &= 7n - 6n \\ &= 7(2b) - 6(7a) \\ &= 14b - 42a \\ &= 14(b - 3a). \end{aligned}$$

Since $b - 3a$ is an integer, then $14 \mid n$. ☐

Exercise 48. Let a, b, d be integers.
If $d|(da + b)$, then $d|b$.

Proof. Suppose $d|(da + b)$.
Then $da + b = dn$ for some integer n.
Hence, $b = dn - da = d(n - a)$.
Since $n - a$ is an integer, then this implies $d|b$. ☐

Exercise 49. Let a, b, d be integers.
If $d|(a + b)$ and $d|a$, then $d|b$.

Proof. Suppose $d|(a + b)$ and $d|a$.
Then $a + b = dk$ and $a = dm$ for some integers k and m.
Thus, $b = dk - a = dk - dm = d(k - m)$.
Since $k - m$ is an integer, then this implies $d|b$. ☐

Exercise 50. Let $x, y \in \mathbb{Z}$.
If $x|y$ and y is odd, then x is odd.

Proof. Suppose $x|y$ and y is odd.
Since $x|y$, then $y = xk$ for some integer k.
Since y is odd, then this implies xk is odd.
Hence, x must be odd. ☐

Exercise 51. If a is an integer and $a^2|a$, then $a \in \{-1, 0, 1\}$.

Proof. Suppose a is an integer and $a^2|a$.
Then $a = a^2k$ for some integer k.
Thus, $0 = a - a^2k = a(1 - ak)$, so either a is zero or a is not zero.
We consider these cases separately.

Case 1: Suppose a is zero.
Then $a = 0$, so $a \in \{0\}$.
Case 2: Suppose a is not zero.
Then $1 - ak = 0$, so $1 = ak$.
Since a and k are both integers, then $k = \pm 1$.
If $k = 1$, then $1 = a(1) = a$.
If $k = -1$, then $-1 = -ak = -a(-1) = a$.
Thus, either $a = 1$ or $a = -1$, so $a \in \{1, -1\}$.

Therefore, in all cases, either $a \in \{0\}$ or $a \in \{1, -1\}$, so $a \in \{0, 1, -1\} = \{-1, 0, 1\}$. □

Exercise 52. Let $a, b, d \in \mathbb{Z}$.
If $d \mid a$ or $d \mid b$, then $d \mid ab$.

Proof. Suppose $d \mid a$ or $d \mid b$.
We consider each case separately.
Case 1: Suppose $d \mid a$.
Then $a = dk$ for some $k \in \mathbb{Z}$.
Thus, $ab = (dk)b = d(kb)$, so $d \mid ab$.
Case 2: Suppose $d \mid b$.
Then $b = dm$ for some $m \in \mathbb{Z}$.
Thus, $ab = a(dm) = (dm)a = d(ma)$, so $d \mid ab$.
Both of these cases show that $d \mid ab$. □

Exercise 53. Let $a, b, d \in \mathbb{Z}$.
Disprove: If $d \mid ab$, then $d \mid a$ or $d \mid b$.

Proof. Here is a counter example.
Let $d = 6$ and $a = 8$ and $b = 9$.
Observe that $6 \mid (8 \cdot 9)$, but $6 \nmid 8$ and $6 \nmid 9$. □

Exercise 54. Let $a, b, m \in \mathbb{Z}$.
If $ab|m$, then $a|m$ and $b|m$.

Proof. Suppose $ab|m$.
Then $m = abk$ for some integer k.
Since $m = abk = a(bk)$ and $bk \in \mathbb{Z}$, then $a|m$.
Since $m = abk = bak = b(ak)$ and $ak \in \mathbb{Z}$, then $b|m$.
Therefore, $a|m$ and $b|m$. □

Exercise 55. Let $a, b, m \in \mathbb{Z}$.
Disprove: if $a|m$ and $b|m$, then $ab|m$.

Proof. Here is a counter example.
Let $a = 4$ and $b = 10$ and $m = 60$.
Then $4|60$ and $10|60$, but, $40 \nmid 60$. □

Exercise 56. Let $m, n \in \mathbb{Z}^+$ such that $n > 1$.
If $n|m$, then $n \nmid m + 1$.

Proof. Suppose $n|m$.
Then there exists an integer a such that $m = na$.
Suppose for the sake of contradiction that $n|(m + 1)$.
Then there exists an integer b such that $m + 1 = nb$.
Hence, $na + 1 = nb$, so $1 = nb - na = n(b - a)$.
Since $b - a$ is an integer, then this implies $n|1$.
Hence, either $n = 1$ or $n = -1$.

Thus, n is not greater than 1.
Therefore, we have $n > 1$ and $n \not> 1$, a contradiction.
Consequently, n cannot divide $m + 1$, so $n \not| (m + 1)$, as desired. □

Exercise 57. If n is an integer, then $n^2 + 2$ is not divisible by 4.

Proof. Let n be an arbitrary integer.
We prove by contradiction.
Suppose $n^2 + 2$ is divisible by 4.
Then there is an integer k such that $n^2 + 2 = 4k$.
Either n is even or not.
We consider these cases separately.
Case 1: Suppose n is even.
Then $n = 2m$ for some integer m.
Thus, $4k = n^2 + 2 = (2m)^2 + 2 = 4m^2 + 2 = 2(2m^2 + 1)$.
Hence, $2k = 2m^2 + 1$.
But, this equation implies the even integer $2k$ equals the odd integer $2m^2+1$, a contradiction.
Case 2: Suppose n is odd.
Then n^2 is odd, so $n^2 + 2$ is odd.
Since $2(2k) = 4k = n^2 + 2$ and $2k$ is an integer, then $n^2 + 2$ is even.
But, this contradicts the fact that $n^2 + 2$ is odd. □

Exercise 58. For any integer $n \geq 0$, it follows that $24|(5^{2n} - 1)$.

Solution. The statement to prove is:
$(\forall n \in \mathbb{Z}, n \geq 0)(24|5^{2n} - 1)$.
Define predicate $p(n) : 24|5^{2n} - 1$ over $\mathbb{N} \cup \{0\}$.
Observe that $24|5^{2n} - 1$ is equivalent to $(25 - 1)|25^n - 1$.
Since we know $x - 1$ divides $x^n - 1$, for every $x \in \mathbb{Z}$ and every $n \in \mathbb{N}$, then we know, in particular, $24|25^n - 1$ for every $n \in \mathbb{N}$.
Thus, we need only prove $24|25^n - 1$ when $n = 0$.
But, $25^0 - 1 = 0$ and $24|0$.
Hence, $p(0)$ is true. □

Proof. We prove by induction(weak).
Basis:
If $n = 0$ then the statement is $24|(5^{2\cdot 0} - 1)$.
This simplifies to $24|0$, which is true.
If $n = 1$ then the statement is $24|(5^{2\cdot 1} - 1)$.
This simplifies to $24|24$, which is true.
Induction:
We must prove $24|(5^{2k} - 1)$ implies $24|(5^{2(k+1)} - 1)$.
Suppose $24|(5^{2k} - 1)$ for any integer $k \geq 1$.
Then $5^{2k} - 1 = 24a$ for some integer a, by definition of divisibility.
Thus $5^{2k} = 24a + 1$.

Observe the following equalities:

$$\begin{aligned} 5^{2(k+1)} - 1 &= 5^{2k+2} - 1 \\ &= 5^2 5^{2k} - 1 \\ &= 25(24a + 1) - 1 \\ &= 25 \cdot 24a + 25 - 1 \\ &= 24(25a + 1) \end{aligned}$$

This shows that $5^{2(k+1)} - 1 = 24(25a + 1)$, which means $24|5^{2(k+1)} - 1$.

It follows by induction that $24|(5^{2n} - 1)$ for any integer $n \geq 0$. $\square$

Exercise 59. Let $n \in \mathbb{Z}$.

Then $5|n^5 - n$.

Solution. Note that the statement $5|n^5 - n$ is equivalent to the statement $n^5 \equiv n \pmod 5$.

We just showed that any integer of the form $n^5 - n$ is even. We now must show that such an integer is divisible by 5.

We factor $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n-1)(n+1)(n^2 + 1) = (n-1)n(n+1)(n^2 + 1)$. Thus $n^5 - n$ is a product of 3 consecutive integers and another factor. If $n = 0$, then $5|0^5 - 0$ since $0 = 5 \cdot 0$.

Suppose n is a natural number.

We consider n divided by 5.

By the Division Algorithm, we know that $n = 5q + r$, where $0 \leq r < 5$.

Thus we have the set of congruence classes modulo 5.

For example, if $r = 0$, then $n = 5q$.

If $r = 1$, then $n = 5q + 1$.

If $r = 2$, then $n = 5q + 2$.

If $r = 3$, then $n = 5q + 3$.

If $r = 4$, then $n = 5q + 4$.

We observe the following partition of natural numbers under congruence modulo 5 for any integer $q \geq 0$:

If $n \in \{2, 7, 12, 17, 22, 27, ...\} = \{5q + 2\}$, then $5|n^2 + 1$.

This set is really the set of all natural numbers which are congruent to 2 (mod 5).

Thus if $n \in [2]_5$, then $5|n^2+1$. This is because if n is an arbitrary element of this set, then $n = 5q+2$, so $n^2+1 = (5q+2)^2+1 = 25q^2+20q+5 = 5(5q^2+4q+1)$.

If $n \in \{3, 8, 13, 18, 23, 28, ...\} = \{5q + 3\}$, then $5|n^2 + 1$.

This set is really the set of all natural numbers which are congruent to 3 (mod 5).

Thus if $n \in [3]_5$, then $5|n^2 + 1$.This is because if n is an arbitrary element of this set, then $n = 5q + 3$, so $n^2 + 1 = (5q + 3)^2 + 1 = 25q^2 + 30q + 10 = 5(5q^2 + 6q + 2)$.

If $n \in \{4, 9, 14, 19, 24, 29, 34, ...\} = \{5q + 4\}$, then $5|n + 1$.

This set is really the set of all natural numbers which are congruent to 4 (mod 5).

Thus if $n \in [4]_5$, then $5|n+1$.This is because if n is an arbitrary element of this set, then $n = 5q + 4$, so $n + 1 = (5q + 4) + 1 = 5q + 5 = 5(q + 1)$.

If $n \in \{5, 10, 15, 20, 25, 30, ...\} = \{5q\}$, then $5|n$.

This set is really the set of all natural numbers which are multiples of 5.

Thus if $n \in [0]_5$, then $5|n$. This is because if n is an arbitrary element of this set, then $n = 5q$.

If $n \in \{1, 6, 11, 16, 21, 26, 31, 36, ...\} = \{5q + 1\}$, then $5|n - 1$.

This set is really the set of all natural numbers which are congruent to 1 (mod 5).

Thus if $n \in [1]_5$, then $5|n-1$.This is because if n is an arbitrary element of this set, then $n = 5q + 1$, so $n - 1 = (5q + 1) - 1 = 5q$.

Thus, regardless of what value n is, one of the factors $n, n-1, n+1$, or n^2+1 is always divisible by 5.

Hence, $n^5 - n$ is divisible by 5.

Now, we can also prove this by induction(weak form). The statement to prove is: for all non-negative integers n, $5|n^5 - n$.

Thus the statement is $S_n : 5|n^5 - n$.

The statement S_k is $5|k^5 - k$.

The statement S_{k+1} is $5|(k + 1)^5 - (k + 1)$. □

Proof. Let $p = n^5 - n$

Then $p = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n - 1)(n + 1)(n^2 + 1)$.

We must prove $5|p$.

By the division algorithm either $n = 5k$ or $n = 5k + 1$ or $n = 5k + 2$ or $n = 5k + 3$ or $n = 5k + 4$ for some integer k.

We consider each case separately.

Case 1: Suppose $n = 5k$.

Then $5|n$, so 5 divides any multiple of n.

Hence, $5|p$.

Case 2: Suppose $n = 5k + 1$.

Since $n - 1 = 5k$, then $5|(n - 1)$.

Hence, 5 divides any multiple of $n - 1$, so $5|p$.

Case 3: Suppose $n = 5k + 2$.

Since $n^2 + 1 = (5k + 2)^2 + 1 = 25k^2 + 20k + 4 + 1 = 25k^2 + 20k + 5 = 5(5k^2 + 4k + 1)$, then $5|(n^2 + 1)$.

Hence, 5 divides any multiple of $n^2 + 1$, so $5|p$.

Case 4: Suppose $n = 5k + 3$.

Since $n^2 + 1 = (5k + 3)^2 + 1 = 25k^2 + 30k + 9 + 1 = 25k^2 + 30k + 10 = 5(5k^2 + 6k + 2)$, then $5|(n^2 + 1)$.

Hence, 5 divides any multiple of $n^2 + 1$, so $5|p$.

Case 5: Suppose $n = 5k + 4$.

Since $n + 1 = (5k + 4) + 1 = 5k + 5 = 5(k + 1)$, then $5|(n + 1)$.

Hence, 5 divides any multiple of $n + 1$, so $5|p$. □

Proof. The statement is $S_n : 5|n^5 - n$.

We prove by induction.

Basis:
If $n = 0$, then the statement is $5|0^5 - 0$, or $5|0$, which is obviously true.
If $n = 1$, then the statement is $5|1^5 - 1$, or $5|0$, which is obviously true.
Induction:
We must prove $S_k \to S_{k+1}$ for $k \geq 1$.
This means we must prove if $5|(k^5 - k)$, then $5|(k+1)^5 - (k+1)$ for $k \geq 1$.
Suppose $5|(k^5 - k)$ for $k \geq 1$.
Then $k^5 - k = 5a$ for some $a \in \mathbb{Z}$, by definition of divisibility.
Observe the following equalities:

$$\begin{aligned}(k+1)^5 - (k+1) &= (k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) - k - 1 \\ &= (k^5 - k) + (5k^4 + 10k^3 + 10k^2 + 5k) \\ &= 5a + 5(k^4 + 2k^3 + 2k^2 + k) \\ &= 5(a + k^4 + 2k^3 + 2k^2 + k)\end{aligned}$$

Thus, $5|(k+1)^5 - (k+1)$.
It follows by induction that $5|(n^5 - n)$ for all non-negative integers. □

Exercise 60. The sum of the cubes of three consecutive natural numbers is divisible by 9.

Proof. We must prove $9|(n^3 + (n+1)^3 + (n+2)^3)$ for all $n \in \mathbb{N}$.
Let $p(n)$ be the predicate $9|(n^3 + (n+1)^3 + (n+2)^3)$ defined over $\mathbb{N}$.
We prove $p(n)$ is true for all $n \in \mathbb{N}$ by induction on n.
Basis:
Since $1^3 + 2^3 + 3^3 = 36$ and $9|36$, then $p(1)$ is true.
Induction:
Let $k \in \mathbb{N}$ such that $p(k)$ is true.
Then 9 divides $k^3 + (k+1)^3 + (k+2)^3$.
Since $(k+3)^3 - k^3 = (k^3 + 9k^2 + 27k + 27) - k^3 = 9k^2 + 27k + 27 = 9(k^2 + 3k + 3)$ and $k^2 + 3k + 3$ is an integer, then 9 divides $(k+3)^3 - k^3$.
Since 9 divides $k^3 + (k+1)^3 + (k+2)^3$ and 9 divides $(k+3)^3 - k^3$, then 9 divides the sum $k^3 + (k+1)^3 + (k+2)^3 + (k+3)^3 - k^3 = (k+1)^3 + (k+2)^3 + (k+3)^3$.
Hence, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for any $k \geq 1$.
It follows by induction that $9|(n^3 + (n+1)^3 + (n+2)^3)$ for all $n \in \mathbb{N}$. □

Exercise 61. For every $n \in \mathbb{Z}^+$, $6|n(n+1)(2n+1)$.

Proof. Let $n \in \mathbb{Z}^+$.
By the division algorithm, there exist unique integers q, r such that $n = 6q + r$ with $0 \leq r < 6$.
Thus, either $n = 6q$ or $n = 6q + 1$ or $n = 6q + 2$ or $n = 6q + 3$ or $n = 6q + 4$ or $n = 6q + 5$.
We consider each case separately.
Case 1: Suppose $n = 6q$.
Then $6|n$, so 6 divides any multiple of n.
Thus, $6|n(n+1)(2n+1)$.

Case 2: Suppose $n = 6q + 1$.

Since $n + 1 = (6q + 1) + 1 = 6q + 2 = 2(3q + 1)$, then $2|(n + 1)$.

Since $2n + 1 = 2(6q + 1) + 1 = 12q + 2 + 1 = 12q + 3 = 3(4q + 1)$, then $3|(2n + 1)$.

Since $2|(n+1)$ and $3|(2n+1)$, then $(2*3)|(n+1)(2n+1)$, so $6|(n+1)(2n+1)$.

Hence, 6 divides any multiple of $(n + 1)(2n + 1)$, so $6|n(n + 1)(2n + 1)$.

Case 3: Suppose $n = 6q + 2$.

Since $n = 2(3q + 1)$, then $2|n$.

Since $n + 1 = (6q + 2) + 1 = 6q + 3 = 3(2q + 1)$, then $3|(n + 1)$.

Since $2|n$ and $3|(n + 1)$, then $(2 * 3)|n(n + 1)$, so $6|n(n + 1)$.

Hence, 6 divides any multiple of $n(n + 1)$, so $6|n(n + 1)(2n + 1)$.

Case 4: Suppose $n = 6q + 3$.

Since $n = 3(2q + 1)$, then $3|n$.

Since $n + 1 = (6q + 3) + 1 = 6q + 4 = 2(3q + 2)$, then $2|(n + 1)$.

Since $3|n$ and $2|(n + 1)$, then $(3 * 2)|n(n + 1)$, so $6|n(n + 1)$.

Hence, 6 divides any multiple of $n(n + 1)$, so $6|n(n + 1)(2n + 1)$.

Case 5: Suppose $n = 6q + 4$.

Since $n = 2(3q + 2)$, then $2|n$.

Since $2n + 1 = 2(6q + 4) + 1 = 12q + 9 = 3(4q + 3)$, then $3|(2n + 1)$.

Since $2|n$ and $3|(2n + 1)$, then $6|n(2n + 1)$.

Hence, 6 divides any multiple of $n(2n + 1)$, so $6|n(n + 1)(2n + 1)$.

Case 6: Suppose $n = 6q + 5$.

Since $n + 1 = (6q + 5) + 1 = 6q + 6 = 6(q + 1)$, then $6|(n + 1)$.

Hence, 6 divides any multiple of $n + 1$, so $6|n(n + 1)(2n + 1)$.

Therefore, in all cases, $6|n(n + 1)(2n + 1)$. □

Proof. Let S be the truth set of $p(n) : 6|n(n + 1)(2n + 1)$.

To prove $S = \mathbb{Z}^+$, we use induction.

Basis:

Since $1(1 + 1)(2 * 1 + 1) = 6$ and $6|6$, then $p(1)$ is true.

