# MT2116: Exam notes

## Part 1: Chapters 2-7

## Chapter 2: mathematical statements, proof, logic and sets

**Mathematical statements:** An assertion that says something mathematical about the values in it. Statements can either be a:

- **Proposition:** a statement that solves for a specific value, and is either true or false.
    - From Eccles: "a proposition is a sentence that is either true or false (but not both)"
    - E.g., 20 is divisible by 4
- **Predicate:** a statement that does not specify the value of the number $n$, and whether the statement is true or false will depend on the so-called 'free variable' $n$.
    - Predicates become propositions when values are assigned to the free variable(s), and in this case they can be proven true or false.
    - E.g., $n^2$ is even

**Universal statements:** assertions about whole groups of things, for example, all natural numbers

- E.g., For every natural number $n$, the number $n^2 + n$ is even.

**Existential statements:** a statement that asserts the existence of a particular number.

- E.g., There is a natural number $n$ such that $2n = 2^n$

**Conjunction:** The combination of statements using $and$. Can be written as '$P$ and $Q$' or '$P \wedge Q$'. Both statements must be true in order for the full compound statement to be true.

**Disjunction:** The combination of statements using $or$. Can be written as '$P$ or $Q$' or '$P \vee Q$'. Only one statement needs to be true for the full compound statement to be true.

**If-then statement:** a statement that asserts that if the first part is true, then the second part must be true for the whole statement to be true. If the first part is false, then nothing can be concluded about the second part of the statement.

- Denoted by $P \Rightarrow Q$, $P$ implies $Q$

**If and only if statement (implication):** a statement that asserts that something can only be true or false when another thing is true or false

- E.g., For all natural numbers $n$, $n^2$ is even if and only if $n$ is even
- Denoted by $P \iff Q$: $P$ is equivalent to $Q$, $P$ if and only if (iff) $Q$

**Converse of a statement:** The converse of an implication (if-then statement) $P \Rightarrow Q$ is $Q \Rightarrow P$. The converse is not automatically true when the implication is, but when it is, $P \iff Q$.

**Contrapositive of a statement:** The contrapositive of the implication $P \Rightarrow Q$ is the statement $\neg Q \Rightarrow \neg P$. The contrapositive is logically equivalent to the implication.

**Proof by contradiction:** One example of this is if you want to prove that $P \Rightarrow Q$ is true. One way you can do this is show that $P$ is true but $Q$ is false (so that the statement is false), then show that this leads to a conclusion that you know is false.

# Chapter 3: natural numbers and proof by induction

**Least member of a set of natural numbers:** If $S$ is a subset of $\mathbb{N}$, then $l$ is a least member or least element of $S$ if $l \in S$ and, for all $s \in S$, $l \leq s$.

**Greatest member of a set of natural numbers:** If $S$ is a subset of $\mathbb{N}$, then $g$ is a greatest member or greatest element of $S$ if $g \in S$ and, for all $s \in S$, $g \geq s$.

**Well-ordering principle:** Every non-empty subset of $\mathbb{N}$ has a least element.

**Induction principle:** Suppose $P(n)$ is a statement involving natural numbers $n$. Then $P(n)$ is true for all $n \in \mathbb{N}$ if the following two statements are true:

i. Base case: $P(1)$ is true;

ii. Induction step: For all $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$

**Strong induction principle:** Suppose $P(n)$ is a statement involving natural numbers $n$. Then $P(n)$ is true for all $n \in \mathbb{N}$ is the following two statements are true:

i. Base case: $P(1)$ is true;

ii. Induction step: For all $k \in \mathbb{N}$, $P(s)$ being true for all $s \leq k \Rightarrow P(k+1)$

In other words, $P(1)$ will be true, $P(k)$ will be true, all of the statements between $P(1)$ and $P(k)$ will also be true, and this implies that $P(k+1)$ will also be true.

