**Undergraduate Topics in Mathematics (3)**
Proof writing, Axiomatic geometry, Numerical analysis

**Nathan Warner**


Northern Illinois
University

Computer Science
Northern Illinois University
United States

## Contents

# Proofs

## 1.1 Intro to proof writing, intuitive proofs

- **Intro to definitions, propositions and proofs: the chessboard problem**: Suppose you have a chessboard (8×8 grid of squares) and a bunch of dominoes (2×1 block of squares), so each domino can perfectly cover two squares of the chessboard.

  Note that with 32 dominoes you can cover all 64 squares of the chessboard. There are many different ways you can place the dominoes to do this, but one way is to cover the first column by 4 dominoes end-to-end, cover the second column by 4 dominoes, and so on

  Math runs on definitions, so let's give a name to this idea of covering all the squares. Moreover, let's not define it just for $8 \times 8$ boards — let's allow the definition to apply to boards of other dimensions

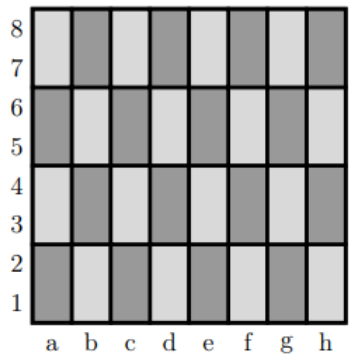
  **Definition.** A perfect cover of an $m \times n$ board with $2 \times 1$ dominoes is an arrangement of those dominoes on the chessboard with no squares left uncovered, and no dominoes stacked or left hanging off the end.

  As we demonstrated above, there exist perfect covers of the $8 \times 8$ chessboard. This is a book about proofs, so let's write this out as a proposition (something which is true and requires proof) and then let's write out a formal proof of this fact.

  **Proposition.** There exists a perfect cover of an $8 \times 8$ chessboard.

  This proposition is asserting that "there exists" a perfect cover. To say "there exists" something means that there is at least one example of it. Therefore, any proposition like this can be proven by simply presenting an example which satisfies the statement.

  ***Proof.*** Observe that the following is a perfect cover.




  We have shown by example that a perfect cover exists, completing the proof. ■

We typically put a small box at the end of a proof, indicating that we have completed our argument. This practice was brought into mathematics by Paul Halmos, and it is sometimes called the Halmos tombstone

One apocryphal story is that Halmos regarded proofs as living until proven. Once proven, they have been defeated — killed. And so he wrote a little tombstone to conclude his proof

What if I cross out the bottom-left and top-left squares, can we still perfectly cover the 62 remaining squares?

As you can probably already see, the answer is yes. For example, the first column can now be covered by 3 dominoes and the other columns can be covered by 4 dominoes each.

What if I cross out just one square, like the top-left square? Can this be perfectly covered?

The answer is no

**Proposition.** If one crosses out the top-left square of an $8 \times 8$ chessboard, the remaining squares can not be perfectly covered by dominoes.

**Proof Idea**. The idea behind this proof is that one domino, wherever it is placed, covers two squares. And two dominoes must cover four squares. And three cover six. In general, the number of squares covered — 2, 4, 6, 8, 10, etc. — is always an even number. This insight is the key, because the number of squares left on this chessboard is 63— an odd number

***Proof.*** Since each domino covers 2 squares and the dominoes are non-overlapping, if one places our k dominoes on the board, then they will cover $2k$ squares, which is always an even number. Therefore, a perfect cover can only cover an even number of squares. Notice, though, that the board has 63 remaining squares, which is an odd number. Thus, it can not be perfectly covered.

What if I take an $8 \times 8$ chessboard and cross out the top-left and the bottom-right squares? Then can it be covered by dominoes?

**Proposition.** If one crosses out the top-left and bottom-right squares of an $8 \times 8$ chessboard, the remaining squares can not be perfectly covered by dominoes.

***Proof.*** Observe that the chessboard has 62 remaining squares, and since every domino covers two squares, if a perfect cover did exist it would require

$$\frac{62}{2} = 31 \text{ dominoes.}$$

Also observe that every domino on the chessboard covers exactly one white square and exactly one black square

Thus, whenever you place 31 non-overlapping dominoes on a chessboard, they will collectively cover 31 white squares and 31 black squares.