Hence, $1 \in S$.

Induction:

Suppose $k \in S$.

To prove $k + 1 \in S$, we must prove $6|(k + 1)(k + 2)(2k + 3)$.

Since $k \in S$, then $6|k(k + 1)(2k + 1)$.

Observe that $(k + 1)(k + 2)(2k + 3) = k(k + 1)(2k + 1) + 6(k + 1)^2$.

Since $6|6$, then 6 divides any multiple of 6.

Hence, $6|6(k + 1)^2$.

Since 6 divides $k(k + 1)(2k + 1)$ and 6 divides $6(k + 1)^2$, then 6 divides the sum $k(k + 1)(2k + 1) + 6(k + 1)^2$.

Thus, 6 divides $(k + 1)(k + 2)(2k + 3)$, as desired. □

Exercise 62. The product of 3 consecutive integers is a multiple of 6.

$\forall n \in \mathbb{Z}, 6|n(n + 1)(n + 2)$.

Proof. Let $n \in \mathbb{Z}$.

Let $p = n(n+1)(n+2)$.

We must prove $6|p$.

By the division algorithm, either $n = 6k$ or $n = 6k+1$ or $n = 6k+2$ or $n = 6k+3$ or $n = 6k+4$ or $n = 6k+5$ for some integer k.

We consider these cases separately.

Case 1: Suppose $n = 6k$.

Then $6|n$, so 6 divides any multiple of n.

Therefore, $6|p$.

Case 2: Suppose $n = 6k+1$.

Since $n+1 = (6k+1)+1 = 6k+2 = 2(3k+1)$, then $2|(n+1)$.

Since $n+2 = (6k+1)+2 = 6k+3 = 3(2k+1)$, then $3|(n+2)$.

Since $2|(n+1)$ and $3|(n+2)$, then $6|(n+1)(n+2)$.

Hence, 6 divides any multiple of $(n+1)(n+2)$, so $6|p$.

Case 3: Suppose $n = 6k+2$.

Since $n = 2(3k+1)$, then $2|n$.

Since $n+1 = (6k+2)+1 = 6k+3 = 3(2k+1)$, then $3|(n+1)$.

Since $2|n$ and $3|(n+1)$, then $6|n(n+1)$.

Hence, 6 divides any multiple of $n(n+1)$, so $6|p$.

Case 4: Suppose $n = 6k+3$.

Since $n = 3(2k+1)$, then $3|n$.

Since $n+1 = (6k+3)+1 = 6k+4 = 2(3k+2)$, then $2|(n+1)$.

Since $3|n$ and $2|(n+1)$, then $6|n(n+1)$.

Hence, 6 divides any multiple of $n(n+1)$, so $6|p$.

Case 5: Suppose $n = 6k+4$.

Since $n+2 = (6k+4)+2 = 6k+6 = 6(k+1)$, then $6|(n+2)$.

Hence, 6 divides any multiple of $n+2$, so $6|p$.

Case 6: Suppose $n = 6k+5$.

Since $n+1 = (6k+5)+1 = 6k+6 = 6(k+1)$, then $6|(n+1)$.

Hence, 6 divides any multiple of $n+1$, so $6|p$.

In all cases, $6|p$. □

Proof. We prove by induction(strong).

Basis:

If $n = 1$ then the statement S_1 is $6|1*2*3$. This simplifies to $6|6$, which is true because 6 = 6 * 1.

If $n = 2$ then the statement S_2 is $6|2*3*4$. This simplifies to $6|24$, which is true because 24 = 6 * 4.

Induction:

We must prove $S_1 \wedge S_2 \wedge ... \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$.

This implies we must prove $S_{k-1} \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$.

For simplicity, let $m = k-1$.

Then $S_{k-1} \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$ becomes

$S_m \wedge S_{m+1} \Rightarrow S_{m+2}$ for $m \geq 1$.

We prove the latter statement using direct proof.

Suppose $S_m \wedge S_{m+1}$ for $m \geq 1$.

We must prove that these assumptions together imply S_{m+2}.

Since $S_m \wedge S_{m+1}$ is true by assumption, then S_m is certainly true.

This implies $6|m(m+1)(m+2)$ which implies $m(m+1)(m+2) = 6a, a \in \mathbb{Z}$, by definition of divisibility.

Thus $m(m+1)(m+2) = m(m^2+3m+2) = m^3+3m^2+2m = 6a$.

Observe the following equalities:

$$\begin{aligned}(m+2)(m+3)(m+4) &= (m+2)(m^2+7m+12)\\ &= m^3+9m^2+26m+24\\ &= (m^3+3m^2+2m)+(6m^2+24m+24)\\ &= 6a+6(m^2+4m+4)\\ &= 6(a+m^2+4m+4)\end{aligned}$$

Since $a+m^2+4m+4 \in \mathbb{Z}$, then by definition of divisibility, $6|(m+2)(m+3)(m+4)$.

Hence $S_m \wedge S_{m+1} \Rightarrow S_{m+2}$ for $m \geq 1$.

Thus, $S_{k-1} \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$.

It follows by strong induction that $6|n(n+1)(n+2)$ for all $n \in \mathbb{N}$. ☐

Exercise 63. The number 6 is the largest natural number that divides $n^3 - n$ for all $n \in \mathbb{N}$.

Proof. We must prove

1. For all natural numbers n, $6|(n^3-n)$.
2. If $m \in \mathbb{N}$ and $m > 6$, then there exists $n \in \mathbb{N}$ such that m does not divide $n^3 - n$.

We first prove $6|(n^3-n)$ for all $n \in \mathbb{N}$ by induction on n.

Let $p(n)$ be the predicate $6|(n^3-n)$ defined over $\mathbb{N}$.

We prove $p(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Basis:

Since $1^3 - 1 = 0$ and $6|0$, then $p(1)$ is true.

Induction:

Let $k \in \mathbb{N}$ such that $p(k)$ is true.

Then 6 divides $k^3 - k$.

Observe that $(k+1)^3-(k+1) = (k^3+3k^2+3k+1)-k-1 = k^3+3k^2+3k-k = (k^3-k)+(3k^2+3k) = (k^3-k)+3k(k+1)$.

Since the product of two consecutive integers is even and $k(k+1)$ is the product of two consecutive integers, then $k(k+1)$ is even, so $2|k(k+1)$.

Hence, $3 \cdot 2|3k(k+1)$, so $6|3k(k+1)$.

Since 6 divides k^3-k and 6 divides $3k(k+1)$, then 6 divides the sum $(k^3-k)+3k(k+1) = (k+1)^3-(k+1)$.

Thus, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for any $k \geq 1$.

It follows by induction that $6|(n^3 - n)$ for all $n \in \mathbb{N}$. ☐

Proof. We next prove:

If $m \in \mathbb{N}$ and $m > 6$, then there exists $n \in \mathbb{N}$ such that m does not divide $n^3 - n$.

Let $m \in \mathbb{N}$ with $m > 6$.

Let n be the natural number 2.

Then $n^3 - n = 2^3 - 2 = 6$.

If $m \in \mathbb{N}$ and $m|6$, then $m \leq 6$, so if $m \in \mathbb{N}$ and $m > 6$, then m does not divide 6.

Since $m \in \mathbb{N}$ and $m > 6$, then we conclude m does not divide 6, so m does not divide $n^3 - n$.

Therefore, there does exist $n \in \mathbb{N}$ such that m does not divide $n^3 - n$, as desired. ☐

Exercise 64. Let $x, y \in \mathbb{Z}$.

If $17|(2x+3y)$, then $17|(9x+5y)$.

Proof. Suppose $17|(2x+3y)$.

Then $2x + 3y = 17m$ for some integer m.

To prove $17|(9x+5y)$, we must prove there exists $n \in \mathbb{Z}$ such that $9x+5y = 17n$.

Let $n = -4m + x + y$.

Since $m, x, y \in \mathbb{Z}$, then $n \in \mathbb{Z}$.

Observe that

$$\begin{aligned}
17n &= 17(-4m + x + y) \\
&= 17(-4m) + 17(x+y) \\
&= (-4)(17m) + 17(x+y) \\
&= (-4)(2x+3y) + 17(x+y) \\
&= -8x - 12y + 17x + 17y \\
&= 9x + 5y.
\end{aligned}$$

Since $17n = 9x + 5y$, then $17|(9x+5y)$. ☐

Exercise 65. Let $a, b \in \mathbb{Z}$ with $b > 0$.

Then there exist unique integers q and r such that $a = bq + r$ with $2b \leq r < 3b$.

Proof. Since $a, b \in \mathbb{Z}$ and $b > 0$, then by the division algorithm, there exist unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.

Since $b, q, r \in \mathbb{Z}$, then $b(q+2) + (r-2b) \in \mathbb{Z}$.

Since $b(q+2) + (r-2b) \in \mathbb{Z}$ and $b \in \mathbb{Z}$ and $b > 0$, then by the division algorithm, when $b(q+2) + (r-2b)$ is divided by b, the remainder is $r - 2b$ with $0 \leq r - 2b < b$.

Observe that $b(q+2) + (r-2b) = bq + 2b + r - 2b = bq + r = a$.

Since $0 \le r - 2b < b$, then $2b \le r < 3b$.

Therefore, there exist unique integers q and r such that $a = bq + r$ and $2b \le r < 3b$. ☐

Exercise 66. Any integer of the form $6k+5$ is also of the form $3k+2$, but not conversely.

Proof. Let $k \in \mathbb{Z}$.

Then $6k + 5 = 6k + 3 + 2 = 3(2k + 1) + 2$.

Let $m = 2k + 1$.

Since $k \in \mathbb{Z}$, then $m \in \mathbb{Z}$, so $6k + 5 = 3m + 2$.

Therefore, any integer of the form $6k+5$ is also of the form $3m+2$ for some integer m.

Conversely, consider the integer 14.

Since $14 = 3 \cdot 4 + 2$, then 14 is of the form $3m + 2$ with $m = 4$.

If $14 = 6k + 5$, then $9 = 6k$, so $k = \frac{3}{2} \notin \mathbb{Z}$.

Thus, there is no integer k such that $14 = 6k + 5$.

Therefore, 14 is of the form $3m + 2$, but not of the form $6k + 5$. ☐

Exercise 67. Every odd integer is either of the form $4k + 1$ or $4k + 3$.

Proof. Let n be any odd integer.

By the division algorithm, there exist unique integers q and r such that $n = 4q + r$ with $0 \le r < 4$.

Thus, either $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$.

Since n is odd, then this implies either $n = 4q + 1$ or $n = 4q + 3$. ☐

Exercise 68. The square of any integer is either of the form $3k$ or $3k + 1$.

Proof. Let $n \in \mathbb{Z}$.

By the division algorithm, there exist unique integers q and r such that $n = 3q + r$ with $0 \le r < 3$.

Thus, either $n = 3q$ or $n = 3q + 1$ or $n = 3q + 2$.

We consider these cases separately.

Case 1: Suppose $n = 3q$.

Then $n^2 = (3q)^2 = 3^2q^2 = 3(3q^2)$.

Let $k = 3q^2$.

Then $k \in \mathbb{Z}$ and $n^2 = 3k$.

Case 2: Suppose $n = 3q + 1$.

Then $n^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$.

Let $k = 3q^2 + 2q$.

Then $k \in \mathbb{Z}$ and $n^2 = 3k + 1$.

Case 3: Suppose $n = 3q + 2$.

Then $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$.

Let $k = 3q^2 + 4q + 1$.

Then $n^2 = 3k + 1$.

Therefore, in all cases, either $n^2 = 3k$ or $n^2 = 3k+1$ for some integer k. □

Exercise 69. The cube of any integer is either of the form $9k$, $9k+1$, or $9k+8$.

Proof. Let $n \in \mathbb{Z}$.
By the division algorithm, there exist unique integers q and r such that $n = 3q + r$ with $0 \leq r < 3$.
Thus, either $n = 3q$ or $n = 3q+1$ or $n = 3q+2$.
We consider these cases separately.
Case 1: Suppose $n = 3q$.
Then $n^3 = (3q)^3 = 27q^3 = 9(3q^3) = 9k$ for integer $k = 3q^3$.
Case 2: Suppose $n = 3q+1$.
Then $n^3 = (3q+1)^3 = 27q^3 + 27q^2 + 9q + 1 = 9q(3q^2+3q+1) + 1 = 9k+1$ for integer $k = q(3q^2+3q+1)$.
Case 3: Suppose $n = 3q+2$.
Then $n^3 = (3q+2)^3 = 27q^3 + 54q^2 + 36q + 8 = 9q(3q^2+6q+4) + 8 = 9k+8$ for integer $k = q(3q^2+6q+4)$. □

Exercise 70. If an integer is both a square and a cube, then it must be either of the form $7k$ or $7k+1$.

Solution. We prove:
1. Every square is of the form $7k, 7k+1, 7k+2, 7k+4$.
2. Every cube is of the form $7k, 7k+1, 7k+6$.

So, this would imply any integer that is both a square and a cube must be of a form that it common to both squares and cubes.
We observe that if n is a square and a cube, then $n = a^6$ for $a \in \mathbb{Z}^+$. □

Proof. We first prove every square is of the form $7k, 7k+1, 7k+2$ or $7k+4$ for some integer k.
Let $n \in \mathbb{Z}$.
Suppose n is a square.
Then $n = a^2$ for some integer a.
By the division algorithm, there exist unique integers q and r such that $a = 7q + r$ with $0 \leq r < 7$.
Thus, either $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$ or $r = 4$ or $r = 5$ or $r = 6$.
We consider these cases separately.
Case 1: Suppose $r = 0$.
Then $a = 7q$.
Therefore, $n = (7q)^2 = 7^2q^2 = 7(7q^2) = 7k$ for integer $k = 7q^2$.
Case 2: Suppose $r = 1$.
Then $a = 7q+1$.
Therefore, $n = (7q+1)^2 = 49q^2 + 14q + 1 = 7q(7q+2) + 1 = 7k+1$ for integer $k = q(7q+2)$.
Case 3: Suppose $r = 2$.
Then $a = 7q+2$.

Therefore, $n = (7q+2)^2 = 49q^2 + 28q + 4 = 7q(7q+4) + 4 = 7k + 4$ for integer $k = q(7q+4)$.

Case 4: Suppose $r = 3$.

Then $a = 7q + 3$.

Therefore, $n = (7q+3)^2 = 49q^2 + 42q + 9 = 7(7q^2) + 7(6q) + (7 * 1 + 2) = 7(7q^2 + 6q + 1) + 2 = 7k + 2$ for integer $k = 7q^2 + 6q + 1$.

Case 5: Suppose $r = 4$.

Then $a = 7q + 4$.

Therefore, $n = (7q+4)^2 = 49q^2 + 56q + 16 = 7(7q^2) + 7 * 8q + (7 * 2 + 2) = 7(7q^2 + 8q + 2) + 2 = 7k + 2$ for integer $k = 7q^2 + 8q + 2$.

Case 6: Suppose $r = 5$.

Then $a = 7q + 5$.

Therefore, $n = (7q+5)^2 = 49q^2 + 70q + 25 = 7(7q^2) + 7 * 10q + (7 * 3 + 4) = 7(7q^2 + 10q + 3) + 4 = 7k + 4$ for integer $k = 7q^2 + 10q + 3$.

Case 7: Suppose $r = 6$.

Then $a = 7q + 6$.

Therefore, $n = (7q+6)^2 = 49q^2 + 84q + 36 = 7(7q^2) + 7 * 12q + (7 * 5 + 1) = 7(7q^2 + 12q + 5) + 1 = 7k + 1$ for integer $k = 7q^2 + 12q + 5$.

Therefore, in all cases, either $n = 7k$ or $n = 7k+1$ or $n = 7k+2$ or $n = 7k+4$ for some integer k. □

Proof. We next prove every cube is of the form $7k, 7k+1$, or $7k+6$ for some integer k.

Let $n \in \mathbb{Z}$.

Suppose n is a cube.

Then $n = a^3$ for some integer a.

We must prove either $n = 7k$ or $n = 7k+1$ or $n = 7k+6$.

By the division algorithm, there exist unique integers q and r such that $a = 7q + r$ with $0 \leq r < 7$.

Thus, either $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$ or $r = 4$ or $r = 5$ or $r = 6$.

We consider these cases separately.

Case 1: Suppose $r = 0$.

Then $a = 7q$.

Therefore, $n = (7q)^3 = 7^3q^3 = 7(7^2q^3) = 7(49q^3) = 7k$ for integer $k = 49q^3$.

Case 2: Suppose $r = 1$.

Then $a = 7q + 1$.

Observe that

$$
\begin{aligned}
n &= (7q+1)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k} \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2 + \binom{3}{2}(7q) + \binom{3}{3} \\
&= (7q)^3 + 3(7q)^2 + 3(7q) + 1 \\
&= (7^3q^3) + 3(7^2q^2) + 3(7q) + 1 \\
&= 7(7^2q^3 + 3 * 7q^2 + 3q) + 1 \\
&= 7(49q^3 + 21q^2 + 3q) + 1.
\end{aligned}
$$

Therefore, $n = 7(49q^3+21q^2+3q)+1 = 7k+1$ for integer $k = 49q^3+21q^2+3q$.
Case 3: Suppose $r = 2$.
Then $a = 7q + 2$.
Observe that

$$
\begin{aligned}
n &= (7q+2)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(2^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(2^1) + \binom{3}{2}(7q)(2^2) + \binom{3}{3}(2^3) \\
&= (7q)^3 + 3(7q)^2(2) + 3(7q)(2^2) + 8 \\
&= (7^3q^3) + (3)(2)(7^2q^2) + (3)(2^2)(7q) + (7 * 1 + 1) \\
&= 7(7^2q^3 + (3)(2) * 7q^2 + (3)(2^2)q + 1) + 1 \\
&= 7(49q^3 + 42q^2 + 12q + 1) + 1.
\end{aligned}
$$

Therefore, $n = 7k + 1$ for integer $k = 49q^3 + 42q^2 + 12q$.
Case 4: Suppose $r = 3$.
Then $a = 7q + 3$.
Observe that

$$\begin{aligned}
n &= (7q+3)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(3^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(3^1) + \binom{3}{2}(7q)(3^2) + \binom{3}{3}(3^3) \\
&= (7q)^3 + 3(7q)^2(3) + 3(7q)(3^2) + 27 \\
&= (7^3q^3) + (3)(3)(7^2q^2) + (3)(3^2)(7q) + (7*3+6) \\
&= 7(7^2q^3 + (3)(3)*7q^2 + (3)(3^2)q + 3) + 6 \\
&= 7(49q^3 + 63q^2 + 27q + 3) + 6.
\end{aligned}$$

Therefore, $n = 7k+6$ for integer $k = 49q^3 + 63q^2 + 27q + 3$.
Case 5: Suppose $r = 4$.
Then $a = 7q+4$.
Observe that

$$\begin{aligned}
n &= (7q+4)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(4^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(4^1) + \binom{3}{2}(7q)(4^2) + \binom{3}{3}(4^3) \\
&= (7q)^3 + 3(7q)^2(4) + 3(7q)(4^2) + 64 \\
&= (7^3q^3) + (3)(4)(7^2q^2) + (3)(4^2)(7q) + (7*9+1) \\
&= 7(7^2q^3 + (3)(4)*7q^2 + (3)(4^2)q + 9) + 1 \\
&= 7(49q^3 + 108q^2 + 48q + 9) + 1.
\end{aligned}$$

Therefore, $n = 7k+1$ for integer $k = 49q^3 + 108q^2 + 48q + 9$.
Case 6: Suppose $r = 5$.
Then $a = 7q+5$.
Observe that

$$
\begin{aligned}
n &= (7q+5)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(5^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(5^1) + \binom{3}{2}(7q)(5^2) + \binom{3}{3}(5^3) \\
&= (7q)^3 + 3(7q)^2(5) + 3(7q)(5^2) + 125 \\
&= (7^3q^3) + (3)(5)(7^2q^2) + (3)(5^2)(7q) + (7*17+6) \\
&= 7(7^2q^3 + (3)(5)*7q^2 + (3)(5^2)q + 17) + 6 \\
&= 7(49q^3 + 105q^2 + 75q + 17) + 6.
\end{aligned}
$$

Therefore, $n = 7q + 6$ for integer $k = 49q^3 + 105q^2 + 75q + 17$.
Case 7: Suppose $r = 6$.
Then $a = 7q + 6$.
Observe that

$$
\begin{aligned}
n &= (7q+6)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(6^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(6^1) + \binom{3}{2}(7q)(6^2) + \binom{3}{3}(6^3) \\
&= (7q)^3 + 3(7q)^2(6) + 3(7q)(6^2) + 216 \\
&= (7^3q^3) + (3)(6)(7^2q^2) + (3)(6^2)(7q) + (7*30+6) \\
&= 7(7^2q^3 + (3)(6)*7q^2 + (3)(6^2)q + 30) + 6 \\
&= 7(49q^3 + 126q^2 + 108q + 30) + 6.
\end{aligned}
$$

Therefore, $n = 7k + 6$ for integer $k = 49q^3 + 126q^2 + 108q + 30$.

