Elementary Number Theory Examples

Jason Sass

August 18, 2025

Construction of $\mathbb{Z}$

Exercise 1. $\mathbb{Z}$ is not well-ordered.

Proof. We prove $\mathbb{Z}$ does not have a least element by contradiction.

Suppose $\mathbb{Z}$ has a least element.
Then there exists $m \in \mathbb{Z}$ such that $m \leq n$ for all $n \in \mathbb{Z}$.
Since $m \in \mathbb{Z}$, then $m - 1 \in \mathbb{Z}$.
Since $0 < 1$, then $m + 0 < m + 1$, so $m < m + 1$.
Hence, $m - 1 < m$.
Thus, $m - 1 \in \mathbb{Z}$ and $m - 1 < m$.
But, this contradicts that m is the least element of $\mathbb{Z}$.
Therefore, $\mathbb{Z}$ does not have a least element.

Since $\mathbb{Z} \subset \mathbb{Z}$ and $\mathbb{Z} \neq \emptyset$ and $\mathbb{Z}$ does not have a least element, then $\mathbb{Z}$ is not well-ordered. □

Elementary Aspects of Integers

Example 2. The number 1 is not even.

Proof. Suppose 1 is even.
Then $1 = 2k$ for some integer k.
Hence, $k = \frac{1}{2}$ is not an integer.
But, this contradicts k is an integer.
Therefore, 1 is not even. □

Proposition 3. *The sum of two even integers is even.*

Proof. Let a and b be any integers.
Suppose a is even and b is even.
Then $a = 2k$ for some $k \in \mathbb{Z}$ and $b = 2m$ for some $m \in \mathbb{Z}$.
Thus $a + b = 2k + 2m = 2(k + m)$.
Let $n = k + m$.

Then $a + b = 2n$.
Since $k \in \mathbb{Z}$ and $m \in \mathbb{Z}$, then $k + m \in \mathbb{Z}$, so $n \in \mathbb{Z}$.
Therefore, $a + b$ is even. □

Proposition 4. *The sum of two integers with opposite parity is odd.*

Proof. Let a and b be any integers.
Suppose a and b have opposite parity.
Then either a is even and b is odd, or a is odd and b is even.
We consider these cases separately.
Case 1: Suppose a is even and b is odd.
Then $a = 2k$ for some $k \in \mathbb{Z}$ and $b = 2m + 1$ for some $m \in \mathbb{Z}$.
Hence, $a + b = 2k + (2m + 1) = (2k + 2m) + 1 = 2(k + m) + 1$.
Let $n = k + m$.
Then $a + b = 2n + 1$.
Since $k \in \mathbb{Z}$ and $m \in \mathbb{Z}$, then $k + m \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition.
Thus, $n \in \mathbb{Z}$.
Therefore, $a + b$ is odd.
Case 2: Suppose a is odd and b is even.
Then $a = 2k + 1$ for some $k \in \mathbb{Z}$ and $b = 2m$ for some $m \in \mathbb{Z}$.
Hence, $a+b = (2k+1)+2m = 2k+(1+2m) = 2k+(2m+1) = (2k+2m)+1 = 2(k + m) + 1$.
Let $n = k + m$.
Then $a + b = 2n + 1$.
Since $k \in \mathbb{Z}$ and $m \in \mathbb{Z}$, then $k + m \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition.
Thus, $n \in \mathbb{Z}$.
Therefore, $a + b$ is odd. □

Proposition 5. *Let $m, n \in \mathbb{Z}$.*
Then $m + n$ is even if and only if m and n have the same parity.

Proof. We first show that if $m + n$ is even then m and n have the same parity.
We use proof by contrapositive.
Suppose m and n do not have the same parity.
Then m and n have opposite parity, so we consider two cases.
Case 1: Suppose m is even and n is odd.
Then $m = 2a$ and $n = 2b + 1$ for some $a, b \in \mathbb{Z}$.
Thus $m + n = 2a + (2b + 1) = 2(a + b) + 1$.
Therefore $m + n$ is odd, implying that $m + n$ is not even.
Case 2: Suppose m is odd and n is even.
Then $m = 2a + 1$ and $n = 2b$ for some $a, b \in \mathbb{Z}$.
Thus $m + n = (2a + 1) + 2b = 2(a + b) + 1$.
Therefore $m + n$ is odd, so $m + n$ is not even.
Either way both cases show that $m + n$ is not even.

Conversely, we show that if m and n have the same parity then $m+n$ is even.
Suppose m and n have the same parity. Then we have two cases to consider.
Case 1: Suppose m and n are both even.
Then $m = 2a$ and $n = 2b$ for some $a, b \in \mathbb{Z}$.
Thus $m + n = 2a + 2b = 2(a + b)$.
Therefore $m + n$ is even.
Case 2: Suppose m and n are both odd.
Then $m = 2a + 1$ and $n = 2b + 1$ for some $a, b \in \mathbb{Z}$.
Thus $m + n = (2a + 1) + (2b + 1) = 2(a + b + 1)$.
Therefore $m + n$ is even.
Either way both cases show that $m + n$ is even. □

Proposition 6. *For every pair of odd integers m and n, the sum $m+n$ is even and the product mn is odd.*

Proof. Let m and n be odd integers.
Since m is odd, then there exists an integer a such that $m = 2a + 1$.
Since n is odd, then there exists an integer b such that $n = 2b + 1$.
Observe that $m + n = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1)$.
Since $a + b + 1$ is an integer, then this implies $m + n$ is even.
Observe that $mn = (2a+1)(2b+1) = 4ab+2a+2b+1 = 2(2ab+a+b)+1$.
Since $2ab + a + b$ is an integer, then this implies mn is odd. □

Proposition 7. ***The product of two odd integers is odd.***
Let $m, n \in \mathbb{Z}$.
If m and n are odd, then mn is odd.

