Number Theory.

- deals with the set of integers ($\mathbb{Z}$), the set of positive integers ($\mathbb{N}$), and the set of rational numbers ($\mathbb{Q}$)

Axioms of $\mathbb{Z}$.
The set of integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

is equipped with two binary operations: addition and multiplication. The following are taken to be its axioms.

1. Closure: If $a, b \in \mathbb{Z}$ then $a + b, a \cdot b \in \mathbb{Z}$.
2. Commutative laws: If $a, b \in \mathbb{Z}$ then $a + b = b + a$ and $a \cdot b = b \cdot a$.
3. Associative laws: If $a, b, c \in \mathbb{Z}$ then $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
4. Distributive law: If $a, b, c \in \mathbb{Z}$ then $(a + b) \cdot c = a \cdot c + b \cdot c$.
5. Identity elements: If $a \in \mathbb{Z}$ then $a + 0 = a$ and $a \cdot 1 = a$.
6. Additive inverse: For all $a \in \mathbb{Z}$ there exists an integer solution x to the equation $a + x = 0$; this integer is denoted $-a$.
7. Cancellation law: If $a, b, c \in \mathbb{Z}$ and $c \neq 0$, then $a \cdot c = b \cdot c$ implies $a = b$.
8. Closure for the positive integers: If a, b are positive integers then $a = b$ and $a \cdot b$ are also positive integers.
9. Trichotomy law: For every integer a, exactly one of the statements $a > 0$, $a = 0$, $a < 0$ is true.
10. Well-ordering property (WOP): Every nonempty set of positive integers has a least element.

Theorem. Principle of Mathematical Induction (PMI).
Let $S \subseteq \mathbb{N}$. If $1 \in S$ and for all $n \in \mathbb{N}$, $n \in S$ implies $n + 1 \in S$, then $S = \mathbb{N}$.
Proof.
Let $S \subseteq \mathbb{N}$. Suppose that $1 \in S$ and for all $n \in \mathbb{N}$, $n \in S$ implies $n + 1 \in S$. Suppose, for the sake of contradiction, that $S \neq \mathbb{N}$. Then, $T := \mathbb{N} \setminus S$ is nonempty. By the well-ordering property, T has a least element, say t. Thus, $t \in \mathbb{N}$ and $t \neq 1$ since $1 \in S$ so that $t > 1$. Thus, $t - 1 > 0$ so that $t - 1 \in \mathbb{N}$. Since t is the least element of T, we get that $t - 1 \in S$. Since $t - 1 \in \mathbb{N}$, then $t - 1 \in S$ implies that $t \in S$. Hence, $t \notin \mathbb{N} \setminus S = T$, which is a contradiction. ■

Theorem. Strong Induction.
Let $S \subseteq \mathbb{N}$. If there exists $k \in \mathbb{N}$ such that $1, 2, \ldots, k \in S$ and for all $n \in \mathbb{N}$ such that $k \leq n$, $1, 2, \ldots, n \in S$ implies $n + 1 \in S$, then $S = \mathbb{N}$.
Proof.
Let $S \subseteq \mathbb{N}$. Suppose that there exists $k \in \mathbb{N}$ such that $1, 2, \ldots, k \in S$ and for all $n \in \mathbb{N}$ such that $k \leq n$, $1, 2, \ldots, n \in S$ implies $n + 1 \in S$. Consider the set $T := \{n \in \mathbb{N} \mid 1, 2, \ldots, n \in S\}$. Since $1, 2, \ldots, k \in S$, then $1, 2, \ldots, k \in T$. Thus, $1 \in T$. Let $n \in \mathbb{N}$. Suppose that $n \in T$. If $n < k$, then $n + 1 \leq k$ so that $n + 1 \in T$. Otherwise, $n \geq k$. Then, $1, 2, \ldots, n \in S$. Hence, by our assumption, $n + 1 \in S$. Thus, $1, 2, \ldots, n + 1 \in S$ so that $n + 1 \in T$. Therefore, by the principle of mathematical induction, $T = \mathbb{N}$. Let $m \in \mathbb{N}$. Then, $m \in T$ so that $1, 2, \ldots, m \in S$. In particular, $m \in S$. Thus, $\mathbb{N} \subseteq S$. ■

Remark.
Note that if instead of the well-ordering property, we use the principle of mathematical induction as the 10^{th} axiom, we can still prove strong induction. In fact, the well-ordering property, the principle of mathematical induction, and strong induction are equivalent to each other. So if we use any one of them as the 10^{th} axiom, we can prove the other two. The proof that they are equivalent is left as an exercise. Hint: prove PMI from WOP, prove strong induction from PMI, and prove WOP from strong induction. Note that we have already done the first two, so all that's left is to prove WOP from strong induction.