Therefore, in all cases, either $n = 7k$ or $n = 7k + 1$ or $n = 7k + 6$ for some integer k. ☐

Proof. Let $n \in \mathbb{Z}$.

Suppose n is a square and a cube.

Then n is a square and n is a cube.

Since every square is of the form $7k, 7k+1, 7k+2, 7k+4$ for some integer k and n is a square, then n is of the form $7k, 7k+1, 7k+2, 7k+4$ for some integer k.

Since every cube is of the form $7m, 7m+1, 7m+6$ for some integer m and n is a cube, then n is of the form $7k, 7k+1, 7k+6$.

Since n is both a square and a cube, then this implies n is of the form that is common to both a square and a cube, so n is of the form $7k$ or $7k+1$. ☐

Exercise 71. There is no integer in the sequence $11, 111, 1111, 11111, ...$ that is a perfect square.

Proof. Let (a_n) be the sequence $11, 111, 1111, 11111, ...$

Then $a_n = 10 * a_{n-1} + 1$ for positive integers $n > 1$ and $a_1 = 11$.

We first prove each term of the sequence has the form $4k+3$ for some integer k.

Thus, we must prove for all $n \in \mathbb{Z}^+$, there exists $k \in \mathbb{Z}$ such that $a_n = 4k+3$.

We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : (\exists k \in \mathbb{Z})(a_n = 4k+3)\}$.

Basis:

Since $1 \in \mathbb{Z}^+$ and $2 \in \mathbb{Z}$ and $a_1 = 11 = 4 * 2 + 3$, then $1 \in S$.

Since $2 \in \mathbb{Z}^+$ and $27 \in \mathbb{Z}$ and $a_2 = 10*a_1+1 = 10*11+1 = 111 = 4*27+3$, then $2 \in S$.

Induction:

Suppose $m \in S$ and $m \geq 2$.

Then $m \in \mathbb{Z}^+$ and there exists $k \in \mathbb{Z}$ such that $a_m = 4k+3$.

Since $m \in \mathbb{Z}^+$, then $m+1 \in \mathbb{Z}^+$.

Since $m+1 > m \geq 2 > 1$, then $m+1 > 1$.

Observe that

$$\begin{aligned} a_{m+1} &= 10a_m + 1 \\ &= 10(4k+3)+1 \\ &= 40k+31 \\ &= 4*10k + (4*7+3) \\ &= 4(10k+7)+3. \end{aligned}$$

Let $p = 10k+7$.

Since $k \in \mathbb{Z}$, then $p \in \mathbb{Z}$ and $a_{m+1} = 4p+3$.

Since $m+1 \in \mathbb{Z}^+$ and there exists $p \in \mathbb{Z}$ such that $a_{m+1} = 4p+3$, then $m+1 \in S$.

Hence, $m \in S$ for $m \geq 2$ implies $m+1 \in S$.

Therefore, by PMI, for all $n \in \mathbb{Z}^+$, there exists $k \in \mathbb{Z}$ such that $a_n = 4k+3$. $\square$

Proof. We next prove every perfect square is either of the form $4k$ or $4k+1$.

Let n be a perfect square.

Then $n \in \mathbb{Z}$ and $n = a^2$ for some integer a.

From a previous exercise we know that the square of an integer leaves remainder 0 or 1 upon division by 4.

Hence, a^2 leaves remainder 0 or 1 upon division by 4, so either $a^2 = 4k$ or $a^2 = 4k+1$ for some integer k.

Therefore, either $n = 4k$ or $n = 4k+1$ for some integer k. $\square$

Proof. We prove the term a_n cannot be a perfect square.

Let a_n be a term of the sequence $11, 111, 1111, ...$

Then a_n has the form $4k + 3$ for some integer k, so a_n is of the form $4k + 3$.

Every perfect square is either of the form $4k$ or $4k + 1$, so if n is a perfect square, then either $n = 4k$ or $n = 4k + 1$.

Hence, if $n \neq 4k$ and $n \neq 4k + 1$, then n is not a perfect square.

Since $4k + 3 \neq 4k$ and $4k + 3 \neq 4k + 1$, then $4k + 3$ is not a perfect square, so a_n is not a perfect square.

Therefore, every term of the sequence $11, 111, 1111, ...$ is not a perfect square, so there is no term of the sequence that is a perfect square. □

Exercise 72. For all $n \in \mathbb{Z}^+$, 7 divides $2^{3n} - 1$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : 7|(2^{3n} - 1)\}$.

Basis:

Since $2^{3*1} - 1 = 7 = 7 * 1$, then 7 divides $2^{3*1} - 1$, so $1 \in S$.

Induction:

Suppose $k \in S$.

Then $k \in \mathbb{Z}^+$ and $7|(2^{3k} - 1)$.

Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$.

Since $7|(2^{3k} - 1)$, then $2^{3k} - 1 = 7x$ for some integer x.

Observe that

$$\begin{aligned} 2^{3(k+1)} - 1 &= 2^{3k+3} - 1 \\ &= 2^{3k} * 2^3 - 1 \\ &= 8 * 2^{3k} - 1 \\ &= 8(2^{3k} - 1) + 8 - 1 \\ &= 8(7x) + 7 \\ &= 7(8x + 1). \end{aligned}$$

Since $x \in \mathbb{Z}$, then $8x + 1 \in \mathbb{Z}$, so 7 divides $2^{3(k+1)} - 1$.

Since $k + 1 \in \mathbb{Z}^+$ and 7 divides $2^{3(k+1)} - 1$, then $k + 1 \in S$.

Hence, $k \in S$ implies $k + 1 \in S$.

Therefore, by PMI, $7|(2^{3n} - 1)$ for all $n \in \mathbb{Z}^+$. □

Exercise 73. For all $n \in \mathbb{Z}^+$, 8 divides $3^{2n} + 7$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : 8|3^{2n} + 7\}$.

Basis:

Since $3^{2*1} + 7 = 16 = 8 * 2$, then 8 divides $3^{2*1} + 7$, so $1 \in S$.

Induction:

Suppose $k \in S$.

Then $k \in \mathbb{Z}^+$ and $8|(3^{2k} + 7)$.

Since $k \in \mathbb{Z}^+$, then $k+1 \in \mathbb{Z}^+$.
Since $8|(3^{2k}+7)$, then $3^{2k}+7 = 8x$ for some integer x.
Observe that

$$\begin{aligned}
3^{2(k+1)} + 7 &= 3^{2k+2} + 7 \\
&= 3^{2k} * 3^2 + 7 \\
&= 9 * 3^{2k} + 7 \\
&= (8+1)3^{2k} + 7 \\
&= 8(3^{2k}) + 3^{2k} + 7 \\
&= 8(3^{2k}) + 8x \\
&= 8(3^{2k} + x) \\
&= 8(9^k + x).
\end{aligned}$$

Since $k, x \in \mathbb{Z}$, then $9^k + x \in \mathbb{Z}$, so 8 divides $3^{2(k+1)} + 7$.
Since $k+1 \in \mathbb{Z}^+$ and 8 divides $3^{2(k+1)} + 7$, then $k+1 \in S$.
Hence, $k \in S$ implies $k+1 \in S$.
Therefore, by PMI, $8|(3^{2n}+7)$ for all $n \in \mathbb{Z}^+$. □

Exercise 74. For all $n \in \mathbb{Z}^+$, $2^n + (-1)^{n+1}$ is divisible by 3.

Proof. We prove by induction on n.
Let $S = \{n \in \mathbb{Z}^+ : 3|2^n + (-1)^{n+1}\}$.
Basis:
Since $2^1 + (-1)^{1+1} = 2+1 = 3 = 3 \cdot 1$, then 3 divides $2^1 + (-1)^{1+1}$, so $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{Z}^+$ and $3|2^k + (-1)^{k+1}$.
Since $k \in \mathbb{Z}^+$, then $k+1 \in \mathbb{Z}^+$.
Since $3|2^k + (-1)^{k+1}$, then $2^k + (-1)^{k+1} = 3x$ for some integer x.
Observe that

$$\begin{aligned}
2^{k+1} + (-1)^{(k+1)+1} &= 2^k \cdot 2 + (-1)^{k+1}(-1) \\
&= 2^k + 2^k - (-1)^{k+1} \\
&= 2^k + (2-1)2^k - (-1)^{k+1} \\
&= 2^k + 2(2^k) - 2^k - (-1)^{k+1} \\
&= 3(2^k) - [2^k + (-1)^{k+1}] \\
&= 3(2^k) - 3x \\
&= 3(2^k - x).
\end{aligned}$$

Since $k, x \in \mathbb{Z}$, then $2^k - x \in \mathbb{Z}$, so 3 divides $2^{k+1} + (-1)^{(k+1)+1}$.
Since $k+1 \in \mathbb{Z}^+$ and 3 divides $2^{k+1} + (-1)^{(k+1)+1}$, then $k+1 \in S$.
Hence, $k \in S$ implies $k+1 \in S$.
Therefore, by PMI, $3|(2^n + (-1)^{n+1})$ for all $n \in \mathbb{Z}^+$. □

Lemma 75. *Every perfect square is of the form $4k$ or $4k+1$ for some integer k.*

Proof. Let $n \in \mathbb{Z}$.

By the division algorithm, there exist unique integers q and r such that $n = 2q + r$ with $0 \leq r < 2$.

Thus, either $n = 2q$ or $n = 2q + 1$.

We consider these cases separately.

Case 1: Suppose $n = 2q$.

Then, $n^2 = (2q)^2 = 4q^2 = 4k^2$ for integer $k = q$.

Case 2: Suppose $n = 2q + 1$.

Then $n^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1 = 4k + 1$ for integer $k = q^2 + q$.

Therefore either $n^2 = 4k$ or $n^2 = 4k + 1$ for some integer k. □

Lemma 76. *Let $n \in \mathbb{Z}$.*

If n is odd, then $8|(n^2 - 1)$.

Proof. Suppose n is odd.

By the division algorithm, there are unique integers q and r such that $n = 4q + r$ with $0 \leq r < 4$.

Thus, either $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$.

Hence, either $n = 2(2q)$ or $n = 2(2q)+1$ or $n = 2(2q+1)$ or $n = 2(2q+1)+1$.

Since n is odd, then this implies either $n = 4q + 1$ or $n = 4q + 3$.

We consider each case separately.

Case 1: Suppose $n = 4q + 1$.

Then $n^2 - 1 = (4q+1)^2 - 1 = 16q^2 + 8q + 1 - 1 = 16q^2 + 8q = 8(2q^2 + q)$.

Since $2q^2 + q \in \mathbb{Z}$, then this implies $8|(n^2 - 1)$.

Case 2: Suppose $n = 4q + 3$.

Then $n^2 - 1 = (4q+3)^2 - 1 = 16q^2 + 24q + 9 - 1 = 16q^2 + 24q + 8 = 8(2q^2 + 3q + 1)$.

Since $2q^2 + 3q + 1 \in \mathbb{Z}$, then this implies $8|(n^2 - 1)$.

Therefore, in all cases, $8|(n^2 - 1)$. □

Proof. Suppose n is odd.

Then $n = 2a + 1$ for some integer a.

Thus $n^2 - 1 = (2a+1)^2 - 1 = 4a^2 + 4a = 4a(a+1)$.

Since a and $a + 1$ have opposite parity we know that their product must be even by proposition **??**.

Thus $a(a+1) = 2b$ for some integer b.

Consequently $n^2 - 1 = 4(2b) = 8b$, and so $8|(n^2 - 1)$. □

Exercise 77. Let $a \in \mathbb{Z}$.

If $2 \nmid a$ and $3 \nmid a$, then $24|(a^2 - 1)$.

Proof. Suppose $2 \nmid a$ and $3 \nmid a$.

Since $2 \nmid a$, then a is odd.

Hence, we know that $8|(a^2 - 1)$.

Since $3 \not| a$, then by the division algorithm, either $a = 3m + 1$ or $a = 3m + 2$ for some integer m.

If $a = 3m+1$, then $a^2 - 1 = (3m+1)^2 - 1 = 9m^2 + 6m + 1 - 1 = 9m^2 + 6m = 3m(3m+2)$, so $3|(a^2 - 1)$.

If $a = 3m + 2$, then $a^2 - 1 = (3m + 2)^2 - 1 = 9m^2 + 12m + 4 - 1 = 9m^2 + 12m + 3 = 3(3m^2 + 4m + 1)$, so $3|(a^2 - 1)$.

In either case, $3|(a^2 - 1)$.

Since $8|(a^2 - 1)$ and $3|(a^2 - 1)$ and $\gcd(8, 3) = 1$, then $(8 * 3)$ divides $a^2 - 1$, so 24 divides $a^2 - 1$. ☐

Exercise 78. Let a and b be odd integers.

Then $8|(a^2 - b^2)$.

Proof. Since a is odd, then we know $8|(a^2 - 1)$, so $a^2 - 1 = 8k$ for some integer k.

Since b is odd, then we know $8|(b^2 - 1)$, so $b^2 - 1 = 8m$ for some integer m.

Thus, $a^2 - b^2 = (8k+1) - (8m+1) = 8k + 1 - 8m - 1 = 8k - 8m = 8(k - m)$.

Since $k, m \in \mathbb{Z}$, then $k - m \in \mathbb{Z}$, so $8|(a^2 - b^2)$. ☐

Exercise 79. If m and n are odd integers, then $m^2 - n^2$ is divisible by 8.

Proof. Suppose m and n are odd integers.

We prove if x is an odd integer, then $x^2 \equiv 1 \pmod 8$.

Suppose x is an odd integer.

Then $x = 2k + 1$ for some integer k.

Thus, $x^2 = 4k^2 + 4k + 1$.

The product of consecutive integers is even, so in particular, $k(k+1)$ is even.

Hence, $2|k(k + 1)$, so $4 * 2|4k(k + 1)$.

Thus, $8|(4k^2 + 4k)$, so $4k^2 + 4k \equiv 0 \pmod 8$.

Hence, $4k^2 + 4k + 1 \equiv 1 \pmod 8$, so $x^2 \equiv 1 \pmod 8$.

Therefore, $m^2 \equiv 1 \pmod 8$ and $n^2 \equiv 1 \pmod 8$.

Thus, $1 \equiv n^2 \pmod 8$.

Since $m^2 \equiv 1 \pmod 8$ and $1 \equiv n^2 \pmod 8$, then $m^2 \equiv n^2 \pmod 8$.

Hence, $8|(m^2 - n^2)$. ☐

Exercise 80. Let a be an odd integer.

Then $24|a(a^2 - 1)$.

Proof. Since $a(a^2 - 1) = a(a - 1)(a + 1) = (a - 1)a(a + 1)$, then $a(a^2 - 1)$ is a product of three consecutive integers.

Since the product of three consecutive integers is divisible by 3, then this implies $3|a(a^2 - 1)$.

Since a is odd, then we know $a^2 = 8k + 1$ for some integer k, so $a^2 - 1 = 8k$.

Hence, $8|(a^2 - 1)$, so 8 divides any multiple of $a^2 - 1$.

Thus, $8|a(a^2 - 1)$.

Since $3|a(a^2 - 1)$ and $8|a(a^2 - 1)$ and $\gcd(3, 8) = 1$, then $(3 * 8)$ divides $a(a^2 - 1)$, so $24|a(a^2 - 1)$. ☐

Exercise 81. The sum of the squares of two odd integers cannot be a perfect square.

Proof. Let x and y be two odd integers.

Then $x = 2a + 1$ and $y = 2b + 1$ for some integers a and b.

Thus,

$$\begin{aligned} x^2 + y^2 &= (2a+1)^2 + (2b+1)^2 \\ &= 4a^2 + 4a + 1 + 4b^2 + 4b + 1 \\ &= 4a^2 + 4b^2 + 4a + 4b + 2 \\ &= 4(a^2 + b^2 + a + b) + 2. \end{aligned}$$

Let $k = a^2 + b^2 + a + b$.

Then $x^2 + y^2 = 4k + 2$ and $k \in \mathbb{Z}$.

Every perfect square is of the form $4k$ or $4k+1$, so if x is a perfect square, then either $x = 4k$ or $x = 4k + 1$ for some integer k.

Hence, if $x \neq 4k$ and $x \neq 4k + 1$ for some integer k, then x cannot be a perfect square.

Since $x^2 + y^2 = 4k + 2$ and $4k + 2 \neq 4k$ and $4k + 2 \neq 4k + 1$, then $x^2 + y^2$ cannot be a perfect square. ☐

Exercise 82. The square of any odd integer is of the form $8k + 1$ for some integer k.

Proof. Let n be any odd integer.

By the division algorithm there exist unique integers q, r such that $n = 4q+r$ with $0 \leq r < 4$.