**Summation formula:** This is another way of proving by induction some quality about a sequence of numbers.

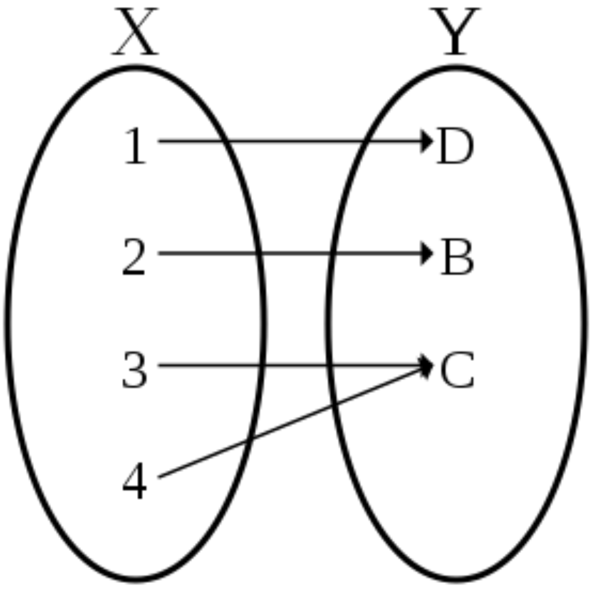
i. Base case: $\sum_{r=1}^{n} a_r = a_1$ (the summation of sequence $a_r$ from $a_1$ to $a_1$ is equal to $a_1$)

ii. Induction step: for $n \in \mathbb{N}$, $\sum_{r=1}^{n} +1a_r = (\sum_{r=1}^{n} a_r) + a_{n+1}$ (the summation of sequence $a_r$ from $a_1$ to $a_{n+1}$ is equal to the summation of sequence $a_r$ from $a_1$ to $a_n$ plus $a_{n+1}$)

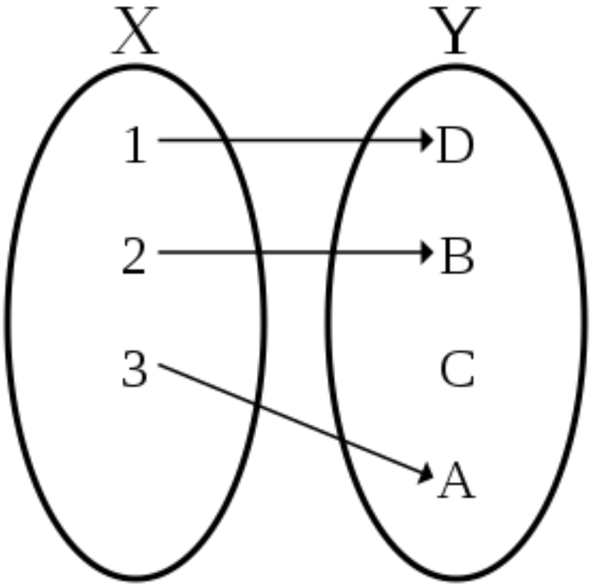
# Chapter 4: functions and counting

**Functions:** Suppose we have sets $X$ and $Y$. A **function** (or a **mapping**) from $X$ to $Y$ is a rule that associates a unique member of $Y$ to each member of $X$. We write $f : X \to Y$. The set $X$ is called the **domain** of $f$ and $Y$ is called the **codomain**. The element of $Y$ that is assigned to $x \in X$ is denoted by $f(x)$ and is called the **image** of $x$. We can write $x \mapsto f(x)$ to indicate that $x$ maps to $f(x)$.

**Surjection:** $f$ is surjective/a surjection if every $y \in Y$ is the image of some $x \in X$. In other words, $f$ is a surjection if and only if $\forall y \in Y, \exists x \in X$ s.t. $f(x) = y$.