Proof. Suppose m and n are odd integers. Then $m = 2a + 1$ and $n = 2b + 1$ for $a, b \in \mathbb{Z}$.

Consequently the product $mn = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$.

Therefore $mn = 2c+1$, where $c = 2ab+a+b \in \mathbb{Z}$, so mn is odd by definition of an odd integer. □

Proposition 8. *Let m and n be integers.*
If mn is odd, then m is odd and n is odd.

Proof. We prove by contrapositive.
Suppose either m is not odd or n is not odd.
We consider these cases separately.
Case 1: Suppose m is not odd.
Then m is even, so $m = 2k$ for some integer k.
Thus, $mn = (2k)n = 2(kn)$.
Since kn is an integer, then this implies mn is even, so mn is not odd.
Case 2: Suppose n is not odd.
Then n is even, so $n = 2k$ for some integer k.
Thus, $mn = m(2k) = 2(km)$.
Since km is an integer, then this implies mn is even, so mn is not odd.
Therefore, in all cases, mn is not odd, as desired. □

Proposition 9. *Let $m, n \in \mathbb{Z}$. If m is even, then mn is even.*

Proof. Suppose m and n are integers and m is even. Then $m = 2a$ for some $a \in \mathbb{Z}$.

Thus $mn = (2a)n = 2(an) = 2b$ where $b = an \in \mathbb{Z}$.
Therefore mn is even, by definition of an even number. □

Proposition 10. *Let $n \in \mathbb{Z}^+$.*
Then n^2 is even iff n is even.

Proof. We prove if n is even, then n^2 is even.
Suppose n is even.
Then $n = 2a$ for some integer a.
Thus, $n^2 = (2a)^2 = 4a^2 = 2(2a^2)$.
Since $2a^2$ is an integer, then this implies n^2 is even, as desired.

Conversely, we prove if n^2 is even, then n is even.
We use proof by contrapositive.
Suppose n is not even.
Then n is odd, so there exists an integer b such that $n = 2b + 1$.
Thus, $n^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1$.
Since $2b^2 + 2b$ is an integer, then this implies n^2 is odd.
Therefore, n^2 is not even, as desired. □

Let $n \in \mathbb{Z}^+$.
Then n^2 is even iff n is even.
Thus, n^2 is not even iff n is not even.
Therefore, n^2 is odd iff n is odd.

Proposition 11. *If two integers have opposite parity, then their product is even.*

Proof. Suppose m and n are integers with opposite parity. Then one of them is odd while the other is even.
Without loss of generality, suppose m is even and n is odd.
Then $m = 2a$ and $n = 2b + 1$ for some $a, b \in \mathbb{Z}$.
It follows that $mn = (2a)(2b + 1) = 2(2ab + a) = 2c$ where $c = 2ab + a \in \mathbb{Z}$
Therefore mn is even, by definition of even. □

Proposition 12. ***The product of two consecutive integers is even.***
The product $n(n + 1)$ is even for every integer n.

Proof. We prove by contradiction.
Suppose the product $n(n + 1)$ is not even for every integer n.
Then there exists an integer x such that $x(x + 1)$ is not even.
Hence, $x(x + 1)$ is odd.
Thus, x is odd and $x + 1$ is odd.

Therefore, $x = 2k + 1$ and $x + 1 = 2m + 1$ for integers k and m.
Since $x + 1 = 2m + 1$, then $x = 2m$, so $2k + 1 = 2m$.
Hence, $1 = 2m - 2k = 2(m - k)$.
Since $m - k$ is an integer, then this implies 1 is even, a contradiction.
Therefore, $n(n + 1)$ is even for every integer n. □

Divisibility in $\mathbb{Z}$

Proposition 13. ***Extended version of the Division Algorithm***
Let $a, b \in \mathbb{Z}$ and $b \neq 0$.
Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.

Proof. Since $b \neq 0$, then either $b > 0$ or $b < 0$.
We consider these cases separately.
Case 1: Suppose $b > 0$.
Then $|b| = b$.
By the division algorithm, when a is divided by $b > 0$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.
Since $|b| = b$ and $0 \leq r < b$, then $0 \leq r < |b|$.
Therefore, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.
Case 2: Suppose $b < 0$.
Then $|b| = -b > 0$.
By the division algorithm, when a is divided by $-b > 0$, there exist unique integers q' and r' such that $a = -bq' + r'$ and $0 \leq r' < -b$.
Let $q = -q'$ and $r = r'$.
Then $a = -bq' + r' = b(-q') + r' = bq + r$ and $0 \leq r < -b$.
Since $|b| = -b$ and $0 \leq r < -b$, then $0 \leq r < |b|$.
Therefore, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$. □

Proposition 14. *The number -1 divides every integer. $(\forall n \in \mathbb{Z})(-1|n)$.*

Proof. Let $n \in \mathbb{Z}$.
Then $-n \in \mathbb{Z}$.
Since $-n \in \mathbb{Z}$ and $n = 1n = (-1)(-n)$, then $-1|n$. □

Proposition 15. *The only integer that zero divides is zero.*
Let $n \in \mathbb{Z}$.
Then $0|n$ iff $n = 0$.

Proof. We prove if $n = 0$, then $0|n$.
Suppose $n = 0$.
Since $0 \in \mathbb{Z}$ and $0 = 0 \cdot 0$, then $0|0$.
Since $n = 0$ and $0|0$, then $0|n$. □

Proof. Conversely, we prove if $0|n$, then $n = 0$.
Suppose $0|n$.
Then $n = 0k$ for some integer k.
Thus, $n = 0k = 0$, so $n = 0$. □

Let $n \in \mathbb{Z}$.
Then $0|n$ iff $n = 0$.
Therefore, $0 \not| n$ iff $n \neq 0$.