Next observe that since both of the crossed-out squares are white squares, the remaining squares consist of 30 white squares and 32 black squares. Therefore, it is impossible to have 31 dominoes cover these 62 squares. ■

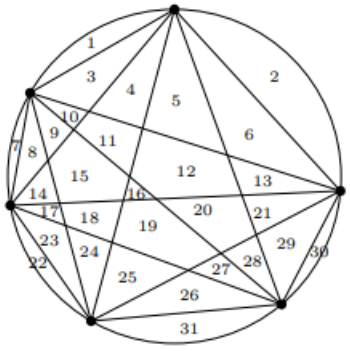
- **Naming Results**: So far, all of our results have been called "propositions." Here's the run-down on the naming of results:
  - A theorem is an important result that has been proved.
  - A proposition is a result that is less important than a theorem. It has also been proved.
  - A lemma is typically a small result that is proved before a proposition or a theorem, and is used to prove the following proposition or theorem.
  - A corollary is a result that is proved after a proposition or a theorem, and which follows quickly from the proposition or theorem. It is often a special case of the proposition or theorem.

  All of the above are results that have been proved — a conjecture, though, has not.
  - A conjecture is a statement that someone guesses to be true, although they are not yet able to prove or disprove it.
- **Conjectures and counterexamples**: As an example of a conjecture, suppose you were investigating how many regions are formed if one places $n$ dots randomly on a circle and then connects them with lines.

$n = 1$ 1 region | $n = 2$ 2 regions | $n = 3$ 4 regions | $n = 4$ 8 regions | $n = 5$ 16 regions

At this point, if you were to conjecture how many regions there will be for the $n = 6$ case, your guess would probably be 32 regions — the number of regions certainly seems to be doubling at every step. In fact, if it kept doubling, then with a little more thought you might even conjecture a general answer: that n randomly placed dots form $2^{n-1}$ regions;

Surprisingly, this conjecture would be incorrect. One way to disprove a conjecture is to find a counterexample to it. And as it turns out, the $n = 6$ case is such a counterexample




$n = 6$
31 regions

This counterexample also underscores the reason why we prove things in math. Sometimes math is surprising. We need proofs to ensure that we aren't just guessing at what seems reasonable. Proofs ensure we are always on solid ground. Further, proofs help us understand why something is true — and that understanding is what makes math so fun

Lastly, we study proofs because they are what mathematicians do

- **The pingeonhole principle**

**Principle**. The principle has a simple form and a general form. Assume $k$ and $n$ are positive integers

**Simple form:** If $n + 1$ objects are placed into $n$ boxes, then at least one box has at least two objects in it.

**General form:** If $kn + 1$ objects are placed into $n$ boxes, then at least one box has at least $k + 1$ objects in it.

**Birthday example**: If there are 330 million people in the united states, how many U.S. residents are guaranteed to have the same birthday according to the pigeonhole principle?

To determine this, let's see what would happen if each date of the year had exactly the same number of people born on it

$$\frac{330 \times 10^6}{366} = 901,639.344.$$

Since 901,639.344 people are born on an average day of the year, we should be able round up and say that at least one day of the year has had at least 901,640 people born on it. That is, with the pigeonhole principle we should be able to prove that there are at least 901,640 people in the USA with the same birthday

**Solution.** Imagine you have one box for each of the 366 dates of the (leap) year, and each person in the U.S. is considered an object. Put each person in the box corresponding to their birthday. By the general form of the pigeonhole principle (with $n = 366$ and $k = 901,639$ and thus $k + 1 = 901,640$), any group of

$$(901,639)(366) + 1.$$

people is guaranteed to contain 901,640 people which have the same birthday.

- **Another pingeonhole example**:

  **Proposition.** Given any five numbers from the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$, two of the chosen numbers will add up to 9.