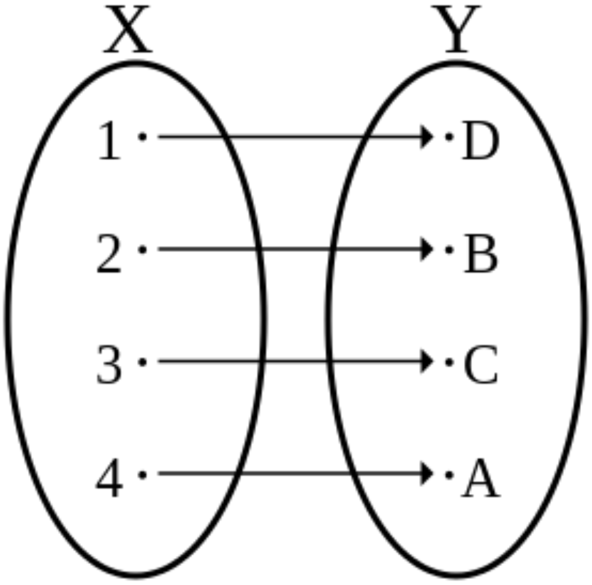


**Injection:** $f$ is injective/an injection if every $y \in Y$ is the image of at most one $x \in X$. The function is an injection if different elements of $X$ have different images ($f(x)$, or values in $Y$) under $f$. $f$ is an injection if and only if $\forall x, x' \in X, x \neq x' \Rightarrow f(x) \neq f(x')$ (for all $x$ and "not $x$" in $X$, $x$ not equaling $x'$ implies that $f(x)$ also doesn't equal $f(x')$, as each $f(x)$ is unique).



**Bijection:** $f$ is bijective/a bijection if it is both an injection and a surjection:

- Each $y \in Y$ is the image of some $x \in X$
- Each $y \in Y$ is the image of no more than one $x \in X$



**Composite functions:** Suppose we have 3 sets, $X, Y$ and $Z$ and two functions, $f : X \rightarrow Y$ and $g : Y \rightarrow Z$. Then the **composition** $gf$ (or $g \circ f$) is the function from $X$ to $Z$ given by:

$$(gf)(x) = g(f(x))(x \in X)$$

**Inverse of functions:** If we have have functions $f : X \rightarrow Y$ and $g : Y \rightarrow X$, then $g$ is an inverse function of $f$ if $(gf)(x) = x$ for all $x \in X$ and $(fg)(y) = y$ for all $y \in Y$. In other words, $y = f(x) \iff x = g(y)$. If a function has an inverse, it has only one inverse ($f^-1$).

- A function has an inverse if and only if it is a bijection. In other words, a function only has an inverse if it is bijection, and if a function is a bijection, it has an inverse.

**Cardinality of a finite set:** Suppose we have the first $m$ elements of the set of natural numbers, denoted by $\mathbb{N}_m$. A set $S$ will have $m$ members if there is a bijection from $\mathbb{N}_m$ to $S$. For $m \in \mathbb{N}$, if $S$ has $m$ members, we say that $S$ has **cardinality** $m$ (or simply, size $m$). The cardinality of $S$ is denoted by $|S|$.

**Pigeonhole principle:** For $m \in \mathbb{N}$ and $n \in \mathbb{N}$, if there is an injection from sets $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n \leq m$. (For examples and generalisations, see pp. 62-66 in the course guide.)

**Infinite sets:** A set $A$ is finite if there is some $n \in \mathbb{N}$ such that the cardinality of $A$ , $|A| = n$. Otherwise, the set is infinite.

# Chapter 5: equivalence relations and the integers

**Relations:** a relationship between ordered pairs which conforms to some rule. For example, for $m, n \in \mathbb{N}$, $m$ and $n$ are related (or $mRn$) when $m + n$ is even.