Greatest common divisor

Proposition 16. *The set of all divisors of* 0 *is* $\mathbb{Z}$.

Proof. Let S be the set of all divisors of 0.
Then $S = \{k \in \mathbb{Z} : k|0\}$.
We must prove $S = \mathbb{Z}$.

We prove $\mathbb{Z} \subset S$.
Let $k \in \mathbb{Z}$.
Since every integer divides zero, then k divides zero, so $k|0$.
Since $k \in \mathbb{Z}$ and $k|0$, then $k \in S$.
Therefore, $k \in \mathbb{Z}$ implies $k \in S$, so $\mathbb{Z} \subset S$.

We prove $S \subset \mathbb{Z}$.
Let $s \in S$.
Then $s \in \mathbb{Z}$ and $s|0$, so $s \in \mathbb{Z}$.
Thus, $s \in S$ implies $s \in \mathbb{Z}$, so $S \subset \mathbb{Z}$.

Since $S \subset \mathbb{Z}$ and $\mathbb{Z} \subset S$, then $S = \mathbb{Z}$. □

Lemma 17. *Let* $a, b \in \mathbb{Z}$.
Then $a|b$ *iff* $-a|b$ *iff* $a|-b$ *iff* $-a|-b$.

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

Proof. Conversely, we prove if $-a|b$, then $a|b$.
Suppose $-a|b$.
Then $b = -ak$ for some integer k.
Thus, $b = -ak = a(-k)$.
Since $-k \in \mathbb{Z}$ and $b = a(-k)$, then $a|b$. □

Proof. We prove $a|b$ iff $a|-b$.

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

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

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

Proof. Conversely, we prove if $-a|-b$, then $a|b4$.
Suppose $-a|-b$.
Then $-b = (-a)n$ for some integer n.
Thus, $b = -(-b) = -[(-a)n] = -[-(an)] = an$.
Since $n \in \mathbb{Z}$ and $b = an$, then $a|b$. □

Proposition 18. 1 ***and*** -1 ***are the only divisors of*** 1
The set of all divisors of 1 *is* $\{1, -1\}$.

Proof. Let S be the set of all divisors of 1.
Then $S = \{k \in \mathbb{Z} : k|1\}$.
Let $T = \{1, -1\}$.
We must prove $S = T$.

We first prove $S \subset T$.
Let $s \in S$.
Then $s \in \mathbb{Z}$ and $s|1$.
Since $s \in \mathbb{Z}$, then either $s > 0$ or $s = 0$ or $s < 0$.

Suppose $s = 0$.
Since $s|1$ and $s = 0$, then $0|1$.
Thus, $1 = 0k$ for some integer k.
Hence, $1 = 0k = 0$, so $1 = 0$, a contradiction.
Therefore, $s \neq 0$.

Since either $s > 0$ or $s = 0$ or $s < 0$, and $s \neq 0$, then either $s > 0$ or $s < 0$.
We consider these cases separately.
Case 1: Suppose $s > 0$.
Since $s \in \mathbb{Z}$ and $s > 0$, then $s \in \mathbb{Z}^+$.
Since $s, 1 \in \mathbb{Z}^+$ and $s|1$, then $s \leq 1$.
Since $s \in \mathbb{Z}^+$ and $0 < s \leq 1$, then $s = 1$.
Case 2: Suppose $s < 0$.
Then $-s > 0$.
By lemma 17, we know that $s|1$ iff $-s|1$.
Since $s|1$, then we conclude $-s|1$.
Since $-s \in \mathbb{Z}$ and $-s > 0$, then $-s \in \mathbb{Z}^+$.
Since $-s, 1 \in \mathbb{Z}^+$ and $-s|1$, then $-s \leq 1$.
Since $-s \in \mathbb{Z}^+$ and $0 < -s \leq 1$, then $-s = 1$, so $s = -1$.

In all cases, either $s = 1$ or $s = -1$, so either $s \in \{1\}$ or $s \in \{-1\}$.
Hence, $s \in \{1\} \cup \{-1\} = \{1, -1\} = T$, so $s \in T$.
Therefore, $s \in S$ implies $s \in T$, so $S \subset T$. □

Proof. We prove $T \subset S$.
Let $t \in T$.
Then either $t = 1$ or $t = -1$.
We consider these cases separately.
Case 1: Suppose $t = 1$.
Since $1 = 1 \cdot 1$, then $1|1$.
Since $1|1$ and $t = 1$, then $t|1$.
Since $t \in \mathbb{Z}$ and $t|1$, then $t \in S$.
Case 2: Suppose $t = -1$.
Since $1 = (-1)(-1)$, then $-1|1$.
Since $-1|1$ and $t = -1$, then $t|1$.
Since $t \in \mathbb{Z}$ and $t|1$, then $t \in S$.

Hence, in all cases, $t \in S$.
Therefore, $t \in T$ implies $t \in S$, so $T \subset S$.

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

Let $n \in \mathbb{Z}$.
If $n|1$, then $n = 1$ or $n = -1$, so $n = \pm 1$.
If $n = \pm 1$, then $n|1$.
Therefore, $n|1$ iff $n = \pm 1$.

Proposition 19. ***A nonzero integer has only finitely many divisors.***
Let $d, a \in \mathbb{Z}$.
If $d|a$ and $a \neq 0$, then $|d| \leq |a|$.

Proof. Suppose $d|a$ and $a \neq 0$.
Since $d|a$, then $a = dk$ for some integer k.

Suppose $k = 0$.
Then $a = dk = d(0) = 0$, so $a = 0$.
But, this contradicts $a \neq 0$.
Therefore, $k \neq 0$.