  We may think to start by listing the pairs that sum to 9. We have

  $$1 + 8$$
  $$2 + 7$$
  $$3 + 6$$
  $$4 + 5.$$

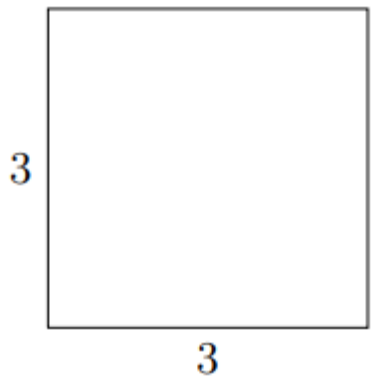
  And of course $8 + 1, 7 + 2, ..$ etc. We see we have four sums, we choose these sums as our boxes. If each of the four sums is a box, and each number is an object, then we are placing five objects into four boxes

  **Proof.** Let one box correspond to the numbers 1 and 8, a second box correspond to 2 and 7, another to 3 and 6, and a final box to 4 and 5. Notice that each of these pairs adds up to 9.

  Given any five numbers from $\{1, 2, 3, 4, 5, 6, 7, 8\}$, place each of these five numbers in the box to which it corresponds; for example, if your first number is a 6, then place it in the box labeled "3 and 6." Notice that we just placed five numbers into four boxes. Thus, by the simple form of the pigeonhole principle, there must be some box which contains two numbers in it. These two numbers add up to 9, as desired

- **Another pingeonhole example**:

  **Proposition.** Given any collection of 10 points from inside the following square (of side-length 3), there must be at least two of these points which are of distance at most $\sqrt{2}$



**Proof.** Divide the $3 \times 3$ square into nine $1 \times 1$ boxes. Placing 10 arbitrary points amongst the boxes gaurantees that at least one box will have at least two points. We observe that the farthest these two points can be from each other is when they sit in two corners such that a diagonal line through the box hits both points. The length of this line is given by

$$\sqrt{1^2 + 1^2} = \sqrt{2}.$$

Thus, we observe that the maximum distance of these two points is $\sqrt{2}$ ■

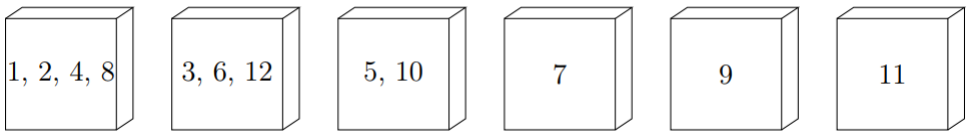
- **Another pingeonhole example**:

**Proposition.** Given any 101 integers from $\{1, 2, 3, ..., 200\}$, at least one of these numbers will divide another

**Solution.** As we ponder about how to construct 100 boxes from the properties of the set, we may wonder how the even and odd members partition this set. Call $S = \{1, 2, 3, ..., 200\}$, $E = \{2, 4, 6, ..., 200\}$, and $O = \{1, 3, 5, ..., 199\}$. Note that $E \cup O = S$. We notice that these two sets are arithmetic sequences, each with difference two. If $a_n = a_1 + (n-1)d$, then

$$\begin{aligned} n &= \frac{a_n - a_1}{2} + 1 \\ \implies n &= 100. \end{aligned}$$

Let's make the odd numbers are boxes. We note that any even number $\ell$ can be written as $\ell = 2^k m$, where $m$ is odd, and $k$ is the highest power of two that divides $\ell$. Thus, in box $m$, we place any number of the form $2^k m$




For any pair of numbers in the same box, the smaller divides the larger. Picking 101 numbers from the set $S$, and only 100 boxes... by the pigeonhole principle we must have atleast two numbers in the same box, and thus the smaller divides the larger. ■.

**Formal proof. Proof.** For each number $n$ from the set $\{1, 2, 3, \ldots, 200\}$, factor out as many 2's as possible, and then write it as $n = 2^k \cdot m$, where $m$ is an odd number. So, for example, $56 = 2^3 \cdot 7$, and $25 = 2^0 \cdot 25$. Now, create a box for each odd number from 1 to 199; there are 100 such boxes.

Remember that we are given 101 integers and we want to find a pair for which one divides the other. Place each of these 101 integers into boxes based on this rule:

If the integer is $n$, then place it in Box $m$ if $n = 2^k \cdot m$ for some $k$.

For example, $72 = 2^3 \cdot 9$ would go into Box 9, because that's the largest odd number inside it.