**Reflexive relations:** For a relation on a set $R$, $R$ is reflective if for all $x \in X, xRx$

**Symmetric relations:** For a relation on a set $R$, $R$ is symmetric is for all $x, y \in X, xRy \iff yRx$

**Transitive relations:** For a relation on a set $R$, $R$ is transitive if for all $x, y$ and $z \in Z$, whenever $xRy$ and $yRz$, we also have $xRz$; that is, $(xRy) \wedge (yRz) \Rightarrow xRz$.

**Equivalence relations:** An equivalence relation is reflexive, symmetric and transitive.

**Equivalence classes:** If $R$ is an equivalence relation on a set $X$, and for $x \in X$, let $[x]$ be the set of all $y \in X$ such that $yRx$. So:

$$[x] = y \in X | yRx$$

Each $[x]$ (or equivalence class) is the subset of $y \in X$, such that $y$ is related to $x$. For example, the equivalence class where $m + n$ is even has two equivalence classes, those where numbers are even, and those where number are odd.

**Equivalence classes and equivalence relations:** If $R$ is an equivalence relation on a set $X$, then:

i. For $x, y \in X$, $[x] = [y] \iff xRy$ (for all elements $x, y$ in the set $X$, the equivalence classes $[x]$ and $[y]$ are the same only when $x$ and $y$ have an equivalence relation).

ii. For $x, y \in X$, if $x$ and $y$ are not related by $R$, then $[x] \cap [y] = \emptyset$ (for all elements $x, y$ in the set $X$, if $x$ and $y$ do not share an equivalence relation then the intersection - or members that belong to both $[x]$ and $[y]$ - will be an empty set. In other words, if $x$ and $y$ are not connected via an equivalence set, they will not have any elements of set $X$ in common.)

**Integers as equivalence relation to the natural numbers:** Say that we have the set $\mathbb{N} \times \mathbb{N}$ of all ordered pairs of natural numbers. Given $(a, b)$ and $(c, d)$ in $X = \mathbb{N} \times \mathbb{N}$, let's define the equivalence relation:

$$(a, b)R(c, d) \iff a + d = b + d$$

This is an equivalence relation because:

- Reflexive: $(a, b)R(a, b) \iff a + b = b + a$, which is true
- Symmetric: $(a, b)R(c, d) \iff a + d = b + c \iff c + b = d + a \iff (c, d)R(a, b)$
- Transitive: If $(a, b)R(c, d)$ and $(c, d)R(e, f)$, then $a + d = b + c$ and $c + f = d + e$. Therefore, $(a + d) + (c + f) = (b + c) + (d + e)$, and cancelling $c$ and $d$ from each side, we get $a + f = b + e$, which means that $(a, b)R(e, f)$.

The equivalence class $[(a, b)]$ contains all $(c, d)$ for which $a + d = b + c$ . In other words, every member of the class $[(a, b)]$ is a pair whose members entered into the function $a + d = b + c$ will get the same answer. For example, the class $[(2, 1)]$ has the members $(2, 1), (3, 2), (4, 3), (5, 4)$ and this class defines the number $5$.

There are three kinds of classes:

- Those that contain a pair of the form $(n + 1, 1)$ for some $n \in \mathbb{N}$, which denote positive integers
- Those that contain a pair of the form $(1, n + 1)$ for some $n \in \mathbb{N}$, which denote negative integers
- That which contains a pair of the form $(1, 1)$, which denotes $0$.

We can do arithmetic with the integers defined in this way. For example, an addition operation:

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$

E.g.: Adding together $+3$ and $-1$, where $+3 = [(4, 1)]$ and $-1 = [(1, 2)]$, and therefore:

$$+3 + -1 = [(4, 1)] + [(1, 2)] = [(4 + 1, 1 + 2)] = [(5, 3)] = [(3, 1)] = +2$$

**Well-Ordering Principle:** For integers $x = [(a,b)]$ and $y = [(c,d)]$, we say that $x < y$ if and only if $a + d < b + c$. For a subset $S$ of $\mathbb{Z}$, $m$ is a **lower bound** for $S$ if for all $s \in S$, $m \leq s$, and $S$ is **bounded below** if it has a lower bound. The number $l$ is a **least member** of $S$ if $l \in S$, and, for all $s \in S, l \leq s$. Moreover, if $S$ is bounded below, then there is precisely one least member.