Since $k \in \mathbb{Z}$ and $k \neq 0$, then either $k \geq 1$ or $k \leq -1$, so $|k| \geq 1$.
Observe that

$$\begin{aligned} |a| &= |dk| \\ &= |d| \cdot |k| \\ &\geq |d| \cdot 1 \\ &\geq |d|. \end{aligned}$$

Therefore, $|a| \geq |d|$, so $|d| \leq |a|$. □

Let $a, d \in \mathbb{Z}$ and $a \neq 0$.
If $d|a$, then $0 \leq |d| \leq |a|$.
Thus, $0 \leq |d|$ and $|d| \leq |a|$.
Since $|d| \leq |a|$ iff $-|a| \leq d \leq |a|$, then we conclude $-|a| \leq d \leq |a|$.
Hence, every divisor of a is less than or equal to $|a|$, so every divisor of a nonzero integer a is less than or equal to $|a|$.
Therefore, a nonzero integer has only finitely many divisors.

Theorem 20. ***equivalent definition of gcd***
Let $a, b \in \mathbb{Z}$ with a and b not both zero.
Let $d \in \mathbb{Z}^+$.
Then $d = \gcd(a, b)$ iff
1. $d|a$ and $d|b$.
2. For every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c \leq d$.

Proof. We prove if $d|a$ and $d|b$ and for every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c \leq d$, then $d = \gcd(a, b)$.

Suppose $d|a$ and $d|b$ and for every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c \leq d$.
To prove $d = \gcd(a, b)$, we must prove d is a common divisor of a and b and any common divisor of a and b divides d.

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

We prove the statement 'any common divisor of a and b divides d'.

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

We must prove $c|d$.

Let $s = \gcd(a, b)$.

Then $s \in \mathbb{Z}^+$ and $s|a$ and $s|b$ and for every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c|s$.

Since $c|a$ and $c|b$ implies $c \leq d$ for every $c \in \mathbb{Z}$, and $s \in \mathbb{Z}$ and $s|a$ and $s|b$, then we conclude $s \leq d$.

Since $c|a$ and $c|b$ implies $c|s$ for every $c \in \mathbb{Z}$, and $d \in \mathbb{Z}$ and $d|a$ and $d|b$, then we conclude $d|s$.

Since $d \in \mathbb{Z}^+$ and $s \in \mathbb{Z}^+$ and $d|s$, then $d \leq s$.

Since $d, s \in \mathbb{Z}$ and $d \leq s$ and $s \leq d$ and $\leq$ on $\mathbb{Z}$ is anti-symmetric, then $d = s$.

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

Since any common divisor of a and b divides any linear combination of a and b, then c divides any linear combination of a and b.

Since $s = \gcd(a, b)$, then s is the least positive linear combination of a and b.

Since s is a linear combination of a and b and c divides any linear combination of a and b, then $c|s$.

Since $c|s$ and $d = s$, then $c|d$, as desired. □

Proof. Conversely, we prove if $d = \gcd(a, b)$, then $d|a$ and $d|b$ and for every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c \leq d$.

Suppose $d = \gcd(a, b)$.

We must prove $d|a$ and $d|b$ and for every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c \leq d$.

We prove $d|a$ and $d|b$.

Since $d = \gcd(a, b)$, then d is a common divisor of a and b.

Therefore, $d|a$ and $d|b$.

We prove the statement 'for every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c \leq d$'.

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

We must prove $c \leq d$.

Since $d = \gcd(a, b)$, then any common divisor of a and b divides d.

Thus, for every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c|d$.

Since $c \in \mathbb{Z}$ and $c|a$ and $c|b$, then we conclude $c|d$.

Since $c \in \mathbb{Z}$, then either $c > 0$ or $c = 0$ or $c < 0$.

Suppose $c = 0$.

Since $c|a$ and $c|b$ and $c = 0$, then $0|a$ and $0|b$.

By proposition 15, we know that $0|a$ iff $a = 0$ and $0|b$ iff $b = 0$.

Since $0|a$ and $0|a$ iff $a = 0$, then we conclude $a = 0$.

Since $0|b$ and $0|b$ iff $b = 0$, then we conclude $b = 0$.

Thus, $a = 0$ and $b = 0$.

But, by hypothesis, a and b are integers not both zero.
Therefore, $c \neq 0$.

Since either $c > 0$ or $c = 0$ or $c < 0$ and $c \neq 0$, then either $c > 0$ or $c < 0$.
We consider these cases separately.
Case 1: Suppose $c > 0$.
Since $c \in \mathbb{Z}$ and $c > 0$, then $c \in \mathbb{Z}^+$.
Since $c \in \mathbb{Z}^+$ and $d \in \mathbb{Z}^+$ and $c|d$, then $c \leq d$.
Case 2: Suppose $c < 0$.
Since $d \in \mathbb{Z}^+$, then $d > 0$.
Since $c < 0$ and $0 < d$, then $c < 0 < d$, so $c < d$.
Therefore, in all cases, $c \leq d$, as desired. □

Proposition 21. *Let* $a, b \in \mathbb{Z}^*$.
Then $\gcd(ka, kb) = |k| \cdot \gcd(a, b)$ *for all* $k \in \mathbb{Z}^*$.