Since 101 integers are placed in 100 boxes, by the pigeonhole principle (Principle 1.5) some box must have at least 2 integers placed into it; suppose it is Box $m$. And suppose these two numbers are $n_1 = 2^k \cdot m$ and $n_2 = 2^\ell \cdot m$, and let's assume the second one is the larger one, meaning $\ell > k$. Then we have now found two integers where one divides the other; in particular $n_1$ divides $n_2$, because:

$$\frac{n_2}{n_1} = \frac{2^\ell \cdot m}{2^k \cdot m} = 2^{\ell - k}.$$

This completes the proof.■

- **Another pigeonhole example**

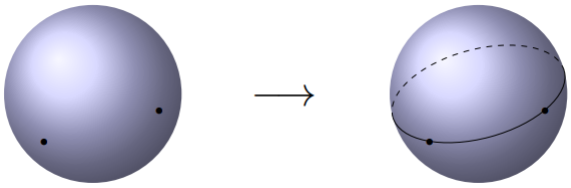
  **Proposition**. Suppose $G$ is a graph with $n \geqslant 2$ vertices. Then $G$ contains two vertices which have the same degree.

  We start by observing that the minimum degree is zero, and the maxmium is $n - 1$. It could happen that a vertex is connected to no other vertices, and a vertex could be connected to all other vertices. If a vertex is connected to all other vertices, than it has degree $n - 1$, because it has an edge going to all vertices but itself. Thus, we have our boxes. But you may notice that we have $n$ boxes for $n$ vertices. This may seem like a problem, but after some thought you may see that it is not possible for the zero box and the $n - 1$ box to both be used for a specific graph $G$. Thus, we have only $n - 1$ boxes for $n$ vertices.

  The rest of the proof is left as an exercise for the reader.

- **Classic Geometry Theorem**. Given any two points on the sphere, there is a great circle that passes through those two points.

  Given a sphere, there are infinitely many ways to cut it in half, and each of these paths of the knife is called a great circle



- **Final pigeonhole example**

  **Proposition**. If you draw five points on the surface of an orange in marker, then there is always a way to cut the orange in half so that four points (or some part of the point) all lie on one of the halves.

***Proof***. Consider an orange with five points drawn on it. Pick any two of these points, and call them $p$ and $q$. By the Classic Geometry Theorem, there exists a great circle passing through these points; angle your knife to cut along this great circle. Because the points are drawn in marker, they are wide enough so that part of these two points appear on both halves.

Now consider the remaining three points and the two halves that you just cut the orange into. Consider these three points to be objects and the halves to be boxes; by the simple form of the pigeonhole principle, at least two of these three points are on the same orange half. These two, as well a portion of $p$ and of $q$, give four points or partial points, as desired ■

## 1.2 Direct proofs

- **Fact about integers**: The sum of integers is an integer, the difference of integers is an integer, and the product of integers is an integer. Also, every integer is either even or odd.

  We are calling these facts because, while they are true and one could prove them, we will not be proving them here

- **Even and odd integers**: An integer $n$ is *even* if $n = 2k$ for some integer $k$

  An integer $n$ is *odd* if $n = 2k + 1$ for some integer $k$

- **Sum of two even integers**

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

  ***Proof.*** Assume $n$ and $m$ are even integers, then $n = 2a$, and $m = 2b$ for some integers $a$ and $b$. Furthermore,

  $$n + m = 2a + 2b = 2(a + b).$$

  Since the sum of two integers is itself an integer, then we have two times an integer, which satisfies the definition of an even number. Hence, the sum $n + m$ is even, where $n$ and $m$ are even. $\int$

- **More on propositions**: We can rewrite our propositions to take the form

  > if *statement* is true, then *other statement* is also true

  For example,

  > if $m$ and $n$ are even, then $m + n$ is also even

  Another way to summarize such statements is this:

  > *some statement* is true implies *some other statement* is true.

  Which allows us to use the implies symbol $\implies$. For example,

  > $m$ and $n$ being even $\implies$ $m + n$ is even

  We have the general form $P \implies Q$, where $P$ and $Q$ are statements

  However, when writing formally, like when writing up the final draft of your homework, these symbols are rarely used. You should write out solutions with words, complete sentences, and proper grammar. Pick up any of your math textbooks, or look online at math research articles, and you will find that such practices are standard.

- **The structure of direct proofs**: A direct proof is a way to prove a "$P \Rightarrow Q$" proposition by starting with $P$ and working your way to $Q$. The "working your way to $Q$" stage often involves applying definitions, previous results, algebra, logic, and techniques. Here is the general structure of a direct proof:

**Proposition**. $P \implies Q$

***Proof.*** Assume $P$

*Explain what $P$ means by applying definitions and/or other results*

$\vdots$ Apply algebra,

$\vdots$ logic techniques.