This also holds in the opposite way for **upper bounds**, **bounded above** and **greatest members**.

# Chapter 6: divisibility and prime numbers

**Divisibility:** For integers $x, y$ we say that $x$ is a multiple of $y$ or $x$ divides $y$ if, for some $q$ in $\mathbb{Z}$, $x = yq$. We use the notation $y \mid x$ to indicate that $y$ divides $x$. We use the notation $y \nmid x$ to indicate that $y$ does not divide $x$ (and thus leaves a remainder).

**Division Theorem:** For any $a$ and $b$ with $b > 0$, there are unique non-negative integers $q$ and $r$ such that:

$$\begin{aligned} a &= bq + r \\ 0 &\leq r < b \end{aligned}$$

**Integer with respect to basis:** Let $t$ be a positive integer. Then any positive integer $x$ can be represented uniquely in the form of a sequence of remainders:

$$x = r_n t^n + r_{n-1} t^{n-1} + \ldots + r_1 t + r_0$$

This can be derived using the following formula. Say that you want to represent the number $(109)_{10}$ in base 2. This number is currently in base 10. We then divide this number repeatedly by 2 to get our result:

$$\begin{aligned} 109 &= 2 \times 54 + 1 \\ 54 &= 2 \times 27 + 0 \\ 27 &= 2 \times 13 + 1 \\ 13 &= 2 \times 6 + 1 \\ 6 &= 2 \times 3 + 0 \\ 3 &= 2 \times 1 + 1 \\ 1 &= 2 \times 0 + 1 \end{aligned}$$

As you can see, we feed successive quotients as the number to solve for until they equal $0$. We can then use the remainders to represent the number in base 2: $(109)_{10} = (1101101)_2$. As you can see, you work from the bottom upwards when writing down the sequence of remainders.

**Greatest common divisor:** Suppose $a, b$ are two integers, at least one of which is not $0$. Then the greatest common divisor (gcd) of $a$ and $b$, denoted by $gcd(a, b)$, is the unique positive integer $d$ with the following properties:

i. $d$ divides both $a$ and $b$ (that is, it is a common divisor of $a$ and $b$)

ii. $d$ is greater than ever other common divisor of $a$ and $b$; that is, if $c \mid a$ and $c \mid b$, then $c \leq d$.

If the gcd of two numbers is $1$, then these numbers are **coprime**

**Euclidean algorithm:** We can use the two following properties of gcds to calculate them:

i. If $b \in \mathbb{N}$ and $a \mid b$, then $gcd(a, b) = a$, because $a$ divides both $b$ and itself

ii. For non-zero integers $a$ and $b$, if $a = bq + r$ where $q, r$ are integers, then $gcd(a, b) = gcd(b, r)$

Using these two facts, we can make successive use of the division theorem to find the $gcd$. For example, let's calculate $gcd(2247, 581)$.

$$\begin{aligned} 2247 &= 581 \times 3 + 504 \\ 581 &= 504 \times 1 + 77 \\ 504 &= 77 \times 6 + 42 \\ 77 &= 42 \times 1 + 35 \\ 42 &= 35 \times 1 + 7 \\ 35 &= 7 \times 5 \end{aligned}$$

The final $r/b$ value is the $gcd$, in this case, $gcd(2247, 581) = 7$

As you can see, the first iteration of the division theorem takes the form: $a = b_n \times q_n + r_n$, and then successive iterations take the form of $b_n = r_n \times q_{n+1} + r_{n+1}$. This continues until there is no remainder.