Proof. Let $k \in \mathbb{Z}^*$.
Then $k \in \mathbb{Z}$ and $k \neq 0$, so either $k > 0$ or $k < 0$.
We consider these cases separately.
Case 1: Suppose $k > 0$.
Then $\gcd(ka, kb) = k \gcd(a, b) = |k| \gcd(a, b)$.
Case 2: Suppose $k < 0$.
Then $-k > 0$ and $|k| = -k$ and $k \neq 0$.
Since $k \neq 0$ and $a \neq 0$, then $ka \neq 0$.
Since $k \neq 0$ and $b \neq 0$, then $kb \neq 0$.
Observe that

$$\begin{aligned} \gcd(ka, kb) &= \gcd(-ka, -kb) \\ &= -k \cdot \gcd(a, b) \\ &= |k| \cdot \gcd(a, b). \end{aligned}$$

In all cases, we have $\gcd(ka, kb) = |k| \cdot \gcd(a, b)$, as desired. □

Definition 22. greatest common divisor of more than two integers
The greatest common divisor is the largest positive common divisor of a finite set of integers not all zero.
Let $a, b, c \in \mathbb{Z}$ with a, b, and c not all zero.
Then d is a **greatest common divisor of** a, b, **and** c iff
1. d is a positive common divisor of a, b, and c.
$d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and $d|c$.
2. Any common divisor of a, b, and c divides d.
For every $e \in \mathbb{Z}$, if $e|a$ and $e|b$ and $e|c$, then $e|d$.

Let $a, b, c \in \mathbb{Z}$ with a, b, and c not all zero.
Let d be the greatest common divisor of a, b, c.
Then $d = \gcd(a, b, c)$.

Therefore, d is a positive common divisor of a, b, c, and any common divisor of a, b, and c divides d.

Since d is a positive common divisor of a, b, c, then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and $d|c$.

Since any common divisor of a, b, and c divides d, then for every $e \in \mathbb{Z}$, if $e|a$ and $e|b$ and $e|c$, then $e|d$.

Proposition 23. $\gcd(a, b, c)$ ***property***

Let a, b, c be integers, no two of which are zero.

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

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

Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and $d|c$, and any common divisor of a, b, c divides d.

Let $e = \gcd(a, b)$.

Then $e \in \mathbb{Z}^+$ and $e|a$ and $e|b$, and any common divisor of a and b divides e.

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

Since $d|e$ and $d|c$, then d is a common divisor of e and c.

Let e' be any common divisor of e and c.

Then $e' \in \mathbb{Z}$ and $e'|e$ and $e'|c$.

Since $e'|e$ and $e|a$, then $e'|a$.

Since $e'|e$ and $e|b$, then $e'|b$.

Since $e'|a$ and $e'|b$ and $e'|c$, then e' is a common divisor of a, b, c, so $e'|d$.

Hence, any common divisor of e and c divides d.

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

Proof. Let $f = \gcd(b, c)$.

Then $f \in \mathbb{Z}^+$ and $f|b$ and $f|c$, and any common divisor of b and c divides f.

Since $d|b$ and $d|c$, then d is a common divisor of b and c, so $d|f$.

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

Let f' be any common divisor of a and f.

Then $f' \in \mathbb{Z}$ and $f'|a$ and $f'|f$.

Since $f'|f$ and $f|b$, then $f'|b$.

Since $f'|f$ and $f|c$, then $f'|c$.

Since $f'|a$ and $f'|b$ and $f'|c$, then f' is a common divisor of a, b, c, so $f'|d$.

Hence, any common divisor of a and f divides d.

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

Proof. Let $g = \gcd(a, c)$.

Then $g \in \mathbb{Z}^+$ and $g|a$ and $g|c$, and any common divisor of a and c divides g.

Since $d|a$ and $d|c$, then d is a common divisor of a and c, so $d|g$.

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

Let g' be any common divisor of g and b.

Then $g' \in \mathbb{Z}$ and $g'|g$ and $g'|b$.

Since $g'|g$ and $g|a$, then $g'|a$.

Since $g'|g$ and $g|c$, then $g'|c$.

Since $g'|a$ and $g'|b$ and $g'|c$, then g' is a common divisor of a, b, c, so $g'|d$.

Hence, any common divisor of g and b divides d.

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

Proof. Observe that

$$\begin{aligned} d &= \gcd(e, c) \\ &= \gcd(\gcd(a, b), c) \\ &= \gcd(a, f) \\ &= \gcd(a, \gcd(b, c)) \\ &= \gcd(g, b) \\ &= \gcd(\gcd(a, c), b). \end{aligned}$$

Therefore, $d = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b)$, as desired. □

Linear Diophantine Equations

Proposition 24. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$ and $c \neq 0$ and $d \in \mathbb{Z}$.*

Then the Diophantine equation $ax + by + cz = d$ is solvable in the integers iff $\gcd(a, b, c) \mid d$.

Proof. We prove the statement : if $\gcd(a, b, c) \mid d$, then $ax + by + cz = d$ is solvable in the integers.

Suppose $\gcd(a, b, c) \mid d$.

To prove $ax + by + cz = d$ is solvable in the integers, we must prove there exist integers x_0, y_0, z_0 such that $ax_0 + by_0 + cz_0 = d$.

Let $r = \gcd(a, b, c)$.

Let $s = \gcd(a, b)$.

Then $r|d$, so $d = rk$ for some integer k.

By proposition 23, $r = \gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

Thus, $r = \gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(s, c)$ is the least positive linear combination of s and c, so there exist integers m and n such that $ms+nc = r$.

Since $s = \gcd(a, b)$, then s is the least positive linear combination of a and b, so there exist integers p and q such that $pa + qb = s$.

Observe that

$$\begin{aligned} d &= rk \\ &= (ms + nc)k \\ &= [m(pa + qb) + nc]k \\ &= (mpa + mqb + nc)k \\ &= mpak + mqbk + nck \\ &= a(mpk) + b(mqk) + c(nk). \end{aligned}$$

Let $x_0 = mpk$ and $y_0 = mqk$ and $z_0 = nk$.

Then $x_0, y_0, z_0 \in \mathbb{Z}$ and $d = ax_0 + by_0 + cz_0$. □

Proof. We prove the statement: if $ax + by + cz = d$ is solvable in the integers, then $\gcd(a, b, c) \mid d$.