Lemma.
Let $a, b \in \mathbb{Z}$ with $b > 0$. Then, there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.
Proof.
Let $a, b \in \mathbb{Z}$ with $b > 0$. If there exists $q \in \mathbb{Z}$ such that $a = bq$ then take $r = 0$ and clearly $0 \leq 0 < b$. Otherwise, suppose that $a - bq \neq 0$ for any $q \in \mathbb{Z}$. Consider the set $S := \{a - bq \mid q \in \mathbb{Z}, a - bq > 0\}$. If $a > 0$, then $a - b \cdot 0 = a > 0$ so that $a \in S$. If $a \leq 0$,

then $a-b(-1+ab) = a+b-ab^2 = b+a(1-b^2) \geq b > 0$ since $a \leq 0$ and $1-b^2 \leq 0$, so that $a-b(-1+ab) \in S$. Thus, $S \neq \varnothing$. By the well-ordering, property, S has a least element, say $a-bq$. Take $r = a-bq > 0$. If $r \geq b$, then $a-b(q+1) = a-bq-b = r-b > 0$ so that $a-b(q+1) = a-bq$ and $a-b(q+1) \in S$, contradicting the fact that $a-bq$ is the least element of S. Thus, $0 < r < b$.
Let $q, r, s, t \in \mathbb{Z}$. Suppose that $a = bq+r$, $a = bs+t$, and $0 \leq r, t < b$. Then, $-b < -r \leq 0$ so that $-b < t-r < b$ and thus $|t-r| < b$. Also, $bq+r = bs+t$ so that $b(q-s) = t-r$. Thus, $|b(q-s)| = b \cdot |q-s| = |t-r|$. If $q-s \neq 0$ then $b > |t-r| = b \cdot |q-s| \geq b \cdot 1 = b$, which is absurd. Thus, $q-s = 0$ so that $q = s$. Therefore, $b \cdot 0 = t-r$ so that $r = t$. ■

Theorem. Division Algorithm.
Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then, there exist unique $q, r \in \mathbb{Z}$ such that $a = bq+r$ and $0 \leq r < |b|$.
Proof.
Let $a, b \in \mathbb{Z}$ with $b \neq 0$. The case $b > 0$ is simply the previous lemma. Suppose that $b < 0$. Note that $|b| = -b > 0$. Then, by the lemma, there exists $q', r' \in \mathbb{Z}$ such that $a = |b| \cdot q' + r'$ and $0 \leq r < |b|$. Take $q = -q'$ and $r = r'$, then $a = (-b)q' + r' = (-b)(-q) + r = bq + r$ and $0 \leq r < |b|$.
Let $q, r, s, t \in \mathbb{Z}$. Suppose that $a = bq+r$, $a = bs+t$, and $0 \leq r, t < |b|$. Then, $-|b| < -r \leq 0$ so that $-|b| < t-r < |b|$ and thus $|t-r| < |b|$. Also, $bq+r = bs+t$ so that $b(q-s) = t-r$. Thus, $|b(q-s)| = |b| \cdot |q-s| = |t-r|$. If $q-s \neq 0$ then $|b| > |t-r| = |b| \cdot |q-s| \geq |b| \cdot 1 = |b|$, which is absurd. Thus, $q-s = 0$ so that $q = s$. Therefore, $b \cdot 0 = t-r$ so that $r = t$. ■

Definition.
Let $a, b \in \mathbb{Z}$. We say that a divides b, denoted by $a|b$, if there exists $q \in \mathbb{Z}$ such that $b = aq$.

Theorem.
Let $a, b, c \in \mathbb{Z}$. Then the following are true.
1. If $a|1$ then $a = \pm 1$.
2. If $a|b$ and $b|c$ then $a|c$.
3. If $a|b$ and $b \neq 0$ then $|a| \leq |b|$.
4. If $a|b$ and $a|c$ then $a|(bx+cy)$ for any $x, y \in \mathbb{Z}$.

Proof.
Let $a, b, c \in \mathbb{Z}$.
1. If $a = \pm 1$ then $1 = a \cdot a$ so that $a|1$. Conversely, suppose that $a|1$. By definition, there exists $l \in \mathbb{Z}$ such that $1 = al$. Also, if $l = 0$ then $al = a \cdot 0 = 0 \neq 1$. Thus, $l \neq 0$. Then, $|l| \geq 1$. And since $1 > 0$, we have that $1 = |a| \cdot |l| \geq |a| \cdot 1$. Thus, $|a| \leq 1$ so that $a = -1, 0, 1$. But if $a = 0$ then $al = 0 \cdot l = 0 \neq 1$. Thus, $a = \pm 1$.
2. If $a|b$ and $b|c$ then $b = am$ and $c = bn$ for some $m, n \in \mathbb{Z}$. Thus, $c = (am)n = a(mn)$ where $mn \in \mathbb{Z}$. Therefore, $a|c$.
3. Suppose $a|b$ and $b \neq 0$. By definition, $b = al$ for some $l \in \mathbb{Z}$. Then, $|b| = |a| \cdot |l|$. Thus, $l \neq 0$ since otherwise, $|a| \cdot |l| = |a| \cdot 0 = 0 \neq |b|$. Thus, $|l| \geq 1$ so that $|b| \geq |a| \cdot 1 = |a|$.
4. If $a|b$ and $a|c$ then by definition, $b = am$ and $c = an$ for some $m, n \in \mathbb{Z}$. Then, $bx+cy = (am)x + (an)y = a(mx) + a(ny) = a(mx+ny)$ where $mx+ny \in \mathbb{Z}$. Thus, $a|(bx+cy)$. ■

Definition.
Let $a, b \in \mathbb{Z}$ such that not both are zero. The greatest common divisor of a and b, denoted by (a, b) or $\gcd(a, b)$, is the positive integer d such that the following are satisfied.
1. $d|a$ and $d|b$.
2. If $c|a$ and $c|b$ then $c \leq d$.