**gcd as integer linear combination:** Suppose $a$ and $b$ are integers (at least one of which is not 0) and let $d = gcd(a, b)$. Then there are $m, n \in \mathbb{Z}$ such that $d = am + bn$. To be clear, $d$ is the gcd that we have found using the Eucledian algorithm, $a$ is the first number we are finding a gcd for and $b$ is the second number.

See the chapter 6 notes on this on how to do it - it is quite complicated and will take a bit to memorise.

The consequence of this is also that $d \mid (ma + nb)$, and if another number $c \mid a$ and $c \mid b$ then $c \mid ma$, $c \mid nb$ and therefore $c \mid d$.

**Coprime numbers and gcd:** If $a, b \in \mathbb{N}$ are coprime, this means that $gcd(a, b) = 1$. If $a \mid r$ and $b \mid r$, then $ab \mid r$. This is because if 1 is the *greatest* common divisor, then $r$ is either going to be $ab$ or some multiple of $ab$.

**Prime numbers:** Primes are natural numbers $p \geq 2$ where the only divisors of $p$ are 1 and $p$. If $p$ is a prime number, and $a, b \in \mathbb{N}$, then $p \mid a$ or $p \mid b$. That is, if a prime divides a product of numbers, then it must divide at least one of the numbers in the product.

**Fundamental Theorem of Arithmetic:** Every integer $n \geq 2$ can be expressed as a product of one or more primes. Furthermore, there is essentially only one such way of expressing $n$: the only way in which two such expressions for $n$ can differ is in the ordering of the prime factors.

The expression of an integer as a product of primes is known as its **prime decomposition**.

# Chapter 7: congruence and modular arithmetic

**Congruence modulo** $m$: Suppose $m$ is a (fixed) natural number, and $a, b$ are integers. Let's define a relation $R$ on the integers $a, b$ if and only if $b - a$ is a multiple of $m$. That is, $aRb \iff m \mid (b - a)$.

**Congruence modulo** $m$ **as an equivalence relation:** This is an equivalence relation that divides all integers up into subsets, or equivalence classes. If $aRb$, we say that $a$ and $b$ are **congruent modulo** $m$ and write $a \equiv b \pmod{m}$. If $a$ and $b$ are not congruent modulo $m$, we write $a \not\equiv b \pmod{m}$.

**Congruence modulo** $m$ **and remainder on division:** For any integers $a$ and for any $m \in \mathbb{N}$, there are unique integers $q$ and $r$ such that: $a = qm + r$ and $0 \leq r < m$. What this means is that, if we look in the range 0, 1, $\ldots, m - 1$, there will be one number that corresponds to the remainder $r$ such that $a \equiv r \pmod{m}$. For example, say that $a = 10$ and $m = 3$. This means that $10 = 3 \times 3 + 1$, or $a \equiv 1 \pmod{m}$.

**Properties of congruence:** Suppose that $m \in \mathbb{N}$ and that $a, b, c, d \in \mathbb{Z}$ with $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:

i. $a + c \equiv b + d \pmod{m}$

ii. $a - c \equiv b - d \pmod{m}$

iii. $ac \equiv bd \pmod{m}$

iv. $\forall k \in \mathbb{Z}, ka \equiv kb \pmod{m}$

v. $\forall n \in \mathbb{N}, a^n \equiv b^n \pmod{m}$

**Congruence classes:** For a particular $x \in \mathbb{Z}$, $[x]_m$ (or the congruence classes modulo $m$) will be all the integers $y$ such that $y \equiv x \pmod{m}$. Each $x$ is congruent to one of the integers in range $0, 1, \ldots, m-1$, and that if $x \equiv y \pmod{m}$ then $[x]_m = [y]_m$. So for each $x \in \mathbb{Z}$, we'll have:

$$[x]_m = [0]_m, \text{ or } [x]_m = [1]_m, \ldots \text{ or } [x]_m = [m-1]_m$$

and we end up with $m$ equivalence classes. Each of the equivalence classes are denoted by their remainder, with $[0]_m$ indicating all $x \in \mathbb{Z}$ which have a remainder of 0 (or in other words, are divisible by $m$).