Suppose $ax + by + cz = d$ is solvable in the integers.

Then there exist integers x_0, y_0, z_0 such that $ax_0 + by_0 + cz_0 = d$, so d is a linear combination of a, b, c.

Since $\gcd(a, b, c)$ is a common divisor of a and b and c, then $\gcd(a, b, c)$ divides any linear combination of a and b and c, so $\gcd(a, b, c) \mid d$. □

Euclidean Algorithm

Lemma 25. ***Euclidean Algorithm lemma***

Let $a, b, q, r \in \mathbb{Z}$ such that $a = bq + r$.

Then

1. *Every common divisor of a and b divides b and r.*
2. *Every common divisor of b and r divides a and b.*
3. $\gcd(a, b) = \gcd(b, r)$.

Proof. We prove 1.

Let $c \in \mathbb{Z}$ be a common divisor of a and b.

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

Hence, $a = cs$ and $b = ct$ for some integers s and t.

Thus, $r = a - bq = cs - (ct)q = cs - ctq = c(s - tq)$.

Since $c - tq \in \mathbb{Z}$ and $r = c(s - tq)$, then $c|r$.

Therefore, $c|b$ and $c|r$. □

Proof. We prove 2.

Let $d \in \mathbb{Z}$ be a common divisor of b and r.

Then $d|b$ and $d|r$, so $b = dm$ and $r = dn$ for some integers m and n.
Thus, $a = bq + r = (dm)q + dn = dmq + dn = d(mq + n)$.
Since $mq + n \in \mathbb{Z}$ and $a = d(mq + n)$, then $d|a$.
Therefore, $d|a$ and $d|b$. □

Proof. We prove 3.
Let $e = \gcd(a, b)$.
Then e is a common divisor of a and b, and every common divisor of a and b divides e.

Since every common divisor of a and b divides b and r, and e is a common divisor of a and b, then we conclude e divides b and r, so e is a common divisor of b and r.
Let $c \in \mathbb{Z}$ be a common divisor of b and r.
Since every common divisor of b and r divides a and b, then we conclude c divides a and b, so c is a common divisor of a and b.
Since every common divisor of a and b divides e, then we conclude c divides e.
Hence, every common divisor of b and r divides e.
Since e is a common divisor of b and r, and every common divisor of b and r divides e, then $e = \gcd(b, r)$.
Therefore, $\gcd(a, b) = e = \gcd(b, r)$. □

Least common multiple

Example 26. Examples of multiples of n
The set of all multiples of 0 is the set $0\mathbb{Z} = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The set of all multiples of 1 is the set $1\mathbb{Z} = \{1k : k \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \in \mathbb{Z}\} = \mathbb{Z}$.
The set of all multiples of 2 is the set $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, ...\}$, the set of all even integers.
The set of all multiples of 3 is the set $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \pm 9, ...\}$.

Fundamental Theorem of Arithmetic

Proposition 27. *The number* 2 *is prime.*

Proof. Since 1 divides every integer, then $1|2$.
Since every integer divides itself, then $2|2$.
Since 1 and 2 are positive integers, and $1|2$ and $2|2$, then 1 and 2 are positive divisors of 2.

We prove there is no positive divisor of 2 other than 1 or 2.

Suppose there is a positive divisor of 2 other than 1 or 2.

Let c be a positive divisor of 2 other than 1 or 2.

Then $c \in \mathbb{Z}^+$ and $c|2$ and $c \neq 1$ and $c \neq 2$.

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

Since $c \geq 1$ and $c \neq 1$, then $c > 1$.

Since $c \in \mathbb{Z}^+$ and $c|2$, then $c \leq 2$.

Since $c \leq 2$ and $c \neq 2$, then $c < 2$.

Thus, $c > 1$ and $c < 2$, so $1 < c < 2$.

Hence $c \in \mathbb{Z}$ and $1 < c < 2$, so there is an integer between 1 and 2.

Since there is no integer between two consecutive integers, then there is no integer between 1 and 2.

Therefore, c does not exist, so there is no positive divisor of 2 other than 1 or 2.

Since 1 and 2 are positive divisors of 2, and there is no positive divisor of 2 other than 1 or 2, then 1 and 2 are the only positive divisors of 2.

Since $2 \in \mathbb{Z}^+$ and $2 \neq 1$, and the only positive divisors of 2 are 1 and 2, then 2 is prime. □

Proposition 28. *Any prime is greater than* 1.

Proof. Let p be a prime.

Then $p \in \mathbb{Z}^+$ and $p \neq 1$.

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

Since $p \geq 1$ and $p \neq 1$, then $p > 1$. □

Let p be a prime.

Then $p \in \mathbb{Z}^+$ and $p > 1$, so $p \geq 2$.

Hence, if p is a prime, then $p \geq 2$.

Therefore, any prime is greater than or equal to 2.

Proposition 29. *A prime is odd iff it is greater than* 2.

Proof. We prove: if a prime is odd, then it is greater than 2.

Let p be an odd prime.

Then p is prime and p is odd.

Since p is prime, then $p \in \mathbb{Z}^+$.

By proposition 28, any prime is greater than 1.

Since p is prime, then we conclude $p > 1$.

Since $p \in \mathbb{Z}^+$ and $p > 1$, then $p \geq 2$.

Since p is odd, then p is not even.

Since $2 = 2 \cdot 1$ and $1 \in \mathbb{Z}$, then 2 is even.

Since 2 is even and p is not even, then $p \neq 2$.

Since $p \geq 2$ and $p \neq 2$, then $p > 2$, as desired. □

Proof. Conversely, we prove if a prime p is greater than 2, then p is odd.

Let p be a prime greater than 2.