Remark.
Whenever (a, b) is mentioned here, it is under the assumption that at least one of a and b is nonzero.

Theorem. Bezout's Theorem.
Let $d = (a, b)$. Then $d = ax+by$ for some $x, y \in \mathbb{Z}$.
Proof.
Let $S = \{au+bv \mid u, v \in \mathbb{Z}, au+bv > 0\}$. S is not empty because $a^2 + b^2 \in S$. Thus, by the well-ordering property, S has a least element, say n. By the division algorithm, $a = nq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. We know that $n = ax+by$ for some $x, y \in \mathbb{Z}$. So $r = a - nq = a - (ax+by)q = a(1-xq) + byq$. Thus, $r \geq 0$ is a linear combination of a and b. If $r > 0$, then $r \in S$ and $r < n$, which contradicts the

fact that n is the least element of S. Thus, $r = 0$, so that $a = nq$ and thus $n|a$. Similarly, $n|b$. Thus, n is a common factor of a and b. Let c be a common divisor of a and b. If $c \leq 0$ then $c < n$ since n is positive. Suppose that $c > 0$. Since $c|a$ and $c|b$, then $c|(ax + by) = n$. Thus, $|c| \leq |n|$. Since $n > 0$, we get that $c \leq n$. Thus, by definition, $n = (a, b) = d$. Therefore, $d = ax + by$. ■

Definition.
If $(a, b) = 1$, we say that a and b are relatively prime.

Theorem.
a and b are relatively prime if and only if there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$.
Proof.
If $(a, b) = 1$ then by Bezout's theorem, there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$.
Suppose that $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Let $d = (a, b)$. Then, $d|a$ and $d|b$ so that $d|ax + by = 1$ and thus $d = 1$. ■

Corollary.
If $(a, b) = d$ then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
Proof.
Suppose $(a, b) = d$. By Bezout's theorem, there exist $x, y \in \mathbb{Z}$ such that $ax+by = d$. Then, $\frac{a}{d} \cdot x + \frac{b}{d} \cdot y = 1$. By a previous theorem, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. ■

Corollary.
If $a|c$ and $b|c$ and $(a, b) = 1$ then $ab|c$.
Proof.
Suppose $a|c$, $b|c$, and $(a, b) = 1$. By definition, there exist $m, n \in \mathbb{Z}$ such that $c = an$ and $c = bm$. By a theorem, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Hence, $acx + bcy = c$ so that $a(bm)x + b(an)y = c$ and $ab(mx + ny) = c$ where $mx + ny \in \mathbb{Z}$. Thus, by definition, $ab|c$. ■

Notation.
$d\mathbb{Z} = \{kd \mid \in \mathbb{Z}\}$

Theorem.
Let $d = (a, b)$. Then $d\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$.
Proof.
Let $(a, b) = d$.
Let $z \in d\mathbb{Z}$. By definition, $z = dk$ for some $k \in \mathbb{Z}$. By Bezout's theorem, $d = ax' + by'$ for some $x', y' \in \mathbb{Z}$. Hence, $dk = a(x'k) + b(y'k)$. Thus, $z = dk \in \{ax + by \mid x, y \in \mathbb{Z}\}$.
Let $z \in \{ax + by \mid x, y \in \mathbb{Z}\}$. Then $z = ax + by$ for some $x, y \in \mathbb{Z}$. Since $d|a$ and $d|b$, we get that $d|z$. So $z = kd$ for some $k \in \mathbb{Z}$. That is, $z \in d\mathbb{Z}$. ■

Euclidean Algorithm.

Lemma.
If $a = bq + r$ where $0 \leq r < b$ then $(a, b) = (b, r)$.
Proof.
Let $d = (a, b)$. Note that $r = a - bq$ is a linear combination of a and b so that $d|r$. Since $d = (a, b)$, we know that $d|b$. Suppose $c|b$ and $c|r$. Then, $c|bq + r = a$. Thus, c is a common divisor of a and b. Hence, $c \leq (a, b) = d$. By definition, $d = (b, r)$. ■

Linear Diophantine Equations.
A diophantine equation is an equation where the unknowns are integers.

Theorem.
Let $d = (a, b)$. The diophantine equation $ax + by = c$ has a solution if and only if $d|c$. If (x_0, y_0) is a particular solution, then all solutions are of the form $\left(x_0 + \frac{b}{d}t, y_0 - \frac{b}{d}t\right)$, for $t \in \mathbb{Z}$.