Thus, either $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$, so either $n = 2(2q)$ or $n = 2(2q) + 1$ or $n = 2(2q + 1)$ or $n = 2(2q + 1) + 1$.

Since n is odd, then this implies either $n = 4q + 1$ or $n = 4q + 3$.

We consider each case separately.

Case 1: Suppose $n = 4q + 1$.

Then $n^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + 2q) + 1 = 8k + 1$ for integer $k = 2q^2 + 2q$.

Case 2: Suppose $n = 4q + 3$.

Then $n^2 = (4q+3)^2 = 16q^2+24q+9 = 16q^2+24q+8+1 = 8(2q^2+3q+1)+1 = 8k + 1$ for integer $k = 2q^2 + 3q + 1$. ☐

Exercise 83. The product of four consecutive integers is one less than a perfect square.

Proof. Let $n \in \mathbb{Z}$.

We must prove there exists $m \in \mathbb{Z}$ such that $n(n+1)(n+2)(n+3) = m^2 - 1$.

Let $m = (n + 1)(n + 2) - 1$.

Since $n \in \mathbb{Z}$, then $m \in \mathbb{Z}$.

Observe that

$$
\begin{aligned}
m^2 - 1 &= [(n+1)(n+2)-1]^2 - 1 \\
&= (n^2+3n+1)^2 - 1 \\
&= (n^2+3n+1-1)(n^2+3n+1+1) \\
&= (n^2+3n)(n^2+3n+2) \\
&= n(n+3)(n+2)(n+1) \\
&= n(n+1)(n+2)(n+3).
\end{aligned}
$$

□

Exercise 84. Let $a \in \mathbb{Z}$.
If $2 \not| a$ and $3 \not| a$, then $24|(a^2+23)$.

Proof. Suppose $2 \not| a$ and $3 \not| a$.
Since $2 \not| a$, then a is odd, so we know $8|(a^2-1)$.
Since $8|(a^2-1)$ and $8|24$, then 8 divides the sum $(a^2-1)+24 = a^2+23$, so $8|(a^2+23)$.
Since $3 \not| a$, then by the division algorithm, either $a = 3q+1$ or $a = 3q+2$ for some integer q.
If $a = 3q+1$, then $a^2+23 = (3q+1)^2+23 = 9q^2+6q+1+23 = 9q^2+6q+24 = 3(3q^2+2q+8)$, so $3|(a^2+23)$.
If $a = 3q+2$, then $a^2+23 = (3q+2)^2+23 = 9q^2+12q+4+23 = 9q^2+12q+27 = 3(3q^2+4q+9)$, so $3|(a^2+23)$.
Thus, in either case, $3|(a^2+23)$.

Since $8|(a^2+23)$ and $3|(a^2+23)$ and $\gcd(8,3)=1$, then $(8*3)|(a^2+23)$, so $24|(a^2+23)$. □

Lemma 85. *The product of 5 consecutive integers is divisible by 5.*

Proof. Let $n \in \mathbb{Z}$.
Let $p = n(n+1)(n+2)(n+3)(n+4)$.
We must prove $5|p$.
By the division algorithm, either $p = 5q$ or $p = 5q+1$ or $p = 5q+2$ or $p = 5q+3$ or $p = 5q+4$ for some integer q.
We consider each case separately.
Case 1: Suppose $n = 5q$.
Then $5|n$, so 5 divides any multiple of n.
Hence, $5|p$.
Case 2: Suppose $n = 5q+1$.
Then $n+4 = (5q+1)+4 = 5q+5 = 5(q+1)$, so $5|(n+4)$.
Thus, 5 divides any multiple of $n+4$, so $5|p$.
Case 3: Suppose $n = 5q+2$.
Then $n+3 = (5q+2)+3 = 5q+5 = 5(q+1)$, so $5|(n+3)$.
Thus, 5 divides any multiple of $n+3$, so $5|p$.

Case 4: Suppose $n = 5q + 3$.
Then $n + 2 = (5q + 3) + 2 = 5q + 5 = 5(q + 1)$, so $5|(n + 2)$.
Thus, 5 divides any multiple of $n + 2$, so $5|p$.
Case 5: Suppose $n = 5q + 4$.
Then $n + 1 = (5q + 4) + 1 = 5q + 5 = 5(q + 1)$, so $5|(n + 1)$.
Thus, 5 divides any multiple of $n + 1$, so $5|p$.

Therefore, in all cases, $5|p$. □

Exercise 86. Let $n \in \mathbb{Z}$.
Then $360|n^2(n^2 - 1)(n^2 - 4)$.

Proof. Let $p = n^2(n^2 - 1)(n^2 - 4)$.
Then $p = n^2(n - 1)(n + 1)(n - 2)(n + 2)$.
We prove $5|p$ and $8|p$ and $9|p$. □

Proof. We prove $5|p$.
Observe that $p = (n - 2)(n - 1)n(n + 1)(n + 2)n$.
Let $a = (n - 2)(n - 1)n(n + 1)(n + 2)$.
Then $p = an$.
Since a is a product of 5 consecutive integers and the product of 5 consecutive integers is divisible by 5, then $5|a$.
Thus, 5 divides any multiple of a, so $5|p$. □

Proof. We prove $8|p$.
Either n is even or n is odd.
We consider each case separately.
Case 1: Suppose n is even.
Then $n = 2k$ for some integer k.
Since $n^2 = (2k)^2 = 4k^2$, then $4|n^2$.
Since $n + 2 = 2k + 2 = 2(k + 1)$, then $2|(n + 2)$.
Since $4|n^2$ and $2|(n + 2)$, then $(4 * 2)|n^2(n + 2)$, so $8|n^2(n + 2)$.
Thus, 8 divides any multiple of $n^2(n + 2)$, so $8|p$.
Case 2: Suppose n is odd.
Then we know 8 divides $n^2 - 1$.
Thus, 8 divides any multiple of $n^2 - 1$, so 8 divides p.

Therefore, in all cases, $8|p$. □

Proof. We prove $9|p$.
By the division algorithm, either $n = 3q$ or $n = 3q + 1$ or $n = 3q + 2$ for some integer q.
We consider each case separately.
Case 1: Suppose $n = 3q$.
Then $n^2 = (3q)^2 = 9q^2$, so $9|n^2$.
Hence, 9 divides any multiple of n^2, so $9|p$.
Case 2: Suppose $n = 3q + 1$.

Since $n-1=3q$, then $3|(n-1)$.
Since $n+2=(3q+1)+2=3q+3=3(q+1)$, then $3|(n+2)$.
Since $3|(n-1)$ and $3|(n+2)$, then $(3*3)|(n-1)(n+2)$, so $9|(n-1)(n+2)$.
Hence, 9 divides any multiple of $(n-1)(n+2)$, so $9|p$.
Case 3: Suppose $n=3q+2$.
Since $n+1=(3q+2)+1=3q+3=3(q+1)$, then $3|(n+1)$.
Since $n-2=3q$, then $3|(n-2)$.
Since $3|(n+1)$ and $3|(n-2)$, then $(3*3)|(n+1)(n-2)$, so $9|(n+1)(n-2)$.
Hence, 9 divides any multiple of $(n+1)(n-2)$, so $9|p$.

Therefore, in all cases, $9|p$. □

Proof. Since $5|p$ and $8|p$ and $\gcd(5,8)=1$, then $(5*8)|p$, so $40|p$.
Since $40|p$ and $9|p$ and $\gcd(40,9)=1$, then $(40*9)|p$, so $360|p$. □

Exercise 87. For all $n \in \mathbb{N}$, n^3+5n is divisible by 6.

Proof. To prove the statement n^3+5n is divisible by 6 for all $n \in \mathbb{N}$, we prove $6|(n^3+5n)$ for all $n \in \mathbb{N}$ by induction on n.

Let $p(n): 6|(n^3+5n)$ be a predicate defined over $\mathbb{N}$.
Basis:
Since $1^3+5*1=6$ and $6|6$, then the statement $p(1)$ is true.
Induction:
Let $k \in \mathbb{N}$ such that $p(k)$ is true.
Then $6|(k^3+5k)$, so there exists an integer m such that $k^3+5k=6m$.

Since the product of two consecutive integers is even and $k \in \mathbb{Z}$, then $k(k+1)$ is even, so there exists $n \in \mathbb{Z}$ such that $k(k+1)=2n$.

Observe that

$$\begin{aligned}
(k+1)^3+5(k+1) &= k^3+3k^2+8k+6 \\
&= k^3+8k+3k^2+6 \\
&= k^3+(5k+3k)+3k^2+6 \\
&= (k^3+5k)+(3k+3k^2)+6 \\
&= (k^3+5k)+(3k^2+3k)+6 \\
&= 6m+3k(k+1)+6 \\
&= 6m+3(2n)+6 \\
&= 6m+6n+6 \\
&= 6(m+n+1)
\end{aligned}$$

Since $m+n+1 \in \mathbb{Z}$, then $6|((k+1)^3+5(k+1))$, so $p(k+1)$ is true.
Therefore, by PMI, the statement $6|(n^3+5n)$ is true for all $n \in \mathbb{N}$. □

Exercise 88. For all $n \in \mathbb{Z}^+$, $n(n+1)(2n+1)$ is divisible by 6.

Proof. By the division algorithm there exist unique integers q, r such that $n = 6q + r$ with $0 \leq r < 6$, so either $n = 6q$ or $n = 6q+1$ or $n = 6q+2$ or $n = 6q+3$ or $n = 6q + 4$ or $n = 6q + 5$.

We consider each case separately.

Case 1: Suppose $n = 6q$.

Then $6|n$, so 6 divides any multiple of n.

Therefore, $6|n(n + 1)(2n + 1)$.

Case 2: Suppose $n = 6q + 1$.

Then $n+1 = 6q+2 = 2(3q+1)$ and $2n+1 = 2(6q+1)+1 = 12q+3 = 3(4q+1)$, so $(n + 1)(2n + 1) = 6(3q + 1)(4q + 1)$.

Hence, $6|(n + 1)(2n + 1)$, so 6 divides any multiple of $(n + 1)(2n + 1)$.

Therefore, $6|n(n + 1)(2n + 1)$.

Case 3: Suppose $n = 6q + 2$.

Then $n = 2(3q + 1)$ and $n + 1 = 6q + 3 = 3(2q + 1)$, so $n(n + 1) = 6(3q + 1)(2q + 1)$.

Hence, $6|n(n + 1)$, so 6 divides any multiple of $n(n + 1)$.

Therefore, $6|n(n + 1)(2n + 1)$.

Case 4: Suppose $n = 6q + 3$.

The $n = 3(2q+1)$ and $n+1 = 6q+4 = 2(3q+2)$, so $n(n+1) = 6(2q+1)(3q+2)$.

Hence, $6|n(n + 1)$, so 6 divides any multiple of $n(n + 1)$.

Therefore, $6|n(n + 1)(2n + 1)$.

Case 5: Suppose $n = 6q + 4$.

Then $n = 2(3q + 2)$ and $2n + 1 = 2(6q + 4) + 1 = 12q + 9 = 3(4q + 3)$, so $n(2n + 1) = 6(3q + 2)(4q + 3)$.

Hence, $6|n(2n + 1)$, so 6 divides any multiple of $n(2n + 1)$.

Therefore, $6|n(n + 1)(2n + 1)$.

Case 6: Suppose $n = 6q + 5$.

Then $n + 1 = 6q + 6 = 6(q + 1)$, so $6|(n + 1)$.

Hence, 6 divides any multiple of $n + 1$.

Therefore, $6|n(n + 1)(2n + 1)$. □

Exercise 89. The number 2 is not a square.

Proof. Suppose 2 is a square.

Then $2 = n^2$ for some integer n, so, $n|2$,

We may assume $n > 0$, since $(-n)^2 = n^2$.

Since $2 = 2 * 1$, then either $n = 1$ or $n = 2$.

If $n = 1$, then $2 = n^2 = 1^2 = 1$, a contradiction.

If $n = 2$, then $2 = n^2 = 2^2 = 4$, a contradiction.

Therefore, 2 is not a square. □

Exercise 90. Let k be a positive odd integer.

Then any sum of k consecutive integers is divisible by k.

Solution. Let k be a positive odd integer.

To prove any sum of k consecutive integers is divisible by k, we let $n+1, n+2, ..., n+k$ be k consecutive integers for some integer n.

We must prove k divides the sum $(n+1)+(n+2)+...+(n+k)$.

Thus, we must prove there exists an integer a such that $(n+1)+(n+2)+...+(n+k)=ka$. $\square$

Proof. Let k be a positive odd integer.

Let $n+1, n+2, ..., n+k$ be k consecutive integers for some integer n.

To prove k divides the sum $\sum_{i=1}^{k}(n+i)$, we must find an integer m such that $\sum_{i=1}^{k}(n+i)=km$.

Observe that

$$\begin{aligned}\sum_{i=1}^{k}(n+i) &= \sum_{i=1}^{k}n+\sum_{i=1}^{k}i\\ &= kn+\frac{k(k+1)}{2}\\ &= k(n+\frac{k+1}{2}).\end{aligned}$$

Since k is odd, then there exists an integer a such that $k=2a+1$.

Thus, $\frac{k+1}{2}=\frac{2a+2}{2}=a+1\in\mathbb{Z}$.

Let $m=n+\frac{k+1}{2}$.

Since n and $\frac{k+1}{2}$ are integers, then m is an integer.

Hence, $\sum_{i=1}^{k}(n+i)=km$, as desired. $\square$

Exercise 91. Let $n\in\mathbb{N}$.

If n is odd, then $(a+b)|(a^n+b^n)$ for all $a,b,n\in\mathbb{Z}^+$.

Proof. Suppose n is odd.

Then $n=2k+1$ for some integer k.

Let $a,b\in\mathbb{Z}^+$.

Observe that

$$\begin{aligned}(a+b)\sum_{i=0}^{2k}(-1)^i a^{2k-i}b^i &= a\sum_{i=0}^{2k}(-1)^i a^{2k-i}b^i+b\sum_{i=0}^{2k}(-1)^i a^{2k-i}b^i\\ &= \sum_{i=0}^{2k}(-1)^i a^{2k+1-i}b^i+\sum_{i=0}^{2k}(-1)^i a^{2k-i}b^{i+1}\\ &= (a^{2k+1}-a^{2k}b+a^{2k-1}b^2+...+ab^{2k})+(a^{2k}b-a^{2k-1}b^2+...-ab^{2k}+b^{2k+1})\\ &= a^{2k+1}+b^{2k+1}\\ &= a^n+b^n.\end{aligned}$$

Since $\sum_{i=0}^{2k}(-1)^i a^{2k-i}b^i$ is an integer and $a^n+b^n=(a+b)\sum_{i=0}^{2k}(-1)^i a^{2k-i}b^i$, then $a+b$ divides a^n+b^n, so $a+b$ divides a^n+b^n for all $a,b\in\mathbb{Z}^+$.

Since n is odd and $a+b$ divides a^n+b^n for all $a,b\in\mathbb{Z}^+$, then we conclude: if n is odd, then $(a+b)|(a^n+b^n)$ for all $a,b,n\in\mathbb{Z}^+$, by conditional introduction. $\square$

Exercise 92. Let n be a positive integer.

Let

$$A = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Then $A^n = I$ iff $4|n$.

Solution. We compute values for A^n and observe a pattern.

Whenever n is a multiple of 4 we observe that $A^n = I$, where I is the identity matrix.

We must prove:

1. if $A^n = I$, then $4|n$.

We'll use the division algorithm to prove $A^n \neq I$.

2. if $4|n$, then $A^n = I$. Assume $4|n$.

We compute A^n. □

Proof. Observe that $A^4 = I$ where I is the identity matrix.

We prove if $4|n$, then $A^n = I$.

Suppose $4|n$.

Then there exists an integer k such that $n = 4k$.

Thus, $A^n = A^{4k} = (A^4)^k = I^k = I$, as desired.

Conversely, we prove if $A^n = I$, then $4|n$.

Suppose $A^n = I$.

We must prove $4|n$.

By the division algorithm, there are unique integers q and r such that $n = 4q + r$ with $0 \leq r < 4$.

Hence, either $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$.

Observe that $A^r = A^{n-4q} = A^n A^{-4q} = IA^{-4q} = A^{-4q} = (A^4)^{-q} = I^{-q} = I$.

Computation shows that $A^1 \neq I$ and $A^2 \neq I$ and $A^3 \neq I$.

Hence, r cannot be $1, 2$ or 3.

Thus, r must be zero.

Therefore, $n = 4q$, so $4|n$, as desired. □

Exercise 93. Let $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$.

Then $\omega^n = 1$ if and only if $3|n$, for any integer n.

Solution. Observe that $\omega \in \mathbb{C}$.

We must prove $(\forall n \in \mathbb{Z})(\omega^n = 1 \leftrightarrow 3|n)$.

Thus, we let $n \in \mathbb{Z}$ be arbitrary.

To prove $\omega^n = 1 \leftrightarrow 3|n$, we must prove:

1. $\omega^n = 1 \Rightarrow 3|n$

2. $3|n \Rightarrow \omega^n = 1$.

Note that $\omega = cis(\frac{2\pi}{3})$.

We compute ω^n for various values of n.

We observe the pattern of repeating powers of ω, namely, $1, \omega, \omega^2$ repeat. □

Proof. Let n be an arbitrary integer.

To prove $\omega^n = 1 \Rightarrow 3|n$, assume $\omega^n = 1$.

We must prove $3|n$.

Using the division algorithm to divide n by 3, we obtain unique integers q and r such that $n = 3q + r$ and $0 \leq r < 3$.

To prove $3|n$, we must prove $r = 0$.

Observe that $\omega^3 = 1$ and

$$\begin{aligned} 1 &= \omega^n \\ &= \omega^{3q+r} \\ &= \omega^{3q}\omega^r \\ &= (\omega^3)^q\omega^r \\ &= (1)^q\omega^r \\ &= 1\omega^r \\ &= \omega^r. \end{aligned}$$

Since $0 \leq r < 3$, then either $r = 0$ or $r = 1$ or $r = 2$.

A computation shows that $\omega^1 \neq 1$ and $\omega^2 \neq 1$.

Thus, r cannot be 1 or 2.

Hence, r must be zero.

Therefore, $n = 3q$, so $3|n$, as desired.

To prove $3|n \Rightarrow \omega^n = 1$, assume $3|n$.

We must prove $\omega^n = 1$.

Since $3|n$, then there exists an integer k such that $n = 3k$.

Thus, $\omega^n = \omega^{3k} = (\omega^3)^k = 1^k = 1$, as desired. ☐

Exercise 94. For all $n \in \mathbb{N}$, $5^n - 4n - 1$ is divisible by 16.

Proof. To prove the statement $5^n - 4n - 1$ is divisible by 16 for all $n \in \mathbb{N}$, we prove $16|(5^n - 4n - 1)$ for all $n \in \mathbb{N}$ by induction on n.