Then p is prime and $p > 2$.

Since $p > 2$, then $p \neq 2$.

Since p is prime, then $p \in \mathbb{Z}^+$ and the only positive divisors of p are 1 and p.

Since $2 \in \mathbb{Z}^+$ and $2 \neq 1$ and $2 \neq p$ and the only positive divisors of p are 1 and p, then 2 cannot be a positive divisor of p.

Hence, $2 \not| p$.

Therefore, p is not even, so p must be odd. □

Let p be a prime.

Then p is odd iff $p > 2$.

If p is odd, then $p > 2$.

Therefore, any odd prime is greater than 2.

If $p > 2$, then p is odd.

Therefore, any prime greater than 2 is odd.

Proposition 30. *The only even prime is* 2.

Proof. Since $2 = 2 \cdot 1$ and $1 \in \mathbb{Z}$, then 2 is even.

By proposition 27, 2 is prime.

Since 2 is prime and 2 is even, then 2 is an even prime.

Suppose p is a prime other than 2.

Then p is prime and $p \neq 2$.

Since p is prime, then $p \in \mathbb{Z}^+$.

By proposition 28, any prime is greater than 1.

Since p is prime, then we conclude $p > 1$.

Since $p \in \mathbb{Z}^+$ and $p > 1$, then $p \geq 2$.

Since $p \geq 2$ and $p \neq 2$, then $p > 2$.

By proposition 29, a prime is odd if it is greater than 2.

Since p is prime and $p > 2$, then we conclude p is odd.

Hence, p is not even.

Therefore, if p is a prime other than 2, then p is not even, so any prime other than 2 is not even.

Since 2 is an even prime, and any prime other than 2 is not even, then 2 is the only even prime. □

Proposition 31. *Let $p \in \mathbb{Z}^+$ and $p \neq 1$.*

Then p is prime iff the set of all positive divisors of p is $\{1, p\}$.

Proof. We prove if the set of all positive divisors of p is $\{1, p\}$, then p is prime.

Let S be the set of all positive divisors of p.

Then $S = \{d \in \mathbb{Z}^+ : d|p\}$.

Suppose the set of all positive divisors of p is $\{1, p\}$.

Then $S = \{1, p\}$.

Since $p \neq 1$, then S contains two distinct elements.

Since $1 \in S$, then $1 \in \mathbb{Z}^+$ and $1|p$.

Since $p \in S$, then $p \in \mathbb{Z}^+$ and $p|p$.

Since $1 \in \mathbb{Z}^+$ and $p \in \mathbb{Z}^+$ and $1|p$ and $p|p$, then 1 and p are positive divisors of p.

Suppose d is a positive divisor of p.

Then $d \in S$.

Since $S = \{1, p\}$, then $S \subset \{1, p\}$.

Since $d \in S$ and $S \subset \{1, p\}$, then $d \in \{1, p\}$, so either $d = 1$ or $d = p$.

Therefore, if d is a positive divisor of p, then $d = 1$ or $d = p$, so any positive divisor of p is 1 or p.

Since 1 and p are positive divisors of p, and any positive divisor of p is 1 or p, then 1 and p are the only positive divisors of p.

Therefore, p is prime. □

Proof. Conversely, we prove if p is prime, then the set of all positive divisors of p is $\{1, p\}$.

Suppose p is prime.

Then $p \in \mathbb{Z}^+$ and $p \neq 1$ and the only positive divisors of p are 1 and p.

Let S be the set of all positive divisors of p.

Then $S = \{d \in \mathbb{Z}^+ : d|p\}$.

We must prove $S = \{1, p\}$.

We first prove $\{1, p\} \subset S$.

Since 1 and p are positive divisors of p, then $1 \in \mathbb{Z}^+$ and $1|p$ and $p \in \mathbb{Z}^+$ and $p|p$.

Since $1 \in \mathbb{Z}^+$ and $1|p$, then $1 \in S$.

Since $p \in \mathbb{Z}^+$ and $p|p$, then $p \in S$.

Thus, $1 \in S$ and $p \in S$, so $\{1, p\} \subset S$.

We next prove $S \subset \{1, p\}$.

Let $d \in S$.

Then $d \in \mathbb{Z}^+$ and $d|p$.

Since the only positive divisors of p are 1 and p and $p \neq 1$, then d must be 1 or p, so either $d = 1$ or $d = p$.

Hence, $d \in \{1\}$ or $d \in \{p\}$, so $d \in \{1\} \cup \{p\}$.

Thus, $d \in \{1, p\}$.

Therefore, $d \in S$ implies $d \in \{1, p\}$, so $S \subset \{1, p\}$.

Since $S \subset \{1, p\}$ and $\{1, p\} \subset S$, then $S = \{1, p\}$, as desired. □

Let $p \in \mathbb{Z}^+$ and $p \neq 1$.
Then p is prime iff the set of all positive divisors of p is $\{1, p\}$.
If p is prime, then the set of all positive divisors of p is $\{1, p\}$.
If the set of all positive divisors of p is $\{1, p\}$, then p is prime.

Example 32. Any prime factorizations of a positive integer that differ only in the order of the factors are considered identical factorizations.
Observe that $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$.
While they differ only in the order of the factors, they are the same prime factorization of 12.

Example 33. Prime power factorization example
The prime power factorization of 360 is $360 = 2^3 \cdot 3^2 \cdot 5$.

Distribution of Primes

Sieve of Eratosthenes

Example 34. primes less than 100
Use the sieve of Eratosthenes to find all primes less than 100.

Solution. The primes less than 100 are:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$
□

Goldbach Conjecture

Example 35. twin primes
Since 3 and 5 are primes and $5 - 3 = 2$, then 3 and 5 are twin primes.
The first five twin prime pairs are: $(3, 5), (5, 7), (11, 13), (17, 19), (29, 31)$.