*Hey look, that's what $Q$ means*

Therefore $Q$ ■

- **Proof by cases**: A related proof strategy is proof by cases. This is a "divide and conquer" strategy where one breaks up their work into two or more cases

The below example of proof by cases will also give us more practice with direct proofs involving definitions. Indeed, when you break up a problem in two parts, those two parts still need to be proven, and a direct proof is often the way to tackle each of those parts

**Proposition.** If $n$ is an integer, then $n^2 + n + 6$ is even.

***Proof.*** Assume $n$ is an integer, then either $n$ is even or it is odd.

*Case I.* Assume $n$ is even, then $n = 2m$ for some integer $m$. Thus, we have

$$\begin{aligned} n^2 + n + 6 &= (2m)^2 + 2m + 6 \\ &= 4m^2 + 2m + 6 \\ &= 2(2m^2 + m + 3). \end{aligned}$$

Observe that $2m^2 + m + 3 \in \mathbb{Z}$. Thus, we have two times an integer, which satisfies the definition of an even number.

*Case 2.* Assume $n$ is odd, then $n = 2m + 1$ for some integer $m$. Thus,

$$\begin{aligned} n^2 + n + 6 &= (2m + 1)^2 + 2m + 1 + 6 \\ &= 4m^2 + 4m + 1 + 2m + 7 \\ &= 4m^2 + 6m + 8 \\ &= 2(2m^2 + 3m + 4). \end{aligned}$$

Since $m$ is an integer, $2m^2 + 3m + 4$ is an integer, and we again have two times an integer, which is an even integer.

We have shown that $n^2 + n + 6$ is even whether $n$ is even or odd. Combined, this shows that $n^2 + n + 6$ is even for all integers $n$ ■

- **Proof by exhaustion (brute force proof)**: A proof by cases cuts up the possibilities into more manageable chunks. If the theorem refers to a collection of elements and your proof is simply checking each element individually, then it is called a *proof by exhaustion* or a *brute force proof*

- **Divisibility**: An integer $a$ is said to divide an integer $b$ if $b = ak$ for some integer $k$. When $a$ does divide $b$, we write $a \mid b$, and when $a$ does not divide $b$, we write $a \nmid b$.

  **Note:** A common mistake is to see something like "$2 \mid 8$" and think that this equals 4. The expression "$a \mid b$" is either true or false

  **Remark.** $a \mid 0$ for any integer $a$, because $0 = a \cdot 0$ for every such $a$

  $0 \nmid b$ for any nonzero integer $b$, because for any such $b$, we have $b \neq 0 \cdot k$ for any integer $k$

- **The transitive property of divisibility**:

  **Proposition**. Let $a, b$, and $c$ be integers, if $a \mid b$ and $b \mid c$, then $a \mid c$

  ***Proof.*** Assume $a, b$, and $c$ are integers. Further assume that $a \mid b$, and $b \mid c$

  > By the definition of divisibility, $a \mid b$ and $b \mid c$ implies $b = ak$ for some integer $k$, and $c = bs$ for some integer $s$
  >
  > If $a \mid c$, we require that $c = ar$ for some integer $r$

  $$\begin{aligned} & b = ak \\ \implies & c = (ak)s \\ \implies & c = a(ks). \end{aligned}$$

  Since $k$ and $s$ are integers, then their product $ks$ is itself an integer. Let $r = ks$. Then $c = ar$, which is precisely the definition of divisiblity, and we conclude that $a \mid c$. ■

- **The division algorithm**:

  **Theorem.** For all integers $a$ and $m$ with $m > 0$, there exist unique integers $q$ and $r$ such that

  $$a = mq + r.$$

  Where $0 \leqslant r < m$. We call $q$ the *quotient* and $r$ the *remainder*

- **Common divisor, greatest common divisor**: Let $a$ and $b$ be integers. If $c \mid a$ and $c \mid b$, then $c$ is said to be a common divisor of $a$ and $b$.

  The greatest common divisor of $a$ and $b$ is the largest integer $d$ such that $d \mid a$ and $d \mid b$. This number is denoted $\gcd(a, b)$.