Let $S = \{n \in \mathbb{N} : (16|(5^n - 4n - 1))\}$.

Basis:

Since $5^1 - 4 * 1 - 1 = 0$ and $16|0$, then $1 \in S$.

Induction:

Let $k \in S$.

Then $k \in \mathbb{N}$ and $16|(5^k - 4k - 1)$.

Since $16|(5^k - 4k - 1)$, then $16|5(5^k - 4k - 1)$.

Since $16|16k$, then 16 divides the sum $5(5^k - 4k - 1) + 16k = 5^{k+1} - 4k - 5 = 5^{k+1} - 4(k + 1) - 1$.

Thus, 16 divides $5^{k+1} - 4(k + 1) - 1$, so $k + 1 \in S$.

Hence, $k \in S$ implies $k + 1 \in S$.

Therefore, by PMI, $5^n - 4n - 1$ is divisible by 16 for all $n \in \mathbb{N}$. ☐

Exercise 95. For all $n \in \mathbb{N}$, $10^{n+1} + 10^n + 1$ is divisible by 3.

Proof. Let $S = \{n \in \mathbb{N} : (3|(10^{n+1} + 10^n + 1))\}$.

Basis:

Since $10^{1+1} + 10^1 + 1 = 111 = 3 \cdot 37$, then $3|(10^{1+1} + 10^1 + 1)$, so $1 \in S$.

Induction:

Let $k \in S$.

Then $k \in \mathbb{N}$ and $3|(10^{k+1} + 10^k + 1)$, so there exists $m \in \mathbb{Z}$ such that $10^{k+1} + 10^k + 1 = 3m$.

Observe that

$$\begin{aligned}
10^{(k+1)+1} + 10^{k+1} + 1 &= 10 \cdot 10^{k+1} + 10 \cdot 10^k + 1 \\
&= (9+1) \cdot 10^{k+1} + (9+1) \cdot 10^k + 1 \\
&= 9 \cdot 10^{k+1} + 10^{k+1} + 9 \cdot 10^k + 10^k + 1 \\
&= (9 \cdot 10^{k+1} + 9 \cdot 10^k) + (10^{k+1} + 10^k + 1) \\
&= (9 \cdot 10^{k+1} + 9 \cdot 10^k) + 3m \\
&= 3(3 \cdot 10^{k+1} + 3 \cdot 10^k) + 3m \\
&= 3(3 \cdot 10^{k+1} + 3 \cdot 10^k + m).
\end{aligned}$$

Since $3 \cdot 10^{k+1} + 3 \cdot 10^k + m$ is an integer, then this implies 3 divides $10^{(k+1)+1} + 10^{k+1} + 1$, so $k+1 \in S$.

Hence, $k \in S$ implies $k+1 \in S$.

Therefore, by PMI, $10^{n+1} + 10^n + 1$ is divisible by 3 for all $n \in \mathbb{N}$. ☐

Exercise 96. For all $n \in \mathbb{Z}^+$, $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ is divisible by 99.

Proof. Let $S = \{n \in \mathbb{Z}^+ : (99|(4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5))\}$.

Basis:

Since $4 \cdot 10^{2(1)} + 9 \cdot 10^{2(1)-1} + 5 = 400 + 90 + 5 = 495 = 99 \cdot 5$, then $99|(4 \cdot 10^{2(1)} + 9 \cdot 10^{2(1)-1} + 5)$, so $1 \in S$.

Induction:

Let $k \in S$.

Then $k \in \mathbb{Z}^+$ and $99|(4 \cdot 10^{2k} + 9 \cdot 10^{2k-1} + 5)$, so there exists $m \in \mathbb{Z}$ such that $4 \cdot 10^{2k} + 9 \cdot 10^{2k-1} + 5 = 99m$.

Observe that

$$\begin{aligned}
4 \cdot 10^{2(k+1)} + 9 \cdot 10^{2(k+1)-1} + 5 &= 4 \cdot 10^{2k+2} + 9 \cdot 10^{2k+2-1} + 5 \\
&= 4 \cdot 10^{2k} \cdot 10^2 + 9 \cdot 10^{2k-1} \cdot 10^2 + 5 \\
&= 4(100) \cdot 10^{2k} + 9(100) \cdot 10^{2k-1} + 5 \\
&= 100(4 \cdot 10^{2k}) + 100(9 \cdot 10^{2k-1}) + 5 \\
&= 100(4 \cdot 10^{2k}) + 100(9 \cdot 10^{2k-1}) + (500 - 495) \\
&= 100(4 \cdot 10^{2k}) + 100(9 \cdot 10^{2k-1}) + 100 \cdot 5 - 99 \cdot 5 \\
&= 100(4 \cdot 10^{2k} + 9 \cdot 10^{2k-1} + 5) - 99 \cdot 5 \\
&= 100(99m) - 99 \cdot 5 \\
&= 99(100m - 5).
\end{aligned}$$

Since $100m - 5$ is an integer, then this implies 99 divides $4 \cdot 10^{2(k+1)} + 9 \cdot 10^{2(k+1)-1} + 5$, so $k + 1 \in S$.

Hence, $k \in S$ implies $k + 1 \in S$.

Therefore, by PMI, $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ is divisible by 99 for all $n \in \mathbb{Z}^+$. □

Exercise 97. Every integer $10^{n+1} + 3 \cdot 10^n + 5$ is divisible by 9 for $n \in \mathbb{N}$.

Solution. We re-state this using the definition of divisibility: $\forall(n \in N), 9|10^{n+1} + 3 \cdot 10^n + 5$.

We must prove the proposition $\forall(n \in N), S_n$ where the statement S_n is $9|10^{n+1} + 3 \cdot 10^n + 5$.

We can work backwards to prove $9|10^{k+1} + 3 \cdot 10^k + 5 \rightarrow 9|10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5$.

If $9|10^{k+1} + 3 \cdot 10^k + 5$ is true, then $10^{k+1} + 3 \cdot 10^k + 5 = 9a$ for some integer a.

Thus, $10^{k+1} + 3 \cdot 10^k = 9a - 5$.

If $9|10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5$, then $10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5 = 9b$ for some integer b.

Thus, $10^{(k+1)+1} + 3 \cdot 10^{k+1} = 9b - 5$.

Hence,$10(10^{k+1} + 3 \cdot 10^k) = 10(9b - 5)$.

So, we can multiply $10^{k+1} + 3 \cdot 10^k = 9a - 5$ by 10 to complete the proof. □

Proof. Let $n \in \mathbb{N}$ and let S_n be the statement 9 divides $10^{n+1} + 3 \cdot 10^n + 5$.

We prove using mathematical induction.

Basis:

For $n = 1$, the statement S_1 is 9 divides $10^{1+1} + 3 \cdot 10 + 5$.

Since $10^{1+1} + 3 \cdot 10 + 5 = 135 = 9 * 15$, then 9 divides $10^{1+1} + 3 \cdot 10 + 5$, so S_1 is true.

Induction:

Let $k \in \mathbb{N}$.

Suppose $9|10^{k+1} + 3 \cdot 10^k + 5$ for any $k \geq 1$.

Then $10^{k+1} + 3 \cdot 10^k + 5 = 9a$ for some integer a.

Observe that

$$\begin{aligned}
10^{k+1} + 3 \cdot 10^k + 5 &= 9a \\
10^{k+1} + 3 \cdot 10^k &= 9a - 5 \\
10^{k+2} + 3 \cdot 10^{k+1} &= 90a - 50 \\
10^{k+2} + 3 \cdot 10^{k+1} + 5 &= 90a - 45 \\
10^{k+2} + 3 \cdot 10^{k+1} + 5 &= 9(10a - 5)
\end{aligned}$$

Since $a \in \mathbb{Z}$, then $10a - 5 \in \mathbb{Z}$.

Therefore, $9|10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5$ for any $k \geq 1$.

Since S_1 is true and 9 divides $10^{k+1} + 3 \cdot 10^k + 5$ implies 9 divides $10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5$ for any integer $k \geq 1$, then 9 divides $10^{n+1} + 3 \cdot 10^n + 5$ for every $n \in \mathbb{N}$. □

Exercise 98. Each number in the sequence 12,102,1002,10002,..., is divisible by 6.

Solution. Let $a = (12, 102, 1002, 10002, 100002, ...)$. We can find an expression for the n^{th} term of the sequence a by observing the pattern:

$$\begin{aligned} a_1 &= 12 = 10^1 + 2 \\ a_2 &= 102 = 10^2 + 2 \\ a_3 &= 1002 = 10^3 + 2 \\ &... \\ a_k &= 10^k + 2 \end{aligned}$$

Hence the n^{th} term of the sequence is $a_n = 10^n + 2$.

We must prove the proposition $\forall(n \in N), S_n$ where the statement S_n is $6|10^n + 2$.

Since S_n is a statement about the natural numbers, we use proof by induction(weak).

Our basis is $n_0 = 1$ and we must prove S_1.

For induction we must prove $S_k \to S_{k+1}$ for any $k \geq 1$.

Thus we must prove $6|(10^k + 2) \to 6|(10^{k+1} + 2)$ for $k \geq 1$.

We use direct proof to assume $6|(10^k + 2)$ for any $k \geq 1$.

This is our induction hypothesis. □

Proof. Let $n \in \mathbb{N}$ and let S_n be the statement $6|10^n + 2$.

We prove using mathematical induction(weak).

Basis: For $n = 1$, the statement S_1 is $6|12$ which is true because $12 = 6 \cdot 2$.

Induction: Let $k \in \mathbb{N}$.

Suppose $6|10^k + 2$ for $k \geq 1$.

Then there is a $b \in \mathbb{Z}$ for which $6b = 10^k + 2$.

Observe that:

$$\begin{aligned} 10^{k+1} + 2 &= 10 \cdot 10^k + 20 - 18 \\ &= 10(10^k + 2) - 18 \\ &= 10(6b) - 18 \\ &= 6(10b - 3) \end{aligned}$$

Hence $6|10^{k+1} + 2$.

This completes the proof that $S_k \to S_{k+1}$ for $k \geq 1$.

It follows by induction that $6|10^n + 2$ for all natural numbers n. □

Exercise 99. Let $n \in \mathbb{Z}$.

Then the only positive divisor of n and $n + 1$ is 1.

Proof. Let S be the set of all positive divisors of n and $n+1$.
Then $S = \{d \in \mathbb{Z}^+ : d|n \wedge d|(n+1)\}$.
We must prove $S = \{1\}$.
Since $1 \in \mathbb{Z}^+$ and $1|n$ and $1|(n+1)$, then $1 \in S$, so $\{1\} \subset S$.

Let $d \in S$.
Then $d \in \mathbb{Z}^+$ and $d|n$ and $d|(n+1)$.
Since $d|n$ and $d|(n+1)$, then d divides any linear combination of n and $n+1$.
In particular, d divides $(-1)(n) + (1)(n+1) = -n + n + 1 = 1$, so $d|1$.
Since $d \in \mathbb{Z}^+$ and $1 \in \mathbb{Z}^+$ and $d|1$, then $d \leq 1$.
Since $d \in \mathbb{Z}^+$, then $d \geq 1$.
Since $d \leq 1$ and $1 \leq d$, then by the anti-symmetric property of $\mathbb{Z}^+$, $d = 1$.
Hence, $d \in \{1\}$, so $S \subset \{1\}$.
Since $S \subset \{1\}$ and $\{1\} \subset S$, then $S = \{1\}$, as desired. □

Exercise 100. Let $n \in \mathbb{Z}^+$.
Then $\gcd(n, n+1) = 1$.

Proof. Since 1 divides any integer, then $1|n$ and $1|(n+1)$, so 1 is a common divisor of n and $n+1$.
Let c be any common divisor of n and $n+1$.
Then $c|n$ and $c|(n+1)$, so c divides the difference $(n+1) - n = 1$.
Hence, $c|1$, so any common divisor of n and $n+1$ divides 1.
Since $1 \in \mathbb{Z}^+$ and 1 is a common divisor of n and $n+1$ and any common divisor of n and $n+1$ divides 1, then by definition of gcd, $1 = \gcd(n, n+1)$. □

Proof. Since $1 = (n+1) - n = -n + (n+1)$ is a linear combination of n and $n+1$, then 1 is a multiple of $\gcd(n, n+1)$, so $\gcd(n, n+1)$ divides 1.
Since the only positive integer that divides 1 is 1, then $\gcd(n, n+1) = 1$. □

Exercise 101. Let $n \in \mathbb{Z}^+$.
Then either $\gcd(n, n+2) = 1$ or $\gcd(n, n+2) = 2$.

Proof. Either n is even or n is odd.
We consider each case separately.
Case 1: Suppose n is even.
Then $n = 2k$ for some integer k.
Thus, $n + 2 = 2k + 2 = 2(k+1)$, so $n+2$ is even.
Since n is even and $n+2$ is even, then 2 divides n and $n+2$, so 2 is a common divisor of n and $n+2$.
Let c be any common divisor of n and $n+2$.
Then $c|n$ and $c|(n+2)$, so c divides the difference $(n+2) - n = 2$.
Hence, $c|2$, so any common divisor of n and $n+2$ divides 2.
Since $2 \in \mathbb{Z}^+$ and 2 is a common divisor of n and $n+2$ and any common divisor of n and $n+2$ divides 2, then $2 = \gcd(n, n+2)$, by definition of gcd.
Case 2: Suppose n is odd.
Since 1 divides any integer, then $1|n$ and $1|(n+2)$.

Let c be any common divisor of n and $n + 2$.
Then $c|n$ and $c|(n + 2)$, so c divides the difference $(n + 2) - n = 2$.
Hence, $c|2$.
Without loss of generality, assume $c > 0$.
Then either $c = 1$ or $c = 2$.
If $c = 2$, then $2|n$, so n is even.
But, this contradicts the assumption n is odd.
Therefore, $c \neq 2$, so $c = 1$.
Hence, any common divisor of n and $n + 2$ must divide 1.
Since $1 \in \mathbb{Z}^+$ and 1 is a common divisor of n and $n + 2$ and any common divisor of n and $n + 2$ divides 1, then $1 = \gcd(n, n + 2)$. □

Exercise 102. Let $k \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
Then $\gcd(n, n + k)|k$.
This means gcd of n and $n + k$ is a factor of k.

Proof. Let $d = \gcd(n, n + k)$.
Then $d|n$ and $d|(n + k)$, so d divides the difference $(n + k) - n = k$.
Therefore, $d|k$. □

Exercise 103. Let $k, n \in \mathbb{Z}$.
Then $\gcd(k, n + k) = 1$ iff $\gcd(k, n) = 1$.

Proof. Suppose $\gcd(k, n) = 1$.
Then there exist integers x, y such that $xk + yn = 1$.
Thus, $1 = xk + yn = xk - yk + yk + yn = k(x - y) + y(k + n) = (x - y)k + y(n + k)$.
Since $x - y$ and y are integers and $(x - y)k + y(n + k) = 1$, then $\gcd(k, n + k) = 1$. □

Proof. Conversely, suppose $\gcd(k, n + k) = 1$.
Then there exist integers s, t such that $sk + t(n + k) = 1$.
Thus, $1 = sk + tn + tk = sk + tk + tn = (s + t)k + tn$.
Since $s + t$ and t are integers and $(s + t)k + tn = 1$, then $\gcd(k, n) = 1$. □

Exercise 104. Let $k, n \in \mathbb{Z}$.
Then $\gcd(k, n + k) = d$ iff $\gcd(k, n) = d$.

Proof. Suppose $\gcd(k, n) = d$.
Then $d \in \mathbb{Z}^+$ and $d|k$ and $d|n$ and if c is any common divisor of k and n, then $c|d$.
Since $d|n$ and $d|k$, then d divides the sum $n + k$, so $d|(n + k)$.
Since $d|k$ and $d|(n + k)$, then d is a common divisor of k and $n + k$.

Let c be any common divisor k and $n + k$.
Then $c|k$ and $c|(n + k)$, so c divides the difference $(n + k) - k = n$.
Hence, $c|n$.
Since $c|k$ and $c|n$, then c is a common divisor of k and n, so $c|d$.
Therefore, any common divisor of k and $n + k$ divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of k and $n+k$ and any common divisor of k and $n+k$ divides d, then by definition of gcd, $d = \gcd(k, n+k)$. $\square$

Proof. Conversely, suppose $\gcd(k, n+k) = d$.

Then $d \in \mathbb{Z}^+$ and $d|k$ and $d|(n+k)$ and if c is any common divisor of k and $n+k$, then $c|d$.

Since $d|k$ and $d|(n+k)$, then d divides the difference $(n+k) - k = n$.

Since $d|k$ and $d|n$, then d is a common divisor of k and n.

Let c be any common divisor of k and n.

Then $c|k$ and $c|n$, so c divides the sum $n+k$.

Since $c|k$ and $c|(n+k)$, then c is a common divisor of k and $n+k$, so $c|d$.

Hence, any common divisor of k and n divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor k and n and any common divisor of k and n divides d, then by definition of gcd, $d = \gcd(k, n)$. $\square$

Exercise 105. Let $k, n \in \mathbb{Z}$.

Then $\gcd(k, n+rk) = d$ for all $r \in \mathbb{Z}$ iff $\gcd(k, n) = d$.

Proof. Suppose $\gcd(k, n) = d$.

Then $d \in \mathbb{Z}^+$ and $d|k$ and $d|n$ and if c is any common divisor of k and n, then $c|d$.

Let $r \in \mathbb{Z}$.

Since $d|k$, then $d|rk$.

Since $d|n$ and $d|rk$, then d divides the sum $n+rk$.

Since $d|k$ and $d|(n+rk)$, then d is a common divisor of k and $n+rk$.

Let c be any common divisor of k and $n+rk$.

Then $c|k$ and $c|(n+rk)$.

Since $c|k$, then $c|rk$.

Since $c|(n+rk)$ and $c|rk$, then c divides the difference $(n+rk) - rk = n$, so $c|n$.

Since $c|k$ and $c|n$, then c is a common divisor of k and n, so $c|d$.

Hence, any common divisor of k and $n+rk$ divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of k and $n+rk$ and any common divisor of k and $n+rk$ divides d, then by definition of gcd, $d = \gcd(k, n+rk)$. $\square$

Proof. Conversely, suppose $\gcd(k, n+rk) = d$ for all $r \in \mathbb{Z}$.

Let $r = 0$.

Then $d = \gcd(k, n+rk) = \gcd(k, n+0k) = \gcd(k, n+0) = \gcd(k, n)$.

Therefore, $\gcd(k, n) = d$. $\square$

Exercise 106. Find all positive integers d such that d divides n^2+1 and $(n+1)^2+1$ for some integer n.

Solution. Let d be a positive integer such that $d|(n^2+1)$ and $d|[(n+1)^2+1]$ for some integer n.

Since $d|(n^2+1)$ and $d|[(n+1)^2+1]$, then d divides any linear combination of n^2+1 and $(n+1)^2+1$.