Example 36. finite sequence of consecutive composite numbers
Find 4 consecutive composite numbers.

Solution. Since $24 = 4 \cdot 6$ and $25 = 5 \cdot 5$ and $26 = 2 \cdot 13$ and $27 = 3 \cdot 9$, then $24, 25, 26, 27$ is a sequence of 4 consecutive composite numbers.

Since $32 = 4 \cdot 8$ and $33 = 3 \cdot 11$ and $34 = 2 \cdot 17$ and $35 = 5 \cdot 7$, then $32, 33, 34, 35$ is another sequence of 4 consecutive composite numbers.

Let $n = 4$
Then $(4 + 1)! + 2, (4 + 1)! + 3, (4 + 1)! + 4, (4 + 1)! + 5$ is a sequence of 4 consecutive numbers.
Thus, $5! + 2, 5! + 3, 5! + 4, 5! + 5$ is the sequence $122, 123, 124, 125$ which are all composite, since $122 = 2 \cdot 61$ and $123 = 3 \cdot 41$ and $124 = 4 \cdot 31$ and $125 = 5 \cdot 25$.
Therefore, another sequence of 4 consecutive composite numbers is $122, 123, 124, 125$.
□

Example 37. binary Goldbach conjecture
Verify the strong Goldbach conjecture for a few numbers.

Solution. Observe the following:
$4 = 2 + 2$
$6 = 3 + 3$
$8 = 3 + 5$
$10 = 3 + 7 = 5 + 5$
$12 = 5 + 7$
$14 = 3 + 11 = 7 + 7$
$16 = 3 + 13 = 5 + 11$
$18 = 5 + 13 = 7 + 11$
$20 = 3 + 17 = 7 + 13$
$22 = 3 + 19 = 5 + 17 = 11 + 11$
$24 = 5 + 19 = 7 + 17 = 11 + 13$ □

Example 38. ternary Goldbach conjecture
Verify the weak Goldbach conjecture for a few numbers.

Solution. Observe the following:
$7 = 2 + 2 + 3$
$9 = 2 + 2 + 5 = 3 + 3 + 3$
$11 = 2 + 2 + 7 = 3 + 3 + 5$
$13 = 3 + 3 + 7 = 3 + 5 + 5$
$15 = 3 + 5 + 7$
$17 = 2 + 2 + 13 = 3 + 3 + 11 = 3 + 7 + 7 = 5 + 5 + 7$
$19 = 3 + 5 + 11 = 5 + 7 + 7$
$21 = 2 + 2 + 17 = 3 + 5 + 13 = 3 + 7 + 11 = 5 + 5 + 11 = 7 + 7 + 7$ □

Example 39. some primes of the form $4n + 3$
Exhibit some primes of the form $4n + 3$ for some integer n.

Solution. Observe that
$3 = 4 \cdot 0 + 3$
$7 = 4 \cdot 1 + 3$
$11 = 4 \cdot 2 + 3$
$19 = 4 \cdot 4 + 3$
$23 = 4 \cdot 5 + 3$
$31 = 4 \cdot 7 + 3$
$43 = 4 \cdot 10 + 3$
$47 = 4 \cdot 11 + 3$.
Therefore, the primes $3, 7, 11, 19, 23, 31, 43$, and 47 are all of the form $4n + 3$. □

Example 40. Pythagorean primes
There are infinitely many primes of the form $4n + 1$.
The primes are : $5, 13, 17, 29, 37, 41, 53, 61, ...$

Proof. Let (a_n) be the arithmetic sequence defined by $a_n = 4n + 1$ and $a_0 = 1$.

Then the sequence is $1, 5, 9, 13, 17, 21, 25, 29, ...$

Since $\gcd(1, 4) = 1$, then 1 and 4 are relatively prime positive integers.

Therefore, by Dirichlet's theorem, the sequence contains infinitely many primes, so there are infinitely many primes of the form $4n + 1$. □

Example 41. There are infinitely many odd primes.

Proof. Let (a_n) be the sequence of odd positive integers given by $a_n = 2n + 1$ and $a_0 = 1$.

Then the sequence is $1, 3, 5, 7, 9, 11, 13, 15, 17, 19, ...$

Since $\gcd(1, 2) = 1$, then 1 and 2 are relatively prime.

Hence, by Dirichlet's theorem, the sequence contains infinitely many primes, so there are infinitely many primes of the form $2n + 1$.

Therefore, there are infinitely many odd primes. □

Congruences

Example 42. $ak \equiv bk \pmod{n}$ **does not imply** $a \equiv b \pmod{n}$**.**

Let n be a fixed positive integer.

Let a, b and k be any integers.

Show that $ak \equiv bk \pmod{n}$ does not necessarily imply $a \equiv b \pmod{n}$.

Solution. Let $n = 6$ and $a = 10$ and $b = 7$ and $k = 2$.

Since $10 \cdot 2 - 7 \cdot 2 = 20 - 14 = 6 = 6 \cdot 1$, then 6 divides $10 \cdot 2 - 7 \cdot 2$.

Thus, $10 \cdot 2 \equiv 7 \cdot 2 \pmod{6}$.

Since $6 \not| 3$ and $3 = 10 - 7$, then 6 does not divide $10 - 7$, so $10 \not\equiv 7 \pmod{6}$.

Therefore, $10 \cdot 2 \equiv 7 \cdot 2 \pmod{6}$, but $10 \not\equiv 7 \pmod{6}$.

Observe that $\gcd(n, k) = \gcd(6, 2) = 2 > 1$.

Since $ak \equiv bk \pmod{n}$, but $\gcd(n, k) > 1$, then $a \not\equiv b \pmod{n}$. □