Note that there is one pair of integers that does not have a greatest common divisor; if $a = 0$ and $b = 0$, then every positive integer $d$ is a common divisor of $a$ and $b$. This means that no divisor is the greatest divisor, since you can always find a bigger one. Thus, in this one case, $gcd(a, b)$ does not exist

- **Bezout's identity**: If $a$ and $b$ are positive integers, then there exist integers $k$ and $\ell$ such that

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

As an example, suppose $a = 12$ and $b = 20$, then $\gcd(12, 20) = 4$, and we have

$$\begin{aligned} 4 &= 12k + 20\ell \\ \implies \ell &= \frac{1}{5} - \frac{3}{5}k. \end{aligned}$$

Let $k = 2$, then we see $\ell = -1$. We see that there are infinitely many solutions, $k = 2, \ell = -1$ is just one of them. Nevertheless, this theorem simply says that at least one solution must exist.

***Proof.*** Assume $a$ and $b$ are fixed positive integers, notice that the expression $ax + by$ can take many values for integers $x$ and $y$. Let $d$ be the *smallest positive integer* that $ax + by$ can be equal. Let $k$ and $\ell$ be the $x$ and $y$ that obtain this $d$. That is,

$$d = ak + b\ell.$$

We now must show that $d$ is a common divisor of $a$ and $b$, and then that it is the *greatest common divisor*

*Part 1 (common divisor).* $d$ is a common divisor of $a$ and $b$ if $d \mid a$ and $d \mid b$. To see that $d \mid a$, we examine the division algorithm. We know that there exsits unique integers $q$ and $r$ such that

$$a = dq + r.$$

With $0 \leqslant r < d$. We have

$$\begin{aligned} r &= a - dq \\ &= a - (ak + b\ell)q \\ &= a - akq - b\ell q \\ &= a(1 - kq) + b(-\ell q). \end{aligned}$$

Observe that $1 - kq$, and $-\ell q$ are both integers, Since $r$ is written in the form $ax + by$, $0 \leqslant r < d$, and $d$ is the smallest positive integer that this form can produce (with the given $a, b$), it must be that $r = 0$. Thus,

$$a = dq + 0 = dq.$$

And we see that $d \mid a$. A similar argument will show that $d \mid b$ as well. This proves that $d$ is a common divisor of $a$ and $b$.

*Part 2 (gcd).* Assume that $d'$ is some other common divisor of $a$ and $b$. We must show that $d' \leqslant d$. If $d'$ is a common divisor of $a$ and $b$, then $d' \mid a$ and $d' \mid b$, which implies $a = d'n$, and $b = d'm$, for some integers $n$ and $m$. If $d = ak + b\ell$, then

$$\begin{aligned} d &= d'nk + d'm\ell \\ &= d'(nk + m\ell) \\ \implies d' &= \frac{d}{nk + m\ell}. \end{aligned}$$

Since $n, k, m, \ell \in \mathbb{Z}$, it follows that $nk + m\ell \in \mathbb{Z}$. Thus, $d' \leqslant d$.

Therefore, we have shown that $d$ is not only a common divisor of $a$ and $b$, but that it is also the largest, and hence the *gcd*. Thus,

$$\gcd(a, b) = d = ak + b\ell.$$

■

A corollary from this result is that $\gcd(ma, mb) = m \gcd(a, b)$. If $\gcd(a, b) = ak + b\ell$, we have

$$\begin{aligned} (ma, mb) &= mak + mb\ell \\ &= m(ak + b\ell) \\ &= m \gcd(a, b). \end{aligned}$$

- **Modulo and congruence**: For integers $a$, $r$, and $m$, we say that $a$ is congruent to $r$ modulo $m$ and we write $a \equiv r \pmod{m}$ if $m \mid (a - r)$.

  For example, $18 \equiv 4 \pmod{7}$ because $18 = 7(2) + 4$, we see that $7 \mid (18 - 4)$

  If $a$ divided by $m$ leaves a remainder of $r$, then $a \equiv r \pmod{m}$. However, this is not the only way to have $a \equiv r \pmod{m}$ — it is not required that $r$ be the remainder when $a$ is divided by $m$; all that is required is that $a$ and $r$ have the same remainder when divided by $m$. For example:

$$18 = 11 \pmod{7}.$$