In particular, d divides the difference $[(n+1)^2+1]-(n^2+1) = (n^2+2n+1)+1-n^2-1 = 2n+1$.

Since $d|(2n+1)$ and $d|(n^2+1)$, then d divides any linear combination of $2n+1$ and n^2+1.

In particular, d divides the sum $4(n^2+1)-(2n+1)^2+2(2n+1) = (4n^2+4)-(4n^2+4n+1)+(4n+2) = 5$.

Since $d \in \mathbb{Z}^+$ and $d|5$, then d must be 1 or 5. □

Exercise 107. If n is a positive integer, find the possible values of $\gcd(n, n+10)$.

Proof. Let $n \in \mathbb{Z}^+$.

Let $d = \gcd(n, n+10)$.

Then $d \in \mathbb{Z}^+$ and $d|n$ and $d|(n+10)$, so d divides any linear combination of n and $n+10$.

In particular, d divides $-n+(n+10) = 10$.

Thus, $d|10$, so d must be one of $1, 2, 5, 10$.

Therefore, $d \in \{1, 2, 5, 10\}$. □

Exercise 108. Let $n \in \mathbb{Z}$.

Then $\gcd(n, 1) = 1$.

Proof. Since 1 and $1-n$ are integers and $(1)(n)+(1-n)(1) = n+1-n = 1+n-n = 1+0 = 1$, then 1 is a linear combination of n and 1.

Hence, 1 is a multiple of $\gcd(n, 1)$, so $\gcd(n, 1)$ divides 1.

The only positive integer that divides 1 is 1, so $\gcd(n, 1) = 1$. □

Exercise 109. Let $n \in \mathbb{Z}^+$.

Then $\gcd(3n+2, 5n+3) = 1$.

Proof. Since 5 and -3 are integers and $5(3n+2)+(-3)(5n+3) = 15n+10-15n-9 = 1$, then $\gcd(3n+2, 5n+3) = 1$. □

Exercise 110. Let $a \in \mathbb{Z}$.

Then $\gcd(a, a+n)$ divides n for all $n \in \mathbb{Z}^+$.

Therefore, $\gcd(a, a+1) = 1$.

Proof. Let $n \in \mathbb{Z}^+$.

Let $d = \gcd(a, a+n)$.

Then d is a common divisor of a and $a+n$, so d divides any linear combination of a and $a+n$.

In particular, d divides the difference $(a+n)-a = n$, so $d|n$.

Therefore, $\gcd(a, a+n)|n$ for any positive integer n.

For $n = 1$ this implies $\gcd(a, a+1)|1$.

The only positive integer that divides 1 is 1, so $\gcd(a, a+1) = 1$. □

Exercise 111. Let $a, b \in \mathbb{Z}$.

Then there exist integers m, n such that $c = ma + nb$ iff $\gcd(a, b)|c$.

Proof. Observe that $\gcd(a, b)|c$ iff c is a multiple of $\gcd(a, b)$ iff c is a linear combination of a and b iff there exist integers m and n such that $c = ma + nb$.

Therefore, $\gcd(a, b)|c$ iff there exist integers m and n such that $c = ma + nb$. ☐

Exercise 112. Let $a, b \in \mathbb{Z}$.

If there exist integers m, n such that $\gcd(a, b) = ma+nb$, then $\gcd(m, n) = 1$.

Proof. Suppose there exist integers m and n such that $\gcd(a, b) = ma + nb$.

Let $d = ma + nb$.

Then d $= \gcd(a, b)$, so $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$.

Hence, $a = dx$ and $b = dy$ for some integers x and y.

Thus, $d = m(dx)+n(dy) = m(xd)+n(yd) = (mx)d+(ny)d = xmd+ynd = (xm + yn)d$.

Since $d \in \mathbb{Z}^+$, then $d > 0$, so $d \neq 0$.

Hence, $1 = xm + yn$.

Since there exist integers x and y such that $xm + yn = 1$, then $\gcd(m, n) = 1$. ☐

Proposition 113. *Let $a, b \in \mathbb{Z}$.*

Then $(a, b) = (a, ka + b)$ for all $k \in \mathbb{Z}$.

Proof. Let $d = \gcd(a, b)$.

Then $d|a$ and $d|b$ and if c is any integer such that $c|a$ and $c|b$, then $c|d$.

Since $d|a$ and $d|b$, then d divides any linear combination of a and b, so d divides $ka + b$.

Since $d|a$ and $d|(ka + b)$, then d is a common divisor of a and $ka + b$.

Let c be an arbitrary integer such that $c|a$ and $c|(ka + b)$.

Then c divides any linear combination of a and $ka + b$.

In particular, c divides $(-k)a + (1)(ka + b) = -ka + ka + b = 0 + b = b$, so $c|b$.

Since $c|a$ and $c|b$, then $c|d$.

Thus, any common divisor of a and $ka + b$ divides d.

Since d is a common divisor of a and $ka + b$ and any common divisor of a and $ka + b$ divides d, then $d = \gcd(a, ka + b)$. ☐

Exercise 114. Let $a, b \in \mathbb{Z}^*$.

For all $d \in \mathbb{Z}^*$, if $d|a$ and $d|b$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}\gcd(a, b)$.

Proof. Let $d \in \mathbb{Z}^*$ such that $d|a$ and $d|b$.

Then $d \neq 0$ and there exist integers k_1 and k_2 such that $a = dk_1$ and $b = dk_2$.

Since $a, b \in \mathbb{Z}^*$, then the greatest common divisor of a and b exists and is unique.

Let $c = \gcd(a, b)$.

Then

$$\begin{aligned} c &= \gcd(dk_1, dk_2) \\ &= d \cdot \gcd(k_1, k_2) \\ &= d \cdot \gcd(\frac{a}{d}, \frac{b}{d}). \end{aligned}$$

Since $c = d \cdot \gcd(\frac{a}{d}, \frac{b}{d})$ and $d \neq 0$, then $\frac{c}{d} = \gcd(\frac{a}{d}, \frac{b}{d})$.
Therefore, $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{\gcd(a,b)}{d} = \frac{1}{d}\gcd(a, b)$. ☐

Exercise 115. Let $a, b, c \in \mathbb{Z}$.
If $\gcd(a, b) = 1$ and $c|a$, then $\gcd(b, c) = 1$.

Proof. Suppose $\gcd(a, b) = 1$ and $c|a$.
Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.
Since $c|a$, then $a = ck$ for some integer k.
Thus, $1 = m(ck) + nb = nb + m(ck) = nb + (mk)c$.
Since n and mk are integers and $nb + (mk)c = 1$, then $\gcd(b, c) = 1$. ☐

Exercise 116. Let $a, b, c \in \mathbb{Z}$.
If $\gcd(a, b) = 1$, then $\gcd(ac, b) = \gcd(c, b)$.

Proof. Suppose $\gcd(a, b) = 1$.
Let $d = \gcd(c, b)$.
Then $d|c$ and $d|b$ and if e is any integer such that $e|c$ and $e|b$, then $e|d$.
We must prove $\gcd(ac, b) = d$.
Since $d|c$, then d divides any multiple of c, so $d|ac$.
Since $d|ac$ and $d|b$, then d is a common divisor of ac and b.
Let $e \in \mathbb{Z}$ such that $e|ac$ and $e|b$.
Since e is a common divisor of ac and b, then e divides any linear combination of ac and b.
Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.
Thus, $c = c \cdot 1 = c(ma + nb) = cma + cnb = m(ac) + (cn)b$, so c is a linear combination of ac and b.
Hence, $e|c$.
Since $e|c$ and $e|b$, then $e|d$, so any common divisor of ac and b divides d.
Since d is a common divisor of ac and b and any common divisor of ac and b divides d, then $d = \gcd(ac, b)$. ☐

Exercise 117. Let $a, b \in \mathbb{Z}$.
Then $\gcd(\gcd(a, b), b) = \gcd(a, b)$.

Proof. Let $d = \gcd(a, b)$.
Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and if c is any common divisor of a and b, then c divides d.
Since $d|d$ and $d|b$, then d is a common divisor of d and b.
Let c be any common divisor of d and b.
Then $c|d$ and $c|b$.

Since $c|d$ and $d|a$, then $c|a$.
Since $c|a$ and $c|b$, then c is a common divisor of a and b, so $c|d$.
Hence, any common divisor of d and b divides d.
Since $d \in \mathbb{Z}^+$ and d is a common divisor of d and b and any common divisor of d and b divides d, then by definition of gcd, $\gcd(d, b) = d$.
Therefore, $\gcd(\gcd(a, b), b) = \gcd(d, b) = d = \gcd(a, b)$, as desired. □

Exercise 118. Let $a, b, c \in \mathbb{Z}$.
If $\gcd(a, b) = 1$ and $c|(a + b)$, then $\gcd(a, c) = \gcd(b, c) = 1$.

Proof. Suppose $\gcd(a, b) = 1$ and $c|(a + b)$.

Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma + nb = 1$.
Let $d = \gcd(a, c)$.
Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|c$.
Since $d|c$ and $c|(a + b)$, then $d|(a + b)$.
Since $d|a$ and $d|(a+b)$, then d divides any linear combination of a and $a+b$.
Since $(-1)a + (1)(a + b) = -a + a + b = 0 + b = b$ is a linear combination of a and $a + b$, then this implies $d|b$.
Since $d|a$ and $d|b$, then d divides any linear combination of a and b.
Since $ma + nb = 1$ is a linear combination of a and b, then this implies $d|1$.
Since $d \in \mathbb{Z}^+$ and $d|1$, then this implies $d = 1$.
Therefore, $\gcd(a, c) = 1$.

Let $e = \gcd(b, c)$.
Then $e \in \mathbb{Z}^+$ and $e|b$ and $e|c$.
Since $e|c$ and $c|(a + b)$, then $e|(a + b)$.
Since $e|b$ and $e|(a + b)$, then e divides any linear combination of b and $a + b$.
Since $(-1)b + (1)(a + b) = -b + a + b = -b + b + a = 0 + a = a$ is a linear combination of b and $a + b$, then this implies $e|a$.
Since $e|a$ and $e|b$, then e divides any linear combination of a and b.
Since $ma + nb = 1$ is a linear combination of a and b, then this implies $e|1$.
Since $e \in \mathbb{Z}^+$ and $e|1$, then this implies $e = 1$.
Therefore, $\gcd(b, c) = 1$. □

Exercise 119. Let $a, b, d \in \mathbb{Z}$ such that d is a common divisor of a and b.
If $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, then $d = \gcd(a, b)$.

Proof. Since d is a common divisor of a and b, then $d|a$ and $d|b$, so $a = dx$ and $b = dy$ for some integers x and y.
Thus, $x = \frac{a}{d} \in \mathbb{Z}$ and $y = \frac{b}{d} \in \mathbb{Z}$.
Suppose $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.
Then there exist integers m and n such that $m(\frac{a}{d}) + n(\frac{b}{d}) = 1$.
Thus, $ma + nb = d$, so d is a linear combination of a and b.
Let $c \in \mathbb{Z}$ such that c is any common divisor of a and b.
Then c divides any linear combination of a and b, so $c|d$.

Thus, any common divisor of a and b divides d.

Since d is a common divisor of a and b and any common divisor of a and b divides d, then $d = \gcd(a, b)$. $\square$

Exercise 120. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$.

Then $\gcd(a + b, a - b)$ is 1 or 2.

Proof. Let $d = \gcd(a + b, a - b)$.

Then $d \in \mathbb{Z}^+$ and $d|(a + b)$ and $d|(a - b)$.

We must prove either $d = 1$ or $d = 2$.

Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.

Thus, $2ma + 2nb = 2$, so 2 is a linear combination of $2a$ and $2b$.

Since $d|(a + b)$ and $d|(a - b)$, then d divides the sum $(a + b) + (a - b) = 2a$, so $d|2a$.

Since $d|(a+b)$ and $d|(a-b)$, then d divides the difference $(a+b)-(a-b) = 2b$, so $d|2b$.

Since $d|2a$ and $d|2b$, then d divides any linear combination of $2a$ and $2b$, so $d|2$.

Since $d \in \mathbb{Z}^+$ and $d|2$, then either $d = 1$ or $d = 2$, as desired. $\square$

Exercise 121. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$.

Then $\gcd(a + 2b, 2a + b)$ is 1 or 3.

Proof. Let $d = \gcd(a + 2b, 2a + b)$.

Then $d \in \mathbb{Z}^+$ and $d|(a + 2b)$ and $d|(2a + b)$.

We must prove either $d = 1$ or $d = 3$.

Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.

Thus, $3ma + 3nb = 3$, so 3 is a linear combination of $3a$ and $3b$.

Since $d|(a + 2b)$ and $d|(2a + b)$, then d divides any linear combination of $a + 2b$ and $2a + b$.

Since $(-1)(a + 2b) + 2(2a + b) = -a - 2b + 4a + 2b = 3a$, then $3a$ is a linear combination of $a + 2b$ and $2a + b$, so $d|3a$.

Since $(2)(a + 2b) + (-1)(2a + b) = 2a + 4b - 2a - b = 3b$, then $3b$ is a linear combination of $a + 2b$ and $2a + b$, so $d|3b$.

Since $d|3a$ and $d|3b$, then d divides any linear combination of $3a$ and $3b$, so $d|3$.

Since $d \in \mathbb{Z}^+$ and $d|3$, then either $d = 1$ or $d = 3$, as desired. $\square$

Exercise 122. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$.

Then $\gcd(a + b, a^2 + b^2)$ is 1 or 2.

Proof. Let $d = \gcd(a + b, a^2 + b^2)$.

Then $d \in \mathbb{Z}^+$ and $d|(a + b)$ and $d|(a^2 + b^2)$.

We must prove either $d = 1$ or $d = 2$.

Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.

Since $d|(a + b)$ and $d|(a^2 + b^2)$, then d divides any linear combination of $a + b$ and $a^2 + b^2$.

Since $(a^2+b^2)-(a-b)(a+b) = a^2+b^2-(a^2-b^2) = a^2+b^2-a^2+b^2 = 2b^2$, then $2b^2$ is a linear combination of $a+b$ and a^2+b^2.

Thus, $d|2b^2$.

Since $(a+b)^2-(a^2+b^2) = (a^2+2ab+b^2)-a^2-b^2 = 2ab$, then $2ab$ is a linear combination of $a+b$ and a^2+b^2.

Thus, $d|2ab$.

Since $1 = ma+nb$, then $2b = 2b(ma+nb) = 2bma+2bnb = 2abm+2b^2n$, so $2b$ is a linear combination of $2ab$ and $2b^2$.

Since $d|2ab$ and $d|2b^2$, then d divides any linear combination of $2ab$ and $2b^2$, so this implies $d|2b$.

Since $2(a+b)^2-4ab-2b^2 = 2(a^2+2ab+b^2)-4ab-2b^2 = 2a^2+4ab+2b^2-4ab-2b^2 = 2a^2$, then $2a^2$ is a linear combination of $a+b$ and $2ab$ and $2b^2$.

Since $d|(a+b)$ and $d|2ab$ and $d|2b^2$, then d divides any linear combination of $a+b$ and $2ab$ and $2b^2$, so $d|2a^2$.

Since $1 = ma+nb$, then $2a = 2a(ma+nb) = 2ama+2anb = 2a^2m+2abn$, so $2a$ is a linear combination of $2a^2$ and $2ab$.

Since $d|2a^2$ and $d|2ab$, then d divides any linear combination of $2a^2$ and $2ab$, so $d|2a$.

Since $1 = ma+nb$, then $2 = 2(ma+nb) = 2ma+2nb$, so 2 is a linear combination of $2a$ and $2b$.

Since $d|2a$ and $d|2b$, then d divides any linear combination of $2a$ and $2b$, so $d|2$.

Since $d \in \mathbb{Z}^+$ and $d|2$, then either $d = 1$ or $d = 2$. ☐

Exercise 123. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$.

Then $\gcd(a+b, a^2-ab+b^2)$ is 1 or 3.

Proof. Let $d = \gcd(a+b, a^2-ab+b^2)$.

Then $d \in \mathbb{Z}^+$ and $d|(a+b)$ and $d|(a^2-ab+b^2)$.

We must prove either $d = 1$ or $d = 3$.

By the division algorithm, $a^2-ab+b^2 = (a+b)(a-2b)+3b^2$, so $3b^2 = (a^2-ab+b^2)-(a+b)(a-2b)$.

Thus, $3b^2$ is a linear combination of a^2-ab+b^2 and $a+b$.

Since $d|(a+b)$ and $d|(a^2-ab+b^2)$, then d divides any linear combination of $a+b$ and a^2-ab+b^2, so $d|3b^2$.

Since $(a+b)^2-(a^2-ab+b^2) = (a^2+2ab+b^2)-a^2+ab-b^2 = 3ab$, then $3ab$ is a linear combination of $a+b$ and a^2-ab+b^2, so $d|3ab$.

Since $1 = ma+nb$, then $3b = 3b(ma+nb) = 3bma+3bnb = 3abm+3b^2n$, so $3b$ is a linear combination of $3ab$ and $3b^2$.

Since $d|3ab$ and $d|3b^2$, then d divides any linear combination of $3ab$ and $3b^2$, so $d|3b$.

Since $2(a^2-ab+b^2)+(a+b)^2-3b^2 = (2a^2-2ab+2b^2)+(a^2+2ab+b^2)-3b^2 = 3a^2$, then $3a^2$ is a linear combination of a^2-ab+b^2 and $a+b$ and $3b^2$.

Since $d|(a^2-ab+b^2)$ and $d|(a+b)$ and $d|3b^2$, then d divides any linear combination of a^2-ab+b^2 and $a+b$ and $3b^2$, so $d|3a^2$.

Since $1 = ma + nb$, then $3a = 3a(ma + nb) = 3ama + 3anb = 3a^2m + 3abn$, so $3a$ is a linear combination of $3a^2$ and $3ab$.

Since $d|3a^2$ and $d|3ab$, then d divides any linear combination of $3a^2$ and $3ab$, so $d|3a$.

Since $1 = ma + nb$, then $3 = 3(ma + nb) = 3ma + 3nb$, so 3 is a linear combination of $3a$ and $3b$.

Since $d|3a$ and $d|3b$, then d divides any linear combination of $3a$ and $3b$, so $d|3$.

Since $d \in \mathbb{Z}^+$ and $d|3$, then this implies either $d = 1$ or $d = 3$. □

Exercise 124. Let n be an integer with $n > 1$.

Then either $\gcd(n-1, n^2+n+1) = 1$ or $\gcd(n-1, n^2+n+1) = 3$.

Proof. Let $d = \gcd(n-1, n^2+n+1)$.

We must prove either $d = 1$ or $d = 3$.

By the division algorithm, we have $n^2 + n + 1 = (n-1)(n+2) + 3$, so $3 = (n^2+n+1) - (n-1)(n+2) = -(n+2)(n-1) + (n^2+n+1)$.