$\mathbb{Z}_m$ **and its addition and multiplication:** We can do operations with the equivalence classes, called **modular arithmetic**. For $m \in \mathbb{N}$, $\mathbb{Z}_m$ is called the set of integers modulo $m$, and is the set of equivalence classes: $[0]_m, [1]_m, \ldots, [m-1]_m$.

We can define operations $\oplus$ and $\otimes$ on $\mathbb{Z}_m$ as follows:

$$[x]_m \oplus [y]_m = [x+y]_m, [x]_m \otimes [y]_m = [xy]_m$$

Note that because congruence classes modulo $m$ are described using values of $x$ between $0, 1, \ldots, m-1$, we will always "simplify" answers down to this value. For example, when $m = 4$, $[2]_4 \oplus [3]_m = [5]_4$. As $5 \equiv 1 \pmod{4}$, the solution is $[1]_4$ .

**Negatives of elements of** $\mathbb{Z}_m$**:** For each $a \in \mathbb{Z}_m$, there is a unique element $-a \in \mathbb{Z}_m$ such that $a + (-a) = 0$. We essentially are looking for some element that when added to $a$ gives an answer in $[0]_m$. Suppose we are in $\mathbb{Z}_4$ and that $a = 3$. Then $-a = 1$, because $3 + 1 = 4 = 0$ in $\mathbb{Z}_4$. Similarly, if $a$ is a negative integer, we can "go down" to the nearest negative number in $[0]_m$ and work out what has been added to it to get that number to get it's congruence class modulo $m$. For example, in $\mathbb{Z}_9$, if $a = -4$, then we can go down to -9 and work out that we have to add 5. This indicates that $a = -4 = 5$.

**Invertible elements of** $\mathbb{Z}_m$**:** A member $x$ of $\mathbb{Z}_m$ is invertible if there is some $y \in \mathbb{Z}_m$ such that (in $\mathbb{Z}_m$) $xy = yx = 1$. If such an inverse exists it is called the inverse of $x$ and is denoted by $x^{-1}$. For example, in $\mathbb{Z}_{10}$, 3 has inverse 7 because, in $\mathbb{Z}_{10}$, $3 \times 7 = 21 \equiv 1 \pmod{10}$. If $x \in \mathbb{Z}_m$ is invertible, then it is possible to cancel $x$ from both sides of an equation in $\mathbb{Z}_m$:

$$xa = xb \Rightarrow a = b \text{ (in } \mathbb{Z}_m)$$

This works because an equation containing $x$ can be multiplied on both sides by its inverse, which then simplifies to 1.

**Coprime and inversion:** Suppose $m \in \mathbb{N}$, then an element $x$ of $\mathbb{Z}_m$ is invertible if and only if $x$ and $m$ are coprime (that is, $gcd(x, m) = 1$).

**Linear equations in $\mathbb{Z}_m$:** Suppose we want to solve the equation $ax = b$ in $\mathbb{Z}_m$. We use the Euclidean algorithm in the following way: we start with the form $m = a \times q + r$, and then solve as per usual. We then work backwards in order to obtain a solution for $x$. Finally, we reduce this number in $\mathbb{Z}_m$.

In $\mathbb{Z}_m$, $ax = b$ has a solution if and only if $d \mid b$, where $d = gcd(a, m)$. This suggests a general method for solving $ax = b$ in $\mathbb{Z}_m$:

- Find $d = gcd(a, m)$
- If $d \nmid b$, there's no solution
- If $d \mid b$, write $b = db_1$. Use Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that $d = xa + ym$. Then the solution is $xb_1$, reduced modulo $m$.

**Systems of linear equations in $\mathbb{Z}_m$:** You can solve two equations simultaneously by adding and subtracting the two equations and attempting to solve for the resulting equations. There may be several solutions, or none.