Thus, 3 is a linear combination of $n-1$ and n^2+n+1, so 3 is a multiple of d.

Hence, $d|3$.

Since $d \in \mathbb{Z}^+$ and $d|3$, then either $d = 1$ or $d = 3$. □

Exercise 125. Let a, b be positive integers.

Then $\gcd(a, b) = 1$ if and only if $\gcd(a + b, ab) = 1$.

Proof. We prove if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

Suppose $\gcd(a, b) = 1$.

Since 1 divides every integer, then $1|(a + b)$ and $1|ab$, so 1 is a common divisor of $a + b$ and ab.

Let $c \in \mathbb{Z}$ such that $c|(a + b)$ and $c|ab$.

Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.

Since $c|(a + b)$ and $c|ab$, then c divides any linear combination of $a + b$ and ab.

Since $a(a + b) - ab = a^2 + ab - ab = a^2$, then a^2 is a linear combination of $a + b$ and ab, so $c|a^2$.

Since $1 = ma + nb$, then $a = a(ma + nb) = ama + anb = a^2m + abn = m(a^2) + n(ab)$, so a is a linear combination of a^2 and ab.

Since $c|a^2$ and $c|ab$, then c divides any linear combination of a^2 and ab, so $c|a$.

Since $b(a + b) - ab = ba + b^2 - ab = ab + b^2 - ab = b^2$, then b^2 is a linear combination of $a + b$ and ab, so $c|b^2$.

Since $1 = ma + nb$, then $b = b(ma + nb) = bma + bnb = abm + b^2n = m(ab) + n(b^2)$, so b is a linear combination of ab and b^2.

Since $c|ab$ and $c|b^2$, then c divides any linear combination of ab and b^2, so $c|b$.

Since $c|a$ and $c|b$, then c divides any linear combination of a and b.

Since $ma + nb = 1$ is a linear combination of a and b, then this implies $c|1$.

Thus, if $c|(a + b)$ and $c|ab$, then $c|1$, so any common divisor of $a + b$ and ab divides 1.

Since 1 is a common divisor of $a + b$ and ab and any common divisor of $a + b$ and ab divides 1, then $1 = \gcd(a + b, ab)$. □

Proof. Conversely, suppose $\gcd(a + b, ab) = 1$.

Since 1 divides every integer, then $1|a$ and $1|b$, so 1 is a common divisor of a and b.

Let $c \in \mathbb{Z}$ such that $c|a$ and $c|b$.

Then c divides any linear combination of a and b, so $c|(a + b)$ and $c|ab$.

Thus, c is a common divisor of $a + b$ and ab, so c divides $\gcd(a + b, ab)$.

Therefore, $c|1$, so any divisor of a and b divides 1.

Since 1 is a common divisor of a and b and any divisor of a and b divides 1, then $1 = \gcd(a, b)$. □

Exercise 126. Let a, b, n be nonzero integers.

If $a|n$ and $b|n$ and $\gcd(a, b) = d$, then $ab|nd$.

Proof. Suppose $a|n$ and $b|n$ and $\gcd(a, b) = d$.

Since $a|n$ and $b|n$, then there are integers k_1 and k_2 such that $n = ak_1$ and $n = bk_2$.

Since $d = \gcd(a, b)$, then d is the least positive linear combination of a and b, so there are integers x and y such that $d = xa + yb$.

Let $e = xk_2 + yk_1$.

Clearly, e is an integer.

Observe that

$$\begin{aligned} abe &= ab(xk_2 + yk_1) \\ &= abxk_2 + abyk_1 \\ &= xa(bk_2) + yb(ak_1) \\ &= xan + ybn \\ &= (xa + yb)n \\ &= n(xa + yb) \\ &= nd. \end{aligned}$$

Since $e \in \mathbb{Z}$ and $nd = abe$, then $ab|nd$. □

Exercise 127. Let a, b, c be positive integers.

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

Proof. Suppose $\gcd(a, b) = 1$ and $c|b$.

Since $\gcd(a, b) = 1$, then there are integers x and y such that $1 = xa + yb$.

Since $c|b$, then $b = cd$ for some integer d.

Observe that $1 = xa + yb = xa + y(cd) = xa + y(dc) = xa + (yd)c$.

Since $x \in \mathbb{Z}$ and $yd \in \mathbb{Z}$ and $xa + (yd)c = 1$, then $\gcd(a, c) = 1$. $\square$

Exercise 128. For all integers $n > 1$, $n - 1$ and $2n - 1$ are relatively prime.

Solution. We express 1 as a linear combination of $n - 1$ and $2n - 1$.

Using the division algorithm to divide $2n - 1$ by $n - 1$ we obtain $2n - 1 = 2(n - 1) + 1$, so $1 = -2(n - 1) + (2n - 1)$. $\square$

Proof. Let n be an arbitrary integer greater than one.

Since $-2 \in \mathbb{Z}$ and $1 \in \mathbb{Z}$ and $-2(n-1) + (1)(2n-1) = -2n+2+2n-1 = 1$, then $\gcd(n - 1, 2n - 1) = 1$. $\square$

Exercise 129. For all integers $n > 1$, $2n - 1$ and $3n - 1$ are relatively prime.

Solution. We express 1 as a linear combination of $2n - 1$ and $3n - 1$.

So, we want to find integers a and b such that $a(2n - 1) + b(3n - 1) = 1$.

To have $2an$ and $3bn$ cancel each other, we can let $a = -3$ and $b = 2$. $\square$

Proof. Let n be an arbitrary integer greater than one.

Since $-3 \in \mathbb{Z}$ and $2 \in \mathbb{Z}$ and $-3(2n-1) + 2(3n-1) = -6n+3+6n-2 = 1$, then $\gcd(2n - 1, 3n - 1) = 1$. $\square$

Exercise 130. Let m and n be positive integers.

Then $\gcd(2^m - 1, 2^n - 1) = 1$ if and only if $\gcd(m, n) = 1$.

Solution. We must prove:

1. if $\gcd(2^m - 1, 2^n - 1) = 1$, then $\gcd(m, n) = 1$.
2. if $\gcd(m, n) = 1$, then $\gcd(2^m - 1, 2^n - 1) = 1$. $\square$

Proof. We prove if $\gcd(m, n) = 1$, then $\gcd(2^m - 1, 2^n - 1) = 1$.

Suppose $\gcd(m, n) = 1$.

Then $ma + nb = 1$ for some integers a and b.

To prove $\gcd(2^m - 1, 2^n - 1) = 1$, we must find integers c and d such that $c(2^m - 1) + d(2^n - 1) = 1$.

Observe that $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + ... + x + 1)$ for any real number x and positive integer k.

We have a flaw here.

If k is a negative integer, then $x^k - 1 = (x - 1)(\sum_{i=1}^{-k}(-x^{-i})$.

Now, couldn't a or b be a negative integer?

If so, then $\sum_{i=1}^{-k}(-x^{-i})$ is not necessarily an integer, but rather a fraction which implies that $x - 1 \not| x^k - 1$.

We have no guarantee that both a and b are always positive, so this proof is not valid if a or b is negative integer!

Let $x = 2m$ and $k = a$.

Then x and k are integers, so $x^k - 1$, $x - 1$, and $x^{k-1} + x^{k-2} + ... + x + 1$ are integers.

Hence, $x - 1 | x^k - 1$, so $2^m - 1 | 2^{ma} - 1$.

Therefore, $2^{ma} - 1 = (2^m - 1)r$ for some integer r.

Let $x = 2n$ and $k = b$.

Then x and k are integers, so $x^k - 1$, $x - 1$, and $x^{k-1} + x^{k-2} + ... + x + 1$ are integers.

Hence, $x - 1 | x^k - 1$, so $2^n - 1 | 2^{nb} - 1$.

Therefore, $2^{nb} - 1 = (2^n - 1)s$ for some integer s.

Observe that

$$\begin{aligned} 1 &= 2^1 - 1 \\ &= 2^{ma+nb} - 1 \\ &= 2^{ma} * 2^{nb} - 1 \\ &= 2^{ma}[(2^n - 1)s + 1] - 1 \\ &= 2^{ma}s(2^n - 1) + 2^{ma} - 1 \\ &= 2^{ma}s(2^n - 1) + r(2^m - 1). \end{aligned}$$

Let $c = r$ and $d = 2^{ma}s$.

Clearly, c and d are integers and $1 = c(2^m - 1) + d(2^n - 1)$, as desired.

Suppose $\gcd(2^m - 1, 2^n - 1) = 1$.

We must prove $\gcd(m, n) = 1$.

Let $d = \gcd(m, n)$.

Then $d|m$ and $d|n$.

Thus, $m = da$ and $n = db$ for some integers a and b.

Suppose for the sake of contradiction that $\gcd(m, n) \neq 1$.

Then $d \neq 1$, so $d > 1$.

Observe that $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + ... + x + 1)$ for any real number x and positive integer k.

We have a flaw here.

If k is a negative integer, then $x^k - 1 = (x - 1)(\sum_{i=1}^{-k}(-x^{-i})$.

Now, couldn't a or b be a negative integer?

If so, then $\sum_{i=1}^{-k}(-x^{-i})$ is not necessarily an integer, but rather a fraction which implies that $x - 1 \not| x^k - 1$.

We have no guarantee that both a and b are always positive, so this proof is not valid if a or b is a negative integer!

Let $x = 2^d$ and $k = a$.

Then x and k are integers, so $x^k - 1$, $x - 1$, and $x^{k-1} + x^{k-2} + ... + x + 1$ are integers.

Hence, $x - 1 | x^k - 1$, so $2^d - 1 | 2^{da} - 1$.

Thus, $2^d - 1 | 2^m - 1$, so $2^m - 1 = (2^d - 1)r$ for some integer r.

Let $x = 2^d$ and $k = b$.

Then x and k are integers, so $x^k - 1$, $x - 1$, and $x^{k-1} + x^{k-2} + ... + x + 1$ are integers.

Hence, $x - 1 | x^k - 1$, so $2^d - 1 | 2^{db} - 1$.

Thus, $2^d - 1 | 2^n - 1$, so $2^n - 1 = (2^d - 1)s$ for some integer s.

Since $\gcd(2^m - 1, 2^n - 1) = 1$, then there are integers x and y such that $x(2^m - 1) + y(2^n - 1) = 1$.

Observe that $x(2^d - 1)r + y(2^d - 1)s = 1$, so $(2^d - 1)(xr + ys) = 1$.

Since $2^d - 1$ and $xr + ys$ are integers whose product is one, then $2^d - 1$ is either 1 or -1.

Since $d > 1$, then $d \geq 2$, so $2^d - 1 \geq 3$, so $2^d - 1 > 0$.

Hence, $2^d - 1 = 1$, so $d = 1$.

But, we have $d \neq 1$ and $d = 1$, a contradiction.

Therefore, $\gcd(m, n) = 1$, as desired. □

Exercise 131. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$.

Let $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

Then $\gcd(a, s) = \gcd(r, b) = \gcd(r, s) = 1$.

Proof. Let $m = \gcd(a, s)$.

Then $m \in \mathbb{Z}^+$ and $m|a$ and $m|s$, so m divides any linear combination of a and s.

Since $1 = ar + bs = ra + bs$ is a linear combination of a and s, then $m|1$.

Since $m \in \mathbb{Z}^+$ and $m|1$, then $m = 1$, so $\gcd(a, s) = 1$.

Let $x = \gcd(r, b)$.

Then $x \in \mathbb{Z}^+$ and $x|r$ and $x|b$, so x divides any linear combination of r and b.

Since $1 = ar + bs = ar + sb$ is a linear combination of r and b, then $x|1$.

Since $x \in \mathbb{Z}^+$ and $x|1$, then $x = 1$, so $\gcd(r, b) = 1$.

Let $y = \gcd(r, s)$.

Then $y \in \mathbb{Z}^+$ and $y|r$ and $y|s$, so y divides any linear combination of r and s.

Since $1 = ar + bs$ is a linear combination of r and s, then $y|1$.

Since $y \in \mathbb{Z}^+$ and $y|1$, then $y = 1$, so $\gcd(r, s) = 1$. □

Exercise 132. If n has a divisor d with $1 < d < n$, then it has a divisor d' with $1 < d' \leq \sqrt{n}$.

Let $n \in \mathbb{Z}$.

Let $d \in \mathbb{Z}$ such that $d|n$ and $1 < d < n$.

Then there exists $d' \in \mathbb{Z}$ such that $1 < d' \leq \sqrt{n}$.

Proof. Suppose there is an integer d such that $d|n$ and $1 < d < n$.

Either $d \leq \sqrt{n}$ or $d > \sqrt{n}$.

We consider these cases separately.

Case 1: Suppose $d \leq \sqrt{n}$.

Let $d' = d$.

Then $d' \in \mathbb{Z}$ and $d' \leq \sqrt{n}$.

Since $1 < d < n$, then $1 < d$, so $1 < d'$.

Thus, $1 < d' \leq \sqrt{n}$.

Therefore, there exists $d' \in \mathbb{Z}$ such that $1 < d' \leq \sqrt{n}$.
Case 2: Suppose $d > \sqrt{n}$.
Since $1 < d < n$, then $1 < d$ and $d < n$ and $1 < n$.
Since $d|n$, then there exists $d' \in \mathbb{Z}$ such that $n = dd'$, so $d'|n$.
Since $d > 1 > 0$, then $d > 0$.

Suppose $d' \leq 1$.
Since $d > 0$, then $n = dd' \leq d \cdot 1 = d$, so $n \leq d$.
Thus, we have $d < n$ and $d \geq n$, a contradiction.
Hence, $d' > 1$.

Suppose $d' > \sqrt{n}$.
Since $n > 1 > 0$, then $n > 0$, so $\sqrt{n} > 0$.
Since $\sqrt{n} < d'$ and $\sqrt{n} > 0$, then $\sqrt{n}\sqrt{n} < \sqrt{n} \cdot d'$.
Since $d' > 1 > 0$, then $d' > 0$.
Since $\sqrt{n} < d$ and $d' > 0$, then $\sqrt{n} \cdot d' < dd'$.
Thus, $n = (\sqrt{n})^2 = \sqrt{n}\sqrt{n} < \sqrt{n} \cdot d' < dd' = n$.
Hence, $n < \sqrt{n} \cdot d' < n$, so $n < n$, a contradiction.
Therefore, $d' \leq \sqrt{n}$.

Since $1 < d'$ and $d' \leq \sqrt{n}$, then $1 < d' \leq \sqrt{n}$.
Therefore, there exists $d' \in \mathbb{Z}$ such that $1 < d' \leq \sqrt{n}$. □

Lemma 133. *Let* $a, b, c \in \mathbb{Z}$.
Then $(a, bc) = 1$ *iff* $(a, b) = (a, c) = 1$.

Proof. We prove if $(a, bc) = 1$, then $(a, b) = (a, c) = 1$.
Suppose $(a, bc) = 1$.
Then there are integers m and n such that $ma + n(bc) = 1$.
Since $1 = ma + nbc = ma + ncb = ma + (nc)b$ and m and nc are integers, then $(a, b) = 1$.
Since $1 = ma + nbc = ma + (nb)c$ and m and nb are integers, then $(a, c) = 1$.

Conversely, suppose $(a, b) = (a, c) = 1$.
Then there are integers x, y, u, v such that $xa + yb = 1$ and $ua + vc = 1$.
Multiplying these equations we obtain $(xa + yb)(ua + vc) = 1 \cdot 1 = 1$.
Hence, $xua^2 + xavc + ybua + ybvc = 1$, so $(xua + xvc + ybu)a + (yv)(bc) = 1$.
Since $xua + xvc + ybu$ and yv are integers, then $(a, bc) = 1$, as desired. □

Exercise 134. Let $a, b \in \mathbb{Z}^+$.
If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.

Proof. Suppose $(a, b) = 1$.
Since $(a, bc) = 1$ iff $(a, b) = (a, c) = 1$ for all $a, b, c \in \mathbb{Z}$, then in particular $(a^2, bb) = 1$ iff $(a^2, b) = (a^2, b) = 1$ and $(b, a^2) = 1$ iff $(b, a) = (b, a) = 1$.
Thus, $(a^2, b^2) = 1$ iff $(a^2, b) = 1$ and $(b, a^2) = 1$ iff $(b, a) = 1$.

Since $1 = (a, b) = (b, a)$, then $(b, a) = 1$.
Since $(b, a^2) = 1$ iff $(b, a) = 1$, then we conclude $(b, a^2) = 1$, so $(a^2, b) = 1$.
Since $(a^2, b^2) = 1$ iff $(a^2, b) = 1$, then we conclude $(a^2, b^2) = 1$. $\square$

Lemma 135. *Let $a, b \in \mathbb{Z}^+$.*
If $(a, b) = 1$, then $(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$.

Proof. Suppose $(a, b) = 1$.
We prove $(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$ by induction on n.
Let $S = \{n \in \mathbb{Z}^+ : (a, b^n) = 1\}$.
Basis:
Since $1 \in \mathbb{Z}^+$ and $(a, b^1) = (a, b) = 1$, then $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{Z}^+$ and $(a, b^k) = 1$.
Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$.
From a previous lemma we know that $(a, bc) = 1$ iff $(a, b) = (a, c) = 1$ for all $a, b, c \in \mathbb{Z}$.
In particular, $(a, b^k b) = 1$ iff $(a, b^k) = (a, b) = 1$.
Since $(a, b^k) = 1$ and $(a, b) = 1$, then we conclude $(a, b^k b) = 1$.
Thus, $(a, b^{k+1}) = 1$.
Since $k + 1 \in \mathbb{Z}^+$ and $(a, b^{k+1}) = 1$, then $k + 1 \in S$.
Therefore, by PMI, $S = \mathbb{Z}^+$, so $(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$. $\square$

Lemma 136. *Let $a, b \in \mathbb{Z}^+$.*
If $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$.

Proof. Suppose $(a, b) = 1$.
We prove $(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$ by induction on n.
Let $S = \{n \in \mathbb{Z}^+ : (a^n, b^n) = 1\}$.
Basis:
Since $1 \in \mathbb{Z}^+$ and $(a^1, b^1) = (a, b) = 1$, then $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{Z}^+$ and $(a^k, b^k) = 1$.
Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$.
Since $(a, bc) = 1$ iff $(a, b) = (a, c) = 1$ for all $a, b, c \in \mathbb{Z}$, then in particular, $(a^{k+1}, b^k b) = 1$ iff $(a^{k+1}, b^k) = (a^{k+1}, b) = 1$ and $(b, a^k a) = 1$ iff $(b, a^k) = (b, a) = 1$ and $(b^k, a^k a) = 1$ iff $(b^k, a^k) = (b^k, a) = 1$.
From a previous lemma we know that if $(a, b) = 1$, then $(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$.
Since $(a, b) = 1$ and $k \in \mathbb{Z}^+$, then $(a, b^k) = 1$, so $(b^k, a) = 1$.
Since $1 = (a^k, b^k) = (b^k, a^k)$, then $(b^k, a^k) = 1$.
Since $(b^k, a^k) = 1$ and $(b^k, a) = 1$, and $(b^k, a^k a) = 1$ iff $(b^k, a^k) = (b^k, a) = 1$, then we conclude $(b^k, a^k a) = 1$.
Thus, $1 = (b^k, a^{k+1}) = (a^{k+1}, b^k)$.

From a previous lemma, we know that if $(a, b) = 1$, then $(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$.

Hence, if $(b, a) = 1$, then $(b, a^n) = 1$ for all $n \in \mathbb{Z}^+$.

Since $1 = (a, b) = (b, a)$ and $k + 1 \in \mathbb{Z}^+$, then we conclude $(b, a^{k+1}) = 1$, so $(a^{k+1}, b) = 1$.

Since $(a^{k+1}, b^k) = 1$ and $(a^{k+1}, b) = 1$, and $(a^{k+1}, b^k b) = 1$ iff $(a^{k+1}, b^k) = (a^{k+1}, b) = 1$, then we conclude $(a^{k+1}, b^k b) = 1$.

Thus, $(a^{k+1}, b^{k+1}) = 1$.

Since $k + 1 \in \mathbb{Z}^+$ and $(a^{k+1}, b^{k+1}) = 1$, then $k + 1 \in S$.

Therefore, by PMI, $S = \mathbb{Z}^+$, so $(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$. □

Exercise 137. Let $a, b \in \mathbb{Z}^+$.

If $a^n \mid b^n$, then $a \mid b$ for all $n \in \mathbb{Z}^+$.

Proof. Let $n \in \mathbb{Z}^+$.

Suppose $a^n \mid b^n$.

Let $d = \gcd(a, b)$.

Then $d \in \mathbb{Z}^+$ and $d \mid a$ and $d \mid b$, so $a = dr$ and $b = ds$ for some integers r and s.

Thus, $d = \gcd(dr, ds) = d \cdot \gcd(r, s)$.

Since $d > 0$, then we divide to obtain $1 = \gcd(r, s)$.

From a previous lemma, we know that if $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$.

Thus, if $\gcd(r, s) = 1$, then $\gcd(r^n, s^n) = 1$ for all $n \in \mathbb{Z}^+$.

Since $\gcd(r, s) = 1$, then we conclude $\gcd(r^n, s^n) = 1$ for all $n \in \mathbb{Z}^+$.

In particular, $\gcd(r^n, s^n) = 1$.

Hence, there exist integers x and y such that $xr^n + ys^n = 1$.

Since $a^n \mid b^n$, then $(dr)^n | (ds)^n$, so $d^n r^n | d^n s^n$.

Since $d \neq 0$, then we have $r^n | s^n$, so $s^n = r^n t$ for some integer t.

Thus, $1 = xr^n + y(r^n t) = r^n(x + yt)$, so $r^n | 1$.

Since $d > 0$ and $a > 0$ and $a = dr$, then $r > 0$.

Since $n > 0$, then $r^n > 0$.

Since $r \in \mathbb{Z}$, then $r^n \in \mathbb{Z}$, so $r^n \in \mathbb{Z}^+$.

Since $r^n \in \mathbb{Z}^+$ and $r^n | 1$ and the only positive integer that divides 1 is 1, then $r^n = 1$, so $r = 1$.

Thus, $a = dr = d(1) = d$.

Hence, $\gcd(a, b) = d = a$.

Since $a | b$ iff $\gcd(a, b) = a$, then we conclude $a | b$, as desired. □

The Euclidean Algorithm

Exercise 138. Express $\gcd(12378, 3054)$ as a linear combination of 12378 and 3054.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$
\begin{aligned}
12378 &= 3054 * 4 + 162 \\
3054 &= 162 * 18 + 138 \\
162 &= 138 * 1 + 24 \\
138 &= 24 * 5 + 18 \\
24 &= 18 * 1 + 6 \\
18 &= 6 * 3 + 0.
\end{aligned}
$$

Thus, $\gcd(12378, 3054) = \gcd(3054, 162) = \gcd(162, 138) = \gcd(138, 24) = \gcd(24, 18) = \gcd(18, 6) = 6$.

We backtrack through the equations to find the linear combination.

$$
\begin{aligned}
6 &= 24 - 18 * 1 \\
&= 24 - (138 - 24 * 5) * 1 \\
&= 6 * 24 - 138 \\
&= 6(162 - 138 * 1) - 138 \\
&= 6 * 162 - 7 * 138 \\
&= 6 * 162 - 7(3054 - 162 * 18) \\
&= 132 * 162 - 7(3054) \\
&= 132(12378 - 3054 * 4) - 7(3054) \\
&= 132 * 12378 - 535 * 3054.
\end{aligned}
$$

Therefore, $\gcd(12378, 3054) = 6 = 132(12378) - 535(3054)$. □

Exercise 139. Compute $\gcd(314, 159)$ as a linear combination of 314 and 159.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$
\begin{aligned}
314 &= 159 * 1 + 155 \\
159 &= 155 * 1 + 4 \\
155 &= 4 * 38 + 3 \\
4 &= 3 * 1 + 1 \\
3 &= 1 * 3 + 0.
\end{aligned}
$$

Thus, $\gcd(314, 159) = \gcd(159, 155) = \gcd(155, 4) = \gcd(4, 3) = \gcd(3, 1) = 1$.

We backtrack through the equations to find the linear combination.

$$
\begin{aligned}
1 &= 4 - 3 * 1 \\
&= 4 - (155 - 4 * 38) * 1 \\
&= -155 + 39(4) \\
&= -155 + 39(159 - 155 * 1) \\
&= 39 * 159 - 40(155) \\
&= 39 * 159 - 40(314 - 159 * 1) \\
&= (-40)(314) + 79(159).
\end{aligned}
$$

Therefore, $\gcd(314, 159) = 1 = -40(314) + 79(159)$.

Hence, a solution to the equation $314x + 159y = 1$ is $x = -40$ and $y = 79$ since $314(-40) + 159(79) = 1$. □

Exercise 140. Compute $\gcd(3141, 1592)$ as a linear combination of 3141 and 1592.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$
\begin{aligned}
3141 &= 1592 * 1 + 1549 \\
1592 &= 1549 * 1 + 43 \\
1549 &= 43 * 36 + 1 \\
43 &= 1 * 43 + 0.
\end{aligned}
$$

Thus, $\gcd(3141, 1592) = \gcd(1592, 1549) = \gcd(1549, 43) = \gcd(43, 1) = 1$.

We backtrack through the equations to find the linear combination.

$$
\begin{aligned}
1 &= 1549 - 43 * 36 \\
&= 1549 - (1592 - 1549 * 1)36 \\
&= 37 * 1549 - 1592 * 36 \\
&= 37(3141 - 1592 * 1) - 1592 * 36 \\
&= 37(3141) - 73(1592).
\end{aligned}
$$

Therefore, $\gcd(3141, 1592) = 1 = 37(314) - 73(1592)$.

Hence, a solution to the equation $3141x + 1592y = 1$ is $x = 37$ and $y = -73$, since $3141(37) + 1592(-73) = 1$. □

Exercise 141. Compute $\gcd(4144, 7696)$ as a linear combination of 4144 and 7696.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$
\begin{aligned}
7696 &= 4144 * 1 + 3552 \\
4144 &= 3552 * 1 + 592 \\
3552 &= 592 * 6 + 0.
\end{aligned}
$$

Thus, $\gcd(4144, 7696) = \gcd(4144, 3552) = \gcd(3552, 592) = 592$.
We backtrack through the equations to find the linear combination.

$$\begin{aligned} 592 &= 4144 - 3552 * 1 \\ &= 4144 - (7696 - 4144 * 1) * 1 \\ &= 2(4144) - 7696. \end{aligned}$$

Therefore, $\gcd(4144, 7696) = 592 = 2(4144) - 7696$.
Hence, a solution to the equation $4144x + 7696y = 592$ is $x = 2$ and $y = -1$, since $4144(2) + 7696(-1) = 592$. □

Exercise 142. Compute $\gcd(10001, 100083)$ as a linear combination of 10001 and 100083.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$\begin{aligned} 100083 &= 10001 * 10 + 73 \\ 10001 &= 73 * 137 + 0. \end{aligned}$$

Thus, $\gcd(10001, 100083) = \gcd(10001, 73) = 73$.
We backtrack through the equations to find the linear combination.

$$\begin{aligned} 73 &= 100083 - 10001 * 10 \\ &= -10(10001) + 100083. \end{aligned}$$

Therefore, $\gcd(10001, 100083) = 73 = -10(10001) + 100083$.
Hence, a solution to the equation $10001x + 100083y = 73$ is $x = -10$ and $y = 1$, since $10001(-10) + 100083(1) = 73$. □

Exercise 143. Find integers x, y such that $299x + 247y = 13$.

Solution. Since $\gcd(299, 247) = 13$, then we know there exist integers x and y such that $299x + 247y = 13$. Hence, there is at least one solution to the equation $299x + 247y = 13$.
We use the Euclidean algorithm to express gcd as a linear combination of integers.

$$\begin{aligned} 299 &= 247 * 1 + 52 \\ 247 &= 52 * 4 + 39 \\ 52 &= 39 * 1 + 13 \\ 39 &= 13 * 3 + 0. \end{aligned}$$

Thus, $\gcd(299, 247) = \gcd(247, 52) = \gcd(52, 39) = \gcd(39, 13) = 13$.

We backtrack through the equations to express gcd as a linear combination.

$$\begin{aligned} 13 &= 52 - 39 \\ &= 52 - (247 - 52 * 4) \\ &= -247 + 5 * 52 \\ &= -247 + 5(299 - 247) \\ &= (-6)(247) + 5 * 299. \end{aligned}$$

Therefore, $x = 5$ and $y = -6$.

Since $299(5) + 247(-6) = 1495 - 1482 = 13$, then $x = 5$ and $y = -6$ is one solution to the equation $299x + 247y = 13$.

There may be other solutions as well.

Let's find another solution to this equation.

Since $\gcd(299, 247) = 13$, then $13|299$ and $13|247$, so $299 = 13 * 23$ and $247 = 13 * 19$.

Thus, $13 = 299x + 247y = (13 * 23)x + (13 * 19)y$.

Dividing by 13 we obtain the equation $1 = 23x + 19y$.

Since 23 and 19 are relatively prime, then $\gcd(23, 19) = 1$, so there must exist integers x and y such that $23x + 19y = 1$, so we know that this equation has at least one solution.

This equation has the same solution as the equation $299x + 247y = 13$.

Thus, one solution to the equation $23x + 19y = 1$ is $x = 5$ and $y = -6$, since $23(5) + 19(-6) = 115 - 114 = 1$.

We will write a computer program to find other pair of integers x and y that are solutions to the equation $23x + 19y = 1$.

There are many solutions to this equation.

Examples are $x = -14$ and $y = 17$ and $x = 24$ and $y = -29$.

If $x = -14$ and $y = 17$, then $23(-14) + 19(17) = -322 + 323 = 1$ and $299(-14) + 247(17) = -4186 + 4199 = 13$.

If $x = 24$ and $y = -29$, then $23(24) + 19(-29) = 552 - 551 = 1$ and $299(24) + 247(-29) = 7176 - 7163 = 13$.

The equation $299x + 247y = 52$ can be reduced since $\gcd(299, 247) = 13$ by dividing by 13.

Thus, we obtain $23x + 19y = 4$. Since $\gcd(23, 19) = 1$, then this equation is saying that 4 is a linear combination of $\gcd(23, 19)$. We know that any linear combination of 23 and 19 is a multiple of $\gcd(23, 19)$. In this case, 4 is a multiple of 1 since $4 = 4 * 1$.

We will write a computer program to find x, y such that $23x + 19y = 4$ and the pair (x, y) will also be a solution to the equation $299x + 247y = 52$.

Example solutions are: $x = 1, y = -1$ and $x = 20, y = -24$ and $x = -18, y = 22$. There are many more solutions as well.

If $x = 1$ and $y = -1$, then $23(1) + 19(-1) = 4$ and $299(1) + 247(-1) = 52$.

If $x = 20$ and $y = -24$, then $23(20)+19(-24) = 4$ and $299(20)+247(-24) = 52$.

If $x = -18$ and $y = 22$, then $23(-18)+19(22) = 4$ and $299(-18)+247(22) = 52$. □

Exercise 144. Which of the integers $0, 1, ..., 10$ can be expressed in the form $12m + 20n$ where m and n are integers?

Solution. Let m and n be arbitrary integers.

Let $a = 12m + 20n$.

Let $S = \{0, 1, 2, ..., 10\}$.

The integer a is a linear combination of 12 and 20.

We know that every linear combination of 12 and 20 is a multiple of $\gcd(12, 20)$.

Since $\gcd(12, 20) = 4$, then every linear combination of 12 and 20 must be a multiple of 4.

Hence, the only integers in S which satisfy this criteria are $0, 4, 8$.

Concretely, we can use Euclidean algorithm:

$4 = 12(2) + 20(-1)$.

Thus, $8 = 2 * 4 = 2(12 * 2 - 20) = 12 * 4 - 2 * 20$.

Also, $0 = 12 * 0 + 20 * 0$. □

Exercise 145. For all integers $n > 1$, $\gcd(2n^2 + 4n - 3, 2n^2 + 6n - 4) = 1$.

Proof. Let n be an arbitrary integer such that $n > 1$.

By the Euclidean algorithm, we have

$$\begin{aligned}
2n^2 + 6n - 4 &= (2n^2 + 4n - 3)(1) + (2n - 1) \\
2n^2 + 4n - 3 &= (2n - 1)(n + 2) + (n - 1) \\
2n - 1 &= (n - 1)(2) + 1 \\
n - 1 &= 1(n - 1) + 0.
\end{aligned}$$

Therefore, by the Euclidean algorithm, $\gcd(2n^2+4n-3, 2n^2+6n-4) = 1$. □

Exercise 146. Find integers x, y, z such that $\gcd(198, 288, 512) = 198x+288y+512z$.

Solution. Let $d = \gcd(198, 288)$.

To compute $\gcd(198, 288)$ we use the Euclidean algorithm.

Observe that

$$\begin{aligned}
288 &= 198 * 1 + 90 \\
198 &= 90 * 2 + 18 \\
90 &= 18 * 5 + 0.
\end{aligned}$$

Thus,

$$\begin{aligned} d &= \gcd(198, 288) \\ &= 18 \\ &= 198 - (90) * 2 \\ &= 198 - (288 - 198 * 1) * 2 \\ &= 198 - 288 * 2 + 198 * 2 \\ &= 198 * 3 + 288(-2). \end{aligned}$$

Since $198x + 288y$ is a linear combination of 198 and 288, then $198x + 288y$ is a multiple of $\gcd(198, 288)$.

Hence, $198x + 288y = du$ for some integer u.

Observe that

$$\begin{aligned} \gcd(198, 288, 512) &= \gcd(\gcd(198, 288), 512) \\ &= \gcd(d, 512) \\ &= \gcd(18, 512). \end{aligned}$$

To compute $\gcd(18, 512)$ we use the Euclidean algorithm.

Observe that

$$\begin{aligned} 512 &= 18 * 28 + 8 \\ 18 &= 8 * 2 + 2 \\ 8 &= 2 * 4 + 0. \end{aligned}$$

Thus,

$$\begin{aligned} \gcd(18, 512) &= 2 \\ &= 18 - (8)2 \\ &= 18 - (512 - 18 * 28)2 \\ &= 18 - 512 * 2 + 18(28 * 2) \\ &= 18(57) + 512(-2). \end{aligned}$$

Therefore,

$$\begin{aligned} \gcd(198, 288, 512) &= 2 \\ &= \gcd(18, 512) \\ &= 18(57) + 512(-2) \\ &= [198(3) + 288(-2)](57) + 512(-2) \\ &= 198(3)(57) + 288(-2)(57) + 512(-2) \\ &= 198(171) + 288(-114) + 512(-2). \end{aligned}$$

Therefore, $x = 171$ and $y = -114$ and $z = -2$. $\square$

Least common multiple

Exercise 147. Compute $lcm(143, 227)$ and $lcm(306, 657)$ and $lcm(272, 1479)$.

Solution. Since $\gcd(143, 227) = 1$, then $lcm(143, 227) = 143 * 227 = 32461$.

Since $\gcd(306, 657) = 9$, then $lcm(306, 657) = \frac{306*657}{9} = 22338$.

Since $\gcd(272, 1479) = 17$, then $lcm(272, 1479) = \frac{272*1479}{17} = 23664$. □

Exercise 148. If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.

Then n is either even or odd.

We consider these two cases separately.

Case 1. Suppose n is even.

Then $n = 2k$ for some $k \in \mathbb{Z}$ and $(-1)^n = 1$.

Thus $1 + (-1)^n(2n - 1) = 1 + (1)(2 \cdot 2k - 1) = 1 + 4k - 1 = 4k$ is a multiple of 4.

Case 2. Suppose n is odd.

Then $n = 2k + 1$ for some $k \in \mathbb{Z}$ and $(-1)^n = -1$.

Thus $1 + (-1)^n(2n - 1) = 1 + (-1)(2(2k + 1) - 1) = 1 - (2(2k + 1) - 1) = 1 - (4k + 2 - 1) = 1 - (4k + 1) = 1 - 4k - 1 = -4k = 4(-k)$ is a multiple of 4. □

Exercise 149. Every multiple of 4 has form $1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$.

Proof. In conditional form, the proposition is as follows:

If k is a multiple of 4, then there is an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n - 1) = k$.

What follows is a proof of this conditional statement.

Suppose k is a multiple of 4. Then $k = 4a$ for some integer a.

We must produce an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n - 1) = k$.

We consider three cases, depending on whether a is zero, positive, or negative.

Case 1. Suppose $a = 0$.

Let $n = 1$.

Then $1 + (-1)^n(2n - 1) = 1 + (-1)(2 \cdot 1 - 1) = 0 = 4 \cdot 0 = 4a = k$.

Case 2. Suppose $a > 0$.

Let $n = 2a$, which is an element of $\mathbb{N}$ because a is positive, making n positive.

Also n is even, so $(-1)^n = 1$.

Thus $1 + (-1)^n(2n - 1) = 1 + (1)(2 \cdot 2a - 1) = 4a = k$.

Case 3. Suppose $a < 0$.

Let $n = 1 - 2a$, which is an element of $\mathbb{N}$ because a is negative, making $1 - 2a$ positive.

Also n is odd, so $(-1)^n = -1$. Thus $1 + (-1)^n(2n - 1) = 1 + (-1)(2(1 - 2a) - 1) = 1 - (1 - 4a) = 4a = k$.

These three cases show that no matter whether a multiple $k = 4a$ is zero, positive, or negative, it always equals $1 + (-1)^n(2n - 1)$ for some natural number n. □